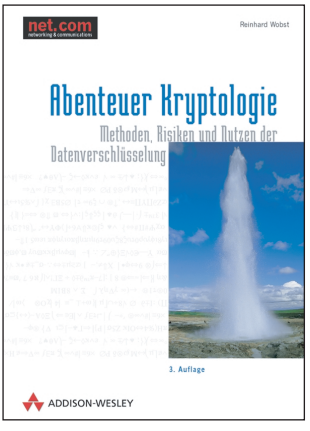
Handbuch IT-Sicherheit

Strategien, Grundlagen und Projekte

net.com
networking & communications

Netzwerke, Sicherheit, Telekommunikation ... zu diesen Themen bietet Ihnen net.com umfassende, praxisnahe Information. Beschrieben werden Standards, Protokolle, Technologien und Tools. Die Autoren geben ihr praxiserprobtes Wissen weiter und helfen Ihnen auf diese Weise, die Vorteile von Technologien und Konzepten zu bewerten und Probleme bei der täglichen Arbeit effizient zu lösen.



Abenteuer Kryptologie

Reinhard Wobst
456 Seiten
*€ **39,95** [D] - € **41,10** [A] - sFr **73,00***
*ISBN **3-8273-1815-7***

Die dritte Auflage des Standardwerks ist wesentlich überarbeitet und aktualisiert worden. Neu ist u.a. der Rijndael-Algorithmus, die DES-Crack-Maschine der EEF, praktisch wirksame Angriffe auf Handy-Authentifizierung, mehr Details zu ECHELON, Überlegungen zur Biometrie u.v.a.m.

Hackerabwehr und Datensicherheit

Avi Rubin
342 Seiten
*€ **39,95** [D] - € **41,10** - sFr **73,00***
*ISBN **3-8273-1941-2***

Als Sicherheitsexperte von AT&T kennt Avi Rubin alle Tricks der Hacker und Datenschnüffler. Der Leser lernt, Angriffe von außen vorauszusehen, zuverlässige Backups durchzuführen, Firewalls einzurichten u.v.m., was der Sicherheit von Datenbanken dient.

PEARSON Education

ADDISON-WESLEY

Herausgegeben von:
Walter Gora
Thomas Krampert

Handbuch IT-Sicherheit

Strategien, Grundlagen und Projekte

Bibliografische Information Der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

10 9 8 7 6 5 4 3 2 1

05 04 03

ISBN 3-8273-2063-1

ein Imprint der Pearson Education Deutschland GmbH,
Martin-Kollar-Straße 10–12, D-81829 München/Germany

Einbandgestaltung: atelier für gestaltung, niesner & huber, Wuppertal
Bildquelle: www.photocase.de
Lektorat: Rolf Pakendorf, rpakendorf@pearson.de
Herstellung: Claudia Bäurle, cbaeurle@pearson.de
Satz: reemers publishing services gmbh, Krefeld, www.reemers.de
Druck und Verarbeitung: Kösel, Kempten (www.KoeselBuch.de)
Printed in Germany

Inhaltsverzeichnis

Vorwort

Sicherheit ist die wesentliche Säule, auf der alle Handlungen im Geschäftsleben basieren. Niemand möchte, dass beispielsweise ein Bezahlungsvorgang zweimal, sondern er soll nur einmal ausgeführt werden, dass Personal- und Gehaltsdaten öffentlich bekannt werden oder dass ein Unbekannter Zugang zu sensiblen Firmendaten erhält. Das Vertrauen in die Sicherheit von Organisationen und technischen Systemen ist damit eine elementare Voraussetzung für alle Transaktionen in der Wirtschaft. Immer neue und komplexere Informationssysteme bieten eine Vielzahl von Schwachstellen, Lücken und Angriffsmöglichkeiten, die in Konsequenz das erforderliche Vertrauen in die Korrektheit und Sicherheit der Geschäftsprozesse eigentlich erschüttern müssten.

Ob das häufig blinde Vertrauen in die Sicherheit der organisatorischen und technischen Systeme gerechtfertigt ist, muss stark bezweifelt werden. Alle Beteiligten, sei es Führungskräfte oder der »simple« Anwender, neigen dazu, die Gefährdungspotenziale herunterzuspielen bzw. aus ihrem Sichtfeld verbannen zu wollen. Schon seit Urzeiten werden die Überbringer negativer Meldungen wenig geachtet; positive Meldungen sind im Umfeld von Sicherheitsanalysen heute kaum vorhanden und im größeren Maßstab auch nicht zu erwarten. Wenn Kreditkarten missbraucht wurden, Angebotsdaten »zufällig« an die Konkurrenz gelangten oder sensible Geschäftsgespräche abgelauscht wurden, dann ist dies ein Ärgernis. Die Gegenmaßnahmen, z.B. die Einführung von SmartCards, Service Management Levels, Public Key Infrastructures etc., ist kaum jemanden eine Erfolgsmeldung wert.

Obwohl Sicherheit bzw. das Vertrauen in die uns umgebenden organisatorischen und technischen Prozesse ein Grundelement unseres Handelns ist, beschäftigen sich nur wenige mit dieser Thematik. Sicherheit ist kein Thema, mit dem sich ein Manager in der Wirtschaft heute vorausschauend profilieren kann. Selbst wenn von Sicherheitsstrategien gesprochen wird, ist dies nur halbherzig gemeint, da die Thematik »Sicherheit« meist nicht als strategisches, d.h. unternehmenspolitisch wichtiges Feld gesehen wird. Die Bedeutung von Sicherheit wird – allen Lippenbekenntnissen zum Trotz – nicht nur gering eingeschätzt, sondern auch als Thematik empfunden, die einem »aufgedrückt« wird und wo kaum ein Handlungsspielraum besteht.

Vor diesem Hintergrund entstand der Gedanke das Thema »IT-Sicherheit« ganzheitlich zu beschreiben und sowohl die Vision als auch die konkreten Vorgehensweisen zur Etablierung einer gesamtheitlichen Sicherheitspolitik zu beschreiben. Dieser Spagat zwischen Vision und Realität kann heute noch nicht geleistet werden, da unsere Projekterfahrungen aufzeigen, dass noch

viel an grundsätzlicher Überzeugungsarbeit zu leisten ist. Nicht die Konzeption und Einführung von sicherheitsschützenden Systemen erbringt den wesentlichen Mehrwert, sondern die Tatsache, dass sich alle Beteiligten über die erforderlichen Maßnahmen und die aus Sicht eines Unternehmens erforderlichen Prioritäten wirklich einig sind.

> ***Sicherheit ist nicht ein einzelnes Produkt, sondern ein Prozess.***
> *Man kann Sicherheit nicht einfach in ein System integrieren. Es ist sehr wichtig die echten Gefahren für das System zu verstehen, entsprechend diesen eine Sicherheits-Policy zu entwickeln, und dabei die richtigen Gegenmaßnahmen zu implementieren.*

Quelle: Bruce Schneier „Secrets and Lies"

Mit diesem Buch wird der Schritt unternommen, dieses weite und hochinteressante Thema dem Leser näher zu bringen. Wir möchten nicht den Anspruch auf Vollständigkeit erheben. Hierzu genügt allein schon die Differenzierung von organisatorischer und technischer Sicherheit. Die Vielfalt von Technik-Büchern zu diesem Thema zeigt, wie IT-Sicherheit akribisch und zu Recht technologisch abgebildet werden kann und muss.

Dennoch möchten wir mit diesem Buch den Versuch wagen, praxisnahe Erfahrungen begreiflich zu machen und dem hohen Stellenwert der IT-Sicherheit gerecht zu werden.

Sicherheit ist wichtiger denn je. Dabei ist die Authentizität der Teilnehmer, die Integrität der übertragenen Daten, ihre Vertraulichkeit (Geheimhaltung) sowie die Verbindlichkeit der Inhalte und deren Nachweisbarkeit eine Aufgabenstellung, die viele komplexe Fragen und Inhalte in sich birgt. Ein angestrebtes Alleinstellungsmerkmal dieses Buches ist seine umfassende Behandlung von Sicherheit in rechtlicher, organisatorischer und technischer Hinsicht. Es mögen zwar Lücken bleiben, aber der Versuch, die einzelnen Themen zu verbinden und nicht nur isoliert zu betrachten, soll unserer Erwartung nach einen Mehrwert für den Leser generieren.

Was dies in Konsequenz bedeutet, zeigen die einzelnen Kapitel dieses Buches. Es geht nicht soviel um Erkenntnisse auf der Bit- und Byte-Ebene, sondern um das fundierte Verstehen von Zusammenhängen auf verschiedenen Ebenen. Dies umfasst sowohl die generelle Thematik des Sicherheitsmanagements (incl. Qualitätssicherung), die gesetzlichen Anforderungen und Verpflichtungen gemäß KonTraG als auch technische Themen, wie z.B. sichere e-Mail oder e-Signatur. Von entscheidender Bedeutung sind juristische Aspekte, die in jüngster Vergangenheit erst die wesentlichen Entwicklungen im Bereich des Schutzes informationstechnischer Systeme impliziert haben. Abgerundet werden diese Ausführungen durch konkrete Projekterfahrungen und -referenzen. Hierzu zählt auch, dass die Sicherheitsanforderungen nicht nur quasi praxisfremd definiert werden, sondern in konkrete Service Level Agreements münden.

Der Dank der Herausgeber gilt an dieser Stelle allen Autoren, deren Beiträge dieses Buch erst möglich gemacht haben. Besonders herzlich bedanken wir uns außerdem bei Frau Kerstin Bonath und Herrn Marcus Depenbusch für ihr Engagement bei der Realisierung dieses Projektes, die für die Koordination und Gestaltung dieses Buches verantwortlich waren.

Sulzbach/Ts.

Dr. Walter Gora, Thomas Krampert

1 Holistischer Ansatz zur IT-Sicherheit

Thomas Krampert

1.1 Einleitung

Die Informationstechnik (IT) hat im Verlauf von nur vier Jahrzehnten eine wichtige, oft sogar lebenswichtige Rolle in fast allen Bereichen der Gesellschaft eingenommen. Als Folge hieraus wurde Sicherheit ein entscheidender Bestandteil der Informationstechnik. Hier stellt sich jedoch die Frage, was verstehen wir unter Sicherheit und insbesondere unter IT-Sicherheit?

Sind es Begriffe wie PKI, VPN, elektronische Signatur, Biometrie, E- und M-Commerce, Kryptografie, Firewall, Intrusion Detection, Wireless-LAN, aber auch Signaturgesetz, Datenschutz, Sicherheitsmanagement usw., die uns im täglichen Leben durch unsere Arbeit oder die Medien die Auseinandersetzung mit diesen Begrifflichkeiten oder Produkten diktieren?

Auf der anderen Seite assoziieren wir Risiko und Gefahr, aber auch die Gegensätze Schutz und Vertrauen mit den Themen wie z.B. Alarmanlagen, Videoüberwachung, Tresor oder Wachdienst.

Für diese zwei Betrachtungsweisen sind die angelsächsischen Begriffe »Security« (IT-Sicherheit) und »Safety« (Betriebssicherheit) am zutreffendsten. Diese Sichtweisen zeigen außerdem, dass die IT-Sicherheit auch mit differenzierten Ansätzen neben der technischen und organisatorischen ebenfalls die physische Sicherheit und deren Risiken betrachten muss.

Sicherheit und Risiko sind wechselseitig voneinander abhängig. Risiko ist nicht vorhandene Sicherheit und umgekehrt. Das Nichtvorhandensein von Sicherheit ist vollständiges Risiko, das Nichtvorhandensein von Risiko stellt vollkommene Sicherheit dar. Beide Extremwerte sind in der realen Welt nicht anzutreffen. Aufgrund der starken Abhängigkeit von Sicherheit und Risiko, auf welche später näher eingegangen wird, werden an dieser Stelle die grundlegenden Sicherheitsbegriffe mit ihren Definitionen erläutert.

Der Begriff der Sicherheit wird wie folgt definiert:

> ***Si|cher|heit**, die; -, -en [mhd. sicherheit, ahd. sichurheit]: 1. <o. Pl.> Zustand des Sicherseins, Geschütztseins vor Gefahr od. Schaden; höchstmögliches Freisein von Gefährdungen: soziale, wirtschaftliche S.; die öffentliche S. und Ordnung; die S. am Arbeitsplatz; die S. der Arbeitsplätze (Garantie für das Bestehenbleiben der vorhandenen Arbeitsplätze); die innere S. (das Gesichert-*

sein des Staates u. der Bürger gegenüber Terrorakten, Revolten u. Gewaltverbrechen); das bietet keine S.; ein Gefühl der S.; in S. sein; jmdn., sich, etw. in S. bringen (jmdn., sich, etw. aus dem Gefahrenbereich wegbringen, [vor dem Zugriff anderer] sichern); du solltest zur S. deinen Schreibtisch verschließen; sich, jmdn. in Sicherheit wiegen (irrtümlicherweise glauben, jmdm. einreden, dass keine Gefahr [mehr] besteht).

Quelle: DUDEN - Deutsches Universalwörterbuch

Des Weiteren wird Sicherheit immer als ein Ziel in einem konkreten Umfeld angesehen, da vollständige Sicherheit in der Praxis nicht erreicht werden kann.

Aus einem leicht anderen Blickwinkel betrachtet, kann Sicherheit auch definiert werden als:

...das Vorhanden sein von Integrität, Verbindlichkeit, Verfügbarkeit und Vertraulichkeit in einem geplanten Ausmaß.

Quelle: Verfahren zur Risikoanalyse - Institut für Informatik der Universität Zürich

In Anlehnung an die zweite Definition können die Ziele, mit welchen Sicherheit erreicht werden soll, mittels sechs Punkten wiedergegeben werden:

- **Vertraulichkeit**: Vertraulichkeit ist gegeben, wenn sichergestellt werden kann, dass Informationen nicht durch unautorisierte Personen, Instanzen oder Prozesse eingesehen werden können.

  ver|trau|lich <Adj.> [zu siehe vertrauen]: 1. nicht für die Öffentlichkeit bestimmt; mit Diskretion zu behandeln; geheim: eine -e Unterredung; etw. ist streng v.; etw. auf Wunsch v. behandeln.

Quelle: DUDEN - Deutsches Universalwörterbuch

- **Integrität**: Integrität ist gewährleistet, wenn Daten oder Systeme nicht unautorisiert manipuliert wurden und dadurch ihre Verfügbarkeit nicht beeinflusst wurde.

  In|teg|ri|tät, die; – [lat. integritas]: a) Makellosigkeit, Unbescholtenheit, Unbestechlichkeit: die I. dieses Mannes ist unbestreitbar; b) (Politik, Rechtsspr.) Unverletzlichkeit [eines Staatsgebietes]: die territoriale I. eines Staates garantieren.

Quelle: DUDEN - Deutsches Universalwörterbuch

- **Verfügbarkeit**: Verfügbarkeit ist gewährleistet, wenn die Funktionalität von Software und Hardware nicht unbefugterweise beeinträchtigt werden.

  ver|füg|bar <Adj.>: [augenblicklich] zur Verfügung stehend; für den sofortigen Gebrauch o. Ä. vorhanden: alle -en Hilfskräfte; -es (Wirtsch.; sofort flüssiges, disponibles) Kapital; das Buch ist zurzeit nicht v.

Quelle: DUDEN - Deutsches Universalwörterbuch

- **Verbindlichkeit:** Verbindlichkeit herrscht vor, wenn alle Aktionen einer Instanz eindeutig zugeordnet und nicht geleugnet werden können.

  Verbindlichkeit, Recht – Verpflichtung des Schuldners zu einer Leistung; sie entspricht der Forderung auf der Gläubigerseite.

`Quelle: Der Brockhaus in einem Band`

- **Authentizität**: Authentizität ist die Voraussetzung für Verbindlichkeit und befasst sich mit der Identität eines Subjektes.

  Au|then|ti|zi|tät die; – <zu ...izität>: Echtheit, Zuverlässigkeit, Glaubwürdigkeit.

`Quelle: DUDEN - Das große Fremdwörterbuch`

- **Betriebssicherheit**: Betriebssicherheit ist gegeben, wenn konsistente und gewünschte Funktionen und Verhalten der Daten und Systeme sichergestellt werden kann. Betriebssicherheit ist die Voraussetzung für Integrität und Verbindlichkeit.

Grundsätzlich gibt es zwei Arten von Risiken. *Spekulative Risiken* bergen neben der Möglichkeit von Verlusten auch die Möglichkeit von Gewinnen in sich. Da sich dieser Beitrag auf den Bereich der Informations- und Kommunikationstechnologien beschränkt, werden im Folgenden die *reinen Risiken*, wie z.B. Brände, Unfälle oder fahrlässiges Verhalten bezüglich dem Umgang mit Informationssystemen behandelt, deren Auswirkungen immer eine nachteilige Konsequenz und einen Verlust mit sich bringen.

Gestützt auf die erste Definition von Sicherheit wird Risiko umgekehrt definiert als:

> *...eine negative Abweichung von einem erwarteten Zustand bezogen auf ein sicherheitsrelevantes Objekt in einem Zielsystem durch ein gefährdendes Ereignis mit verschiedenen wahrscheinlichen Ausprägungen.*

`Quelle: Verfahren zur Risikoanalyse - Institut für Informatik der Universität Zürich`

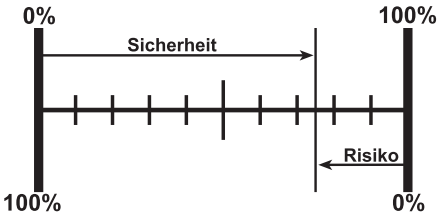
> ***Ri|si|ko**, das; -s, -s u. ...ken, österr. auch: Risken [älter ital. ris(i)co, eigtl. = Klippe (die zu umschiffen ist), über das Vlat. zu griech. rhíza = Wurzel, übertr. auch: Klippe]: möglicher negativer Ausgang bei einer Unternehmung, mit dem Nachteile, Verlust, Schaden verbunden sind; mit einem Vorhaben, Unternehmen verbundenes Wagnis: kein/ein R. eingehen, auf sich nehmen; bei einer Sache das R. in Kauf nehmen; die Risiken bedenken; das R. laufen (das Wagnis auf sich nehmen).*

`Quelle: DUDEN - Deutsches Universalwörterbuch`

Die Eintrittswahrscheinlichkeit und die negative Zielabweichung kann dabei bewertet werden.

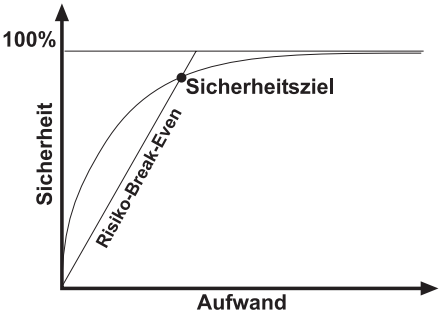
Wie schon erwähnt wurde, sind Sicherheit und Risiko gegenseitig voneinander abhängig. Wird die Sicherheit als ein Ziel betrachtet, so kann deren Zusammenhang mittels folgender Abbildung verdeutlicht werden.

Abbildung 1.1: Sicherheitsziel



Wird in einem weiteren Schritt der für die Erreichung eines bestimmten Sicherheitsniveaus aufzubringende Aufwand mitberücksichtigt, so kann dessen Zusammenhang der nächsten Abbildung entnommen werden.

Abbildung 1.2: Sicherheitsniveau



Vollständige Sicherheit kann in der Praxis nicht erreicht werden. Risiken, welche auf der Entscheidungsgrundlage einer Risikoanalyse als tolerierbar eingestuft worden sind, werden als Restrisiko geduldet.

1.2 Verfahren zur Bewertung der Sicherheit

Das traditionelle Verfahren zur Erarbeitung von Sicherheits- bzw. Schutzkonzepten für Produkte oder Gesamtsysteme ist die umfassende Risikoanalyse mit anschließender Auswahl individueller, speziell auf den vorliegenden Anwendungsfall abgestimmter Sicherheitsmaßnahmen oder -mechanismen. Sicherheitsverantwortliche sehen sich dabei jedoch vielfach mit zwei verwandten Problemfeldern konfrontiert:

- Die für diesen Prozess eigentlich erforderlichen personellen oder finanziellen Ressourcen stehen oft nicht zur Verfügung.
- Der Lebenszyklus moderner IT-Produkte und Gesamtlösungen ist oft so kurz, deren Komplexität jedoch so hoch, dass die Erarbeitung des individuellen Sicherheits- bzw. Schutzkonzepts nicht rechtzeitig abgeschlossen werden kann.

Ähnliche Probleme ergeben sich oft bei der Revision oder Transparentmachung von IT-Sicherheit.

Um den erforderlichen Gesamtaufwand für IT-Sicherheit zu minimieren, wird daher in der Praxis meist auf (vereinfachte) Standard-Verfahren zurückgegriffen, die den Sicherheitsverantwortlichen in methodischer oder inhaltlicher Hinsicht unterstützen. Sowohl für Produkte als auch für Gesamtlösungen haben sich nebeneinander unterschiedliche Verfahren im Themenbereich IT-Sicherheit etabliert. Diese IT-Sicherheitsverfahren überlappen teilweise inhaltlich, setzen jedoch unterschiedliche Schwerpunkte und richten sich an verschiedene Zielgruppen.

Für Unternehmen ergeben sich dadurch u.a. die folgenden Fragestellungen:

- Welche Sicherheitsaussage lässt sich auf Grundlage der einzelnen Verfahren treffen?
- Welche IT-Sicherheitsverfahren sind inhaltlich für einen bestimmten vorliegenden Anwendungsfall als Hilfsmittel geeignet?
- Bei welchen Verfahren zur IT-Sicherheit ist die verwendete Methode dem vorliegenden Problem angemessen?

Folgende Verfahren im Themenumfeld IT-Sicherheit können dabei Beachtung finden:

- Basel II
- CobiT ***[1]***
- FIPS 140-1/2
- ISO/IEC 17799 und BS 7799 ***[2]***
- ISO 9000
- ISO TR 13335
- IT-Grundschutz- und IT-Sicherheitshandbuch (BSI) ***[3]***
- ITSEC/Common Criteria ***[4]***
- KonTraG

Diese Liste erhebt keinesfalls den Anspruch der Vollständigkeit, umfasst jedoch nach Meinung des Autors die Verfahren mit größter Relevanz im betrachteten Themenumfeld.

Generell sollten aber darüber hinaus je nach Anforderung z.B.

- das Bundesdatenschutzgesetz (BDSG),
- das Telekommunikationsgesetz (TKG),
- die Fernmeldeüberwachungsverordnung (FÜV),
- die Telekommunikationsüberwachungsverordnung (TKÜV) und
- das Signaturgesetz (SigG)

Beachtung finden.

Ein Vergleich von Verfahren ist in einem Leitfaden *[5]* durch die Arbeitsgruppe »Sicherheit und Vertrauen im Internet« der Initiative D 21 durchgeführt worden.

Die betrachteten Verfahren können anhand der Merkmale

- produktorientiert,
- systemorientiert,
- technisch,
- organisatorisch

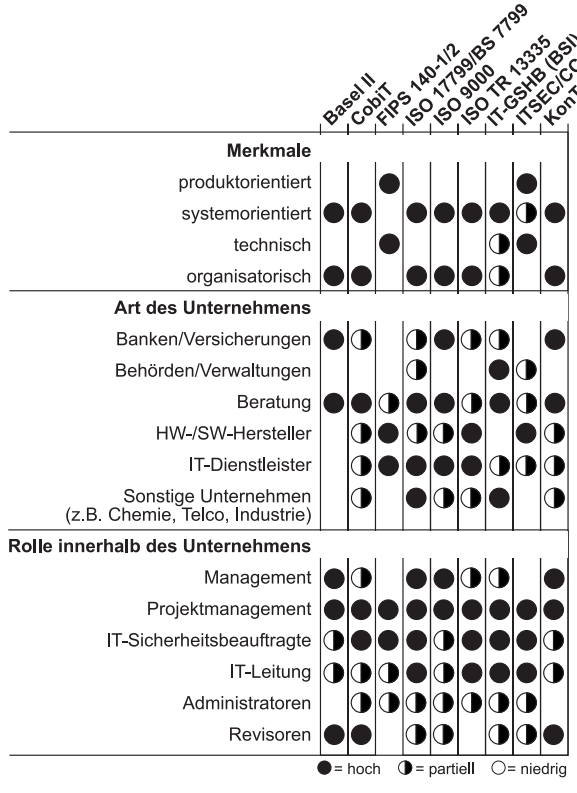
eingeteilt werden.

Ein weiteres Unterscheidungsmerkmal für die betrachteten Verfahren sind die Zielgruppen, an die sie sich jeweils richten. Dabei stellen sich zwei Fragen:

- An welche Arten von Unternehmen richtet sich das jeweilige Verfahren?
- Welche Rollen bzw. Positionen innerhalb der Unternehmen werden angesprochen?

Abbildung 1.3 gibt eine erste Orientierung in diesen Fragen:

Abbildung 1.3: Tabelle über Merkmale, Relevanz, Ausrichtung von IT-Sicherheitsverfahren



1.2.1 Zwei Beispiele

Basel II

Vor rund 10 Jahren hat der Baseler Ausschuss für Bankenaufsicht die derzeit geltenden Eigenkapitalvereinbarungen für Banken veröffentlicht. Der Ausschuss hat im Januar 2001 einen Vorschlag zur Änderung der internationalen Eigenkapitalregelung vorgestellt. Allgemein ist der Entwurf unter der Bezeichnung Basel II bekannt. Ab dem Jahr 2005 sollen die Bestimmungen in mehr als 100 Ländern in nationales Recht umgesetzt werden, um eine größere Sicherheit des Weltfinanzsystems zu erreichen.

Der Entwurf sieht dabei folgende Anforderungen an das Management vor:

- Mindestkapitalanforderungen (Eigenkapitalbedarf hängt direkt ab von Kredit- und operationellen Risiken)
- Aufsichtliches Überprüfungsverfahren
- Marktdisziplin (weitgehende Offenlegungsverpflichtungen des eigenen Risikomanagements)

Die Höhe des Eigenkapitals soll sich zukünftig stärker an den individuellen Kreditrisiken sowie den operationellen Risiken der Bank orientieren. Zu den operationellen Risiken zählen auch die IT-Risiken.

KonTraG

Der Gesetzgeber sieht für Aktiengesellschaften eine Haftung des organschaftlichen Unternehmensmanagements vor, wenn dieses eine Organisationspflicht verletzt. Damit unterliegt das Management einer Verpflichtung, die es erforderlich macht, die Unternehmensorganisation nicht nur ordnungsgemäß einzurichten, sondern auch ständig auf auftretende Lücken im Sicherheitskonzept hin zu überwachen. Diese Verpflichtung hat der Gesetzgeber durch das KonTraG (»Gesetz zur Kontrolle und Transparenz im Unternehmensbereich«) in § 91 des Aktiengesetzes (AktG) in Normierung der bisherigen Rechtslage nunmehr festgeschrieben. Danach sind gemäß § 91 Abs. 2 des AktG geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem aufzubauen, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig erkannt werden. Das Management wird so auch zur Einrichtung eines Risikomanagements im Hinblick auf

- risikobehaftete Geschäfte,
- Unrichtigkeiten der Rechnungslegung,
- Verstöße gegen gesetzliche Vorschriften

verpflichtet.

Das KonTraG ist bezüglich des einzurichtenden Risikomanagements sehr allgemein gehalten. Obwohl nicht explizit erwähnt, ergibt sich für die Unternehmen aus dem KonTraG eindeutig die Verpflichtung, geeignete Maßnah-

men zum Schutz gegen IT-Sicherheitsrisiken einzuführen. Art und Umfang dieser Maßnahmen ergeben sich aus einer Risikoanalyse als Teil des Risikomanagementprozesses, die für jedes Unternehmen individuell durchgeführt werden muss.

Neben der Risikophilosophie/-politik müssen insbesondere Informationen über die Risikoanalyse (Risikoidentifikation und -bewertung) sowie die Auf- und Ablauforganisation schriftlich fixiert werden. Außerdem sind Zuständigkeiten und Verantwortlichkeiten klar und eindeutig zu definieren.

Die Risikenbetrachtungen sowohl bei Basel II als auch beim KonTraG bedürfen der Einbindungen und Anwendung von speziellen IT-Risikoanalysen gemäß der nachfolgend aufgeführten Verfahren.

Die anschließende Tabelle gibt einen Überblick über die Ausrichtung der Verfahren unter Zugrundelegung verschiedener Kriterien, wobei anzumerken ist, dass diese Einschätzung auf der Meinung des Autors beruht.

Verfahren / Kriterien	CobiT	FIPS 140-1/2	ISO 17799 BS 7799	ISO 9000	ISO TR 13335	GSHB (BSI)	ITSEC/CC
Zielsetzung und Inhalt	Methode zur Unterstützung und Abwicklung geschäftsrelevanter Abläufe zur Begrenzung der entstehenden Risiken	Federal Information Processing Standards (FIPS) zur Validierung von Krypto-Modulen	Maßnahmen mit Best-practice-Ansatz	Norm zur Einheitlichkeit von Qualitätsmanagementsystemen	Derzeit vier „Technical Reports" für das IT-Sicherheitsmanagement, ohne bestimmte Lösungen zu erzwingen	Kataloge mit Standard-Sicherheitsmaßnahmen	Kriterienwerke für funktionale und qualitative Anforderungen an die Untersuchungsgegenstände
Vorgehens-/ Anwendungsweise	Prozessorientiert; beschreibt 34 kritische IT-Prozesse und ca. 300 Kernaufgaben	Entwicklungs- und Validierungskriterien gegen „vorgegebene, festdefinierte Testsuite"	Leitfaden für Informations-Sicherheitsmanagementsystem (ISMS)	Dokumentation der Prozesse im Qualitätsmanagement einer Organisation wird bezogen auf die eigenen Tätigkeiten aufgebaut	Theoretische Hinwiese über Methoden/Modelle; geben keine Vorgehensweisen und Lösungen vor	Fünf-Schichtenmodell. Durch vergebene Bausteine kann die IT-Landschaft komponentenorientiert dargestellt werden	Spezifikation für funktionale und qualitative Aspekte der Prüfgegenstände
Berücksichtigung Gesetze/Standards	Keine Hinweise auf rechtliche Aspekte in Deutschland	Versuch als Alternative zu den CC als Prüfkriterien zu platzieren	Wird nur eingeschränkt auf nationale Gesetzgebung eingegangen; fordert jedoch Bestimmung der relevanten Gesetze, um diese einzuhalten	ISO 9000 berührt direkt keine Gesetze, ist jedoch eine internationale Norm	Unabhängig von nationalen Gesetzgebungen; ihre Berücksichtigung wird jedoch eingefordert	Bundesbeauftragte stellt für den Datenschutz (BfD) ein eigenständiges Zusatzkapitel zur Verfügung	Berührt direkt keine Gesetze; Common Criteria sind jedoch aktuell als ISO/IEC 15408 eine internationale Norm
Skalierbarkeit	Wegen Matrixstruktur dem Anwender möglich einzelne Domänen oder Prozesse zu betrachten; sieben Geschäftsanforderungen als Untermenge auszuwählen	Testbereiche werden in vier hierarchisch aufbauenden Stufen strukturiert	Unabhängig von der Größe der betrachteten Institution	Sind die Anforderungen sehr komplex geht das Prüfverfahren eher in die Tiefe	Auf spezifischen Eigenheiten beliebiger Institutionen und ihrer IT-Infrastruktur anzupassen	Mechanismus für die Gruppierung gleichartiger Komponenten	Hängt von Komplexität des Prüfgegenstandes und der Tiefe des Prüfverfahrens ab
Aktualität/ Aktualisierbarkeit	Dritte Ausgabe (Erscheinungsjahr 2000) als „offener Standard" publiziert	Extrem aktuell und sehr erfolgreich im Bereich der Kryptographie	Derzeit zweite Version, eine regelmäßige Aktualisierung ist vorgesehen, es existieren jedoch keine fest verbindlichen Zyklen	Relativ stabil und werden selten geändert	Werden in unregelmäßigen Abständen aktualisiert	Werden zweimal pro Jahr überarbeitet und ergänzt	Relativ stabil und werden selten geändert

Abbildung 1.4: IT-Sicherheitsverfahren im Überblick (1)

Abbildung 1.5: IT-Sicherheitsverfahren im Überblick (2)

Verfahren Kriterien	CobiT	FIPS 140-1/2	ISO 17799 BS 7799	ISO 9000	ISO TR 13335	GSHB (BSI)	ITSEC/CC
Vollständigkeit	Methode zur Erfassung IT-orientierter und begleitender Prozesse; eine Ergänzung um systemspezifische Maßnahmen ist erforderlich	Einige Vollständigkeitsmängel	Enthält generische Standard-Sicherheitsmaßnahmen; enthält keine produktorientierten technologieorientierte Maßnahmen; orientieren sich an dem Baseline-Security-Ansatz	Es wird nur die Funktionalität der IT-Landschaft innerhalb der dokumentierten Prozesse sichergestellt; keine Überprüfung der Technologie an sich	Anleitungen für die Definition der IT-Sicherheitsprozesse	Enthält sowohl generische als auch produkt- oder technologiespezifische Standard-Sicherheitsmaßnahmen; ist hauptsächlich auf den Schutz von Informationen, IT-Anwendungen und IT-Systeme mit „normalen" Sicherheitsanforderungen ausgerichtet; höhere Sicherheitsanforderungen müssen durch zusätzliche Maßnahmen ergänzt werden	Beliebige IT-Systeme, IT-Produkte und IT-Komponenten sind überprüfbar. Durch die Definition von Sicherheitsniveaus können unterschiedliche Prüftiefen erreicht werden
Anwendbarkeit/ Handhabbarkeit	Ist unabhängig von der internen Struktur oder der Rechtsform eines Unternehmens einsetzbar	In der Regel nicht auf gängige Unternehmensstrukturen anwendbar.	Von der Institutionsstruktur weitgehend unabhängig	Eine Anwendbarkeit ist durch die Einbindung in die Managementprozesse zu 100% gegeben; unabhängig von Organisationstyp und Organisationsgröße	Für alle Institutionen unabhängig, zielen jedoch auf IT-Sicherheitsprozesse	Von der Unternehmensstruktur weitgehend unabhängig	Direkte Anwendbarkeit auf gängige Unternehmensstrukturen dürfte eher die Ausnahme sein, der Aufwand ist so hoch, dass eine Einzelprüfung nur selten gerechtfertigt ist
Tool-Unterstützung	CobiT Advisor, CobiT Self Assessment	Nicht öffentlich verfügbar; kann nur bei NIST durchgeführt werden	Auf BS 7799 abgestimmte spezifische Tools	Stark von Unternehmen abhängig; alle am Markt verfügbaren Tools können betrachtet werden	Nicht sinnvoll	BSI-Tool IT-Grundschutz; USEIT-BSI-Tool Sichere UNIX-Administration; am Markt sind weitere IT-Sicherheits-Tools verfügbar	Frei verfügbares Werkzeug, CC-Toolbox

Kriterien / Verfahren	CobiT	FIPS 140-1/2	ISO 17799 BS 7799	ISO 9000	ISO TR 13335	GSHB (BSI)	ITSEC/CC
Internationalität	In englischer und deutscher Sprache verfügbar	Nur in englischer Sprache verfügbar, Übersetzung ist nicht geplant	In englischer und deutscher Fassung vorliegend	Internationale Norm	Internationale Norm	Deutschsprachige Version, englische Übersetzung	International akzeptiert
Qualifizierung/ Zertifizierung	Kein Zertifikat im eigentlichen Sinn; wird von vielen Wirtschaftsprüfungsorganisationen im Rahmen der Jahresabschlussprüfung zur Prüfung des IT-Kontrollumfelds eingesetzt	Nordamerikanisches Akkreditierungsschema	Spezifisch auf eine Zertifizierungsgrundlage ausgerichtet; Basis für ein Zertifizierungssystem	Prüfungen und Zertifizierungen werden von akkreditierten, unabhängigen Stellen durchgeführt; Zertifikate werden z.B. vom TÜV oder der DQS ausgestellt und veröffentlicht	Zertifizierung ist nicht vorgesehen	Qualifizierungsschema, um die erfolgreiche Umsetzung des IT-Grundschutzes zu dokumentieren; Einstiegsstufe, Aufbaustufe, IT-Grundschutz-Zertifikat	Prüfungen werden von akkreditierten Prüflabors durchgeführt; Erteilung eines Zertifikats vom BSI und von akkreditierten Zertifizierungsstellen
Aufwand für Durchführung (intern/extern)			Aufwand stark unterproportional zur Größe; Gruppenbildungen ermöglicht eine Aufwandsreduktion	Aufwand für eine Prüfung ist abhängig von der Schlüssigkeit der Dokumentation und der Funktionalität der anderen Prozesse		Bei inhomogenen IT-Landschaften steigen Aufwand und Kosten, schlimmstenfalls proportional zur Anzahl der Komponenten	Aufwand mit wachsender Komplexität und Prüftiefe steigt sehr stark an
Kosten für Umsetzung	Eine vollständige Analyse aller Kontrollziele kann in ca. einem Arbeitsmonat abgeschlossen sein	Die Kosten und die Zeiten für eine Validierung sind erheblich geringer als für eine CC-Evaluierung	Stark abhängig von der generellen organisatorischen Qualität; der Aufwand orientiert sich stark am Umfang der Risikoanalyse	Aufwand und Kosten sind relativ gering; es sind keine kostenintensiven Dienstleistungen oder Sicherheitskomponenten gefordert; Kosten entstehen durch den personellen und organisatorischen Aufwand; eine Aufwandsschätzung dieses Teilbereiches nur schlecht möglich	Stark abhängig von der generellen organisatorischen Qualität; der Aufwand orientiert sich stark am Umfang der Risikoanalyse	Die Kosten ergeben sich daher durch den organisatorischen und personellen Aufwand und die Durchführung der IT-Grundschutz-Analyse; ein Unternehmen mittlerer Größe sollte mindestens 3 Arbeitsmonate einplanen	Aufwand nach einem der Kriterienwerke ist eher hoch; Problem der zeitnahen Aktualisierung von Prüfergebnissen ist derzeit noch als ungelöst zu betrachten

Abbildung 1.6: IT-Sicherheitsverfahren im Überblick (3)

1.3 Anwendbarkeit der Verfahren

Die unterschiedlichen Zielsetzungen und Zielgruppen der betrachteten Verfahren zeigt, dass ein angemessenes IT-Sicherheitsniveau für eine Gesamtlösung nur dann erreicht werden kann, wenn sowohl Hersteller als auch Anwender von Informationstechnik dazu beitragen.

Keines der betrachteten Verfahren verspricht »umfassende« Sicherheit. Behandelt werden jeweils nur Teilaspekte des Problems, eine vorliegende Gesamtlösung angemessen vor den relevanten Bedrohungen zu schützen. In den meisten Fällen ist es daher zweckmäßig, die Verfahren synergetisch zu nutzen.

1.4 Verfahrensunabhängige Vorgehensweise

Um eine Systematik in die Vorgehensweise und bei der Untersuchung von Abläufen (Prozessen) einzuführen, wird das in zahlreichen Organisations- und Sicherheitsprojekten der C_sar AG benutzte Infrastrukturaufbaumodell nachfolgend erklärt. Dieses Modell definiert vier Ebenen, die

- Geschäftsprozessebene,
- Organisationsebene,
- Anwendungsebene,
- IuK-Infrastrukturebene,

auf denen die Untersuchungsgegenstände erhoben werden können. Dieses Vorgehen ist angesichts unterschiedlicher Typen von Abläufen mit unterschiedlichen Wirkungskreisen sinnvoll und erleichtert eine nachfolgende Analyse.

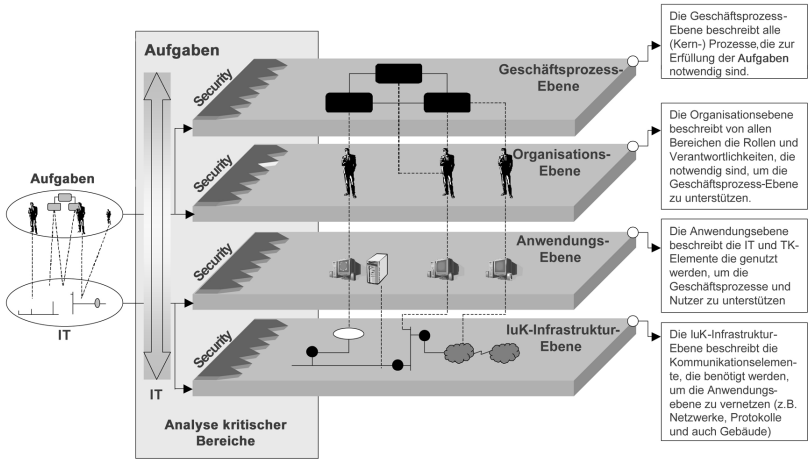


Abbildung 1.7: Aufbaumodell IT-Sicherheit

1.4.1 Geschäftsprozessebene

Auf dieser Ebene werden die Aufträge und Produkte (insbesondere Dienstleistungen) erfasst, kurz beschrieben und anschließend klassifiziert. Die Grundlage der Klassifikation bildet die Bedeutung des Prozesses für die Sicherstellung der Arbeitsfähigkeit (Abläufe mit externen Schnittstellen). Hierbei wird unterschieden zwischen Abläufen, die für die Arbeitsfähigkeit von

- unmittelbarer,
- kurzfristiger,
- langfristiger,
- oder keiner

Bedeutung sind.

Primär werden die Geschäftsprozesse mit einem unmittelbaren oder kurzfristigen Einfluss auf die Arbeitsfähigkeit als kritische Abläufe identifiziert. Diese Abläufe werden vorrangig behandelt, mit dem Ziel, eine vollständige Erfassung, Bewertung der Kritikalität und Analyse der IT-Abhängigkeit, sowie des Absicherungsbedarfs durchzuführen.

Abläufe mit langfristiger bzw. keiner Bedeutung für die Sicherstellung der Versorgung werden erfasst und exemplarisch analysiert. Als Grundlage einer Folgeklassifikation in diesem Bereich wird die Bedeutung identifizierter Prozesse und somit der im Fall einer Störung oder eines Ausfalls auf erzeugte Schäden gelegt. Im Fall einer gegebenenfalls notwendigen Priorisierung der Untersuchungen können diese beispielsweise in

- personelle Bereiche,
- Informations- und Organisationsbereiche,
- materielle Bereiche

gegliedert werden.

1.4.2 Organisationsebene

Ausgehend von den identifizierten Prozessen wird im Folgeschritt erhoben, welche Organisationseinheiten in die Erfüllung des Kernprozesses in welchem Umfang eingebunden sind. Zielsetzung ist es, die für die wesentlichen Kernprozesse notwendigen organisatorischen Bereiche bzw. Elemente zu identifizieren.

Aufgrund der enormen Vielfalt von Strukturen innerhalb der Unternehmen oder der Öffentlichen Verwaltung wird in diesem Punkt analog zur Vorgehensweise auf der Geschäftsprozessebene die Klassifikation der beteiligten Organisationsstellen für den beschriebenen Prozess als

- unmittelbar verantwortlich oder
- mittelbar/querschnittlich verantwortlich

vorgenommen. Ebenfalls analog zur Vorgehensweise auf der Geschäftsprozessebene werden primär die Organisationsstellen mit einer unmittelbaren Verantwortung für die Kernabläufe Gegenstand einer vertieften Bearbeitung. Organisationsstellen mit mittelbarer oder querschnittlicher Verantwortung werden mit einer Kurzbeschreibung versehen und in diesem Kontext nicht weiter vertieft.

1.4.3 Anwendungsebene

Für die als kritisch eingestuften Abläufe wird im nächsten Schritt der Informationserhebung die erste Stufe der IT-Durchdringung, die Anwendungsebene, ermittelt. Damit werden diejenigen IT- und TK-Elemente identifiziert, die einerseits direkt für die Unterstützung der kritischen Kernprozesse eingesetzt werden und andererseits von den Mitarbeitern in den als kritisch identifizierten organisatorischen Bereichen für die Erfüllung ihrer Arbeit benötigt werden.

Aufgrund der existierenden Vielfalt von Architekturbeschreibungsmodellen kann beispielsweise dieser Erhebung die Nomenklatur und die Systematik des V-Modells zugrunde gelegt werden. Die Betrachtungstiefe kann wie folgt definiert werden:

- System: Regelfall als kleinste Beschreibungseinheit.
- Segment: In begründeten Fällen als wesentlicher und in sich abgeschlossener Bestandteil sehr großer Systeme.

1.4.4 IuK-Infrastrukturebene

Analog zur Anwendungsebene wird aufgrund ihres querschnittlichen Versorgungscharakters die Infrastrukturebene erfasst. Darunter fallen alle informations- und telekommunikationstechnische-Elemente (IuK) mit Infrastrukturcharakter, insbesondere im Bereich der Vernetzung und drahtloser Kommunikation.

Für die Ermittlung der Risiken im Bereich der klassischen IT-Sicherheit (security) aber auch für die Betriebssicherheit (safety) werden die zu Anfang erklärten Begriffe bewertet.

- Verfügbarkeit

  Hier ist die erforderliche Mindestverfügbarkeit der betrachteten Größe zu bewerten in Zusammenhang mit der erwarteten Wahrscheinlichkeit, dass diese nicht gewährleistet werden kann.

- Integrität

  Hier ist zu bewerten, ob und ggf. wie weit die betrachtete Größe von ihrem tatsächlichen »Wert«/»Inhalt« (insbesondere bei Daten) abweichen darf oder missbräuchlich verwendet werden kann ohne ihre Nutzbarkeit zu verlieren in Zusammenhang mit der erwarteten Wahrscheinlichkeit, dass dies nicht gewährleistet werden kann.

- Vertraulichkeit

  Hier ist zu bewerten, ob und ggf. in wie weit die betrachtete Größe nicht auch anderen als einem bestimmten Adressaten(-kreis) zugänglich sein darf in Zusammenhang mit der erwarteten Wahrscheinlichkeit, dass dies nicht gewährleistet werden kann.

- Zuverlässigkeit

  (entsprechend dem englischen »reliability«)
  Hier ist zu bewerten, ob die betrachtete Größe ihre »Leistung« in der geforderten Art und Weise (z.B. Erfüllen von Quality-of-Service-Anforderungen) erbringt in Zusammenhang mit der erwarteten Wahrscheinlichkeit, dass dies nicht gewährleistet werden kann.

- Verlässlichkeit

  (entsprechend dem englischen »dependability«)
  Hier ist zu bewerten, ob die Erwartungen des Nutzers oder Prozess, dass die betrachtete Größe ihre »Leistung« in der geforderten Art und Weise (z.B. Erfüllen Quality-of-Service-Anforderungen) erbringt und nicht in (aus Sicht des Nutzers) unakzeptabler Weise vom erwarteten Verhalten abweicht, erfüllt werden können in Zusammenhang mit der erwarteten Wahrscheinlichkeit, dass dies nicht gewährleistet werden kann.

Verlässlichkeit wird dabei als Oberbegriff verstanden, der die übrigen genannten sowie weitere Begriffe umfasst, z.B. solche, die Aspekte der Betriebssicherheit (safety) beschreiben. Für die geforderte Bewertung der Kritikalität der Prozesse bedeutet das aber nicht, dass auf die Bewertung bzgl. Verfügbarkeit, Integrität, Vertraulichkeit und Zuverlässigkeit verzichtet werden kann.

Beispiele für Risiken im Bereich der Vertraulichkeit, Integrität und Verfügbarkeit sind:

- Einbringen von Software mit Schadenswirkung (z.B. Viren, Trojanische Pferde, logische Bomben oder Netzwürmer) in IT-Systeme
- Manipulation/Schädigung/Zerstörung von Betriebssystemen oder Applikationssoftware (einschl. betroffener Datensätze)
- Unzureichend gesicherte Fernadministrationszugänge
- Manipulationen durch »Innentäter« (z.B. Administratoren oder Nutzer)
- mit Fehlern oder Risiken behaftete Software
- Manipulation von Kommunikationsverbindungen
- ...

aber auch Faktoren wie:

- mangelndes Sicherheitsbewusstsein (bei Mitarbeitern und Vorgesetzten)
- Schnelllebigkeit der Technik

- Outsourcing
- Komplexität der Systeme
- nicht hinreichend qualifiziertes Personal
- ...

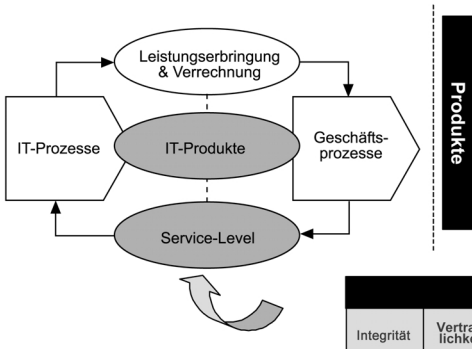
Ein umfassender Schutz gegen alle Bedrohungen ist selbst für kritische Bereiche nicht zu realisieren, geschweige denn zu finanzieren. Ziel muss es sein, einen angemessenen Schutz zu erreichen. Das Maß für den Umfang des Schutzes ist die Art und Höhe des möglichen Schadens. Die Klassifizierung von Schäden ist über die Zuordnung in unterschiedliche Kategorien möglich:

- materiell (Objekte/Werte)
- finanziell (Vermögen/Geld)
- immateriell (Ansehen/Vertrauen)
- personell (Leben/Gesundheit)

Dabei können die immateriellen Schäden (z.B. ein Vertrauensverlust) wesentlich kritischer sein als Vermögensschäden.

Besonders wichtig ist für den Schutz kritischer Bereiche mögliche Kettenreaktionen auf andere organisatorische oder technische Bereiche weitgehend auszuschließen.

Die Identifikation von IT-Komponenten und deren Bewertung der Schutzwürdigkeit versetzt die IT-Verantwortlichen in die Lage, ihre Sicherheits-Anforderungen zu definieren.



Klassifizierung	Schutzziele: Integrität	Vertraulichkeit	Verfügbarkeit	Nachweisbarkeit	Identifizierung & Authentifizierung	Autorisierung
Beeinträchtigung der Aufgabenerfüllung						
Negative Außenwirkungen						
Finanzielle Auswirkungen						
Verstoß gegen Gesetze und Vorschriften						

Abbildung 1.8: Schutzwürdigkeitsmatrix

1.5 Fazit

Im Rahmen der IT-Sicherheit und des Sicherheitsmanagements, welches das Ziel der Erreichung von Sicherheit verfolgt, ist die Untersuchung und die folgliche Behandlung von Risiken unerlässlich. Welches Verfahren sich generell am besten für die Erkennung und Bewertung von Risiken in der Praxis eignet, kann abschließend nicht festgelegt werden. Die jeweiligen Vor- und Nachteile der Methoden müssen kundenspezifisch gegeneinander abgewägt werden. Des Weiteren darf der Einbezug von situativen Einflussfaktoren bei der Auswahl des jeweiligen Analyseverfahrens nicht unterlassen werden. Einen entscheidenden Einfluss auf die Wahl des Verfahrens werden die Haltung des Managements bezüglich Sicherheitsaspekten und, damit zusammenhängend, die für die Durchführung zur Verfügung stehenden sowohl finanziellen als auch personellen Ressourcen haben.

Quellen: *[1]* COBIT, 3rd edition, Stand 13.09.2001

[2] ISO/IEC 17799, BS 7799, Management von Informationssicherheit Teil 1 + 2, Dezember 2000

[3] IT-Grundschutzhandbuch, BSI, Mai 2002

[4] Common Criteria, Leitfaden BSI, Version 1.0, Mai 2001

[5] IT-Sicherheitskriterien im Vergleich, Initiative D21, Stand 20.12.2001

2 Management der Organisation, Organisation der Sicherheit

Thomas Mai

2.1 Allgemeines

Der Einsatz der EDV, vor allem im Rahmen vernetzter Computersysteme, ist mittlerweile für fast alle Unternehmen eine Selbstverständlichkeit. Durch diesen Trend, der nicht mehr umkehrbar ist, steigt der Bedarf und vor allem die Bedeutung nach einer qualifizierten Auseinandersetzung mit solchen Themen wie z.B. Datensicherheit, Datenschutz, Sicherheitsrisiken usw..

Der korrekte und sicherheitsbewusste Umgang mit Informationen und Daten, deren Verlust oder Missbrauch ein Unternehmen in der heutigen Zeit – siehe hierzu Abbildung 2.1 – empfindlich beeinträchtigen oder sogar um dessen Existenz bringen können, ist hierbei als wichtiger Bestandteil der Unternehmensorganisation zu sehen.

Von besonderer Bedeutung ist die Tatsache, dass in den meisten Fällen Irrtümer und Nachlässigkeiten bei den eigenen Mitarbeitern in der Organisation ausschlaggebend für Probleme im Bereich IT-Sicherheit sind. Hierbei sind auch Mängel in der Dokumentation zum Thema IT-Sicherheit als ein wichtiger Grund für Probleme zu nennen. IT-Sicherheit ist somit in erster Linie eine Frage der internen Organisation.

Die Organisation der Sicherheit darf hierbei nicht das Betätigungsfeld einzelner EDV-Interessierter sein, sondern muss als Managementaufgabe angesehen werden. Das in diesem Zusammenhang umzusetzende IT-Sicherheitsmanagement muss jedoch Bestandteil eines umfassenden Managementsystems sein, über welches in diesem Beitrag Aussagen getroffen werden.

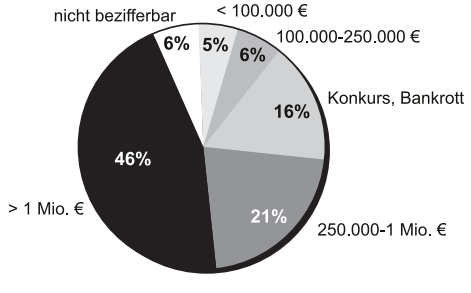


Abbildung 2.1: Schäden durch den Verlust elektronischer Daten

Quelle: Wirtschaftswoche Nr. 30 vom 18.07.2002

2.2 Integrierte Managementsysteme

Unternehmen arbeiten erst dann effektiv, wenn alle miteinander verknüpften relevanten organisatorischen und sicherheitstechnischen Prozesse und Aktivitäten systematisch definiert und geregelt sind.

Es besteht natürlich die Möglichkeit, die verschiedenen Systeme wie z.B. Qualitätsmanagementsystem und IT-Sicherheitsmanagementsystem separat auf Basis vorhandener Normen und Konzepte zu entwickeln. Der für eine Organisation sinnvolle Weg ist jedoch die Integration von Organisation und IT-Sicherheit durch eine gesamtheitliche Betrachtungsweise und durch interdisziplinäres Denken. Hierzu eignet sich in hervorragender Weise die Verknüpfung von Qualitätsmanagement und IT-Sicherheitsmanagement zu einem integrierten Informationssicherheits-Managementsystem (ISMS), welches nachfolgend beschrieben ist.

2.2.1 Qualitätsmanagementsystem (QMS)

Qualitätsmanagement ist untrennbar mit der ISO 9000-Normenreihe verbunden. Die Zahl der Unternehmen, die sich in den letzten Jahren haben zertifizieren lassen ist stark gestiegen. Allein in Deutschland waren Ende 1999 rund 30.000 Unternehmen zertifiziert *[1]*. Zudem kann davon ausgegangen werden, dass fünf- bis zehnmal mehr Organisationen ein normenkonformes Qualitätsmanagementsystem aufgebaut haben, ohne es zertifizieren zu lassen *[2]*.

Die ISO-Normenreihe beinhaltet seit Dezember 2000 folgende drei QMS-Normen:

- ISO 9000:2000
  Qualitätsmanagementsysteme – Grundlagen und Begriffe
- ISO 9001:2000
  Qualitätsmanagementsystem – Anforderungen
- ISO 9004:2000
  Qualitätsmanagementsysteme – Leitfaden zur Leistungsverbesserung

Die DIN EN ISO 9001 legt die Anforderungen an ein QMS fest und kann für Zertifizierungs- und Vertragszwecke eingesetzt werden.

Wichtig für das Verständnis von Qualitätsmanagement ist, das Qualität nur durch systematisches Handeln zu erreichen ist. Systematisches Handeln erfordert in erster Linie eindeutige und transparente

- Organisationsstrukturen,
- (Prozess-)Abläufe,
- Verantwortlichkeiten,
- Kommunikations- und Informationswege.

Systematisches Handeln erfordert zudem eindeutige und transparente

- Vorgaben/Politik,
- Kennzahlensysteme,
- Bewertungen,
- Maßnahmen zur Verbesserungen.

Somit ist Qualitätsmanagement vor allem eine Managementaufgabe, die unter Einbeziehung aller Organisationseinheiten und Beteiligten zu erfolgen hat.

Die genannten Voraussetzungen für ein funktionierendes Qualitätsmanagementsystem sind aber auch Voraussetzung für ein IT-Sicherheitsmanagementsystem.

Von Bedeutung ist zudem der prozessorientierte Ansatz der DIN ISO 9001. Das hierin aufgeführte Prozessmodell (siehe Abbildung 2.2) hat die Aufgabe, das komplexe System einer Organisation prozessorientiert darzustellen. Dieses Prozessmodell bildet die Grundlage für die Integration weiterer Systeme, unter anderem auch des IT-Sicherheitsmanagementsystems.

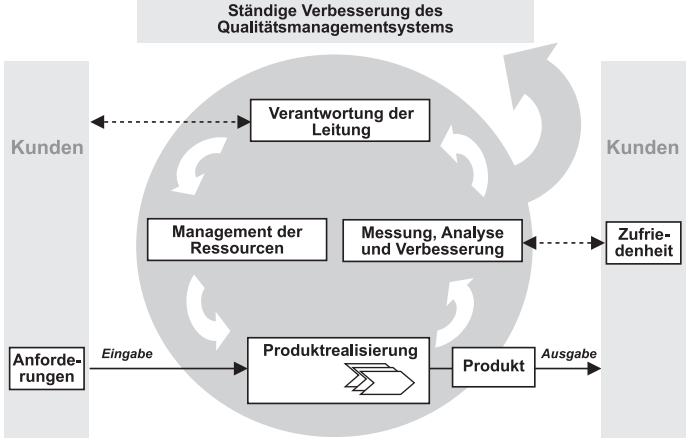


Abbildung 2.2: Modell eines prozessorientierten Qualitätsmanagementsystems nach DIN EN ISO 9001

2.2.2 IT-Sicherheitsmanagementsystem

Das IT-Sicherheitsmanagementsystem stellt die Grundlage dar, um eine angemessene Informationssicherheit zu erzielen. Hierbei ist zu beachten, dass das IT-Sicherheitsmanagementsystem nicht als Kostenfaktor, sondern als eine Vorleistung zur Vermeidung von Verlusten zu betrachten ist.

In Übereinstimmung mit den Voraussetzungen für ein QM-System ist auch für das IT-Sicherheitsmanagementsystem festzuhalten, dass die Grundlagen für ein solches Managementsystem durch das Management selbst geschaffen werden müssen.

IT-Sicherheit ist ebenso wie QM eine Aufgabe des Managements

Ein wesentlicher Punkt ist ebenfalls die Integration des IT-Sicherheitsmanagements in die Gesamtorganisation. Die Bildung einer separaten Organisation für IT-Sicherheit, die ihre eigenen unabhängigen Ziele und Vorgaben verfolgt, ohne hierbei in das Gesamtsystem eingebunden zu sein, führt unweigerlich zu Missmanagement.

IT-Sicherheit muss Bestandteil der bestehenden Organisationsstruktur, des bestehenden Systems sein

Grundlage eines IT-Sicherheitsmanagementsystems ist die Definition folgender Basisvorgaben:

- IT-Sicherheitspolitik
- Festlegung der Strategien
- grundsätzliche Zielvorgaben
- Organisation und Verantwortlichkeiten für IT-Sicherheit

Entwicklung und Fortschreibung von Politik, Strategie, Zielvorgaben

Alle Managementkonzepte, nicht nur im Rahmen des IT-Sicherheitsmanagements, betonen die besondere Relevanz der Basisvorgaben und deren Umsetzung in eine entsprechende Planung und auf operativer Ebene.

IT-Sicherheitspolitik und IT-Strategien legen die grundsätzliche Ausrichtung einer Organisation in Bezug auf die IT-Sicherheit fest und bestimmen damit die langfristige Entwicklung. Hierauf ist besonderes Augenmerk zu richten.

Die IT-Sicherheitspolitik bildet die Basis für die Entwicklung und die Umsetzung eines risikogerechten und wirtschaftlich angemessenen IT-Sicherheitsmanagements. Sie stellt das Grundlagendokument dar, das die sicherheitsbezogenen Ziele und Werte, die Gesamtstruktur des IT-Sicherheitskonzeptes und die Verantwortlichkeiten verbindlich festlegt.

Mit der IT-Sicherheitspolitik wird dokumentiert, welche strategische Position das Management u. a. zur Erstellung und Umsetzung des Sicherheitskonzeptes und zur Erreichung der IT-Sicherheitsziele auf allen Ebenen der Organisation einnimmt.

Wichtig ist, dass das Management in vollem Umfang hinter der IT-Sicherheitspolitik und den darin festgehaltenen Zielen steht.

IT-Sicherheitspolitik und IT-Strategien dürfen nicht losgelöst von weiteren Vorgaben wie z.B. Qualitätspolitik entwickelt werden. Zudem muss gewährleistet werden, dass bei ihrer Entwicklung alle relevanten »Interessengruppen« angemessen berücksichtigt werden.

IT-Sicherheitspolitik und IT-Strategien haben sich an den gesetzlichen Anforderungen zu orientieren. Diese sind den wenigsten Unternehmen bekannt. Längst nicht alle Organisationen setzen als Beispiel die Anforderungen des

Bundesdatenschutzgesetzes um. Die Regelungen der Telekommunikations- und Teledienstgesetze, die für die Protokollierung bei Firewalls und Web-Servern eine Rolle spielen, sind nicht durchgehend bekannt. Ähnlich unbekannt ist das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), das Firmen zur Einrichtung von Risikomanagementsystemen verpflichtet.

IT-Sicherheitspolitik und IT-Strategien müssen auf Basis »Management by Fact« definiert werden. Das bedeutet, dass IT-Sicherheitspolitik und IT-Strategien auf der Grundlage fundierter und objektiver Informationen festgelegt werden müssen. Zu diesem Zweck muss jedes Unternehmen durch geeignete aufbau- und ablauforganisatorische Regelungen und durch Festlegung von Verantwortlichkeiten sicherstellen, dass die erforderlichen Daten und Informationen ermittelt werden.

IT-Sicherheitspolitik und IT-Strategien haben allen Mitarbeitern eine klare Vorstellung von der strategischen Ausrichtung der Organisation zu vermitteln und dadurch ihre eigene Rolle im Entwicklungsprozess der Organisation zu verdeutlichen. Daher muss regelmäßig ermittelt werden, ob die Aktivitäten zur organisationsweiten Verbreitung von Politik und Strategien zum Erfolg geführt haben, d.h. ob und inwieweit die Mitarbeiter sich ihrer bewusst sind.

Als nächster Prozess erfolgt die Übersetzung der IT-Sicherheitspolitik und IT-Strategien in lang- und kurzfristige Zielvorgaben sowie konkrete Maßnahmenpläne und Sicherheitskonzepte. Aus den Zielen der Gesamtorganisation sind in einem durchgehenden und für die Betroffenen transparenten Prozess Vorgaben für alle hierarchischen Ebenen und Organisationseinheiten zu entwickeln und damit wiederum Ziele, die klare Bezüge zur IT-Sicherheitspolitik und zu den IT-Strategien aufweisen. Dieses Vorgehen trägt dazu bei, den Mitarbeitern ihre Rolle in der Geschäftstätigkeit und ihren Beitrag zum Organisationserfolg zu vermitteln. Dadurch wird gewährleistet, dass sie sich gemeinsamen Organisationszielen verpflichtet fühlen und »an einem Strang ziehen«.

Entwicklung und Fortschreibung der Organisation, von Verantwortlichkeiten

Methodisches Sicherheitsmanagement ist zur Gewährleistung umfassender und angemessener IT-Sicherheit unerlässlich. Dabei handelt es sich um einen kontinuierlichen Prozess, der die Sicherheitsziele gewährleisten soll. Die angestrebte Sicherheitspolitik sowie die angestrebten IT-Sicherheitsziele können nur erreicht werden, wenn das IT-Sicherheitsmanagement organisationsweit umgesetzt wird. Dieser übergreifende Charakter des IT-Sicherheitsmanagements macht es notwendig, die

- IT-Sicherheitsmanagementorganisation,
- Verantwortlichkeiten,

- Befugnisse und
- Kommunikationswege

innerhalb der Organisation festzulegen.

Zentrale Aufgaben im IT-Sicherheitsmanagement kommen hierbei folgenden Funktionen/Gremien zu:

- dem Management
- ggf. dem IT-Sicherheitsmanagemement-Team
- dem IT-Sicherheitsbeauftragten
- dem Datenschutzbeauftragten
- dem Administrator
- den IT-Anwendern

Die dauerhafte oder zeitlich befristete Delegation von Aufgaben, Kompetenzen und Verantwortungen im Rahmen der IT-Sicherheit erfolgt durch:

- Das ausdrückliche, schriftliche Übertragen von Aufgaben an den betroffenen Mitarbeiter. Das bedeutet, dass jeder Mitarbeiter klare Stellenziele und einen festumrissenen Aufgabenbereich bzw. Schwerpunkte seiner Tätigkeit bezogen auf die IT-Sicherheit zugewiesen bekommt.
- Das Übertragen der erforderlichen Kompetenzen und Verantwortungen an die mit der Aufgabenwahrnehmung beauftragte Stelle zur Durchführung der Aufgabe im Rahmen der IT-Sicherheit. Innerhalb dieses Verantwortungsbereiches handelt und entscheidet der Stelleninhaber selbstständig.
- Überwachungsmaßnahmen, die der Delegierende ergreift, zur Sicherstellung, dass der Delegationsempfänger die Aufgabe tatsächlich entsprechend den ihm übertragenen Kompetenzen durchführt.

Die Konkretisierung der genannten Punkte erfolgt im Rahmen der Stellenbeschreibungen.

Organisatorische Sicherheit ist umfassend zu betrachten. Das bedeutet, dass über die Organisation hinaus, Fremdunternehmen und Outsourcing-Partner mit einbezogen werden.

Entwicklung und Fortschreibung des Sicherheitskonzeptes

Auf Basis der IT-Sicherheitspolitik ist das IT-Sicherheitskonzept zu konzipieren.

Die Erarbeitung eines IT-Sicherheitskonzepts kann auf nachfolgend aufgeführten Grundlagen durchgeführt werden:

- ISO/IEC 17799 (auf Basis des British Standard BS 7799) als ein mehr organisatorischer Ansatz
- IT-Grundschutzhandbuch, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das IT-Sicherheitskonzept auf der Basis des IT-Grundschutzhandbuches hat hierbei zum Inhalt:

- Schutzbedarfsfeststellung
- Bedrohungs- und Schwachstellenanalyse
- Risikoanalyse- und Bewertung
- Kosten-Nutzen-Analyse
- Restrisikobetrachtung
- Schulungen

Mit dem IT-Sicherheitskonzept wird keine Ausarbeitung geschaffen, die lediglich den Charakter einer Momentaufnahme hat und mit der Änderung von technischen Randbedingungen oder Beurteilungen schnell an Wert verliert. Vielmehr ist es ein fortschreibungsfähiges Konzept.

Die Fortschreibung dieses Konzeptes in definierten Zyklen ist erforderlich, da jedes Sicherheitskonzept dynamische Komponenten besitzt, deren Änderungen Auswirkungen auf die identifizierten Risiken und damit auch auf die zu ergreifenden Sicherheitsmaßnahmen haben.

Entwicklung und Fortschreibung der Risikoanalyse

Eine wesentliche Aufgabe des IT-Sicherheitsmanagements ist das Erkennen und Einschätzen von Sicherheitsrisiken und deren Reduktion auf ein tragbares Maß.

In einer Risikoanalyse wird versucht, die Risiken zu erkennen und zu bewerten und so das Gesamtrisiko zu ermitteln. Ziel ist es, in weiterer Folge dieses Risiko so weit zu reduzieren, dass das verbleibende Restrisiko quantifizierbar und akzeptierbar wird.

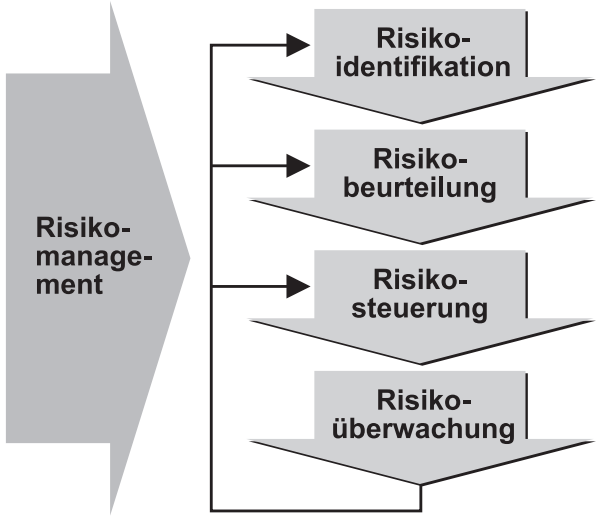


Abbildung 2.3: Bestandteile eines Risikomanagementsystems

Unter Risikomanagement wird somit die Gesamtheit aller systematischen Maßnahmen der Identifikation, Analyse, Bewertung und Steuerung jener Risiken verstanden, die den Betreiber in seinen IT-Sicherheitszielen bedrohen.

Risikoidentifikation. Die Risikoidentifikation beinhaltet eine strukturierte, detaillierte und vollständige Erfassung aller wesentlichen Risiken, bzw. Schadensgefahren und Verlustpotentiale aller relevanter Aktivitäten einschließlich ihrer Wirkungszusammenhänge. Sie dient als Informationsbasis für die nachgelagerten Prozessschritte.

Risikobeurteilung. An die Risikoidentifikation knüpft die Risikobeurteilung an. Hierbei handelt es sich um die zielgerichtete Analyse und Bewertung interner und externer Risikopotentiale.

Risikosteuerung. Gegenstand der Risikosteuerung ist die aktive Beeinflussung, der im Rahmen von Risikoidentifikation und -beurteilung ermittelten und analysierten Risiken. Ziel ist es, alle wesentlichen Schadensgefahren und Verlustpotentiale durch gezielte steuernde Maßnahmen zu kontrollieren. Hierbei stehen grundsätzlich folgende Strategiealternativen zur Verfügung:

- Vermeiden➜
  - Unterlassen risikoträchtiger Geschäfte
- Überwälzen➜
  - Weitergabe des Risikos an Geschäftspartner
- Vermindern➜
  - Reduktion auf ein Restrisiko
- Akzeptieren➜
  - kontinuierliche Beobachtung in Kauf genommener Risiken

Die Verminderung von Risiken bedeutet, den identifizierten Risiken eine geeignete Steuerungsmaßnahme entgegenzusetzen.

Das Akzeptieren von Risiken, die sich nur minimal auf die Organisation auswirken, kommt darin zum Ausdruck, dass keine weitergehenden Steuerungsmaßnahmen erforderlich werden. Die permanente Überwachung ist aber auch in diesem Zusammenhang von eminenter Wichtigkeit.

Risikoüberwachung. Unter Risikoüberwachung ist die Kontrolle der Durchführung zur Risikosteuerung ergriffener Maßnahmen zu verstehen. Sie geht von den jeweiligen Verantwortlichen aus und wird gegenüber den operativ Verantwortlichen ausgeübt.

Abbildung 2.4: Beispielhafte Risiken für das IT-Sicherheitsmanagement einer Organisation

Entwicklung und Fortschreibung des Notfallmanagements

Es ist von existenzieller Bedeutung für eine Organisation potentielle bzw. reale Sicherheitsprobleme

- zu entdecken,
- hierauf angemessen zu reagieren,
- diese zu analysieren sowie
- aus diesen Präventivmaßnahmen abzuleiten.

Abhängig von der Schwere und Häufigkeit der auftretenden Probleme haben diese Einfluss auf die IT-Sicherheitspolitik des Betreibers.

IT-Sicherheit im laufenden Betrieb

Umfassendes IT-Sicherheitsmanagement beinhaltet nicht zuletzt auch die Aufgabe, die IT-Sicherheit im laufenden Betrieb aufrechtzuerhalten und gegebenenfalls veränderten Bedingungen anzupassen.

Zu den erforderlichen Aktivitäten zählen:

- Aufrechterhaltung des erreichten Sicherheitsniveaus

  dies umfasst:

  - Wartung und administrativen Support von Sicherheitseinrichtungen,
  - die Überprüfung von Maßnahmen auf Übereinstimmung mit der IT-Sicherheitspolitik (Security Compliance Checking),
  - die fortlaufende Überwachung der IT-Systeme (Monitoring),
  - Reaktion auf sicherheitsrelevante Ereignisse (Incident Handling),
  - Change Management.

2.2.3 Informationssicherheits-Managementsysteme (ISMS)

Die Verknüpfung eines Qualitätsmanagementsystems nach DIN EN ISO 9001:2000 und eines IT-Sicherheitsmanagementsystems kann mit relativ geringem Aufwand über ein ISMS auf Basis der Forderungen der BS 7799 erfolgen. Die Forderungen der BS 7799 lassen sich gut in ein Qualitätsmanagementsystem integrieren.

Historie

1993 wurde der CoP (Code of Practice) for Information Security Management verabschiedet, welcher als Basis für eine effektive Sicherheitsorganisation mit definierten Sicherheitsstandards für Unternehmen entwickelt wurde.

Zwei Jahre nach seiner Verabschiedung (1995) erhielt der CoP den offiziellen Status eines Britischen Standards (BS 7799).

Kurz nach der Fertigstellung von BS 7799-1 wurde der Prozess zur Entwicklung eines Informationssicherheits-Managementsystems erarbeitet. Dies ist Inhalt des BS 7799-2.

Der British Standard BS7799 wird in zwei Teilen herausgegeben:

- BS 7799-1: jetzt ISO IEC 17799, Dezember 2000
  Management von Informationssicherheit
  Leitfaden zum Management von Informationssicherheit
- BS 7799-2: 1999
  Management von Informationssicherheit
  Spezifikation für Informationssicherheits-Managementsysteme

Die BS 7799-1 hält in ihrem Vorwort zu ihrer Aufgabe fest:

> *»Die Norm BS 7799-1 (ISO IEC 17799) wurde 1995 das erste Mal herausgegeben, um eine umfassende Sammlung von Maßnahmen bereitzustellen, in der die besten Praktiken in der Informationssicherheit enthalten sind. Sie soll gemeinsamer Bezugspunkt zur Identifizierung der verschiedenen Maßnahmen sein, die für die meisten Situationen erforderlich sind, in denen Informationssysteme in Industrie und Handel zum Einsatz kommen.«*
> *»In der überarbeiteten Fassung von 1999 werden die neuesten Entwicklungen in der Anwendung von Informationsverarbeitung berücksichtigt, insbesondere Netzwerke und Kommunikationstechnologie. Außerdem wird die Beteiligung von Unternehmen an der Informationssicherheit und ihre Verantwortung betont.«*

BS 7799-1 beinhaltet somit 136 Einzelmaßnahmen für die Einführung, Implementierung und Erhaltung eines Informationssicherheits-Managementsystems.

Die BS 7799-2 hält in ihrem Vorwort zu ihrer Aufgabe fest:

> *»Die Norm BS 7799-2 dient als Basis für die Beurteilung eines Managementsystems für Informationssicherheit (ISMS – Information Security Management System) für die Gesamtheit oder einen Teil einer Organisation. Sie kann als Basis für ein formales Verfahren zur Zertifizierung verwendet werden.«.*
> *»Diese Spezifikation basiert auf der Norm BS 7799-1, Management von Informationssicherheit, Teil 1: Leitfaden zum Management von Informationssicherheit, die Richtlinien für das beste Vorgehen bei der Erfüllung der Anforderungen dieser Spezifikation gibt.«*

Die BS 7799-2 bzw. der international anerkannte Leitfaden ISO/IEC 17799 (auf Basis des British Standard BS 7799), ist ein anerkanntes europäisches Regelwerk für die Implementierung eines Informations-Sicherheits-Managementsystems (ISMS).

Anforderungen an das Informationssicherheits-Managementsystem nach ISO/IEC 17799

Eine Organisation hat ein dokumentiertes Informationssicherheits-Managementsystem zu schaffen, welches folgende Punkte umfasst:

1. Definition der Informationssicherheitspolitik
2. Bestimmung des Anwendungsbereiches des Informationssicherheits-Managementsystems

   Die Grenzen hinsichtlich der Merkmale der Organisation, des Standortes, der Werte und der Technologie sind festzulegen.
3. Durchführung einer angemessenen Risikoanalyse

   Die Risikoanalyse muss die Bedrohungen der Werte, die Schwachstellen und Auswirkungen auf die Organisation identifizieren und die Höhe des Risikos bestimmen.
4. Managen des Risikos

   Die zu verwaltenden Risikobereiche sind auf der Basis der Informationssicherheitspolitik der Organisation und des erforderlichen Grads an Gewährleistung von Sicherheit zu identifizieren.
5. Festlegung der Überwachungsmaßnahmen und deren Umsetzung

   Geeignete Sicherheitsziele und Maßnahmen sind zur Implementierung durch die Organisation auszuwählen und die Auswahl ist zu begründen.
6. Nachweis der Anwendung

   Eine Erklärung der Anwendbarkeit ist zu erstellen. Die ausgewählten Sicherheitsziele und Maßnahmen sowie die Gründe für ihre Auswahl sind in der Erklärung zur Anwendbarkeit zu dokumentieren. Diese Erklärung muss auch eine Aufzeichnung über den etwaigen Ausschluss bestimmter Maßnahmen enthalten.

Zur Einführung eines Informationssicherheits-Managementsystem nach BS 7799-2 ist es erforderlich, die vollständige Umsetzung der Forderungen, die Wirksamkeit und Angemessenheit des Systems zu gewährleisten. Hierbei – und dies ist zu betonen – ist eine Integration in ein bestehendes QM-System leicht möglich.

Die Forderungen der BS 7799-2 sind nachfolgend aufgeführt:

1. **Sicherheitspolitik**

   Stichwort: Informationssicherheitspolitik.

2. **Organisation der Sicherheit**

   Stichworte: Infrastruktur der Informationssicherheit, Sicherheit bei dem Zugang durch Fremdunternehmen, Outsourcing.

3. **Einstufung und Kontrolle der Werte**

   Stichworte: Zurechenbarkeit für Werte, Einstufung von Informationen.

4. **Personelle Sicherheit**

   Stichworte: Sicherheit bei der Stellenbeschreibung und bei der Bereitstellung von Ressourcen, Benutzerschulung, Verhalten bei Sicherheitsvorfällen und Störungen.

5. **Physische und umgebungsbezogene Sicherheit**

   Stichworte: Sicherheitszonen, Sicherheit der Geräte.

6. **Management der Kommunikation und des Betriebs**

   Stichworte: Betriebsverfahren und -verantwortlichkeiten, Systemplanung und -abnahme, Schutz vor bösartiger Software, Haushaltsorganisation, Netzwerkmanagement, Umgang mit und Sicherheit von Datenträgern, Austausch von Informationen und Software.

7. **Zugangskontrolle**

   Stichworte: Geschäftsanforderungen an die Zugangskontrolle, Verwaltung der Zugriffsrechte der Benutzer, Verantwortung der Benutzer, Netzzugriffskontrolle, Kontrolle des Betriebssystemzugriffs, Zugriffskontrolle für Anwendungen, Überwachung des Systemzugriffs und der Systembenutzung, Mobile Computing und Telearbeit.

8. **Systementwicklung und -wartung**

   Stichworte: Sicherheitsanforderungen an Systeme, Sicherheit in Anwendungssysteme, kryptografische Maßnahmen, Sicherheit von Systemdateien, Sicherheit bei Entwicklungs- und Supportprozessen.

9. **Management des kontinuierlichen Geschäftsbetriebs**

   Stichwort: Aspekte zur Aufrechterhaltung des Geschäftsbetriebs.

10. **Einhaltungen der Verpflichtungen**

    Stichworte: Einhaltung gesetzlicher Verpflichtungen, Überprüfung der Sicherheitspolitik und der Einhaltung technischer Normen, Überlegungen zum Systemaudit.

Mit Hilfe der Standards des BS 7799 ist es für Organisationen möglich ein zertifizierungsfähiges Managementsystem aufzubauen, das einen präventiven und ganzheitlichen Ansatz hat.

Zusammenfassend ist festzuhalten, dass ein solches Informationssicherheits-Managementsystem nach BS 7799 folgende Nutzen aufweist:

- Strukturelle Vorgehensweise im Umgang mit dem Thema IT-Sicherheit
- Ermittlung, Einschätzung und Beherrschung von Risiken und somit die Schaffung eines angemessenen Risikobewusstseins innerhalb einer Organisation
- Präventives Handeln statt Reaktion auf Vorfälle
- Erfassung und Bewertung aller Werte einer Organisation (Informationen, Daten, Dokumente, Geräte, Hardware, Software, Dienste, Image)
- Reduzierung von Haftungsrisiken für das Management
- Schaffung eines IT-Sicherheitsbewusstseins innerhalb einer Organisation
- Positiver Werbeauftritt in Richtung möglicher Auftraggeber (Schaffung von Kundenvertrauen)
- Imagesteigerung nach Außen

Die genannten positive Effekte können sich jedoch nur ergeben, wenn – und hierbei kann wiederum die BS 7799 zitiert werden – für die Implementierung eines IT-Sicherheitsmanagements folgende wichtigen Faktoren berücksichtigt werden:

- Die Vorgabe konkreter IT-Sicherheitsvorgaben (Politik, Ziele)
- Die Implementierung der IT-Sicherheit in Übereinstimmung mit der Organisation
- Das Engagement des Managements
- Eine umfassende Risikoanalyse
- Umfassende und aktuelle Schulungen im Rahmen der IT-Sicherheitsvorgaben

Literatur. *[1]* ISO (Hrsg.): The ISO Survey of ISO 9000 and ISO 14000 Certificates, 9th cycle, Genf 2000

[2] Seghezzi, H.D.: Integriertes Qualitätsmanagement, München, Wien 1996

3 Zertifikat zur IT-Sicherheit

Isabel Münch

Dr. Harald Niggemann

3.1 Kann ich meine IT-Sicherheit zertifizieren lassen?

Viele Unternehmen und Behörden sehen derzeit die Notwendigkeit nach einem Zertifikat, das ihre umfangreichen Bemühungen um die IT-Sicherheit ihres Unternehmen würdigt. Hierfür werden unter anderem folgende Gründe aufgeführt:

- IT-Dienstleister müssen mit Hilfe eines Zertifikats einen vertrauenswürdigen Nachweis führen, dass sie die Maßnahmen nach dem IT-Grundschutzhandbuch realisiert haben;
- Kooperierende Unternehmen möchten sich darüber informieren, welchen Grad von IT-Sicherheit sie ihren Geschäftspartner zusichern können;
- Von Institutionen, die an ein Netz neu angeschlossen werden, wird der Nachweis verlangt, dass sie eine ausreichende IT-Sicherheit besitzen, damit durch den Anschluss ans Netz keine untragbaren Risiken entstehen;
- Unternehmen und Behörden möchten dem Kunden bzw. Bürger gegenüber ihre Bemühungen um eine ausreichende IT-Sicherheit deutlich machen.

3.2 Was ist IT-Grundschutz bzw. was ist eine ausreichende IT-Sicherheit?

Im IT-Grundschutzhandbuch *[1]*, das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben wird, werden Standardsicherheitsmaßnahmen für typische IT-Systeme empfohlen. Das Ziel dieser IT-Grundschutz-Empfehlungen ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das einerseits für den normalen Schutzbedarf angemessen und ausreichend ist und andererseits als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann.

Um den sehr heterogenen Bereich der IT einschließlich der Einsatzumgebung besser strukturieren und aufbereiten zu können, verfolgt das IT-Grundschutzhandbuch das Baukastenprinzip. Die einzelnen Bausteine spiegeln typische Bereiche des IT-Einsatzes wider, wie beispielsweise Client-Server-Netze, bauliche Einrichtungen, Kommunikations- und Applikationskomponenten. In jedem Baustein wird zunächst die zu erwartende Gefährdungslage beschrieben, wobei sowohl die typischen Gefährdungen als auch die pauschalisierten Eintrittswahrscheinlichkeiten berücksichtigt werden. Diese Gefährdungslage bildet die Grundlage, um ein spezifisches Maßnahmenbündel aus den Bereichen Infrastruktur, Personal, Organisation, Hard- und Software, Kommunikation und Notfallvorsorge zu generieren. Die Gefährdungslage wird zur Sensibilisierung angeführt, für die Erstellung eines Sicherheitskonzeptes nach IT-Grundschutz wird sie nicht weiter benötigt. Um das für einen durchschnittlichen Schutzbedarf notwendige Sicherheitsniveau zu erreichen, brauchen die Anwender die vorgenannten aufwändigen Analysen nicht durchzuführen. Es ist vielmehr ausreichend, die für das relevante IT-System oder den betrachteten IT-Verbund entsprechenden Bausteine zu identifizieren und die darin empfohlenen Maßnahmen konsequent und vollständig umzusetzen.

Mit Hilfe des IT-Grundschutzhandbuchs lassen sich IT-Sicherheitskonzepte einfach und arbeitsökonomisch realisieren.

Bei der traditionellen Risikoanalyse werden zunächst die Gefährdungen ermittelt und mit Eintrittswahrscheinlichkeiten bewertet, um dann die geeigneten IT-Sicherheitsmaßnahmen auszuwählen und anschließend das noch verbleibende Restrisiko bewerten zu können.

Bei Anwendung des IT-Grundschutzhandbuchs wird hingegen nur ein Soll-Ist-Vergleich zwischen empfohlenen und bereits realisierten Maßnahmen durchgeführt. Dabei festgestellte fehlende und noch nicht umgesetzte Maßnahmen zeigen die Sicherheitsdefizite auf, die es durch die empfohlenen Maßnahmen zu beheben gilt.

Erst bei einem signifikant höheren Schutzbedarf muss zusätzlich eine ergänzende Sicherheitsanalyse unter Beachtung von Kosten- und Wirksamkeitsaspekten durchgeführt werden. Hierbei reicht es dann aber in der Regel aus, die Maßnahmenempfehlungen des IT-Grundschutzhandbuchs durch entsprechende individuelle, qualitativ höherwertige Maßnahmen, zu ergänzen.

Bei den im IT-Grundschutzhandbuch aufgeführten Maßnahmen handelt es sich um Standardsicherheitsmaßnahmen, also um diejenigen Maßnahmen, die für die jeweiligen Bausteine nach dem Stand der Technik umzusetzen sind, um eine angemessene Sicherheit zu erreichen. Teilweise wird mit diesen Maßnahmen auch bereits ein höherer Schutzbedarf abgedeckt, trotzdem sind sie in den jeweiligen Bereichen das Minimum dessen, was vernünftigerweise an Sicherheitsvorkehrungen umzusetzen ist.

Angesichts der Innovationsschübe und Versionswechsel im IT-Bereich ist das IT-Grundschutzhandbuch auf leichte Erweiterbarkeit und Aktualisierbarkeit ausgerichtet. Das BSI überarbeitet und aktualisiert regelmäßig das

IT-Grundschutzhandbuch, um die Empfehlungen auf dem Stand der Technik zu halten.

Das IT-Grundschutzhandbuch ist somit ein lebendes Werk. Dasselbe gilt für die IT-Grundschutz-Zertifizierung. Es empfiehlt sich immer, regelmäßig auf den BSI-Webseiten nachzusehen, ob es Neuigkeiten in diesem Bereich gibt oder sich auf die Mailinglisten zum IT-Grundschutz setzen zu lassen, um automatisch auf dem Laufenden gehalten zu werden.

Die aktuelle Ausgabe des IT-Grundschutzhandbuch (Version Mai 2002) ist um die Bausteine

- Windows 2000 Client,
- Windows 2000 Server,
- Internet-PC sowie
- Novell eDirectory

erweitert worden.

Neben diesen neuen Bausteinen wurden zahlreiche Ergänzungen und Aktualisierungen der vorhandenen Texte vorgenommen. So enthält der Peer-to-Peer-Baustein nun auch Sicherheitsempfehlungen für Windows 2000 und Linux.

3.3 Wer kann zertifizieren? Wie wird man Auditor?

Der Antrag auf Lizenzierung als IT-Grundschutz-Auditor beim BSI ist natürlichen Personen vorbehalten. Die Teilnahme am Lizenzierungsverfahren ist gebührenpflichtig.

Für die Teilnahme am Lizenzierungsverfahren *[2]* zum IT-Grundschutz-Auditor gelten folgende Zulassungsvoraussetzungen:

- Der Antragsteller muss ausreichende Kenntnisse im Bereich der IT-Sicherheit besitzen und diese auch praktisch angewendet haben. Daher muss er nachweisen, dass er in den zurückliegenden zwei Jahren im Umfeld der IT-Sicherheit tätig gewesen ist. Beispiele für entsprechende Tätigkeitsfelder sind IT-Sicherheitsbeauftragte oder Berater für IT-Sicherheit.
- Insbesondere sollte er im Bereich IT-Sicherheitsmanagement Aufgaben wie die folgenden wahrgenommen haben:
  - Entwicklung von IT-Sicherheitszielen, -strategien sowie IT-Sicherheitsleitlinien,
  - Umsetzung bzw. Überprüfung von IT-Sicherheitsleitlinien,
  - Initiierung, Steuerung und Kontrolle des IT-Sicherheitsprozesses,

- Erstellung des IT-Sicherheitskonzepts,
- Überprüfung von IT-Sicherheitsmaßnahmen,
- Aufbau und Durchführung von Schulungs- und Sensibilisierungsprogrammen,
- Beratung in übergreifenden IT-Sicherheitsfragen.

- Der Antragsteller muss in den zurückliegenden fünf Jahren mindestens drei Projekte durchgeführt haben, in denen die Anwendung des IT-Grundschutzhandbuchs wesentlicher Bestandteil war. Hierzu zählen sowohl interne Projekte innerhalb einer Organisation als auch externe Projekte, z.B. Beratungsdienstleistungen. Beispiele für geeignete Projektinhalte sind IT-Sicherheitskonzeptionen oder IT-Sicherheitsrevisionen gemäß dem IT-Grundschutzhandbuch.

Kann die Fachkunde nicht ausreichend nachgewiesen werden, wird der Antragsteller nicht für das Lizenzierungsverfahren zugelassen.

Nach der 1,5-tägigen Schulung findet eine Prüfung über die Anwendungsweise und Inhalte des IT-Grundschutzhandbuchs und insbesondere über das Prüfschema für IT-Grundschutz-Audits statt. Nach erfolgreicher Prüfung wird der Abschluss des Lizenzierungsvertrages mit dem BSI möglich.

Die Lizenz wird erteilt, wenn folgende Bedingungen erfüllt sind:

- die Fachkundennachweise sind ausreichend
- die Schulungsveranstaltung wurde absolviert
- die Prüfung wurde bestanden
- der Lizenzierungsvertrag zwischen BSI und Auditor wurde unterzeichnet
- die Kosten für die Lizenzerteilung wurden entrichtet

Die Lizenzurkunde enthält folgende Informationen:

- vollständiger Name und Adresse des Lizenznehmers
- auf Wunsch Name und Adresse des Arbeitgebers
- Beginn der Gültigkeit
- Ende der Gültigkeit

Die Lizenzurkunde bestätigt, dass der Lizenznehmer für die Dauer der Gültigkeit befugt ist, IT-Grundschutz-Audits für die Erlangung von IT-Grundschutz-Zertifikaten durchzuführen. Er darf außerdem IT-Grundschutz-Selbsterklärungen (Einstiegsstufe oder Aufbaustufe) durch ein Testat bestätigen.

Die Lizenzurkunde des Herausgebers dieses Buches, Thomas Krampert, führt die BSI-Registrierungsnummer:

BSI-GSL-0011-2002

Diese Bezeichnung hat folgende Bedeutung:

BSI = Lizenzverleihende Stelle

GSL = IT-Grundschutz-Lizenz

0011 = laufende Vorgangsnummer

2002 = Jahr der Lizenzvergabe

Durch jährliche Auditoren-Treffen wird der Erfahrungsaustausch zwischen den lizenzierten IT-Grundschutz-Auditoren ermöglicht. Eine Lizenz ist für einen Zeitraum von fünf Jahren gültig.

Das BSI kann auch eine erteilte Lizenz entziehen, wenn der Auditor mehrfach am Erfahrungsaustausch nicht teilnimmt oder schwerwiegende Verstöße gegen das Prüfschema vorliegen.

3.3.1 Aufgaben des Auditors

Das Prüfschema für Auditoren *[3]* beschreibt die verbindliche Vorgehensweise, wie Auditoren die für die Erlangung einer Selbsterklärung (Einstiegsstufe oder Aufbaustufe) oder eines IT-Grundschutz-Zertifikats erforderlichen Prüfungen durchführen müssen.

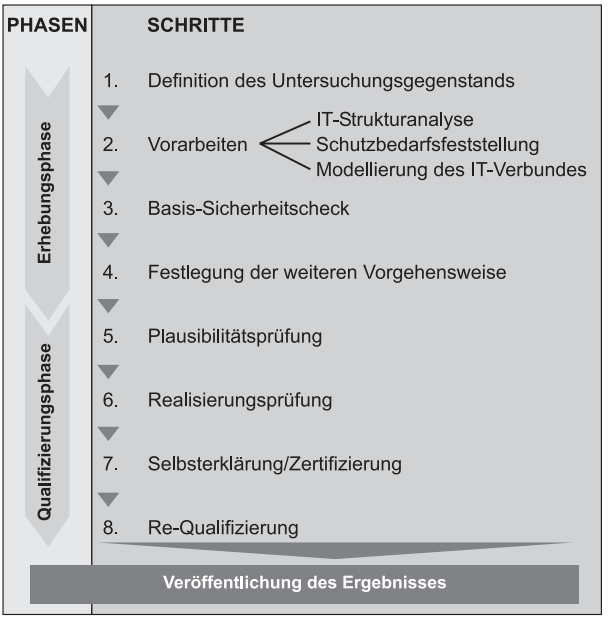


Abbildung 3.1: Aufgaben des Auditors

3.4 Wie komme ich als Unternehmen zum Zertifikat?

Mit dem Qualifizierungs- und Zertifizierungsschema für IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird Behörden und Unternehmen diese Möglichkeit gegeben, ihre Aktivitäten zur IT-Sicherheit und die erfolgreiche Umsetzung von IT-Grundschutz nach innen und außen zu dokumentieren. Rechtliche Grundlagen des Verfahrens sind das Errichtungsgesetz des Bundesamtes für Sicherheit in der Informationstechnik sowie ein entsprechender Erlass des Bundesministeriums des Innern vom 6. Februar 2001. Mit einem solchen Zertifikat kann ein Unternehmen oder eine Behörde für einen ausgewählten IT-Bereich nachweisen, dass ein Sicherheitsmanagementsystem etabliert ist und dass die erforderlichen baulichen, personellen, organisatorischen und technischen IT-Grundschutzmaßnahmen realisiert sind.

Grundlage für die Vergabe eines IT-Grundschutz-Zertifikats ist die Durchführung eines Audits durch einen externen, beim BSI lizenzierten Auditor. Der Herausgeber dieses Buches, Thomas Krampert, ist ein vom BSI lizenzierter IT-Grundschutz-Auditor.

Ziel der IT-Grundschutz-Zertifizierung ist es, einen Maßstab für die tatsächlich umgesetzten Standard-Sicherheitsmaßnahmen in informationstechnischen Einrichtungen von Behörden und Unternehmen zu etablieren und damit die Möglichkeit des Nachweises eines definierten Sicherheitsniveaus anzubieten.

Das BSI hat derzeit drei Ausprägungen der IT-Grundschutz-Qualifizierung definiert:

3.4.1 IT-Grundschutz-Zertifikat

Das IT-Grundschutz-Zertifikat stellt den höchsten Grad an Vertrauenswürdigkeit und das höchste Sicherheitsniveau dar. Das Zertifikat wird durch Zertifizierungsstellen vergeben, die für die Vergabe des IT-Grundschutz-Zertifikats akkreditiert sind, derzeit nur durch das BSI selbst. Voraussetzung ist, dass die Umsetzung der im IT-Grundschutzhandbuch beschriebenen und im vorliegenden Fall relevanten Standard-Sicherheitsmaßnahmen durch einen lizenzierten Auditor bestätigt ist.

Die Umsetzung aller für einen vorliegenden Anwendungsfall relevanten IT-Grundschutzmaßnahmen können jedoch unter Umständen mit erheblichem Aufwand verbunden sein. Die zwei Vorstufen des eigentlichen IT-Grundschutz-Zertifikats erlauben eine schrittweise Umsetzung der Standard-Sicherheitsmaßnahmen:

Selbsterklärung »IT-Grundschutz Aufbaustufe«

*Voraussetzung für die Selbsterklärung »IT-Grundschutz Aufbaustufe ist, dass die Behörde oder das Unternehmen die **wichtigsten** Standard-Sicherheitsmaßnahmen des IT-Grundschutzhandbuchs umgesetzt hat.*

Zitat: IT-Grundschutzhandbuch, Version Mai 2002

Die notwendigen Vorarbeiten und Erhebungen können dabei sowohl von Dritten als auch von Mitarbeitern der eigenen Institution erfolgen. Die Selbsterklärung wird darauf basierend von einem zeichnungsbefugten Vertreter der Institution abgegeben.

Selbsterklärung »IT-Grundschutz Einstiegsstufe«

*Die IT-Grundschutz-Qualifizierung in der Einstiegsstufe wird erreicht, wenn die Behörde oder das Unternehmen lediglich die **unabdingbaren** Standard-Sicherheitsmaßnahmen des IT-Grundschutzhandbuchs umgesetzt hat.*

Zitat: IT-Grundschutzhandbuch, Version Mai 2002

Wie bei der Aufbaustufe können die Vorarbeiten und Erhebungen sowohl durch Dritte als auch durch eigene Mitarbeiter erfolgen. Die Selbsterklärung wird wiederum von einem zeichnungsbefugten Vertreter der Institution abgegeben. Das durch die Selbsterklärung »IT-Grundschutz Einstiegsstufe« dargestellte Sicherheitsniveau ist das geringste der drei Ausprägungen.

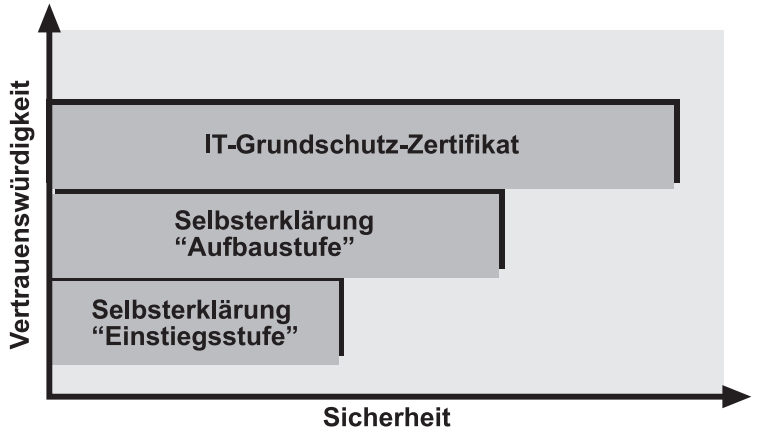


Abbildung 3.2: Darstellung der Sicherheitsausprägungen

Die Einstiegs- bzw. Aufbaustufe dienen als Meilensteine bis zur Erreichung des IT-Grundschutz-Zertifikats.

Nur das IT-Grundschutz-Zertifikat attestiert die Realisierung eines »umfassenden IT-Grundschutzes«.

Zitat: IT-Grundschutzhandbuch, Version Mai 2002

Welche Maßnahmen müssen für welche Stufe der IT-Grundschutz-Qualifizierung umgesetzt sein? Zu jedem Baustein des IT-Grundschutzhandbuchs werden die Maßnahmen für die drei Ausprägungen gekennzeichnet:

»**A**« Die Umsetzung dieser Maßnahme ist für alle Stufen der IT-Grundschutz-Qualifizierung erforderlich.

»**B**« Die Umsetzung dieser Maßnahme ist für die Aufbaustufe und für das Zertifikat erforderlich.

»**C**« Die Umsetzung dieser Maßnahme ist nur für das IT-Grundschutz-Zertifikat erforderlich.

»**Z**« Die Umsetzung dieser zusätzlichen IT-Sicherheitsmaßnahmen sollte zur Steigerung der IT-Sicherheit erfolgen, ist jedoch zur Qualifizierung nach IT-Grundschutz nicht erforderlich.

Tab. 3.1: Auszug aus einem Baustein IT-Grundschutz

Einstieg	Aufbau	Zertifikat	Zusätz.	Maßnahme	Prio.	Maßnahmentitel	Begründung
			Z	M 1.29	(3)	Geeignete Aufstellung eines IT-Systems (optional)	
	B			M 2.3	(2)	Datenträgerverwaltung	
	B			M 2.4	(2)	Regelungen für Wartungs- und Reparaturarbeiten	
A				M 2.9	(2)	Nutzungsverbot nicht freigegebener Software	
		C		M 2.10	(3)	Überprüfung des Software-Bestandes	
A				M 2.13	(2)	Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln	
			Z	M 2.22	(2)	Hinterlegen des Passwortes	
A				M 2.25	(1)	Dokumentation der Systemkonfiguration	

Für die Qualifizierung nach IT-Grundschutz *[4]* ist ein Prozess zu durchlaufen, der sich in zwei Phasen unterteilen lässt: Die Erhebungsphase und die Qualifizierungsphase. Innerhalb dieser Phasen werden 8 Schritte durchlaufen, die nachfolgend dargestellt werden.

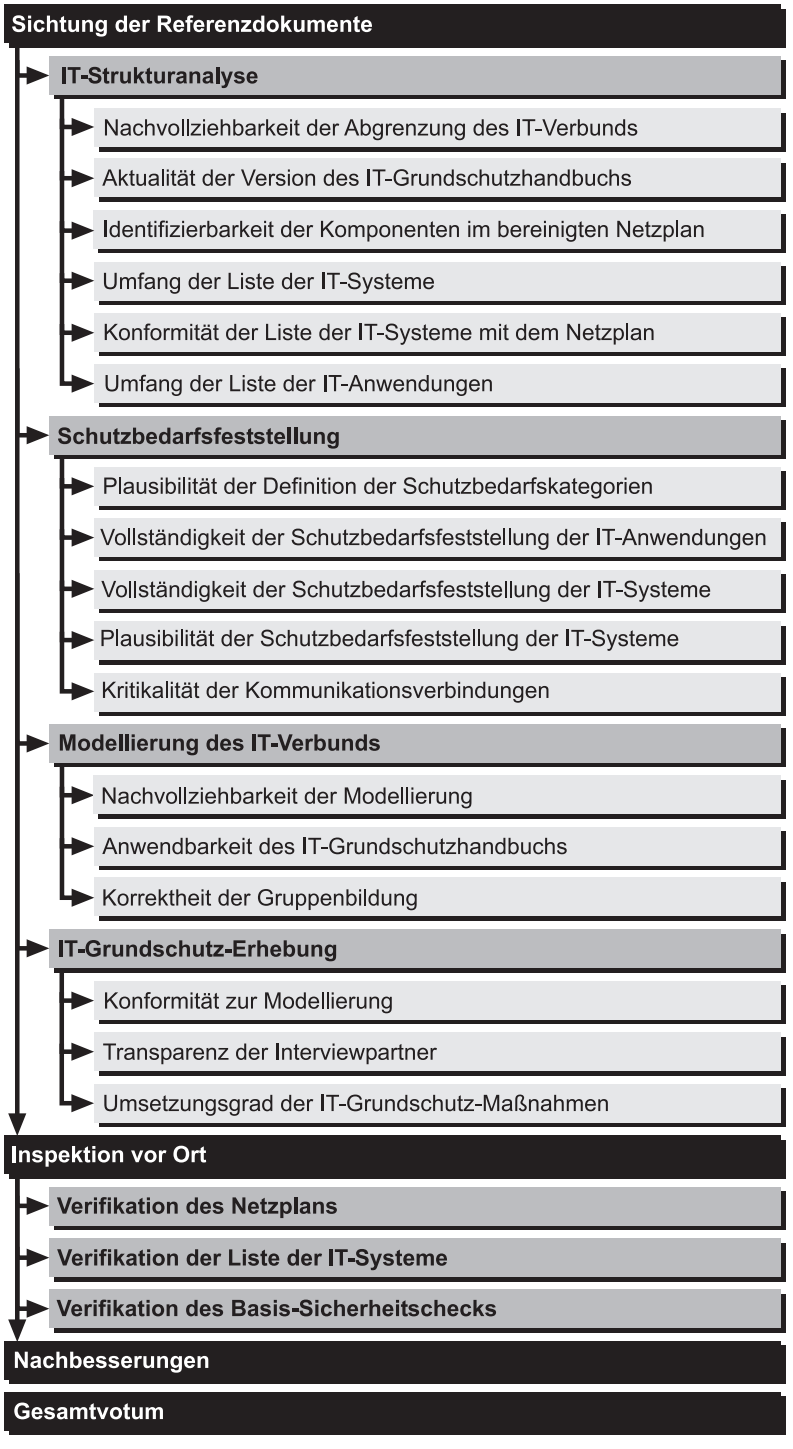


Abbildung 3.3: Qualifizierungsprozess

Erhebungsphase

Bei der Erhebungsphase werden – wie der Name schon sagt – die Vorarbeiten im Hinblick auf die Qualifizierung durchgeführt.

Schritt 1: Definition des Untersuchungsgegenstands. Es wird festgelegt, welcher Teilbereich des Unternehmens bzw. der Behörde untersucht werden soll. Der Untersuchungsgegenstand wird dabei als »IT-Verbund« bezeichnet.

> *Um eine angemessene Sicherheitsaussage zu gewährleisten, sollte der betrachtete IT-Verbund mindestens die Fachanwendungen einer Organisationseinheit oder eines Geschäftsprozesses und alle hierzu benötigten informationstechnischen Komponenten umfassen.*

`Zitat: Qualifizierung nach IT-Grundschutz, Eckpunktepapier`

Einzelne Clients, Server oder Netzverbindungen sind nicht geeignete Untersuchungsgegenstände.

Schritt 2: Vorarbeiten. Grundlage für die Qualifizierung nach IT-Grundschutz ist das IT-Grundschutzhandbuch des BSI. Im einzelnen sind dies folgende Vorarbeiten:

- IT-Strukturanalyse (siehe Kapitel 2.1 im IT-Grundschutzhandbuch)
- Schutzbedarfsfeststellung (siehe Kapitel 2.2 im IT-Grundschutzhandbuch)
- Modellierung des IT-Verbunds (siehe Kapitel 2.3 im IT-Grundschutzhandbuch)

Die Bausteine des IT-Grundschutzhandbuchs, die für den jeweiligen IT-Verbund obligatorisch für die Qualifizierung sind, werden im Kapitel 2.3 des Handbuchs definiert und sind bei der Modellierung zu berücksichtigen.

Schritt 3: Basis-Sicherheitscheck. Die Vorgehensweise zur Durchführung eines Basis-Sicherheitschecks ist im IT-Grundschutzhandbuch beschrieben. Der Status für jede Maßnahme, die in modellierten Bausteinen des Handbuchs beschrieben sind, wird bei der Durchführung des Basis-Sicherheitschecks ermittelt. Dieser kann vier verschiedene Werte annehmen:

»ja«	Alle Empfehlungen in der Maßnahme sind sinngemäß umgesetzt.
»entbehrlich«	Die Maßnahme muss im vorliegenden Umfeld nicht umgesetzt werden. Eine stichhaltige und nachvollziehbare Begründung liegt vor.
»teilweise«	Einige Empfehlungen in der Maßnahme sind nicht oder nur teilweise umgesetzt.
»nein«	Die Empfehlungen in der Maßnahme sind größtenteils nicht umgesetzt.

Alle Standard-Sicherheitsmaßnahmen, die für die angestrebte Stufe der IT-Grundschutz-Qualifizierung erforderlich sind, müssen entweder den Umsetzungsstatus »entbehrlich« oder »ja« haben. Entscheidend ist dabei, dass die Maßnahmen nach Sinn und Zweck umgesetzt sind. Aufgrund der vielfältigen Einsatzumgebungen und individuellen Rahmenbedingungen ist eine »wortgetreue« Umsetzung der IT-Grundschutzmaßnahmen in vielen Fällen nicht zweckmäßig.

Schritt 4: Festlegung der weiteren Vorgehensweise. Nun kann eine Voraussage darüber getroffen werden, ob eine Qualifizierung nach IT-Grundschutz möglich ist:

> *Haben praktisch alle mit »A« gekennzeichneten Maßnahmen den Status »ja« oder »entbehrlich«, können die nachfolgenden Schritte des Qualifizierungsprozesses mit dem Ziel der Selbsterklärung »Einstiegsstufe« durchlaufen werden.*
>
> *Haben praktisch alle mit »A« oder »B« gekennzeichneten Maßnahmen den Status »ja« oder »entbehrlich«, können die nachfolgenden Schritte des Qualifizierungsprozesses mit dem Ziel der Selbsterklärung »Aufbaustufe« durchlaufen werden.*
>
> *Haben praktisch alle mit »A«, »B« oder »C« gekennzeichneten Maßnahmen den Status »ja« oder »entbehrlich«, können die nachfolgenden Schritte des Qualifizierungsprozesses mit dem Ziel der Zertifizierung durchlaufen werden.*

`Zitat: Qualifizierung nach IT-Grundschutz, Eckpunktepapier`

Eventuell sind Nachbesserungen erforderlich. Nach Umsetzung der fehlenden Maßnahmen ist der Umsetzungsstatus zu aktualisieren.

Jetzt kann die eigentliche Qualifizierung beginnen.

Qualifizierungsphase

Schritt 5: Kann die eigentliche Qualifizierung beginnen?
Plausibilitätsprüfung. Der Auditor nimmt folgende Plausibilitätsprüfungen vor:

> *Der definierte IT-Verbund muss eine sinnvolle Mindestgröße haben und dient beispielsweise zur IT-Unterstützung einer Fachaufgabe oder einer Organisationseinheit.*
>
> *Die IT-Strukturanalyse und die Schutzbedarfsfeststellung müssen plausibel sein.*
>
> *Die Modellierung des IT-Verbundes muss ordnungsgemäß sein.*
>
> *Der Basis-Sicherheitscheck muss vollständig und die Ergebnisse, insbesondere die Begründungen, müssen plausibel sein.*

`Zitat: Qualifizierung nach IT-Grundschutz, Eckpunktepapier`

Schritt 6: Realisierungsprüfung. Der im Basis-Sicherheitscheck ermittelte Umsetzungsstatus wird stichprobenartig überprüft. Hierzu ist die erarbeitete Modellierung des vorliegenden IT-Verbunds Ausgangsbasis. Der Auditor muss für die Realisierungsprüfung aus der Modellierung des vorliegenden IT-Verbunds folgende Bausteine auswählen:

Der Baustein IT-Sicherheitsmanagement wird in jedem Fall überprüft. Hierdurch wird sichergestellt, dass IT-Sicherheit in der Institution ordnungsgemäß gesteuert wird.

Aus jeder der fünf Schichten wird mindestens ein Baustein geprüft. Damit wird erreicht, dass sich die Realisierungsprüfung auf möglichst verschiedene Aspekte der IT-Sicherheit erstreckt.

Der Auditor wählt weitere vier Bausteine in eigenem Ermessen. Dadurch können insbesondere Bausteine überprüft werden, deren wirksame Umsetzung für die Gesamtsicherheit besonders kritisch ist oder zweifelhaft erscheint.

Zitat: Qualifizierung nach IT-Grundschutz, Eckpunktepapier

Der Auditor muss dann die tatsächliche Realisierung dieser zehn Bausteine überprüfen.

Eine Auskunft über die Realisierung der Maßnahme dieser Bausteine reicht hierbei nicht, sondern die praktische Realisierung wird im Detail anhand von Dokumentation, Begehung, Rechnerkonfiguration etc. überprüft.

Zitat: Qualifizierung nach IT-Grundschutz, Eckpunktepapier

Werden bei der Realisierungsprüfung sämtliche Angaben des Basis-Sicherheitschecks korrekt vorgefunden und wurden die erforderlichen Maßnahmen tatsächlich realisiert, wird davon ausgegangen, dass die Ergebnisse des Basis-Sicherheitschecks den tatsächlichen Sicherheitsstatus des IT-Verbunds widerspiegeln.

Schritt 7: Selbsterklärung/Zertifizierung. Folgende Bedingungen müssen für die Selbsterklärung umgesetzt sein:

Der Auditor hat die Plausibilitätsprüfung mit positivem Ergebnis durchgeführt.

Der Auditor hat die Realisierungsprüfung mit positivem Ergebnis durchgeführt.

Der Auditor stellt fest, dass praktisch sämtliche Maßnahmen der angestrebten Ausprägung der IT-Grundschutz-Qualifizierung erfüllt sind.

Zitat: Qualifizierung nach IT-Grundschutz, Eckpunktepapier

Jede Institution kann bei Erfüllung dieser Bedingungen eine IT-Grundschutz-Selbsterklärung abgeben. Die Selbsterklärung muss von einem zeichnungsbefugten Vertreter der Institution ausgesprochen werden.

Eine unabhängige akkreditierte Zertifizierungsstelle kann der Institution das IT-Grundschutz-Zertifikat verleihen, wenn die obigen Voraussetzungen erfüllt sind. Die Schritte 5, 6 und 7 müssen dann von einem für IT-Grundschutz lizenzierten Auditor durchgeführt worden sein.

Schritt 8: Re-Qualifizierung. Da der Baustein »IT-Sicherheitsmanagement« obligatorisch für die Realisierungsprüfung ist, wird bei einem funktionierenden IT-Sicherheitsmanagement davon ausgegangen, dass der nachge-

wiesene IT-Sicherheitszustand für die Dauer von zwei Jahren aufrecht erhalten werden kann. Rechtzeitig vor Ablauf des Zertifikates sollte eine Wiederholungsprüfung (Re-Qualifizierung) angestoßen werden.

3.5 Wie kann ich meine erreichte IT-Sicherheit kundtun?

Durch die Veröffentlichung des Ergebnisses wird ein Instrumentarium geschaffen, das dem Unternehmen die Möglichkeit gibt, seine Bemühungen um die IT-Sicherheit und das erreichte Sicherheitsniveau am Markt zu platzieren.

Eine Selbsterklärung oder ein Zertifikat muss verschiedene Aspekte umfassen, die dann im Rahmen der Qualifizierungsaussage veröffentlicht werden:

- Abgrenzung

  Der IT-Verbund ist abzugrenzen und verbal zu beschreiben.

- Sicherheitsaussage

  Die Qualifizierungsstufe (Einstiegsstufe, Aufbaustufe, Zertifikat) ist anzugeben.

- Gültigkeitszeitraum

  Die Gültigkeit (Selbsterklärung, Zertifikat) ist auf einen Zeitraum von zwei Jahren zeitlich begrenzt, um Änderungen in der IT und neue Versionen des IT-Grundschutzhandbuchs einfließen lassen zu können.

- Version

  Diese Version des IT-Grundschutzhandbuchs ist in der Qualifizierungsaussage anzugeben.

- Qualifizierende Stelle

  Es ist anzugeben, wer die Qualifizierungsentscheidung gefällt hat und die Selbsterklärung bzw. das Zertifikat verantwortet. Bei einem Zertifikat ist im Gegensatz zu einer Selbsterklärung sowohl der Auditor als auch die Zertifizierungsstelle zu benennen.

Hierzu ist ein **Auditreport** zu erstellen, der die Ergebnisse der Schritte 1 bis 7 umfasst. Der Auditreport, der vom Auditor und der qualifizierten Institution zu unterzeichnen ist, wird nicht veröffentlicht. Im Fall der Zertifizierung wird der Auditreport der Zertifizierungsstelle vorgelegt, nicht jedoch bei der Selbsterklärung.

Die IT-Grundschutz-Selbsterklärungen und IT-Grundschutz-Zertifikate können auf dem BSI-WWW-Server veröffentlicht werden. Das BSI veröffentlicht auch regelmäßig das IT-Grundschutzhandbuch, die akkreditierten Zertifizierungsstellen und die lizenzierten IT-Grundschutz-Auditoren.

3.6 Was sagt das Zertifikat aus?

Zusammenfassend sagt das IT-Grundschutz-Zertifikat aus, dass eine Behörde oder ein Unternehmen den im IT-Grundschutzhandbuch des BSI definierten IT-Sicherheitszustand erreicht hat.

Das IT-Grundschutz-Zertifikat stellt einen ersten Schritt in Richtung »messbare« IT-Sicherheit in Behörden und Unternehmen dar. Anhand eines etablierten und praxisbewährten Katalogs von Standard-Sicherheitsmaßnahmen – dem IT-Grundschutzhandbuch des BSI – wird eine Aussage über den tatsächlich vorhandenen IT-Sicherheitszustand in dem betrachteten IT-Verbund getroffen. Neben dem eigentlichen IT-Grundschutz-Zertifikat, das von akkreditierten Zertifizierungsstellen vergeben wird, kann auch eine Qualifizierung in Form einer »Selbsterklärung Einstiegsstufe« und einer »Selbsterklärung Aufbaustufe« vorgenommen werden. Diese beiden Selbsterklärungen sind als Meilensteine auf dem Weg zum IT-Grundschutz-Zertifikat zu verstehen und dienen dazu, die Hürde beim Einstieg in den Qualifizierungsprozess zu verringern. Alle drei Ausprägungen der Qualifizierung nach IT-Grundschutz können auf Wunsch vom BSI veröffentlich werden. Auf diese Weise lassen sich die eigenen Bemühungen um IT-Sicherheit und die erfolgreiche Umsetzung der Standard-Sicherheitsmaßnahmen transparent machen.

Literaturangaben: *[1]* IT-Grundschutzhandbuch, Version Mai 2002

[2] Zertifizierung nach IT-Grundschutz, Lizenzierungsschema für IT-Grundschutz-Auditoren, Stand 14.02.2002, BSI

[3] Prüfschema für Auditoren, Stand 30.01.2002, BSI

[4] Qualifizierung nach IT-Grundschutz, Eckpunktepapier

4 Die Integration von Schutzbedarfsanalyse und IT-Grundschutz nach BSI

Christian Friberg

Carsten Gerhardt

Prof. Dr. Norbert Luttenberger

4.1 Motivation

»Aller Anfang ist schwer« und »Wo beginnen?«, das sind nicht nur die Stoßseufzer von Praktikanten, die ihren Praktikumsbericht schreiben, von Diplomanden, die ihre Diplomarbeit schreiben, von Ingenieuren, die ein Lastenheft schreiben, und von Informatikern, die eine Programmspezifikation schreiben, sondern auch von Netzwerkadministratoren und Security-Spezialisten, die die Aufgabe übertragen bekommen haben, die IT-Infrastruktur eines Betriebes »sicher« zu machen. Zu unübersehbar die Aufgabe: Soll man zuerst einmal ein Firewall-System installieren, lieber die gelben Klebezettel mit den Passwörtern von den Bildschirmen der Benutzer reißen oder den studentischen Hilfskräften das Super-User-Passwort wegnehmen, das diese erhalten haben, »damit sie arbeiten können«. Und zu groß ist der zu erwartende Widerstand der Benutzer: »Produzieren wir hier nur noch Sicherheit, oder sollen wir auch noch produktiv arbeiten?«

Zum Glück gibt es doch eine Lösung, wird mancher sagen: Es gibt doch das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI-GSHB) *[2]*. In der Tat umfasst dieses Handbuch nicht nur eine Menge außerordentlich nützlicher und wichtiger Detailangaben (auf die man beim ersten Durchblättern unweigerlich stößt), sondern auch eine gut begründete Systematik, deren Ziel es ist, den Arbeitsaufwand für den Netzwerkadministrator und den Security-Spezialisten für die große Mehrzahl der Anwendungsfälle zu senken. Ein verdienstvoller Schritt in die richtige Richtung also. Man wird am BSI-GSHB nicht vorbeikommen.

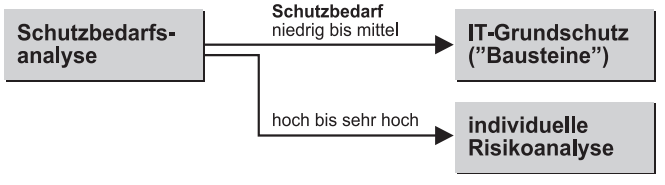


Abbildung 4.1: Vorgehensweise nach BSI-Methode

Und dennoch. Schaut man genauer nach, liest man im Kap. 2.1 des BSI-GSHB ein Caveat:

> *»Für IT-Systeme mit mittlerem Schutzbedarf … ist lediglich die Umsetzung der in diesem Handbuch empfohlenen Maßnahmen erforderlich. Für IT-Systeme mit hohem Schutzbedarf bleibt neben dem IT-Grundschutz prinzipiell die Durchführung einer detaillierten Risikoanalyse (z. B. nach dem IT-Sicherheitshandbuch) erforderlich. Für die Unterscheidung zwischen mittlerem und hohem Schutzbedarf wird … eine diesbezügliche Vorgehensweise (Schutzbedarfsfeststellung) vorgestellt.«*

Quelle: BSI-GSHB, Kap. 2.1

Vor der Durchführung einzelner Sicherheitsmaßnahmen muss also eine sog. Schutzbedarfsfeststellung durchgeführt werden, auf deren Korrektheit größter Wert zu legen ist, denn

> *»..werden bei der Schutzbedarfsfeststellung bereits Fehler gemacht, so pflanzen sich diese im weiteren Verfahren fort und sind kaum noch zu korrigieren«.*

Quelle: BSI-GSHB, Kap. 2.1

Aus diesen methodischen Grundlagen ergab sich die Motivation für unsere Arbeit:

- Zum einen ging es darum, ein rechnergestütztes Werkzeug zu entwickeln, mit dem der gesamte Prozess der Umsetzung von IT-Sicherheitsmaßnahmen – von der Schutzbedarfsfeststellung bis zur Umsetzung von detaillierten Maßnahmen – gesteuert und begleitet werden kann.
- Zum anderen wurde bald klar, dass die vom BSI vorgeschlagene Methode für die Schutzbedarfsanalyse zu technikzentriert ist. Die von uns vorgenommene methodische Innovation baut – in bewusster Distanz zur BSI-Schutzbedarfsfeststellung – auf Geschäfts- und Projektprozessen auf und ist damit besser an den Zielen von Benutzern und Organisationen orientiert.
- Diese innovierte Methode prägt selbstverständlich das von uns entwickelte rechnergestützte Werkzeug SECMAN (Security Manager), dessen hervorstechendes Merkmal die rollenbasierte Interaktion mit unterschiedlichen Typen von Benutzern ist.

In diesem Aufsatz werden wir zunächst den vom BSI vorgeschlagenen methodischen Ansatz für die Schutzbedarfsanalyse darstellen und kritisieren und dann unsere eigenen methodischen Überlegungen erläutern. Wir stellen danach das Werkzeug SECMAN vor und zeigen den darin enthaltenen rollenbasierten Ansatz. Wir schließen mit einem Ausblick auf künftige Entwicklungen.

4.2 Die BSI-Methode zur Schutzbedarfsfeststellung

Der klassische Ansatz zur Herstellung eines gewissen Sicherheitsniveaus einer Organisation ist die *Risikoanalyse [3]*. Da mit der Risikoanalyse ein ggf. sehr hoher Aufwand verbunden ist, schlägt das BSI eine vereinfachte Methode vor, die man als eine Untermenge der Risikoanalyse betrachten kann, und die vom BSI mit der Bezeichnung *Schutzbedarfsfeststellung* versehen wurde. Um diesen Begriff besser bestimmen zu können, soll er im folgenden von der Risikoanalyse abgegrenzt werden.

4.2.1 Risikoanalyse

Die Risikoanalyse setzt sich zusammen aus Risikoidentifikation und der Risikobewertung. Die *Risikoidentifikation* (die auch in der Schutzbedarfsanalyse der BSI-Methode auftaucht, und zwar als Aufzählung von *Gefährdungen*) ist auf die spezifische Risikosituation des Unternehmens abgestimmt und erfasst möglichst alle Risiken, die das Unternehmen treffen können. Die Identifikation technischer Risiken – nur um solche geht es uns hier – basiert z.B. auf Systemanalysen, Fehlerbaumanalysen oder Störfallanalysen. Für die Identifikation von Risiken im IT-Bereich schlägt das BSI eine »Baustein«-orientierte Systematik vor, die grob gesehen folgende Bereiche umfasst:

- Organisation
- Personal
- Notfallvorsorge-Konzept
- Datensicherungskonzept
- Infrastruktur
- Nicht-vernetzte IT-Systeme
- Vernetzte Systeme
- Datenübertragungseinrichtungen
- Telekommunikation
- Sonstige IT-Komponenten

Bei der *Risikobewertung* geht es darum, einerseits die bei Eintritt des Risikos verursachten finanziellen Auswirkungen (Schadenausmaß) zu quantifizieren und andererseits eine Schadenseintrittswahrscheinlichkeit abzuschätzen. Bei der Abschätzung des Schadensausmaßes bedient man sich verschiedener Instrumente und Methoden. Bei der PML- bzw. MPL-Analyse wird z.B. für die Beurteilung eines Großschadenrisikos der *Maximum Possible Loss* (MPL) oder der *Probable Maximum Loss* (PML) ermittelt. Stoßen die quantitativen Verfahren an ihre Grenzen, so bedient man sich qualitativer

Aussagen. Das Schadenausmaß kann bei fehlender Quantifizierbarkeit nach den Kategorien »gering«, »mittel«, »groß« und »katastrophal« eingeteilt werden. Die Schadeneintrittswahrscheinlichkeit wird in der Praxis fast immer qualitativ nach den Kategorien »sehr gering«, »gering«, »mittel«, »hoch« und »sehr hoch« gewichtet. Vor allem betriebswirtschaftliche Schäden (Marktverlust, Imageverlust etc.) können so besser abgebildet werden.

Die erkannten Risiken werden – gegliedert nach ihren finanziellen Auswirkungen und der Eintrittswahrscheinlichkeit – in einer *Risikomatrix* zusammengestellt. Die Risikomatrix liefert in komprimierter und übersichtlicher Form Informationen über die Risikolage eines Unternehmens, um so die Priorität, mit welcher die Maßnahmen zur Risikobewältigung realisiert werden sollen, festzulegen. In der Risikomatrix kann eine individuelle Akzeptanzlinie abgebildet werden, die festlegt, ab welchem Schwellenwert ein Handlungsbedarf ausgelöst wird. Bei der Ermittlung der Gesamtrisikolage müssen auch die Risikointerdependenzen berücksichtigt und aggregiert werden. Insbesondere bei den modernen Produktionsmethoden (Just-in-time, Single-Sourcing etc.) gewinnt die Aggregation der Einzelrisiken an Bedeutung.

Die Durchführung einer organisationsweiten Risikoanalyse ist – wie man sich leicht vorstellen kann – sehr aufwändig und verlangt von den durchführenden Personen große Erfahrung. Insbesondere erfordert die Risikoanalyse einen Überblick sowohl über die Bedeutung einzelner Objekte für die zu untersuchende Organisation als auch über die möglichen Gefahren und entsprechende Maßnahmen zu ihrer Beseitigung. Häufig ist dieser Ansatz daher mit den dafür zur Verfügung stehenden Ressourcen nicht durchführbar.

4.2.2 Schutzbedarfsfeststellung nach BSI-Methode

Um mit einfacheren Mitteln ein gewisses Schutzniveau herstellen zu können, geht das BSI von einem vereinheitlichten Bedrohungsszenario aus, das aus Risikoanalysen verschiedener Organisationen hervorgegangen ist. Dadurch kann das Expertenwissen über Sicherheitsprobleme in einem Satz von Maßnahmen zusammengeführt und dem Sicherheitslaien zur Verfügung gestellt werden.

Wie am Anfang des Abschnitts dargestellt, ist die *Schutzbedarfsanalyse* der erste Schritt innerhalb der BSI-Methode. Sie umfasst drei Schritte:

1. Erfassung der zu schützenden IT-Systeme: Rechner, Server, Netze usw.
2. Erfassung der zu diesen IT-Systemen zugehörigen IT-Anwendungen und Informationen und Zuordnung der Wichtigkeit der IT-Schutzziele *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* zu diesen Anwendungen und Informationen. (Vertraulichkeit soll sicherstellen, dass der Zugriff auf bestimmte Daten und Informationen nur berechtigten Benutzern ermöglicht wird. Integrität bezeichnet die Korrektheit, Manipulationsfreiheit

und Unversehrtheit von Daten und Informationen. Unter Verfügbarkeit versteht man die Fähigkeit eines IT-Systems, Daten und Informationen, Prozesse und IT-Anwendungen zur rechten Zeit bereitzustellen.)

3. Schutzbedarfsfeststellung: Der Schutzbedarf richtet sich nach dem Ausmaß der Schäden, die eintreten würden, wenn die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Anwendung und/oder Informationen beeinträchtigt würden.

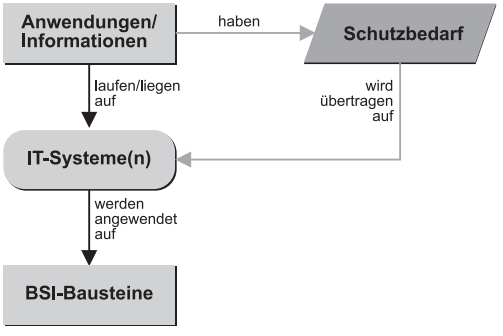


Abbildung 4.2: Die BSI-Schutzbedarfsanalyse

Der Schutzbedarf wird in drei Kategorien eingeteilt:

- **niedrig bis mittel**: Die Schadensauswirkungen sind begrenzt und überschaubar. Die vom BSI vorgeschlagenen Grundschutzmaßnahmen sind in der Regel ausreichend.
- **hoch**: Die Schadensauswirkungen können beträchtlich sein, Schutzmaßnahmen sollten auf Basis einer individuellen Risikoanalyse ermittelt werden.
- **sehr hoch**: Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen. Eine individuelle Risikoanalyse ist unbedingt erforderlich.

Die BSI-Schutzbedarfsanalyse lässt sich von der Risikoanalyse in drei Punkten abgrenzen:

1. Im Gegensatz zur Schutzbedarfsanalyse betrachtet die Risikoanalyse nicht nur Schadensauswirkungen, sondern auch Schadenseintrittswahrscheinlichkeit.
2. Im Gegensatz zur Schutzbedarfsanalyse ist die Risikoanalyse nicht nur auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ausgerichtet, sondern kann ggf. weitere Schutzziele betrachten.
3. Die Risikoanalyse versucht, wann immer möglich mit quantitativen Maßen vorzugehen; darauf wird in der Schutzbedarfsanalyse von vornherein verzichtet.

Das Ziel des vom BSI vorgeschlagenen *IT-Grundschutzes*, der auf dieser Schutzbedarfsanalyse aufbaut, ist es, durch die geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den *mittleren Schutzbedarf* angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Anwendungen dienen kann. Für bekannte Gefährdungen und Schwachstellen hat das BSI überschlägige Risikobetrachtungen vorweggenommen und geeignete Maßnahmenbündel für typische IT-Konfigurationen, Umfeld- und Organisationsbedingungen erarbeitet. Der Anwender des IT-Grundschutzhandbuchs muss diese aufwändigen Analysen nicht wiederholen, er muss lediglich dafür Sorge tragen, dass die empfohlenen Maßnahmen konsequent und vollständig umgesetzt werden.

Vom BSI wird die Durchführung der Schutzbedarfsanalyse (nachdrücklich) empfohlen, um sicherzustellen, dass in der betrachteten Organisation keine IT-Systeme mit hohem oder sehr hohem Schutzbedarf »übersehen« werden, für die die mehr oder weniger pauschalen IT-Grundschutzmaßnahmen nicht ohne weiteres ausreichend sind. Für solche Systeme werden individuelle Sicherheitsuntersuchungen angemahnt, die unter Beachtung von Kosten- und Wirksamkeitsaspekten geeignete Sicherheitsmaßnahmen zu identifizieren helfen, die über den IT-Grundschutz hinausgehen.

Die SECMAN-Methode, die im folgenden Abschnitt detailliert dargestellt wird, umfasst als integralen Bestandteil eine modifizierte Schutzbedarfsanalyse, die – bei aller Verwandtschaft mit der BSI-Methode – eine bessere Ausrichtung der Schutzmaßnahmen an den Werten und der Struktur des Unternehmens verspricht.

4.3 Die SECMAN-Methode

Zur Definition einer angemessenen Methode für die Schutzbedarfsanalyse ist ein schwieriges Problem zu lösen: Wie wird die Auswirkung von möglicherweise eintretenden Schäden korrekt »bewertet«. Offensichtlich werden die Schadensauswirkungen falsch erfasst, wenn man sie auf die IT-Systeme selbst bezieht, da

> *»deren Wert … meistens nur einen geringen Teil des Gesamtwertes aus[macht], die strategische und operative Bedeutung der IT liegt oft weit höher. Daher ist es wichtig, sich […] klarzumachen, wie stark die Aufgabenerfüllung innerhalb der Institution von der eingesetzten IT abhängt«*

(BSI-GSHB, Kap. 1.2)

Das BSI schlägt – wie gezeigt – zur Lösung des angeführten Problems vor, die Bewertung von Schadensauswirkungen anhand der »Anwendungen und Informationen« vorzunehmen, die auf den IT-Systemen installiert, gespeichert, verarbeitet werden, und dazu deren Schutzbedarf bezüglich Vertraulichkeit, Integrität und Zuverlässigkeit anzugeben. Leider wird

jedoch dieser Ansatz in der BSI- Grundschutzanalyse nur halbherzig unterstützt, und darüber hinaus scheint uns dieser Ansatz aus zwei Gründen wenig hilfreich:

- Viele Anwendungen (z.B. Textverarbeitung) tauchen in vielen Kontexten auf. Es ist jedoch stets der betriebliche Kontext von Projekt- und Geschäftsprozessen, der über die Wichtigkeit der Erreichung eines Schutzziels entscheidet. Es können von daher nicht allein »Anwendungen« sein, denen ein »Wert« und damit ein Schutzbedarf zukommt.
- Das Gleiche trifft für die angeführten »Informationen« zu: Auch diese können nicht isoliert betrachtet werden. In aller Regel ist in einer Organisation oder in einem Projekt nicht nur eine einzelne Information wichtig, sondern ein Verbund aus einer Vielzahl von Informationen, der als ganzer betrachtet werden muss. Es führt zu einem methodisch problematischen Vorgehen, eine technische Zeichnung losgelöst von den zugehörigen textuellen Erläuterungen zu betrachten. Auch hier geht es also wieder um die Einbettung von Informationen in komplexe Geschäfts- und/oder Projektprozesse.

Die SECMAN-Methode sieht deshalb eine Schutzbedarfsanalyse vor, die auf einer Analyse der organisationsinternen Geschäfts- und Projektprozesse und der von diesen Prozessen benötigten Ressourcen beruht. Geschäftsprozesse sind z.B. die regelmäßige Systemadministration, die Pflege der Internet-Präsenz, aber auch Buchhaltungsverfahren; typische Projektprozesse sind z.B. Entwicklung, Test, Auslieferung usw. Wir werden im folgenden abkürzend nur noch von Prozessen sprechen. Alle Prozesse benötigen Ressourcen, die konkrete IT-Systeme oder aber abstrakte Beschreibungen der benötigten Arbeitsmittel sein können. Diesen Ressourcen werden die o.a. Schutzziele zugeordnet.

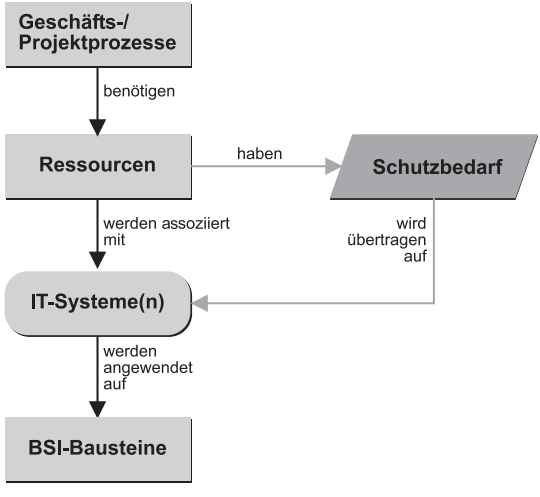


Abbildung 4.3: SECMAN-*Methode*

Der Ablauf einer Sicherheitsanalyse in SECMAN gliedert sich in die folgenden Schritte:

1. Die von einem Prozess benötigten Ressourcen werden in einem »Prozessinventar« erfasst.
2. Der Schutzbedarf der Ressourcen wird prozessspezifisch von den Prozessbeteiligten bestimmt. Z.B. legt der Leiter eines Entwicklungsprojekts fest, dass die Integrität der Java-Quelldateien besonders schützenswert ist.
3. Die Prozessressourcen werden mit konkreten Objekten aus dem IT-Verbunds der Organisation assoziiert. Diese Assoziation ist in aller Regel von einem Sicherheitsbeauftragten durchzuführen. Dieser verknüpft z.B. die Java-Quelldateien mit dem Server, auf dem diese Daten mitsamt dem zugehörigen Source Code Control System abgelegt ist. (Ggf. lässt sich aufgrund des unterschiedlichen Charakters von abstrakten Ressourcen und konkreten IT-Objekte nicht immer eine eindeutige Abbildung zwischen den Sichten definieren. Eine nur lose Assoziation reicht für eine algorithmische Auswertung nicht, erleichtert jedoch die manuelle Informationsgewinnung.)
4. Der prozessspezifisch ermittelte Schutzbedarf wird auf die konkreten Objekte des IT-Verbunds übertragen. Diese Übertragung ist in aller Regel von einem Sicherheitsbeauftragten durchzuführen. Für unser Beispiel bedeutet dies, dass er sämtliche Ressourcen sichtet, die mit dem Server assoziiert sind (also z.B. die Java-Quelldateien, aber ggf. auch Ressourcen aus weiteren Prozessen) und aus deren Schutzbedarf einen Schutzbedarf für den Server ableitet.
5. Die Bewertung des Schutzbedarfs fließt in die Sortierung der Maßnahmen für den Sicherheitsaudit ein. Dem für die Sicherheit des Servers verantwortlichen – also z.B. dem Systemadministrator – würden in unserem Beispiel diejenigen Maßnahmen bevorzugt angezeigt werden, die die Integrität des Servers erhöhen.

Auf dieser Basis können einige wichtige Fragen beantwortet werden:

- Welche Maßnahmen sollen aufgrund der Wertigkeit der exponierten Objekte für das Unternehmens und aufgrund der Unternehmensstruktur *bevorzugt* ausgeführt werden?
- Welche Maßnahmen *passen* besonders gut auf den Schutzbedarf eines Unternehmenswertes? (Ist es z.B. sinnvoller, eine Kundendatei zu verschlüsseln oder den Zugang zu einem Serverraum zu überwachen?)
- Welche Maßnahmen haben *schädliche* »Nebenwirkungen«? (Die Integrität und die Verfügbarkeit von Daten kann z.B. durch Anlegen einer Sicherungskopie erhöht werden, ihre Vertraulichkeit wird dadurch aber möglicherweise in Frage gestellt.)

Für diese Art der Schutzbedarfsanalyse wird offensichtlich Wissen benötigt, welches zwar in der Organisation vorhanden ist, sich aber über mehrere Personen verteilt (z.B. Abteilungsleiter, Projektleiter, Sicherheitsbeauftragter).

Die Erstellung und Durchführung von Sicherheitsaudits muss also als kooperativer Prozess verstanden werden, der Fachwissen auf der einen und Sicherheitswissen auf der anderen Seite benötigt. Besonders wichtig dabei ist, dass der Schutzbedarf aus der Sicht der Prozessverantwortlichen so formuliert werden kann, dass von konkreten technischen Details, wie dieser Schutz zu erbringen ist, abstrahiert werden kann.

4.4 Das SECMAN-Tool

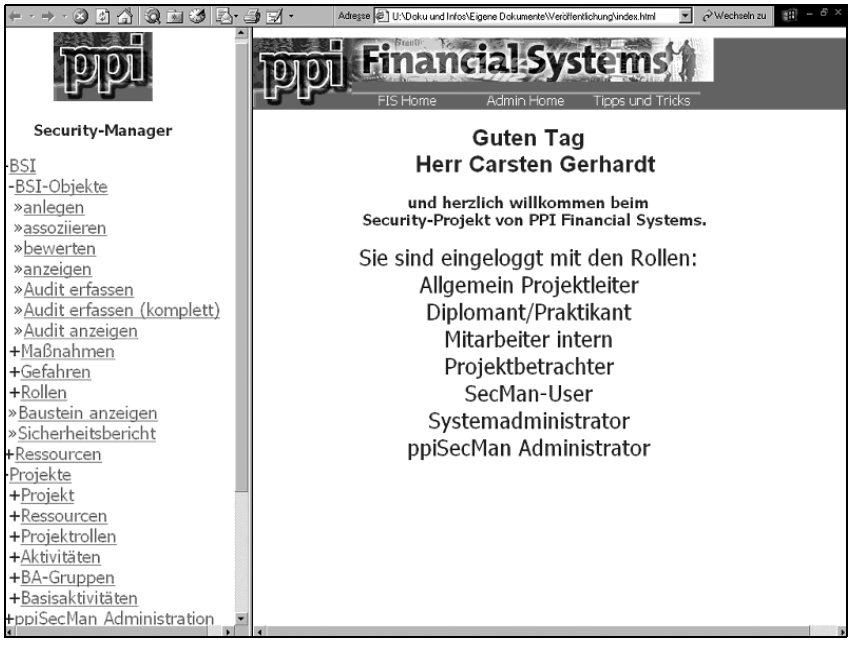


Abbildung 4.4: Das SECMAN-*Tool*

4.4.1 Rollenbasierte Zugriffskontrolle

Die dargestellte SECMAN-Methode erfordert, dass bei der Erfassung und Verarbeitung eines Sicherheitsaudits zwischen Personen mit Projektwissen und solchen mit Sicherheitswissen differenziert werden kann. Konsequenterweise ist für das SECMAN-Tool ein Rollenmodell entwickelt worden, das diese Differenzierung berücksichtigt. Dabei werden die jeweiligen Wissenskomponenten nicht direkt Benutzern, sondern bestimmten Rollen (Aufgabenbeschreibungen) zugeordnet. Auf diesem Rollenmodell baut eine rollenbasierte Zugriffskontrolle (*Role Based Access Control*, RBAC) auf.

Rollenbasierte Zugriffskontrolle ist ein Konzept, welches schon lange in der Informationsverarbeitung verwendet wird, aber erst Anfang der 90er Jahre formal definiert wurde ***[4] [5]***. Mit RBAC wird eine möglichst flexible Verwaltung von Zugriffsrechten, aber auch von Aufgaben und Pflichten angestrebt.

Rechte, Aufgaben und Pflichten werden dabei nicht direkt an einzelne Personen gebunden, sondern an Rollen, die diese Benutzer einnehmen können. Die jeweiligen Rechte, Aufgaben und Pflichten werden damit Personen nur indirekt zugeordnet. Eine wichtige Frage bei der Generierung von RBAC-Regularien ist damit die Definition von Rollen, die geeignet sind, die Aufgabenverteilung in der zu modellierenden Organisation angemessen wiederzugeben. Diese Rollen lassen sich oft aus den Aufgabenbeschreibungen entnehmen (top down) oder aber aus den aktuell vorhandenen Benutzerrechten ableiten (bottom up). Es sind einige erfolgversprechende Ansätze entwickelt worden, um Rollen direkt aus *Use Cases* ***[6]*** oder anderen formalen Betrachtungen der Organisation zu gewinnen ***[7] [8] [9]***. Der Vorteil der rollenbasierten Vorgehensweise besteht darin, dass bei einer Veränderung der Zuordnung von Rechten, Aufgaben und Pflichten zu bestimmten Personen einfach nur die Rollenzuordnung für diese Personen angepasst werden muss.

In der SECMAN-Methode wird die Struktur der Aufgabenverteilung durch Rollen modelliert. Diese Rollen dienen im ersten Schritt zur Modellierung der Aufgabenbereiche und der damit zusammenhängenden Arbeitsprozesse, Ressourcen und Bewertungen.

Diese Rollen werden darüber hinaus zur Zugriffskontrolle im SECMAN-Tool genutzt (RBAC). Eine Rolle, die in der Prozessmodellierung als Projektleiter definiert ist, darf entsprechend in SECMAN diejenigen Einträge bearbeiten, die zur Erfassung der projektbezogenen Daten und Bewertungen dienen. Analog gilt dies für permanente Funktionsbeschreibungen wie z.B. Ressortleiter (Administrator oder Leiter innerer Dienst). Diese Zugriffskontrolldefinitionen werden auch auf Rollen ausgedehnt, die in der Modellierung der Organisation u.U. nicht zu finden sind und eine nur interne Bedeutung haben. Dies kann z.B. ein Sicherheitsexperte sein, der die Abbildung zwischen Projektwissen und BSI-Objekten herstellen soll. In der SECMAN-Methode bietet es sich an, für folgende drei Aufgaben verschiedene Rollen mit der Durchführung zu betreuen:

1. Erfassung von Projektwissen, insbesondere von Ressourcen und ihrer Bewertung – hier sind z.B. Projektleiter gefragt.
2. Erfassung von realen Objekten und Durchführung von Audits nach BSI-Grundschutzhandbuch – viele dieser Aufgaben werden z.B. vom Systemadministrator wahrgenommen.
3. Assoziation zwischen Projektressourcen und BSI-Objekten und Bewertung dieser Objekte anhand der Projektinformation – diese Rolle sollten Personen mit Einblick in Firmeninterna und Sicherheitsfragen einnehmen.

Dieses Beispiel zeigt, wie inhaltlich unterschiedliche Aufgaben, die auch unterschiedlich erfahrenes und qualifiziertes Personal zur Durchführung benötigen, durch eine Modellierung mit einem Rollenmodell abgebildet werden können.

Auch die BSI-Grundschutzmethode arbeitet mit einem Rollenkonzept. Für die Erfassung und Verarbeitung von Sicherheitsaudits definiert sie zwei Typen von Rollen, die sich durch die Verantwortlichkeit für die Durchführung von Maßnahmen unterscheiden:

1. Initiieren von Maßnahmen
2. Durchführen von Maßnahmen

Die Integration dieses Rollenkonzepts in das Rollenkonzept von SECMAN erfolgt durch ein Mapping von SECMAN-Rollen auf BSI-Rollen. Diese Abbildung von Rollen erfolgt frei definierbar. Ist ein Benutzer von SECMAN für eine SECMAN-Rolle zugelassen, die mit einer BSI-Rolle assoziiert ist, so ist er damit indirekt für die Initiierung oder Durchführung einer Maßnahme zuständig. Die Verwendung der Rollen wird durch ein Konzept von persönlicher Verantwortlichkeit für die Durchführung von BSI- Maßnahmen erweitert. Die Möglichkeit, Mitarbeiter persönlich für die Durchführung von Maßnahmen verantwortlich zu machen, ist schon in der Definition des Grundschutzhandbuches enthalten. Ist nun ein Benutzer über die Rollenzuordnungen für die Initiierung einer Maßnahme zugelassen, so kann er einer anderen Person diese Verantwortung aufbürden. Diese Vorgehensweise erweitert das Rollenkonzept, welches Rollen Rechten zuordnet, auf die Zuteilung von Pflichten. Mit SECMAN kann so z.B. die Verantwortung für die Maßnahme M 1.15 (»Geschlossene Fenster und Türen«) für ein Objekt an einen bestimmten Mitarbeiter vergeben werden.

4.4.2 Das SECMAN-Programmsystem

Bei der Implementation von SECMAN wurde auf größtmögliche Flexibilität geachtet. Daher wurde SECMAN als 3-Tier-Web-Application implementiert. Somit sind die Anforderungen auf Client-Seite minimal; jeder Rechner mit einem Web-Browser und Netzzugang kann als Client dienen. Die von SECMAN verwalteten Daten werden in einer Datenbank gespeichert. Die Web-Application setzt sich aus mehreren Scripten zusammen, welche die HTML-Seiten für das Web-Frontend erzeugen.

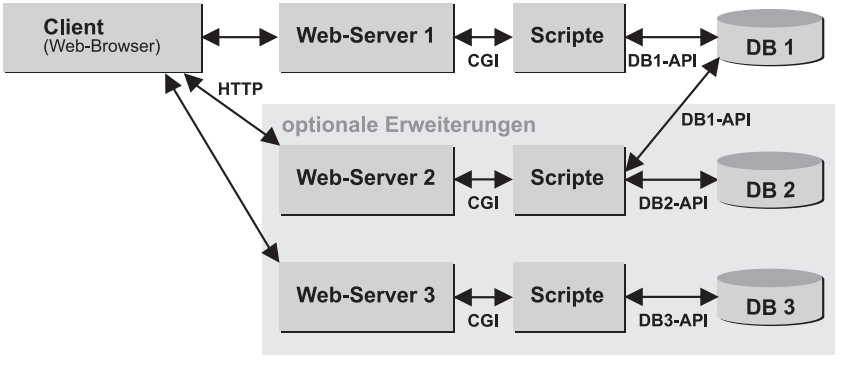


Abbildung 4.5: Struktur des SECMAN - Programmsystems

SECMAN ist so konzipiert, dass mehrere Scriptsprachen und mehrere Datenbanken nebeneinander verwendet werden können. Somit können Informationen, die u.U. bereits in anderen vorhandenen Datenbanken vorliegen, relativ einfach in SECMAN integriert werden. Zudem ist es möglich, Teile von SECMAN auf verschiedene Server zu verteilen.

Auf der Server-Seite setzt sich SECMAN aus mehreren Modulen zusammen. Die wichtigsten sind:

- das Basismodul,
- das Prozesserfassungsmodul und
- das BSI-Grundschutzmodul.

Die Objekte dieser Module können miteinander assoziiert werden.

Das *Basismodul* überprüft die Autorisation für den Zugriff auf die angeforderte Funktion der Module und stellt diesem Informationen über den Benutzer und seine aktiven Rollen zur Verfügung. Damit kann innerhalb der Funktionen eine weitere Einschränkung der angezeigten Informationen oder der Funktionalität selbst erreicht werden. Zum Beispiel kann sich ein Benutzer bei der Funktion »Anzeige eines BSI-Audits« lediglich die Maßnahmen anzeigen lassen, für die er durch seine Rollen verantwortlich ist, oder die Funktion »Passwort ändern« erlaubt einem Benutzer, nur sein eigenes Passwort zu ändern.

Die Identifikation der Benutzer wird mit Hilfe von nicht-permanenten Cookies realisiert. Wenn ein Benutzer eine Anfrage ohne einen gültigen Cookie an das System stellt, wird die Anfrage vom Basis-Sicherheits-Modul nicht an die entsprechende Funktion weitergeleitet, sondern zunächst eine Authentifizierung mit Benutzername und Passwort verlangt. Bei einer erfolgreichen Authentifizierung wird für den Benutzer eine Session eingerichtet. Zu der Session werden der Benutzer, die Zeit der letzten Aktivität und die aktiven Rollen gespeichert und eine eindeutige Identifikation der Session wird beim Client als Cookie gespeichert.

Im *Projekterfassungsmodul* werden folgende Daten erfasst und verwaltet:

- beteiligte Rollen
- beteiligte Mitarbeiter und ihre Rollen im Projekt
- verwendete Ressourcen
- Aktivitäten der Rollen und der dafür benötigten Ressourcen
- Bewertungen zum Schutzbedarf der Ressourcen
- Bedeutung der Aktivitäten zur erfolgreichen Durchführung der Projektarbeit

Bei SECMAN liegt die Konzentration bei der Analyse der Geschäftsprozesse auf der Erfassung einzelner Handlungen innerhalb der Prozesse. Eine mögliche Beschreibung einer solchen Handlung ist z.B.: »Ein Entwickler bearbei-

tet C-Quellcode mit einem Editor«. Dabei wird ermittelt, welche Rolle (Entwickler) eine Handlung (C-Quellcode editieren) durchführt, welche Ressourcen zur Durchführung als Hilfsmittel benötigt werden (Editor) und welche Ressourcen durch die Handlung beeinflusst werden (C-Quellcode).

Sicherheitsanforderungen für diese Handlungen werden durch die Bewertung der drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit der beteiligten Ressourcen und Bedeutung der Handlung zur Realisierung der Unternehmensziele berücksichtigt.

Das *BSI-Grundschutzmodul* bietet folgende Funktionen:

- Erfassung der Objekte aus der Strukturanalyse
- Festlegung und Erfassung von Audits für die Objekte
- Bewertung von Maßnahmen bzgl. ihrer Wirksamkeit
- Berichte über den Umsetzungsgrad der Maßnahmen
- Kostenverfolgung von Maßnahmen
- Übersichten über die Abhängigkeiten von Maßnahmen und Gefahren

Dabei erlaubt das BSI-Modul an vielen Stellen einen einfachen Zugriff auf die originalen Beschreibungen des BSI im aktuellen Kontext. Dadurch wird die Arbeit mit dem Modul erleichtert und eine Sensibilisierung für sicherheitsrelevante Aspekte gefördert.

In SECMAN werden z.T. Daten aus verschiedenen Bereichen und Sichtweisen erfasst und verwaltet, welche untereinander eine logische Verbindung besitzen, jedoch nicht eindeutig zusammen gehören. Dies sind zum einen Rollen aus der Prozessanalyse und Rollen aus dem Grundschutzhandbuch, zum anderen sind es Ressourcen aus den Prozessanalysen und Objekte aus der BSI-Strukturanalyse.

Diese Anhängigkeiten können in SECMAN als m:n-Assoziationen erfasst werden. Somit können von jeder Seite zu einem Objekt die damit assoziierten Objekte der andern Seite erfragt werden. Mit Hilfe der Assoziationen wird der manuelle Informationstransfer zwischen Sicherheitsanforderungen aus den Projektinformationen und den BSI-Analysen erleichtert.

4.5 Zusammenfassung und Ausblick

Mit SECMAN haben wir ein Instrument vorgestellt, um eine Sicherheitsanalyse nach dem BSI-Grundschutzhandbuch mit einer Schutzbedarfsanalyse zu erweitern, die firmeninternes Know-how in die Analyse integriert. Die ersten Anwendungen verliefen erfolgreich und haben sowohl bei Administratoren, wie auch im Management einen sehr positiven Eindruck hinterlas-

sen. Die Bewertung der Sicherheitsanforderungen für die in den Projekten eingesetzten Ressourcen führten zudem zu einer Sensibilisierung der beteiligten Mitarbeiter.

In Zukunft könnte eine Verbesserung der Handhabbarkeit der Datenerhebung, insbesondere im Bereich der Projekterfassung, den Nutzwert des Programmsystems erhöhen. Geplant hierfür sind generische Projektdefinitionen oder die Übernahmen von Daten aus anderen Programmsystemen und Datenbanken (z.B. einer Mitarbeiter-DB), was durch das offene Konzept der Implementation (sowohl bei der Plattform wie auch der Sprache) erleichtert wird.

Der Bereich der Schutzbedarfsanalyse und der Bewertung der BSI-Objekte mit Hilfe der Assoziationen erfordert noch viel Überblick über technische und organisatorische Zusammenhänge. Hier könnte ein System zur Erkennung von Abhängigkeiten den Benutzer unterstützen. Hierzu wurde z.B. in ***[10]*** ein Fuzzy-Ableitungssystem zur Risikoanalyse unter Verwendung unscharfer Daten vorgestellt, dessen Integration gerade untersucht wird.

Literatur. ***[1]*** SECMAN ist ein interner Name und steht als Abkürzung für Security Manager. SECMAN bezeichnet in diesem Beitrag eine rollenbasierte Methode und ein Werkzeug, das von der Uni Kiel entwickelt und im Weiteren unterstützend von der PPI Financial Systems GmbH, Kiel in Diplomarbeiten umgesetzt wurde.

[2] Bundesamt für Sicherheit in der Informationstechnik:
IT-Grundschutzhandbuch.
Köln (Bundesanzeiger-Verlag) 2001, ISBN 3-88784-915-9
http://www.bsi.bund.de/gshb/deutsch/menue.htm.

[3] Philip E. Fites, Martin P.J. Kratz, Alan F. Brebner:
Control and Security of Computer Information Systems.
Rockville u.a. (Computer Science Press, Inc.) 1989, ISBN 0-7167-8191-3.

[4] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman:
Role-Based Access Control Models.
IEEE Computer 29, 2, 38-47 (Feb 1996).

[5] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, Ramaswamy Chandramouli:
Proposed NIST Standard for Role-Based Access Control.
ACM Transactions on Information and System Security 4, 3, 224-274 (Aug. 2001).

[6] E. B. Fernandez and J. C. Hawkins:
Determining Role Rights from Use Cases.
Presented at 2nd Workshop on Role-Based Access Control, Fairfax, VA, USA, 1997.

[7] Gerhard Schimpf:
Role-Engineering Critical Success Factors for Enterprise Security Administration.
Position Paper for the 16th Annual Computer Security Application Conference, New Orleans, 12/2000.

[8] Haio Röckle:
Rollenbasierter Zugriffsschutz.
IT-Sicherheit – Praxis der Daten und Netzsicherheit 1/99, Datakontext-Fachverlag GmbH, Frechen.

[9] Steffen E. Seufert:
Der Entwurf strukturierter rollenbasierter Zugriffskontrollmodelle.
Informatik Forschung und Entwicklung (2002) 17: 1-11 Springer-Verlag.

[10] Arndt Schönberg, Wilfried Thoben:
Ein unscharfes Bewertungskonzept für die Bedrohungs- und Risikoanalyse Workflow-basierter Anwendungen.
In »Sicherheit und Electronic Commerce (WS SEC '98)«, Essen, Oktober 1998.

5 Bedrohungen für Unternehmen

Frank Wiltner

Geschafft! Endlich kann die Firewall in Betrieb genommen werden und alle Mitarbeiter können E-Mail und Internet nutzen. Schneller und einfacher soll nun alles werden. Alles wurde gründlich durchdacht, ein zweistufiges Firewall-Konzept soll das Firmennetzwerk absichern. Ein direkter Datenverkehr zwischen dem Internet und dem lokalen Netzwerk ist nicht gestattet. Stattdessen dient ein Proxy, ein Webserver, der Seiten aus dem Internet lädt und lokal zur Verfügung stellt, zwischen den Firewalls als Vermittlungsstelle für die übertragenen Daten. Damit sind alle Risiken eingeschränkt.

Sicher?

Vor einiger Zeit wurden wir von einem IT-Dienstleistungsunternehmen gebeten, die beschriebene Firewall-Umgebung genau zu untersuchen. Bei den Administratoren der Firewall bis hin zum IT-Management war man sich der Gefahren, die durch das Internet drohen, durchaus bewusst. Dementsprechend hat das Management genügend Mittel bereit gestellt und die Administratoren haben Konzeption und Konfiguration nach bestem Wissen und Gewissen vorgenommen.

Das Ergebnis war eine mehrstufige Firewall, bei der jedes Detail perfekt durchdacht war. Moderne Systeme, lange getestete Software, Beachtung von Vorgaben, z.B. des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und das Handeln nach »Best Practices« waren die Voraussetzungen für ein sicheres System nach dem Stand der Technik. Für das Surfen im Internet muss der Anwender auf einen Proxy zugreifen. Dieser war auch für Zugriffe aus dem Internet auf bestimmte Server des Unternehmens bestimmt.

Alles bestens? Nein. Der Proxy wurde massiv von Hackern aus aller Welt als Anonymisierungsserver missbraucht. Gleichzeitig war, auf Grund der Vertrauensstellung des Proxys, der uneingeschränkte Zugriff auf das gesamte Unternehmensnetzwerk aus dem Internet möglich. Wir haben dies durch die Kompromittierung verschiedener Systeme des Unternehmens nachgewiesen.

Wie konnte es dazu kommen? Vielleicht können die folgenden Ausführungen ein wenig dazu beitragen, den Ausgangspunkt der Bedrohungen und die Umstände, die sie begünstigt haben, aufzudecken.

Nach einer kurzen zusammenfassenden Betrachtung der Ursachen für Bedrohungen und der Möglichkeit, diese aufzudecken, werden mögliche Angreifer und ihre Motivation vorgestellt. Daran anschließend werden die gängigen Angriffe auf IT-Systeme erläutert. Anschließend werden weitere Bedrohungen dargestellt.

5.1 Ursachen für Bedrohungen

Störfaktor M. Die überwiegende Anzahl der Bedrohungen geht vom Menschen aus. Doch nicht nur aufgrund vorsätzlicher Handlungen, oftmals ist fehlendes Wissen, Leichtfertigkeit und das falsche Einschätzen der Umgebung ein entscheidender Faktor.

Neben dem Menschen selbst bietet seine fast kompromisslose und selten kritische Hingabe zur Technik weitere Möglichkeiten. Die Technik wird immer komplexer, Ausfälle oder Fehler im System werden damit immer wahrscheinlicher.

Oft wirken auch mehrere Faktoren nebeneinander oder sie bauen aufeinander auf. So kann sich aus einem kleinen Ärgernis schnell eine kritische Störung der Geschäftsprozesse entwickeln.

Ein achtlos weggeworfenes Papier mit dem niedergeschriebenen Passwörtern, das in die falschen Hände gerät oder Nachlässigkeit in der Netzwerk- und Serverkonfiguration sind in der Verbindung mit der kriminellen Energie eines Hackers der perfekte Nährboden für erfolgreiche Angriffe auf Ihr Netzwerk.

Führende amerikanische Computer Institute, wie das CSI (Computer Security Institute) in Verbindung mit dem FBI (Federal Bureau of Investigation), ermitteln in regelmäßigen Abständen die Ursachen und Auswirkungen Hacker-Angriffen, dem Befall mit Viren oder ähnlichen sicherheitsrelevanten Vorkommnissen.

Dabei lassen sich in den letzten Jahren einige deutliche Trends feststellen:

- das Internet ist zum bestimmenden Ausgangspunkt für Angriffe geworden,
- Angriffe auf die Verfügbarkeit der Systeme nehmen drastisch zu,
- die Kosten, die Firmen aus Angriffen entstehen, steigen immens und
- die Aktivitäten internationaler Regierungen und Geheimdienste nehmen zu.

Weiterhin wird festgestellt, dass ein großer Anteil der Angriffe von Innentätern durchgeführt wird. Enttäuschte oder entlassene Mitarbeiter, die sich an ihrem Arbeitgeber rächen oder ihn bewusst schädigen wollen, haben durch ihre Kenntnisse der internen Strukturen sehr gute Möglichkeiten für Angriffe.

5.2 Analyse der Bedrohungen

Die spezifischen Bedrohungen, die den Unternehmenserfolg gefährden, können in einer Bedrohungsanalyse ermittelt werden. Gleichzeitig werden hier Verknüpfungen von Bedrohungen und die damit verbundenen Auswirkungen festgestellt. In einer anschließenden Risikoanalyse wird die Wahrscheinlichkeit für das Eintreten der in der Bedrohungsanalyse beschriebenen Ereignisse dargestellt.

Die Ergebnisse beider Analysen bilden die Grundlage für die Ermittlung des Return on Investments (RoI) für IT-Sicherheitsmaßnahmen. So wie die Bedrohungsanalyse den möglichen Schadenswert darstellt, ermittelt die Risikoanalyse die Eintrittswahrscheinlichkeit. Nicht immer lassen sich diese Werte in Zahlen ausdrücken. Imageverlust, die Verletzung von Gesetzen und Vorschriften sowie das Nichteinhalten von Verträgen zieht oft nicht abschätzbare Folgen für die weitere Unternehmensentwicklung nach sich.

In der Risiko- und Bedrohungsanalyse versuchen wir, diesen Gefahren Rechnung zu tragen und sowohl materielle als auch immaterielle Wirkungen der Bedrohungen qualitativ als auch quantitativ anschaulich darzustellen. In einer Risikomatrix werden die untragbaren Risiken deutlich hervorgehoben.

Aus der Kombination von Angriffswahrscheinlichkeit und Schadenshöhe ergibt sich das spezifische Gefahrenpotenzial, das konkrete Risiko für ein Unternehmen. Lassen sich nun beispielsweise in einem Sicherheitskonzept Maßnahmen entwickeln, die mit einem geringeren finanziellen Aufwand umgesetzt werden können, als die auf Grund des ermittelten Risikos erwarteten Wiederherstellungskosten betragen werden, ist das RoI positiv.

5.3 Täter

In den folgenden Abschnitten werden verschiedene Angriffe vorgestellt, die immer wieder von verschiedenen Personengruppen gegen Unternehmen und Privatpersonen durchgeführt werden. Doch wer sind diese Personen? Welche Beweggründe haben die Angreifer, zum Beispiel das Netzwerk eines großen Online-Buchhändlers komplett lahm zu legen?

5.3.1 Geheimdienste

Während in der Vergangenheit überwiegend fremde Militär- und Staatsführungen das Ermittlungsziel der Geheimdienste waren, suchen die Dienste nach dem Ende des Kalten Krieges nach neuen Betätigungsfeldern.

Zunächst verdeckt, inzwischen aber ganz offen, konzentrieren sich die Geheimdienste aller Welt auf das Ausspionieren der Volkswirtschaften anderer Länder und zunehmend auch Unternehmen der freien Wirtschaft.

Diese neue, umfassende Form der Wirtschaftsspionage wird von den Regierungen der entsprechenden Staaten finanziell und politisch unterstützt, dies belegen unter anderem entsprechende Berichte des deutschen Amtes für Verfassungsschutz. Als Beispiel möge die nahezu lückenlose Überwachung des Europäisch-Amerikanischen Telekommunikationsaufkommens mittels des amerikanischen Abhörsystems Echelon gelten.

Insbesondere die sehr gute finanzielle und technische Ausstattung der Geheimdienste gestattet Angriffe, die anderen Personengruppen nicht möglich wären. So muss davon ausgegangen werden, dass Geheimdienste in der Lage sind, selbst verschlüsselte Daten in kürzester Zeit oder gar in Echtzeit zu entschlüsseln.

5.3.2 Industriespionage

Doch nicht nur Geheimdienste, auch große Unternehmen beschäftigen professionelle Einheiten zum Ausspähen des Mitbewerbs. Obwohl ihnen typischerweise nicht dieselben finanziellen Mittel zur Verfügung stehen, lohnt sich der Aufwand bei der Erkundung von Konzernstrategien, Unternehmensdaten oder Forschungsergebnissen ihrer Konkurrenten.

5.3.3 Hacker

Hacker sind selten an politische oder finanzielle Organisationen gekoppelt. Zumeist ist ihr einziges Ziel die Selbstdarstellung, der Beweis, es auch mit professionell abgesicherten Systemen aufnehmen zu können.

Der »wahre« Hacker ist weder an Daten oder Informationen, noch an einer finanziellen Schädigung seines Opfers interessiert. Sein Antrieb ist der Ruhm, die Hoffnung, als »Überwinder elektronischer Grenzen« in die Geschichte einzugehen. Sein technisch ausgereiftes Wissen behält er für sich oder teilt es mit Gleichgesinnten in Hackerorganisationen oder Diskussionsforen im Internet.

Andere Hacker streben durch die Veröffentlichung von Sicherheitslücken in Betriebssystemen und Anwendungen nach Ruhm. Oft liefern sie auch kleine Programme zum Nachprüfen ihrer Erkenntnisse mit. In kürzester Zeit sind im Internet Tools verfügbar, die Windows oder Linux »knacken« und damit die Betriebssicherheit gefährden.

Diese ermöglichen es auch Anwendern mit geringem technischen Kenntnissen, einzelne Systeme oder ganze Netzwerke anzugreifen. Auf Grund des fehlenden Bewusstseins über die Folgen ihres Handelns hinterlassen sie oft eine breite Spur der Verwüstung.

5.3.4 Softwareentwickler

Viele Softwareprodukte enthalten sogenannte Hintertüren (engl. Back Doors), die die Entwickler bewusst eingebaut haben. Obwohl diese meist nur zum Testen der Programme oder Systeme unter Betriebsbedingungen und zum Einspielen neuer Programmversionen dienen sollen, können diese Schnittstellen aber auch immer zum unbefugten Zugriff auf Daten und Informationen missbraucht werden.

Es muss davon ausgegangen werden, dass eine Reihe solcher Hintertüren auf aktives Betreiben von Geheimdiensten implementiert werden. Als Beispiel soll hier an den berüchtigten NSA-Key in der Crypto-Software des Microsoft Windows Betriebssystems erinnert werden (dessen Verbindung zur NSA (National Security Agency) bis heute weder bestätigt noch ausgeschlossen ist).

5.3.5 Fremdpersonal

Wartungs- oder Reinigungspersonal, Mitarbeiter von Fremd- und Zeitarbeitsfirmen, Studenten, ohne diese flexiblen Arbeitskräfte sind viele unserer täglichen Arbeiten nicht mehr denkbar. Auf Grund des ihnen gestatteten physischen Zutritts zu Räumen oder einem notwendigen logischen Zugang zu Computersystemen sind sie wohl in der Lage, Angriffe gegen Unternehmen durchzuführen.

5.3.6 Administratoren

Administratoren besitzen zur Durchführung ihrer Arbeit umfangreiche Privilegien. Diese können, oft begünstigt durch unklare Verantwortlichkeiten und mangelnde Kontrolle, für eigene Zwecke missbraucht werden. Mit Hilfe ihrer technischen Möglichkeiten können Administratoren zudem leicht ihre Spuren verwischen, so dass Manipulationen und Diebstähle lange Zeit oder gar für immer unentdeckt bleiben.

5.3.7 Mitarbeiter

Auch wenn die Mitarbeiter in der Regel wenig Rechte besitzen, die zudem auf die eigene Arbeitsstation beschränkt sind, reichen die Rechte in der Regel aus, um Angriffe gegen Anwendungen und Systeme im lokalen Netzwerk durchzuführen. Neugier, Spieltrieb, Überlastung oder Langeweile sind ihr Antrieb. Unzufriedene Mitarbeiter können ihrem Arbeitgeber aber auch gezielt Schaden zufügen.

5.4 Vorsätzliche Manipulation

Zu den Bedrohungsarten gehören auch die vorsätzliche Manipulation mit ihren entsprechenden Ausprägungen, die nachfolgend erörtert werden.

5.4.1 Angriffe über das Internet

Neben einer Reihe herkömmlicher Angriffsmöglichkeiten, vom unberechtigten Eindringen in Gebäude, über das Befragen von Mitarbeitern bis zum Anzapfen von Telefonleitungen, ist das Internet die wesentliche Quelle für Angriffe mit einem Ursprung außerhalb des Unternehmens. Doch die im Internet verbreiteten Technologien werden auch im internen Netzwerk eingesetzt, so dass die hier beschriebenen Bedrohungen auch – und sogar noch einfacher – von Innentätern ausgehen können.

Angriffe über die Internetverbindung des Opfers werden durch das zu Grunde liegende Netzwerkprotokoll TCP/IP ermöglicht. Dieses Protokoll wurde in den 60er Jahren des vergangenen Jahrhunderts mit der Annahme vertrauenswürdiger Teilnehmer entwickelt. Eine Absicherung der Netzzugänge, z.B. durch eine Autorisierung der Benutzer oder Verschlüsselung der übertragenen Daten, ist nicht enthalten.

Die weite Verbreitung des Wissens über TCP/IP deckt Sicherheitslücken im so genannten TCP/IP-Stack oder in TCP/IP basierten Diensten einerseits sehr schnell auf, andererseits werden Informationen über neue Schwächen und Implementierungsfehler nahezu täglich im Internet veröffentlicht und damit sehr schnell verbreitet.

Bei einem Angriff über das Internet gibt es grundsätzlich zwei verschiedene Ansatzpunkte. Ein Teil der Angriffe nutzt **Sicherheitslücken** in den angebotenen Diensten gezielt aus und ermöglicht es dem Angreifer oft, sich wie ein lokal angemeldeter Administrator zu bewegen. In dem anderen Teil begibt man sich in eine so genannte **Man-In-The-Middle**-Position zwischen den Benutzer und den angesprochenen Server. Das bedeutet, dass der Angreifer alle Daten zwischen dem Benutzer und dem Server über seinen Computer leitet.

Sicherheitslücken bestehen in der Regel aus Programmierfehlern in Programmen wie E-Mail- oder Web-Servern. Die Entwickler der Software haben vielleicht eine Hintertür eingebaut oder – für die Entwicklung und das Testen notwendige – Debugging-Informationen im fertigen Programm nicht entfernt. Meist sind es aber kleine Fehler, wie ungenügend getestete Puffer, die es dem Angreifer erlauben, einen beliebigen eingespielten Code oder Anwendungen des Servers auszuführen.

Man-In-The-Middle-Attacken sind schwieriger vorzubereiten. Befindet sich der Angreifer nicht schon in dieser Position, z.B. als Internet Service Provider oder Verwalter der Netzwerksysteme, muss er sich in die Position bringen. Er muss den Datenstrom zwischen einem Benutzer und dem Server über sein System umleiten. Dies kann er tun, indem er dem Benutzer falsche Zieladressen (nämlich seine) übermittelt. Er kann allerdings auch Netzwerkkomponenten auf dem Weg zwischen Benutzer und Server so manipulieren, dass sie alle Daten über sein System schicken.

5.4.2 Unerlaubter Zugriff auf Systeme

Die einfachste Möglichkeit, Zugriff zu fremden Systemen zu erlangen, bringt das Protokoll TCP/IP bzw. darauf aufsetzende Dienste gleich mit: die Übertragung aller Daten im Klartext. Viele der gängigen und nach wie vor weit verbreiteten Anwendungsprotokolle (z.B. http, telnet, ftp, POP3) übermitteln Benutzernamen und dazu gehörendes Passwort unverschlüsselt und für jeden lesbar.

Dies kann man leicht überprüfen. Programme, die den gesamten ein- und ausgehenden Datenverkehr protokollieren, sind im Internet frei zugänglich (z.B. Ethereal). Startet ein Anwender dieses Programm auf dem Arbeitsplatzrechner zusammen mit dem Lieblings-Mail-Client, erhält er nach kurzer Zeit folgenden Datenstrom auf Port 110: *...USER administrator ok PASS geheim ok...* Der Benutzer *administrator* hat das Passwort *geheim*, das Mail-Programm sendet dies in kurzen regelmäßigen Abständen an den Mail-Server, um den Posteingang zu prüfen.

Ein Angreifer, der in der Lage ist, den Datenstrom im Netzwerk mitzulesen, wird in kurzer Zeit eine Reihe von Passwörtern erfahren. Oft gibt es dann ein Benutzerkonto auf diesem oder einem anderen Rechner, für den der mitgelesene Benutzername und das Passwort gültig sind, da Benutzer meist für mehrere Systeme (Internet-Einwahl, E-Mail, Online Banking) dasselbe Passwort verwenden.

Doch auch angeblich verschlüsselte Passwörter bieten nicht immer den erhofften Schutz. In der Regel sind Passwörter nicht wirklich verschlüsselt, sondern mit einer festen, allseits bekannten Einwegfunktion kodiert. Das Ergebnis, der so genannte Hash, wird im Rechner gespeichert. Beim Anmelden des Benutzers wird die Funktion erneut ausgeführt und das Ergebnis mit dem gespeicherten Hash verglichen. Ein Angreifer kann sich dies zunutze machen, indem er die Funktion mit Wörtern aus einem Wörterbuch durchführt oder durch einfaches Probieren aller Möglichkeiten (Brute Force).

Abhilfe schaffen hier nur sehr lange Passwörter (>8 Zeichen), die aus Groß- und Kleinbuchstaben, sowie Zahlen und Sonderzeichen bestehen.

Voraussetzung ist jedoch, dass auch das eingesetzte Betriebssystem oder die verwendete Software die Sicherheitsbemühungen unterstützt. In seiner Standardkonfiguration legt Microsoft Windows größtmöglichen Wert auf Kompatibilität. Das führt zum Beispiel dazu, dass Windows Passwörter vor der Kodierung in Großbuchstaben umwandelt. Zudem werden längere Passwörter in Teilen von je sieben Zeichen getrennt kodiert. Dies erleichtert die Suche nach Passwörtern erheblich.

Doch nicht nur das Ausnutzen bekannt gewordener Passwörter ermöglicht den unerlaubten Zugriff auf Systeme. Immer wieder tauchen im Internet Informationen über Sicherheitslücken in Anwendungen und Systemen auf, die sich Angreifer zu Nutze machen.

Ein beliebter Angriffspunkt sind so genannte Buffer Overflows in Internet-Dienstprogrammen. Die Entwickler der Programme müssen für bestimmte Eingaben, wie dem Benutzernamen des POP3-Dienstes eines Mail-Server, einen festen Bereich im Speicher festlegen. Nehmen wir an, sie haben für den Namen 50 Zeichen vorgesehen (was im Normalfall auch ausreichen sollte). Gibt ein Angreifer nun einen Namen mit einer Länge von wesentlich mehr als 50 Zeichen ein, überschreibt er damit andere Bereiche des Speichers. In der Folge wird das Programm unweigerlich abstürzen. Die Kunst des Angreifers besteht nun darin, den Absturz so zu steuern, dass das System mit ganz bestimmten Befehlen fortfährt. So kann z.B. eine Eingabe-Konsole geöffnet oder eine bestimmte Datei an eine vorgegebene E-Mail-Adresse gesendet werden.

Klingt schwierig? Ist es aber nicht. Einige grundlegende Programmierkenntnisse genügen vollauf. Die Befehle, die die Maschine ausführen soll, werden in der Zeichenkette übergeben, die das Programm zum Absturz bringt. Beim Absturz werden Register im Zielrechner so manipuliert, dass der Befehlszeiger auf die Zeichenkette im Speicher zeigt und der Rechner an dieser Stelle weiterarbeitet.

5.4.3 Abhören und Modifikation von Daten

Dieser Abschnitt konzentriert sich auf Angriffe aus der Man-In-The-Middle-Position. Zunächst soll die Frage beantwortet werden, wie sich ein Angreifer in diese Position bringen kann.

Die Zeiten, als einige elitäre Informatikstudenten Dutzende interessanter IP-Adressen auswendig kannten, sind längst vorbei. Heute sprechen wir die Systeme mit einem leicht zu merkenden Namen wie **www.meinebank.de** an. Um diesen Namen in eine numerische Adresse wie 123.45.67.89 umzuwandeln, fragt der Rechner des Benutzers einen Verzeichnisdienst (DNS– Domain Name Service). Das hier verwendete Protokoll ist – wen wundert's – nicht gesichert. Der Rechner stellt die Anfrage und vertraut der ersten Antwort die er erhält. Ist nun der Angreifer in Lage, der Antwort des befragten DNS-Server zuvorzukommen, und mit einer gefälschten IP-Adresse zu antworten, wird der Benutzer freiwillig alle Daten an den Rechner mit der vorgetäuschten Adresse senden.

Doch auch bei Verwendung der richtigen IP-Adresse kann der Angreifer die Daten über sein System umlenken. Steuerprotokolle für den Datenverkehr im Internet, wie ICMP (Internet Control Message Protocol), RIP (Router Information Protocol) oder OSPF (Open Shortest Path First), ermöglichen es, den angegriffenen Rechner oder Netzwerkkomponenten auf dem Weg zwischen dem Benutzer und dem Server dazu zu bringen, die Daten an das System des Angreifers zu senden.

Diese Man-In-The-Middle-Position bietet dem Angreifer die Möglichkeit, alle Daten, die der Benutzer zum Server sendet, abzufangen, zu lesen und verändert oder unverändert weiterzusenden. Darauf bauen verschiedene Angriffe auf, die im folgenden vorgestellt werden.

TCP/IP ist ein verbindungsorientiertes Protokoll. Ein Benutzer baut eine Verbindung zu einem Server auf, auf dieser Verbindung werden nun alle Daten übertragen. **Session Hijacking** nennt man die Übernahme der bestehenden Verbindung durch einen Angreifer zwischen Benutzer und Server. Bei einem derartigen Angriff bricht die Verbindung für den Benutzer ab und der Server sendet von nun an alle Daten an den Angreifer. Die besondere Gefahr dieses Angriffs besteht darin, dass ein Angreifer sogar eine Verbindung missbrauchen kann, für die sich der Benutzer zuvor am Server authentisieren musste. Damit erhält der Angreifer alle Rechte des Benutzers.

Bei einer anderen **Man-In-The-Middle**-Attacke wird bereits die Verbindungsanfrage über den Rechner des Angreifers umgeleitet. Der Angreifer gibt sich gegenüber dem Benutzer als Server und gegenüber dem Server als Benutzer aus. Alle Daten, auch Authentisierungsinformationen, laufen über den Angreifer. Besonders makaber an diesem Angriff ist, dass auch eine Verschlüsselung der Daten, z.B. durch SSL (Secure Socket Layer), keinen Schutz bietet. Eine Verschlüsselung besteht zwischen Benutzer und Angreifer, sowie zwischen Angreifer und Server. Der Angreifer selbst gelangt jedoch in Kenntnis des Klartextes.

SSL wird häufig für Internet-Transaktionen wie Online-Banking oder Online-Shopping verwendet. Ein Schlüssel oder ein Schloss im Browserfenster soll den Benutzer von der Sicherheit der Transaktion überzeugen. Gelingt jedoch der oben beschriebene Angriff, ist die Sicherheit trügerisch. Viele Banken setzen noch immer das von T-Online bekannte PIN/TAN-Verfahren (Personal Identification Number, Transaction Number) ein. Wenn der Benutzer sich an der Bank anmeldet, gelangt der Angreifer in die Kenntnis von Kontonummer und PIN. Gibt der Benutzer nun eine TAN ein, um beispielsweise eine Überweisung durchzuführen, ist der Angreifer im Besitz einer gültigen TAN.

5.4.4 Angriff auf die Verfügbarkeit von Systemen

Immer mehr Unternehmen verwenden das Internet für den Aufbau von leistungsfähigen Vertriebskanälen. Online-Versandhäuser und Online-Buchhandlungen wenden sich direkt an den Kunden (b2c – Business to Customer), Zuliefer- oder Dienstleistungsunternehmen stellen ihre Dienste anderen Unternehmen zur Verfügung (b2b – Business to Business).

In beiden Fällen ist die Verfügbarkeit der entsprechenden Systeme von entscheidender Bedeutung, ein Ausfall hat direkte finanzielle Konsequenzen.

Jedoch steigt die Zahl von Angriffen gegen die Verfügbarkeit (Denial-Of-Service-Angriffe) weiter und ihre Auswirkungen werden immer katastrophaler. Grundsätzlich dient ein solcher Angriff nur dem Ziel, das entsprechende System oder Teile davon zum Absturz zu bringen oder vorhandene Ressourcen (Anzahl an Verbindungen, Rechenzeit, Bandbreite) voll auszuschöpfen.

Dies geschieht durch das Ausnutzen von Sicherheitslücken im TCP/IP-Stack, in Betriebssystemen oder Anwendungsprogrammen, durch die diese Software zum Absturz gebracht wird. Oft sind diese Systeme nicht verfügbar, bis sie manuell neu gestartet werden.

Ein Server stellt für jede Verbindung Arbeitsspeicher und Rechenzeit zur Verfügung. Öffnet ein Angreifer Tausende solcher Verbindungen, ist der Server nicht mehr in der Lage, andere Benutzer zu bedienen. Der Server ist nicht mehr erreichbar und kann unter der Last zusammenbrechen.

Um dies zu verhindern, wird oft die Anzahl der gleichzeitigen Verbindungen pro Benutzer beschränkt. Hacker haben daher unzählige Rechner im Internet so manipuliert, dass sie gleichzeitig auf einen bestimmten Server zugreifen. Mit diesem verteilten Angriff (Distributed-Denial-Of-Service-Angriff) wurden große Internet-Portale wie Yahoo und der Online-Buchhändler Amazon.com lahmgelegt.

Doch auch scheinbar unempfindliche Netzwerkkomponenten wie Router und Switches und sogar Firewalls sind nicht vor Denial-of-Service-Angriffen sicher. Diese aktiven Komponenten speichern Verbindungsdaten in Tabellen. Gelingt es dem Angreifer, diese Tabellen zu füllen, wird das System keine weiteren Verbindungen mehr zulassen. Im Falle der Firewall besteht sogar die Möglichkeit, dass Daten ungefiltert weitergeleitet werden.

Erleichtert wird dies durch die Art des Verbindungsaufbaus des TCP/IP Protokolls – dem so genannten Three-Way-Handshake. Der Client sendet ein SYN-Paket (Synchronization), eine Verbindungsanfrage. Der Server antwortet mit SYN/ACK (Synchronization/Acknowledge), Verbindungsanfrage bestätigt. Der Client müsste nun ein ACK (Acknowledge) schicken, eine Bestätigung, dass die Verbindung besteht. Sendet ein Angreifer eine Reihe von SYN-Paketen (SYN-Flooding), sind die Tabellen der aktiven Komponenten voll mit Daten über halboffene Verbindungen, die gar nicht oder erst nach langer Zeit gelöscht werden.

5.4.5 Missbrauch von Anwendungen

Anwendungen müssen für die Benutzer verfügbar sein, damit sie ihren Dienst versehen können. Datei-, Druck- und Datenbankserver sind im lokalen Netzwerk ansprechbar, E-Mail-, FTP- und HTTP-Server sogar im gesamten Internet.

Der Zweck der Systeme ist genau bestimmt. Für genau diesen Zweck wurden sie konzipiert, angeschafft und konfiguriert. Doch oft werden Systeme von berechtigten Benutzern für andere Zwecke missbraucht. Auf Dateiservern werden Audio- oder Videodateien aus dem Internet gespeichert, andere Server werden zum Spielen verwendet.

Das Versenden von tausenden E-Mails, vielleicht mit anzüglichen Inhalten oder unerwünschter Werbung, über den im Internet frei zugänglichen Mail-Server an Dritte ist sicher genau so unerwünscht wie das Ausnutzen ihrer

HTTP- und FTP-Server für das Einrichten so genannter Warez-Sites durch Web-Piraten für die Verteilung von illegalen Inhalten. Auf diesen Seiten findet man dann Raubkopien von Spielen und Programmen, Seriennummern für Anwendungsprogramme, Programme zum Hacken, aber auch raubkopierte Spielfilme und Musikdateien.

Die Mitarbeiter können die ihnen anvertrauten IT-Systeme beabsichtigt oder unbeabsichtigt missbrauchen. Absicht muss man z.B. unterstellen, wenn die Mitarbeiter im Rahmen ihrer Tätigkeit unberechtigt Informationen lesen, die nicht für sie bestimmt sind, oder Sicherheitslücken ausnutzen, um ihre Zugriffsrechte unzulässig zu erweitern.

Mitarbeiter können ihr System oder andere Systeme unbeabsichtigt kompromittieren, indem sie zum Beispiel:

- Programme aus dem Internet laden und ausführen, die Viren oder Trojanische Pferde enthalten oder
- Internetseiten laden, die manipulierte ActiveX-Controls, Java-Applets oder JavaScript bzw. BasicScript enthalten.

In der Folge können die betroffenen Systeme von externen Angreifern frei benutzt werden, um weitere Angriffe durchzuführen.

5.4.6 Viren, Würmer und Trojanische Pferde

I LOVE YOU!

Sicher erinnern Sie sich an den massiven Befall von E-Mail-Systemen in aller Welt vor einigen Jahren mit diesem Virus. Und haben Sie nicht auch mit dem Gedanken gespielt, die Mail trotz aller Warnungen zu öffnen?

Genau genommen handelt es sich gar nicht um einen Virus, sondern um einen *Wurm*. Wo liegt der Unterschied?

Ein *Virus* infiziert Dateien wie ausführbare Dateien oder Dokumentendateien. Beim Öffnen der Dateien aktiviert das Virus seine Schadensroutine, es löscht z.B. die Festplatte. Dann nistet es sich im Hauptspeicher ein und kann nun andere Dateien infizieren. Verbreiten kann sich das Virus nur durch die Weitergabe der Dateien.

Ein Beispiel ist das Melissa-Virus, der Microsoft-Word-Dokumente befällt und schon seit vielen Jahren aktiv ist. Melissa nutzt die Makro-Funktionen von Word und wird durch das Öffnen eines verseuchten Dokumentes geladen. Beim Öffnen eines anderen Dokumentes oder dem Erzeugen eines neuen Dokumentes hängt das Virus die schädlichen Makros an das Dokument an.

Dagegen verbreitet sich ein Wurm direkt, durch das Ausnutzen bestimmter Funktionen in Anwendungsprogrammen. Der I-LOVE-YOU-Wurm nutzt das Adressbuch und die Mailfunktionen von Outlook, um sich selbst an andere Opfer zu schicken.

Ein anderes Beispiel ist der Code Red-Wurm, der in diesem Jahr Tausende von Web-Servern befallen hat. Der Wurm nutzte eine Sicherheitslücke im Microsoft-Internet-Information-Server, die seit über zwei Jahren bekannt ist, um auf Funktionen des Servers zuzugreifen. Da dies auf demselben Weg passiert, wie der Abruf von Webseiten, konnte keine Firewall eingreifen. Und da keine Dateien infiziert wurden, waren auch Anti-Viren-Programme hilflos.

Der Wurm versendete sich selbst an weitere, zufällig ausgewählte Web-Server im Internet. Noch heute, ein halbes Jahr nach dem ersten Auftreten, lassen sich entsprechende Einträge in den Log-Files finden. Dennoch war, was die Verteilung betrifft, Code Red relativ uneffektiv. Wegen der zufälligen Auswahl der Zielrechner wurden einige Server mehrfach befallen, andere gar nicht. Es muss jedoch davon ausgegangen werden, dass die Routine zur Verteilung inzwischen so optimiert ist, dass das gesamte Internet in wenigen Sekunden angegriffen werden kann. Dies geschieht z.B. durch systematischen Befall ganzer Subnetze oder der Verwendung eines verteilten Adressbuches.

In den letzten Jahren haben so genannte *Trojanische Pferde* einen zweifelhaften Ruf erlangt. Der Name rührt aus der Tatsache, dass die schädlichen Inhalte zumeist in scheinbar nützlichen Programmen versteckt sind. Einmal installiert, stellen Sie in der Regel einen Internet-Dienst zur Verfügung, zu dem sich ein Angreifer verbinden kann, um Kontrolle über den befallenen Rechner zu erlangen. Des weiteren erhält der Angreifer auch alle Informationen über Eingaben des Benutzers oder den Inhalt von Festplatten und Laufwerken. Selbst die aktuelle Bildschirmanzeige bleibt ihm nicht verborgen.

Relativ jung dagegen ist das Tarnen *Trojanischer Pferde* in Werbebannern. Diese gehören inzwischen zum Alltag im Internet. Die Ersteller von Webseiten und die Programmierer von Freeware-Programmen versuchen so, ihre kostenlose Angebote zu finanzieren. Normalerweise sind Werbebanner nicht gefährlich, sie bringen jedoch auch nur wenig Nutzen. Um den zu erhöhen, sammeln einige dieser Banner alle Informationen eines Benutzers (IP-Adresse, Laufwerksinhalte, Tastatureingaben) und senden sie an einen Sammel-Server. Dort sollen die Gewohnheiten des Benutzers ausgewertet werden, um Werbung gezielter anbringen zu können. Dass dabei auch vertrauliche Daten, wie Passwörter oder Kreditkartendaten übermittelt werden, stört die Betreiber kaum.

5.5 Menschliches Fehlverhalten

In den vorangegangenen Abschnitten wurden Szenarien vorgestellt, die von Angreifern von innerhalb oder außerhalb von Organisation ausgehen und von diesen vorsätzlich verursacht werden.

Doch Bedrohungen entstehen nicht nur durch Vorsatz. Menschen machen menschliche Fehler. Ob aus Leichtfertigkeit, fehlender Konzentration oder dem Mangel an Fachwissen; kleine Fehler in unserer alltäglichen Arbeit können Angreifern Tür und Tor öffnen.

Ein wesentliches Glied in unserer IT-Landschaft sind die Administratoren, die das reibungsfreie Funktionieren der Systeme und Anwendungen gewährleisten. Durch eine richtige Konfiguration der Anwendungen und Systeme sind sie dabei auch für deren Sicherheit verantwortlich. Fehlkonfiguration und Abweichung von bestehenden Richtlinien können zu einem Sicherheitsrisiko werden und Angriffe wie zuvor beschrieben ermöglichen.

Doch auch die ungetestete Übernahme einer neuen Konfiguration in einem produktiven System kann die Verfügbarkeit des Systems massiv bedrohen. Dies kann nur durch den Einsatz einer Testumgebung verhindert werden, die äquivalent zur Produktivumgebung installiert wird. Hier können neue Konfigurationen, die Implementierung neuer Software oder das Einspielen von Updates ausführlich getestet werden.

Die Standardkonfiguration, mit der Betriebssysteme wie Windows 2000/XP, Unix oder Linux ausgeliefert werden, ist oft auf größtmögliche Kompatibilität zu bestehenden Anwendungen, weniger auf Sicherheit ausgerichtet. Probleme, die daraus entstehen können sind:

- Vergabe von zu vielen Berechtigungen an Benutzer,
- unnötige Aktivierung von Standard-Diensten,
- unzureichende Filterung von Datenströmen (Paketfilter),
- unzureichendes Passwortmanagement,
- unzureichende Protokollierung und
- fehlende Patches/Updates.

Die Verantwortung für die IT-Sicherheit allein zentralen Stellen oder den Administratoren zu überlassen, würde die globale Bedeutung der IT-Sicherheit abmindern. Jeder Einzelne ist an seinem Arbeitsplatz für die Sicherheit seines Umfeldes verantwortlich und kann damit zu einem Sicherheitsrisiko in seinem Bereich werden. Oft sind einfache Benutzer ohne weitergehende Berechtigungen das bevorzugte Ziel von Angreifern. Durch gezielte Fragen (Social Engineering) kann ein Angreifer von den Benutzern erste Ansatzpunkte für einen erfolgreichen Angriff erfahren. Ihn interessieren zunächst Informationen über die Netzwerktopologie, den Namen eines Servers und seine IP-Adresse. Auch der Name eines Benutzers und sein Passwort sind von wesentlicher Bedeutung und können meist erfolgreich erfragt werden.

Im einfachsten Fall ruft der Angreifer die Systemverwalter an, gibt vor ein Mitarbeiter zu sein und bittet um das Rücksetzen des Passwortes. Aber auch der umgekehrte Weg ist möglich. Der Angreifer ruft einen Mitarbeiter an, gibt sich als Systemverwalter aus und bittet um die gewünschten Informationen.

Mangelnde Sachkenntnis und fehlendes Sicherheitsbewusstsein, beides hervorgerufen durch unzureichende Schulungen der Mitarbeiter, sind die Grundlage für den Erfolg entsprechender Angriffe.

5.6 Organisatorische Schwachstellen

Die Erreichung und Aufrechterhaltung eines angemessenen Sicherheitsniveaus erfordert neben einer Reihe von technischen Maßnahmen auch umfangreiche organisatorische Regelungen. Diese müssen, entsprechend dem Aufbau eines Unternehmens, in allen Bereichen und Ebenen der Aufbauorganisation festgelegt und durchgesetzt werden.

Fehlen solche Regelungen, können die vorab genannten Bedrohungen sehr leicht zu konkreten Sicherheitslücken werden. Sicherheitsrelevante Vorfälle werden dann entweder zu spät als solche erkannt oder ihre Auswirkungen können nicht eingeschränkt werden.

Organisatorische Probleme entstehen beispielsweise:

- durch nicht geklärte Zuständigkeiten,
- durch unzureichende organisatorische Abläufe (z.B. in der Anwendungsentwicklung),
- durch fehlende oder unvollständige Richtlinien,
- durch unzureichende Erarbeitung von IT-Sicherheitskonzepten,
- durch mangelnde Fortbildung der Mitarbeiter zum Thema IT-Sicherheit oder
- durch fehlende Kontrollmaßnahmen (z.B. Durchführung von Security-Audits).

Die Wirksamkeit organisatorischer Regelungen wird durch solche Probleme untergraben. Welchen Nutzen hat das beste Virenschutzsystem oder die teuerste und ausgereifteste Firewall, wenn Benutzer und Administratoren immer wieder versuchen, deren Wirksamkeit zu umgehen? Durch präzise Arbeitsanweisungen für den Umgang mit Internet und E-Mail, verbunden mit regelmäßigen Schulungen über die Risiken dieser Medien, können die mit der Nutzung des Internet verbundenen Gefahren viel besser vermieden werden, als durch komplexe technische Einrichtungen.

Ebenso muss die Verantwortung des Einzelnen für die von ihm genutzten Anwendungen und Systeme gestärkt werden. Nur so kann gewährleistet werden, dass auftretende Störungen frühzeitig erkannt und beseitigt werden können.

5.7 Technisches Versagen

Blue Screen of Death, Mediation Guru, Core Dump, Kernel Panic, fast jedes Betriebssystem hat seinen eigenen Begriff für den Totalabsturz. Und jeder hat ihn schon einmal erlebt. Die Technik hat versagt, wieder einmal. Mal ist die

Hardware schuld (Festplattencrash, Ausfall von Systemteilen, elektromagnetische Störung in Kabeln, Fehler in Speicherbausteinen). Ein anderes Mal die Software (Fehler in Firmware, Treibern oder Anwendungsprogrammen).

5.8 Katastrophen

Der letzte betrachtete Bereich von Bedrohungen umfasst die so genannte »Höhere Gewalt«. Zu diesen Ereignissen, die sich meist nicht verhindern lassen, gehören Erdbeben, Feuer, Wassereinbrüche, aber auch der Ausfall der externen Stromversorgung oder Kommunikationseinrichtungen.

Die Wahrscheinlichkeit, dass solch ein Ereignis eintritt, ist relativ gering. Im Falle eines Falles sind jedoch meist große Teile der Systeme betroffen, bzw. die Auswirkungen sind gravierend und nur mit hohem Aufwand zu beseitigen.

So kann, z.B. bei Bauarbeiten auf dem Gelände, ein Hauptstromkabel durch Baggerarbeiten durchtrennt werden. Die Folge ist zunächst der Totalausfall aller Systeme. Doch auch nach dem Wiederherstellen der Stromversorgung droht weiteres Ungemach. Mit hoher Wahrscheinlichkeit sind die Server nicht ordnungsgemäß heruntergefahren. Bei vielen der gängigen Dateisysteme sind dabei Dateien unwiederbringlich zerstört.

»Kein Problem, spielen wir das Backup wieder ein«, werden Sie vielleicht sagen. »Backup, welches Backup?«, entgegnet aber vielleicht der Administrator.

Natürlich haben Sie ein Backup. Doch hat auch schon mal jemand das Wiederherstellen der Dateien getestet? Welche Schritte sind zu gehen, um das Gesamtsystem wieder zum Laufen zu bringen? Dies klärt ein Notfall-Plan – sofern er existiert.

Größere Schäden, in der Regel auch nicht durch einen Notfall-Plan zu beheben, verursacht ein Brand. In diesem Fall geht es meist nur noch um die Rettung von Daten und die Minimierung der Auswirkungen. Deshalb darf der Brand auch nie durch eine Sprinkleranlage gelöscht werden. Auch muss darauf geachtet werden, dass die Datensicherungsbestände nicht in räumlicher Nähe der Serversysteme gelagert werden.

5.9 Zusammenfassung

Die Zahl der Bedrohungen für ein Unternehmen ist enorm. Die vorangegangenen Abschnitte haben vielleicht dazu beitragen können, die wesentlichen Bedrohungen vorzustellen.

Es ist wichtig, die spezifischen Bedrohungen zu kennen, die unter Umständen des Erfolg eines Unternehmens gefährden können. Dann können auch Maßnahmen definiert werden, die das Risiko einschränken.

Die Implementierung einer Firewall allein reicht nicht aus, das Unternehmensnetzwerk abzusichern. Dies hat das Beispiel am Anfang des Kapitels deutlich gezeigt. Es ist notwendig, die Maßnahmen aufeinander abzustimmen. Das Ziel muss es sein, einen Level an Sicherheit festzulegen, der über das gesamte Unternehmen, also Organisation, Personal, Infrastruktur und Technik, gewährleistet wird. Gleichzeitig muss in regelmäßigen Abständen der aktuelle Stand der IT-Sicherheit überprüft werden.

IT-Sicherheit ist ein fortlaufender Prozess. Veränderte Geschäftsprozesse bedingen neue Anforderungen an die Sicherheit der Unternehmensdaten. Gleichzeitig bringt die rasante Veränderung des weltweiten IT-Marktes das Auftreten neuer Bedrohungen mit sich.

6 Sicherheitsbewusstsein im Mittelstand

Detlef Schumann

6.1 Einleitung

Im betrieblichen Alltag eines Unternehmens nimmt der Einsatz von Technologien der Informationstechnik stetig zu. Die schnelle Abwicklung von Aufträgen, eine wirtschaftliche Lagerhaltung oder ein effektiver Informationsaustausch innerhalb des Unternehmens oder mit anderen Partnern sind unter anderem notwendige Faktoren für eine wirtschaftliche Produktionsweise viele Betriebe. Vielfach steuern IT-Systeme nicht nur die Produktion, sondern sind auch verantwortlich für haustechnische (Telefon-, Klima- und Heizungsanlagen) sowie sicherheitstechnische Anlagen (Brandmelde- und Überwachungsanlagen). Leider ist das Bewusstsein über die eigene Abhängigkeit von IT-Systemen und die daraus resultierende Verletzlichkeit nicht ausreichend vorhanden.

Informationssicherheit für unternehmenskritische Daten, geistiges Eigentum wie Konstruktionszeichnungen oder Patente und Kundendaten wird immer noch als Phänomen angesehen. Beim potenziellen Risiko eines elektronischen Angriffes mangelt es vielerorts noch an der notwendigen Sensibilität. Denn Informationen als eigentlicher Vermögenswert eines Unternehmens werden immer noch zu wenig erkannt. Jede Kompromittierung der Vertrauenswürdigkeit oder Integrität könnte dabei den Verlust des Kundenvertrauens oder eines Wettbewerbsvorteils nach sich ziehen.

Sicherheitsaspekte für mittelständische Unternehmen umfassen dabei insbesondere die Anbindung an öffentliche Netze (Internet), die Sicherheit des lokalen Netzes sowie die Anwendungssicherheit. Generell bedingt die Informationssicherheit dabei Maßnahmen, um die Authentizität, Vertraulichkeit, Integrität und Verbindlichkeit von Nachrichten und Informationen sowie die Verfügbarkeit und die berechtigte Benutzung von betrieblichen Ressourcen sicherzustellen.

6.2 Grundlegende Begriffe und Sachverhalte

6.2.1 Aspekte der IT-Sicherheit

Mit der zunehmenden Vernetzung innerhalb und außerhalb der Firmen droht die Gefahr, dass sich Unberechtigte Zugang zu Informationen und Daten verschaffen und Manipulationen vornehmen, um den Unternehmen zu schaden, oder sich einen eigenen Vorteil zu verschaffen. Die Abschätzung dieses Gefahrenpotenzials macht es nötig abzuklären, gegen wen man sich schützen will.

Zum Beispiel kann für eine Organisation das Gefahrenpotenzial aus der Gruppe der Personen in folgende verschiedene Kategorien eingeteilt werden:

- verärgerte ehemalige Mitarbeiter,
- unehrliche Mitarbeiter,
- Mitarbeiter mit schlechter Schulung,
- Hacker oder
- Mitbewerber.

Bei dieser Einteilung ist zu beachten, dass diese Gruppen die Sicherheitsvorkehrungen zum Teil bewusst, aber auch unbewusst untergraben.

Mehrere Studien belegen, dass sicherheitsgefährdende Vorfälle in Unternehmungen zu 60% bis 80 % aus den eigenen Reihen erfolgen.

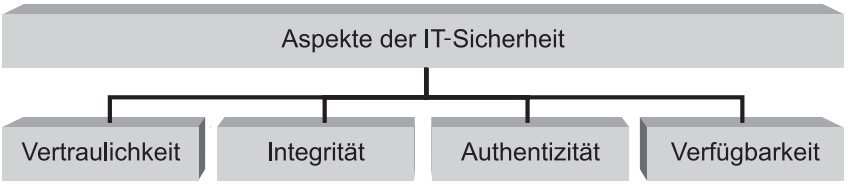


Abbildung 6.1: Aspekte der IT-Sicherheit

Die vier Kategorien *Vertraulichkeit, Integrität, Authentizität* und *Verfügbarkeit* bilden die Kriterien, die ein Sicherheitskonzept für ein Unternehmen erfüllen muss. Es sind Anforderungen an ein Modell, das Maßnahmen bereitzustellen hat, um ihre Einhaltung gewährleisten zu können.

Mit *Vertraulichkeit* ist gemeint, dass zu bearbeitende vertrauliche Daten, nur den berechtigten Personen zugänglich sind. Ein Verlust liegt bereits vor, wenn nicht genügend Sorgfalt bezüglich ihrer Geheimhaltung eingehalten wird.

In jedem einzelnen Unternehmensbereich muss mit geeigneten Maßnahmen der Eingriff Unbefugter in interne Datenbestände verhindert werden.

Der Ausschluss einer unberechtigten Änderung der verarbeiteten Daten wird als *Integrität* bezeichnet. Dabei ist gemeint, dass der gewünschte Empfänger genau die Daten einer Nachricht erhält, die der Absender übertragen hat. Dieses Integritätskriterium ist auch innerhalb eines Betriebes zu beachten. Ein interner Mitarbeiter muss beim Dateiaufruf exakt die Informationen bekommen, die zuletzt so gespeichert wurden. Es besteht die Gefahr, dass Unberechtigte im internen Datenbestand der Firma Manipulationen vornehmen oder Online-Dokumente beim Datentransfer verändern.

Unter der *Authentizität* von Daten wird verstanden, dass der Empfänger erkennen kann, wer der wirkliche Absender eines Dokumentes ist. Der Absender muss aber auch Gewissheit haben, dass die gesendeten Daten nur an den beabsichtigten Empfänger gelangen.

Als vierter Aspekt der Sicherheitsanforderungen gilt die Gewährleistung der *Verfügbarkeit* von IT-Dienstleistungen, IT-Funktionen, Informationen und Daten. Sie sollen jederzeit in voller Funktionalität benutzbar sein.

6.3 Sicherheit im mittelständischen Betrieb

6.3.1 Einteilung der mittelständischen Unternehmen

Die kleinen und mittelständischen Unternehmen haben in der Bundesrepublik Deutschland eine entscheidende volkswirtschaftliche Bedeutung. Viele wirtschaftliche Eckzahlen wie steuerpflichtige Umsätze, Bruttowertschöpfung aller Unternehmen, Beschäftigungszahlen aller Arbeitnehmer oder Ausbildungsplätze werden zum großen Teil durch diese Unternehmen getragen.

Zur Beschreibung der quantitativen Kriterien von mittelständischen Unternehmen kommen die Betriebsgröße, die Beschäftigtenzahl und der Jahresumsatz in Betracht. Aufgrund dieser Richtgrößen werden in Deutschland die Unternehmen wie folgt eingeteilt.

Unternehmensgröße	Zahl der Beschäftigten	Jahresumsatz in €
Klein	Bis 9	Bis unter 500 T
Mittel	10 bis 499	Über 500 T bis 50 Mio.
Groß	Über 500	Über 50 Mio.

Tab. 6.1: Einteilung Unternehmen

Tendenziell ist zu bemerken, dass Unternehmen mit zunehmender Größe und strukturellem Aufbau in Sachen Informationssicherheit ein höheres Niveau erreichen. In der Betrachtung wird auf Unternehmen bis zu maximal 500 Mitarbeiter eingegangen, da diese Unternehmensgruppe in der Regel ein nicht so groß ausgeprägtes Sicherheitsbewusstsein entwickelt hat.

6.3.2 Gefahrenpotenzial

Bei der Nennung der möglichen Gefahrenpotenziale kann nur eine kleine Auswahl getroffen werden. Die folgende Auflistung erhebt nicht den Anspruch auf Vollständigkeit:

- Jedes mittelständische Unternehmen ist potenziell gefährdet.

  Es existieren keine mittelständischen Unternehmen, die nicht über sensible Informationen oder Kommunikationsbeziehungen verfügen. Die Gefahr des Risikos Opfer von Wirtschaftsspionage zu werden, steigt mit der Zunahme von Beziehungen nach außen, über die Informationen ausgetauscht werden sollen. Zu einer weiteren Erhöhung des Gefahrenpotenzials tragen auch solche Entwicklungen wie z.B. Outsourcing oder die Auslagerung von Wartungstätigkeiten (Fernwartung) bei.

- Gesamtstrategien in der Informationstechnologie sind in mittelständischen Unternehmen selten vorhanden.

  Investitionen in Informationstechnik erfolgt meistens nur in erforderlichen Einzelsegmenten. Die Entscheidungen für den Einsatz von neuen Technologien werden für bestimmte Bereiche nach Notwendigkeit getroffen. Solche Investitionen sind zum Beispiel der Einsatz von ERP- oder CRM-Softwarelösungen (Enterprise Resource Planning oder Customer Relationship Management). Diese Anschaffungen erfolgen aber nicht im Rahmen einer gesamten IT-Strategie sondern nur punktuell.

- In der Regel werden keine IT-Sicherheitskonzepte bei der Anschaffung von Informationstechnologien mit eingekauft.

  Die Investition erfolgt nur zur Lösung von Problemen in einzelnen Bereichen des Unternehmens. Notwendige Planungen und die Bereitstellung von Mitteln für die IT-Sicherheit werden in diesem Zusammenhang nicht mit berücksichtigt.

- Sicherheitsgefahren wachsen mit der Nutzung von Informationstechnologie.

  Es besteht ein enger Zusammenhang zwischen der Erhöhung des Gefahrenpotenzials und der Intensität der Nutzung von neuen Technologien. In Unternehmen mit einer hohen Nutzung sind viel mehr, da bereits aufgetretene, Sicherheitsvorfälle bekannt, als in Unternehmen mit einer geringeren Nutzung. Gleichzeitig ist aber zu bemerken, dass in solchen Unternehmen die Schäden durch Fehler der eigenen Mitarbeiter geringer

ausfallen. Dies ist darin begründet, dass in Firmen mit einer intensiven Nutzung der Informationstechnologie die Qualifizierung der Mitarbeiter besser ist.

- Alle Unternehmensbereiche in mittelständischen Unternehmen sind Sicherheitsgefahren ausgesetzt.

  Die betriebswirtschaftlichen Bereiche (z.B. Finanzbuchhaltung, Controlling, Forschung und Entwicklung, Produktion) in einem Unternehmen sind lohnende Angriffsziele für Wirtschaftsspionage.

6.3.3 Die Fähigkeit der Bewältigung von Sicherheitsgefahren

Mit abnehmender Größe von Unternehmen ist auch der Fähigkeit der Bewältigung von Sicherheitsgefahren eine Grenze gesetzt. In kleinen Unternehmen fehlt meistens eine hinreichende Sicherheitsstrategie. Mit der Annahme einer täglichen Datensicherung sei die Firma hinreichend auf einen Datenverlust abgesichert, wird jede weitere Investition in Sicherheit vernachlässigt.

Des Weiteren fehlen den mittelständischen Unternehmen in der Regel eine strategische Planung sowie ausreichend qualifiziertes und sensibilisiertes Personal.

Die großen Schwierigkeiten bei der Bewältigung von Sicherheitsgefahren werden bei den kleinen und mittleren Unternehmen nicht nur durch die geringen personellen sondern auch durch die niedrigen finanziellen Ressourcen hervorgerufen.

Weitere Punkte der schlechten Bewältigung von Sicherheitsgefahren sind:

- Schlechtes Problembewusstsein auf der unteren Mitarbeiterebene sowie bei der Unternehmensleitung.

  Ein großer Schwachpunkt ist in der fehlenden Sensibilität bei den Mitarbeitern zu sehen. Das Management in einem Unternehmen – welches die Unternehmensstrategie entscheidet – hat oft ebenfalls ein geringes Bewusstsein in Fragen der IT-Sicherheit. Vielerorts ist das Problem zu erkennen, dass die Unternehmensleitung sich der Problematik von Sicherheitsgefahren verschließt und der Meinung ist, dass ihre Firma viel zu uninteressant für etwaige Attacken ist. Viele Unternehmer vertreten den Standpunkt, dass sie keine schützenswerten Informationen besitzen.

- Reaktion mit technischen Mitteln auf eingetretene Schäden.

  In den meisten Unternehmen wird auf eingetretene Schäden mit technischen Mitteln, wie z.B. Verbesserung des Virenschutzes oder Einsatz einer Firewall reagiert. Bei dieser Vorgehensweise erfolgen die höchsten Investitionen in technische oder bautechnische Maßnahmen und notwendige Investitionen in organisatorische oder personelle Maßnahmen werden vernachlässigt.

- Sicherheit wird nicht als umfassender Prozess verstanden.

  In vielen Unternehmen werden Investitionen in Sicherheitsprodukte getätigt, wenn bereits Schwachstellen aufgetreten sind und Maßnahmen getroffen werden müssen. Diese Vorgehensweise ist aber nicht in einem Prozess verankert, der sich mit einer kontinuierlichen Auseinandersetzung zu Sicherheitsfragen beschäftigt.

- Mangelnde Unterstützung durch die Unternehmensleitung.

  Viele Unternehmen werden durch einen kleinen Personenkreis geführt, welcher sich mit der Problematik IT-Sicherheit wenig oder gar nicht auseinandersetzt. Die Kosten für mögliche Schäden von Sicherheitsgefahren und deren Auswirkungen auf das Unternehmen lassen sich schwer ermitteln und werden daher durch die Geschäftsleitung nicht genug beachtet.

  Es werden den Sicherheitsproblemen nicht genügend Aufmerksamkeit geschenkt, weil eine Einbindung in die Betriebsabläufe schwer möglich ist und die Produktorientierung durch den Unternehmer eine solche Sicht erschwert. Langfristige Entscheidungen in eine IT-Strategie und der damit verbundenen IT-Sicherheit sind aus Zeit- und finanziellen Gründen durch das Management nicht vorhanden.

- Finanzielle und personelle Ressourcen.

  Ressourcenprobleme vor allem finanzieller und personeller Art führen in mittelständischen Unternehmen dazu, dass Investitionen nicht langfristig geplant und vorbereitet werden, sondern mehr oder weniger sprunghaft erfolgen und sich auf unbedingt erforderliche Maßnahmen konzentrieren.

  Die Anstellung von Sicherheitsbeauftragten oder auch die Freistellung von Mitarbeitern für die IT-Sicherheit übersteigt in vielen Firmen die vorhandenen Möglichkeiten und werden nicht vorgenommen.

- Einsatz von externen Dienstleistungsunternehmen.

  Aufgrund der zuvor erwähnten geringen Kapazitäten müssten mittelständische Unternehmen verstärkt aus externe Dienstleister zurückgreifen. Diese Inanspruchnahme scheitert nicht nur an den anfallenden Kosten, sondern auch an starren Denkweisen des Managements, die keinem Dritten Einblick in das Unternehmen geben wollen.

- Fehlende Schulung und Weiterbildung in Fragen der IT-Sicherheit.

  Durch eine hohe Arbeitsbelastung der Mitarbeiter in mittelständischen Unternehmen ist der Zeitaufwand für notwendige Schulungs- oder Informationsveranstaltungen sehr begrenzt. Die starke Einbindung der Mitarbeiter in den Betriebsalltag lässt wenig Spielraum für solche Maßnahmen.

  Gleichzeitig spielen in diesem Zusammenhang auch die geringen finanziellen Ressourcen eine wichtige Rolle.

- Großunternehmen verlangen immer mehr Sensibilität in Sicherheitsfragen von den mittelständischen Unternehmen.

  Durch die engere Anbindung von Mittelstandsbetrieben an den Produktionsprozess von Großunternehmen wird das Verlangen dieser an eine umfassende IT-Sicherheitspolitik auch innerhalb des Mittelstandes größer. Viele große Konzerne verlangen heute von ihren Zulieferern zur Sicherung ihrer eigenen sensiblen Daten ein hohes Sicherheitsniveau. Leider ist die Unterstützung seitens der »Großen« noch nicht ausgeprägt genug.

6.3.4 Vorhandene Sicherheitslücken im Mittelstand

Eine genaue Analyse der unterschiedlichen Gefahrenpotenziale hat einen großen Einfluss auf geeignete Strategien für die Gefahrenvorbeugung und -abwehr. Jedes mittelständische Unternehmen muss sich die Frage stellen, woher Bedrohungen kommen können. Folgende Fragen können gestellt werden:

- Werden die meisten Schäden
  - durch die eigenen Mitarbeiter,
  - durch den bewussten Missbrauch von Informationen oder
  - durch Datendiebstahl von Externen verursacht?
- Welche Wirkungen haben Viren oder Trojanische Pferde?
- Wie wirken sich Software-Anomalien oder Software-Defekte aus?

Im Folgenden werden einige häufig vorkommende Sicherheitsprobleme aufgelistet:

- Fehler durch eigene Mitarbeiter.

  Die meisten Schäden werden durch Mitarbeiter verursacht. Die meisten Schäden entstehen durch:

  - Nichtbefolgung von Vorschriften und Anweisungen,
  - Unzureichende Ausbildung,
  - Unachtsamkeit und Überforderung,
  - Unzufriedenheit und mangelnde Motivation oder
  - Zielgerichtetes Handeln.
- Social Hacking (Erschleichung von Passwörtern).

  Durch eine geringe Sensibilisierung der Mitarbeiter in Fragen der IT-Sicherheit haben die sogenannten Social-Hacking-Attacken immer mehr Erfolg. Gerade in mittelständischen Unternehmen ist diese Methode ein leichtes Mittel um an sensible Informationen zu gelangen. Das Verfahren basiert nicht auf komplizierten technischen Verfahren und ist mit einfachen Mitteln möglich. Dabei versucht der Angreifer, über Telefon oder

ein persönliches Gespräch an Passwörter oder Zugriffscodes zu gelangen. Diese Methode ist in Unternehmen mit einer geringen Sicherheitskultur in den meisten Fällen äußerst erfolgreich.

- Einsatz von Firewall-Lösungen.

  In immer mehr mittelständischen Unternehmen werden Firewalls zum Schutz eingesetzt. Diese entsprechen zum größten Teil den technischen Anforderungen. Diese Lösungen sind aber selten in einem umfassenden Sicherheitskonzept integriert, welches ein eigenes Firewall-Konzept verlangt. In dieser Konzeption ist nicht nur der Einsatz einer Firewall beschrieben, sondern auch, dass diese ständig überwacht und aktualisiert werden muss. Nicht selten erfolgen erfolgreiche Angriffe über bekannte Sicherheitslücken in den eingesetzten Firewalls.

- Datenverschlüsselung.

  Der Datenaustausch mit anderen Unternehmen erfolgt sehr oft über E-Mail. Es werden nicht nur der normale Schriftverkehr über dieses Medium abgewickelt sondern auch sensible Daten wie Konstruktionszeichnungen, Bilanzen, Angebote versendet. Eine Verschlüsselung oder digitale Signaturen sind in den wenigsten Unternehmen etabliert.

- Schulungen im Bereich IT-Sicherheit.

  Wie oben schon beschrieben, erfolgen die meisten Schäden durch die eigenen Mitarbeiter. Schulungen zum Thema Sicherheit werden aber in den meisten mittelständischen Betrieben »stiefmütterlich« behandelt. Erst bei Sicherheitsvorfällen oder eingetretenen Schäden wird reagiert.

- Sicherheitsbeauftragter.

  Die wenigsten Unternehmen haben die Rolle eines IT-Sicherheitsbeauftragten etabliert. Gerade die Rolle eines Sicherheitsbeauftragten ist jedoch wichtig für die Umsetzung einer umfassenden Sicherheitsstrategie im Unternehmen. Diese Stelle muss mit den entsprechenden Kompetenzen ausgestattet sein, um dieses Ziel zu erreichen.

6.4 Auswege aus dem mangelnden Sicherheitsbewusstsein

Die folgenden Ausführungen sind als Anregung zu verstehen und bieten einige Ansatzpunkte für eine Verbesserung der Sicherheitslage und die Sicherheitsperspektiven der mittelständischen Unternehmen.

6.4.1 Etablierung eines unternehmensweiten IT-Sicherheitsmanagements

IT-Sicherheitsmanagement stellt jenen Teil des allgemeinen Risikomanagements dar, der die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von IT-Systemen gewährleisten soll.

Dabei handelt es sich um einen kontinuierlichen Prozess, dessen Strategien und Konzepte ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf fortzuschreiben sind.

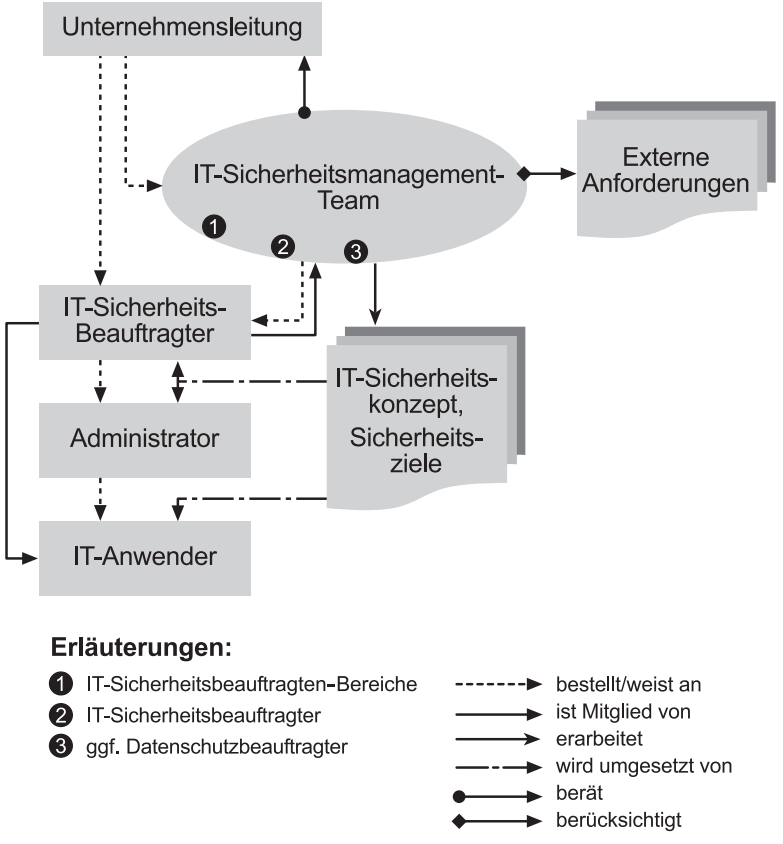


Abbildung 6.2: Aufbau eines Sicherheitsmanagements

Die angestrebte Sicherheitspolitik sowie die angestrebten IT-Sicherheitsziele können nur erreicht werden, wenn das IT-Sicherheitsmanagement organisationsweit umgesetzt wird.

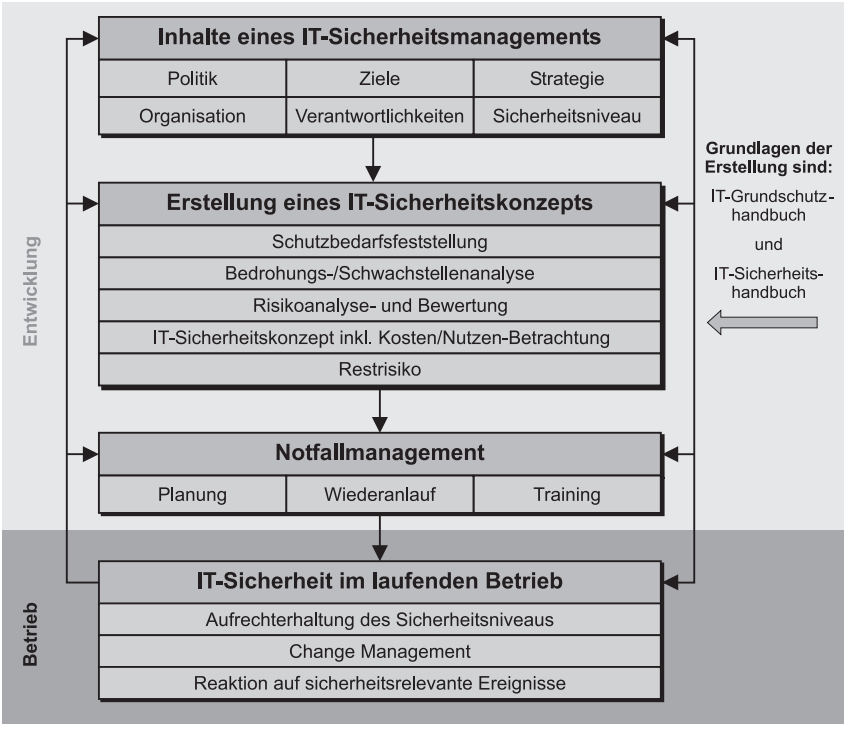


Abbildung 6.3: Aktivitäten Sicherheitsmanagement

Dieser übergreifende Charakter des IT-Sicherheitsmanagements macht es notwendig

- die IT-Sicherheitsmanagementorganisation,
- die Verantwortlichkeiten, und
- die Kommunikationswege

innerhalb der des Unternehmens festzulegen.

Zentrale Aufgaben im IT-Sicherheitsmanagement kommen dabei

- dem IT-Sicherheitsmanagement-Team,
- dem IT-Sicherheitsbeauftragten des Unternehmens,
- bei Bedarf den IT-Sicherheitsbeauftragten der Bereiche,
- bei Bedarf den Datenschutzbeauftragten und
- den Administratoren

zu.

Der Aufbau eines behördenweiten IT-Sicherheitsmanagements ist notwendig, um einen sicheren Betrieb der Informationstechnologie im Unternehmen zu gewährleisten.

6.4.2 IT-Sicherheitsbeauftragter im Unternehmen

Eine Aufgabe des IT-Sicherheitsbeauftragten wird u.a. sein, den Mitarbeitern die Bedeutung bzw. Klassifizierung der Schadenswerte noch eingehender zu vermitteln, um mit jeder Fortschreibung des Sicherheitskonzepts die Qualität der Ergebnisse sicherzustellen.

Zu den Pflichten des Sicherheitsbeauftragten gehören:

- Die verantwortliche Mitwirkung an der Erstellung des IT-Sicherheitskonzepts
- Die Gesamtverantwortung für die Realisierung der ausgewählten Sicherheitsmaßnahmen
- Die Planung und Koordination von Schulungs- und Sensibilisierungsveranstaltungen
- Die Gewährleistung der IT-Sicherheit im laufenden Betrieb
- Die Verwaltung der für IT-Sicherheit zur Verfügung stehenden Ressourcen

6.4.3 Erstellung und Weiterentwicklung eines Sicherheitskonzepts

Ein aufgestelltes unternehmensweites Sicherheitskonzept ist kein statisches, unveränderbares Dokument, sondern muss stets auf seine Wirksamkeit, Aktualität und die Umsetzung in der täglichen Praxis überprüft werden. Insbesondere ist es von Bedeutung, dass die Liste der existierenden bzw. noch umzusetzenden Sicherheitsmaßnahmen stets dem tatsächlichen aktuellen Stand entspricht. Es ist regelmäßig fortzuschreiben aufgrund

- von Veränderungen technischer Rahmenbedingungen,
- von Veränderungen organisatorischer Rahmenbedingungen,
- von Veränderungen von Schadenswerten und/oder Häufigkeiten,
- des Auftretens neuer Bedrohungen,
- des Wegfalls bisheriger Bedrohungen,
- sich dadurch verändernden Risiken und
- der Einführung neuer Applikationen.

Ziel muss es sein, das erreichte Sicherheitsniveau zu erhalten bzw. in den kritischen Punkten zu erhöhen.

Voraussetzungen für eine effiziente und zielgerichtete Fortschreibung des IT-Sicherheitskonzepts sind:

- Die laufende Überprüfung von Akzeptanz und Einhaltung der IT-Sicherheitsmaßnahmen

- Die Protokollierung von Schadensereignissen
- Die Kontrolle der Wirksamkeit und Angemessenheit der Maßnahmen

6.4.4 Regelmäßige Audits der IT-Sicherheitsmaßnahmen

Im IT-Sicherheitsprozess geht es nicht nur darum, das angestrebte IT-Sicherheitsniveau zu erreichen, sondern dieses auch dauerhaft zu gewährleisten. Um die bestehende IT-Sicherheitspolitik aufrechtzuerhalten und fortlaufend zu verbessern, werden alle IT-Sicherheitsmaßnahmen regelmäßig überprüft. Regelmäßig heißt hierbei aber nicht, dass die Audits an vorhersagbaren Terminen stattfinden, da angekündigte Audits meist ein verzerrtes Bild des Untersuchungsgegenstands ergeben.

Audits sind vor allen Dingen darauf ausgerichtet, Mängel abzustellen. Für die Akzeptanz von Audits ist es wichtig, dass dies allen Beteiligten als Ziel der Audits erkennbar ist und dass die Audits nicht den Charakter von »Schulmeisterei« haben. Es ist daher sinnvoll, während einer Kontrolle mit den Beteiligten über mögliche Problemlösungen zu sprechen und entsprechende Abhilfen vorzubereiten.

Die Audits können durch externe oder interne Auditoren durchgeführt werden und sollten, soweit möglich, auf standardisierten Tests und Checklisten basieren. Interne Audits werden durch den IT-Sicherheitsbeauftragten durchgeführt. Dieser legt Anzahl, Häufigkeit und Umfang der Audits in Absprache mit dem IT-Sicherheitsmanagementteam fest.

Im Rahmen der Audits wird festgestellt, ob die IT-Sicherheitsmaßnahmen auf allen Ebenen im laufenden Betrieb umgesetzt werden. Darüber hinaus wird mit den Audits ermittelt, inwieweit die IT-Sicherheitsmaßnahmen bezogen auf die Sicherheitsanforderungen geeignet sind. Zudem wird überprüft, ob die getroffenen Maßnahmen mit den gesetzlichen und betrieblichen Vorgaben übereinstimmen.

Die Ergebnisse werden in einem IT-Sicherheitsreport festgehalten. Dieser sollte auch die vorgeschlagenen Korrekturmaßnahmen aus fachlicher Sicht enthalten.

6.4.5 Sensibilisierung des Sicherheitsbewusstseins bei den Mitarbeitern

Nur durch Verständnis und Motivation ist eine dauerhafte Einhaltung und Umsetzung der Richtlinien und Vorschriften zur IT-Sicherheit zu erreichen. Um das Sicherheitsbewusstsein aller Mitarbeiter zu fördern und den Stellenwert der IT-Sicherheit innerhalb des mittelständischen Unternehmens besonders hervorzuheben, sollte ein umfassendes, organisationsweites Sensibilisierungsprogramm erstellt werden, das zum Ziel hat, IT-Sicherheit zu einem integrierten Bestandteil der täglichen Arbeit zu machen. Dieses Pro-

gramm ist systemübergreifend zu betrachten. Es ist Aufgabe eines dafür Verantwortlichen – im Allgemeinen der IT-Sicherheitsbeauftragte – die Anforderungen aus den einzelnen Teilbereichen und systemspezifische Anforderungen hier einfließen zu lassen und entsprechend zu koordinieren.

Für die Sicherheit des Unternehmens kann eine Reihe von Maßnahmen nicht technisch erzwungen werden, sondern muss sich auf das Mitwirken der Mitarbeiter stützen. Das Sicherheitsbewusstsein der Anwender kann durch entsprechende Schulungen bzw. Informationen sensibilisiert und dadurch auch die Bereitschaft erhöht werden, bestimmte Unbequemlichkeiten in Kauf zu nehmen, die manche Sicherheitsmaßnahme möglicherweise mit sich bringt. Im Rahmen der Ausbildung bzw. der Einführung neuer Mitarbeiter sollte daher unbedingt auch auf das Thema Sicherheit eingegangen werden und der Sinn für potenzielle Bedrohungen geschärft werden, auch wenn sie bisher noch nicht aufgetreten sind.

Gerade in Bereichen, die eigentlich über eine perfekte Zugangskontrolle verfügen, gelingt es immer wieder, dass Unberechtigte sich Zutritt aufgrund von sozialen Verhaltensweisen verschaffen. Die Mitarbeiter mit Zugangsberechtigung zu sensitiven Bereichen sind anzuweisen, sich der Berechtigung von Zutrittswilligen stets zu versichern, insbesondere

- unbekanntes Personal, das über keine entsprechende Zugangsberechtigung verfügt, nicht aus falsch verstandener Kollegialität in diese Bereiche zu lassen,
- nicht aus falsch verstandener Höflichkeit Unbekannten, die über keine entsprechende Zugangsberechtigung verfügen und sich nicht in Begleitung eines berechtigten Mitarbeiters befinden, den Zugang zu ermöglichen.

Es ist die Entwicklung einer Unternehmenskultur anzustreben, in der Sicherheit, insbesondere auch IT-Sicherheit, positiv aufgefasst wird, d.h. als Maßnahme zur langfristigen Sicherung von Arbeitsplätzen und nicht als Behinderung der Arbeit. Nur so ist eine gewisse Kontrolle der Mitarbeiter untereinander zu erreichen, die zur Verhinderung interner Sabotage oder deren Entdeckung beitragen kann. Solche Strategien greifen nur langsam, bilden aber langfristig den wirksamsten Schutz.

Schulung der Mitarbeiter in IT-Sicherheit

Über das allgemeine Sensibilisierungsprogramm hinaus sind Schulungen zu Teilbereichen der IT-Sicherheit erforderlich, wenn sich durch Sicherheitsmaßnahmen einschneidende Veränderungen z.B. im Arbeitsablauf ergeben.

Das Schulungsprogramm ist für das jeweilige Unternehmen spezifisch zu entwickeln. Folgende exemplarische Themen können Inhalt dieses Programmes sein:

- Sicherheitspolitik und -infrastruktur
- Organisation des IT-Sicherheitsmanagements

- Regelmäßige Überprüfung von Sicherheitsmaßnahmen
- Bauliche Sicherheit
- Schutz von Gebäuden, Technikräumen und Büroräumen
- Verantwortlichkeiten der Mitarbeiter
- Hardware- und Softwaresicherheit
- Identifikation und Authentisierung
- Berechtigungssysteme, Virenschutz

6.4.6 Schulung der Mitarbeiter vor Programmnutzung

Durch unsachgemäßen Umgang mit IT-Anwendungen hervorgerufene Schäden können vermieden werden, wenn die Benutzer eingehend – vor Inbetriebnahme – in die IT-Anwendungen eingewiesen werden. Daher ist es unabdingbar, dass die Benutzer vor der Übernahme IT-gestützter Aufgaben ausreichend geschult werden. Dies betrifft sowohl die Nutzung von Standardprogrammpaketen als auch von speziell entwickelten IT-Anwendungen.

Darüber hinaus müssen auch bei umfangreichen Änderungen in einer IT-Anwendung Schulungsmaßnahmen durchgeführt werden.

6.4.7 Internetnutzung

Um die Gefährdungen, die durch Angriffe aus dem Internet auf lokale Daten oder Rechner im LAN (Local Area Network, lokales Netzwerk) entstehen, zu verringern, ist es erforderlich, Rechner einzusetzen, die nur mit dem Internet vernetzt sind und keine weitere Netzverbindung zu dem LAN haben.

Ein unternehmensweites Konzept für die Internetnutzung ist festzulegen.

Bestandteil dieser Regelung sind unter anderem die hard- und softwaretechnische Ausstattung des Arbeitsplatzes, eine Benutzerrichtlinie und das Virenschutzkonzept.

6.4.8 Festlegung der Sicherheitspolitik für E-Mail-Nutzung

Vor der Freigabe von E-Mail-Systemen muss festgelegt werden für welchen Einsatz E-Mail vorgesehen ist.

Das Unternehmen muss eine Sicherheitspolitik für den E-Mail-Dienst festlegen, in der folgende Punkte beschrieben sind:

- Wer einen E-Mail-Anschluss erhält
- Die Regelungen, die von den Mail-Administratoren und den E-Mail-Benutzern zu beachten sind

- Bis zu welchem Vertraulichkeits- bzw. Integritätsanspruch Informationen per E-Mail versandt werden dürfen
- Ob und unter welchen Rahmenbedingungen eine private Nutzung von E-Mail erlaubt ist
- Wie die Benutzer geschult werden
- Wie jederzeit technische Hilfestellung für die Benutzer gewährleistet wird

E-Mails die intern versandt werden, dürfen das interne Netz nicht verlassen. Eine Übertragung von E-Mails über das Internet, deren Inhalt einen vertraulichen Charakter haben, sollten nicht ohne Verschlüsselung und digitale Signatur versendet werden.

6.5 Fazit

In einem hochkomplexen System wirken viele Bedrohungen auf die unterschiedlichsten Komponenten ein. Gegen diese Bedrohungen müssen Schutz- und Gegenmaßnahmen aktiviert und gepflegt werden. Um einen hohen Grad an Sicherheit zu erhalten, ist eine weitere Sensibilisierung nicht nur der Mitarbeiter sondern auch in den Managementebenen der Unternehmen zu etablieren. Es muss die Aufgabe der Unternehmensführung sein, einen kontinuierlichen Sicherheitsprozess im gesamten Geschäftsbereich zu installieren und ständig weiterzuentwickeln.

Dazu muss auch die Einsicht vorhanden sein, dass dieser Prozess mit Hilfe von externen Dienstleistern und der verstärkten Einbindung eigener Kräfte vorangetrieben werden kann.

Es ist auch zu berücksichtigen, dass wegen unzureichender Maßnahmen im Bereich Organisation und Personal Vorkehrungen im technischen Bereich weitgehend sinnlos werden können.

7 Kryptografie: Entwicklung, Methoden und Sicherheit

Daniel Wirth

7.1 Einleitung

Was haben Julius Cäsar, Maria Stuart und die deutsche U-Boot-Flotte des zweiten Weltkrieges mit moderner Informations- und Kommunikationstechnologie gemeinsam? Die Antwort ist einfach: die Kryptografie.

Ohne uns Gedanken über die tatsächliche Sicherheit zu machen, verwenden und vertrauen wir täglich kryptografischen Anwendungen. Bei der Verwendung von EC-Karten genauso wie bei der Nutzung eines Mobiltelefons basieren die grundlegenden Technologien auf Verschlüsselungsmethoden, deren Sicherheit wir einfach als gegeben voraussetzen.

Um die heute verwendeten Verfahren und die daraus entstehenden Probleme zu verstehen, muss zunächst die historische Entwicklung betrachtet werden, die zur modernen Kryptografie führte. Schon seit Jahrtausenden senden Herrscher verschlüsselte Nachrichten an ihre Heerführer in der trügerischen Gewissheit, dass der Inhalt einer abgefangenen Botschaft dem Gegner verschlossen bliebe. Häufig richtete jedoch genau dieses blinde Vertrauen in die Sicherheit der Kryptografie großen Schaden an, da dadurch manchmal dem sicheren Transport der Nachricht nicht genügend Sorgsamkeit zukam.

In der Vergangenheit, genauso wie heute, entwickeln Kryptologen immer neue und bessere Algorithmen und Verschlüsselungsmethoden, während Kryptoanalytiker im Gegensatz dazu versuchen, den Klartext ohne Kenntnis des Schlüssels zu rekonstruieren. Heute werden sensible Daten durch aufwändige kryptografische Verfahren geschützt, deren tatsächlicher Schutz auf mathematischen Annahmen beruht. Wie wir sehen werden, gibt es jedoch keinen Beweis für die Sicherheit der meistgebrauchten Algorithmen.

Wie sicher kann sich demnach der Benutzer moderner Verfahren hinsichtlich der Integrität, Vertraulichkeit und Verfügbarkeit seiner verschlüsselten Daten sein?

Um diese Frage zu beantworten, betrachten wir zunächst die historische Entwicklung der Kryptografie und schildern die wichtigsten Verschlüsselungsverfahren. Die dabei auftretenden Probleme sind im Wesentlichen dieselben, die bei modernen Methoden zum Erfolg der Kryptoanalyse führen und damit die Sicherheit der Kryptografie beeinträchtigen.

7.2 Monoalphabetische Verschlüsselung

Der Chiffre des Julius Cäsar

Der römische Kaiser Julius Cäsar gilt als der Erfinder und ist der Namensgeber eines sehr einfachen Verfahrens, der Cäsar-Verschlüsselung.

Julius Cäsar (100 v. Chr. bis 44 v. Chr.) bediente sich eines einfachen Verfahrens zur Verschlüsselung der Botschaften an seine Kriegsherren. Er vertauschte die Buchstaben seiner Nachricht und schuf damit eine ganze Gattung von Chiffren. Sie sind heute nach ihm benannt: die sogenannten Cäsaren. Ein Cäsar ist eine Verschlüsselung, in der jeder Buchstabe durch ein anderes Zeichen aus einem einzelnen Ersatzalphabet ausgetauscht wird. Jeder Buchstabe erhält dabei jedes Mal die gleiche Ersetzung. Man spricht deshalb von monoalphabetischen Verschlüsselungen.

Der römische Kaiser verwendete die einfachste Variante, die sogenannte Verschiebung oder Rotation. Jeder Buchstabe wird durch sein Pendant ersetzt, das um n Stellen versetzt im Alphabet steht (im Folgenden bezeichnen wir dies mit Rot-n).

Tab. 7.1: Beispiel: die Cäsar-Verschiebung

Original-alphabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Geheim-alphabet Rot-3	D E F G H I J K L M N O P Q R S T U V W X Z Y A B C

Im folgenden Beispiel verschlüsseln wir eine einfache Nachricht mit diesem Verfahren. Wie wir sehen, können wir auf den ersten Blick nur schwerlich auf den Inhalt der Nachricht schließen.

Tab. 7.2: Beispiel für eine verschlüsselte Nachricht

Klartext	D I E S I S T E I N G E H E I M T E X T
Geheimtext	G L H V L V U H L Q J H K H L P X H A X

Mit roher Gewalt: »Brute Force«

Die Kryptoanalyse einer Cäsar-Verschiebung ist jedoch vergleichsweise einfach. Da unser Alphabet aus nur 26 Buchstaben besteht, existieren auch nur 26 Möglichkeiten, das Verfahren anzuwenden. Man spricht von 26 möglichen Schlüsseln.

Es ist ein einfaches Unterfangen, alle 26 Schlüssel der Reihe nach durchzuprobieren und so den Text zu entschlüsseln. Bei einer ausreichenden Länge des Geheimtextes führt nur ein Schlüssel zu einem sinnvollen Ergebnis.

Diese Methode der Kryptoanalyse wird auch als »Brute-Force« (engl. »mit roher Gewalt«) bezeichnet, da blind jeder mögliche Schlüssel getestet wird, ohne weitere Schwächen des Verschlüsselungsverfahrens auszunutzen.

Um die Kryptoanalyse zu erschweren, wurde das Verschlüsselungsverfahren verbessert, indem statt der Verschiebung um *n* Zeichen, eine Permutation (willkürliche Vertauschung) des Alphabets verwendet wird: der Buchstaben-Cäsar. So erhält man auf ebenfalls einfache Weise eine weit größere Zahl von Schlüsseln.

Original-alphabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Geheim-alphabet	G U E N F K S B L M Q Y A T C W P X D Z J V I O R H

Tab. 7.3: Beispiel: ein Buchstaben-Cäsar

Klartext	D I E S I S T E I N G E H E I M T E X T
Geheim-text	N L F D L D Z F L T S F B F L A Z F O Z

Tab. 7.4: Beispiel für eine verschlüsselte Nachricht

Die Anzahl der Schlüssel lässt sich leicht berechnen. Für den ersten Buchstaben des Alphabets bestehen 26 Möglichkeiten der Ersetzung. Für den zweiten bleiben nach der Festlegung des ersten noch 25, für den dritten 24, und so weiter. Die Anzahl der Schlüssel beträgt so immerhin:

$$26 \text{ x } 25 \text{ x } 24\text{x } ...\text{x } 3 \text{ x } 2 \text{ x } 1 = 26! \sim 4 \text{ x } 10^{26}$$

$$\sim 400\,000\,000\,000\,000\,000\,000\,000\,000$$

Es liegt auf der Hand, dass so viele Möglichkeiten nicht mehr auf einfache Weise getestet werden können. Selbst mit der Unterstützung moderner Computersysteme würden wir mit der Brute-Force-Methode $1\text{x}10^{13}$ Jahre benötigen, das ist etwa 13.000 Mal länger als das Alter unseres Universums. Dabei sei angenommen, dass ein leistungsfähiger moderner Computer eine Million Schlüssel pro Sekunde testen kann.

Die Häufigkeitsanalyse

Dennoch stellt der Buchstaben-Cäsar keinen wirksamen Schutz dar, da auch die Kryptoanalyse Fortschritte machte und schnell eine Lösung fand, die Häufigkeitsanalyse. In jeder Sprache tauchen die verwendeten Laute in unterschiedlicher Häufigkeit auf. In der folgenden Tabelle sind die Häufigkeiten der einzelnen Buchstaben dieses Artikels aufgeführt, natürlich ohne die enthaltenen Tabellen:

Tab. 7.5: Häufigkeit der vorkommenden Buchstaben

A	B	C	D	E	F	G	H	I	J
5,5%	1,8%	3,3%	5,1%	18,2%	1,6%	2,6%	4,4%	7,8%	0,18%
K	L	M	N	O	P	Q	R	S	T
1,2%	4,0%	2,4%	9,4%	2,6%	1,1%	0,06%	7,3%	7,0%	6,1%
		U	V	W	X	Y	Z		
		4,3%	1,0%	1,6%	0,15%	0,27%	1,1%		

Der Tabelle ist mit Leichtigkeit zu entnehmen, dass der meistverwendete Buchstabe das »E« ist, gefolgt von »N«, »I«, »R«, »S« »T« und »A«. Bei einer längeren verschlüsselten Botschaft ist zu erwarten, dass die Häufigkeitsverteilung der Tabelle ähnlich ist. Dies ist der Hinweis, der zur erfolgreichen Kryptoanalyse führt. Taucht im Geheimtext z.B. das »N« am zahlreichsten auf, so entspricht er höchstwahrscheinlich dem »E« im Klartext. Die oben genannte Gruppe der zweitwichtigsten Buchstaben lässt sich zwar nicht sofort dem Klartextbuchstaben zuordnen. Dennoch gelingt es nach kurzer Zeit, Teile der verschlüsselten Botschaft zu erkennen und daraus auf die noch fehlenden Buchstaben zu schließen. Ist dazu die Häufigkeitsverteilung der einzelnen Buchstaben nicht ausreichend, so können ebenfalls die so genannten Bigramme, d.h. Paare aufeinanderfolgender Buchstaben analysiert werden. Die wichtigsten deutschen Bigramme sind:

Tab. 7.6: Die wichtigsten Bigramme

EN	ER	CH	TE	DE	ND	EI	IE	IN	ES
3,9%	3,8%	2,8%	2,3%	2,0%	2,0%	1,9%	1,8%	1,7%	1,5%

Das Schicksal Maria Stuarts

Die entscheidende Schwäche der monoalphabetischen Verschlüsselung wurde auch der schottischen Königin Maria Stuart (1542 bis 1588) zum Verhängnis. Nachdem sie gestürzt wurde, wurde Maria Stuart von der englischen Königin und Halbschwester Marias, Elisabeth I. unter Hausarrest gestellt. 1586, nachdem sie 18 Jahre in ihrem Gefängnis verbracht hatte, planten Marias Anhänger unter Anführung ihres Pagen Anthony Babingtons die Ermordung Elisabeths und die Wiedereinsetzung der Schottin als Regentin.

Doch der Minister Francis Walsingham setzte einen Spion ein, der das Vertrauen der Gefangenen gewann und zum Boten zwischen Maria und Babington wurde. Das Komplott wurde enttarnt und Maria wurde infolge dieser Verschwörung des Hochverrats angeklagt. Die Vertreter der Anklage verwendeten den Schriftverkehr zwischen Maria Stuart und ihren Anhängern als Hauptbeweis. Die Nachrichten waren zwar verschlüsselt, jedoch nur mit einer monoalphabetischen Methode. Im Vergleich zum Buchstaben-Cäsar hatten die Verschwörer das Alphabet zwar um ein paar Eigenschaften erweitert, die das Brechen des Codes erschweren sollten, doch hatten sie nicht mit der Genialität des Kryptoanalytikers Thomas Phelippes gerechnet.

Dieser beherrschte die oben beschriebene Häufigkeitsanalyse nahezu in Perfektion. Es war ihm ein Leichtes, dem Gericht die entschlüsselten Botschaften vorzulegen.

Das Resultat der schwachen Verschlüsselung ist gemeinhin bekannt. Maria Stuart wurde zum Tode verurteilt und am 8. Februar 1588 hingerichtet.

7.3 Polyalphabetische Verschlüsselung

Die Vigenère-Chiffre

Eine Möglichkeit, der entscheidenden Schwäche der monoalphabetischen Chiffre zu begegnen, ist die Verwendung eines unterschiedlichen Alphabets für jedes zu verschlüsselnde Zeichen. Der französische Diplomat Blaise de Vigenère entwickelte im 16. Jahrhundert das nach ihm benannte Verfahren.

Bei der Vigenère-Verschlüsselung werden 26 verschiedene Alphabete verwendet. Diese werden in Form einer Cäsar-Verschiebung gegeneinander um je eine Stelle verschoben und untereinander in eine Tabelle, dem so genannten Vigenère-Quadrat eingetragen:

Klartext	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Rot-1	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
Rot-2	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
Rot-3	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
…	
Rot-25	Z A B C D E F G H I J K L M N O P Q R S T U V V X Y
Rot-26	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Tab. 7.7: Auszug aus dem Vigenère-Quadrat

Für jedes Zeichen des zu verschlüsselnden Geheimtextes wird eine andere Zeile des Quadrats verwendet, wobei die Reihenfolge der zu verwendenden Zeilen durch ein Codewort bestimmt wird. Das Codewort ist der Schlüssel der Chiffre, es muss Sender und Empfänger bekannt sein.

Codewort: CAESAR

Die in der Tabelle enthaltenen Alphabete werden in der Reihenfolge verwendet, in der ihr jeweils erster Buchstabe im Codewort vorkommt. Ist die Nachricht länger als das Codewort, so wird es einfach wiederholt:

Tab. 7.8: Beispiel für eine verschlüsselte Nachricht:

Klartext	N	A	C	H	R	I	C	H	T
Schlüssel	C	A	E	S	A	R	C	A	E
Geheimtext	P	A	G	Z	R	Z	E	H	L

Der erste Buchstabe des Klartextes »N« wird mit dem ersten Buchstaben des Schlüssels »C« chiffriert, das heißt, es wird die zweite Zeile »Rot-2« verwendet. »N« wird demnach durch ein »P« ersetzt. Die Verschlüsselung des zweiten Zeichens »A« erfolgt mit dem »A« des Schlüssels. Das Ergebnis ist ebenfalls ein »A«, d.h. der Buchstabe wird durch sich selbst ersetzt. Dies ist eine wichtige Eigenschaft dieser Methode, da auch der Ausschluss eines Zeichens einen wichtigen Hinweis für die Kryptoanalyse liefert.

Um die Vorgehensweise klarer zu erläutern, werden die Chiffriervorgänge der ersten fünf Zeichen und die dafür verwendeten Alphabete in dem folgenden Vigenère- Quadrat deutlich gemacht.

Tab. 7.9: Das vollständige Vigenère-Quadrat

Klartext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rot-1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
Rot-2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
Rot-3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
Rot-4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
Rot-5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
Rot-6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
Rot-7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
Rot-8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
Rot-9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
Rot-10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
Rot-11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
Rot-12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L

Rot-13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Rot-14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Rot-15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Rot-16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Rot-17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Rot-18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Rot-19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Rot-20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
Rot-21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
Rot-22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Rot-23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Rot-24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	V	X
Rot-25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	V	X	Y
Rot-26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Sicherheitsproblem: die Schlüssellänge

Diese Methode erscheint im Vergleich zur monoalphabetischen Verschlüsselung sicher. In der Tat wurde erst im 19. Jahrhundert ein erfolgreiches kryptoanalytisches Verfahren entwickelt.

Das verwendete Codewort ist kurz und seine Wiederholung gibt den entscheidenden Hinweis zur Dechiffrierung, da dadurch auch in dem verschlüsselten Text Wiederholungen auftreten. So gibt es in unserem Beispiel mit einem sechsstelligen Codewort auch nur sechs Möglichkeiten, um ein Wort zu verschlüsseln. Ist der Geheimtext ausreichend lang, so werden häufige Worte mit Sicherheit wiederholt und etwa jedes sechste ist identisch verschlüsselt.

Wie wir schon an diesem Beispiel erkennen, ist die Länge des verwendeten Schlüssels ein kritischer Faktor der Kryptografie.

Leicht kann man aus dem kurzen Codewort einen längeren Schlüssel erhalten. Dazu wird jeder Buchstabe des Codeworts nur ein einziges Mal verwendet und der Rest des Alphabetes wird angehängt.

Der Schlüssel: CAESRBDFGHIJKLMNOPQTUVWXYZ

Doch leider ist auch dieser immerhin mehr als fünfmal längere Schlüssel auch nicht ausreichend. Wird ein längerer Test damit chiffriert, so treten hier dieselben Wiederholungen auf wie bei dem kürzeren Codewort. Die Analyse dauert nur ein wenig länger.

7.4 One Time Pad – die sicherste Verschlüsselung

Wenn wir die Idee des vorausgegangenen Abschnitts jedoch weiter reifen lassen und uns einen Schlüssel vorstellen, der dieselbe Länge wie der Klartext aufweist, so scheitern auch alle bislang geschilderten Methoden der Kryptoanalyse und der Text kann ohne die Kenntnis der Schlüssels nicht dechiffriert werden.

Mit einer ausreichenden Schlüssellänge ist eine Chiffre also sicher. Dennoch stellt sich das Problem, dass sowohl Sender als auch Empfänger denselben Schlüssel kennen und verwenden müssen. Es bietet sich daher an, denselben, sehr langen Schlüssel immer wieder zu verwenden. Wir müssen aber davon ausgehen, dass ein Kryptoanalytiker zur Kenntnis mehrerer verschlüsselter Botschaften gelangen könnte. Dann reduziert sich das Problem wieder auf das gleiche wie bei einem zu kurzen Schlüssel.

Die Lösung dazu ist theoretisch sehr simpel: Es wird jeder Schlüssel nur ein einziges Mal verwendet und danach vernichtet. Das Verfahren ist natürlich nur dann sicher, wenn die einzelnen Schlüssel keinerlei Ähnlichkeit haben, also zufällig erzeugt wurden. Sender und Empfänger müssen einen identischen Satz von Schlüsseln vorhalten. Dazu kann man die Vorstellung entwickeln, die Schlüsselsätze befänden sich auf einem Block und es wird nach jedem Chiffriervorgang eine Seite abgerissen und vernichtet. Diese Methode der Verschlüsselung bezeichnet man als »One Time Pad«, nach der englischen Bezeichnung für einen Schreibblock.

Tatsächlich kann mathematisch bewiesen werden, dass ein auf dem Zufall basierender One-Time-Pad nicht zu brechen ist. Der One-Time-Pad ist damit das einzig bekannte Verschlüsselungsverfahren mit mathematisch bewiesener Sicherheit. In der Praxis ist der Aufwand für einen One-Time-Pad jedoch aufgrund der aufwändigen Schlüsselverteilung sehr hoch, deshalb fand er selten Verwendung.

7.5 Enigma – mechanische Verschlüsselungsmaschine

Die Enigma war die wohl bekannteste Entwicklung der polyalphabetischen Verschlüsselung. Sie bedeutete deren mechanische Automatisierung. Zwar waren schon zuvor, vor allem in Kriegen, Chiffrierscheiben verwendet worden, diese basierten jedoch alle auf monoalphabetischen Verfahren und waren entsprechend unsicher.

Die Enigma basierte je nach Version auf drei oder vier Walzen, die jeweils eine Permutation der Zeichen vornahmen. Da die Walzen wie ein Zählwerk nach jedem Buchstaben die Anordnung änderten, änderte sich auch der Algorithmus für jedes chiffrierte Zeichen. Damit waren bei der dreistufigen Maschine erst *nach 26 x 26 x 26 = 17.576* Zeichen Wiederholungen zu erkennen. Da die Anfangsstellung der Walzen frei gewählt werden konnte, ergaben sich nochmals so viele Möglichkeiten, die Verschlüsselung zu beginnen.

Weiterhin konnten die Walzen ver- und gegen andere ausgetauscht werden. Üblich war zum Beispiel ein Satz von fünf Walzen, von denen je drei verwendet wurden. Damit erhöht sich die Möglichkeiten, die Maschine zu konfigurieren um den Faktor 60.

Jedes zu chiffrierende Zeichen durchlief die Maschine zweimal, einmal vorwärts und auf einem anderen Weg zurück. Dabei konnte ein Zeichen jedoch nicht mit sich selbst verschlüsselt werden. Diese Tatsache lieferte den Kryptoanalytikern einen wichtigen Hinweis zum Ausschluss falscher Lösungsansätze. Blieb bei einem Dechiffrierversuch im entschlüsselten Text ein Zeichen gleich, so war die grundlegende Vermutung falsch.

Diese Schwäche war es jedoch nicht, die schließlich zur Kompromittierung der Enigma führte, sondern die uhrwerkgleiche Periodizität ihrer Bewegungen. Der polnische Mathematiker Marian Rejeweski entdeckte bei seiner Analyse von deutschen Funksprüchen eine Regelmäßigkeit. Da die Deutschen gemäß ihrer Anweisung zu Beginn jeder Botschaft einen sogenannten Tagesschlüssel zweimal hintereinander übermittelten, konnte Rejewski daraus schließen, wie derselbe Buchstabe bei wiederholter Anwendung der Enigma verschlüsselt wurde. Er entdeckte, dass nach einer endlichen Anzahl von Wiederholungen wieder der ursprüngliche Buchstabe ausgegeben wurde.

Durch diese Vorarbeit gelang es dem britischen Aufklärungsdienst schließlich, die Chiffre automatisiert zu brechen. Die Briten hatten in Bletchley Park eine Gruppe Wissenschaftler zusammengerufen, um der Enigma-Verschlüsselung auf die Schliche zu kommen. In diesem Umfeld hatte der geniale britische Mathematiker Alan Touring die Idee, mit einer Maschine die möglichen Einstellungen der Enigma automatisiert durchzuprobieren.

Das Problem daran war, dass der deutsche Code täglich gewechselt wurde und somit wenig Zeit blieb, die vielen verschiedenen Möglichkeiten durchzutesten. Es wurden Maschinen entwickelt, in denen dem Prinzip nach viele

Enigmen in Parallelarbeit alle Möglichkeiten ausprobierten. Nach ihrem Äußeren »Bomben« genannt, verketteten sie mehrere Enigmen, um gemäß der polnischen Entdeckung den Prozess automatisch zu beenden, wenn der richtige Code gefunden war. Voraussetzung für den automatischen Ablauf war jedoch, dass jeden Tag ein neuer Hinweis auf den Inhalt der Nachrichten bekannt war. Die Deutschen machten es den Kryptoanalytikern dabei leicht, sie übermittelten täglich zur gleichen Zeit eine Wettermeldung.

Die erfolgreiche Entschlüsselung der Enigma hielt die britische Regierung noch Jahre über das Ende des zweiten Weltkrieges hinweg geheim. Die britischen Kryptoanalytiker in Bletchley Park verwendeten im Übrigen den One-Time-Pad, um die entschlüsselten Botschaften der Enigma-Maschine an ihre Regierung zu übermitteln. Der sensible Charakter der Daten rechtfertigte den großen Aufwand. Hätten die deutsche Militärs gewusst, das ihre Nachrichten nicht mehr sicher sind, so wäre die wichtigste Informationsquelle der Briten wohl schnell versiegt.

Da die deutsche Marine sich aber der Maschine vollkommen sicher war, übermittelte sie während gesamten zweiten Weltkrieges die Positionen ihrer U-Boote an die Alliierten. Als Resultat der Entschlüsselung kamen über 100.000 deutsche U-Boot-Fahrer im zweiten Weltkrieg ums Leben.

7.6 Der Siegeszug der digitalen Verschlüsselung

Die Enigma war nicht die einzige polyalphabetische Verschlüsselungsmaschine. Im zweiten Weltkrieg verwendeten die alliierten Streitkräfte ebenfalls verschiedene mechanische Verschlüsselungsautomaten. Alle Entwicklungen hatten jedoch prinzipbedingt ähnliche Schwächen wie die Enigma. Sie basierten auf einer Verkettung monoalphabetischer Verschlüsselungen, die in zyklischen Verfahren wiederholt wurden. Des Weiteren waren sie langsam und unhandlich. Erst mit der Entwicklung der Mikroelektronik und der elektronischen Rechenmaschine begann der nächste Abschnitt der Kryptografie.

7.7 Grundlagen der binären Verschlüsselung

Binärdarstellung

Nach dem zweiten Weltkrieg begann die Entwicklung der Computer. Computer können unsere Sprache oder unser Zahlensystem nicht direkt verarbeiten. Sie arbeiten prinzipiell mit zwei verschiedenen Spannungszuständen, die 1 oder 0 bedeuten. Diese minimale Informationseinheit nennt man ein Bit (engl. Abk. für »Binary Digit«). Zahlen und Buchstaben müssen durch sie ausgedrückt werden.

Eine binäre Darstellung unseres Alphabets für die Übertragung von Nachrichten ist unproblematisch und wurde schon weit früher entwickelt. Samuel Finley Morse entwickelte eine binäre Codierung für die Verwendung in Telegraphen. Dabei berücksichtigte er ebenfalls die Häufigkeitsverteilung der einzelnen Buchstaben. Er verwendete für die meistgebrauchten Buchstaben die kürzesten und einfachsten Codes (vgl. Häufigkeitsanalyse):

A	B	C	D	E	F	G	H	I	J	K	L	M
•–	–•••	–•–•	–••	•	••–•	––•	••••	••	•–––	–•–	•–••	–
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
–•	–––	•––•	––•–	•–•	•••	–	••–	•••–	•––	–••–	–•––	––••

Tab. 7.10: Binäre Darstellung des Alphabets

Mit einem Binäralphabet können jedoch auch beliebig andere Informationen ausgedrückt werden. Der Einfachheit halber verwenden wir jedoch nicht das Morse-Alphabet, sondern entwickeln eine eigene Binärdarstellung unseres Alphabets. Dazu nummerieren wir die Buchstaben der Reihe nach durch und übersetzen jede Zahl in eine Binärdarstellung. In der Binärdarstellung werden die Zahlen in Potenzen der Zahl zwei ausgedrückt.

Beispiel: Die Zahl 26 mit der Binärdarstellung 11010:

$$\underline{\mathbf{1}} \times 2^4 + \underline{\mathbf{1}} \times 2^3 + \underline{\mathbf{0}} \times 2^2 + \underline{\mathbf{1}} \times 2^1 + \underline{\mathbf{0}} \times 2^0 = 16 + 8 + 0 + 2 + 0 = 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
00000	00001	00010	00011	00100	00101	00110	00111	01000	01001	01010	01011	01100
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
01101	01110	01111	10000	10001	10010	10011	10100	10101	10110	10111	11000	11001

Tab. 7.11: Beispielhafte eigene Binärdarstellung unseres Alphabets

In der Praxis wird eine andere Kodierung für das Alphabet verwendet. Der übliche Standard ist der ASCII (American Standard Code for Information Interchange), der insgesamt 256 Zeichen binär darstellt.

Wir übertragen heute jedoch nicht nur Texte in elektronischer Form, sondern zum Beispiel auch Bilder oder Dateien. Die Grundlage dafür schuf Claude Elwood Shannon 1948 in seiner Veröffentlichung »A Mathematical Theory of Communication« im Bell System Technical Journal. Er beschreibt darin, wie beliebige Daten in elektronischer Form übermittelt werden können, indem sie in eine Reihe von 0 und 1 übersetzt werden.

Binärer One-Time Pad

Mit der fortschreitenden Verbreitung der Computer in der Industrie entstand der Bedarf einer Methode für die elektronische Verschlüsselung von Daten. In der Binärdarstellung lassen sich mit Computern sehr einfach Verschlüsselungen durchführen. Zum Beispiel verschlüsseln wir einen Klartext mit einem binären One Time Pad und der so genannten XOR -Verknüpfung. Diese Operation mit zwei Eingangsparametern ergibt den Wert eins, wenn die Werte verschieden sind und null, wenn sie gleich sind. Die Funktion ist gleichzeitig ihre eigene Umkehrfunktion; das bedeutet, sie wird identisch auch zum Entschlüsseln verwendet.

Tab. 7.12: Beispiel: XOR-Verknüpfung von binären Werten a und b

a	0	0	1	1
b	0	1	0	1
XOR (a,b)	0	1	1	0

Mit dieser Verknüpfung und einer beliebig langen zufälligen Binärzahl (dem One-Time Pad), kann ein Geheimtext verschlüsselt werden:

Tab. 7.13: Beispiel: Verschlüsselung mit einem binären One Time Pad

Klartext	G	E	H	E	I	M	N	I	S
Binärdarstellung a	00110	00100	00111	00100	01000	01100	01101	01000	10010
Schlüssel b	10010	01110	10010	10101	10100	10101	10101	01010	10110
Geheimtext XOR(a,b)	10100	01010	10101	10001	11100	11001	11000	00010	00100

So haben wir eine einfache Möglichkeit geschaffen, einen One-Time-Pad mit einem Computer zu verwenden. 1919 wurde dem Angestellten einer amerikanischen Telegrafiegesellschaft Gilbert S. Vernam ein Patent für den binären One Time Pad erteilt. Sein kommerzieller Erfolg scheiterte jedoch am zentralen Hauptproblem der Methode: der Schlüsselverteilung. Die benötigte große Zahl von Schlüsseln musste immer noch allen Kommunikationspartnern auf sicherem Wege überbracht werden.

7.7.1 Der DES – unsichere Grundlage heutiger Kommunikation

Entwicklung des Data Encryption Standard (DES)

Die US-amerikanische Behörde NBS (National Bureau of Standards, heute NIST – National Institute of Standards and Technology) begann 1972 ein Programm zur Festlegung eines Standards für die digitale Verschlüsselung. Das Ziel ist klar: es sollte Unternehmen und Behörden ermöglicht werden,

auf Basis eines gemeinsamen Verschlüsselungsprotokolls Daten und Applikationen auszutauschen. Als die Behörde 1973 zur Einreichung von Vorschlägen aufrief, stellte sie folgende Anforderungen:

- Der Algorithmus muss hohen Sicherheitsanforderungen genügen
- Vollständige Veröffentlichung des Algorithmus
- Der Algorithmus muss einfach zu verstehen sein
- Die Sicherheit muss durch den Schlüssel allein zustande kommen, nicht durch die Vertraulichkeit des Algorithmus
- Der Algorithmus muss allen Benutzern lizenzfrei zu Verfügung gestellt werden
- Der Algorithmus muss vielseitig in verschiedenen Anwendungen eingesetzt werden können
- Der Algorithmus muss ohne hohe Kosten in elektronischen Gerätschaften implementiert werden können
- Der Algorithmus muss effizient sein
- Der Algorithmus muss verifizierbar sein
- Der Algorithmus muss exportierbar sein.

Dem ersten Aufruf folgten keine ausreichenden Vorschläge, so wurde der Aufruf ein Jahr später wiederholt.

IBM reichte daraufhin den Algorithmus »Lucifer« ein, der zu Beginn der siebziger Jahre unter der Leitung des deutschstämmigen Mathematikers Horst Feistel entwickelt wurde. Die Funktionsweise soll hier nicht im Detail beschrieben werden, da sie sehr technisch ist und zum Verständnis der Problematik kaum beiträgt.

Der Algorithmus basiert auf einem 128-Bit-Schlüssel. Das entspricht $2^{128} \sim$ 300 000 000 000 000 000 000 000 000 000 000 000 000 Möglichkeiten. Prinzipiell arbeitet Lucifer ähnlich wie sein mechanischer Vorgänger Enigma, nur dass in diesem Verfahren Bits und nicht Buchstaben in sechzehnmaliger Wiederholung in komplizierter Weise durcheinandergewirbelt werden. Dazu wird der Klartext in einzelne Blöcke unterteilt, auf die das Verfahren angewendet wird. Man spricht deshalb von einem »Block Cipher«.

Lucifer erfüllte alle Anforderungen und war ein geeigneter Kandidat für den neuen Standard. Unter dem Einfluss des US-Geheimdienstes NSA (National Security Agency) wurde die Schlüssellänge auf 56 Bit reduziert und am 23. November 1976 bundesweiter Standard (FIPS PUB 46) der USA und für die Verschlüsselung nichtgeheimer Regierungskommunikation freigegeben. Der Hintergrund der Beschränkung auf 56 Bit wurde erst im letzen Jahrzehnt klarer: diese Schlüssellänge erschien dem Geheimdienst als ausreichend sicher für zivile Anwendungen, da nichtmilitärische Organisationen nicht über ausreichende Rechenleistung verfügen würden, um den

Schlüssel zu brechen. Die NSA selbst jedoch verfügt über die leistungsfähigsten Rechner der Welt und wäre gerade noch in der Lage, die DES- chiffrierten Botschaften zu entschlüsseln. Trotz aller Zweifel, die diese Abschwächung bei den Experten hervorrief, wurde der Algorithmus 1983, 1988, 1993 und 1998 erneut durch die Behörde zertifiziert.

DES wird bezwungen

In den letzten Jahren kommen immer mehr Zweifel an der Sicherheit von DES auf. Insbesondere der israelische Mathematikprofessor Adi Shamir bewies Hartnäckigkeit im Versuch, den DES- Algorithmus zu knacken. Shamir ist einer der Gründer der Firma RSA-Security, die bis 2000 die Patente an konkurrierenden Algorithmen hielt.

1991 veröffentlichte er die Ergebnisse jahrelanger Kryptoanalyse. Das Ergebnis wies zwar eine minimale mathematische Schwäche auf, diese ist aber eher theoretischer Natur und in der Praxis nicht ausnutzbar.

Doch mit dem raschen Fortschritt der Mikroelektronik war die erfolgreiche Kryptoanalyse des Standardalgorithmus nicht mehr aufzuhalten. Die Firma RSA Security veranstaltete mehrere Wettbewerbe zur »Brute-Force«-Entschlüsselung von DES. Wie bei der Cäsar-Verschiebung dargestellt, werden der Reihe nach alle möglichen Schlüssel ausprobiert. Da es sich immerhin um $2^{56} \sim 70\,000\,000\,000\,000\,000$ Möglichkeiten handelt, ist der Rechenaufwand immens und nur sehr aufwändige Systeme konnten die notwendige Leistung erbringen.

Tab. 7.14: Wettbewerbe zur »Brute-Force«-Entschlüsselung

Wettbewerb	Durchführung	Zeitaufwand
RSA DES Challenge I	Erfolgreich gelöst im Zeitraum vom 13.03.1997 bis zum 17.06.1997 durch die Internet-Gemeinde »DESCHAL« unter Leitung von Rocke Verser aus Loveland CO, USA.	97 Tage
RSA DES Challenge II – a	Ausgeschrieben am 13.01.1998. Gelöst durch die Internet Gemeinde Distributed.net. (http://www.distributed.net).	39 Tage
RSA DES Challenge II – b	Ausgeschrieben am 13.07.1998. Gelöst durch die Electronic Frontier Foundation mit Hilfe der speziell für diesen Einsatz entwickelten Hardwarelösung »Deep Crack«. Die Kosten für die Hardware blieben unter 250.000 USD.	3 Tage
RSA DES Challenge III	Ausgeschrieben am 12. Dezember 1998. Gelöst durch Distributed.net in Kooperation mit der Electronic Frontier Foundation.	< 1 Tag (22 Stunden, 15 Minuten)

Diese drei Wettbewerbe wurden ausgeschrieben und erfolgreich beendet. Die Ergebnisse zeigen, dass eine Entschlüsselung von DES mit der Brute-Force Methode heutige Hardware nicht länger vor unlösbare Probleme stellt. Zwar verwenden die beteiligten Internetgemeinden die ungenutzte Prozessorleistung von bis 100.000 PCs und die speziell angepasste Maschine Deep Crack, doch wenn man die Leistung auf die heutige Mikroelektronik überträgt, so kann DES mit einem vertretbaren finanziellen Aufwand (ca. 50.000 USD) in kürzester Zeit dechiffriert werden (ca. unter eine Stunde).

Die Nachbesserung 3DES

Um die Hürde für die Entschlüsselung höher zu legen, wurde eine stärkere Variante von DES entwickelt. Die Ziffer drei in 3DES steht für »triple«, für die dreifache Ausführung von DES. Tatsächlich wird das bekannte Verfahren dreimal hintereinander angewendet. Dabei werden drei Schlüssel a, b und c verwendet.:

1. DES-Verschlüsselung mit dem Schlüssel a
2. DES-Entschlüsselung mit dem Schlüssel b
3. DES-Verschlüsselung mit dem Schlüssel c

In der Praxis wird häufig für den ersten und den dritten Schritt derselbe Schlüssel verwendet (c = a).

Bislang wurde noch keine erfolgreiche Attacke auf 3DES veröffentlicht, der Algorithmus gilt als sicher. Die Entschlüsselung ist im Vergleich zum einfachen DES schwierig: Es reicht nicht aus, die Methode zum Entschlüsseln von DES einfach dreimal hintereinander anzuwenden. Ob nämlich beispielsweise der Schlüssel a richtig bestimmt wurde, erfährt der Angreifer erst dann, wenn er auch die anderen Schlüssel erraten hat.

Die wichtigste Anwendung: PIN der EC-Karte

Bis 1998 basierte die PIN der weitverbreiteten EC-Karte auf der einfachen DES-Verschlüsselung mit einer Schlüssellänge von 56 Bit. Dass dieses Verfahren mittlerweile nicht mehr als sicher anzusehen ist, wurde auch von manchen Gerichten anerkannt:

> *»Durch den Sachverständigen wurde dargelegt, dass es durchaus möglich ist, auch ohne Kenntnis der persönlichen Geheimzahl diese zu ermitteln. Dafür ist ein Kartenlesegerät sowie ein Laptop mit entsprechendem Programm ausreichend [...]. Dies ist innerhalb von Minuten durchaus durchführbar.«*

`Amtsgericht Oschatz, Urteil vom 6.2.1996`

> *»Aufgrund der durchgeführten Beweisaufnahme sieht es das Gericht nunmehr aber nicht mehr nur für theoretisch denkbar, sondern für praktisch erwiesen an, dass die PIN selbständig durch Entschlüsseln anhand der auf der Karte gespei-*

cherten Daten ermittelt werden kann, das Sicherheitssystem der Banken mithin nicht mehr so sicher ist, dass von einem Anscheinsbeweis zugunsten der Banken ausgegangen werden kann.«

Amtsgericht Frankfurt am Main, Urteil vom 01.09.1998, Az. 30 C 2119/97-45

Um zu verstehen, wie ein Dieb in Kenntnis der geheimen PIN einer gestohlenen Karte gelangen konnte, erläutern wir kurz, wie die PIN im Rechenzentrum der Banken erzeugt wurde:

Die vierte bis achte Stelle der Bankleitzahl, die zehnstellige Kontonummer und eine einstellige Kartenfolgenummer wurden zu einer Zahl zusammengefügt und mit einem bankeigenen, geheimen Institutsschlüssel DES-verschlüsselt. Die PIN war ein Teil des Ergebnisses und sie kann Werte zwischen 1000 und 9999 annehmen. Sie wurde nicht auf der Karte gespeichert und bei der Verwendung an einem Bankautomaten innerhalb Deutschlands üblicherweise online im Rechenzentrum der Bank geprüft.

Um die PIN auch im Ausland ohne Online-Verbindung zur ausstellenden Bank überprüfen zu können, wurden so genannte Poolschlüssel verwendet. Mit einem Poolschlüssel wurde aus den Kundendaten ebenfalls eine vierstellige Zahl gebildet und die Differenz dieser Zahl zur PIN auf den Karten gespeichert. So enthielt jede EC-Karte die Ergebnisse drei verschiedener Poolschlüssel.

Mindestens einer der Poolschlüssel war in sicherer Form in jedem Geldautomaten gespeichert. Mit Hilfe der gespeicherten Differenz wurde am Automaten die eingegebene PIN überprüft. Der Automat wiederholte die Verschlüsselungsprozedur und subtrahierte die gespeicherte Differenz von dem Ergebnis. Für eine erfolgreiche Authentisierung musste die Zahl mit der am Automaten eingegebenen identisch sein. Ein Dieb musste nun also nur einen der Poolschlüssel kennen und konnte aus der Karteninformation die PIN beliebig vieler EC-Karten rekonstruieren.

Der Schutz war jedoch nicht ganz so löchrig wie es zunächst erscheint, da die Poolschlüssel gesperrt werden konnten. Der Automat löschte in diesem Fall bei der nächsten Automatenoperation den Differenzwert von der EC-Karte.

Wie bereits erwähnt wurde dieses Verfahren 1998 durch ein sichereres abgelöst.

7.7.2 Advanced Encryption Standard (AES) – der neue Maßstab

Wie wir festgestellt haben, bietet DES keine zuverlässige Sicherheit mehr. Trotz der erneuten Zertifizierung im Jahr 1998 begann die zuständige Behörde NIST bereits 1997 mit der Arbeit an einem neuen Standard. Mit einem »Call for Algorithms« forderte sie auf, Verschlüsselungsalgorithmen einzureichen, die mindestens folgende Eigenschaften haben sollten:

- Der Algorithmus sollte schneller als (3)DES sein
- Der Algorithmus sollte auf der Basis eines Schlüssels kodieren und dabei den gleichen Schlüssel für Ver- und Entschlüsselung verwenden
- Der Algorithmus muss ein »Block Cipher« sein, es muss eine Blockgröße von 128 Bit unterstützt werden
- Der Algorithmus sollte in Verbindung mit dieser Blockgröße Schlüssellängen von 128 Bit, 192 Bit und 256 Bit unterstützen

Insgesamt wurden fünfzehn Algorithmen eingereicht, die teils von Unternehmen, teils von wissenschaftlich tätigen Kryptologen entwickelt wurden:

Algorithmus	Eingereicht von
CAST-256	Entrust Technologies, Inc. (vertreten durch Carlisle Adams)
CRYPTON	Future Systems, Inc. (vertreten durch Chae Hoon Lim)
DEAL	Richard Outerbridge, Lars Knudsen
DFC	CNRS – Centre National pour la Recherche Scientifique – Ecole Normale Superieure (vertreten durch Serge Vaudenay)
E2	NTT – Nippon Telegraph and Telephone Corporation (vertreten durch Masayuki Kanda)
FROG	TecApro Internacional S.A. (vertreten durch Dianelos Georgoudis)
HPC	Rich Schroeppel
LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
MAGENTA	Deutsche Telekom AG (vertreten durch Dr. Klaus Huber)
MARS	IBM (vertreten durch Nevenko Zunic)
RC6TM	RSA Laboratories (vertreten durch Burt Kaliski)
RIJNDAEL	Joan Daemen, Vincent Rijmen
SAFER+	Cylink Corporation (vertreten durch Charles Williams)
SERPENT	Ross Anderson, Eli Biham, Lars Knudsen
TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson

Tab. 7.15: Beiträge am »Call for Algorithm« der Behörde NIST, Quelle: http://csrc.nist.gov/encryption/aes/round1/round1.htm#algorithms)

Nach einem aufwändigen Testverfahren wurde schließlich Rijndael für den Advanced Encryption Standard (AES) ausgewählt. Die Auswahlkriterien für den neuen Standard umfassten im Wesentlichen die Sicherheit, Lizenzfreiheit und die Geschwindigkeit, mit der der Algorithmus in einer Hardware- und Softwareumsetzung arbeiten kann. Rijndael wurde am 26.11.2001 in der Federal Information Processing Standard Publication 197 (FIPS-197) veröffentlicht und wird (3)DES in naher Zukunft ersetzen.

7.7.3 One way hashes – Einwegfunktionen

Alle bislang betrachteten Verschlüsselungsverfahren sind sogenannte symmetrische Algorithmen, d.h. es wird derselbe Schlüssel für Ver- und Entschlüsselung verwendet. Dabei haben wir stillschweigend vorausgesetzt, das die Verschlüsselungsfunktion umkehrbar ist. Aus der Schulmathematik kennen wir einige umkehrbare Funktionen, zum Beispiel die Addition und die Multiplikation, die durch die Subtraktion und die Division umgekehrt werden können. Jedoch kennen wir auch Funktionen, die nicht so leicht umzukehren sind, zum Beispiel die Bildung einer Quersumme. Bei einer Quersumme werden die einzelnen Ziffern einer Zahl addiert.

Tab. 7.16: Beispiel: Quersummenbildung

Klartextzahl	846.243.462.537
Quersumme	81

Es ist klar, das aus der Quersumme 81 nicht eindeutig auf die Klartextzahl geschlossen werden kann. Eine Funktion mit dieser Eigenschaft nennt man eine »Hash-Funktion«.

Lassen Sie uns ebenfalls eine Hashfunktion für eine computertaugliche Binärdarstellung betrachten, die sogenannte CRC-Prüfung (»Column-Row-Checksum«). Hier werden aus den Reihen und Spalten eines Blocks von Binärzahlen erweiterte XOR-Quersummen gebildet. Betrachten wir unsere oben entwickelte Binärdarstellung für das Wort »Geheimnis« und stellen die ersten 25 Bits in einem Quadrat dar:

Tab. 7.17: Beispiel: CRC-Prüfung

G	0	1	1	0	0	0	Quersumme der Zeilen
E	0	0	1	0	0	1	
H	0	0	1	1	1	1	
E	0	0	1	0	0	1	
I	0	1	0	0	0	1	
		0	0	0	1	1	
		Quersumme der Spalten					

Aus der so berechneten Quersumme 01111 00011 lässt sich der Klartext nicht rekonstruieren.

Überprüfung der Datenintegrität

Dennoch gibt es für diese nichtumkehrbaren Funktionen sehr sinnvolle Anwendungen: Es kann verifiziert werden, ob Daten während der Übertragung verändert wurden. Übermittelt der Sender neben dem eigentlichen Dateninhalt auch das Ergebnis einer Hashfunktion (man spricht auch von

»Hash-Wert« oder nur »Hash«), so kann der Sender überprüfen, ob die Nachricht verändert wurde. Die oben dargestellte CRC-Prüfung wird z.B. bei Modems verwendet, die damit überprüfen, ob die empfangenen Daten bei der akustischen Übertragung durch das Telefonnetz beschädigt wurden. Zugegebenermaßen ist die Methode sehr simpel und es wird mit ein wenig Mühe gelingen einen Text zu fälschen, der die identische Quersumme ergibt.

Moderne Hash-Verfahren

Jedoch wurden zu genau diesem Zweck eine Vielzahl von Einwegfunktionen entwickelt, die in aufwändigen mathematischen Berechnungen einen nichtreproduzierbaren Hash-Wert wiedergeben. Die heute am häufigsten verwendeten Verfahren tragen die Bezeichnungen MD5 von RSA-Security und SHA1 von der amerikanischen Behörde NIST. Als Beispiel bilden wir den MD5-Wert eines Textes und einer leicht veränderten Variante.

Klartext	MD5
Hängt den Schurken, nicht freilassen!	bcc7cbddacb95decabd415c2c50c8480
Hängt den Schurken nicht, freilassen!	556e4d4d07bd2ae03de5a4bc1fb1e877

Tab. 7.18: Beispiel: MD5-Summen

Wie wir sehen können, kann die kleinste Veränderung einer Nachricht ihren Sinn vollständig umkehren. Die Hash-Funktion ergibt jedoch ebenfalls ein völlig anderes Resultat und die Veränderung kann sofort erkannt werden. Eine günstige Eigenschaft des MD5-Algorithmus ist die von der Größe des Klartextes unabhängige Länge des Ergebnisses. Es ist immer 128 Bit lang.

Passwörter sind niemals verschlüsselt

Die wohl heute wichtigste Anwendung für Einwegfunktionen ist die Speicherung von Passwörtern, mit denen sich Benutzer an ihrem Computer anmelden. Die Passwörter sind entgegen verbreiteter Meinung genau genommen nicht verschlüsselt. Der Benutzer gibt bei der erstmaligen Bedienung des Systems sein Passwort ein, um es zu »setzen«. Der Computer bildet mit einer Einwegfunktion einen Hash-Wert und speichert diesen ab, nicht aber das Kennwort selbst. Dies ist sinnvoll, da bei einer (symmetrischen) Verschlüsselung der Prozess umkehrbar ist und so zum Beispiel der Systemadministrator in Kenntnis des Geheimtextes kommen kann.

Wenn der Prozess nicht umkehrbar ist, wie kann dann die Authentisierung des Benutzers funktionieren? Die Lösung ist simpel: Wenn der Benutzer bei seinem Anmeldeversuch sein Passwort erneut eingibt, so wird dieses mit der gleichen Einwegfunktion bearbeitet und der erzeugte Hash-Wert dem abgespeicherten gegenübergestellt.

Wörterbücher helfen beim Erraten von Passwörtern

Mit einer Einwegfunktion bearbeitete Passwörter scheinen demnach sicher zu sein. Obwohl die direkte Rekonstruktion an der Nichtumkehrbarkeit der Funktion scheitert, gibt es dennoch Methoden, um ein Passwort zu rekonstruieren. Die einfachste Methode ist natürlich, das Passwort zu erraten. Besteht das Passwort z.B. aus dem Namen des Benutzers, so kann der Angreifer natürlich unschwer das Konto des Benutzers missbrauchen.

Schwieriger wird es jedoch, wenn das Passwort nicht direkt erraten wird. Aber auch dann gibt es eine Möglichkeit, den meisten Passwörtern auf die Schliche zu kommen. Der Angreifer benutzt dazu dieselbe Hash-Funktion wie das Betriebssystem selbst. Aus einem Wörterbuch entnimmt er der Reihe nach ein Wort nach dem Anderen und wendet die Funktion an. Das Ergebnis vergleicht er mit dem abgespeicherten Hash-Wert. Natürlich wird diese aufwändige Prozedur nicht manuell durchgeführt, es wird ein Computerprogramm und eine elektronisches Wörterbuch verwendet. Damit kann der Angreifer in kurzer Zeit eine große Zahl von Passwörten ausprobieren und wird schließlich das richtige finden. Die Voraussetzung ist natürlich, dass das Passwort auch tatsächlich ein Wort ist.

Eine gängige Methode, um diesen Angriff zu unterbinden ist z.B. die Verwendung eines Gedichtes zur Erzeugung eines Passwortes. Dabei wird der erste Buchstabe jedes Wortes verwendet und zu einem Kennwort zusammengesetzt.

7.7.4 Ein neues (altes) Problem: Der Schlüsselaustausch

Trotz aller Finesse haben alle bislang betrachteten Verfahren das gleiche Problem: die Schlüsselverteilung. Was nützt der raffinierteste und komplizierteste Chiffre, wenn ein extrem hoher Aufwand zur sicheren Übergabe des zur Ver- und Entschlüsselung verwendeten Schlüssels betrieben werden muss.

Lösung: Asymmetrisches Diffie-Hellmann-Verfahren

1975, also schon vor der Festlegung des Data Encryption Standards veröffentlichten Whitfield Diffie und Martin Hellmann das nach ihnen benannte Diffie-Hellmann-Verfahren für einen erfolgreichen Schlüsselaustausch. Bis dato war die gängige Ansicht, dass sich Absender und Empfänger treffen müssten, um einen Schlüssel auf sicherem Wege auszutauschen.

Das Diffie-Hellmann-Verfahren wird als asymmetrisch bezeichnet, da bei diesem verschiedene Schlüssel zur Chiffrierung und Dechiffrierung verwendet werden. Die Schlüssel müssen immer paarweise zusammenpassen.

Der Empfänger erhält ein solches Schlüsselpaar. Einen der Schlüssel behält er für sich und nennt ihn seinen privaten Schlüssel **a**. Den anderen Schlüssel **A** bezeichnet er als öffentlich und stellt ihn dem Sender und dem Rest der Welt in einem öffentlichen Verzeichnis zur Verfügung.

Sender	sendet Schlüssel **A**	Empfänger
		a (priv.)
A	**?**	**A** (öffentlich)

Wenn der Sender nun seine Nachricht an den Empfänger verschlüsseln möchte, so verwendet er dessen öffentlichen Schlüssel **A**.

Sender	Sende mit **A** verschlüsselten Klartext	Empfänger
		a
A	**?**	**A**

Nur der gewünschte Empfänger besitzt den dazu passenden privaten Schlüssel **a** und kann die ursprüngliche Nachricht wiederherstellen.

Das Problem ist, dass der Empfänger sich der Identität des Absenders nicht sicher sein kann. Jeder, dem der Schlüssel **A** zugänglich geworden ist, kann eine Nachricht damit senden.

Aber auch dafür bietet diese Verfahren eine Lösung: Der Sender erhält ebenfalls ein eigenes Schlüsselpaar (**B,b**) und publiziert den öffentlichen Schlüssel **B**.

Sender	Sende Schlüssel **B**	Empfänger
		a (priv.)
A	**?**	**A** (öffentlich)

Die Nachricht, die er mit dem öffentlichen Schlüssel **A** des Empfängers chiffriert hatte, verschlüsselt er erneut mit seinem privaten Schlüssel **b**.

Sender	Sende mit **A & b** verschlüsselten Klartext	Empfänger
b		**a**
B,A	**?**	**A,B**

Der Empfänger verwendet nun zuerst den öffentlichen Schlüssel des Senders **B** und dann seinen eigenen privaten **a**, um die Nachricht zu dechiffrieren. Damit ist zusätzlich sichergestellt, dass die Nachricht nur vom Eigentümer des zum öffentlichen Schlüssel **B** passenden privaten Schlüssel **b** kommen kann. Man bezeichnet die zusätzliche Verschlüsselung mit dem eigenen Schlüssel auch als »Signieren« der Nachricht.

Die Idee war revolutionär, zum ersten Mal war ein Prinzip geschaffen, wie Nachrichten sicher ausgetauscht werden konnten, ohne dass sich die Kommunikationspartner zuvor treffen mussten, um einen gemeinsamen Schlüssel auszutauschen.

Ronald Rivest, Adi Shamir und Leonard Adleman (RSA)

Das Problem dabei war nur, dass zur Zeit der Veröffentlichung kein asymmetrischer Algorithmus bekannt war, der die geforderten Eigenschaften aufwies. Nach der Veröffentlichung der grundlegenden Idee einer asymmetrischen Verschlüsselung beteiligten sich viele Mathematiker an der Suche nach einem geeigneten Algorithmus. 1977 schließlich entdeckten die Informatiker Ronald Rivest und Adi Shamir mit dem Mathematiker Leonard Adleman am Massachusetts Institute of Technologie eine geeignete Funktion:

$$c = m^e \pmod{n}$$

Die Funktion basiert auf der sogenannten Modul-Arithmetik. Diese kennen wir prinzipiell aus der Schule als Rest bei einer Division. Wenn wir zum Beispiel die Zahl zehn durch sieben teilen, so bleibt als unteilbarer Rest die drei. Natürlich hat genau diesen Rest nicht nur die zehn, sondern z.B. auch die Zahlen 17, 24 und 703. Man spricht das Resultat als »drei modulo sieben«.

Beispiel: modulo sieben

$$10 = 3 \pmod{7}$$

$$17 = 3 \pmod{7}$$

$$24 = 3 \pmod{7}$$

$$703 = 3 \pmod{7}$$

Die Wirkungsweise des RSA-Algorithmus lässt sich am einfachsten anhand eines Beispiels erläutern. Nehmen wir an, wir wollten den Buchstaben »T« verschlüsseln. Dieser hat in unserer Binärdarstellung den Wert 19.

1. Zunächst benötigt der Empfänger einen privaten Schlüssel **a**. Dieser besteht beim RSA-Algorithmus aus zwei Primzahlen **p** und **q**. Die Primzahlen sollten möglichst groß sein, wir wählen der Einfachheit halber aber **p=3** und **q=7**.
2. Des Weiteren braucht er einen öffentlichen Schlüssel **A**. Dieser besteht aus dem Produkt N von **p** und **q** ***(N = 3 x 7 = 21)*** und einer weiteren Primzahl **e**. Wählen wir **e=5**. Diesen Schlüssel stellt er in einem öffentlichen Verzeichnis für alle bereit, die ihm eine verschlüsselte Nachricht zukommen lassen wollen.
3. Der Absender verwendet die beiden Werte, um seinen Klartext »T« verschlüsseln. Unseren Wert 19 für das »T« setzt er in die Formel anstelle der Variable **m** ein und wendet die Formel an, um den Geheimtext **c** zu erzeugen:

$c = m^e \pmod n$

$= 19^5 \pmod{21}$

$= 2.476.099$

$= 10 \pmod{21}$

4. Der Sender übermittelt den Geheimtext c = 10 an den Empfänger.
5. Zur Entschlüsselung verwendet der Empfänger seinen privaten Schlüssel, bestehend aus ***p*** und ***q***. Er wendet die gleiche Funktion an, nur mit anderen Variablen:

$m = c^d \pmod n$

Die Potenz **d** muss dabei aus dem privaten und öffentlichen Schlüssel berechnet werden:

$d \times e = 1 \pmod{[(p-1) \times (q-1)]}$

$\Leftrightarrow \quad d \times 5 = 1 \pmod{12}$

$\Rightarrow \qquad d = 5$

Dann ergibt sich für der entschlüsselten Geheimtext:

$m = 10^5 \pmod{21}$

$= 100.000$

$= 19 \pmod{21}$

Aus **m=19** ergibt sich wieder der Klartext »T«. Der Empfänger kann also mit seinem privaten Schlüssel den Klartext wiederherstellen, den der Sender mit dem öffentlichen chiffriert.

1983 erhielt das Massachusetts Institute of Technologie das US-Patent für den RSA-Algorithmus (Nr. 4.405.829, »Cryptographic Communications System And Method«) und lizenzierte ihn exklusiv an die von den drei Entwicklern gegründete Firma RSA Security. Die Verschlüsselungsroutinen fast jeder Software, die wir heute benutzen, verwenden diesen Algorithmus (z.B. MS Windows, MS Internet Explorer, Mobiltelefone). Die Patentrechte verloren am 20. September 2000 ihre Gültigkeit.

Grundlage der Sicherheit: die Primfaktorzerlegung

Der RSA-Algorithmus basiert auf der Schwierigkeit, aus dem Produkt zweier Primzahlen wieder auf die Primzahlen selbst zu schließen. In unserem Beispiel mit **N=21** ist es natürlich sehr leicht, auf **p=3** und **q=7** zu schließen. Anders verhält es sich, wenn die verwendeten Primzahlen sehr groß sind. In der Tat ist die Primfaktorzerlegung ein mathematisch sehr zeitaufwändiger Prozess. Genau darauf basiert die Sicherheit des Verfahrens. Es werden Primzahlprodukte verwendet, deren Zerlegung in ihre Primzahlbestandteile selbst unter Verwendung aller heute vorhandenen Computer länger als das Alter des Universums dauern würde. Dies gilt für alle heute bekannten Methoden zur Primfaktorzerlegung.

Und dies ist die wichtigste Einschränkung bei der Verwendung des RSA-Algorithmus. Es ist durchaus möglich, wenngleich unwahrscheinlich, das ein findiger Mathematiker irgendwann (zum Beispiel morgen) einen schnelleren Weg entdeckt, ihn veröffentlicht und damit der RSA-Methode die Grundlage entzieht.

Geschwindigkeitsprobleme

Ein weiteres Problem des RSA-Algorithmus ist die Geschwindigkeit. Der Algorithmus wird von Computern etwa eintausendmal langsamer abgearbeitet als DES. Deshalb wird in der heutigen Praxis der (3)DES- oder AES-Mechanismus für die Datenübertragung benutzt. Der symmetrische Schlüssel dafür wird jedoch von einem Zufallsgenerator erzeugt und dann mit dem geschilderten RSA-Verfahren dem Kommunikationspartner übermittelt.

Der Mann in der Mitte

In der Logik der asymmetrischen Verschlüsselung existiert eine weitere Lücke, die von einem Angreifer ausgenutzt werden kann. Nehmen wir an, der Spion generiert sich selbst ein Schlüsselpaar. Auf eine Anfrage des Absenders nach dem öffentlichen Schlüssel des Empfängers sendet er ihm seinen eigenen öffentlichen Schlüssel. Er kann nun die verschlüsselte Nachricht abfangen und entschlüsseln. Damit seine Tat unentdeckt bleibt, verschlüsselt er nun die Nachricht erneut mit dem Schlüssel des richtigen Empfängers und sendet ihm die Botschaft erneut. Dies funktioniert auch mit zusätzlich signierten Nachrichten. Der Schutz davor ist einfach und effektiv: der private Schlüssel des Kommunikationspartners wird vor der Verwendung verifiziert, z.B. durch ein Telefongespräch. Diese Methode des Angriffs wird als »man in the middle« bezeichnet.

Public Key Infrastructures (PKI)

Um eine umfassendere Möglichkeit zur Verifizierung von öffentlichen Schlüsseln zu schaffen, verwendet man sogenannte »Public Key Infrastructures«. Der Kern einer solchen Struktur sind die sogenannten »Certificate Authorities« (CA). Das sind Systeme, die zur Erstellung und Verteilung von Schlüsselpaaren dienen.

Jeder Benutzer erhält ein individuelles Zertifikat, das Informationen über seine Person und seinen öffentlichen Schlüssel enthält. Dieses Informationspaket wird mit dem privaten Schlüssel der CA signiert. Seinen privaten Schlüssel erhält der Benutzer auf einer Chipkarte, Diskette oder in gedruckter Form.

Möchte ein Kommunikationspartner sichergehen, dass er den richtigen Schlüssel seines Gegenübers verwendet, so kann er dessen Zertifikat mit dem öffentlichen Schlüssel der CA überprüfen. Damit wird viel Sicherheit und Bequemlichkeit gewonnen. Jeder Beteiligte muss nur noch den öffentlichen Schlüssel der CA einmalig manuell verifizieren und abspeichern. Jedes weitere Schlüsselpaar kann anschließend damit automatisiert überprüft werden.

Anwendungsbeispiel: Virtuelle Private Netze (VPN)

Ein häufiges Problem beim Aufbau einer IT-Infrastruktur stellt die Anbindung von Niederlassungen, Außendienstmitarbeitern oder externen Dienstleistern an das Firmennetzwerk dar.

Häufig wurden für diese Verbindungen Wählverbindungen aufgebaut oder Standleitungen angemietet. Beides ist mit hohen Telekommunikationskosten verbunden. Stattdessen fällt heute häufiger die Wahl auf ein Virtuelles Privates Netz, das im Vergleich dazu die kostengünstige Kommunikationsplattform des Internets nutzt. Im Internet übermittelte Daten sind jedoch als unsicher zu betrachten, da die einzelnen Datenwege und -stationen nicht unter der Kontrolle der Kommunikationspartner stehen und ein einfaches Ziel für neugierige Dritte darstellen.

Deshalb werden die Daten über das Internet verschlüsselt übermittelt. Dazu wird bei allen beteiligten Kommunikationspartnern ein sogenanntes VPN-Gateway verwendet. Es ist ein dezidiertes Gerät oder Teil einer Software und verschlüsselt alle gesendeten Daten vor dem Eintritt ins Internet und entschlüsselt die empfangenen Inhalte. Zur schnellen und ökonomischen Verschlüsselung wird üblicherweise (3)DES oder AES verwendet. Der Schlüssel wird jedoch zuvor durch einen Zufallsgenerator generiert und in einem asymmetrischen Verfahren ausgetauscht. Dazu müssen die Anwender bei der erstmaligen Verwendung nur ein einziges Mal den öffentlichen Schlüssel des Partners verifizieren.

Anwendungsbeispiel: Mobilfunkstandard GSM

Während bei VPN in erster Linie auf die Verschlüsselung der übertragenen Daten Wert gelegt wird und die Identifizierung des Kommunikationspartners nur Mittel zum Zweck ist, bildet eine Public Key Infrastructure die Grundlage des heutigen Mobilfunkstandards GSM (»Global Systems for Mobile communications«).

Bei einem herkömmlichen Festnetzanschluss erfolgt die Zuordnung des Kunden über den Anschluss in seinen Räumlichkeiten. Verbindungen, die über diesen Anschluss aufgebaut werden, erscheinen auf der Rechnung des

Kunden. Ein Mobiltelefon kann hingegen räumlich unbegrenzt verwendet werden und eine solche Zuordnung ist nicht möglich. Deshalb wird eine andere Lösung für die Identifikation des Vertragspartners eingesetzt.

In jedes Mobiltelefon wird vor der ersten Inbetriebnahme eine Chipkarte eingesetzt. Der Chip beinhaltet das für den Benutzer personalisierte Zertifikat inklusive seines privaten Schlüssels. Der dazu passende öffentliche Schlüssel wird zentral bei der CA des Mobilfunkanbieters gelagert. Bucht sich das Telefon in das Netz des Anbieters ein, so kann es mit Hilfe des Schlüsselpaares eindeutig identifiziert und die erzeugten Kosten können dem Kunden in Rechnung gestellt werden.

7.8 Die Lösung der Zukunft: Quantenkryptografie ist sicher

Die Grundlage aller heute verwendeten Verfahren ist die Mikroelektronik, die mathematische Algorithmen verarbeitet. Zwischen Kryptografie und Kryptoanalyse besteht ein Wettlauf um die leistungsfähigeren Computersysteme. Im Folgenden soll ein Konzept vorgestellt werden, das auf physikalischen Grundlagen beruht und so sicher ist, wie die Naturgesetze gültig sind.

Licht lässt sich physikalisch auf zwei zunächst grundverschiedene Arten beschreiben: als Teilchen oder als Welle. Demnach hat ein Lichtteilchen (»Photon« oder »Lichtquant«) ebenfalls die Eigenschaften einer Welle. Diese Welleneigenschaft kann man sich als Schwingung des Teilchens in eine oder gleichzeitig in mehrere Richtungen vorstellen.

Mit einem Polarisationsfilter kann die Welle polarisiert werden, d.h. es werden die Schwingungsrichtungen gefiltert, die orthogonal zur Ausrichtung des Filters sind. Dieser Effekt wird zum Beispiel bei einfachen Sonnenbrillen zur Reduktion der Strahlungsintensität verwendet.

Die Quantenkryptografie nutzt die Polarisierung von einzelnen Lichtteilchen zur Übertragung, bzw. zur Erzeugung von Schlüsseln. Der Sender polarisiert die Photonen, der Empfänger misst sie.

Nehmen wir der Einfachheit halber an, die Lichtquanten könnten in vier Arten polarisiert werden, in horizontaler, vertikaler und zwei diagonalen Richtungen. Jeder der möglichen Richtungen wird der digitalen Wert 0 oder 1 zugeordnet:

Tab. 7.19: Polarisierung der Lichtquanten

Richtung	Horizontal	Vertikal	Links-Diagonal	Rechts-Diagonal
Symbol	—	|	\	/
Wert	0	1	0	1

Zur Messung der Polarisationsrichtung der Photonen wird ein Kalkspatkristallprisma verwendet. Genau betrachtet bestimmt das Prisma nicht die genaue Positionsrichtung der Photonen. Der Kristall emittiert die aufgenommenen Photonen in Abhängigkeit ihrer Polarisation in zwei verschiedene Richtungen. Dabei ist die Polarisation der Photonen der einen Emissionsrichtung orthogonal zu der Polarisation der Teilchen in der anderen Flugbahn.

Ein Photon, das bereits vor Kontakt mit dem Prisma in einer der beiden Vorzugsrichtungen polarisiert war, durchfliegt das Prisma unbeeinflusst und behält seine Polarisation bei. Ist die Polarisationsrichtung jedoch in einem 45°-Winkel zu der Kristallachse gedreht, so wird es mit einer je fünfzigprozentigen Wahrscheinlichkeit eine der beiden Richtungen annehmen. Dies bedeutet, dass von 100 Photonen dieser Art je 50 parallel und 50 senkrecht zur Kristallachse polarisiert werden.

Genau diese Eigenschaft macht man sich bei der Quantenkryptografie zu Nutze. Es werden zwei dieser Detektoren verwendet, die um genau diesen trickreichen Winkel von 45° zueinander gedreht sind. Der Empfänger verwendet diese Filter, die wir mit rektilinear und diagonal bezeichnen:

Schema	Rektilinear	Diagonal
Symbol	+	×

Tab. 7.20: Filtersymbole

Photonen durchqueren den für ihre Polarisationsrichtung passenden Filter unverändert. Stoßen sie jedoch auf den um 45 Grad gedrehten Filter, so nehmen sie beide mögliche Richtungen zu je 50% an:

Gesendete Polarisation						Filter	Gemessene Polarisation					
—	\	—	\	/	|	×	\	\	/	\	/	\
|	/	/	—	\	|	+	|	—	|	—	|	|

Tab. 7.21: Polarisation der Photonen

Damit sind die physikalischen Grundlagen der Quantenkryptografie vollständig und wir kommen zum Ablauf der Schlüsselgenerierung:

1. Der Sender polarisiert die gesendeten Lichtteilchen willkürlich in vertikaler, horizontaler oder in einer diagonalen Richtung:

—	\	—	\	/	|	|	/	/	—	\	|
0	0	0	0	1	1	1	1	1	0	0	1

2. Der Empfänger misst die Polarisation und wählt dazu willkürlich zwischen dem rektilinearen und diagonalen Polarisationsfilter:

×	+	+	×	×	+	×	+	+	+	×	?

3. Der Empfänger notiert sich die erhaltenen Messergebnisse und behält sie für sich:

\	|	—	\	/	|	\	—	|	—	\	|
0	1	0	0	1	1	0	0	1	0	0	1

4. Der Empfänger befragt den Sender, bei welcher Messung der richtige Filter verwendet wurde. Diese Kommunikation kann dabei über ein öffentliches Medium (z.B. ein Telefongespräch oder per Internet) erfolgen, da ein Dritter entweder die gesendeten oder die gemessenen Photonen nicht kennt. Die Messungen mit dem falschen Filter werden gestrichen:

-	-	✓	✓	✓	✓	-	-	-	✓	✓	✓
0	~~1~~	**0**	**0**	**1**	**1**	~~0~~	~~0~~	~~1~~	**0**	**0**	**1**

Sowohl Sender wie Empfänger sind nun im Besitz des gemeinsamen Schlüssels 0011001. Dieser kann in einer für die zu übermittelnde Nachricht ausreichenden Länge erzeugt werden.

Gemäß der Heisenbergschen Unschärferelation kann eine Messung nur ein einziges Mal durchgeführt werden, da die Messung die Polarisation beeinflusst. Dadurch kann die Schlüsselübertragung nicht unbemerkt belauscht werden.

Ein unbeteiligter Dritter kann die übertragenen Photonen also nicht messen, ohne auf frischer Tat ertappt zu werden. Die gewonnene Information ist so nutzlos, da der »belauschte« Schlüssel nicht verwendet wird. Aus den Informationen des filter-verifizierenden Telefongesprächs kann er ebenfalls nichts gewinnen, da er nicht weiß, ob eine 1 oder eine 0 übertragen wurde.

Da mit dieser Methode ein beliebig langer zufälliger Schlüssel erzeugt und ausgetauscht werden kann, bietet die Quantenkryptografie demnach eine vollkommen sichere Schlüsselerzeugung nach dem Vorbild des binären One-Time-Pad. Es kann eine beliebig lange Nachricht verschlüsselt über herkömmliche Wege übertragen werden (z.B. mit dem beschriebenen XOR-Mechanismus).

Zwar existieren schon erste Umsetzungen dieser neuen Forschungsergebnisse, sie sind jedoch noch sehr teuer, langsam und haben eine weitere entscheidende Einschränkung: Da die Photonen während ihres Fluges von Sender zu Empfänger nicht verstärkt werden können, ist die Reichweite limitiert. Die zur Zeit längste überbrückte Strecke ist die Distanz von Lausanne nach Genf – 67 Kilometer.

7.9 Zusammenfassung

Wie die Geschichte der Verschlüsselung zeigt, bestand zu jeder Zeit ein Wettkampf zwischen Kryptografie und Kryptoanalyse. Dies hat sich bis heute nicht geändert, es kann kein Sieger festgelegt werden. Zur Zeit scheint jedoch das Feld der Kryptologen die Nase vorn zu haben. Die asymmetrischen Methoden sind weit verbreitet und akzeptiert. Die symmetrischen Methoden haben mit der Einführung des Advanced Encryption Standards einen bedeutenden Vorsprung erzielt.

Jedoch sind sowohl symmetrische als auch asymmetrische Verfahren nicht absolut sicher und weder durch einen mathematischen Beweis noch durch Naturgesetze gesichert. Die Geheimdienste haben in der Vergangenheit eine erfolgreiche Entschlüsselung niemals veröffentlicht, da sie sich sonst der Grundlage ihres Erfolges beraubt hätten. Ebenso wenig wird ein Krimineller die Erfolge seiner unrechtmäßigen Taten verlautbaren. Zwar wird die Informations- und Kommunikationssicherheit in vielen öffentlichen Foren (z.B. des Internets) ständig diskutiert und potenzielle Schwächen werden aufgedeckt, aber auch dadurch entsteht keine absolute Sicherheit. Die Frage ist nicht ob, sondern wann eine Sicherheitslücke aufgedeckt wird und vor allem durch wen.

Der bewusste Umgang mit sensiblen Daten muss zur Selbstverständlichkeit jedes Entscheidungsträgers werden. Genauso wenig wie wichtige Dokumente auf dem Empfangstisch des Besucherraumes präsentiert werden, sollten sie z.B. auch nicht unverschlüsselt per E-Mail versendet werden. Erreichen die Dokumente sogar einen kritischen Status, von dem vielleicht die Existenz des Unternehmens abhängt, so muss die Sicherheit der elektronischen Übermittlung genauestens untersucht und gegebenenfalls ausgebessert werden.

Ob in der Zukunft ein absolut sicherer Standard entwickelt wird ist unklar. Zwar ist das angeführte Beispiel der Quantenkryptografie ein interessanter Weg, doch ob und wann sie zu einer standardisierten Lösung reift, ist heute noch nicht absehbar. Bis dahin bleibt uns nichts anderes übrig, als unsere Kommunikationswege mit Argwohn zu betrachten.

8 Juristische Aspekte beim Einsatz biometrischer Verfahren

Astrid Albrecht

Dr. Thomas Probst

8.1 Einführung

Die rechtliche Einordnung einer biometrischen Erkennung und insbesondere die rechtlichen Anforderungen an einen Einsatz biometrischer Verfahren hängen von generellen Prinzipien der einschlägigen nationalen Rechtsordnung ab. Die folgenden Überlegungen *[1]* beziehen sich auf vornehmlich deutsche Regelungen. Neben grundsätzlichen Rahmenbedingungen sind auch bereichsspezifische Bedingungen zu beachten, bei denen es auf die ganz konkrete Anwendung ankommt. Zu den generellen Anforderungen unserer Rechtsordnung gehören etwa die Menschenwürde und der Grundsatz der Verhältnismäßigkeit. Die Menschenwürde ist grundsätzlich bei einem Einsatz von Biometrie dadurch betroffen, dass auf natürliche Weise mit einem Menschen verbundene körperliche Merkmale und Funktionen zu bestimmten (Erkennungs)-zwecken instrumentalisiert werden. Bedenklich kann dies dann sein, wenn jemand dazu verpflichtet wird, seinen Körper zu Zwecken der Informationsauswertung (für ein biometrisches Verfahren) zur Verfügung zu stellen. Auch die umfassende Katalogisierung der Persönlichkeit durch eine einheitliche Personenkennziffer kann einen Würdeverstoß darstellen, wie das Bundesverfassungsgericht 1983 in dem bekannten Volkszählungsurteil festgestellt hat. Verhältnismäßigkeit ist überall dort gefordert, wo widerstreitende Interessen auftreten können, hier vor allem des Betreibers eines biometrischen Verfahrens einerseits und des Nutzers andererseits.

Abhängig vom Anwendungsumfeld sind beim Einsatz biometrischer Verfahren unterschiedliche rechtliche Anforderungen zu beachten. Im staatlichen Bereich können neben verfassungsrechtlichen Grundsätzen straf(prozessuale) Regelungen, Ausweisgesetze, Grenzkontrollvorschriften, Sozial(versicherungs)recht eine Rolle spielen. In datenschutzrechtlicher Hinsicht ist bei einem verpflichtenden Einsatz von Biometrie grundsätzlich eine gesetzliche Grundlage erforderlich.

Im Bereich der nichtstaatlichen Verwendung spielen neben dem Bundesdatenschutzgesetz (BDSG) *[2]* vor allem die Regelungen der Mitbestimmungsrechte in Betrieben sowie zivilrechtliche Regelungen (Bürgerliches Gesetzbuch: BGB, Zivilprozessordnung: ZPO) eine Rolle.

8.2 Datenschutzrechtliche Aspekte

8.2.1 Einleitung

Biometrische Verfahren arbeiten mit spezifischen körperlichen Merkmalen, die bestimmten natürlichen Personen zugeordnet werden. Biometrische Informationen sind daher grundsätzlich personenbezogene Daten. Sie unterliegen damit in aller Regel dem Schutz des informationellen Selbstbestimmungsrechts, welches das Bundesverfassungsgericht bereits 1983 im sog. Volkszählungsurteil aus dem verfassungsrechtlich geschützten allgemeinen Persönlichkeitsrecht entwickelt hat. Das informationelle Selbstbestimmungsrecht enthält für die Betroffenen (d.h. die Nutzer) die Befugnis, grundsätzlich selbst über Preisgabe und Verwendung ihrer Daten zu bestimmen.

Konkret bedeutet das für biometrische Anwendungen: Wird die flächendeckende Einführung eines biometrischen Systems im staatlichen Bereich geplant (z. B. Ausstattung von Ausweispapieren zur Kontrolle der Berechtigungen bei staatlicher Leistungsvergabe etc.), so ist dies nur aufgrund eines Gesetzes möglich, das – wie alle Gesetze – dem Verhältnismäßigkeitsgrundsatz entsprechen muss. (Etwas anderes gilt allerdings, wenn Systeme lediglich für die Abwicklung des internen Betriebs bei staatlichen Stellen eingeführt werden, wie z. B. Zugangssysteme.) Beim Einsatz biometrischer Verfahren im privaten Bereich sind die entsprechenden Vorschriften des Bundesdatenschutzgesetzes über die nicht-öffentlichen Stellen zu beachten.

In das BDSG von 2001 sind die Grundsätze der Datenvermeidung und Datensparsamkeit als allgemeine Grundsätze aufgenommen worden, die bei der Auswahl von Datenverarbeitungsanlagen beachtet werden müssen. Bei den einzelnen Verarbeitungsschritten, insbesondere Datenerhebung und -verarbeitung, ist dann zu beachten, inwieweit diese Daten überhaupt erforderlich sind. Für den Einsatz eines biometrischen Systems bedeutet dies u.a., dass, wenn alternative Methoden zur Verfügung stehen, die datenschutzfreundlichste Lösung gewählt werden muss, was im Einzelfall auch die Wahl eines nicht-biometrischen Systems bedeuten kann. Beim Einsatz eines biometrischen System aber kommt es vor allem auf die nachfolgend im Einzelnen erwähnten Aspekte an.

Neben datenschutzrechtlichen Beschränkungen gibt es auch Vorschriften, die aus Datenschutzsicht *für* die Einführung (entsprechend gestalteter) biometrischer Verfahren sprechen. So kann vor allen Dingen im Bereich der Datensicherheit ein höheres Niveau erreicht werden. Die Gewährleistung

der Datensicherheit umfasst u.a. die Zugangskontrolle, die Benutzerkontrolle und die Zugriffskontrolle und ist nach § 9 BDSG (bzw. den entsprechenden Vorschriften der Länder) geboten.

Optimal ist der Einsatz biometrischer Verfahren dann, wenn datenschutzrechtliche Klippen umschifft, also rechtliche Anforderungen eingehalten und gleichzeitig Datenschutz und Datensicherheit gefördert werden können (so genannten *datenschutzfördernden Techniken* oder *privacy enhancing technologies – PET*).

8.2.2 Problemfelder bei der Verwendung biometrischer Daten

Biometrische Daten weisen im Gegensatz zu anderen personenbezogenen Daten gewisse Besonderheiten auf, die in den folgenden Abschnitten diskutiert werden. Zusätzlich werden Gestaltungshinweise für biometrische Verfahren gegeben, um den aufgeführten Problemen in der Praxis zu begegnen.

Datenvermeidung und -sparsamkeit

Das BDSG schreibt vor, bei der Datenerfassung und -speicherung deren Erforderlichkeit genau zu beachten (d.h., sich sparsam zu verhalten) ***[3]***. So ist es zum bloßen Feststellen der Identität bzw. Berechtigung in den meisten Anwendungsumgebungen überhaupt nicht erforderlich, die einzelnen Identifikationsvorgänge zu speichern. Wird von vornherein darauf verzichtet, Daten zu erheben und zu speichern, entstehen keine Datenbestände, die dann auch nicht missbraucht werden können. Sollte dennoch eine Datenerhebung etwa für eine erforderliche Protokollierung notwendig sein, muss sich diese auf den angemessenen Umfang beschränken. Das bedeutet, dass nur die Daten erhoben und gespeichert werden dürfen, die für die eigentliche Erkennung auch tatsächlich notwendig sind. Zudem müssen (interne) Regelungen getroffen werden, wann, wie und durch wen die Protokolldateien auszuwerten und zu löschen sind. Dazu gehört die vorherige Regelung von Zugriffsrechten, die restriktiv vergeben werden sollten und etwa durch das Vier-Augen-Prinzip zusätzlich beschränkt werden können. Darüber hinaus sollte auch geregelt werden, in welchen zeitlichen Abständen Protokolldaten wieder aus der Datenbank gelöscht werden müssen.

Keine unbemerkte Erhebung der biometrischen Daten

Bei biometrischen Verfahren sollte grundsätzlich ausgeschlossen sein, dass von den Benutzern (hier eher Betroffenen) ein biometrisches Merkmal ohne deren Kenntnis technisch erfasst wird. Vielmehr sollten die Verfahren so gestaltet sein, dass in jedem Fall die willentliche Mitwirkung des Nutzers erforderlich ist. Dies gilt sowohl für die Referenzdatenerfassung (Enrolment) als auch für die spätere Überprüfung des biometrischen Merkmals des Betroffenen. Eine aktive Mitwirkung des Nutzers macht das Verfahren zudem transparenter, baut daher vermutlich unberechtigte Ängste ab und

trägt somit zur Akzeptanz des Systems bei. Wegen Verletzung des Rechts auf informationelle Selbstbestimmung sind daher grundsätzlich solche Installationen abzulehnen, bei denen z. B. beim bloßen Passieren einer bestimmten Stelle für die Betroffenen unerkennbar biometrische Merkmale erfasst werden.

Informationsgehalt der biometrischen Daten

Zur Wahrung des informationellen Selbstbestimmungsrechts der Betroffenen sollten nur solche biometrische Verfahren eingesetzt werden, bei denen sich aus den Identifikationsdaten kein sog. überschießender Informationsgehalt ergibt, der für den eigentlichen Zweck der Authentisierung nicht notwendig ist. Rückschlüsse auf den gesundheitlichen Zustand des Merkmalsträgers sollten daher von vornherein technisch nicht möglich sein, oder aber jedenfalls nicht ausgewertet werden. Da üblicherweise aus den biometrischen Rohdaten solche Rückschlüsse leichter als aus den Referenzdaten (Templates) gezogen werden können, sollte auf die Speicherung von Rohdaten ganz verzichtet werden. Bei solchen zusätzlichen Informationen unterliegen biometrische Daten als besondere Arten personenbezogener Daten weiteren Beschränkungen in der Verarbeitung ***[4]***.

Hierbei ist auch zu beachten, dass diesbezüglich die technische Machbarkeit einzelner biometrischer Verfahren noch nicht abschließend wissenschaftlich erforscht ist und daher auch mögliche, erst in der Zukunft entdeckte Zusatzinformationen berücksichtigt werden müssen. Dies unterstreicht um so mehr die Forderung, auf unnötige, sich aber möglicherweise in der Zukunft als besonders sensibel herausstellende Datenbestände zu verzichten.

Rückschließbarkeit auf natürliche Personen

Die Möglichkeit, aus den Identifikationsdaten unmittelbar auf die dahinterstehende natürliche Person rückschließen zu können, sollte erschwert oder ausgeschlossen werden. So gibt es biometrische Rohdaten, die auch eine manuelle Identifikation zulassen (etwa Bilder von Gesichtern) – diese sollten nicht gespeichert werden, wenn sie nicht unbedingt (etwa für Protokollzwecke) gebraucht werden.

Es sind Verfahren bekannt, die bei der Verarbeitung der biometrischen Eingabedaten für den Vergleich mit den Referenzdaten beispielsweise zusätzlich noch eine Zufallszahl einfließen lassen, die nur auf einer Chipkarte im Besitz des Betroffenen gespeichert ist. Der Rückschluss allein aus den Referenzdaten auf die natürliche Person ist in diesem Fall nicht möglich, es bedarf vielmehr zusätzlich der Chipkarte. Auch sollte ausgeschlossen werden, dass aus mehreren biometrischen Identifikationen, sozusagen akkumulierend, auf die natürliche Person rückgeschlossen werden kann, etwa indem mit Hilfe des Merkmals mehrere Datenbestände verknüpft werden.

Dauerhafte Bindung zwischen biometrischen Daten und Personen

Beim Erzeugen von biometrischen Datenbeständen (Referenzdaten, Eingabedaten, Rohdaten) muss bedacht werden, dass die Bindung zwischen den Daten und der Person in den meisten Fällen auf natürliche Weise gegeben ist und dauerhaft anhält. Dadurch ergibt sich eine noch über lange Zeit hinweg wirkende Missbrauchsgefahr der Daten. Abhilfe können hier solche Verfahren schaffen, die bei der Berechnung der Referenzdaten noch weitere, veränderbare Daten mit einbeziehen (etwa Zufallszahlen) oder auf willkürlich veränderbaren biometrischen Merkmalen basieren.

Ort der Speicherung der biometrischen Daten

Werden die biometrischen (Referenz-)Daten beim Nutzer (auf einem Token, z.B. einer Chipkarte oder einer anderen mobilen Speichereinheit) gespeichert, so hat dieser eher die Möglichkeit der Kontrolle über seine Daten. Ein zentraler Datenbestand birgt dagegen Gefahren für das informationelle Selbstbestimmungsrecht, nicht zuletzt wegen der weitgehenden Übermittlungsbefugnisse im Privatbereich und der umfassenden Datenerhebungsbefugnisse der Strafverfolgungsbehörden. Je mehr Daten zentral abgelegt und auf diese zumindest theoretisch zugegriffen werden kann, je größer sind die Begehrlichkeiten, die bei Behörden und privaten Stellen entstehen können. Kann auf eine zentrale Speicherung der Referenzdaten auch nach sorgfältiger Abwägung nicht verzichtet werden (etwa weil der Umgang mit individuellen Speichermedien wie Chiparten bei der betrachteten Anwendung für Nutzer und Betreiber unzweckmäßig ist), so müssen insbesondere die Zugriffsbefugnisse genau definiert sein. Über etwaige Übermittlung an Dritte müssen die Betroffenen im Allgemeinen informiert werden.

Ein weiteres Problem besteht darin, dass zentrale Datenbestände üblicherweise ohne Wissen (und Zutun) des Benutzers ausgewertet werden können, was ebenso dessen Selbstbestimmungsrecht einschränkt. Der Einsatz identischer Verfahren in unterschiedlichen Anwendungen führt für den Nutzer zu erhöhten Risiken, da sein biometrisches Merkmal als ein (im Gegensatz zu Name und Adresse) unveränderbares Personenkennzeichen verwendet werden und sein jeweiliges Nutzungsverhalten zu einem umfassenden Profil zusammengeführt werden kann. Eine dezentrale Speicherung ist daher in den allermeisten Fällen vorzuziehen.

8.2.3 Konkrete Empfehlungen beim Einsatz biometrischer Verfahren aus datenschutzrechtlicher Sicht

Allgemeine Anforderungen

Generell muss darauf geachtet werden, dass die Verfahren für die Nutzer transparent sind, die Revisionsfähigkeit gegeben ist und eine ausreichende Dokumentation der Datenverarbeitung (Software, Hardware, Datenfluss,

organisatorisches Umfeld, Sicherheitsmaßnahmen) erfolgt. Dies ergibt sich bereits aus den allgemeinen Anforderungen an IT-Systeme. Werden personenbezogene Daten verarbeitet, finden sich entsprechende Regelungen in den Vorschriften über die Datensicherheit in den Datenschutzgesetzen ***[5]***. Die betrieblichen Datenschutzbeauftragten sollten bei Einführung und Betrieb der Verfahren einbezogen werden; unter bestimmten Voraussetzungen *müssen* sie sogar (im Rahmen einer sogenannten »Vorabkontrolle«) eingebunden werden ***[6]***. Daneben ist der Grundsatz der *Zweckbindung* zu beachten, der eine Nutzung der Daten zu anderen Zwecken als denen, für die die Datenerhebung ursprünglich erfolgte, grundsätzlich nicht zulässt. So dürfen beispielsweise Protokolldaten, die aus Gründen der Datensicherheit angelegt wurden, nur zur Revision der Datenverarbeitung und nicht für andere Zwecke verwendet werden, s. § 31 BDSG.

Zulässigkeit der Verarbeitung biometrischer Daten

Personenbezogene Daten im Sinne von § 3 Abs.1 BDSG liegen immer dann vor, wenn sich die fraglichen Informationen einer bestimmten natürlichen Person zuordnen lassen. Bei biometrischen Datensätzen muss grundsätzlich davon ausgegangen werden, dass ein Personenbezug herstellbar ist. Grundsätzlich sind Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig, wenn ein Gesetz oder eine andere Rechtsvorschrift es erlaubt oder anordnet, oder der Betroffene eingewilligt hat ***[7]***.

Rechtsvorschriften als Zulässigkeitstatbestand. Es kommen mehrere Rechtsvorschriften in Betracht, die eine Zulässigkeit für die Datenerhebung, -verarbeitung und -nutzung begründen: Dies können zum einen die Zulässigkeitstatbestände nach § 28 Abs.1 BDSG sein; sie umfassen im Wesentlichen:

- Datenerhebung, -verarbeitung und -nutzung als Mittel für die Erfüllung eigener Geschäftszwecke, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient ***[8]*** (Beispiel: Speicherung von Uhrzeit und Ort bei Abhebungen an Geldautomaten im Rahmen eines Kontoführungsvertrages mit einer Bank, nicht aber der Einsatz eines Gesichtserkennungssystems durch eine Hotelkette, um Hotelgäste bei zukünftigen weiteren Besuchen am Empfangstresen namentlich begrüßen zu können)
- Datenerhebung, -verarbeitung und -nutzung zur Wahrung berechtigter Interessen der verantwortlichen Stelle ***[9]***, soweit diese erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (Beispiel: Interessen eines Arbeitgebers an der Absicherung eines Systems zur Vermeidung von Schäden, etwa in Rechenzentren, zum Diebstahlschutz etc). Allerdings müssen hier immer die schutzwürdigen Interessen der Arbeitnehmer abgewogen werden; zusätzlich müssen deren Mitbestimmungsrechte beachtet werden (siehe Abschnitt Mitbestimmungsrechte).

Nach § 28 Abs.1 S. 2 BDSG muss zudem beachtet werden, dass bei einer Datenerhebung stets die Zwecke, für die die Daten verarbeitet oder genutzt werden, konkret festzulegen sind; eine nachträglich Zweckänderung ist nur in Ausnahmefällen möglich. Dies bedeutet beispielsweise, dass bei der Einführung eines biometrischen Systems durch einen Arbeitgeber als Zutrittskontrolle eine gleichzeitige Verwendung der Daten zur Zeiterfassung für die spätere Lohnabrechnung im Vorfeld geregelt sowie den Arbeitnehmern mitgeteilt werden muss.

Als weitere Rechtsvorschrift kommt insbesondere beim Einsatz biometrischer Verfahren am Arbeitsplatz neben einem Tarifvertrag auch eine Betriebsvereinbarung in Betracht, die dann sowohl die Berücksichtigung der Arbeitnehmerrechte regelt (siehe auch Abschnitt Mitbestimmungsrechte) als auch die Rechtsgrundlage für die Datenverarbeitung darstellt. Um eine Datenverarbeitung im Sinne von § 4 Abs. 1 BDSG legitimieren zu können, werden allerdings an Form und Inhalt einer Betriebsvereinbarung einige Anforderungen gestellt:

- Zum einen muss sie die Verarbeitung personenbezogener Daten *ausdrücklich* für zulässig erklären.
- Aus ihr müssen sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Arbeitnehmer erkennbar ergeben (»Gebot der Normenklarheit«).
- Der Grundsatz der Verhältnismäßigkeit muss beachtet werden (Abwägung der widerstreitenden Interessen).
- Schließlich darf sie nicht wesentlich zu Lasten des Arbeitnehmers von den Vorschriften des Bundesdatenschutzgesetzes abweichen.

Umsetzungsprobleme können meist bei der Interpretation von zivilrechtlichen Altverträgen (etwa Verträgen mit Bankkunden) entstehen, wenn nämlich diese bei neuen Sachverhalten (etwa die Neueinführung eines biometrischen Verfahrens) daraufhin überprüft werden müssen, ob die bestehenden Verträge die neue Anwendung ebenfalls abdecken. Häufig schaffen eine Vertragsänderung bzw. der Abschluss eines Neuvertrages oder aber Vereinbarungen, die für alle Nutzer gültig sind, mehr Klarheit.

Einwilligung der Betroffenen als Zulässigkeitstatbestand. In der Neufassung des BDSG von 2001 wurden die Anforderungen an eine datenschutzrechtlich wirksame Einwilligung ***[10]*** präzisiert: Sie muss *freiwillig* und *informiert* und *bestimmt* sein. Dies bedeutet im Einzelnen: Sie muss auf der freien Entscheidung des Betroffenen beruhen, den Zweck und Umfang der vorgesehenen Datenverarbeitung festlegen sowie ausreichende (und verständliche) Informationen über diese enthalten, damit der Betroffene in etwa die Tragweite seiner Entscheidung absehen kann. Daneben gibt es gewisse formale Vorschriften, etwa dass eine datenschutzrechtliche Einwilligung im äußeren Erscheinungsbild von anderen Erklärungen hervorgehoben sein muss und grundsätzlich schriftlich zu erfolgen hat.

Insbesondere die Anforderungen an eine *informierte* Einwilligung setzen voraus, dass dem Betroffenen der Gang der Datenverarbeitung, der Ort der Speicherung etc. verständlich, d.h. unkompliziert und ohne verwirrende technische Details, vermittelt wird. Da eine umfassende Aufklärung üblicherweise hilft, eventuelle Ängste abzubauen, wird eine ausreichende Transparenz voraussichtlich auch die Akzeptanz der Nutzung des Verfahrens steigern. Hinzu kommt, dass die Bedienung und Handhabung erfahrungsgemäß gerade bei biometrischen Systemen leichter fällt, wenn die Arbeitsweise des Systems bekannt ist.

Zu beachten ist, dass der Zweck und Umfang der Datenverarbeitung zum Zeitpunkt der Einwilligung festgeschrieben wird und ohne erneute Einwilligung nur noch marginal, nicht aber in wesentlichen Punkten geändert werden darf. Insbesondere darf ohne Einwilligung keine Datenübertragung an Dritte erfolgen, sofern nicht gesetzlich zugelassene Gründe vorliegen. Vor einer solchen Datenübermittlung ist zu prüfen, inwieweit schutzwürdige Belange des Betroffenen überwiegen. Ist dies der Fall, ist eine solche Übertragung zu unterlassen; ggf. müssen die Betroffenen von der Übermittlung benachrichtigt werden.

Probleme bei der Verwendung von Einwilligungen können sich ergeben, wenn Zweifel an der *Freiwilligkeit* der Einwilligung auftreten: Dies dürfte etwa im Rahmen bestehender Arbeitsverhältnisse der Fall sein, wenn Arbeitnehmer bei Nichterteilung der Einwilligung (unausgesprochener Weise) mit beruflichen Nachteilen oder sogar Kündigung zu rechnen hätten. Eine Regelung mittels Betriebsvereinbarungen oder Tarifverträgen ist daher einzelvertraglichen Vereinbarungen (wie individuellen Einwilligungen) vorzuziehen.

Weitere Empfehlungen

Im Rahmen einer großflächigen Einführung muss außerdem bedacht werden, dass wegen der Vielzahl der biometrischen Vergleiche auch bei kleinen Fehlerraten die absolute Anzahl von Fehlentscheidungen recht groß werden kann. Hier sind sinnvolle Regelungen mit dem Umgang von Zurückweisungen durch das biometrische System erforderlich, denn die große Zahl von sowohl berechtigten Zurückweisungen als auch fehlerhaften Entscheidungen kann sowohl zu bedingungslosem Technikglauben (»der Computer hat immer recht«) als auch zum Vertrauensverlust in die Technik (»der Computer funktioniert mal wieder nicht«) verleiten. Zu berücksichtigen sind hierbei vor allem die Rechtsfolgen, die daraus erwachsen können (z.B. haftungsrechtliche Fragen), aber auch ablauforganisatorische Folgen, wenn etwa aufgrund eines Gerätefehlers wichtige Räume (z.B. Serverräume) nicht betreten werden können oder große Personengruppen betroffen sind.

8.3 Weitere juristische Fragen

Soll mittels eines biometrischen Verfahrens z.B. der Signiermechanismus einer elektronischen Signatur freigeschaltet oder ein biometrisches System im elektronischen Rechts- und Geschäftsverkehr im weitesten Sinne eingesetzt werden, stellt sich die Frage, welche zivil- und zivilprozessrechtlichen Voraussetzungen bestehen und welche Rechtsfolgen eintreten können.

8.3.1 Anwendung biometrischer Merkmale bei elektronischen Signaturen

Die Anwendung biometrischer Verfahren im Rahmen elektronischer Signaturen ist nach den entsprechenden Vorschriften im Signaturgesetz (SigG) *[11]* und in der Signaturverordnung (SigV) *[12]* zulässig. Das bedeutet, dass auch bei der sog. qualifizierten elektronischen Signatur, die besondere Voraussetzungen erfüllen muss, biometrische Merkmale zur Identifikation des Signaturschlüssel-Inhabers eingesetzt werden dürfen *[13]*. Die Besonderheit der qualifizierten Signatur liegt darin, dass zum einen besondere Anforderungen an die technische und organisatorische Sicherheit gestellt werden, wie z.B. an die sog. sichere Signaturerstellungseinheit (in der Regel die Signaturkarte). Zum anderen sind an die Verwendung der qualifizierten elektronischen Signatur bestimmte materielle und prozessuale Rechtsfolgen geknüpft (s. u.). Das biometrische Merkmal darf hier das wissensbasierte Verfahren, also PIN (personal identification number) oder Passwort ersetzen, muss aber zusätzlich an ein Besitzelement gekoppelt werden, d.h. die Verwendung eines Besitzelements wie etwa einer Karte ist auch mit Biometrie obligatorisch *[14]*. Die mit einer biometrisch gesicherten elektronischen Signatur versehene elektronische Willenserklärung hat bei entsprechend technischer Gestaltung und Einhaltung von Sicherheitsanforderungen voraussichtlich einen höheren Beweiswert vor Gericht als eine elektronische Signatur, die nur mit PIN abgesichert wurde.

Auf die Verwendung biometrischer Verfahren angewendet, bedeutet dies Folgendes: wird das Gericht von einer hohen (Überwindungs-)Sicherheit des biometrischen Verfahrens überzeugt sein, wird A schwerlich beweisen können, dass er die von X vorgelegte Bestellung nicht aufgegeben hat. A muss also für die Bestellung einstehen und zahlen, wenn er nicht nachweisen kann, dass die Verwendung der Signatur ausnahmsweise doch durch einen Dritten möglich war. Kommt das Gericht dagegen zur Überzeugung, dass der (biometrisch geschützte) Zugang zur verwendeten elektronischen Signatur von einem Unberechtigten (theoretisch) überwunden werden konnte, wird die Firma die behauptete Bestellung nicht durchsetzen können, A muss nicht zahlen. Bei der rechtlichen Beurteilung ist also entscheidend, inwieweit das Gericht von der Sicherheit des eingesetzten biometrischen Systems überzeugt werden kann. Zu hohe Technikgläubigkeit kann hier genauso zu ungerechten Ergebnissen führen wie unbegründete Zweifel.

8.3.2 Verwendung einer qualifizierten elektronischen Signatur

Bestimmte formgebundene Rechtsgeschäfte, die früher nur mit der eigenhändigen Unterschrift wirksam waren, können heute auch mit der qualifizierten elektronischen Signatur erfolgen (§ 126a BGB). Eine Bindung an eine bestimmte Form erfolgt stets nur dann, wenn dem Rechtsgeschäft eine besondere Bedeutung zukommt, die Beteiligten sich etwa des besonderen Risikos bewusst werden sollen, das sie eingehen (Warnfunktion mit Übereilungsschutz), oder für den Fall eines späteren Rechtsstreits ein Beweis besonders wichtig ist (Beweisfunktion). Bei der elektronischen Form macht das Gesetz keinen Unterschied danach, ob die Signatur mittels PIN oder Biometrie freigeschaltet wurde. In der Praxis, insbesondere vor Gericht, kann dies aber in Zukunft einen erheblichen Unterschied machen. Aufgrund der bekannten Schwächen einer PIN kann niemals sicher davon ausgegangen werden, dass auch wirklich der berechtigte Signaturinhaber die Signatur abgegeben hat.

Neben dieser elektronischen Form wird der qualifizierten elektronischen Signatur auch in prozessualer Hinsicht ein »Vertrauensvorschuss« gewährt. Wird diese verwendet, wird per Gesetz nunmehr zunächst vermutet, dass diese auch tatsächlich vom berechtigten Signaturinhaber verwendet wurde (§ 292a ZPO). Der Gesetzgeber hat hierfür einen gesetzlichen Beweis des ersten Anscheins geschaffen. Dies führt dazu, dass der Signaturinhaber, dessen Signatur durch einen unberechtigten Dritten missbraucht wurde, de facto beweisen muss, dass dieser mit seiner PIN und Signaturkarte eine Signatur in seinem Namen und ohne sein Wissen abgeben konnte.

Welche praktischen und rechtlichen Auswirkungen kann nun der Einsatz biometrischer Merkmale bei der qualifizierten Signatur haben? Beim Einsatz biometrischer Verfahren anstelle der PIN kann grundsätzlich davon ausgegangen werden, dass ein Missbrauch nicht so einfach möglich ist – wenn das biometrische System entsprechend gegen Missbrauch abgesichert ist und die dargestellten Überwindungsmöglichkeiten so weit wie möglich ausgeschlossen wurden. Dann würde die Annahme der elektronischen Form sowie der Beweis des ersten Anscheins eher gerechtfertigt sein. Allerdings kommt es auch hier entscheidend auf die tatsächliche und überprüfbare Sicherheit des Systems an. Ist dieses nämlich nur vermutet sicher (ähnlich wie bei der PIN), darf einem Nutzer das »Restrisiko« nicht zugerechnet werden: Dieser würde sonst im Zweifelsfall für eine Signatur haften, die er nicht abgegeben hat, und nur mit erheblichen Schwierigkeiten nachweisen können, dass sein biometrisches Merkmal nachgemacht oder verfälscht wurde. Unberechtigte Technikgläubigkeit würde daher die Situation für alle Beteiligten verschlechtern.

8.3.3 Strafrechtliche Relevanz

Im strafrechtlichen Bereich können biometrische Verfahren in unterschiedlicher Hinsicht zum Einsatz kommen. Sie können vor allem dazu dienen, die Identität eines Straftäters nachzuweisen, Tatverdächtige zu ermitteln (positiv) und auszuschließen (negativ).

Vor allem bei der strafprozessualen Beweisführung kann der Einsatz biometrischer Erkennungsverfahren insofern relevant sein, als bei vermutet hoher Sicherheit des eingesetzten Verfahrens die Verwendung des körperlichen Merkmals eines Verdächtigen gegen ihn verwendet werden kann. Zu denken wäre hier an kriminelle Handlungen, die nur aufgrund des Zugangs zu einem geschützten Bereich erfolgen können. Auch hier ist wiederum die Sicherheit des Verfahrens entscheidender Maßstab dafür, in welchem Umfang die Verwendung eines biometrischen Merkmals zugunsten oder zulasten des Berechtigten ausgelegt werden wird. Als Beispiel sei hier die DNA-Analyse angeführt, die erst nach langjähriger Prüfung ihrer (technisch begründeten) Aussagekraft als strafprozessuales Beweismittel zugelassen wurde ***[15]***. Dabei ist zu berücksichtigen, dass im Strafprozessrecht aufgrund der verfassungsrechtlich garantierten Unschuldsvermutung stets gesetzlich genau bestimmte Beweisregeln und damit prinzipiell strengere Maßstäbe gelten als etwa im Rahmen der freien Beweiswürdigung im Zivilprozessrecht.

Im Zusammenhang mit Befugnissen der Strafverfolgungsbehörden nach strafprozessualen Regelungen ist davon auszugehen, dass diese unter bestimmten Voraussetzungen die Befugnis haben, auf biometrische Daten zuzugreifen. Dies gilt grundsätzlich sowohl für Daten die bei Behörden gespeichert sind, als auch für solche, die bei privaten Stellen verwendet werden. Hier können auch Mitwirkungspflichten der Betreiber entstehen, wenn es z.B. darum geht, nicht nur einen biometrischen Datensatz herauszugeben, sondern auch mit einem anderen abzugleichen.

Anerkannte Methoden der erkennungsdienstlichen Behandlung sind die Erhebung und Speicherung biometrischer Rohdaten in Form von Fingerabdrücken und Lichtbildern. Im AFIS-System ***[16]***, das seit 1992 beim BKA (Bundeskriminalamt) eingesetzt wird, werden aus den so gewonnen Rohdaten der Fingerabdrücke Templates erstellt und diese zusammen mit den Rohdaten abgespeichert. Zudem ist die Feststellung sonstiger körperlicher Merkmale wie Tätowierungen, Klang der Stimme oder Schriftproben zulässig und üblich.

Schließlich ist in strafrechtlicher Hinsicht noch zu beachten, dass Rechte anderer nicht in strafwürdiger Weise beeinträchtigt werden dürfen, wenn ein biometrisches Verfahren eingesetzt wird. Soll etwa durch ein Videoüberwachungssystem das eigene Haus abgesichert werden, muss dies im rechtmäßigen Rahmen des Hausrechts erfolgen. So dürfen z.B. von Passanten auf dem angrenzenden Bürgersteig oder der Straße ohne konkreten Anlass einer Tatverdächtigung keine Aufnahmen gemacht und gespeichert werden ***[17]***.

8.3.4 Haftung des Betreibers für das biometrische System

Bei dem Betrieb eines biometrischen Systems muss zudem berücksichtigt werden, dass es sich stets um ein technisches System handelt, das bestimmte Funktionen in der konkreten Anwendung übernehmen soll. Hier muss, wie bei anderen technischen Systemen auch, bedacht werden, in welchem Umfang ein Betreiber für welche Funktionalitäten des Systems einstehen muss. Während dieser auf der einen Seite Ansprüche gegen den Hersteller haben kann, wenn das System nicht die zugesagten Eigenschaften hat, ist er selbst gegenüber seinem (End-)Kunden ebenfalls verpflichtet. Dies gilt auch, wenn eine biometrische Komponente in ein Gesamtsystem integriert wird. So ist etwa beim Schutz des Zugangs zum Online-Banking der Nutzer nur bei ordnungsgemäßer Funktion der biometrischen Zugangskontrolle in der Lage, z.B. Rechnungen fristgerecht zu bezahlen oder Aktienhandel zu betreiben. Systemausfälle oder Funktionsstörungen können hier zur Haftung des Betreibers führen, die dieser auch nicht umfassend in seinen Allgemeinen Geschäftsbedingungen ausschließen kann.

8.3.5 Allgemeine Geschäftsbedingungen beim Einsatz biometrischer Verfahren

Die kundenfreundliche Ausgestaltung der Allgemeinen Geschäftsbedingungen, insbesondere der Haftungsfragen, ist bei der Verwendung biometrischer Erkennung im elektronischen Geschäftsverkehr als vertrauensbildende und damit unmittelbar akzeptanzfördernde Maßnahme anzusehen. Kann auf der einen Seite auch mittels Biometrie keine hundertprozentige Sicherheit erlangt werden, sollten die Betreiber biometrischer Verfahren auf der anderen Seite dem End-Kunden das verbleibende Restrisiko mittels kundenfreundlicher Geschäftsbedingungen abnehmen. Nach den rechtlichen Grundsätzen zur Regelung der Allgemeinen Geschäftsbedingungen und der allgemeinen Mitverschuldensregelung im Zivilrecht ist von folgenden Grundsätzen auszugehen:

- Eine vollständige Abwälzung der Haftung auf den Nutzer im Falle des Missbrauchs eines biometrischen Systems wäre grundsätzlich unzulässig. In der Regel muss der Betreiber für die Sicherheit seines (biometrischen) Systems einstehen, da diese in seiner Sphäre liegt und der Nutzer keinen Einblick oder gar Einfluss darauf hat. Betreiber können sich im Gegensatz zum Kunden mit entsprechenden Versicherungen zudem gegen derartige Risiken absichern.
- Die Schaffung von solchen Sorgfaltspflichten, die an einen missbrauchssicheren und störungsfreien Umgang mit dem verwendeten biometrischen Merkmal knüpfen, wäre sozialinadäquat und daher ebenfalls nicht zulässig. Viele der in biometrischen Verfahren verwendeten körperlichen Merkmale sind öffentlich zugänglich und können nicht verborgen werden (z.B. der auf dem Weinglas im Restaurant zurückgelassene Fingerab-

druck, oder das Gesicht/die Stimme in der Öffentlichkeit). Der Nutzer hat keinen Einfluss darauf, ob ein Dritter (erfolgreich) versucht, seinen Fingerabdruck nachzumachen, sein Gesicht/seine Stimme unbemerkt aufzunehmen etc. Darüber hinaus wäre es nicht zulässig, dem Nutzer bei Veränderungen des Merkmals aufgrund von Verletzungen oder Erkrankungen, aber auch bei »freiwilligen« Veränderungen z.B. der Frisur ein Mitverschulden aufzubürden, wenn die Erkennung deshalb temporär nicht funktioniert.

- Eine vollständige Befreiung des Betreibers von Pflichten zur Haftung bei zeitweiligen Beschränkungen und Unterbrechungen des biometrischen Systems wäre schließlich auch unzulässig. Die Zulässigkeit von Haftungsbeschränkungen wegen technischer Störungen hängt allerdings auch vom konkreten Anwendungsgebiet ab. Grundsätzlich ist ein Betreiber jedoch verpflichtet, geeignete Vorkehrungen für die Funktionsfähigkeit und Betriebssicherheit des eigenen Systems zu treffen. Hier ist zudem zu berücksichtigen, dass bei Schäden, die durch technische Störungen und Funktionsmängel dem Nutzer des Systems entstehen, der Betreiber für diese grundsätzlich Ersatz leisten muss.
- Abschließend würde eine kundenfreundliche Regelung der Beweislastverteilung und damit des Risikos des Prozessverlustes eine solche Beweislastverteilung beinhalten, die im Schadensfall dem Betreiber auferlegt, dem Kunden nachzuweisen, dass dieser für den Schaden verantwortlich ist, und nicht umgekehrt der Kunden beweisen muss, dass er diesen nicht verursacht hat.

8.3.6 Betrieblicher Einsatz, insbesondere: Betriebsvereinbarungen

Bei Einführung eines biometrischen Systems in den Betrieb, als Zutritts-, Anwesenheits- und Verweildauerkontrolle oder Zugangs- und Zugriffssicherung etwa zum PC muss ein Arbeitgeber grundsätzlich davon ausgehen, dass eine vorhandene Arbeitnehmervertretung an dem Entscheidungsprozess beteiligt werden muss. Dies dient dem gesetzlich vorgeschriebenen Schutz der Persönlichkeit der betriebsangehörigen Arbeitnehmer. Im Folgenden werden die rechtlichen Voraussetzungen nach den betriebsverfassungsrechtlichen Grundlagen dargestellt und aufgezeigt, in welcher Art und Weise und zu welchem Zeitpunkt der Betriebsrat beteiligt werden muss, was über gesetzliche Pflichten hinaus zu beachten ist und welche (rechtlichen) Konsequenzen das Übergehen eines Mitbestimmungsrechts haben kann.

Mitbestimmungsrecht des Betriebsrats

Grundsätzlich ist die Zustimmung des Betriebsrats einzuholen, wenn es um die Einführung technischer Einrichtungen geht, sofern diese Einrichtungen zur Überwachung der Leistung oder des Verhaltens des Arbeitnehmers bestimmt sind *[18]*.

Ein biometrisches System, dass im Rahmen der Zeiterfassung oder der Zugangskontrolle eingesetzt wird, stellt grundsätzlich eine technische Einrichtung zur Überwachung dar. Hierbei kommt es nur darauf an, dass das System objektiv für eine Überwachung geeignet ist. Der konkrete Wille des Arbeitgebers, es auch tatsächlich zu Überwachungszwecken einzusetzen, ist hierbei nicht von Bedeutung.

Eine Überwachung liegt allerdings dann nicht vor, wenn auf das Verhalten oder die Leistung des jeweiligen Arbeitnehmers keine Rückschlüsse gezogen werden können. Dies wäre z.B. dann der Fall, wenn das biometrische System lediglich als eine Art Schlüsselersatz eingesetzt wird, um dem Arbeitnehmer den Zutritt zum Betriebsgelände oder den Zugang zum PC zu ermöglichen, und auf die Erhebung von Protokolldaten vollständig verzichtet wird.

Da allerdings in der Regel schon aus Gründen der Revisionssicherheit, Daten erhoben werden, ist grundsätzlich vom Eingreifen der hier angesprochenen Mitspracheregelung auszugehen.

Zeitpunkt der Beteiligung

Sollen biometrische Verfahren als Kontrolleinrichtungen eingesetzt werden, braucht der Betriebsrat zwar nach den gesetzlichen Regelungen noch nicht im Planungsstadium beteiligt zu werden. Zwingend ist der Betriebsrat erst dann zu beteiligen, wenn eine Entscheidung über das Ob, die Anzahl, den Zeitraum, die Zweckbestimmung und Wirkungsweise der Kontrolleinrichtung getroffen werden soll. Jedoch muss der Arbeitgeber den Betriebsrat rechtzeitig, d.h. bereits im Planungsstadium, über die geplante Einführung biometrischer Verfahren unterrichten ***[19]***.

Zum Zwecke des gütlichen Miteinanders von Arbeitgeber und Betriebsrat sowie im Interesse der Arbeitnehmerrechte ist jedoch auch bei fehlendem gesetzlichem Zwang zu empfehlen, den Betriebsrat frühestmöglich einzubeziehen. Der Betriebsfrieden wird letztlich nicht unerheblich davon abhängen, ob der Betriebsrat den Arbeitgeber bei Einführung des biometrischen Systems unterstützt, was zu guter Letzt auch entscheidenden Einfluss auf die Akzeptanz des biometrischen Systems durch die Arbeitnehmer haben wird. Neben der gesetzlich vorgesehenen Unterrichtung des Betriebsrates können außerdem gemeinsame Ausschüsse von sachverständigen Vertretern der Arbeitgeber- und Betriebsratsseite gebildet werden ***[20]***. Diese können die weiteren Verhandlungen zwischen Arbeitgeber und Betriebsrat erheblich erleichtern.

Ausübung des Mitbestimmungsrechts

Die Zustimmung des Betriebsrats sollte durch eine entsprechende Betriebsvereinbarung erfolgen. Die erforderliche Vereinbarung muss ohnehin schriftlich niedergelegt werden ***[21]***, was auch erheblich zu Rechtssicherheit und Transparenz beiträgt. Die Betriebsvereinbarung beansprucht zudem unmittelbare und zwingende Geltung gegenüber dem Arbeitgeber und der

Arbeitnehmerschaft *[22]*. Ihr kommt daher sog. Rechtsnormcharakter zu, was erhebliche Auswirkungen auf die Rechtsverbindlichkeit und Verstöße gegen die getroffenen Regelungen hat.

Der Rechtsnormcharakter der Betriebsvereinbarung hat folgende Auswirkungen:

- Ein Verstoß gegen eine Betriebsvereinbarung bewirkt die Unwirksamkeit der abweichend getroffenen Abrede zwischen Arbeitgeber und dem einzelnen Arbeitnehmer innerhalb des Arbeitsvertrages. Der Arbeitnehmer muss dieser Abrede in diesem Fall nicht Folge leisten, was erheblichen Einfluss auf die Ordnung im Betrieb haben kann.
- Auch bereits zuvor getroffene abweichende Individualvereinbarungen zwischen dem Arbeitgeber und einzelnen Arbeitnehmern treten hinter Betriebsvereinbarungen zurück, verlieren also faktisch ihre Gültigkeit.
- Der Vorrang der Betriebsvereinbarungen gilt auch dann, wenn die Individualvereinbarung eine im Vergleich zur Betriebsvereinbarung für den Arbeitnehmer eigentlich günstigere Regelung trifft.

Weitere Schutzpflichten gegenüber dem Arbeitnehmer

Neben den dargestellten Pflichten, die Rechte der Arbeitnehmer mittelbar über deren Vertretung im Betrieb zu gewährleisten, hat der Arbeitgeber weitere unmittelbare Pflichten zum Schutz der Arbeitnehmer, die bei Einführung eines biometrischen Systems ebenfalls zu beachten sind.

Der Arbeitgeber hat dafür Sorge zu tragen, dass nicht in unzulässiger Weise in das allgemeine Persönlichkeitsrecht des Arbeitnehmers eingegriffen wird *[23]*. Dieses gewährt dem Einzelnen nicht nur einen »abgeschirmten Bereich persönlicher Entfaltung«, sondern das schon im Abschnitt Datenschutz angesprochene »Recht auf informationelle Selbstbestimmung«.

Durch die Verwendung eines biometrischen Systems wird der Arbeitnehmer zur Überlassung persönlicher Daten an den Arbeitgeber verpflichtet, wodurch in sein allgemeines Persönlichkeitsrecht eingegriffen wird. Aufgrund seiner Schutzpflicht darf der Arbeitgeber ein biometrisches System daher nur dann einführen, wenn dabei die Verhältnismäßigkeit gewahrt bleibt. Dabei kommt es entscheidend darauf an, ob sich der mit der Einführung verbundene Eingriff in das Persönlichkeitsrecht des Arbeitnehmers im konkreten Fall bei objektiver Würdigung des Einzelfalles als zwingend erforderlich erweist. Hier muss eine sorgfältige Abwägung der Interessen des Arbeitgebers mit denen des Arbeitnehmers erfolgen, wobei die Angemessenheit einer biometrischen Erkennung (im Gegensatz zur bisher verwendeten Erkennungsmethode) und die Geeignetheit für die Zwecke der Zutritts-/Zugangssicherung zu prüfen sind. So ist z.B. der Einsatz von Überwachungskameras gekoppelt mit einem Gesichtserkennungssystem nur dann zulässig, wenn dieser nicht ausschließlich der Kontrolle der Arbeitnehmer dient, sondern eine solche Kontrolle aus besonderen Sicher-

heitsgründen (wie etwa bei Bankschaltern oder in Atomkraftwerken) geboten erscheint. Auch in diesem Zusammenhang bietet sich wiederum eine frühzeitige Einbindung der Arbeitnehmervertretung an.

8.4 Verbrauchersicht

Verbraucher, die Waren und Dienstleistungen aller Art in Anspruch nehmen, können künftig mit Anwendungen biometrischer Verfahren vor allem dort konfrontiert werden, wo eine Überprüfung der Berechtigung erforderlich ist. Dies kann z.B. auf Anwendungen beim Online-Banking zutreffen, wenn es darum geht, sich für den Zugang zum eigenen Bankkonto zu authentifizieren, oder bei der Freischaltung einer Signaturkarte. Der Einsatz von Biometrie im Verbraucheralltag kann bei richtiger Auswahl der Merkmale und Gestaltung der Verfahren zu höherer Sicherheit der jeweiligen Anwendung und zu mehr Bequemlichkeit auf der Nutzerseite führen. Im Interesse der Verbraucher bzw. der Akzeptanz durch die Nutzer sollten beide Aspekte bei der Konzeption gleichberechtigt gewichtet werden, wobei allerdings je nach Anwendung ohne weiteres unterschiedliche Sicherheitsstufen gewählt werden können.

Chancen und Risiken biometrischer Verfahren liegen nicht zuletzt wegen der generell lebenslangen Personengebundenheit biometrischer Merkmale an das jeweilige Individuum nahe beieinander. Auf der einen Seite könnten die Nachteile des im fraglichen Bereich bisher überwiegend angewandten Prinzips von Besitz und Wissen (z.B. Karte und PIN oder Passwort) künftig überwunden werden, da die Sicherheit der Anwendung nicht mehr ausschließlich in der Geheimhaltung der PIN und einer stets sicheren Aufbewahrung der Karte durch den Berechtigten gewährleistet werden muss. Aus dieser Forderung leiten die Anbieter (u.a. insbesondere die Banken) bis heute zum Teil unzumutbare Sorgfaltspflichten für den Verbraucher ab, die wiederum zu einer ungerechten Haftungs- und Beweislastverteilung führen.

Auf der anderen Seite ergeben sich durch den Einsatz von Biometrie bisher nicht bekannte Risiken, die vor allem den Datenschutz und die Datensicherheit betreffen. Daher muss die Sicherheit biometrischer Daten auch in reinen Convenience-Anwendungen gewährleistet sein. Auch muss aus diesem Grunde Sicherheit in Bezug auf Biometrie stets zweiseitig betrachtet werden, und zwar sowohl in Bezug auf die Sicherheit der dabei verwendeten biometrischen als auch auf die mittels Biometrie zu schützenden Daten. Ergänzend dazu ist eine verbraucherfreundliche Gestaltung der der jeweiligen Anwendung zugrunde liegenden Allgemeinen Geschäftsbedingungen von entscheidender Bedeutung.

Der praktische Einsatz biometrischer Verfahren im Verbraucheralltag ist nicht nur in solchen Bereichen zu erwarten, in denen sich der Verbraucher frei für oder gegen die Nutzung der Biometrie entscheiden kann. Neben einem möglicherweise verpflichtenden Einsatz im hoheitlichen/staatlichen

Bereich, bei dem der Verbraucher stärker in seiner Eigenschaft als Bürger betroffen ist, könnten auch prinzipiell freiwillige Anwendungen, etwa im privatwirtschaftlichen Bereich, zu einem faktischen Benutzungszwang führen. Dies kann immer dann der Fall sein, wenn durch die Biometrie das herkömmliche Authentifizierungsverfahren ersetzt werden soll, so zum Beispiel beim Zugang zum Online-Banking oder beim Zutritt zu räumlich geschützten Bereichen (Flugzeug etc.). Die Option, ein biometrisches Verfahren nicht zu benutzen, wäre dann faktisch nicht mehr gegeben.

Auch die Sozialverträglichkeit eines biometrischen Systems ist von besonderer Bedeutung. Nicht alle Menschen können jedes Verfahren nutzen, da sie so verschieden sind wie ihre körperlichen Merkmale voneinander abweichen. Darüber hinaus gehört zu einem nicht-diskriminierenden Einsatz von Biometrie stets die Berücksichtigung derer, die u.a. aus den dargestellten Gründen eine biometrische Erkennung ablehnen.

Schließlich sind aus Sicht des Verbraucherschutzes neben den Aspekten des Datenschutzes und der Datensicherheit auch und gerade die Nutzerakzeptanz, die Bedienerfreundlichkeit und die Gestaltung der Einsatzumgebung von entscheidender Bedeutung. Nicht zuletzt muss bei der Auswahl und Konzeption eines biometrischen Systems für eine bestimmte Anwendung hinsichtlich des erforderlichen Nutzens für die Anwender sorgfältig abgewogen werden, ob ein Einsatz von Biometrie tatsächlich dazu führen wird, die gewünschte Aufgabe effizienter und wirtschaftlicher zu lösen, und gleichzeitig Sicherheit und Bequemlichkeit für die Nutzer gegenüber einem Verfahren ohne Biometrie mit einem merklichen Mehrwert zu verbessern.

8.5 Ausblick

Beim Einsatz biometrischer Systeme ist demzufolge die Berücksichtigung rechtlicher Aspekte von entscheidender Bedeutung. Nicht nur im allgemeinen datenschutzrechtlichen Kontext, sondern darüber hinaus auch z.B. im betrieblichen Bereich ist es dabei wichtig, diese Aspekte von vornherein möglichst schon in die Planung einzubeziehen. Vor allem im Hinblick auf den notwendigen Datenschutz der betroffenen Nutzer kann bereits das einzusetzende biometrische System auch nach den Grundsätzen besonders datenschutzfreundlicher Technologien (PET) ausgewählt werden, d.h. beispielsweise nach den Grundsätzen einer möglichst großen Datenvermeidung und -sparsamkeit und unter Verzicht auf zentrale Speichermethoden.

Mögen gerade die datenschutzrechtlichen Anforderungen oftmals eher als »Hemmschuh« für einen breitflächigen Einsatz biometrischer Verfahren insgesamt angesehen werden, so darf dabei auf der anderen Seite jedoch nicht vernachlässigt werden, dass es insbesondere auch Anforderungen an die Datensicherheit nach BDSG sind, die einen Einsatz biometrischer Verfahren erst ermöglichen bzw. fördern. Denn wo personenbezogene Daten geschützt werden müssen, kommen biometrische Systeme prinzipiell besser in Betracht

als solche Authentifizierungsmethoden, die lediglich personenbezogen, aber ohne die oftmals wünschenswerte unmittelbare Personenbindung funktionieren. Da biometrische Verfahren aber selbst ebenfalls mit persönlichen Daten arbeiten, ist ein bestimmtes Mindestmaß an Funktionalität und Sicherheit unabdingbar. Dies spiegelt sich auch in den genannten Signaturregelungen wieder, die eine bestimmte Evaluierungsstufe nach Common Criteria (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik) verlangen, wenn biometrische Verfahren zur Freischaltung des Signaturschlüsselmechanismus eingesetzt werden sollen.

Das Restrisiko, das auch bei angemessen sicheren biometrischen Systemen noch verbleibt, wird gerade im Verhältnis Unternehmer-Verbraucher, also B2C-Commerce, über die entsprechenden Allgemeinen Geschäftsbedingungen gestaltet werden. Diese finden ihre rechtlich zulässigen Grenzen in den allgemeinen Rechtsgrundsätzen vor allem des Bürgerlichen Rechts. Hier muss – neben den hier ebenfalls diskutierten verbraucherpolitischen Gesichtspunkten – stets ein ausgewogenes Verhältnis zwischen den schutzwürdigen Interessen der Betroffenen und den berechtigten Interessen der Betreiber gefunden werden. Dies bedarf der Erfüllung relevanter Anforderungen, ist aber durchaus möglich und realisierbar. Dies sollte dieser Beitrag aufzeigen.

Literatur. *[1]* Dieser Text ist ein leicht veränderter Auszug aus Kapitel 6 des Kriterienkataloges »Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren«, Version 2.0, der von der Arbeitsgruppe 6 »Biometrische Identifikationsverfahren« des TeleTrusT Deutschland e.V. (*www.teletrust.de*) erstellt wurde. Dieser ist unter *http://www.teletrust.de/publikat.asp?id=40600* elektronisch abrufbar oder kann bei TeleTrusT angefordert werden.

[2] Bundesdatenschutzgesetz vom 22.05.2001, BGBl. 2001 I Nr. 23.

[3] Stichwort »Datensparsamkeit«, §3a BDSG.

[4] nach § 3 IX BDSG.

[5] s. z.B. Anlage zu § 9 BDSG und die sich daraus ergebenden Pflichten.

[6] s. § 4d Abs. 5 BDSG.

[7] § 4 Abs.1 BDSG

[8] § 28 Abs.1 Nr. 1 BDSG

[9] § 28 Abs.1 Nr. 2 BDSG

[10] § 4a BDSG

[11] Signaturgesetz vom 16.05.2001, BGBl. 2001 I Nr. 22

[12] Signaturverordnung vom 16.11.2002, BGBl. 2001 I Nr. 59

[13] §§ 17 Abs. 1 Satz 1 SigG in Verbindung mit 15 Absatz 1 SigV

[14] § 15 Abs. 1 Satz 1 SigV

[15] vgl.§81g I StPO und DNA-Identitätsfeststellungsgesetz vom 07.09.1998, BGBl. I S.2646

[16] Automatisches Fingerabdruck Identifizierungs System

[17] dies folgt u.a. aus §§ 22, 23 Kunsturhebergesetz

[18] § 87 Abs.1 Nr.6 Betriebsverfassungsgesetz (BetrVG)

[19] §§ 90, 111 BetrVG

[20] § 28 Abs. 3 BetrVG

[21] § 77 Abs. 2 S. 1 BetrVG

[22] § 77 Abs. 4 BetrVG

[23] § 75 Abs. 2 BetrVG

Weitere Literaturangaben. Leger, L./ Nolde, V., *Biometrische Verfahren*, Deutscher Wirtschaftsdienst 2002.

Behrens, M./Roth, R., *Biometrische Identifikation*, Vieweg 2001.

Albrecht, A., *Biometrische Verfahren zum Nutzen für Verbraucher* , DuD 2000, S. 332 ff.

Albrecht, A./Probst, T., *Biometrische Verfahren – im Einklang mit Verbraucher- und Datenschutz?*, AgV-Forum 01/2001, S. 32 ff.

Köhntopp, M.: *Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren*, S. 177 ff., in: Horster, Patrick (Hrsg.): *Sicherheitsinfrastrukturen – Grundlagen, Realisierung, Rechtliche Aspekte, Anwendungen*; Vieweg 1999

Jain, A./Bolle, R./Pankati, S., *Biometrics: Personal Identification in Networked Society*, Norvell 1999.

Probst, T., *Biometrie und SmartCards*, DuD 2000, 322 ff.

9 IT-Sicherheit aus Nutzersicht – Strategien für Sicherheit und Akzeptanz

Hansjörg Höltkemeier

Das Thema »Sicherheit« gilt als eine der zentralen Herausforderungen in der Informationstechnologie. Je leistungsfähiger die Systeme werden, je mehr Daten verarbeitet und gesammelt werden, desto mehr Bedeutung erhalten die Systeme und die Sicherung derselben. Dabei gilt es, jeden missbräuchlichen Zugriff zu verhindern, also die Systeme durch technische und organisatorische Maßnahmen gegen Missbrauch, Manipulation oder Zerstörung zu sichern.

Mit der zunehmenden Vernetzung durch das Internet und dem breiten Vordringen des Electronic Commerce hat diese Problematik in den vergangenen Jahren nicht nur quantitativ eine neue Dimension erhalten. Unbekannte Nutzer sollen jetzt sogar auf das System zugreifen, sie sollen allerdings nach wie vor das System nicht gefährden können.

Auf der Nutzerseite zeigt sich eine ähnlich ambivalente Situation. Hier wird z.B. einerseits die (fehlende) Sicherheit immer wieder als einer der bedeutendsten Hinderungsgründe für den elektronischen Handel genannt und andererseits belegt das tatsächliche Verhalten, dass diese für eine höhere Sicherheit weder einen höheren Preis noch eine komplexere Bedienung zu akzeptieren bereit sind (siehe Abbildung 9.1).

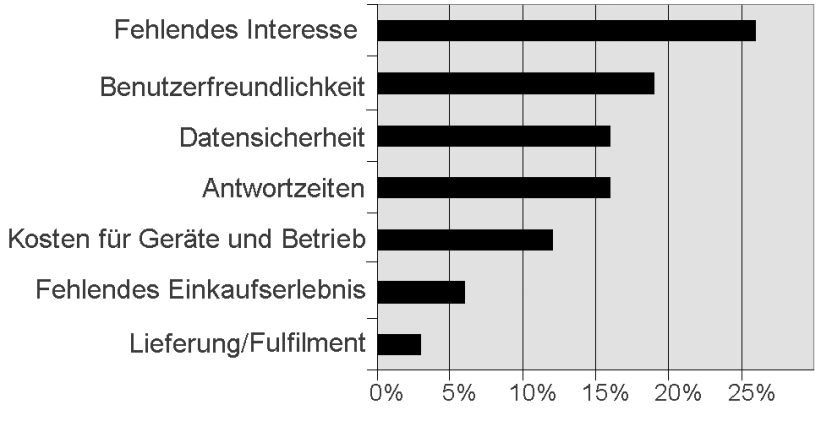


Abbildung 9.1: Hemmnisse des E-Commerce

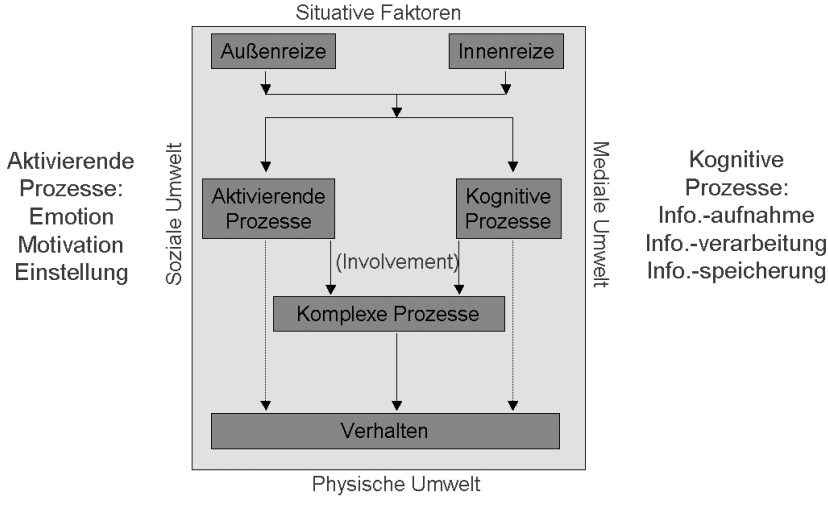
Nach den enormen Anstrengungen, die in diesem Bereich auf Anbieterseite unternommen werden, gilt heute vielfach: »Es ist sicher und keiner geht hin…«. Dieses ist Anlass für ein Überdenken und Differenzieren des Themas »IT-Sicherheit« vor allem in kundenorientierten Anwendungen. IT-Sicherheit ist ein zentrales, keineswegs aber nur ein Technologiethema. Der vorliegende Beitrag widmet sich der IT-Sicherheit deshalb aus der Perspektive der Nutzer-/Kundenakzeptanz und stellt nachfolgend Hintergründe und beispielhaft Lösungsansätze für Nutzer-orientierte IT-Sicherheitslösungen vor.

9.1 IT-Sicherheit aus Nutzersicht

9.1.1 Grundlagen zum Nutzerverhalten

Der Mensch entscheidet selten vollständig rational im Sinne des »homo oeconomicus« *[1]*. Er entscheidet vielmehr subjektiv, situativ und nicht zuletzt unter Nutzung verschiedener Strategien zur Vereinfachung und Beschleunigung mehrdimensionaler Entscheidungen. Die wahrnehmbare Entscheidung resultiert nach den Erkenntnissen der Konsumentenverhaltensforschung aus dem Zusammenwirken psychologischer und sozialer Aspekte, wie das nachfolgend aufgezeigte Modell der Konsumentenverhaltensforschung verdeutlicht.

Abbildung 9.2: Erklärungsansatz für das Konsumentenverhalten



Eine spezifische Reizkonstellation (Außen- und/oder Innenreize) löst aktivierende Prozesse aus, die den Kunden grundsätzlich zum Handeln motivieren, aber auch entsprechend persönlicher Einstellungen erste Handlungsoptionen vorgeben oder ausschließen. Diese Einstellungen basieren auf eigenen Erfahrungen oder sind durch Vermittlung im sozialen Umfeld

zustande gekommen und bedeuten gleichsam Vorentscheidungen im weiteren Prozess bis zur endgültigen Handlung. Parallel setzen kognitive Prozesse in Form der Aufnahme, Verarbeitung und Speicherung der jeweils vorliegenden und neu hinzukommenden Informationen ein. In dieser kognitiven Behandlung des Problems bewertet der Konsument die Zielerreichung und seine aktuellen Handlungsalternativen laufend neu. Er ermittelt so die Richtung und die Intensität für sein weiteres Handeln, also z.B. auch, welche weiteren Informationen für eine Entscheidung sinnvoll zu beschaffen sind oder ob der Prozess nicht aufgrund fehlender Erfolgsaussichten (die Aufwändungen zur Vollendung der Handlung übersteigen den erwarteten Nutzen) oder drohender Gefahren (die dann ggf. in keinem Verhältnis zum erwarteten Nutzen stehen) abgebrochen werden sollte.

Der Nutzer handelt also insofern ökonomisch, als das seinem Handeln ein laufendes Kalkül zu Grunde liegt, in das neben den Eigenschaften des Produktes und der damit verbundenen Nutzenerwartung im Verhältnis zum jeweiligen Preis auch zahlreiche andere monetäre und nicht-monetäre Komponenten wie die Aufwändungen zur Realisierung der Kaufentscheidung (Anfahrtswege, Online-Kosten, Wartezeiten etc.) und die bei und mit dem Kauf entstehenden Risiken (Fehlinvestitionsrisiko, Preisrisiko, Betrugsrisiko etc.) eingehen.

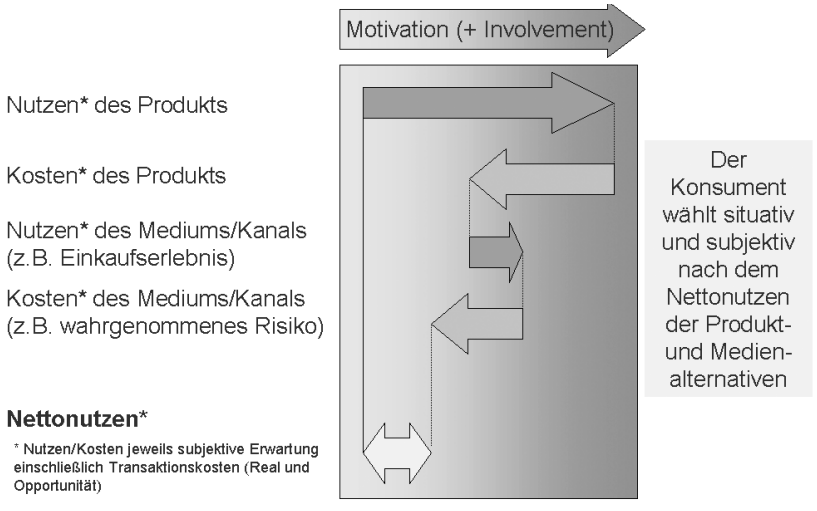
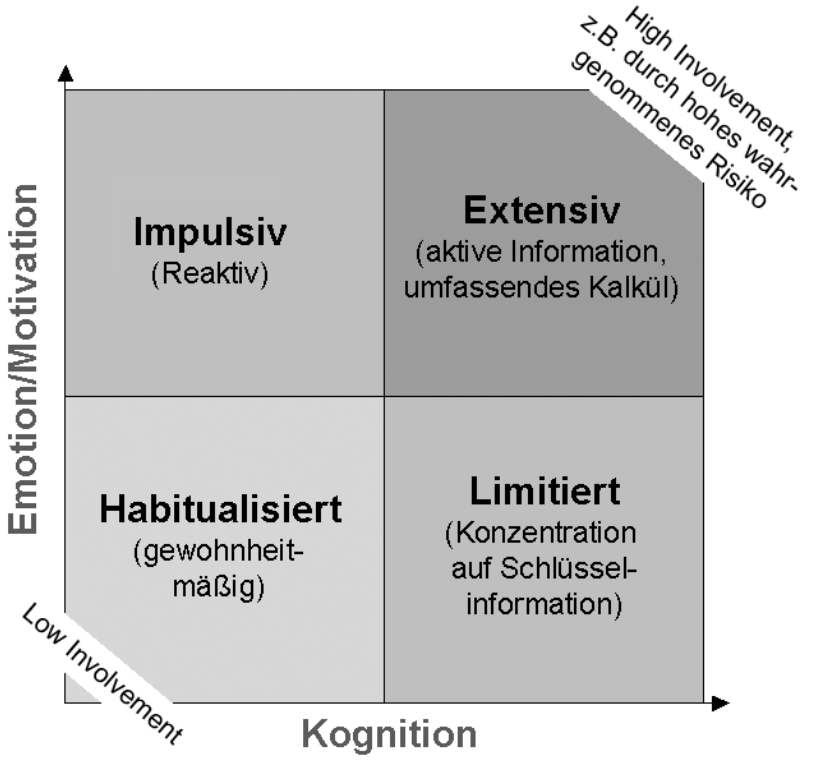


Abbildung 9.3: Das Kalkül des Konsumenten

In diesem Prozess neigt der Konsument allerdings regelmäßig zu vereinfachenden Handlungsmustern. In Abhängigkeit von seinem jeweiligen Interesse an der Kaufentscheidung, z.B. determiniert vom wahrgenommenen Risiko, werden schon mit dem Erreichen einer hinreichenden Sicherheit Entscheidungen gefällt. Diese äußern sich als Impulskäufe, limitierte Kaufentscheidungen auf der Basis von Schlüsselinformationen oder im gewohnheitsmäßigen Rückgriff auf bekannte Vertriebskanäle, Marken oder Produkte. Das

letztgenannte Handlungsmuster ist dabei besonders geeignet, um die Risiken einer Fehlentscheidung zu minimieren und die Komplexität des weiteren Auswahlprozesses nachhaltig zu reduzieren.

Abbildung 9.4: Typologien des Entscheidens



Der Konsument handelt also auch aus der verhaltenswissenschaftlichen Perspektive keineswegs irrational, andere Effekte überlagern nur häufig die rationale und extensive Entscheidung. So erfolgt die Bewertung der Handlungsalternativen lediglich auf der Basis der situativ vorhandenen und verfügbaren, subjektiv relevanten Informationen, sie ist stark abhängig von den jeweiligen »Einstellungen« des Nutzers und sie wird nicht unerheblich von der Bedeutung der Entscheidung für den Konsumenten und dem wahrgenommenen Risiko beeinflusst. Auch aus dieser Sichtweise heraus müssen Konzepte zur IT-Sicherheit überprüft werden.

9.1.2 IT-Sicherheit im Handlungskalkül des Nutzers

Aus Nutzersicht kann die IT-Sicherheit also dann verhaltensbeeinflussend wirksam werden, wenn das Thema überhaupt als relevante Komponente einer Handlungsalternative wahrgenommen und/oder situativ durch entsprechende Informationen repräsentiert wird. IT-Sicherheit fließt ferner über

Einstellungen des Nutzers auch ohne akut neue Informationen als Prädisposition für oder gegen eine IT-basierte Lösung in den Handlungsprozess ein und ihr Einfluss ist nicht zuletzt abhängig von der Verfügbarkeit weiterer Daten als Schlüsselinformationen in der Handlungssituation. Alle drei Aspekte gilt es bei der Planung von Sicherheitskonzepten im Umfeld der Informationstechnologie und mehr noch des E-Commerce zu berücksichtigen und zu steuern.

Wahrnehmungen der IT-Sicherheit am Beispiel des E-Commerce

Nutzer von E-Commerce-Applikationen verfügen zumeist über eigene Endgeräte und haben damit als »private IT-Betreiber« zunächst das gleiche Sicherheitsbedürfnis, wie in der Einführung auch für Unternehmen festgestellt wurde. Die Systeme sollen gegen Missbrauch, Manipulation und Zerstörung gesichert sein. Dabei ist zu konstatieren, dass die Einstellung zum Thema »IT-Sicherheit« auf Nutzerseite zwar kritisch, aber bei weitem nicht so gefestigt und verhaltensbestimmend ist, wie dieses bei professionellen Anbietern vermutet wird. Die Nutzer sind für das Thema eher sensibilisiert als grundsätzlich negativ vorbelastet und machen ihr Verhalten daher weit mehr von situativen Faktoren abhängig, als dieses z.B. bei der grundsätzlichen Entscheidung für oder gegen einen elektronischen Vertriebsweg der Fall ist. Offensichtlich ist die erlebte Bedrohung angesichts der üblicherweise relativ geringeren Bedeutung eines privaten Systems deutlich schwächer ausgeprägt, was sich nicht zuletzt auch in einer unterdurchschnittlichen Sicherheitsausstattung privater Systeme niederschlägt.

Dennoch wird die fehlende Sicherheit als eines der zentralen Argumente gegen die Nutzung elektronischer Vertriebskanäle angeführt. Für die potenziellen Nutzer des Internet und netzbasierter E-Commerce-Applikationen gewinnen Sicherheitsthemen damit situativ an Bedeutung. Die bisherige Entwicklung des E-Commerce und das Monitoring des Nutzerverhaltens bei ausgewählten E-Commerce-Applikationen lässt dazu die nachfolgenden Gedanken- und Verhaltensmuster erkennen:

- **Bei der Auswahl der Produkte** geht die Unsicherheit bezüglich der zugesagten Eigenschaften des Produktes und der Verlässlichkeit des zumeist unbekannten Vertriebspartners in das Kalkül um die Vorteilhaftigkeit des Online-Kaufs mit ein. Dieses erklärt einerseits die besondere Eignung standardisierter Produkte wie Bücher und CDs und untermauert andererseits die besondere Bedeutung einer eingeführten Marke im E-Commerce. Dieser Aspekt ist zwar typisch für das räumlich und zeitlich ungebundene digitale Geschäftsmodell, wird aber nicht unter dem Stichwort »IT-Sicherheit« diskutiert und kann durch entsprechende Sicherheitskonzepte auch nicht entschärft werden.
- **Bei der Bestellung der Produkte** dominiert nachfolgend die Sorge um die missbräuchliche Verwendung der persönlichen Daten, die mit der Bestellung übersendet werden. Dabei sind wiederum zwei Möglichkeiten des Missbrauchs von besonderer Bedeutung. Zum einen könnten

sich Unbefugte Zugang zu den an den Vertragspartner gesendeten Daten verschaffen und diese missbräuchlich verwenden und zum anderen könnte der Vertragspartner selbst die gewonnenen Daten zu anderen als den vertraglich vereinbarten Zwecken, also z.B. für Direktmarketingmaßnahmen oder gar zum Verkauf an Dritte nutzen. Auch hier sind reine Technikkonzepte zur IT-Sicherheit nur bedingt geeignet, die Sorge der Nutzer zu zerstreuen. Zwar kann der Anbieter die Sicherung seiner Datenhaltung gegen unbefugten Zugriff erklären und vielleicht sogar nachweisen, spätestens die weitere Verwendung dieses Assets durch den Anbieter selbst ist aber IT-seitig nicht mehr abzusichern.

- **Die Versendung der Daten** geht einher mit der Befürchtung, dass Unbefugte die entsprechenden Informationen »abfangen« und wie oben missbräuchlich nutzen könnten. Eine besondere Sensibilität existiert dabei bei der Übermittlung von Kreditkartennummern, Geheimzahlen, Passwörter etc., weshalb das Payment nach wie vor zur Achillesferse des E-Commerce zählt. Obwohl es sich hier nur teilweise um den Zuständigkeitsbereich des Anbieters handelt, der Nutzer kann sich gleichermaßen um die Sicherheit der Übertragung, z.B. durch Verschlüsselung bemühen, gibt es hier die bereits etablierte und akzeptierte Lösungen. Es wird aber umso deutlicher, dass nach wie vor objektive Sicherheit und subjektive Wahrnehmung bei vielen Nutzern nicht übereinstimmen und besonders sensible Daten nur ungern über das weltweite Datennetz versendet werden.
- Große Unsicherheiten entstehen schließlich auch bei solchen Applikationen, die den Download und die Ausführung zusätzlicher Programme erfordern. Diese könnten – für den Laien in seinen Folgen kaum abschätzbar – nicht nur Viren oder anderweitig schädliche Programme enthalten, sondern auch bei in sich einwandfreier Programmqualität durch Inkompatibilitäten mit bestehenden Programmen das System des Nutzers lahm legen *[2]*. So treffen auch vielfach gerade jene Programme, die die Applikation über integrierte Sicherheitsmechanismen schützen sollen, bei der erstmaligen Ausführung auf große Skepsis.

Es sind also individuelle Handlungssituationen und Unsicherheiten, die das Nutzungsverhalten jeweils spezifisch beeinflussen. Sie können zu jedem Zeitpunkt auf das Kalkül des Nutzers einwirken, bis dieser die Nutzung schließlich verweigert.

Einstellung: IT-Sicherheit als »Hygienefaktor« der Nutzungsentscheidung

In der Analyse der relevanten Handlungssituationen fällt auf, dass die Aspekte der »Sicherheit« resp. der »IT-Sicherheit« zu keinem Zeitpunkt positiv in das Kalkül um die Nutzung der Systeme eingehen. Die Argumentation dreht sich immer um die potenziellen Risiken der digitalen Alternative, z.B. im Vergleich mit der anonymen und aus Datenschutzsicht unkritischen Alternative der Barzahlung in physischen Verkaufsstellen. Die IT-Sicherheit zählt damit zu den sog. »Hygienefaktoren«, die sich dadurch aus-

zeichnen, dass sie zwar negativ auf Kaufentscheidungen einwirken und diese sogar letztlich verhindern können, niemals jedoch einen absolut positiven Beitrag liefern. Dieses bedeutet einerseits, dass die Vorteilhaftigkeit der digitalen Alternative aus anderen als aus Sicherheitsaspekten herleitbar sein muss, aber andererseits auch, dass subjektiv fehlende Sicherheit die Akzeptanz eines Angebots wesentlich einschränken kann. Ferner muss konstatiert werden, dass technische Maßnahmen zur Verbesserung der IT-Sicherheit nur einen Beitrag zur Erhöhung dieses subjektiven Sicherheitsgefühls leisten können. Technische Lösungen können nur im Kontext eines integrierten Sicherheitskonzepts zur Geltung kommen, zumal sie überwiegend auch für den Nutzer sichtbar werden und dessen Akzeptanz erfordern.

In der Wahrnehmung der Nutzer taucht das Thema »IT-Sicherheit« nämlich auch immer dann auf, wenn:

- die Sicherheitsmechanismen nur unter Mitwirkung der Nutzer realisiert werden können. Aktuelle Sicherheitskonzepte basieren z.B. auf der Installation eines speziellen Programms auf dem System des Nutzers, sie bedürfen teilweise zusätzlicher Komponenten wie dem Kartenleser beim HBCI-Banking oder bei der digitalen Signatur oder sie verlangen die erstmalige Registrierung und Authentifizierung des Nutzers in einer Bankfiliale oder bei anderen autorisierten Stellen. Selbst wenn der Nutzer nicht allzu sensibel gegenüber möglichen Sicherheitsmängeln ist, hat er sich mit der Handhabung der Sicherheitstechnologien zumeist intensiv auseinander zu setzen.

Die Handhabbarkeit der Sicherheitslösung ist damit ein zweiter wesentlicher Hygienefaktor bei der akzeptanzorientierten Planung von Sicherheitskonzepten. Wie zuvor schon für die IT-Sicherheit selbst hergeleitet, kann auch eine einfache Handhabung derselben keinen Mehrwert für den Nutzer bieten, wohl aber den potenziellen Kunden und Nutzer verleiden und von der adäquaten Nutzung des Angebots abhalten.

Informationen, insbesondere Schlüsselinformationen im Kaufprozess

Die Analyse der relevanten Handlungssituationen hat gezeigt, dass die »Sicherheit« vor allem als Unsicherheit wahrgenommen und als Risiko in das Kalkül eingeht. Auf wahrgenommenes Risiko wiederum reagieren die Nutzer, indem sie dieses entweder unmittelbar in die Kalkulation einbeziehen oder durch zusätzliche Informationssuche zu reduzieren versuchen. Je weniger verlässliche Information die Nutzer dann unmittelbar erhalten bzw. je größer der Aufwand zur Beschaffung weiterer Informationen ist, desto eher geht die Unsicherheit als negative Bewertung in das Kalkül ein.

Bei der Analyse der in kritischen Situationen zur IT-Sicherheit des Anbieters und der spezifischen Applikation bereitgestellten Informationen wird häufig erkennbar, wie weit die Anbietersicht und die der potenziellen Nachfrager auseinanderliegen können. Technische Informationen wie der Hinweis auf eine »128-bit SSL-Verschlüsselung« bei der Datenübertragung, mehrseitige Datenschutzbestimmungen, die gesondert aufgerufen werden sollen

oder Zertifizierungen, die ihrerseits neu sind und z.T. von ebenso unbekannten wie kleinen Anbietern vergeben bzw. die auch von großen Anbietern unter neuem Namen gelauncht werden, signalisieren dem Spezialisten eine vertrauenswürdige Architektur, sind aber für den »technischen Laien« vielfach nichtssagend und mitunter gar verwirrend. Hier setzt sich in der Praxis erst allmählich die Erkenntnis durch, dass die beschriebene Sicherheit für den Kunden erst dann Wert erhält, wenn der Anbieter diese, z.B. über entsprechende Gestaltung der Geschäftsbedingungen absichert, also z.B. subjektiv darüber hinausgehende Risiken übernimmt oder wenn leistungsfähige und bekannte Institutionen mit ihrem Namen als Zertifizierer und Dienstleister (z.B. in einer Treuhänderfunktion) agieren. Auch aus Kunden- oder Nutzersicht gibt es allerdings noch keine Verfahren, die als Marktstandard etabliert sind und entsprechend kommunikativ vermarktet werden können.

Gerade in der Konzeption und Kommunikation zur IT-Sicherheit zeigen sich jenseits der technologischen Ausgestaltung große Potenziale zur Optimierung im Sinne der Akzeptanzsteigerung.

9.1.3 Konsequenzen für die akzeptanzorientierte Konzeption von IT-Sicherheit

Die vorangegangenen Ausführungen haben gezeigt, dass sich die objektive, zumeist technisch determinierte IT-Sicherheit signifikant von der subjektiven Wahrnehmung der Nutzer unterscheiden kann. Diese sind nicht grundsätzlich kritisch, erleben aber situativ Unsicherheit insbesondere bezüglich der unbefugten Nutzung ihrer persönlichen Daten. Der Anbieter muss dem begegnen. Die IT-Sicherheit ist ebenso wie die Nutzerfreundlichkeit ein Hygienefaktor der Kaufentscheidung. Sicherheit ist eine notwendige, aber keine hinreichende Bedingung für die Akzeptanz von E- und M-Commerce-Applikationen.

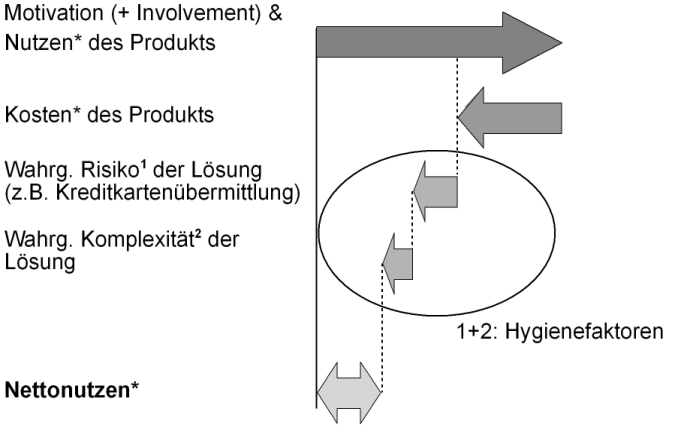


Abbildung 9.5: Wahrgenommene Unsicherheit und Komplexität als Hygienefaktoren der IT-Nutzung

Zur Lösung des Problems bedarf es zwar grundsätzlich der technischen Lösung, handlungsentscheidend sind aber die verbleibende subjektive Wahrnehmung der (Un-)Sicherheit sowie die wahrgenommene Komplexität der Prozesse zur Sicherstellung des angestrebten Sicherheitsstandards. Hier bieten sich entsprechend technische, organisatorische und kommunikative Lösungsansätze an.

9.2 Lösungsansätze mit Praxisbeispielen

Die vorangegangenen Ausführungen haben schon erkennen lassen, dass es keine Standardlösung für das vorgestellte Sicherheits- und Wahrnehmungsproblem gibt. Nachfolgend sollen deshalb zunächst die wesentlichen Handlungsmöglichkeiten anhand von Praxisbeispielen aufgezeigt und daraufhin eine Handlungsempfehlung zur Ermittlung der optimalen Strategie abgeleitet werden.

Die Handlungsalternativen für akzeptanzorientierte IT-Sicherheitskonzepte setzen konsequent an den in Abb. 9.6 aufgezeigten Handlungsfeldern an. Es gilt,

- sowohl das Risiko
- als auch Komplexität des Nutzungsprozesses zu reduzieren.

In jeder dieser beiden Ausprägungen gibt es wiederum zwei verschiedene Möglichkeiten, nämlich:

- das Problem konzeptionell zu lösen, also die Optimierung in der Applikation und der begleitenden Sicherheitslösung anzustreben und/oder
- unabhängig von der tatsächlichen Lösung die Wahrnehmung des Kunden zu beeinflussen und zu verändern, also kommunikativ vorzugehen.

Zusammen ergeben sich die nachfolgend aufgezeigten vier Handlungsfelder, in denen einzeln oder kombiniert an der Akzeptanzsteigerung von Sicherheitskonzepten durch die Nutzer gearbeitet werden kann.

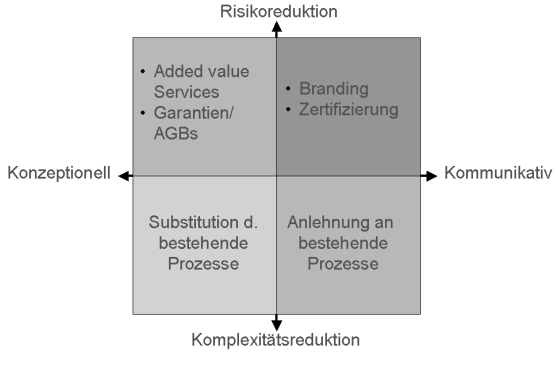


Abbildung 9.6: Handlungsrahmen zur Akzeptanzsteigerung in der IT-Sicherheit

Nachfolgend sollen die vier Felder erläutert und die entsprechenden Ansätze mit Beispielen belegt werden.

9.2.1 Konzeptionelle Ansätze

Die technische Lösung zur Sicherstellung einer objektiven Sicherung der Systeme und Applikationen bildet immer die Basis der IT-Sicherheit, sie ist aber nur bedingt relevant für die Handlung des Nutzers. Gleichwohl bieten sich konzeptionelle Möglichkeiten zur Verbesserung des wahrgenommenen Nutzen-/Kosten-Verhältnisses, also solche, die mitunter direkt auf die Gestaltung der Strukturen und Prozesse einwirken, an.

Konzeptionelle Ansätze zur Risikoreduktion

Konzeptionelle Optimierungen können gleichermaßen auf der Nutzen- wie auf der Kosten-, resp. Risikoseite ansetzen. Im ersten Fall soll durch Added Value Services bei unverändertem Risiko der Nutzen erhöht und damit der subjektive Risikoanteil für den spezifischen Anwendungsfall reduziert werden, im zweiten Fall erfolgt eine tatsächliche Risikoreduktion, indem der Anbieter durch Garantien oder die entsprechende Ausgestaltung seiner Applikation sowie der rechtlichen Grundlagen (AGBs) das Risiko für den Nutzer limitiert.

Added Value Services. Der Added Value-Ansatz verspricht dem Nutzer mit dem einen kritischen Prozess, im Umfeld der IT-Sicherheit also z.B. mit der Registrierung oder mit dem Download einer Payment-Applikation einen Zusatznutzen, der über die Kernapplikation hinausgeht und im subjektiven Kalkül zusätzlich auf der Haben-Seite verbucht werden kann. Wenn also bis dahin der erkennbare Nutzen das wahrgenommene Risiko oder die erwartete Komplexität noch nicht gerechtfertigt hat, soll dieser zusätzliche Beitrag das Kundenvotum nun positiv beeinflussen. Added Value Services setzen damit nicht bei der Reduzierung der Hygienefaktoren an, sondern fügen Motivatoren hinzu.

Dieser Motivator kann im einfachsten Fall ein einzelner unmittelbarer Anreiz z.B. in Form einer Gutschrift, eines Rabattes oder eines Geschenks sein. So versucht z.B. »amazon.de« derzeit (Stand 9/2002) aus Besuchern Käufer zu machen, indem jedem Besucher, der sich bei Amazon registriert, fünf Euro für den ersten Einkauf gutgeschrieben werden. Ähnliche Rabattierungen und Gutschriften gibt es auch bei diversen Payment-Anbietern, wie z.B. bei »paybox«, also überall dort, wo die initiale Nutzung oder Registrierung die zentrale zu überwindende Hürde für die Nutzung darstellt und nach der Registrierung die Prozesse weitestgehend vereinfacht und in der subjektiven Wahrnehmung risikoarm sind. Im Beispielfall »Amazon« kann der Nutzer nach der aufwändigeren ersten Registrierung per »One Click« Waren bestellen und liefern lassen.

Einzelne monetäre und nicht-monetäre Anreize sind aber nur dort sinnvoll, wo ohnehin mit einer engen Kundenbindung gerechnet werden kann. In anderen Fällen bietet es sich an, solche Added Value Services zu konzipieren

und anzubieten, die den Kunden immer wieder zur Nutzung animieren. Dieses können Marktinformationen im Umfeld des Online-Banking (Consors u.a.) oder breiter Content für das Micropayment (z.B. Firstbuy) sein, der dann in sog. Service-Portalen zusammen gefasst werden kann. Im letztgenannten Fall ergeben sich unmittelbare Folgen auch für die technische Realisierung des Sicherheitskonzepts.

Wenngleich also die Sicherheit als Hygienefaktor keinen positiven Beitrag zum Nutzenkalkül des Kunden bieten kann, lassen sich diese über Added Value Services motivieren, die Sicherheitsbedenken bei der Nutzung der IT-Systeme zumindest anders zu bewerten. Dieses Kosten-/Nutzen-Verhältnis lässt sich natürlich auch verbessern, indem das Risiko für den Nutzer und Kunden tatsächlich begrenzt wird.

Risikobegrenzung durch Garantien o.ä. In jenen Fällen, in denen die tatsächliche objektive Sicherheit der IT-Lösung die der subjektiven Wahrnehmung der potenziellen Nutzer deutlich übertrifft und die Komplexität der Materie eine Angleichung über einen einfachen Kommunikations- und Lernprozess nicht zulässt, bietet es sich an, das tatsächlich niedrige Risiko auch konzeptionell zum Ausdruck zu bringen. Der Anbieter übernimmt in diesem Fall die vermeintliche Differenz zwischen objektiver Sicherheit und subjektiver Wahrnehmung, in dem er z.B. an Stelle von technischen Hinweisen wie »SSL (Secure Socket Layer)-Verschlüsselung« Garantien bezüglich der Sicherheit der Datenübertragung oder der Datenhaltung abgibt und den Kunden damit von erwarteten Folgerisiken freistellt. Die Verbindung zum IT-Sicherheitskonzept ist dabei unübersehbar. Der Anbieter kann natürlich nur die Sicherheit ernsthaft garantieren, die er mit seinen Systemen selbst beeinflussen und sicherstellen kann.

Beispiele für solche Garantien finden sich besonders bei den E-Commerce-Ablegern klassischer Handels- und vor allem Versandhandelsunternehmen. Diese sind es gewohnt, den Kunden von den Risiken der speziellen Distributionsform zu entbinden (vereinfachtes Umtauschrecht im Fernabsatz etc.) und die Folgekosten genauestens zu kalkulieren und sie übertragen diesen Ansatz jetzt konsequent und erfolgreich auf das E-Business.

Garantien und andere Selbstverpflichtungen sind dabei einfach zu kommunizieren, die möglichen Konsequenzen für den Anbieter sind aber nicht zu unterschätzen und bedürfen einer genauen Planung. Der Anbieter muss sich bei seinen Zusagen auf die aus Nutzersicht subjektive Komponente der Risikowahrnehmung beschränken und er muss die Folgekosten solcher Risikoübernahmen auf der Basis eines fundierten Sicherheitskonzeptes abschätzen können. Wo dieses nicht möglich ist, bieten sich allenfalls kommunikative Ansätze zur Risikoreduzierung. Die sind jedoch weitaus weniger planbar und nur vordergründig einfacher als die konzeptionellen Vorgehensweisen.

Konzeptionelle Ansätze zur Komplexitätsreduktion

Wie zuvor gezeigt, ist die Komplexität einer Applikation nicht nur selbst eine Behinderung für den Nutzer, Komplexität vermittelt in Verbindung mit sicherheitsrelevanten Prozessen auch ein entsprechend hohes Risiko. Je

komplexer die Sicherheitsmaßnahmen, desto risikobehafteter erscheint offensichtlich die Applikation.

Bei der Konzeption von IT-Sicherheitskonzepten mit Schnittstellen zu zufälligen Nutzern und potenziellen Kunden gilt es deshalb, die Komplexität der Prozesse weitestgehend zu reduzieren. Dieses kann geschehen, indem entweder die Prozesse der Applikation den Denkmustern der Nutzer angepasst oder Teile des Prozesses von der Nutzerschnittstelle in das Backoffice verlegt und damit aus Nutzersicht substituiert werden.

Nutzerfreundlichkeit. Die Komplexität einer Handlungssituation ergibt sich aus verschiedenen exogenen und endogenen Einflussfaktoren. Neben der Anzahl der zu berücksichtigenden Handlungsparameter und der Festlegung des Prozesses sind dieses vor allem das Wissen und die Vorbildung des Nutzers sowie dessen kognitive Fähigkeiten. Je mehr nachvollziehbare Verbindungen sich zu bisherigen Erfahrungen herstellen lassen und je weniger Überraschungen die Applikation bereithält, im Fachjargon spricht man hier von kognitiven Dissonanzen, desto weniger komplex und risikobehaftet erscheint die Lösung.

Zur Ausgestaltung der Nutzerfreundlichkeit einer Applikation existieren dabei ganze Studien und Bücher. Sie soll hier bis auf die Wiedergabe weniger Leitsätze nicht weiter detailliert werden. Als grundsätzlicher Anspruch sei genannt:

- Die auf Kundenseite notwendigen Schritte sollten bekannten Prozessen und Handlungsmustern folgen und jeweils Ziel und Fortschritt erkennen lassen. Der Nutzer stellt bei jedem Handlungsschritt das Weitergehen in Frage, wenn er dem Ziel nicht näher kommt.
- Das Prozessdesign muss die Wissensbasis der Nutzer berücksichtigen. Je mehr Assoziationen zu gelerntem und verarbeitetem Wissen bestehen, desto reibungsloser fügt sich die neue Applikation ein und umso schneller begreift der Nutzer die Handhabung.
- Besonders komplexe Zusammenhänge lassen sich einfacher graphisch als textlich erfassen, mithin sollte im Sinne der Vermittelbarkeit Multimedialität angestrebt werden.

Mit der Akzeptanzorientierung hält damit auch die Nutzerfreundlichkeit (Usability) Einzug in das Sicherheitskonzept. Dabei ist sicherzustellen, dass Aufwand (Komplexität und Kosten) und Nutzen (Sicherheit) in einem vernünftigen und vertretbaren Verhältnis zueinander stehen.

Substitution von kundenseitigen Prozessen . Bei der Konzeption von IT-Sicherheitskonzepten mit Schnittstellen zu zufälligen Nutzern und potenziellen Kunden gilt es, die Komplexität der Prozesse weitestgehend zu reduzieren. Dieses kann z.B. auch geschehen, indem Teile des Prozesses von der Nutzerschnittstelle in das Backoffice verlegt und damit in die Verantwortung des Anbieters übernommen werden. Auch hier agieren die klassischen Versandhandelsunternehmen beispielhaft, wenn sie mit automatischen

Plausibilitätsprüfungen (z.B. bei der Adressenabfrage) den Kunden von der Authentifizierung (zur Sicherstellung der Integrität der Daten) freistellen und sogar Rechtschreibfehler ausgleichen.

Auf die IT-Sicherheit digitaler Lösungen übertragen heißt das, dass der Kunde an der Benutzerschnittstelle und in seinem Beitrag zum Sicherungsprozess entlastet wird, der Anbieter diese Unsicherheit aber z.B. durch die Vernetzung mit anderen Datenbanken und Dienstleistern wieder ausgleicht. Die wahrnehmbare Reduzierung der Komplexität und der damit assoziierten Unsicherheiten auf Nutzerseite intendiert damit u.U. sogar eine objektive Verschlechterung der IT-Sicherheit, wenn das Substitut nicht die Qualität eines komplexen Sicherungsverfahrens, z.B. durch Authentifizierung am Bank- oder Postschalter, erfüllt. Um dieses überhaupt abschätzen zu können, ist es auch hier notwendig, in einem integrierten IT-Sicherheitskonzept die Anforderungen an interne und externe Prozesse und Datenbanken eindeutig zu fixieren und laufend zu überprüfen.

Beispielhaft kann das Mobile Payment für das E- und M-Commence angeführt werden. Die Ausführung der Bezahlfunktion ist nach wie vor einer der kritischsten Momente bei der Nutzung internetbasierter und mobiler Anwendungen. Zu heterogen sind die vielfach kartenbasierten Bezahlsysteme, zu komplex die Registrierung vor allem für überschaubare Dienstleistungen im Micropayment, zu unbekannt teilweise aber auch die Anbieter der Lösungen, als dass der Kunde subjektiv einfach und sicher eine Bezahl-Transaktion durchführen könnte.

Das Bezahlen mit dem Mobiltelefon kann sich deshalb zu einer echten Alternative zu den karten-basierten Verfahren elektronischen Bezahlens entwickeln. Da das Mobiltelefon zum einen in den Kernzielgruppen der E- und M-Commerce-Anbieter quasi flächendeckend verbreitet und akzeptiert ist und zum anderen ein maßgeblicher Teil der Mobilfunknutzer bereits seine Identität gegenüber den Mobilfunkanbieter verifiziert hat, ist eine zusätzliche Registrierung vermeidbar. Die SIM-Karte kann die Geld- oder Kreditkarte ersetzen und die Authentifizierung kann sich auf die Zuordnung des Bedieners zum Telefon, beispielsweise durch Abfrage einer Geheimzahl beschränken. Sicherheit und Bedienerfreundlichkeit sind optimal vereinbar, was sich auch in der grundsätzlichen Akzeptanz dieser Art des Bezahlens seitens der potentiellen Nutzer bestätigt *[3]*.

Noch gelten zwar in der Branche die proprietären Services der einzelnen Provider – aktuell zum Beispiel die MultiMedia Services (MMS) – als ein zentrales Kundengewinnungs- und Kundenbindungsinstrument, weshalb Offenheit und Interoperabilität, also der Zugriff auf und die Nutzung von Daten und Diensten anderer Provider und eben auch eine übergreifende Bezahlfunktion vermieden wird, aber hier scheint ein Umdenken stattzufinden und Interoperabilität scheint das erklärte Ziel zu sein.

Interoperabilität bedeutet dabei:

- Gleiches Handling für Kunden unterschiedlicher Mobilfunkanbieter

- Contentlieferanten und Händler können ihre Inhalte über einen einzigen Partner in verschiedene Portale und Netzwerke einbringen
- Die Operator können völlig neue Services wie das »Person-to-Person-Payment«, zum Beispiel bei Online Auktionen, anbieten

Die Betreiber des Online-Business bekommen jetzt die Möglichkeit, mit nur einem Partner ein interoperables, flexibles und sicheres Online-Bezahlsystem einzuführen und zu nutzen, da der Sicherheitslevel der Telekommunikationsunternehmen in den meisten Fällen ausreichend sein dürfte, die Sicherheitsanforderungen, z.B. von E-Commerce-Anbietern zu erfüllen. Dass dieser Abgleich zwischen Datenbasis und Sicherheitskonzept notwendige Voraussetzungen für den vorgestellten Ansatz ist, haben wir vorab erläutert.

9.2.2 Kommunikative Ansätze

Kommunikative Ansätze zur Risikoreduktion

Ist die subjektive Risikowahrnehmung der Nutzer zu hoch und soll oder kann das tatsächliche Kosten-/Nutzenverhältnis nicht gebessert werden, so bleibt immer noch die Möglichkeit der kommunikativen Beeinflussung. Die Wahrnehmung des (potenziellen) Nutzers soll über Informationen, resp. Schlüsselinformationen risiko- bzw. komplexitätsmindernd beeinflusst werden. Dabei ist es im Übrigen weitestgehend unerheblich, wie sicher die Anwendung tatsächlich ist. Kommunikativ ist es vielmehr möglich und vielfach angestrebt, das wahrgenommene Restrisiko einer IT-Sicherheitslösung unabhängig vom tatsächlichen Risiko zu machen. Die Kommunikation ist damit auch unabhängig von der tatsächlichen technischen Lösung und basiert allein auf vertrauensbildenden Maßnahmen z.B. durch Nutzung einer starken Marke oder durch Zertifizierung.

Vertrauensbildung durch Branding. Die eingangs gemachten Ausführungen zum Konsumenten- und Nutzerverhalten haben gezeigt, dass wahrgenommenes Risiko bevorzugt über Schlüsselinformationen reduziert wird, um der Komplexität des vollständigen Entscheidungsprozesses zu entgehen. In diesem Zusammenhang zählen vor allem die Meinungen und persönlichen Erfahrungen im sozialen Umfeld des Konsumenten. In den Fällen, in denen diese unmittelbaren Erfahrungen nicht zur Verfügung stehen, füllen die Einstellungen zu Unternehmen und Marken häufig diese Wissens- und Erfahrungslücke aus. Ein starkes Unternehmen, das hinter dem System steht, resp. das System nutzt, signalisiert dem Nutzer Verlässlichkeit und Nachhaltigkeit.

Ganz im Gegensatz dazu stand zunächst das Verhalten der Marktteilnehmer im E-Commerce. Einerseits drängten, bedingt durch die Geschwindigkeit der Entwicklungen im Internet, zunächst kleine Start-up-Unternehmen mit innovativen Lösungen in den Markt und andererseits wollten die etablierten Player ihre Marken durch die Experimente im Internet nicht schwächen und launchten deshalb ihre entsprechenden Initiativen unter neuen Namen. Erst

in der jüngeren Vergangenheit ist ein Umdenken zu beobachten und die Online-Aktivitäten werden – wo möglich – unter das starke Markendach des klassischen Geschäfts gezogen. Beispielhaft sei die Deutsche Bank genannt.

Bei der akzeptanzorientierten Konzeption von IT-Sicherheitslösungen ist dieser Aspekt zu berücksichtigen, wenn es um die Auswahl der Komponenten und Partner geht. Es kann aus Akzeptanzgründen Sinn machen, der sichersten oder einfachsten oder preiswertesten Lösung eine solche mit hinreichender Sicherheit vorzuziehen, wenn die letztgenannte mit einem starken Namen verknüpft ist und in entsprechendem Maße Vertrauen transportiert. Für ein solches Branding bieten sich z.B. in hervorragender Weise Banken und Versicherungen an, während die IT-Anbieter nur unter Ihresgleichen einen Ruf transportieren. Dieses funktioniert allerdings nur, wenn eine glaubhafte Verbindung hergestellt werden kann, das Unternehmen also einen Teil der Lösung beisteuert oder diese zumindest selbst nutzt.

Lässt die Lösung keinen partnerschaftlichen Ansatz mit einem entsprechenden Unternehmen zu, bietet sich immer noch die Möglichkeit der Zertifizierung durch ein solches an.

Zertifizierung/Gütesiegel. Der normale Nutzer oder Kunde ist gar nicht in der Lage, die Sicherheit einer IT-Lösung in den für ihn relevanten Dimensionen zu bewerten. Es fehlt an Methoden, Referenzen, Prüfverfahren etc. Genau diese Lücke wollen jene Unternehmen schließen, die über solches Know-how sowie solche Verfahren verfügen und die die Ergebnisse als Zertifikate oder Gütesiegel, wie z.B. das »Trusted Shop«-Siegel ausweisen. Für den Nutzer soll die professionelle Bewertung eigene Bewertungsversuche ersetzen. Vergleichbar der »TÜV-Plakette« verspricht die positive Bewertung ein definiertes Mindestmaß an Sicherheit.

Unabhängig von der tatsächlichen Professionalität der Überprüfung, ist der Effekt aus Sicht der Nutzerakzeptanz allerdings fraglich, solange es in diesem Umfeld bisher weder spezifizierte Sicherheitslevel noch definierte Verfahren gibt. Der potenzielle Kunde kann die Aussage eines Gütesiegels ebensowenig einschätzen, wie die Sicherheitslösung selbst. Gleichwohl gilt es im Rahmen eines ganzheitlichen und akzeptanzorientierten Sicherheitskonzepts etwaige Standardisierungstendenzen und mögliche Zertifizierungen im Auge zu behalten, um mit der eigenen Lösung auch dem Regelwerk zu entsprechen und bei weiterer Verbreitung der Gütekriterien durch Kompatibilität einen einfachen Zertifizierungsprozess zu erreichen.

Kommunikativer Ansatz zur Komplexitätsreduktion

Interne und regelmäßige Nutzer eines Systems können i.d.R. in der Handhabung des Systems und der Sicherheitsmechanismen geschult werden. Für diese macht es zudem Sinn, sich auch mit komplexen und wechselnden Passwörtern zu beschäftigen, da sie die Systeme weit häufiger nutzen. Externe Kunden werden sich dagegen aus den genannten Überlegungen zur angestrebten Vereinfachung der Handlungsentscheidungen weit weniger Mühe geben, ein komplexes System zu verstehen und zu erlernen.

Hier ist es dennoch mit den klassischen Mitteln der Werbung möglich, Verhaltensänderungen zu erzielen. Wenn der Prozess nicht weiter den Erwartungen der potenziellen Kunden angepasst werden kann, kann durch periodische Vermittlung ggf. die Wahrnehmung beeinflusst werden. Dem Kunden kann dazu über verschiedene Medien die Handhabung des Systems so häufig und so lange erklärt werden, bis dieser den Ablauf des Prozesses verinnerlicht hat und im Bedarfsfall anzuwenden in der Lage ist. Diese Vorgehensweise möchte ich mit einem völlig untypischen und der IT fernen Beispiel belegen.

Vor einigen Jahren brachte Mike Krüger, ein deutscher Entertainer, ein Gauklerlied heraus, dass im Refrain auf eine komplexe Bedienungsfolge verwies. Diese lautete: »Sie müssen nur den Nippel durch die Lasche zieh´n und mit der kleinen Kurbel ganz nach oben dreh´n. Dort erscheint sofort ein Knopf und da drücken Sie dann drauf und schon..«. Dann sollte genau das passieren, was der Protagonist, also z.B. ein Fallschirmspringer in freien Fall, unmittelbar erreichen wollte. Im Lied war es jeweils zu spät, wenn der Protagonist die Anleitung verstanden hatte und umsetzen wollte. Hatte man das Lied jedoch ausreichend oft gehört, war die Handlungsfolge klar und die Komplexität der Bedienung – der Lacheffekt im obigen Beispiel – subjektiv reduziert.

Die Systematik eines Sicherheitskonzepts wird sich in den wenigsten Fällen für einen Werbefeldzug eignen, aber wenn z.B. ein neues Produkt werblich gelauncht wird, mag es eine Option sein, den Prozess verständlich aufzubereiten und in die Werbung einfließen zu lassen.

9.2.3 Methode zur Ermittlung des optimalen nutzerorientierten Sicherheitskonzepts

Für die Entwicklung eines integrierten Sicherheitskonzepts gibt es unter Akzeptanz-Gesichtspunkten keine vollständig neue Methodik. Nach wie vor muss zunächst der objektive Sicherheitsbedarf ermittelt und mit den entsprechenden Strukturen und Prozessen fixiert werden. Hinzu kommt dann allerdings die Analyse und Bewertung der zukünftigen Nutzer bezüglich ihrer Risikowahrnehmung. Je nach Konstellation zwischen subjektiver und objektiver Sicherheit gilt es dann, die ursprüngliche Konzeption anzupassen, bis sich bei hinreichender Sicherheit die geforderte Nutzerakzeptanz ergibt. Dabei sind alle vier Handlungsfelder einzubeziehen, aber grundsätzlich gilt:

- Je mehr die Unsicherheiten aus dem Prozess heraus entstehen, desto eher sollten konzeptionelle Ansätze gewählt werden, um den Kunden resp. Nutzer nachhaltig zu entlasten
- Je größer die Differenz zwischen wahrgenommenem und tatsächlichem Risiko, desto mehr Potenzial bietet sich für kommunikative Maßnahmen
- Die Nutzerfreundlichkeit ist in allen Ausprägungen ausdrücklich zu berücksichtigen

In der Praxis ergibt sich deshalb zumeist die nachfolgende Vorgehensweise:

- Entwicklung der originären Konzeption zur IT-Sicherheit (aus Innensicht)
- Evaluation der Nutzerakzeptanz
- Prüfung der konzeptionellen Möglichkeiten zur Verbesserung der Nutzerakzeptanz
- Werbliche Begleitung

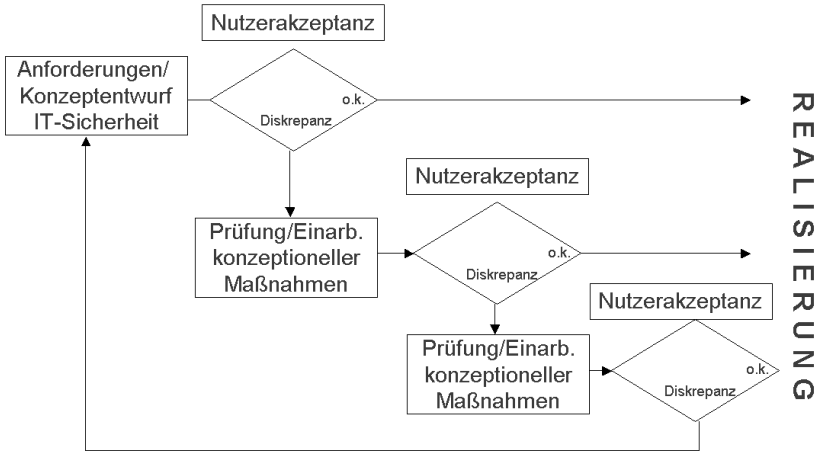


Abbildung 9.7: Methode zur Entwicklung eines kundenakzeptierten IT-Sicherheitskonzepts

Dabei zeigt sich immer wieder, dass aus der Innensicht hervorragende Lösungen aus Nutzersicht nur schwer nachvollziehbar sind und die Akzeptanz nachhaltig negativ beeinflussen. In Applikationen mit hohem externen Nutzeranteil und entsprechend hohem Akzeptanzbedarf gehen die Evaluation der Zielgruppen und deren Anforderungen deshalb immer häufiger direkt in die ersten Konzeptentwürfe zur IT-Sicherheit ein, was den weiteren Entwicklungsprozess deutlich fördern kann.

9.3 Zusammenfassung/Fazit

IT-Sicherheit wird gemeinhin mit dem Schutz von IT-Systemen vor Missbrauch, Manipulation und Zerstörung gleichgesetzt. Es dominiert eine Innensicht, in der jeder externe Zugriff eine potenzielle Bedrohung darstellt und komplexe Verfahren dort, wo der Zugriff von außen gewünscht ist, eine hinreichende Absicherung bieten.

Aus der Außenperspektive ergeben sich bei der Nutzung dieser gesicherten Systeme jedoch mitunter zwei andersartige und dennoch ebenso bedeutsame Problemstellungen. Zum einen bezieht sich die Angst vor Missbrauch, Manipulation und Zerstörung nicht mehr auf die Seite des Anbieters, sondern auf das eigene System und mehr noch auf die eigenen persönlichen Daten und zum anderen intendieren die teilweise äußerst komplexen Ver-

fahren der Anbieter zur Sicherung ihrer Infrastruktur eher weitere Unsicherheiten bezüglich der richtigen Handhabung und der tatsächlichen Sicherheit der angebotenen Applikation. Je mehr der Nutzer für die Sicherheit tun muss, desto mehr wird ihm bewusst, welche Risiken mit der Applikation verbunden sind. Die wahrgenommenen (und nicht mehr die realen) Unsicherheiten gehen dann unmittelbar in das Handlungskalkül des Nutzers ein, der je nach Risikofreudigkeit die Nutzung früher oder später verweigert. In diversen Studien wird die (Un-) Sicherheit immer wieder als zentrales Hemmnis für die Nutzung des E-und M-Commerce genannt.

Der Anbieter sollte diesem Umstand bereits bei der Konzeption der IT-Sicherheit entgegen wirken und die Nutzeranforderungen resp. die Nutzerakzeptanz berücksichtigen, um Risiko und Komplexität tatsächlich oder auch nur in der Wahrnehmung des Nutzers oder potenziellen Kunden zu beeinflussen. Ein umfassendes IT-Sicherheitskonzept liefert die Basis für die entsprechenden Überlegungen und Kalkulationen und es profitiert von den entsprechenden nutzerseitigen Implikationen, denn auch die Kosten-Nutzen-Relation für die Sicherheitssysteme verbessert sich mit der verbesserten Nutzerakzeptanz und einer intensiveren Nutzung.

Literaturangaben: *[1]* Vereinfachend sollen nachfolgend »Kunden« und »Nutzer« gleichgesetzt werden und diejenigen bezeichnen, die das System, z.B. einen Online-Shop, benutzen wollen. Anbieter sind demgegenüber die Shop-Betreiber, also diejenigen, welche die tatsächliche Sicherheitstechnik zur Verfügung stellen und die i.d.R. auch den rechtlichen Rahmen bestimmen, in dem Online-Geschäfte ablaufen. So bezieht sich der Artikel zumeist auf die Konstellation des E- und M-Commerce, wenngleich die grundsätzlichen Erkenntnisse auch auf andere Fälle übertragbar sind. Die Bezeichnungen »Kunde«, »Konsument« etc. soll dabei selbstverständlich auch die weibliche Ausprägung einschließen.

[2] Zur Zeit wird z.B. eine intensive Diskussion um sog. Dialer geführt, die das System des Nutzers nach einem unbeabsichtigten Download selbständig so konfigurieren, dass die Einwahl in das Internet fortan über besonders teure Mehrwertrufnummern geführt wird.

[3] In der aktuellen Mobinet-Studie (Nr. 4) der Unternehmensberatung A.T. Kearney gaben 44 Prozent der weltweit befragten Mobilfunknutzer an, ihr Handy prinzipiell auch zum Bezahlen einsetzen zu wollen, wobei sich zuvor immerhin 40 Prozent der Nutzer der grundsätzlichen Möglichkeit einer Zahlungsfunktion im Mobiltelefon bewusst waren.

Weitere Literaturangaben: Kroeber-Riel, W./Weinberg, Peter
Konsumentenverhalten, München 1999

Merz, M.
E- Commerce und E- Business. Marktmodelle, Anwendungen und Technologien, Heidelberg 2001

Cole, T./Gromball, P.
Das Kunden-Kartell, München 2000

10 Scheinbar sicher – Eine Zusammenfassung von Ergebnissen aktueller Befragungen und Expertengespräche

Ulrich Falke

Die Szenarien und Schlüsse, die sich aus den aktuellen Studien zum Thema IT-Sicherheit in Unternehmen und Organisationen entwickeln lassen, wären als beruhigende Bettlektüre kaum geeignet. Auch dürften sie so manche Führungskräfte und DV-Leiter, wenn nicht schlaflose Nächte bereiten, so aber aus dem Gefühl vermeintlicher Unverwundbarkeit herausreißen – oder aber, sie umgekehrt in ihren Befürchtungen und Ahnungen stärken und bestätigen. Im internationalen Vergleich jedenfalls sieht die Situation im Bundesgebiet nicht gerade rosig aus. Zwar ist, so die EDS/IDC-Studie – eine der drei nachfolgend zitierten Analysen – in deutschen Unternehmen das Sicherheitsbewusstsein am höchsten, tatsächlich wähnen sich die Verantwortlichen aber oft »in (falscher) Sicherheit«. Und: »Deutsche Top-Manager verschlafen gerade die zunehmende Bedeutung von strategischer Sicherheitsplanung«.

10.1 Zur Einstimmung

Monokulturen sind anfällig und die Produktion nur eines einziges Erzeugnisses birgt auf einem von schwankender Nachfrage bestimmten Markt ein erhöhtes Risiko. Bei Krankheiten und Ausfällen ist zudem auf einen Schlag der gesamte Bestand und damit die ganze wirtschaftliche Grundlage gefährdet – das wurde mir schon früh während meiner regelmäßigen Aufenthalte in einer Bauernfamilie beigebracht. Neben den schönen Ferienerlebnissen als Stadtkind auf dem Lande gehört die Erinnerung an diese einleuchtende und leicht verständliche Erkenntnis zu den sich mir tief eingeprägten Regeln der wirtschaftlichen Vernunft. Inzwischen hat sich der Sohn und Erbfolger, den ich früher immer beim Beackern der Felder begleitet hatte, gelernter Agrarökonom, Landwirtschaftsmeister und engagierter Repräsentant der regionalen Landwirtschaftskammer, aber doch auf einen einzigen Zweig festgelegt: Der vor Jahren an den Dorfrand ausgesiedelte Hof ist heute ein Glied in der Kette der Putenfleischproduktion.

Heterogene Strukturen sind weniger anfällig und sie bieten besseren Schutz vor Zerstörungen und Totalausfällen, eine einleuchtende und leicht verständliche Empfehlung auch für die IT-Sicherheit: Möglicherweise aber doch nur ein Vorurteil und solange gültig, bis die nächste Generation zum Zuge kommt? Zunächst soll es hier aber darum gehen, die Lage der IT-Sicherheit in bundesdeutschen Betrieben, Institutionen und öffentlichen Behörden näher zu erläutern. Dazu dienen dem Autor vor allem die Ergebnisse von drei aktuellen Erhebungen.

Den empirischen und den Maßstäben der Wissenschaft verpflichteten Analysen sind zudem Äußerungen und Interviews von Experten und Entscheidungsträgern gegenübergestellt, für die ich bewusst keine standardisierte Form, sondern unterschiedliche journalistische Genres gewählt habe. Denn, so hatte ich es mir vorgenommen, der Text sollte – dem Thema angemessen – eine »heterogene Struktur« erhalten. Neben dem Vorstellen, Zusammenfassen und Vergleichen der aktuellen Studien zum Thema IT-Sicherheit in Unternehmen und Organisationen, wollte ich den eher theorielastigen Ansatz durch Zitate und O-Töne auflockern und damit abwechslungsreicher gestalten. Sie sollten den als Patchwork oder Collage gestalteten Text insgesamt abrunden. Für ihre Gesprächsbereitschaft und Auskünfte zur Vertiefung des Themas und zum Gelingen des Beitrags möchte ich mich daher nochmals bedanken bei Werner Gegenbauer, Präsident der Industrie- und Handelskammer zu Berlin, bei Dr. Michael Wendel, Sicherheitsbeauftragter des Presse- und Informationsamtes der Bundesregierung und bei Lothar-Karl Reiter, Leiter der IT-Sicherheit bei Audi in Ingolstadt.

10.2 Die Studien: Teilnehmer überdurchschnittlich sensibilisiert

10.2.1 KES/KPMG-Sicherheitsstudie 2002

260 Unternehmen und Behörden hatten sich an der von KES – Zeitschrift für Kommunikations- und EDV-Sicherheit – und dem Beratungsunternehmen KPMG gemeinsam durchgeführten Sicherheitsstudie 2002 zum Thema IT-Sicherheit in die Karten schauen lassen. Teilgenommen haben vor allem große mittelständische Unternehmen und Großunternehmen und -institutionen. Im Durchschnitt beträgt die Zahl ihrer Beschäftigten über 8000. Der größte befragte Betrieb zählt mehrere hunderttausend Mitarbeiter.

Der Anteil der Angestellten in der jeweiligen Informationsbearbeitung ist bei den beteiligten Firmen und Organisationen mit über 400 Beschäftigten ebenfalls sehr hoch. Das führen die Autoren der in KES (2002, Ausgaben 3 und 4) zusammengefassten Studienergebnisse, Prof. Dr. Reinhard Voßbein (MIMCert GmbH) und Dr. Jörn Voßbein (UIMC Dr. Vossbein GmbH & Co. KG) auf die vergleichsweise hohe Quote beteiligter großer Institutionen zurück. Eine gleichlautende Erklärung geben sie auch dafür, dass bei diesen

Unternehmen und Organisationen im Durchschnitt 16 Mitarbeiter ausschließlich für Aufgaben der IT-Sicherheit beschäftigt sind und diese Zahl über dem anzunehmenden gesamtwirtschaftlichen Mittel liegt. Tatsächlich sind rund ein Drittel der Befragten in der Kreditwirtschaft oder bei Versicherungen beschäftigt, über 15 Prozent kommen aus Behörden und öffentlichen Einrichtungen und über zehn Prozent sind Beratungshäusern zuzuordnen. Nicht zuletzt deswegen sprechen Voßbein und Voßbein von einer »eher positiv verzerrten Stichprobe, bei der man eine erhöhte Sensibilisierung in Sachen Sicherheit vermuten kann«, um zu folgern: »Die IT-Security dürfte sich im Allgemeinen noch deutlich schlechter darstellen.«

Ein weiterer Indikator dafür, dass sich vor allem die Großen und IT-Nahen der jeweiligen Branchen und Institutionen als auskunftsfreudig erwiesen haben, ist auch in der ebenfalls hohen Zahl der von ihnen eingesetzten Clients und PCs zu sehen, die im Durchschnitt bei 4000 liegt. Zusammen verfügen sie über fast 900 Großrechner. Zudem entfallen zehn Prozent ihrer Endgeräte, insgesamt 150.000 Stück, auf mobile Systeme wie Notebooks oder PDAs (Personal Digital Assistants).

10.2.2 Die silicon.de-Umfrage »IT-Sicherheit 2002«

An der im Mai 2002 durchgeführten Studie »IT-Sicherheit 2002« hatten sich knapp 500 Leser von silicon.de beteiligt. Ein Fünftel der Anwender kommen aus Kleinbetrieben mit bis zu 19 Mitarbeitern, 22 Prozent arbeiten in Unternehmen und Institutionen mit 20 bis 99 Beschäftigten. Mittelständler mit 100 bis 499 Arbeitplätzen stellen mit knapp 30 Prozent die größte Gruppe der Teilnehmer dar. Auf die nächste Größenordnung, den Betrieben von 500 bis 4999 Beschäftigten, entfallen rund 19 Prozent der Probanten und Großunternehmen mit über 5000 Arbeitnehmern waren zu knapp 10 Prozent vertreten. Den Schwerpunkt der Studie bildet somit der Mittelstand mit einer Beschäftigtenzahl von 20 bis 5000.

Die mit jeweils über 20 Prozent größten Teilnehmergruppen stammen aus den Branchen: Verarbeitende Industrie, Dienstleistungsgewerbe sowie Informationstechnologie- und Telekommunikationsindustrie. Die restlichen Teilnehmer ordnen sich zu wechselnden Anteilen dem Handel, der öffentlichen Verwaltung, dem Gesundheitsbereich, dem Kreditwesen und schließlich den Medien zu.

40 Prozent der Befragten sind für den IT-Einsatz ihres Unternehmens verantwortlich, 21 Prozent der Teilnehmer werden als IT-Experten klassifiziert, 13 Prozent sind in der Geschäftsleitung tätig, zwölf Prozent leiten eine Abteilung. Alle anderen sind unter der Kategorie »sonstige Funktionen und Tätigkeiten« zusammengefasst.

Aufgrund dieser Verteilung dürfte, wie der Rezensent der silicon.de-Studie, Christoph Hammerschmidt, in seiner Download-Version vom Juni 2002 schreibt, bei der Untersuchung ebenfalls eine positive Verzerrung stattgefunden haben.

10.2.3 »Die Position von Unternehmen in Europa und Südafrika zum Thema »Cybercrime« – Eine Studie von EDS und IDC«

Die von EDS, des weltweit führenden herstellerunabhängigen IT-Service-Unternehmens und Muttergesellschaft der C_sar AG, gemeinsam mit IDC Ende vergangenen Jahres durchgeführte Erhebung, verfolgt einen weiter gefassten Ansatz.

Für die Referenten, Dr. Klaus Schmidt – Global Chief Technologist und EDS Fellow – und Peter Windt – Service Line Manager »Web Application Infrastructure« -, der im April 2002 von ihnen veröffentlichten Ergebnisse stand der internationale Vergleich und die Frage im Vordergrund: Wie schneiden die Unternehmen und Organisationen der Bundesrepublik im Konzert mit denen anderer Länder beim Thema IT-Sicherheit und Cybercrime ab? Dafür wurden jeweils 350 Unternehmen aus insgesamt sechs Staaten befragt: Neben denen im Bundesgebiet Betriebe in vier weiteren europäischen Ländern – Frankreich, Großbritannien, Italien und Spanien – sowie in Südafrika.

Auch diese Befragung bezieht ihre Daten in erster Line aus den mittelständischen Betrieben. 44 Prozent der Unternehmen beschäftigen mehr als 500 Mitarbeiter, 56 Prozent haben 100 bis 500 Arbeitsplätze.

Bei 75 der Befragten handelt es sich um IT-Verantwortliche, rund acht Prozent sind für die Netzwerk-Aktivitäten zuständig und fünf Prozent arbeiten im Bereich der IT-Sicherheit.

Trotz ihrer zum Teil recht unterschiedlichen Herangehensweisen und Fragestellungen stimmen die drei Studien in ihren Ergebnissen und Interpretationen oft erstaunlich genau überein. Die Gemeinsamkeiten und Unterschiede sollen im Folgenden näher vorgestellt werden:

Ursachen der Schadensfälle

Die größten Risiken bilden, laut der von KES und KPMG durchgeführten Sicherheitsstudie, die »direkt von Menschen verursachten Schäden«, gefolgt von den Gefährdungen und Zerstörungen durch Malware wie Viren, Würmer und Trojanische Pferde. Das gilt sowohl für die tatsächlich eingetroffenen Schädigungen wie für die Risikoeinschätzungen der Teilnehmer. Auf Platz drei rangieren Softwaremängel. Anders die silicon.de-Umfrage: Bei ihren Probanten steht die Furcht vor Viren an oberster Stelle, gefolgt von der Angst vor unberechtigtem Zugang. Allerdings verzichtet die Erhebung auf die Frage nach den direkt von Menschen verursachten Schädigungen. EDS und IDC gingen auch hier einen eigenen Weg und ließen von den Teilnehmern selbst definieren, was sie unter Cybercrime verstehen. Im Ergebnis nehmen wiederum Viren mit drei von vier der möglichen Mehrfachnennungen die Spitzenposition ein. Mit weitem Abstand folgen: Zerstörung von Daten (42 Prozent), Diebstahl von Daten (24 Prozent) und Vandalismus durch Hacker (21 Prozent). Tatsächlich waren, so das Ergebnis der Studie,

deutsche Unternehmen nicht nur am häufigsten von Cybercrime-Angriffen betroffen, »sie hatten – bezogen auf das einzelne Unternehmen – auch noch die höchste Angriffs-Frequenz!«

Die KES/KPMG-Analyse bietet zudem einen Blick in die Zukunft. Danach bestehen die auffälligsten Veränderungen bei den Einschätzungen der Befragten im Vergleich zur aktuellen Situation vor allem bei »Hardware bedingte technische Defekte und Qualitätsmängel«, die auf der Liste der zwölf am häufigsten genannten Störungen von Platz sechs auf Platz zehn zurückfallen. Hier dürfte sich vor allem die Erwartung niederschlagen, dass die Systeme und Anwendungen mit zunehmender Produktionsreife immer stabiler und störungsfreier funktionieren und »Kinderkrankheiten« mit der Zeit einfach abgeschüttelt werden.

Künftig höher schätzen die Teilnehmer hingegen das Risiko der unbeabsichtigten Fehler von Externen, etwa von Wartungstechnikern, ein. Diese Gefährdungsquelle rückt von gegenwärtig Rang zehn auf den vierten Rang vor.

Beinahe unverändert bleibt jedoch die Entwicklung bei den »Spitzenreitern«: Irrtum und Nachlässigkeit eigener Mitarbeiter, Malware sowie Software bedingte technische Defekte beziehungsweise Qualitätsmängel. In dieser Gruppe läuft allerdings die Malware künftig, nach Einschätzung der Probanden, den Unzulänglichkeiten des eigenen Personals den Rang ab. Möglicherweise setzen die Befragten dabei auf die zunehmende Vertrautheit der Beschäftigten mit ihren Arbeitsgeräten und Anwendungen oder auf künftige Erfolge von geplanten Schulungs- und Fortbildungsprogrammen.

Irren ist menschlich

Bei den »direkt von Menschen verursachten Gefahren« (KES/KPMG) handelt es sich in der Regel um unbeabsichtigte Irrtümer und Fehler der eigenen Mitarbeiter. Hinter den Beeinträchtigungen verbergen sich somit keine Sabotageakte oder feindliche Motive des Personals. Der Grund ist vielmehr schlicht Unaufmerksamkeit und Nachlässigkeit. Allenfalls spekulieren ließe sich in diesem Zusammenhang darüber, ob Erklärungsansätze, wie sie die Tiefenpsychologie anbietet und wie sie unter anderem unter dem Begriff »passiv-aggressiv« gefasst werden, weiterhelfen. Unbeabsichtigt und fahrlässig jedenfalls waren auch die weiteren knapp zehn Prozent der registrierten, von Menschen direkt verursachten Beeinträchtigungen durch externe Dienstleister.

Daher, und hierbei sind sich alle drei Studien wieder einig, wäre eine permanente Sensibilisierung der Mitarbeiter dringend nötig. Doch gerade daran hapert es bislang bei den Firmen und Organisationen im Bundesgebiet. Im internationalen Vergleich bilden, so die EDS/IDC-Studie, Unternehmen in Deutschland »das Schlusslicht«. Stattdessen setzen sie auf den regelmäßigen Informationsfluss und Ad-hoc-Trainings. Dabei ist, wie Schmidt und Windt für EDS/IDC weiter ausführen, IT-Sicherheit ein Thema, das sich laufend weiter entwickelt und daher permanent trainiert werden muss. Wer nicht ständig dafür sorgt, dass sich alle Mitarbeiter darauf einstellen, wird immer schneller verletzbar, schreiben die Autoren. Die gleiche Schlussfolgerung legt auch die silicon.de-Studie nahe. Denn fast vier von fünf Befragten räu-

men »weichen« Maßnahmen wie der Heranbildung eines Sicherheitsbewusstseins bei Mitarbeitern den gleichen Rang ein, wie der eher technisch zu verstehenden Sicherung des Netzwerks.

Um eine kontinuierliche Sensibilisierung für das Thema Sicherheit geht es primär auch Lothar-Karl Reiter, IT-Verantwortlicher bei Audi, München. Vor zwei Jahren haben er und sein Team ein Projekt gestartet, das einen vollständigen Ansatz zur Erhöhung der IT- Sicherheit verfolgt. Dazu gehörten neben technischen Implementierungen und Prozessoptimierungen auch Schulungen und die Ausarbeitung und Durchsetzung eines Regelwerks.

Herr Reiter, Sie sind bei Audi für die IT-Sicherheit verantwortlich. Was sind die Schwerpunkte Ihrer Arbeit?

Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität – das sind die Begriffe, um die es beim Thema IT-Sicherheit allgemein geht und das sind auch die Aufgaben hier bei uns.

Das heißt, wir gewährleisten, dass geschäftliche und personenbezogene Daten geschützt bleiben und nicht nach außen gelangen. Und wir sorgen dafür, dass alle Daten, dort wo sie gebraucht werden und hingehören, jederzeit verfügbar sind. Integrität von Daten ist gegeben, wenn Steuerdaten für die Fertigung richtig übertragen werden und somit die hohe Qualität der Fahrzeuge erhalten bleibt. Schon geringfügige Änderungen der Daten könnten zu erheblichen Qualitätseinbußen oder Sicherheitsrisiken führen. Das links und rechts übereinstimmen, auch dafür sind wir also da. Authentizität heißt in erster Linie, für rechtliche Sicherheit bei der Verwendung von IT zu sorgen. Das trifft besonders beim E-Business zu. Wer bei wem bestellt und was, wann und wohin geliefert wird, darüber muss Gewissheit und Verbindlichkeit bestehen.

Worin sehen Sie das größte Gefahrenpotenzial für die IT-Sicherheit?

Nicht in Angriffen von Hackern oder in der Wirtschaftsspionage, auch nicht bei den Virusangriffen. Diese Attacken und Störungsversuche werden in der Öffentlichkeit oft übertrieben dargestellt. Entscheidend ist es dagegen, interne Prozesssicherheit zu erhalten. Um das zu erreichen, müssen Ziele definiert und eine Policy aufgestellt werden. Das setzt voraus, dass das Umfeld und der interne Zustand bekannt sind. Und IT-Sicherheit muss unter wirtschaftlichen Gesichtspunkten betrachtet werden. Sie funktioniert nicht nach dem Gießkannenprinzip, sondern nach Prioritäten und Schwerpunkten. Zentrale Bedeutung hat daher die Frage, wo liegen die Werte im Unternehmen, die besonders geschützt werden müssen. So lassen sich Angriffe am effizientesten begegnen und verhindern.

Was sollte dabei noch optimiert werden?

Es geht bei einer Verbesserung in erster Linie um Organisationsstrukturen und weniger um Technik. So sollten alle Richtlinien vollständig und sauber dokumentiert sein. IT-Sicherheit ist ein fortlaufender Prozess. Daran arbeiten wir.

Wie wird das Thema IT-Sicherheit bei Audi bewertet?

Grundsätzlich sind die Mitarbeiter und das Management für das Thema sensibilisiert, und es wird von der Firmenleitung als wichtige Aufgabe eingeschätzt. Unser Ziel ist es, alle Beteiligten mit ins Boot zu holen. Wenn jeder weiß, wie er

sich verhalten muss und was er zum Schutz beitragen kann, werden wir es auch am ehesten schaffen, mögliche Angriffe abzuwehren. Vieles haben wir in dieser Hinsicht schon geschafft, einiges müssen wir noch tun. Seit drei Jahren gibt es unsere Abteilung bei Audi. Vor zwei Jahren haben wir mit einem eigenen Projekt begonnen, mit dem wir einen vollständigen Ansatz verfolgen. Neben technischen und infrastrukturellen Teilprojekten geht es um den fortlaufenden Prozess der Sensibilisierung, um Schulungen zu dem Thema und um die Ausarbeitung und Durchsetzung eines Regelwerkes IT-Sicherheit.

Im Vergleich zu diesem positiven Beispiel erkennen die drei empirischen Studien hingegen erhebliche Kenntnislücken und Versäumnisse gerade auch bei den Entscheidern der Unternehmen. So bemängeln Voßbein und Voßbein (KES/KPMG), dass nach Auskunft der von ihnen Befragten nur ein geringer Teil des Managements »IT-Sicherheit als vorrangiges Ziel« und nur die Hälfte des Top-Management das Thema »als gleichrangiges Ziel im Rahmen der Informationsverarbeitung« ansieht. Deren Kenntnisstand beurteilen sie überwiegend als mittelmäßig bis eher schlecht. »Bei Anwendern in weniger sensitiven Bereichen liegt diese Beurteilung sogar bei über 80 Prozent«. Auch im internationalen Vergleich erhalten die Führungskräfte deutscher Unternehmen die schlechtesten Noten. Nur gut die Hälfte der Befragten stimmt zu, dass ihr Management sich der Bedeutung von IT-Sicherheit bewusst ist. Zum Vergleich: Bei den Spitzenreitern Südafrika sind es 91 Prozent und in Italien 71 Prozent der Teilnehmer. silicon.de hebt demgegenüber positiv hervor, dass bei immerhin fast einem Drittel der Unternehmen, IT-Sicherheit »mittlerweile Chefsache ist«.

Eine vergleichsweise optimistische Einschätzung ergibt sich zudem für den Rechenzentrumsbereich. Drei von vier der von KES/KPMG-Befragten sehen die Informationssicherheit dort als gut bis sehr gut an. Aber, so die KES-Autoren, »je »weiter« sich die Systeme von der zentralisierten zur verteilten Informationstechnik bewegen, desto schlechter wird die Einschätzung der Sicherheitslage«.

Datenverlust – der größte anzunehmende Unfall

Diese Bilanz erstaunt umso mehr, als der Datenverlust – in allen erfassten Analysen einheitlich – als »größter anzunehmender Unfall in einem Datenzentrum« (silicon.de, Juni 2002) angesehen wird. Laut KES/KPMG wäre dieser Schaden für 16 Prozent der Teilnehmer sogar gleichzusetzen mit dem finanziellen Ende des Unternehmens. Nicht zuletzt deshalb ist beinahe flächendeckend eine automatisierte Datensicherung realisiert. Dennoch malen die Interpreten der EDS/IDC-Studie in diesem Zusammenhang ein düsteres Bild. Denn ihnen zufolge sind die deutsche Firmen zwar am stärksten auf Datenverlust fokussiert, gleichzeitig aber am wenigsten in der Lage, die möglichen Gefahren des Cybercrime für sich zu klassifizieren. Sie kennen die Gefahr nicht, glauben sich aber davor sicher. »Ein riskanter Widerspruch«, warnen Schmidt und Windt. Zudem sind deutsche Unternehmen am wenigsten auf die Unterbrechung von wichtigen Workflows vorbereitet.

Übereinstimmen die Teilnehmer der unterschiedlichen Befragungen auch bei den Bewertungen der verschiedenartigen Risiken. An der Spitze steht für sie der Imageverlust, gefolgt von Verstößen gegen Gesetze, Vorschriften oder Verträge. Drohende finanzielle Konsequenzen landen bei dieser Abwägung dagegen im Mittelfeld.

Bemerkenswert ist in diesem Zusammenhang auch, dass die große Mehrzahl der Teilnehmer zwar angibt, ihnen sei das Bundesdatenschutzgesetz bekannt und würde von ihnen umgesetzt, jedoch einem Viertel der Befragten die Telekommunikations- und Teledienstgesetze gänzlich unbekannt sind. Angesichts ihrer Bedeutung gerade für das E-Business sowie für die Protokollierung auf Firewalls und Webservern sei das, so die Autoren der KES-Analyse, »eine ernüchternde Quote«.

Einen ähnlich geringen Bekanntheitsgrad besitzt auch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), welches sich zunächst an die Vorstände börsennotierter Gesellschaften wendet. Es verpflichtet die Unternehmen zur Einrichtung von Risikomanagementsystemen. Viele Wirtschaftsrechtler vertreten aber zudem die Meinung, dass sich vergleichbare Prüfungen auch aus der Sorgfaltspflicht der Geschäftsführer anderer Unternehmensformen ergeben.

Viren, Würmer und andere Eindringlinge

Naturgemäß bietet das Internet die größte Eintrittspforte für Störungen und Manipulationen. Dennoch erlauben trotz der Risiken für die internen Netze nur zehn Prozent der befragten Unternehmen ihren Beschäftigten keinerlei private Nutzung des Internets. Dabei verwendet ein Großteil der Unternehmen das World Wide Web und E-Mails für alle Beschäftigten. Sie nehmen, darauf weisen Voßbein und Voßbein hin, damit zugleich datenschutzrechtliche Probleme, wie sie mit der Kontrolle der privaten Aktivitäten verbunden sind, in Kauf.

Die größte Gefahr aus dem Internet geht nach Meinung der Befragten aller zitierten Studien eindeutig von der Malware aus. Bei 74 Prozent der Probanten wurden laut KES/KPMG-Sicherheitsstudie, im vergangenen Jahr Viren, Wurmbefall oder das Eindringen von Trojanern gemeldet. Die silicon.de-Umfrage spricht sogar von drei von vier Unternehmen, die im vergangenen Jahr »mindestens einen Virus im Haus« hatten. Im Vergleich zum Vorjahr ist dies eine Steigerung von schadhafter Software um 70 Prozent. Dabei seien, so die KES-Autoren, die meisten Vorfälle »glimpflich« verlaufen. Nur bei einem Viertel der Vorfälle hatte es mittlere bis größere Beeinträchtigungen gegeben. Als Durchschnittssumme für die eingetretenen Schäden hatte die Analyse einen Schätzwert von rund 26.000 Euro ermittelt.

Aber auch der Viren-Fehlalarm und schließlich der Virenschutz selbst haben ihren Preis. Falscher Alarm ist bei immerhin 50 Prozent der Teilnehmer der KES/KPMG-Studie bereits schon einmal ausgelöst worden, mit einem verursachten Schadenswert von durchschnittlich mehr als 8.000 Euro. silcon.de-Autor Christoph Hammerschmidt weist zudem auf eine zweite negative

Nebenwirkung der Antivirensoftware hin: Da sie zunehmend komplexere Checks durchführen muss, gerate sie allmählich an ihre Kapazitätsgrenzen. Zudem dauert der Start-up der Rechner durch die zusätzlichen Installationen länger, was produktive Arbeitszeit koste. Auch deshalb seien aufmerksame und geschulte Mitarbeiter im Kampf gegen Schädlinge so enorm wichtig.

E-Mails bieten der Malware den breitesten Einfallsweg – nur bei den Bootviren sind es naturgemäß die Disketten. Aber auch die Summe der Schädlinge, die ihren Weg über Netzwerke (Internet und LAN) nehmen, ist ebenfalls hoch, schreiben die Rezensenten der KES/KPMG-Studie. Entwarnung könne jedoch auch nicht für die Datenträger als Infektionsrisiko gegeben werden: Bei Fileviren, Makroviren und Würmern stehen weiterhin Disketten und vermutlich auch CD-ROMs auf Platz zwei der Gefahrenliste. Lediglich bei Trojanischen Pferden nimmt der Download aus dem Internet die erste Position ein. Ein anhaltender Rückgang der Störungsfälle sei im übrigen auch bei den Klassen der File- und Bootviren nicht zu verzeichnen.

»37 Prozent der Befragten haben keinen Angriffsversuch gegen Verfügbarkeit, Vertraulichkeit oder Integrität ihres Internetzugangs vermerkt« (KES 2002/3). Bei der Frage nach den Web-Servern registrierten 57 Prozent der Probanden keine dieser Attacken. An den ersten Stellen liegen hier mit 43 Prozent Hack-Versuche und Denial-of-Service-Angriffe (29 Prozent). Bei den Webservern rangierten DoS-Angriffe (28 Prozent) vor Spionage und »Defacement«, dem vandalistischen Verändern von Inhalten (16 Prozent).

Die Maßnahmen gegen neue Malware-Bedrohungen sind dabei beschränkt. So mussten trotz ihres verschiedenartigen Virenschutzes rund ein Drittel der Beteiligten in den vergangenen zwei Jahren »nennenswerte Beeinträchtigungen« etwa durch den Loveletter oder Nimda hinnehmen.

Hacking wird dagegen allgemein überbewertet. Das jedenfalls legt die Auswertung zu der Frage nach den Gefahrenbereichen der spürbaren Beeinträchtigungen nahe. Laut Voßbein und Voßbein (KES/KPMG) findet hier »eine Wahrnehmungsverzerrung in der öffentlichen Diskussion« statt. Eine mögliche Erklärung mag darin liegen, dass Hacking zu den in der Presse bevorzugt dargestellten Arten von Cyber-Angriffen gehört: Geschichten von den anscheinend genialen Computercracks. Teenager, die mit einfachstem Equipment aus ihren Jugendzimmern oder Clubräumen heraus den Großen und Mächtigen das Fürchten lehren, bieten den Stoff für romantisch verklärte Rebellion. Zudem bedienen sie das von vielen Presseorganen bevorzugte Muster der Personifizierung. Das mag auch ein Grund dafür sein, dass es beispielsweise der zwischenzeitlich vom Saulus zum Paulus konvertierte Chaos Computer Club in kürzester Zeit geschafft hat, sich in der Öffentlichkeit nicht nur einen Namen, sondern ein positives Image zu verschaffen.

Auch für die von den EDS/IDC-Analytikern befragten Probanden steht Vandalismus durch Hacking mit 21 Prozent an vierter Stelle der erhobenen Cybercrime-Definition, wobei Mehrfachnennungen möglich waren. Von den direkt von Menschen verursachten Beeinträchtigungen der vergangenen zwei Jahre, so die KES/KPMG-Studie, werden nur acht Prozent dem

Hacking, worunter unter anderem Vandalismus, Probing und Missbrauch gefasst ist, zugeordnet. Immerhin weitere sechs Prozent der deutlichen Beeinträchtigung in diesem Feld gehen auf das Konto von »unbefugte Kenntnisnahmen, Informationsdiebstahl und Wirtschaftsspionage«. Je zwei weitere Prozent werden der »Manipulation zum Zwecke der Bereicherung« und der Sabotage zugerechnet.

Abbildung 10.1: Auszug aus der EDS-Studie zum Thema Cybercrime

Bedrohung	durch	Risiken	EDS Service	Maßnahmen
Datendiebstahl / Wirtschaftsspionage	Mitbewerber	finanzieller Verlust; Kundenverlust; Imageverlust	Begutachtung; Konzeptionierung; Implementierung;	Verfahrensanweisungen, Firewall, IDS, PKI, Contentscanner
vertraulichen Firmendaten	Mitarbeiter		Betrieb	
Kundendaten	Hacker			
personenbezogenen Daten		+ Strafverfolgung		
Finanz- / Umsatzdaten				
Mitlesen von Datenströmen	Mitbewerber	finanzieller Verlust; Kundenverlust; Imageverlust	Begutachtung; Konzeptionierung;	
Mail	Mitarbeiter		Implementierung; Betrieb	Verfahrensanweisungen, Secure Mail, PKI
WAN - Verbindungen	Hacker			VPN, PKI
Transaktionen über das Internet				VPN, PKI
Extranet				VPN, PKI
Virenbedrohung	Mitbewerber	finanzieller Verlust; Kundenverlust; Imageverlust	Begutachtung; Konzeptionierung;	Verfahrensanweisungen, Virenscanner
Mail	Mitarbeiter		Implementierung;	
Server	Hacker		Betrieb	
Arbeitsstationen				
Weiterleitung an Dritte		+ Schadensersatz-forderungen		
Veränderung von Daten	Mitarbeiter	finanzieller Verlust; Kundenverlust; Imageverlust	Begutachtung; Konzeptionierung;	z.B. Firewall, IDS
vertraulichen Firmendaten	Hacker		Implementierung;	
Kundendaten			Betrieb	
personenbezogenen Daten		+ Strafverfolgung		
Finanz- / Umsatzdaten				
Webinhalte / Firmendarstellung				

Abbildung 10.2: Auszug aus der EDS-Studie zum Thema Cybercrime

Bedrohung	durch	Risiken	EDS Service	Maßnahmen
Daten Verlust durch Fremdeinwirkung	Mitbewerber	finanzieller Verlust; Kundenverlust; Imageverlust	Begutachtung; Konzeptionierung;	z.B. Backup, Firewall, IDS
vertraulichen Firmendaten	Mitarbeiter		Implementierung;	
Kundendaten	Hacker		Betrieb	
personenbezogenen Daten		+ Strafverfolgung		
Finanz- / Umsatzdaten				
Webinhalte / Firmendarstellung				
Daten Verlust ohne Fremdeinwirkung	Hardwareausfall	finanzieller Verlust; Kundenverlust; Imageverlust	Begutachtung; Konzeptionierung;	Backup, Business Continuity
vertraulichen Firmendaten	Katastrophe		Implementierung;	
Kundendaten	menschliches Versagen		Betrieb	
personenbezogenen Daten				
Finanz- / Umsatzdaten				
Webinhalte / Firmendarstellung				
zeitweiser Ausfall	Hardwareausfall	finanzieller Verlust; Kundenverlust	Begutachtung; Konzeptionierung;	Infrastruktur Planung; Hochverfügbarkeit
Arbeitsausfall	Mitarbeiter		Implementierung;	
Produktionsausfall	Katastrophe	+ Imageverlust	Betrieb	
	menschliches Versagen			
	Hacker			
	Mitbewerber			
fahrlässiger Umgang mit persönlichen Daten	Administratoren	finanzieller Verlust; Kundenverlust; Imageverlust	Begutachtung; Konzeptionierung;	Arbeitsanweisung, Schulung,
Speicherung	Mitbewerber	+ Strafverfolgung	Implementierung;	Datenschutzbeauftragter,
Verarbeitung	Mitarbeiter	+ Strafverfolgung	Betrieb	Audits
Auswertung	Hacker	+ Strafverfolgung		
Weitergabe		+ Strafverfolgung		
Umgang mit Logfiles		+ Strafverfolgung		

Virenscanner gehören zum Standard-Repertoire

Virenschutzmechanismen wurden in nahezu allen Clients und Server eingepasst – bei mobilen Endgeräten beträgt diese Quote, laut KES/KPMG-Sicherheitsstudie, 88 Prozent. Dabei dominieren Virenscanner. Bei über der Hälfte der Server, Gateways und PCs wird sogar die Software von mindestens zwei verschiedenen Anbietern genutzt. Drei von vier Unternehmen verwenden zudem Prüfsummenprogramme. Angriffserkennung durch Intrusion Detection Systems (IDS) sind mit 40 Prozent jedoch verhältnismäßig wenig im Einsatz. Der gleiche Anteil an Unternehmen plant die Anschaffung dieses Systems jedoch für ihre Server.

Den größten Aufwand betreiben die Firmen und Institutionen bei den Firewall- und Betriebssystem-Protokollen. Sie werden meist mehrmals in der Woche überprüft. Die Web- und E-Commerce-Applikationen kontrollieren die Befragten hingegen oft nur anlassbezogen oder sogar überhaupt nicht. Einen Penetrationstest ließen im vergangen Jahr zwei von drei der befragten Unternehmen durchführen, fast vier Fünftel davon in bezug auf die Internet-Infrastruktur und die Hälfte bei kritischen Systemen von innen.

Organisation der Abwehr

Gestalt erhält die IT-Sicherheit in der Funktion des IT-Sicherheitsbeauftragten. Er trägt, so das Ergebnis des KES/KPMG-Reports, die Verantwortung bei rund einem Drittel der befragten Unternehmen für die Erstellung der Konzeptionen sowie für die Notfall- und Deeskalationsmaßnahmen. Eine vergleichbar starke Stellung hat bei diesen Aufgaben nur noch der jeweilige Leiter der Datenverarbeitung. Einen Sicherheitsbeauftragten leistet sich, so Michael Vogel, ein zweiter Rezensent der silicon.de-Studie, jedoch nur ein Drittel der mittelständischen Betriebe im Vergleich zu immerhin zwei Drittel der Großunternehmen.

Welche Aufgabenbereiche die zentrale Figur in seinem Abwehrkampf gegen Angriffe und Störungen von innen und außen zu verantworten hat, soll das mit Dr. Michael Wendel, IT-Sicherheitsbeauftragter des Presse- und Informationsamtes der Bundesregierung, geführte Interview exemplarisch verdeutlichen:

Herr Dr. Wendel, was sind die wichtigsten Aufgaben des Referates Informations- und Nachrichtentechnik des Bundespresseamtes?

> *An erster Stelle steht für uns die Verfügbarkeit von Unterrichtungsdienstleistungen. Das geschieht nach Vordringlichkeit. Oberste Priorität haben die politischen Entscheidungsträger, das Bundeskanzleramt, die Bundesministerien und obersten Bundesbehörden. Für sie gilt, so sagen wir, 24/7, das heißt, sie müssen 24 Stunden am Tag, sieben Tage pro Woche auf die Meldungen der wichtigsten deutschen und internationalen Presseagenturen zugreifen können. Das ist zugleich unser Flaggschiff. Pro Monat sind es hier im Durchschnitt rund 10 Millionen hits (Zugriffe) auf unser entsprechendes webbasiertes Intranet-Informationsangebot.*

Ein weiterer Schwerpunkt bildet die gezielte Unterrichtung von Fachjournalisten im In- und Ausland. Gerade dieser Bereich wurde in den vergangenen Jahren stark ausgebaut.

Schließlich gehört zu dem politischen Auftrag, die Bürgerinnen und Bürger nicht nur im Inland, sondern, dann in der Regel über Multiplikatoren wie beispielsweise Goethe-Institute, auch im Ausland über die Regierungsarbeit zu informieren. In diesem Zusammenhang sind wir verantwortlich und beaufsichtigen die von einem externen IT-Dienstleister betriebenen Internetservices, http://www.bundesregierung.de, http://www.bundeskanzler.de und cvd.bundesregierung.de.

Welche Vorkehrungen und Sicherheitsmaßnahmen haben Sie dafür getroffen?

Für die Verteilung von Agenturmeldungen steht ein Doppelserversystem zur Verfügung, das auf Linux, also auf einer Open-Source-Basis aufbaut. Die beiden Systeme sind mit einem heartbeat-Mechanismus verbunden, replizieren Produktivinhalte alle zehn Sekunden und schlagen sofort Alarm, wenn das Zwillings-System nicht mehr richtig funktioniert. Als Carrier und Klammer zu externen Anwendern nutzen wir vor allem den IVBB (Informationsverbund Berlin Bonn). Innerhalb seiner an sich schon heterogenen Struktur und seinen mehrfachen Sicherheitsstufen setzen wir zusätzliche Hürden wie beispielsweise weitere Virenscanner ein und minimieren dadurch das Risiko von Angriffen oder Manipulationen.

Zudem werden Sicherheitseinstufungen vorgenommen. Und jede IT-Investition, das gilt auch für externe Dienstleister, die von uns sehr genau und kontinuierlich überprüft werden, muss die strengen Richtlinien unseres formalen Abnahmeverfahrens erfüllen. Sicherheitschecks lassen wir zum Teil auch von Beratungsunternehmen durchführen. So hat beispielsweise die C_sar AG den Auftrag erhalten, die Überprüfung des von dem externen IT-Dienstleister betriebenen Internetauftritts der Bundesregierung durchzuführen. Standard und Maßstab ist für uns das Grundschutzhandbuch des BSI (Bundesamt für Sicherheit in der Informationstechnik) und, wie bei allen obersten Bundesbehörden, ein Sicherheitskonzept als Teil des jährlich neu erstellten IT-Rahmenkonzeptes. Darüber hinaus werden die unter unserer Beteiligung von verschiedenen Arbeitskreisen der öffentlichen Verwaltung aus Bund, Ländern und Gemeinden gemeinsam entwickelten Richtlinien erfüllt. Selbstverständlich werden auch regelmäßig Sicherheitskopien des aktuellen Datenbestandes hergestellt und in einem feuersicheren Safe aufbewahrt.

Wie wird das Thema IT-Sicherheit in Ihrem Hause bewertet?

Wenn alles läuft, findet es wenig Beachtung, wenn es aber eine Störung gibt, dann glühen die Leitungen. Tatsächlich hat sich die Sensibilität gegenüber diesem Thema nach den Terroranschlägen des 11. Septembers deutlich erhöht. Allen ist die Verwundbarkeit von bislang sicher geglaubten Systemen auf tragische Weise vor Augen geführt worden. Auch wenn wir uns schon von der Lage her im Zentrum des Hauses befinden, wurden wir vorher häufiger als »diejenigen aus dem Elfenbeinturm« angesehen.

Wie hoch sind die Ausgaben für Sicherheit im Verhältnis zu den gesamten IT-Investitionen?

> *Die Ausgaben für die IT-Sicherheit kann ich nur schätzen. Vieles kann man nicht eindeutig berechnen, das trifft auf die Räume und das Personal ebenso wie auf die gesamte Infrastruktur zu. Wir sprechen hier von »eh da«-Positionen. Als Größenordnung schätze ich einen Anteil von 10 bis 15 Prozent.*

Einen eigenen Sicherheitsbeauftragten können sich insbesondere viele der kleineren und mittelgroßen Mittelständler allerdings schlicht nicht leisten. So kommt für sie als Alternative vor allem das Ausgliedern notwendiger IT-Aufgaben in Frage. Tatsächlich betreiben drei Viertel der befragten Betriebe und Institutionen Outsourcing. Die KES/KPMG-Studie schließt bei diesen Zahlen allerdings unter anderem die Entsorgung von Datenträgern mit ein, die zusammen mit Managed Firewalls/IDS den Löwenanteil ausmachen. Kritisch sieht es jedoch bei den vertraglichen Vereinbarungen mit ihren Outsourcing-Unternehmen aus, bei denen an die 40 Prozent der vertraglichen Vereinbarungen Anforderungen an die IT-Sicherheit nicht explizit geregelt sind. Ähnliches trifft bei den Anforderungen des Datenschutzes zu.

Eine eindeutig positive Entwicklung hingegen registrieren Voßbein und Voßbein bei den Sicherheitsberatungen. 60 Prozent der Befragten greifen demnach regelmäßig oder gelegentlich auf externe Berater zurück. Mit dem erfreulichem Resultat, dass die Hälfte der Unternehmen angeben, »uneingeschränkt« mit dem Beratungsergebnis »zufrieden« und nur drei Prozent »nicht zufrieden« zu sein. Die Spitzenpositionen nehmen die Risikoanalysen und Konzeptionsentwicklung ein, gefolgt von Schwachstellenanalysen, Penetrationstests sowie Strategie- und Managementberatung. Die Grundlagen für das methodischen Vorgehen bilden neben dem IT-Grundschutzhandbuch des BSI von Beratern selbst entwickelte Verfahren, Softwareanalyse-Tools sowie das IT-Sicherheitshandbuch des BSI. An der Spitze der Prüfungsobjekte stehen generell Datenklassifizierung und Zugriffsrechte der Ablauforganisation, ferner softwareorientierte Prüfungen. Schließlich unterziehen die von KES/KPMG Befragten mit über 40 Prozent auch Konzeptionen und Zielsetzungen einer Sicherheitsprüfung.

Vor allem für den nicht zuletzt aufgrund seiner finanziellen Möglichkeiten in Punkto IT-Sicherheit auf die hinteren Plätzen verbannten Mittelstand, bezieht Werner Gegenbauer in seinem von dem Autor erbetenen Statement Stellung. Als Lösung für eine wirksame Unterstützung schlägt der Präsident der Berliner Industrie- und Handelskammer die Einrichtung eines speziell auf die Belange von kleineren und mittelgroßen Betriebe ausgelegtes CERT (Computer Emergency Response Team) vor:

> *IT-Sicherheit ist im Unternehmen eine ständige Herausforderung, die leider immer noch unterschätzt wird. Diese Herausforderung ist nicht neu, aber sie wächst in dem Maße, wie Unternehmen sich untereinander vernetzen und auf die Funktionsfähigkeit ihrer IT-Systeme existenziell angewiesen sind. Die Gefahrenpotenziale und Schadensfälle haben sich in den letzten Jahren vervielfacht.*

Insbesondere kleine und mittlere Unternehmen, die sich keine eigenen Spezialisten leisten können, neigen aus Zeitmangel und fehlender Kenntnis dazu, die Probleme zu unterschätzen.

Vor diesem Hintergrund müssen wir über leistungsfähige Informations- und Dienstleistungsstrukturen für kleine und mittlere Unternehmen nachdenken. Die Industrie- und Handelskammern spielen hier als erste Anlaufstelle eine wichtige Rolle. Sie können zumindest dafür sorgen, dass die Gefahren besser erkannt werden und systematischer angegangen werden. In Informationsveranstaltungen, Workshops und Arbeitskreisen informieren die einzelnen IHKs über Gefahren und Praxislösungen zur Vermeidung von Schadensfällen.

Dauerhaft wird das nicht ausreichen. Wir benötigen eine starke Kooperation von Kammern, Verbänden und IT-Dienstleistern zur gezielten Information und Beratung von kleineren und mittleren Unternehmen über die täglich wachsenden Angriffsmöglichkeiten ihrer IT-Systeme. Ein IT-Notfallzentrum (CERT) für den Mittelstand wäre eine gute Möglichkeit, diese Firmen wirksamer zu unterstützen.

Annehmen müssen die Unternehmen die neuen Herausforderungen jedoch selbst. Hier sind auch nicht nur die IT-Verantwortlichen, sondern die Unternehmenschefs selbst gefragt und verantwortlich. In der Mehrzahl der Fälle lässt sich mit rein organisatorischen Maßnahmen der größere Teil der Gefahrenpotenziale schon ausschalten.

Eigentlich selbstverständlich: Business Continuity Pläne

Schriftlich fixierte Strategien bei Störungen, Beeinträchtigungen und Notfällen müssten, so die einhellige Meinung der Rezensenten, zum Standard-Rüstzeug jedes Unternehmens gehören.

Bei den ermittelten Ergebnissen zu den realisierten Regelwerken klaffen die Studien jedoch auseinander. Nach dem KES/KPMG-Report haben entsprechende Pläne 56 Prozent der Befragten ausgearbeitet. Zudem basieren auch die Sicherheitsmaßnahmen danach zu 70 Prozent auf schriftlichen Formulierungen. Bei Internet und E-Mail sind das sogar 86 Prozent. Laut silicon.de-Bericht trifft diese Ausarbeitung von verbindlichen Regeln beim Mittelstand dagegen nur zu einem Viertel der befragten Betrieben zu. Bei den Großunternehmen, da stimmt die Analyse wieder mit den Zahlen von KES/KPMG und EDS/IDC überein, liegt zu 50 Prozent ein Business Continuity Plan vor. Sie sind somit »kontrollierbar, revisionsfähig und nach den Grundsätzen ordnungsmäßiger Projektabwicklung nachvollziehbar« (KES). Tatsächlich kontrollieren drei Viertel der Betriebe und Organisationen diese Maßnahmen vor allem mit dem Instrument der Revision.

Schließlich prüft ein Großteil der Teilnehmer auch die Eignung ihrer Konzepte. Dafür nutzen sie in erster Linie Schwachstellen- und Risikoanalysen sowie Notfall- und Wiederanlaufübungen. Und das mit Erfolg: Denn 90 Prozent der Prüfungen haben Schwachstellen aufgedeckt, mit deren Beseitigung zum Zeitpunkt der Erhebung von KES und KPMG rund drei Viertel

der Befragten noch beschäftigt waren. Lediglich ein Prozent hatte daraus bislang keine Aktivität ergriffen. Bei 60 Prozent der Fälle erstreckt sich die Überprüfung auf einzelne Systeme und bei rund einem Drittel auf alle geschäftskritischen Systeme.

»Ein EDV-Notfall- oder Wiederanlaufkonzept mit schriftlicher Fixierung und Validierung besitzen allerdings nur ein Viertel der Unternehmen«, schränkt der KES-Bericht ein. Auch sind die Hochverfügbarkeitsanforderungen von E-Business-Systemen nur bei einem Bruchteil der Konzepte berücksichtigt. Ihre vergleichbaren Ergebnisse führten die Referenten der EDS/IDS-Studie denn auch zu der provokanten Frage: »Was nützen sichere Daten, wenn niemand weiß, wie es im wirklichen Krisenfall weiter geht?«

Elektronische Signatur und Verschlüsselung

Nur rund ein Viertel der Teilnehmer setzt elektronische Signaturen in ihrer Kommunikation mit Geschäftspartnern oder Kunden ein. Neben reinen Softwarelösungen rangieren die Chip-Karten abgeschlagen auf einem zweiten Platz. Voßbein und Voßbein folgern daraus, dass für die elektronischen Signaturen in bezug auf Gesetzeskonformität noch keine guten Aussichten bestehen. Und auch die silicon.de-Umfrage stellt nüchtern fest: »Von einer Akzeptanz dieser Technik auf breiter Front kann indessen keine Rede sein.«

Beim Thema PKI (Public Key Infrastructure) sieht das schon wieder anders aus. Bereits über 60 Prozent der Befragten haben eine PKI realisiert – eine beträchtliche Steigerung im Vergleich zur Erhebung im Vorjahr. Da waren es lediglich sieben Prozent. Spitzenpositionen bei den Einsätzen belegen die E-Mail-Verschlüsselung, gefolgt von den Tele-Arbeitsplätzen, Dateiverschlüsselung und VPN (Virtual Private Network). Meist ist das Herkunftsland für die Auswahl einer PKI-Lösung wichtig, so die KES-Autoren. Ein weiteres entscheidendes Kriterium bildet die Automatisierung der Prozesse zur Erstellung und Verwaltung von Zertifikaten.

Bei den Maßnahmen zur Verschlüsselung konzentrieren sich die Betriebe und Institutionen auf ausgewählte sensitive Daten. Vor allem die Festplatten und Dateien mobiler Endgeräte werden, so der KES-Report, im hohen Maße chiffriert. Bei der Detailfrage nach einer Verschlüsselung von E-Mails gaben 13 Prozent der Befragten an, jede Nachricht, die verschlüsselt werden kann, auch zu chiffrieren. Und, unter der Voraussetzung, dass die Adressaten über einen Kryptopartner verfügen, macht dieser Anteil bei sensitiven Dateien sogar 44 Prozent aus. PGP (Pretty Good Privacy; Programm für PKI-Verschlüsselung) steht als verwendeter Standard mit nahezu dem doppelten Wert wie S/MIME (Secure/Multipurpose Internet Mail Extensions; Sicherheits-/Mehrzweckerweiterungen für Internet/E-Mail) dabei an einsamer Spitze.

Im Vergleich zu den verwendeten Verschlüsselungsverfahren, folgern Voßbein und Voßbein, werden elektronische Signaturen außerordentlich selten eingesetzt.

10.3 Fazit: Das Bewusstsein bestimmt das Sein

Diese aus der philosophischen Debatte entliehene Formel lässt sich auch auf das zentrale Ergebnis der in diesem Beitrag zusammengeführten Studien und Stellungnahmen von Experten und Funktionsträgern anwenden. Denn die Gesprächspartner sind sich mit den zitierten Rezensenten der hier vorgestellten Befragungen in ihrer Einschätzung einig, dass es weniger um die Technik geht, die allerdings ebenfalls sorgfältig ausgewählt und gezielt eingesetzt werden muss, als vielmehr um die Optimierung von Organisationsprozessen und generell um die Sensibilisierung für das Thema Sicherheit in der Informationstechnologie. Überein stimmen sie auch in ihrer Auffassung, dass effektiver Schutz ein kontinuierliches Engagement verlangt. Bewusstsein für die Gefahren von innen und außen zu schärfen und die nötige Aufmerksamkeit auf die Vermeidung und Abwehr von Störungen und Angriffen zu lenken, bedarf einer permanenten Gestaltung.

Dabei reicht es nicht, auf Virenscanner und Firewalls oder eine automatisierte Datensicherung zu vertrauen, wie sie immerhin zum Minimalprogramm fast aller mindestens mittelgroßen Unternehmen und Organisationen gehören. Gefordert sind ein Sicherheitsmanagement und eine ausformulierte Policy mit schriftlich fixierten und verbindlichen Regularien. Nur dadurch kann gewährleistet werden, dass jeder Beteiligte für den Notfall gerüstet ist und weiß, wie er sich zu verhalten hat. Schließlich geht es um nicht weniger als die Sicherstellung der Business Continuity und damit nicht nur um die Vermeidung von wirtschaftlichen Einbußen, sondern auch von Imageverlust.

Die Entwicklung des strategischen Konzeptes und eines abgestimmten Verhaltenskodexes ist eine originäre Aufgabe des Sicherheitsbeauftragten oder alternativ des Leiters der Datenverarbeitung. Wegen der Komplexität der Materie werden dabei zudem vielfach externe Berater hinzugezogen. Mit in der Regel positiven Ergebnissen und hoher Zufriedenheit auf Seiten der Kunden. Erfolgreiches Outsourcing betreiben insbesondere die »Großen« und »IT-Nahen« auch bei ihren Sicherheitsüberprüfungen.

Gerade für den Mittelstand, der sich eigene Sicherheitsbeauftragte und größere IT-Teams oft nicht leisten kann, bietet Outsourcing eine aussichtsreiche Möglichkeit. Denn die kleineren und mittleren Unternehmen haben bei Fragen der Sicherheit den größten Nachholbedarf. Ein pragmatischer Vorschlag stammt in diesem Zusammenhang von Werner Gegenbauer. Der Präsident der Berliner Industrie- und Handelskammer regt ein eigenes »IT-Notfallzentrum«, einen CERT, speziell für die Belange des Mittelstands an. Für diese Initiative und zur weiteren Vernetzung von Kammern, Verbänden und IT-Dienstleistern sieht er insbesondere die IHKs (Industrie- und Handelskammern) in der Pflicht, weil sie in der Regel die ersten Anlaufstellen für die mittelständischen Unternehmen bilden. Gefragt und gefordert sind dabei aber nicht die IT-Verantwortlichen allein, sondern zu aller erst die Firmenchefs selbst. IT-Sicherheit muss von oben gelebt werden. Dann werden alle Bereiche erfasst und die gelebte Kultur der Sicherheit strahlt auf alle Ebenen aus.

11 Modernes Sicherheitsmanagement

Dr. Frank Bourseau

11.1 Einleitung

Policies, gesetzliche Vorschriften, eingeführte Sicherheitstechniken, neue Technologien – das sind nur einige Punkte, denen modernes Sicherheitsmanagement heute in einer umfassenden, aber gleichzeitig lebbaren Form Rechnung tragen muss, um sich vom Image des lästigen und teuren Behinderers im Unternehmen zu verabschieden. IT-Risiko- und Sicherheitsmanagement hat sich besonders im Finanzdienstleistungsbereich zu einem entscheidenden Wettbewerbsfaktor entwickelt, seit immer offensichtlicher wird, dass sich eine moderne Bank einen nachlässigen Umgang mit Sicherheitsfragen im buchstäblichen Sinn nicht mehr leisten kann. Denn nicht nur die Gesamtheit der Kreditrisiken bestimmt in Zukunft die Bonität einer Bank und damit ihre Wettbewerbsfähigkeit, sondern ebenso die »operationellen Risiken«, zu denen auch die IT- oder treffender die Informationsrisiken, gehören. Welchen Einflüssen unterliegt das Sicherheitsmanagement eines IT-Dienstleisters für Banken und wie kann eine effiziente Umsetzung im Unternehmen erreicht werden?

Eine entscheidende Basis für Geschäfte mit einer Bank bildet Vertrauen und Seriosität. Finanzinstitute, denen nicht genug Vertrauen entgegengebracht wird, bescheidet man auch keinen seriöser Umgang mit Geld und daher wird ihnen kein langfristiger Erfolg am Markt vergönnt sein. Eine weitere Basis ist jedoch auch die innovative Kraft eines Unternehmens, die sich auf wechselnde Markterfordernisse schnell einstellen kann. Zu diesen Erfordernissen zählt auch die Öffnung für neue Techniken, Zugangswege etc. Neue Techniken stellen jedoch auch neue Herausforderungen an die Absicherung dar und die Komplexität der mittlerweile eingesetzten Technologien macht eine übersichtliche Herangehensweise zur Ermittlung von Risiken immer schwieriger.

Das Wissen über Sicherheitsmanagement in und außerhalb von Unternehmen steckt jedoch noch vielfach in den Kinderschuhen, auch viele im IT-Bereich Beschäftigte stellen sich unter Sicherheitsmanagement hauptsächlich die Installation von Firewalls und Virenscannern vor oder siedeln Sicherheitsmanagement im Bereich der Benutzeradministration an. Tatsächlich waren Sicherheitsverantwortliche in den vergangenen Jahren oft in dem Glauben, jedes Sicherheitsproblem mit Technik in den Griff bekommen zu können. Mittlerweile scheint sich jedoch die Erkenntnis durchzusetzen, dass

Sicherheit in den Prozessen eines Unternehmens zu implementieren ist, und diese Prozesse werden gebildet von technikfernen wie auch techniknahen Abläufen.

11.1.1 Praktische Sicherheitsherausforderungen

Einige beispielhafte Herausforderungen im praktischen Sicherheitsmanagement in der S-Finanzgruppe sind:

- Die insgesamt zu verwaltende Infrastruktur besteht aus vielen rechtlich und technisch eigenständigen Netzen, die über ein gemeinsames Kernnetz verfügen. Sicherheitsprobleme in einem Teilnetz dürfen nicht auf die restlichen angeschlossenen Netze wirken.
- Jedes Institut hat neben dem zentralen IT-Dienstleister weitere regionale oder überregionale Dienstleister, denen z.B. zu Wartungszwecken Zugang auf Teile der IT-Infrastruktur eingeräumt werden muss.
- Automatisierter Datenaustausch erfolgt nicht nur mit Millionen von Privat- und Firmenkunden sondern auch mit vielen nationalen und internationalen Datennetzen (Banken, Kreditkartenorganisationen, Clearing-Systeme etc.).
- Verschiedenste Zugangswege sind zu unterstützen, und die dabei angewandten Anwendungsprotokolle folgen unterschiedlichen Standards. Auch wenn der Trend zur Abwicklung über das Medium Internet zu verzeichnen ist, bedeutet dies noch nicht eine Einheitlichkeit der über dieses Basisnetz abgewickelten höheren Protokolle.
- Zunehmende Standardisierung des Datenverkehrs über Internettechnologien und der Anschluss an das »Netz der Netze« lässt alle bekannten Gefahren, wie Denial-of-Service-Attacken, Viren oder Spyware für die eigene IT zur brisanten Bedrohung werden. »Security by Obscurity«, die sich auf die Unbekanntheit der Datenverarbeitung und Protokolle im Unternehmensbackbone stützte, gehört bereits seit längerem der Vergangenheit an.
- An die S-Finanzgruppe werden als größter nationaler Debit-Kartenemittent und Betreiber des größten nationalen Finanz-Selbstbedienungsnetzes hohe Anforderungen an die Absicherung dieses Netzes und die damit verbundene kryptografische Schlüsselverwaltung gestellt.

11.1.2 Gesetze, Abkommen

Neben den praktischen Anforderungen an das IT-Sicherheitsmanagement beginnen sich jedoch auch regulatorische Rahmenbedingungen entscheidend zu ändern, indem sie zunehmend die Verpflichtung zu einem umfassenden Risiko- und Sicherheitsmanagement in das Pflichtenheft von Unternehmen besonders im Finanzbereich aufnehmen. Allgemeingültigkeit hat bereits seit längerer Zeit das Gesetz zur Kontrolle und Transparenz im

Unternehmensbereich (KonTraG), das dem Management die Einführung von effizienten Risikomechanismen auferlegt, um frühzeitig auf bestandsgefährdende Entwicklungen im Unternehmen aufmerksam zu werden. Im Bankenbereich spielt das »Gesetz über das Kreditwesen« (KWG) eine bestimmende Rolle; für IT-Dienstleister ist insbesondere der §25a KWG relevant, der das Outsourcing von Geschäftsbereichen einer Bank regelt. Noch im Entwurfsstadium durch den Basler Ausschuss für Bankenaufsicht befinden sich die Basler Eigenkapitalvereinbarungen (Basel II), ähnlich wie eine angekündigte Maßnahmensammlung zur IT, die durch das BAFin (Bundesanstalt für Finanzdienstleistungsaufsicht, ehem. BAKred) ausgearbeitet wird.

Die für das Sicherheitsmanagement wesentlichen Eckpunkte dieser Regularien sind teilweise übereinstimmend und schreiben ähnliche Vorgehensweisen vor. Als Beispiel sei hier der Entwurf des Basler Ausschusses für Bankenaufsicht genannt, der in einem Konzeptpapier die »Risiko-Management-Prinzipien für Electronic Banking« beschreibt. »Electronic Banking« ist hier zwar nur ein kleiner Ausschnitt des Bankbetriebs, die prinzipiellen Vorschriften sind jedoch übertragbar auf alle Bereiche und Anwendungen.

11.2 Basel II: »Risk-Management – Principles for Electronic Banking«

Das mit dem Begriff Basel II belegte Entwurfspaket stammt vom Basler Ausschuss für Bankenaufsicht, der sich aus den Zentralbanken der G10-Länder, Spanien und Luxemburg zusammensetzt. Es ist als Ablösung der Basler Eigenkapitalvereinbarungen von 1988 konzipiert und reformiert die Mindestkapitalanforderungen für Banken, die nach dem Entwurf unmittelbar von den Kredit- und den operationellen Risiken einer Bank abhängen. Zu den operationellen Risiken gehören die IT-Risiken, z.B. die besonders öffentlichkeitswirksamen Risiken beim Electronic Banking. Zum Management dieser Risiken werden folgende Vorschläge gemacht, die auf drei Säulen ruhen ***[1]***:

Abbildung 11.1: Basel II Risiko-Management-Prinzipien

11.2.1 Geschäftsführungs- und Managementaufsicht bzw. -verantwortung

Dem Management werden Pflichten auferlegt, die in vergleichbaren Regelungen bis zur Haftung des Vorstandes gehen und nicht auf E-Banking beschränkt sind. Insbesondere hat der Vorstand dafür Sorge zu tragen, dass sämtliche Aktivitäten einer Bank permanenten Aufsichts- und Kontrollmechanismen unterliegen, die es ihm ermöglichen, negative Entwicklungen frühzeitig zu erkennen und gegenzusteuern. Dieser Überwachungsprozess schließt auch die durch Outsourcing ausgelagerten Geschäftsbereiche mit ein und zwingt die Unternehmensleitung dazu, die Anforderungen an das eigene Unternehmen auch auf Dienstleister auszudehnen. Es versteht sich von selbst, dass insbesondere ausgelagerte IT-Dienstleistungen davon betroffen sind.

11.2.2 Sicherheitspolicies und -maßnahmen

Dem Unternehmen wird auferlegt, folgende Maßnahmen für ein effektives Sicherheitsmanagement umzusetzen. Die grundsätzlichen Sicherheitsziele Vertraulichkeit, Integrität und Authentizität sind über die Implementierung geeigneter Maßnahmen sicher zu stellen. Dazu gehören auch Maßnahmen zur Autorisierung und zur Trennung von Verantwortlichkeiten innerhalb von E-Banking-Systemen, um absichtliche oder versehentliche Fehler einzelner Personen nicht zu unabsehbaren Schäden führen zu lassen. Eine Maßnahme in dieser Richtung ist z.B. die Trennung von Entwicklung und Administration. Alle diese Maßnahmen müssen in Audits überprüft und die Funktionstrennungen in Tests auf tatsächliche Unumgehbarkeit untersucht werden.

11.2.3 Risikomanagement gegen juristische und Reputationsschäden

Die dritte Säule des Regelwerks bilden Maßnahmen zur Vorsorge gegen juristische Probleme wie z.B. die Veröffentlichung von Informationen zur Identifikation und den Regeln der Bank auf den Webseiten sowie die Einhaltung der geltenden Datenschutzrichtlinien. Auch durch einen nur kleinen Ausfall einer Komponente kann die Verfügbarkeit von Anwendungen lange Zeit gestört sein, falls keine effektiven Kapazitäts-, Wiederanlauf- und Notfallplanungen zur Verfügung stehen. Nicht zuletzt, um dem durch solche oder ähnliche Vorfälle auf dem Spiel stehenden Ruf des Unternehmens nicht zu schaden, sind Planungen zur Reaktion auf unvorhergesehene Zwischenfälle wie interne oder externe Angriffe auf die Banking-Systeme zwingend durchzuführen.

11.2.4 Katalog von Empfehlungen zur Umsetzung

Die Basel-II-Entwickler gehen sogar noch weiter und detaillieren die Maßnahmen bis auf die tiefere technische und organisatorische Ebene. Beispielsweise wird die Einrichtung von Sicherheitsprofilen, expliziten Sensitivitätsklassifizierungen, Zugangskontrollen zur Durchsetzung von Funktionstrennungen, Antivirensoftware, Intrusion Detection u.a. angeraten, um die in den allgemeineren Kapiteln geforderten Maßnahmen durchzusetzen. Weiter wird z.B. empfohlen, in regelmäßigen Abständen Penetrationstests durchzuführen und die Policies und Sicherheitsmaßnahmen bei outgesourcten Dienstleistungen periodisch zu überprüfen.

Festzuhalten bleibt, wenn man die Regelungen der verschiedenen Gesetze auf einen gemeinsamen Nenner zu bringen versucht, dass einem Finanzinstitut und seinen Outsourcing-Partnern in naher Zukunft ohne ein nachweisbar funktionierendes Sicherheits- und Risikomanagement für die IT höhere Risiken und damit finanzielle Belastungen zugerechnet werden müssen.

11.3 Unterstützung des Sicherheitsmanagements durch Standards

Bei der konkreten Ausgestaltung der Einführung eines Risiko- und Sicherheitsmanagements können Standards wichtige Hilfestellungen leisten. Beispiele für Sicherheitsstandards sind:

- Die Anleitung zur Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach dem britischen Standard BS 7799 -2 und die dazugehörige Best-Practice-Sammlung BS 7799 -1 (ISO/IEC 17799) ***[2]***
- Die Reports zur Umsetzung einer Sicherheitsstrategie nach ISO TR 13335 ***[3]***
- Das Grundschutzhandbuch des deutschen BSI (Bundesamt für Sicherheit in der Informationstechnik) ***[4]***
- Das S-Finanzgruppen-interne Sicherheitsrahmenwerk des Sparkassen-Informatik-Zentrums

Die Schnittmenge aller dieser Standards ist relativ hoch, aus jedem lassen sich die wichtigsten Hinweise zur Umsetzung eines Sicherheitsmanagements im Unternehmen ableiten. Jedes Unternehmen muss daher je nach seinen Zielen und sonstigen implementierten Prozessen den für die Umsetzung geeigneten Weg finden.

11.3.1 Maßnahmen zur Einführung eines Informationssicherheitsmanagementsystems nach BS 7799

Als Beispiel sei der Maßnahmenkatalog nach dem britischen Standard BS 7799-2 genannt, der vor allen Dingen zur Zertifizierung eines Sicherheitsmanagementsystems herangezogen werden kann und folgende Bestandteile fordert:

1. Sicherheitspolitik
2. Organisation der Sicherheit
3. Festlegung und Bewertung zu schützender Objekte und Prozesse
4. Physische Sicherheit und Infrastruktur
5. Netzwerk- und Systemmanagement
6. Personelle Sicherheit
7. Zugriffs- und Zugangskontrolle
8. Systementwicklung und -wartung
9. Aufrechterhaltung der Geschäftsprozesse
10. Einhaltung von Verpflichtungen (Compliance)

Gleichzeitig ist für eine Zertifizierung ein nachweisbar funktionierendes Risikomanagement zu erbringen. Die Prozesse und Maßnahmen nach BS 7799 -2 lassen durch ihre generische Formulierung einen relativ weiten Spielraum für die konkrete Implementierung im Unternehmen und erfahren erst durch die Best-Practice-Sammlung ISO 17799 eine (nicht erzwungene) Detaillierung.

11.3.2 Was ist der Nutzen von Standards

Standards geben wichtige Hilfestellungen bei der Etablierung eines Informationssicherheitsmanagementsystems und tragen zur Vergleichbarkeit von Sicherheitsniveaus bei. Sie können Sicherheitsaudits vereinfachen und verkürzen und sind daher für IT-Dienstleister besonders interessant.

Sie bilden in der Regel wegen ihres Umfangs und ihrer Abstraktion keine Basis für das Marketing von Sicherheit im Unternehmen, sondern müssen zur effizienten Verbreitung im Unternehmen mit verschiedensten Umsetzungshilfen angereichert werden.

11.4 Das Sicherheitsmanagement in der dvg

Die dvg hat sich für die Herangehensweise entschieden, die bereits seit einigen Jahren existierende Sicherheitsarchitektur nach den strukturellen Vorgaben des britischen Standards BS 7799 auszurichten. Diese Prozesssicht auf das Sicherheitsmanagement ist abgestimmt auf das etablierte Prozessmanagement der dvg – z.B. das bereits in sämtlichen Bereichen des Unternehmens praktizierte Risikomanagement.

11.4.1 Die dvg-Sicherheitsarchitektur

Zur notwendigen Etablierung des Sicherheitsmanagements im Unternehmen gehören die in generischer Form formulierten Sicherheitsziele und Policies, die über wenige Kernsätze nicht hinausgehen sollten und quasi als Sicherheitsgrundgesetz im Unternehmen von der Geschäftsführung verabschiedet werden (z.B. Gewährleistung der Vertraulichkeit). Diesen Grundgesetzen werden Strategien und Konzepte zugeordnet, die Anleitungen dazu enthalten, mit welchen Mitteln das Unternehmen die Einhaltung der Policies zu erreichen gedenkt (z.B. Verschlüsselung). Als letzte breite Ebene enthält diese Pyramidendarstellung der Sicherheitsarchitektur die konkrete Ausformulierung von Verfahrens- und Arbeitsanweisungen (z.B. Verschlüsselung für Notebooks). Diese Gesamtdarstellung stellt den Fundus dar, aus dem für alle Mitarbeiter und Prozesse des Unternehmens die in ihrem Kontext notwendigen Sicherheitsregelungen abgeleitet von den Kernpolicies extrahierbar sind. Zugeordnet sind den einzelnen Aktivitäten die im Sicherheitsprozess beschriebenen Rollen.

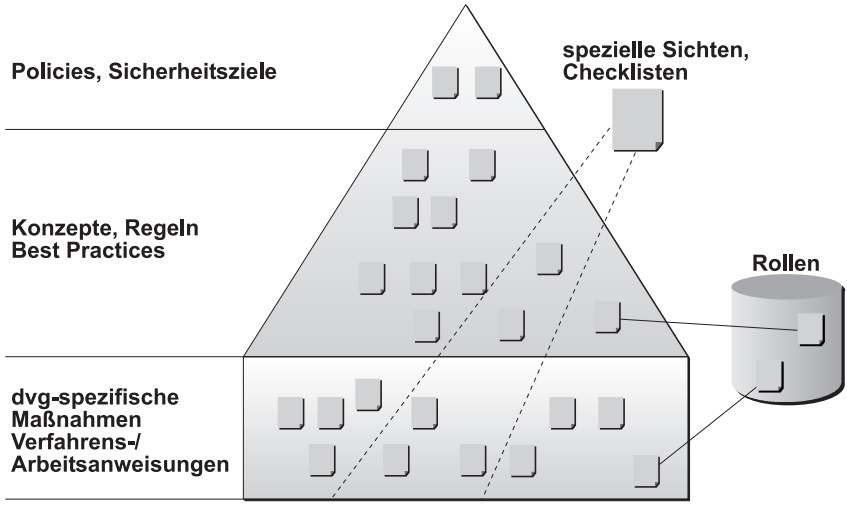
11.4.2 Umsetzung des dvg-Sicherheitsmanagements

In der konkreten täglichen Arbeit im Unternehmen ist eine Policysammlung der oben beschriebenen Art für die nicht direkt mit Sicherheit betrauten Mitarbeiter erfahrungsgemäß eher abschreckend und droht als »Schrankware« in den Regalen des Sicherheitsmanagers zu verstauben. Wie werden die Konzepte zum Leben erweckt und Sicherheitsdenken als Selbstverständlichkeit im Unternehmen verankert?

- Über Veranstaltungen, die nicht trockenen Sicherheitsschulungen gleichen, sondern durch Vorführen der Gefahren zum Nachdenken über die eigenen Verhaltensweisen anregen, werden die Mitarbeiter für das Thema sensibilisiert.
- Das Thema muss so aufbereitet werden, dass das weit verbreitete Vertrauen in die Sicherheitstechnik als »Rundum-Sorglos-Paket« beendet wird und jedem Mitarbeiter die eigene Rolle als Sicherheitsverantwortlicher in seinem Bereich vor Augen geführt wird.

- Die Einführung von Sicherheitstechnik darf nicht nach dem Motto »PKI ist in – die brauchen wir jetzt auch« erfolgen, sondern muss sich an den Anwendungserfordernissen und den Ergebnissen der Risikoanalyse und des Risikomanagements orientieren. Nur so wird das Sicherheitsmanagement seine technischen Investitionen auch gegenüber dem Management auf Dauer rechtfertigen können.
- Das Sicherheitsmanagement muss sich als lösungsorientierter Dienstleister präsentieren, der Sicherheitsvorgaben für den speziellen Kontext eines Projektes oder eines Mitarbeiters in einfacher Form aufbereitet und zur Verfügung stellt, nach Möglichkeit in Form von »Quick Manuals«, Checklisten u.ä. Nur so wird die Motivation im Unternehmen, sich mit Sicherheitsfragen zu befassen, kontinuierlich anwachsen und zu einem breiteren Sicherheitsbewusstsein bei Management und Mitarbeitern führen.
- Für die nicht direkt mit Sicherheitsfragen konfrontierten Mitarbeiter können einfache Hinweise (KISS-Prinzip: Keep It Simple, Stupid), die als Risikoführer am Arbeitsplatz dienen, langfristig mehr an Sicherheitsgewinn bringen als neue aufwändig zu administrierende technische Lösungen. (Ein erfolgreiches und kostengünstiges Intrusion Detection System kann einfach die Wachsamkeit aller Mitarbeiter sein.)

Abbildung 11.2: Sicherheitsmanagement der dvg



11.4.3 Zusammenarbeit mit dem Risikomanagement

Wichtig bei der Behandlung von Risiken ist deren konsistente Behandlung im gesamten Unternehmen, unabhängig von Art und Herkunft. Risiken, ob wirtschaftliche, technische, organisatorische o.a., entstehen an den verschiedenen Stellen und werden in der dvg bei den Verantwortlichen (Risiko-Ownern) festgestellt und dem übergreifend tätigen Risikomanagement gemeldet. Dieses analysiert die Meldungen und stellt sie dem Management

verdichtet zur Verfügung, damit Gegenmaßnahmen eingeleitet werden können. Aufgabe des IT-Sicherheitsmanagements ist es an dieser Stelle, Methoden zur Erhebung der IT-Risiken zur Verfügung zu stellen, die die Risiko-Owner in die Lage versetzen, gegebenenfalls mit Coaching des Sicherheitsmanagements, Schwachstellen und Risiken zu beschreiben. Darüber hinaus muss das Sicherheitsmanagement natürlich Vorschläge zur Reduzierung der Risiken unterbreiten und Wirtschaftlichkeitsbetrachtungen von Sicherheitsmaßnahmen unterstützen. Auf diese Weise garantiert eine enge Zusammenarbeit zwischen Risiko- und Sicherheitsmanagement eine konsistente Behandlung von Risiken.

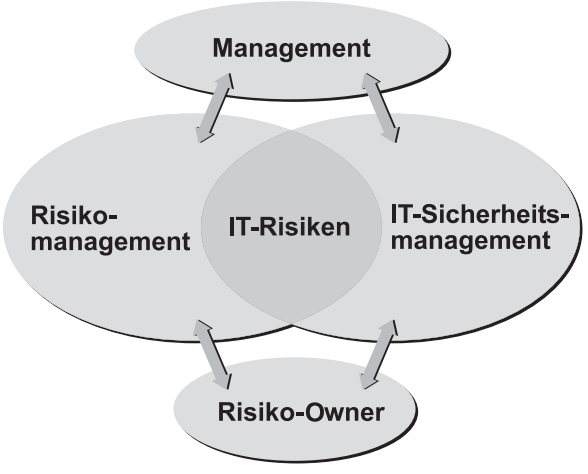


Abbildung 11.3: Risiko und Sicherheit

11.4.4 Praktische Erfahrungen

Sicherheitsziele

Wesentlich für die Begründung eines praktikablen Sicherheitsmanagements ist die Definition von Sicherheitszielen, an denen Sicherheitsmaßnahmen ausgerichtet und priorisiert werden können. Angesichts allenthalben schmaler werdender IT-Budgets ist es nicht mehr möglich, dass Sicherheitsverantwortliche aus ihrer eigenen Sicht heraus Maßnahmen ohne Wirtschaftlichkeitsbetrachtung durchführen. Vielmehr muss anhand vom Management verabschiedeter Sicherheitsziele die Grundlage für eine Messlatte gelegt werden, mit der Sicherheitsmaßnahmen wirtschaftlich bewertet werden können. Darüber hinaus geben Sicherheitsziele den Rahmen vor, in dem Incident-Response-Szenarien entwickelt werden können. Ansonsten wird bei konkreten Sicherheitsvorfällen die Reaktion in Panik oder per Zufallsentscheidung erfolgen und den potentiellen Schaden eventuell vergrößern. Beispiel hierfür ist eine Abwägung zwischen Vertraulichkeitssicherung und Verfügbarkeitssicherung, falls es z.B. einem Hacker gelungen ist, einen Online-Auftritt zu penetrieren. Beide Ziele lassen sich in solch einem Fall nicht gleichzeitig erreichen, hier geben die Sicherheitsziele die konkrete Handlungsanweisung vor.

Checkliste für Sicherheitstechnologen

Die dvg hat im Zusammenhang mit der Aufbereitung von zielgruppengerechten Sicherheitsrichtlinien z.B. in der Anwendungsentwicklung sehr gute Erfahrungen mit einer Checkliste und Risikorichtlinien gemacht, die die im Anwendungsentwicklungsprojekt für Sicherheit verantwortlichen Mitarbeiter in die Lage versetzen, ohne umständliches Suchen die im Projekt zu behandelnden Risiken zu beschreiben und strukturierte Sicherheitskonzepte in kurzer Zeit zu erstellen. Die Sicherheitsabteilung steht bei Problemen und Fragen als Coach zur Verfügung und übernimmt die Qualitätssicherung des Ergebnisses. Der verbreitete Fehler, Sicherheit erst im Nachhinein in bereits existierende Systeme implementieren zu müssen, wird auf diese Weise von Anfang an vermieden.

CERT (Computer Emergency Response Team)

Administratoren, egal für welchen Bereich, sind aufgrund ihrer Auslastung oft nicht in der Lage, die für ihre Systeme relevanten Sicherheitshinweise aus der Flut der täglich auftretenden Warnungen zu verfolgen und ihre Systeme dementsprechend zeitnah auf dem neusten Stand zu halten. An dieser Stelle können Expertenteams, die die für das Unternehmen relevanten Meldungen filtern und schnelle Maßnahmen vorschlagen, für das tägliche Sicherheitsmanagement erhebliche Vorteile bringen und das Unternehmen auch ohne Einsatz weiterer Technik ein gutes Stück sicherer machen.

Einführung neuer Techniken (z.B. Personal Digital Assistants, PDAs)

Das Sicherheitsmanagement hat sich ständig den Herausforderungen neuer Techniken zu stellen und sollte nicht als Behinderer sondern konstruktiver Ratgeber bei der Einführung zur Seite stehen. Die beispielsweise bei der Einführung von PDAs entstehenden Sicherheitsrisiken für die unternehmensinterne IT sind mit wachsender Funktionalität, Rechenleistung und den vielfältigen Kommunikationsschnittstellen der Geräte durchaus angestiegen, während die »out of the box« verfügbaren Sicherheitsfunktionen noch kaum ausgebildet sind. Hier wurde in der dvg nach Betrachtung der Risiken eine zentral gesteuerte Replizierungslösung der »wilden« Einzelplatzinstallation von PDAs vorgezogen. Diese bietet neben klaren Administrationsvorteilen auch einen erheblichen Sicherheitsgewinn.

Internet-Sicherheit

Unter Internet-Sicherheit wird häufig nur die Abschottung des Firmennetzes vom Internet über Firewalls etc. verstanden.

Wie vielschichtig dieses Gebiet sein kann, zeigt jedoch folgendes Beispiel: Viele Unternehmen machen sich keine Gedanken darüber, wie verwundbar Web-Präsenzen sein können, die oft von kleinen Dienstleistern ohne Sicherheits-Know-how erstellt und dann bei günstigen Web-Hostern plaziert werden. Abgesehen vom Imageverlust, der bei erfolgreichem Hacking einer solchen Web-Seite entstehen kann, sind auch schwerere Folgen denkbar.

Wenn beispielsweise von diesem Präsenzangebot auf eigene eigentlich gut gesicherte E-Commerce/E-Banking-Angebote verzweigt wird, könnte ein Hacker versuchen diesen Link auf eigene Seiten umzulenken und allzu sorglose Kunden zur Eingabe ihrer Daten veranlassen.

Dieses Beispiel zeigt die Notwendigkeit, im Sicherheitsmanagement gesamte Prozessketten und nicht isolierte Abläufe zu betrachten. Diese Prozessketten müssen insbesondere den Faktor Mensch miteinbeziehen, der in vielen Fällen der eigentliche Angriffspunkt eines Hackers ist, während ein Angriff auf ausgefeilte Sicherheitstechnik demgegenüber auch einem Hacker oft als zu aufwändig erscheint.

Neue Herangehensweise an Sicherheitsadministration

Ein weiteres die Komplexität des Sicherheitsmanagements reduzierendes Projekt beschäftigt sich mit den Möglichkeiten, die Rechte- und Gruppenadministration anwendungsübergreifend über ein Metadirectory zu steuern. Als Nebenprodukt beinhaltet dies z.B. die durch immer mehr Anwendungen auf verschiedenen Plattformen ausufernde Passwortadministration jedes Mitarbeiters wieder auf ein vernünftiges und daher auch risikoärmeres Maß zurückzuführen.

11.5 Fazit

Das Sicherheitsmanagement unterliegt landläufig vielen Vorurteilen: Es fordere teure und hohe Sicherheitsmaßnahmen, beschränke sich auf Sicherheitstechnik, schreibe ordnerfüllende, lebensferne Sicherheitsanweisungen und behindere das Unternehmen bei der Wertschöpfung.

Modernes Sicherheitsmanagement hat jedoch gänzlich andere Ziele:

Bedrohungen und Risiken müssen im Gesamtkontext bewertet werden, technische, organisatorische oder andere Maßnahmen zur Risikominimierung müssen eingeleitet und bei deren Umsetzung unterstützt werden. Das Sicherheitsmanagement ist letztlich eine Teilaufgabe jedes Mitarbeiters und muss sich den Veränderungen im Unternehmen schnell anpassen. Als ein Prozess unter vielen im Unternehmen sorgt es für die Einhaltung eines stabilen Sicherheitsniveaus sowie gesetzlicher und sonstiger Anforderungen. Sicherheits- und Risikomanagement zählen heute nicht mehr zu den lästigen Pflichten eines Unternehmens, sie sind zu einer wirtschaftlichen Säule geworden, auf der jedes Unternehmen aufbauen muss. Dieser Entwicklung kann nur durch ein modernes Sicherheitsmanagement Rechnung getragen werden, das nicht in den Regalen als »Schrankware« verstaubt, sondern jeden Unternehmensprozess und jeden Mitarbeiter als flexible Unterstützung begleitet.

Literatur. ***[1]*** *http://www.bis.org/publ/bcbc82.htm*

[2] http://www.bsi-global.com: ISO17799

[3] http://www.iso.ch

[4] http://www.bsi.de/gshb

12 IT-Sicherheit durch Risikomanagement

Henryk Konhäuser

12.1 Vorwort

Es war einmal ein Mann, der lebte glücklich und zufrieden. Er genoss jeden Tag und machte sich wenig Gedanken über Schicksal oder Vorsehung, bis er sich eines Tages, vielleicht aus purer Neugierde, vielleicht aber auch aus Leichtsinn, die Frage stellte, ob das Leben nicht seine eigenen Regeln hat. Und damit meinte er nicht etwa die Tatsache, dass es überall auf der Welt Gesetze und geschriebene Verhaltensnormen gibt, oder dass Rülpsen nach einer Mahlzeit in vielen Gegenden als ungezogen, in anderen wiederum als Kompliment an die Hausfrau gilt.

Nein, unser Mann war ein sauberer Denker. Die von Menschen für Menschen gemachten Regeln interessierten ihn nicht. Was er plötzlich wissen wollte, war die Antwort auf die Frage, ob das Leben, unabhängig von uns Menschen, seine ganz eigene Regelhaftigkeit hat. Die Frage, ob es neben der künstlich geschaffenen Ordnung der Welt, unbeeinflussbare Dinge gibt. Und während sich unser Mann noch Gedanken über Vorsehung und Bestimmung macht, wird ihm langsam klar, dass er, ohne es wirklich zu wollen, die Frage nach Ursprung und Beeinflussung von Risiken zu beantworten versuchte.

Noch nie vorher hatte er sich Gedanken um seine persönliche Sicherheit gemacht und nie war ihm irgend etwas passiert. Doch nun stellte sich ihm ernsthaft die Frage, ob dieses Verhalten auch künftig Garant für ein sorgenfreies Leben sein kann. Wie hatte er bloß bisher überlebt, seine Entscheidungen getroffen? War etwa sein bisheriges Leben und seine Handlungen absurd und wirklichkeitsfremd gewesen? Hatte er bisher nur Glück gehabt, dass ihm nichts passiert ist?

Und um dieser Frage auf den Grund zu gehen, suchte er Rat bei einem bekannten Wissenschaftler. So fragte er den Gelehrten, ob es nachweislich klare, eindeutige Regeln für richtige Entscheidungen in Lebensfragen oder verlässliche Gesetze zur Voraussage zukünftiger Ereignisse gäbe. Aber selbstverständlich antwortete dieser, dass auf diese Fragen ein Teilgebiet der Mathematik klare Antworten gäbe; nämlich die Wahrscheinlichkeitslehre und die sich auf sie gründende Statistik. So könne man zum Beispiel auf Grund jahrzehntelanger Untersuchungen mit an Sicherheit grenzender Wahrscheinlichkeit annehmen, dass die Benutzung von Verkehrsflugzeugen

für 99,92 Prozent der Passagiere vollkommen sicher sei, 0,08 Prozent aber bei Abstürzen ums Leben kämen. Als unser Mann dann nur noch wissen wollte, zu welchem Prozentsatz er persönlich gehört, waren die wissenschaftlichen Grenzen schnell ausgelotet.

Wäre er bloß nie auf diese unselige Frage gestoßen, denn mit ihr war es irgendwie um seine Zufriedenheit und seine Sorglosigkeit geschehen. Hatte er sich früher mit Urvertrauen und kindhafter Unschuld dem Leben hingegeben, wurde er nun regelrecht sicherheitsbesessen. So begann unser Mann immer intensiver nach potentiellen Risiken und ihren bestimmbaren Parametern zu suchen. Und obwohl er zusätzlich zu seinen Untersuchungen konkrete Maßnahmen ergriff, um die immer häufiger festgestellten Gefahren zu bannen, fühlte er sich nicht wirklich sicherer.

So begann unser Mann plötzlich sogar dem Horoskop in der Tageszeitung Aufmerksamkeit zu schenken. Was die guten und erfreulichen Voraussagen betraf, so traten sie entweder ein oder nicht. Ihr Nichteintreten war zwar enttäuschend, stellte aber keine besondere Gefahr für ihn dar. Die warnenden Voraussagen hingegen erwiesen sich als unvergleichlich verlässlicher. Denn als er eines Morgens beim Frühstück las, dass heute besondere Vorsicht geboten sei, da den unter seinem Sternzeichen Geborenen besondere Unfallgefahren drohe, entschied er sich zu Fuß zur Arbeit zu gehen und ließ das Auto stehen. An der Fußgängerunterführung angekommen erinnerte er sich daran, dass gehen zwar sicherer sein sollte als fahren, dass aber bekanntlich auch jeder 13. Schritt gefahrvoll sein soll, von der 13. Treppenstufe ganz zu schweigen. Auf der 12. Stufe angekommen entschied er folgerichtig, sein Schicksal heute nicht herauszufordern und übersprang die vermeintliche Gefahrenstelle, rutschte auf der 14. Stufe aus und knallte mit dem Kopf an das Treppengeländer. Das Horoskop hatte also recht!

Am Ende erging es unserem Mann fast so wie dem bekannten Tausendfüßler, der anfing darüber nachzudenken, wie es ihm eigentlich möglich war, mit so vielen Beinen mit solcher Eleganz und fließenden Harmonie sich sicher zu bewegen und wie er ein mögliches Verknoten der Beine verhindern konnte – er stolperte!

12.2 Einleitung

Hätte unser Mann das Risiko objektiv bewertet, wäre Hekate wohl nicht zum Zuge gekommen. Der Autor möchte mit den nachfolgenden Ausführungen einen Beitrag zur Bewertung von Risiken und zum Betrieb von Risikomanagement-Systemen geben. Er stellt nachfolgend ein System vor, welches nicht nur den eigentlichen Risikomanagement-Prozess und somit auch die Behandlung von IT-Risiken abzudecken vermag, sondern darüber hinaus auch die Basis für integrierte Management-Systeme darstellt. Die Tatsache, dass eine Vielzahl von Unternehmen bereits über zahlreiche unterschiedliche Management-Systeme wie z.B. Qualitäts-, IT-Sicherheits- und Umweltmanagement-Systeme verfügen, lassen eine ganzheitliche und interdisziplinäre Betrachtung angebracht erscheinen.

Das nachfolgend beschriebene Modell eines Risikomanagement-Systemes deckt daher nicht nur die Anforderungen der DIN EN ISO 9000ff. sowie DIN EN ISO 14000ff ab, es erfüllt darüber hinaus auch die Kriterien des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) sowie anderer internationaler Standards, wie zum Beispiel der ISO/IEC 17799, ein Standard für die Sicherheit von Informationssystemen. Die dargestellten Elemente stellen in Aufbau und Inhalt einen denkbaren Mindeststandard dar, unter dessen Zuhilfenahme eigene oder fremde Risikomanagement-Systeme miteinander vergleichbar und in der Folge auch bewertbar gemacht werden können.

12.3 Das System

Das in der Folge näher beschriebene Risikomanagement-System besteht aus acht Elementen, die sich in gleicher oder ähnlicher Form auch in den vorgenannten Normen wiederfinden.

Abbildung 12.1: Elemente eines Risikomanagement-Systems

Mit Ausnahme von Element IV »Prozess«, sind alle anderen Elemente Standardelemente eines integrierten Management-Systems. Aufbau und Verzahnung gewährleisten ein ziel- und prozessorientiertes Risikomanagement unter Integration vorhandener, gegebenenfalls auch zu vereinheitlichenden Managementelementen. Unter Anwendung dieser Risikomanagement-Methode können unter anderem IT-Risiken systematisch erfasst, analysiert, bewertet und minimiert werden. Gleiches gilt selbstverständlich auch für alle anderen Arten von Risiken.

12.3.1 Politik

Risikomanagement ist Chefsache! Wie ein Unternehmen mit Risiken umzugehen hat, muss die Unternehmensleitung entscheiden, getreu dem Grundsatz: »Wer die Verantwortung trägt, muss auch die Entscheidungskompetenz haben!«. Und unstrittig in diesem Zusammenhang ist auch die Tatsache: Je qualifizierter die Entscheidungsgrundlagen, desto niedriger die Fehlentscheidungsquoten.

Doch gerade die Frage nach potentiellen Risiken und Gefährdungsszenarien für Unternehmen, ist ähnlich facettenreich wie die Mineralogie, Biologie oder andere Grundsatzlehren. Demzufolge ist die Leitung eines Unternehmens gut beraten, sich vor einer Entscheidung über Chancen und Risiken qualifiziert informieren zu lassen. Und um diesen Entscheidungsprozess entsprechend zu initiieren, muss die Unternehmensführung Leitlinien festlegen, welche die unternehmerischen Ziele bezogen auf den Umgang mit Risiken definieren.

Dies könnte beispielhaft wie folgt aussehen:

»Den Unternehmenserfolg gefährdende Risiken werden umfassend inventarisiert, analysiert, minimiert und kontinuierlich kontrolliert.«

»Entscheidungsprozesse werden unter Wahrung unternehmerischer Chancen risikoorientiert systematisiert«.

»Unser Risikomanagement ist richtungsweisend und vereint die Sicherheitsansprüche unserer Mitarbeiter, Kunden und Gesellschafter.«

Als integrierter Bestandteil eines funktionierenden Risikomanagement-Systems, ist die Risikopolitik der Generalauftrag der Unternehmensleitung an die Gesamtorganisation zur Umsetzung der hier beschriebenen Ziele. Die Risikopolitik lässt bereits in begrenztem Umfange Rückschlüsse auf die Risikofreudigkeit und somit auch auf den Sicherheitsstandard eines Unternehmens zu. Damit ist die IT-Sicherheit integrierter Bestandteil der unternehmerischen Risikokultur.

12.3.2 Strategie

Erst die Risikostrategie konkretisiert die unternehmerischen Risikoziele. Aufbauend auf den allgemeinen strategischen Zielen, welche regelmäßigen Evaluierungen zu unterziehen sind, stützen und sichern konkrete funktionalstrategische Ziele die unternehmerischen Gesamtziele. Wichtig im Zusammenhang mit der Definition der strategischen Risikoziele ist in besonderem Maße die Orientierung an der Unternehmensstrategie. Risikomanagement kann nur dann erfolgreich und sinnvoll praktiziert werden, wenn der Risikobewältigungsprozess so zeitnah und effizient erfolgt, dass die Ergebnisse für anstehende Entscheidungen auch qualifiziert zur Verfügung stehen. Risikomanagement als integrierte Entscheidungsphase optimiert die Entscheidungsgrundlagen und minimiert die Überraschungseffekte.

Die Risikostrategie muss konkrete Maßnahmen verbunden mit verbindlichen Zeitfenstern enthalten. Risikostrategien sind von der für Risikomanagement verantwortlichen Abteilung zu erarbeiten und vor der Offizialisierung durch die für Unternehmensstrategie zuständige Stelle prüfen zu lassen. Dieser Ablauf gewährleistet, dass sich die Risikomanagement-Strategie nicht verselbstständigt, sondern vielmehr integrierter Bestandteil der Unternehmensstrategie ist und bleibt.

Die Einhaltung der festgelegten strategischen Ziele ist durch den/die Unternehmensstrategen zu auditieren. Die Erarbeitung und Vorlage eines Projektplanes für jedes Einzelziel ermöglicht ein noch effizienteres Auditing entlang der definierten Meilensteine.

12.3.3 Organisation

Verantwortlichkeiten

Die Gesamtverantwortung für Risikomanagement und somit selbstverständlich auch für den IT-Bereich betreffende Risiken, liegt naturgemäß bei der Geschäftsführung. Bei mehreren Geschäftsführern empfiehlt sich die Zuordnung in den Geschäftsbereich mit dem geringsten Risikopotential. Ist ein Vorsitzender der Geschäftsführung bestellt, bietet sich hier die verantwortliche Übernahme des Risikomanagements an. Risikomanagement als eine der wesentlichen Managementaufgaben ist bereits im Geschäftsverteilungsplan entsprechend zu dokumentieren.

Die Verantwortung erstreckt sich hierbei neben der Strukturierung und dem Betrieb einer Managementorganisation primär auf folgende Risikoprozesskette:

- Risikoinventur
- Risikobewältigung
- Risikokontrolle

Da ein ausgeprägtes Risikobewusstsein elementarer Bestandteil der Führungsaufgabe von Mitarbeitern in leitenden Positionen ist, muss es selbstverständlich sein, dass sie für den Risikoprozess in ihrem Bereich verantwortlich zeichnen (Risiko-Inhaber).

Aufbauorganisation

Ob und in welchem Umfang die Geschäftsführung alleine in der Lage ist, den Risikoprozess ohne weitere Unterstützung eigenverantwortlich und für alle wesentlichen Risikopotentiale durchzuführen, hängt stark von der Größe und Komplexität des Geschäftes ab. Zusätzliche Schwierigkeiten können sich nicht nur aus unterschiedlichen Bewertungsmaßstäben, Sichtweisen, Beziehungen oder Affinitäten ergeben; Interessenskonflikte der Risiko-Inhaber sind an der Tagesordnung, zwangsläufig und eher normal.

Daher ist es unerlässlich, neben dem Risiko-Inhaber die Funktion des Risikomanagers einzurichten, der die Risk-Management-Methode des Betriebes vereinheitlicht und die Kommunikation im Rahmen der Risikoprozesskette zwischen den betroffenen Fachabteilungen und der Geschäftsführung standardisiert und aufrecht erhält.

Funktionsbeschreibungen

Risikomanager. Stellenziel dieser Funktion ist die Konzeption und Organisation sowie der Betrieb und die Weiterentwicklung eines auf die jeweiligen Unternehmensgegebenheiten angepassten Risikomanagement-Systems. Der Kompetenzschwerpunkt des Risikomanagers liegt klar im Risikomanagement-Prozess, der Methode zur Identifikation, Bewertung, Bewältigung und Überwachung unternehmerischer Risiken. Der Risikomanager verfasst, veröffentlich und pflegt die notwendige Risikodokumentation.

Darüber hinaus stellt er die Kommunikation zwischen den Risiko-Inhabern und der Unternehmensleitung hinsichtlich des Risikoportfolios sicher, führt Risiko-Schulungen durch und gewährleistet im Sinne eines »Vier-Augen-Prinzips« die zentrale Überwachung der Unternehmensrisiken.

Risiko-Inhaber. Der Risiko-Inhaber ist derjenige, in dessen Verantwortungsbereich sich ein Risiko auswirkt. Der Risikomanager bedient sich bei der Risikoinventur und -bewertung seiner Mithilfe, da er detaillierte Kenntnisse über Zusammenhänge und Abläufe in seinem Aufgabenbereichen aufweisen kann. Es ist von entscheidender Bedeutung, dass die Risikolandschaft des Risiko-Inhabers möglichst umfassend untersucht wird und sich der Risiko-Inhaber darüber im klaren ist, dass die Identifikation, Bewältigung und Überwachung von Risiken der Minimierung des Risikopotenzials in seinem Aufgabenbereich dient und somit von existentieller Bedeutung für den Erfolg seiner Abteilung und des ganzen Unternehmens ist.

12.3.4 Prozess

Der eigentliche Risikoprozess stellt einen in sich geschlossenen Regelkreislauf dar. Diese Methode gewährleistet, dass sowohl einmal erfasste Risiken nicht in Vergessenheit geraten, als auch neue Risiken systematisch identifiziert werden.

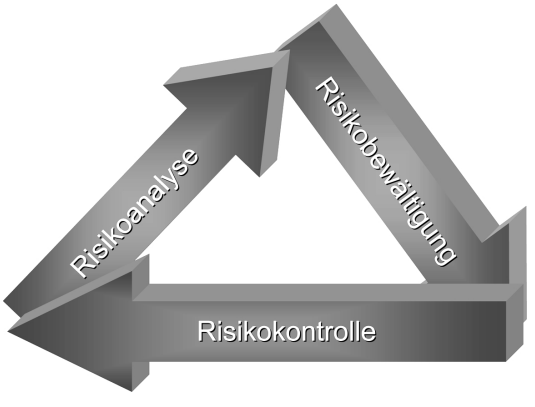


Abbildung 12.2: Risikoprozess

Risikoinventur

Identifikation. Um einen Überblick über die unternehmensweit vorhandene Risikostruktur zu erhalten, ist zunächst eine Inventarisierung aller potenziellen Risiken, der vorhandenen Maßnahmen zur Risikobewältigung sowie der jeweiligen Frühwarnindikatoren durchzuführen. Zwangläufig integriert ist dabei auch mögliches IT-Risikopotenzial. Eine isolierte Betrachtungsweise der IT-Landschaft sollte unterbleiben, um die möglichen IT-Gefährdungspotenziale einem objektivierten Vergleich im Sinne einer ganzheitlichen Risikoprofilierung unterziehen zu können. Eine kleine Auswahl denkbaren Risikopotenzials ist der nachfolgenden Grafik zu entnehmen.

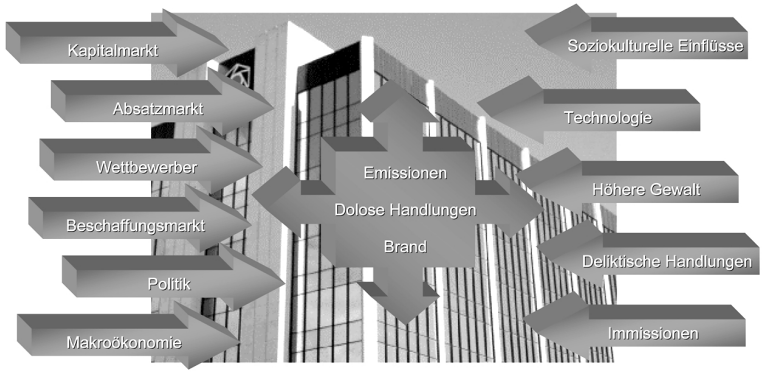


Abbildung 12.3: Denkbares Risikopotential

Sinnvollerweise wird die Risikoidentifikation und -inventarisierung durch den Risikomanager in direkter Zusammenarbeit mit den jeweiligen Risiko-Inhabern durchgeführt. Dieser Prozess gewährleistet einerseits eine durchgängige und möglichst lückenlose Risikobetrachtung unter Nutzung von Risiko- und Fach-Know-how und andererseits eine standardisierte Risikosensibilisierung. Als Ergebnis erhält das Unternehmen einen individuellen Risikokatalog, der neben den entdeckten Gefährdungsszenarien mögliche Erscheinungsformen, Ursachen und potenzielle Auswirkungen beschreibt.

Ein entsprechendes DV(Datenverarbeitungs)-Tool als Client-Server-Version, mit möglichst freier Editierbarkeit, ist dabei von unschätzbarem Wert.

Da sich die Risikostruktur eines Unternehmens kontinuierlich ändern kann, ist ein zeitnahes Screening des möglichen Risikopotenzials sowohl zentral wie auch dezentral unerlässlich. Darüber hinaus muss die Überprüfung des Risikoportfolios zyklisch mindestens einmal jährlich durchgeführt werden. Veränderungen des Risikokataloges sind grundsätzlich zentral zu pflegen.

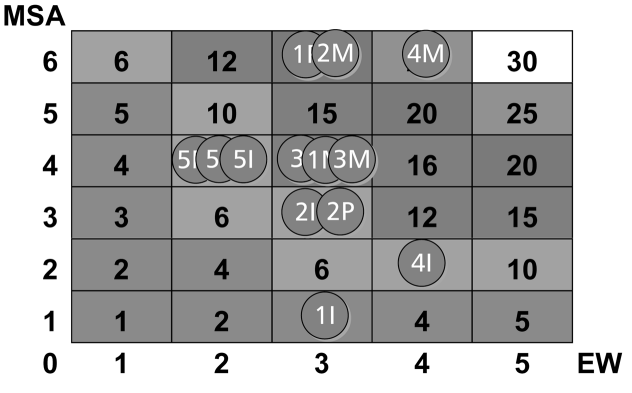
Bewertung. Für jedes identifizierte Risiko ist eine Bewertung vorzunehmen. Bei der Berechnung des Risikos werden materielle (M), personelle (P) und immaterielle (I) Risikofaktoren berücksichtigt.

Abbildung 12.4: Risikofaktoren

Die drei aufgezeigten Faktoren ermöglichen eine ausgewogene und dennoch dezidierte Betrachtung der unternehmerischen Risikostruktur. Sie verfügen über individuelle, frei editierbare Bewertungsmaßstäbe und werden über einen Umrechnungsschlüssel miteinander vergleichbar gestaltet. So können materielle Schäden wie der Ausfall der DV-Anlage ebenso qualifiziert bewertet werden wie personelle und immaterielle Auswirkungen, ohne die sonst zwangsläufige Materialisierung oder Kumulation durchführen zu müssen.

Die Werte selber resultieren aus der Multiplikation der jeweiligen maximalen Schadenshöhe (MSA) mit der Eintrittswahrscheinlichkeit (EW) eines einzelnen Risikos.

Abbildung 12.5: Wertetabelle von Risiken, Risikoprofil



Die Risikobewertung kann sinnvoll nur mit Hilfe standardisierter Software-Instrumente durch den Risiko-Inhaber unter Mitwirkung des Risikomanagers durchgeführt werden.

Risikoprofil. Anhand der ermittelten Risikofaktoren vergleicht der Risikomanager die unterschiedlichen Risiken hinsichtlich ihrer Bedeutung. Hierzu nimmt er eine Einstufung vor. Die Risikoeinstufung führt er durch, indem die ermittelten Risikofaktoren in Stufen eingeordnet werden. Die Festlegung einer Wesentlichkeitsgrenze durch die Geschäftsführung dient der sicheren Identifikation der Top-Risiken.

Im Ergebnis entsteht ein Risikoprofil, das die Netto-Risiken der jeweiligen Szenarien beschreibt. Durch Festsetzung einer Wesentlichkeitsgrenze wird aus dem Risikoprofil ersichtlich, welche Risiken unbedingt mit Maßnahmen der Risikobewältigung versehen werden müssen (Top-Risiken).

Das Risikoprofil ist einem kontinuierlichen Wandel unterworfen. Dadurch, dass die Top-Risiken mit Maßnahmen versehen werden, erfahren sie eine geringere Einstufung und finden sich weiter unten im Profil wieder. Folgerichtig stehen ständig neue Risiken an der Spitze, mit denen entsprechend verfahren wird. Die Risikoeinstufung ermöglicht die Ermittlung eines Risikoprofils (Prioritätenliste). Der Risikomanager bildet dieses Risikoprofil, indem das Risiko mit dem höchsten vorkommenden Risikofaktor (und zwar unabhängig davon, ob materiell, personell oder immateriell) an die erste Stelle gestellt wird. Enthalten zwei Risiken diesen höchsten Risikofaktor, wird nach dem nächst höheren Risikofaktor unterschieden; wenn immer noch Gleichheit besteht, nach dem Dritten. Sind zwei Risiken in allen drei Risikofaktoren identisch, so teilen sie sich die Position im Risikoprofil.

Risikobewältigung

Sicherheitsziele. Für jedes erfasste Risiko ist ein Sicherheitsziel zu definieren. Dies geschieht unter Einbindung der Geschäftsführung. Hierbei ist besonders auf die Berücksichtigung etwaiger Chancen zu achten. Denn es macht wenig Sinn, ein hohes Risiko ohne erkennbaren Vorteil einem gleichwertigen Risiko mit großem Gewinnpotential vorzuziehen. Mit der Definition von Sicherheitszielen legt die Geschäftsführung fest, welches Risiko zur Wahrung unternehmerischer Chancen eingegangen werden darf. Als Grundlage dient das im Ergebnis der im vorangegangenen Prozessschritt Risikoanalyse entstandene Risikoprofil, in dem jedes Risiko durch drei Risikofaktoren charakterisiert wird.

Bei den Top-Risiken beginnend, wird für jedes Risiko festgelegt, bis auf welchen Wert die Risikofaktoren gesenkt werden sollen. Primäres Ziel ist es dabei, Top-Risiken durch geeignete Maßnahmen so weit zu minimieren, dass die Risiko-Faktoren unter den für Top-Risiken festgelegten Grenzwert gesenkt werden (z.B. < 15).

Mechanismen. Abhängig vom Sicherheitsziel werden jedem Risiko die passenden und angemessenen Maßnahmen der Risikobewältigung (Sicherheitsmechanismen) zugeordnet. Sicherheitsmechanismen reduzieren vorhandene Risikowerte. Um hierbei eine entsprechende Quantifizierung der Veränderungspotenziale erkennen zu können, werden die einzelnen Maßnahmen in sechs Mechanismusklassen (MK) eingeordnet.

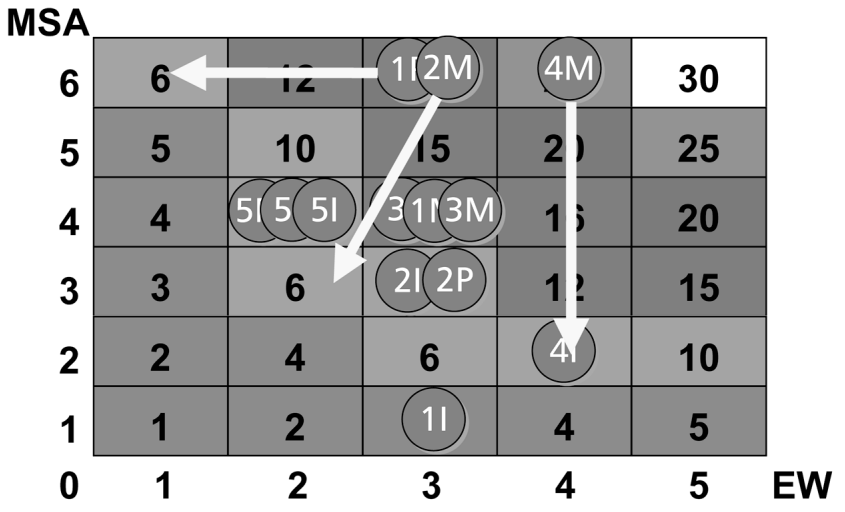


Abbildung 12.6: Zielanforderungen im Risikoprofil

Maßgeblichen Einfluss auf die Wahl des Mechanismus haben die Höhe des drohenden Risikos, die potenziellen Chancen sowie der Aufwand für die Einführung des jeweiligen Mechanismus. Zu präferieren sind wirtschaftliche und pragmatische Lösungen, die die Entscheidungsprozesse nicht lähmen.

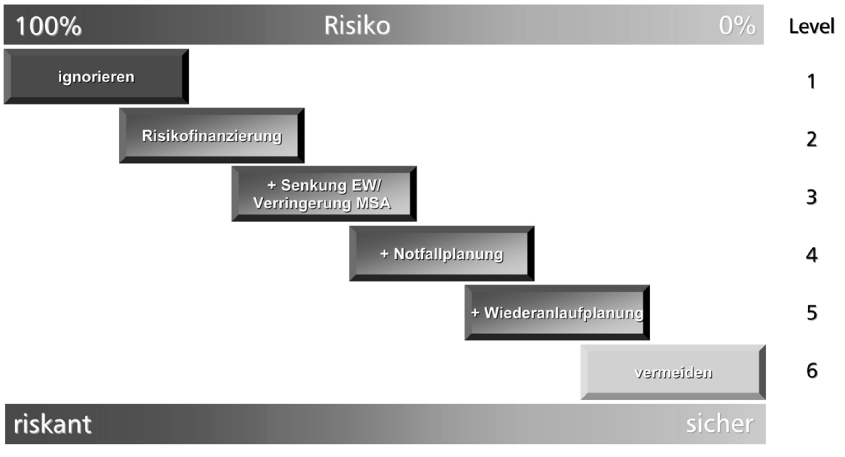


Abbildung 12.7: Mechanismusklassen

Durch die Zuordnung der standardisierten Mechanismusklassen zu den jeweiligen Risiken erstellt der Risikomanager das Sicherheitsprofil, in dem jedem Risiko der erreichte Sicherheitslevel zugeordnet ist. Dieses gibt Aufschluss über die Risikokultur des Unternehmens.

Risiko-Aktivitäten-Plan. Die zur Bewältigung eines Risikos zu ergreifenden Sicherheitsmechanismen werden in Form zu treffender Einzelmaßnahmen vom Risiko-Inhaber in Zusammenarbeit mit dem Risikomanager festgelegt.

Um auch die Umsetzung der Mechanismen entsprechend dem Risikoportfolio überwachen zu können, werden alle Einzelmaßnahmen in einen Risiko-Aktivitäten-Plan (Risk Activity Plan, RAP) eingearbeitet. Dieser enthält neben den umzusetzenden Maßnahmen die Umsetzungsverantwortlichen, die Meilensteine sowie die erwarteten Kosten der Maßnahme. Für die Detailplanung ist der Risiko-Inhaber verantwortlich.

Der RAP gilt als Arbeitsauftrag für die mit der Umsetzung der Maßnahmen Beauftragten. Er wird der Geschäftsführung monatlich präsentiert. Handlungsbedarf wird somit zeitnah und effektiv kommuniziert und initiiert.

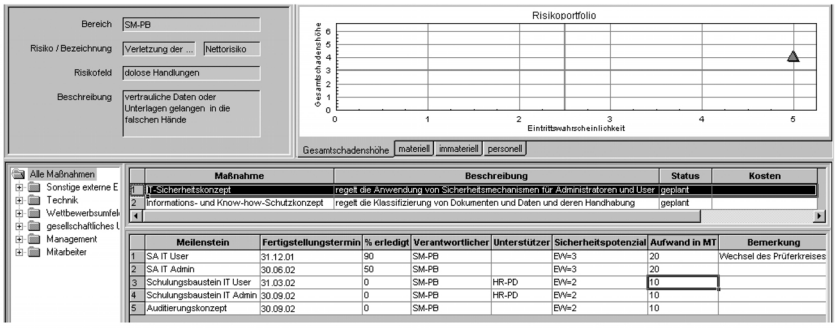


Abbildung 12.8: Risiko-Aktivitäten-Plan

Testat. Vor der endgültigen Einführung eines Mechanismus erfolgt die Abnahme durch den Risikomanager. Dieser prüft, ob die Vorgaben umgesetzt worden sind. Die Abnahme wird formell durch ein internes Testat bestätigt. Dieses wiederum ist Grundlage für die anschließende Überleitung in die Auditierungsphase. Grundsätzlich gilt, dass alle testierten Mechanismen einer regelmäßigen Kontrolle durch den Risikomanager unterliegen.

Risikokontrolle

Die Risikokontrolle teilt sich auf in die Überwachung bereits identifizierter Risiken sowie der Früherkennung neuer Risiken.

Risikoüberwachung. Bei der Risikoüberwachung gilt es, geeignete Frühwarnindikatoren zu monitoren. Hierzu werden die durch das Risiko bedrohte Zielgröße sowie zugehörige Einflussgrößen ermittelt. Dieser Prozessschritt lässt sich sinnvollerweise bereits im Rahmen der Risikoidentifikation mit erledigen.

Die Einflussgrößen selber haben bestimmte Anforderungen zu erfüllen. So müssen sie einerseits messbar sein und andererseits mit der Zielgröße korrelieren, sowie eine gewisse Prognosefähigkeit aufweisen.

Frühwarnindikatoren sind durch den Risikomanager in Zusammenarbeit mit dem Risiko-Inhaber und den jeweiligen Fachbereichen zu ermitteln. Hierbei werden sowohl die Sollwerte wie auch die Toleranzgrenzen festgelegt, bei deren Unter- bzw. Überschreitung wiederum geeignete, vorher festgelegte Gegenmaßnahmen einzuleiten sind. Die Überwachung dieser Frühwarnindikatoren und die Meldung über das Erreichen der Toleranz-

schwellen erfolgt zeitnah an den Risikomanager und obliegt dem Risiko-Inhaber. Soweit Toleranzwerte zum Beispiel elektronisch überwacht werden können, bietet sich auch eine automatische Informationsweiterleitung an.

Risikofrüherkennung. Um parallel zur Risikoüberwachung auch eine qualifizierte Risikofrüherkennung durchführen zu können, ist es unabdingbar, den Risiko-Inhaber in ausreichendem Maße zu schulen und zu sensibilisieren. Denn der Risiko-Inhaber ist üblicherweise der Erste, der entscheidende Änderungen in seiner Risikolandschaft überhaupt zu erkennen vermag.

Der wesentliche Unterschied zur Risikoüberwachung besteht darin, dass wir bei der Risikofrüherkennung nicht über vorherbestimmbare »harte Indikatoren« verfügen. Frühwarnschwellen sind somit nicht vorhanden. Die Risikoidentifikation über »weiche Indikatoren« findet mehr oder weniger in der Kreativität und Sensibilität der Risiko-Inhaber ihren Ursprung. Hierbei ist von entscheidender Bedeutung, dass potenzielle Risiken, erscheinen sie auch noch so abstrakt, den Risikoregelkreislauf absolvieren. Nur so ist sichergestellt, dass frühzeitig auch auf noch nicht näher verifizierbare Risiken reagiert werden kann.

12.3.5 Dokumentation

Der Aufbau der Risiko-Dokumentation gliedert sich zunächst in zwei grundsätzliche Bereiche:

- Verfahrensdokumentation
- Risikodokumentation

Verfahrensdokumentation

Verfahren und Prozesse lassen sich am ehesten über eine möglichst schlanke Dokumentationshierarchie beschreiben. Die jeweiligen Inhalte bauen aufeinander auf. Bewährt hat sich folgende Struktur:

- Leitlinie
- Richtlinie
- Anweisungen

Leitlinie. Die Risikomanagement-Leitlinie beschreibt die Risikopolitik des Unternehmens. Gleichfalls stellt sie die Verbindlichkeitserklärung der Gesamtgeschäftsführung dar und ist Auftrag an die jeweilige Gesamtorganisation, die beschriebenen Ziele umzusetzen und zu wahren.

Die Leitlinien bilden die Grundlage für das Risikomanagement-System und das Selbstverständnis aller Beschäftigten des Betriebes.

Für die Erarbeitung der Risiko-Leitlinien ist der Risikomanager verantwortlich und zuständig. Die inhaltliche Prüfung erfolgt z.B. durch den Leiter Strategische Unternehmensentwicklung und die Genehmigung durch die Gesamtgeschäftsführung.

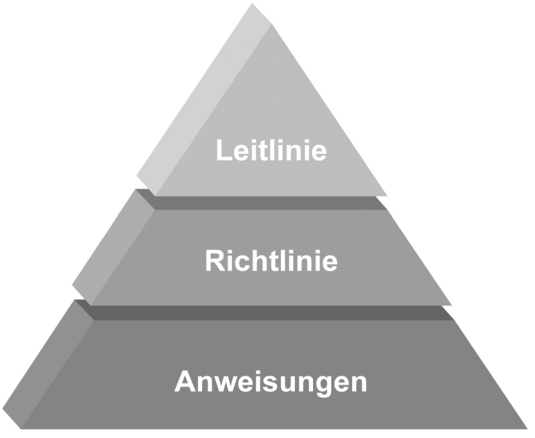


Abbildung 12.9: Dokumentationshierarchie

Richtlinie. Die Risikomanagement-Richtlinie beschreibt das Risikomanagement-System, dessen Aufbau, die Elemente und die Hauptprozesse. Sie steckt die Rahmenbedingungen des Systems ab und bildet die Grundlage für alle weiteren Regelungen und Anweisungen.

Die Erarbeitung der Risikomanagement-Richtlinie ist Aufgabe des Risikomanagers. Die inhaltliche Prüfung erfolgt beispielsweise durch den Leiter Interne Revision, die Genehmigung durch den für Risikomanagement verantwortlichen Geschäftsführer.

Anweisungen. Anweisungen sind verbindliche Handlungs- und Verhaltensvorgaben, die keinerlei Handlungsspielräume zulassen. Hierbei unterscheiden wir Risikoanweisungen und Arbeitsanweisungen.

Risikoanweisungen regeln, über die eigene Abteilung hinaus, Verhalten, Verfahren und/oder Prozesse zur Wahrung der Risikoziele unter Berücksichtigung der Rahmenvorgaben aus der Risikomanagement-Richtlinie. Risikoanweisungen werden inhaltlich von einer repräsentativ betroffenen Abteilung (z.B. Personalwesen, Produktion, Entwicklung) geprüft und vom Risikomanager genehmigt. Eine typische Risikoanweisung ergeht üblicherweise an alle Risiko-Inhaber.

Arbeitsanweisungen hingegen regeln im Detail das Verhalten der Mitarbeiter der Abteilung Risikomanagement selber sowie alle Verfahren und Prozesse im Rahmen der Durchführung des Risikoprozesses. Sie werden in der Regel ebenfalls vom Risikomanager selber verfasst.

Risikodokumentation

Das Identifizieren, Bewerten und Kommunizieren von Risiken muss transparent und nachvollziehbar gestaltet sein. Eine entsprechende Dokumentation ist unerlässlich. Folgende Dokumentationen sind daher mindestens vorzusehen:

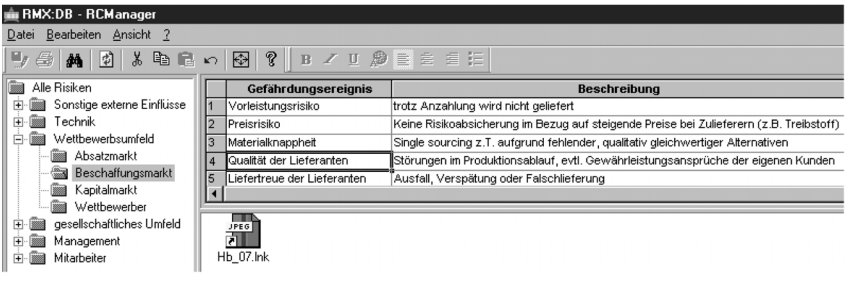
- Risikokatalog
- Risikoreport
- Risikoübersichtsplan

Risikokatalog. Zahlreiche Aspekte sprechen für den Aufbau und die Verwendung eines strukturierten Risikokataloges zum Einstieg in die Risikoidentifikation. Dieser umfasst neben potentiellen Gefahren ihre möglichen Erscheinungsformen, Ursachen und Auswirkungen. Praktische Beispiele wie Schadensberichte von Versicherern, Presseveröffentlichungen oder sogar Vorfälle aus dem eigenen Unternehmen können die Visualisierung und Sensibilisierung entscheidend stützen.

Eine weitere Indikation für einen dokumentierten Risikokatalog ist das einheitliche Verständnis der Risiko-Inhaber über Gefährdungspotenziale. Da jeder Risiko-Inhaber vornehmlich über seine eigenen Lebenserfahrungen einen äußerst individuellen Fokus in Risikofragen entwickelt hat, hilft die Beschreibung bei der standardisierten Betrachtung.

Darüber hinaus bietet erst der Risikokatalog die Möglichkeit, die anschließende Risikobewertung systematisch durchzuführen. Bewährt hat sich in diesem Zusammenhang eine Aufteilung der Risikopotenziale in »Muss- und Optionalrisiken«. Zuvor festgelegte Risiken müssen damit zwangsläufig einer Bewertung unterzogen werden, andere wiederum können in Abhängigkeit der tatsächlichen Risikosituation geprüft werden.

Abbildung 12.10: Risikokatalog



Risikoreport. Von besonderer Bedeutung ist die Dokumentation der individuellen Quantifizierung der einzelnen Risikopotenziale. Diese erfolgt in einem Risikoreport, welcher wiederum folgende Mindestangaben enthält:

- Betroffener Bereich
- Risiko-Inhaber
- Risikobeschreibung
- Risikowert Brutto
- Zielwert
- Einzuführende Mechanismen
- Risikowert Netto

Die vorgenommene Bewertung einzelner Risiken muss transparent und nachvollziehbar sein. Ob Wirtschaftsprüfer, Gesellschafter, Geschäftsführer oder andere verantwortliche Führungskräfte eines Unternehmens, alle müssen in der Lage sein, die getroffenen Annahmen hinsichtlich Eintrittswahrscheinlichkeit und Schadensauswirkungen reproduzieren zu können.

Ausgehend vom Bruttopotenzial eines Risikos muss das gewünschte Ziel, wie auch die sich aus der Einführung von Sicherheitsmechanismen ergebenden Risikopotenzialveränderungen, plausibel dargestellt sein.

Die Archivierung der jeweils evaluierten Risikobewertungen ist selbstredend und ermöglicht erst die dezidierte Betrachtung der Entwicklung einzelner Risiken und Bewältigungsstrategien.

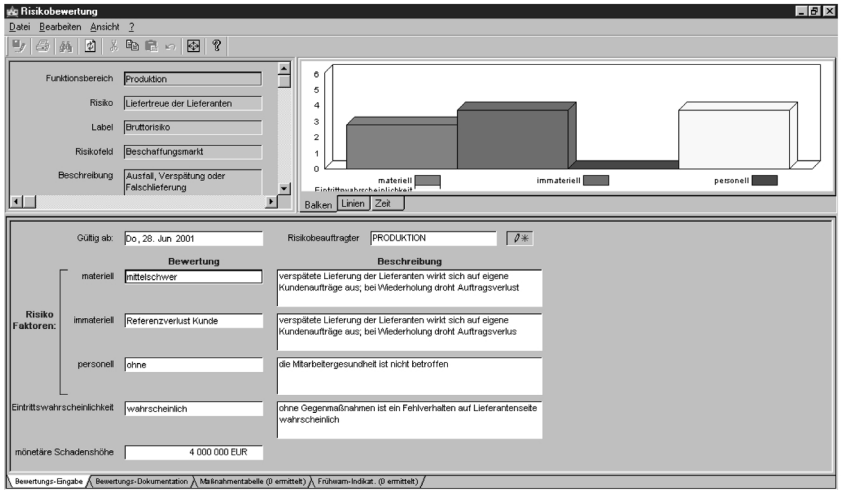


Abbildung 12.11: Risikoreport

Risikoübersichtsplan. Die aus den vorgenannten Risikobewertungen hervorgehenden Einzelinformationen miteinander zu vergleichen oder tendenzielle Entwicklungen über die Zeitachse darzustellen, ist Aufgabe des Risikoübersichtsplans.

Dieser ist, sofern kein akuter Handlungsbedarf besteht, in regelmäßigen Zeitabständen der Unternehmensleitung zur Kenntnis zu geben. Hierzu bieten sich beispielsweise die Geschäftsführungssitzungen des Unternehmens an. Die Unternehmensleitung hat nicht nur das Recht, sondern vielmehr auch die Verpflichtung, sich in überschaubaren Zeitabständen über das Risikoportfolio und den Stand der Bewältigungsaktivitäten ein Bild zu machen.

Abbildung 12.12: Risikoübersichtsplan

Bereich: Produktion

Platz	Risiko:	*Beschreibung:*	Risk-Owner	Brutto-MF	Brutto-IF	Brutto-PF	Netto-MF	Netto-IF	Netto-PF
1	Materialknappheit B N	Single sourcing z.T. aufgrund fehlender, qualitativ gleichwertiger Alternativen	PRODUKTION	16	16	0	12	12	0
2	Qualität der Lieferanten RMX10.ENT1003 [Zeichenfolge] B N	Störungen im Produktionsablauf, evtl. Gewährleistungsansprüche der eigenen Kunden	PRODUKTION	12	16	0	6	8	0
2	Liefertreue der Lieferanten B N	Ausfall, Verspätung oder Falschlieferung	PRODUKTION	12	16	0	6	8	0
4	Preisrisiko B N	Keine Risikoabsicherung im Bezug auf steigende Preise bei Zulieferern (z.B. Treibstoff)	PRODUKTION	6	0	0	0	0	0

12.3.6 Schulung

Das Element Schulung berücksichtigt alle aktuell erkennbaren sowie zukünftig zu erwartenden betrieblichen Erfordernisse, bezogen auf den Bedarf notwendiger Wissensvermittlung aus dem Bereich Risikomanagement. Es dient vornehmlich der Risikosensibilisierung, dem Anwendungs- und Durchführungstraining und der Schaffung einer einheitlichen Risikokultur.

Schulungsplan

Der Schulungsplan umfasst das komplette Angebot aller von der Abteilung Risikomanagement angebotenen bzw. geforderten Schulungsmaßnahmen. Im Einzelnen enthält er folgende Angaben:

- Bezeichnung der Schulungsmaßnahme
- organisations- oder funktionsorientierte Zielgruppe
- Schulungszeitpunkt
- Wiederholungszyklus

Abbildung 12.13: Risikomanagement-Schulungsplan

SCHULUNGSPLAN **Risikomanagement** Seite 1/1

	Zielgruppen organisationsorientiert					Zielgruppen funktionsorientiert					Schulungszeitpunkt					Wiederholungszyklen				
Schulungsmodul/ Schulungsbaustein	GF	GL	OFK	FK	MA	SI	PV	PR	REN	BSH	vor	-3	-6	-12	n.B.	4/12	2/12	1/12	1/24	n.B.
Risikosensibilisierung	✓	✓	✓	✓	✓						✓								✓	
Risiken im Treasury				✓	✓							✓						✓		
Personalrisiken				✓	✓					✓					✓		✓			
Risiken in der Produktion				✓	✓	✓		✓					✓							
IT-Sicherheit	✓	✓	✓	✓	✓	✓					✓									✓
Vertriebsrisiken	✓	✓	✓	✓	✓									✓				✓		

Der Risikomanagement-Schulungsplan ist vom Risikomanager jährlich zu evaluieren und in Abstimmung mit dem Leiter Personalwesen festzulegen. Der Schulungsplan ist verbindliche Planungsvorgabe für die Führungskräfte des Unternehmens. Die Veröffentlichung wird sinnvollerweise an die

allgemeinen unternehmerischen Planungszyklen angepasst, so dass die gewünschten Schulungsmaßnahmen von den jeweiligen Verantwortlichen sowohl terminlich wie auch budgetbezogen eingeplant werden können. Diese wiederum sind gehalten, alle nicht bedarfsorientierten Schulungsangebote für das kommende Jahr entsprechend den Vorgaben des Schulungsplanes für ihre Mitarbeiter zwingend mit einzuplanen.

Schulungsbaustein

Alle Beschäftigten eines Unternehmens müssen berechtigt sein, anlass- und zielbezogene Schulungsmaßnahmen initiieren zu dürfen. Die eigentliche Entwicklung neuer Schulungsbausteine ist und bleibt jedoch Aufgabe der Abteilung Risikomanagement.

Schulungsbausteine beschreiben ein Schulungsthema systematisch und enthalten folgende Mindestinformationen:

- Bezeichnung
- Zielgruppe
- Präambel
- Lernziele
- Lerninhalte
- Zeitbedarf
- Lernstufe
- Lehrmethode
- Lehrmittel

Der Risikomanager koordiniert alle Schulungsangebote und prüft die Sinnhaftigkeit und Machbarkeit in Absprache mit der für Fort- und Weiterbildung verantwortlichen Abteilung. Er genehmigt neue Schulungsbausteine und pflegt diese in den Risikomanagement-Schulungsplan ein.

Schulungsmodul

Häufig bietet es sich an, nicht nur ein Schulungsthema isoliert zu beleuchten, sondern mehrere Themen zusammenzufassen. Die beschriebenen Schulungsbausteine bieten hierfür eine breite Gestaltungsvielfalt zum Aufbau von Schulungsmodulen. Art- oder themenverwandte Bausteine werden hierbei sinnvoll miteinander kombiniert, um Schulungsmaßnahmen effizienter und rationeller zu gestalten.

So bietet sich z.B. die Zusammenlegung von Themen wie IT-Security, Informations- und Know-how-Schutz an.

Ausbildungsplan

Auf der Basis der verbindlichen Schulungsplanung erfolgt die Ausbildungsplanung. Diese wird üblicherweise durch das Personalwesen erstellt und gibt Aufschluss über die für alle Beschäftigten geplanten und terminierten Schulungsmaßnahmen.

Die Durchführung von Pflichtveranstaltungen sind hierbei automatisch durch die mit Fort- und Weiterbildung beauftragte Abteilung zu initiieren; dagegen orientiert sich die Durchführung von Wahlveranstaltungen an der jeweiligen Nachfrage.

12.3.7 Kommunikation

Nicht kommunizieren geht nicht! Nichts sagen bedeutet passiv kommunizieren. Keine Informationen zu geben führt dazu, unnötigen Spielraum für Geschichten, Gerüchte und Fehldarstellungen zu bieten.

Es ist daher von elementarer Bedeutung Art, Form, Inhalt, Zyklus und Umfang der Risikokommunikation sowohl firmenintern wie auch extern zu regeln und zu pflegen. Wir unterscheiden hierbei grundsätzlich folgende Kommunikationsarten:

- Regelmäßige Kommunikation
- Ereignisorientierte Kommunikation

Regelmäßige Kommunikation

Unternehmensintern. Zur Information aller Beschäftigten über Risikoangelegenheiten bieten sich die klassischen, unternehmenseigenen Informationsorgane wie Mitarbeiterzeitschriften, Intranet oder sogar ein abteilungsspezifisches Mitteilungsorgan an. Regelmäßige Artikel schärfen die Sinne der Belegschaft, zeigen dass ein System lebt und sensibilisieren.

So sind beispielsweise Berichte über erfolgreiche Risikoprävention oder die Auditergebnisse externer Prüfinstitutionen nicht nur informativ, sie motivieren auch und regen die Beteiligungsbereitschaft an.

Geschäftsbericht. Unternehmensbezogene Risiken nach außen zu kommunizieren, erfordert ein hohes Maß an Risikokultur und Professionalität. Der jährliche Geschäftsbericht ist hierfür eine hervorragende Plattform und Pflicht.

Finden sich meist auf den ersten Seiten der Image-Broschüren doch die Ziele und Leitlinien der Unternehmen wieder, so ist es nur konsequent, an anderer Stelle auch über die jeweiligen Ergebnisse und Aktivitäten zu berichten.

Über Risiken offen zu kommunizieren bedeutet in erster Linie zu zeigen, dass Gefährdungspotential überhaupt erkannt wurde und nicht einfach negiert wird. Selbst wenn in Einzelfällen die Risikominimierungsstrategie

fehl schlägt oder die Risiken die Chancen übersteigen, ist der offene und ehrliche Umgang mit Risikopotenzial eher ein klares Zeichen für Ehrlichkeit und somit ein klarer Vertrauensbonus.

Ereignisorientierte Kommunikation

Ad-hoc-Meldungen. Besondere Situationen erfordern besondere Maßnahmen. Dieser Grundsatz trifft selbstverständlich in besonderem Maße auf aktuelle und gravierende Veränderungen der Risikolandschaft eines Unternehmens zu. Überschreitet ein Risiko einen zuvor definierten Grenzwert oder wird ein Risiko neu identifiziert, welches zuvor festgelegte Wesentlichkeitsparameter überschritten hat, gilt es, die Unternehmensleitung und gegebenenfalls auch die Gesellschafter umgehend darüber zu informieren.

Als probates Mittel hierfür hat sich die ad hoc Meldung erwiesen, die im Übrigen für Aktiengesellschaften zur externen Kommunikation gesetzlich sogar vorgeschrieben ist. In Form, Aufbau und Inhalt mit dem zuvor beschriebenen Risikoreport vergleichbar, dient sie zur Mitteilung ohne Zeitverzug.

12.3.8 Auditierung

Zur Überprüfung des Vorhandenseins, der Effizienz und auch der Notwendigkeit sind sowohl die testierten Mechanismen, wie auch das gesamte Risikomanagement-System regelmäßigen Prüfungen/Audits zu unterziehen.

Wir unterscheiden hierbei folgende Auditarten:

- Interne Prozess-, Verhaltens- und Verfahrensaudits
- Interne Systemaudits
- Externe Systemaudits

Interne Prozess-, Verhaltens- und Verfahrensaudits

Jeder implementierte und mittels eines Testates als eingeführt dokumentierte Sicherheitsmechanismus ist einer regelmäßigen Prüfung zu unterziehen. Als Hilfsmittel zur systematischen Mechanismuskontrolle haben sich folgende Tools erwiesen:

- Auditplan
- Auditprotokoll

Auditplan. Zunächst erfasst der Risikomanager jeden testierten Mechanismus in einem Auditplan. Der Auditplan beinhaltet die nachfolgend aufgeführten Mindestangaben:

- Mechanismus
- Referenznummer
- Auditor (Intern/Extern)
- Kalenderwoche der Prüfung

Verantwortlich für die Erarbeitung des Auditplanes ist der Risikomanager. Der Auditplan ist jährlich zu evaluieren und durch die Geschäftsführung genehmigen zu lassen.

Auditprotokoll. Jedes vorgesehene Audit verfügt durch eine Referenznummer über eine eindeutige Kennung sowie ein bereits vorbereitetes Protokoll. Dieses dient dem Risikomanager als Prüfleitfaden und gibt u.a. über folgendes Aufschluss:

- Auditgegenstand
- Prüfumfang
- Prüfkriterien
- Auditgegenstand
- Auditfragen
- Feststellungen
- Korrekturmaßnahmen/Termine
- Verantwortlichkeiten

Entsprechend den Auditergebnissen wird eine eskalierende Verteilung und Information vorgenommen. Audits mit Beanstandungen führen automatisch zur Re-Auditierung.

Ein entscheidendes Merkmal der vorgenannten Auditprotokolle ist, dass die vorbereiteten Auditfragen ausnahmslos geschlossene Fragen sind. Sie lassen weder von den Auditkriterien noch von den festgestellten Prüfungsergebnissen her Interpretationsspielraum. Somit sind die Audits weitgehend objektiviert und die Ergebnisse nur unter Vorsatz manipulierbar.

Internes Systemaudit

Um das Risikomanagement-System kontinuierlich evaluieren und optimieren zu können, ist im Auftrage der Geschäftsführung jährlich mindestens ein System-Audit durch die interne Revisionsabteilung durchzuführen. Hierbei ist nicht nur das Managementsystem selber, sondern auch die Risiko-Methode als solche einer Prüfung zu unterziehen.

Darüber hinaus haben sich Performanceprüfungen durch die interne Revision als äußerst probates Mittel erwiesen, um die implementierten Mechanismen hinsichtlich ihres tatsächlichen Wirkungsgrades zu überprüfen.

Die vorbeschriebenen Prüfszenarien sind im Übrigen einige der wenigen Kontraindikationen für die revisionsseitige Übernahme des Risikomanagements in Personalunion.

Externes Systemaudit

Lediglich in den Kinderschuhen stecken die Anforderungen Externer an Aufbau, Strukturen, Prozesse und Betrieb von Risikomanagement-Syste-

men. Weder die Prüfleitfäden der Wirtschaftprüfer noch die Fragenkataloge oder Risikostandards externer Prüfinstitutionen verfügen zur Zeit über einen ganzheitlichen Prüfansatz.

Nur rudimentär vorhandene Standardisierungsbemühungen wie der Australisch/Neuseeländische Standard über die Ausgestaltung von Risikomanagement-Systemen (AS/NZS 4360:1999) lassen erste Ansätze qualifizierter Vereinheitlichung erkennen.

Externe Systemaudits sind daher mit Vorsicht zu genießen, da die fehlende Standardisierung zwangsläufig zu Interpretations- und Beurteilungsdifferenzen und somit zu vermeidbaren Diskussionen führt.

Zertifizierungen/Zulassungen

In Ermangelung der notwendigen Grundlagen für eine denkbare Zertifizierung eines Risikomanagement-Systems, gibt es zur Zeit auch keine Zertifizierungen. Die Bemühungen zahlreicher Institutionen, Risikomanagement in vorhandene Zertifizierungsstrukturen wie z.B. DIN ISO 9000 ff zu pressen, ließen sich sicherlich ausführlich kommentieren. Doch solange nicht einmal Einigkeit bei der Durchführung des Risikoprozesses besteht, ist an Systemzertifizierungen wohl eher nicht zu denken.

12.4 Schlussbemerkung

Denken wir nun an unseren Mann vom Anfang zurück, bleibt zu hoffen, dass das Thema »Risiko« ein wenig von seiner reinen Schicksalhaftigkeit verloren hat. Mit ein wenig Systematik und nicht zu übertreibendem Wissenschaftlichkeitsansatz ist es durchaus möglich, jegliche Art von Risiken in einen vernünftigen Gesamtkontext zu bringen. Risiken sind nun einmal integrierter Bestandteil unseres Daseins. Sie zu negieren ist »Vogel-Strauss-Verhalten«, sich wie unser eingangs beschriebener Mann zu verhalten ist nicht ratsam.

13 Sicherheit: Eine metaphorische Betrachtung

Walter Hammerschmid

13.1 Einleitung

Vorweg ein paar Worte zu meiner Person: Ich bin seit 1977 im Bereich IT tätig und habe dabei wohl eine breite Palette von Berufs- und Rechnergruppen gestreift. Angefangen als Software Designer (damals hieß dies noch Programmierer) über Systemmanager, Netzwerkmanager und zuletzt CSO (Chief Security Officer; Sicherheitsmanager hätten wir früher mal gesagt), wobei sich natürlich in jeder dieser Berufsgruppen einige Unterbezeichnungen anführen ließen. Ach ja, »damals« hatten wir noch die Zeit, dass wir versuchen konnten, in die so genannten Tiefen der Materie einzudringen. Es war halt alles ein wenig einfacher; alleine wenn ich daran denke, dass wir damals mit reinen ASCII-Terminals auskommen mussten und Grafik nur von sündhaft teuren Plottern kannten...

Ich will aber keinesfalls den Eindruck erwecken, dass ich einer von denen bin, die nur in der Vergangenheit leben. Ganz im Gegenteil, es ist nur – meiner Meinung nach – manchmal von Vorteil auch die Geschichte oder besser gesagt die Entwicklung zu kennen, auf welche unsere heutigen Errungenschaften basiert. Es könnte sonst leicht vorkommen (rein hypothetisch natürlich), dass wir vergessen, worin die Vorteile oder die Nachteile von diversen Entwicklungen liegen und so vielleicht das Rad öfters neu erfinden. Ich erinnere mich dabei etwa an die IT-»Steinzeit«, wo alles auf dem einen, übermächtigen Zentralrechner lief und dieser eventuell sogar irgendwo in der fremden, weiten Welt stand. Natürlich kamen irgendwann einmal einige schlaue Köpfe auf die Idee, die Rechnerleistungen direkt zum Anwender, also zu uns auf oder unter den Schreibtisch, zu bringen. Und wenn wir uns heute wieder umsehen, so zentralisieren wir in weiten Bereichen wieder so manches. Der Unterschied zu damals ist allerdings, dass es heute Client/Server heißt. Zugegeben, es ist etwas extrem vereinfacht und abstrahiert, aber vom Prinzip sind wir, sozusagen, wieder am Anfang. Selbstverständlich hat jeder dieser Entwicklungsschritte entscheidende Vorteile gegenüber seinen Vorgängern, neue Namen (ja sogar fast eine eigene Sprache), sowie neue Hard- und Software um diese Vorteile einfach und ohne unnötiges Hintergrundwissen anwendbar zu machen.

Aber dies sollte ja eigentlich gar nicht mein Thema sein. Ich will eigentlich ein paar Gedanken zu Papier bringen, welche Vorstellung so mancher (lebende oder bereits verstorbene Personen sind dabei natürlich nicht

gemeint) von der IT-Sicherheit hat und wie diese Vorstellungen in der Praxis umgesetzt werden. Ach ja, vorweg noch etwas in eigener Sache, sozusagen mein persönliches Fangnetz: Alle Gedanken, die ich so von mir gebe, sind rein persönlicher Natur und müssen sich nicht mit der Meinung meines Dienstgebers decken. Zusätzlich sind Ähnlichkeiten mit Personen, Unternehmen oder anderen Dingen rein zufällig und nicht beabsichtigt (wie der genaue Wortlaut bei den diversen Spielfilmen lautet, habe ich leider vergessen; ich meine aber das, was dort ausgesagt wird).

13.2 Mit Sicherheit kein Märchen...

Verlassen wir jetzt gedanklich einfach die heutige Zeit und gehen in eine längst vergangene Zukunft. Es könne sich um eine Zeit handeln, in welcher Zauberer, Feen, Elfen und manch andere magische Geschöpfe genau so selbstverständlich sind wie Ritter mit elektronischen Pferden und Laser-Schwertern. Sie werden sich jetzt sicher fragen, warum ich diese Zeit bevorzuge und nicht einfach gedanklich das Mittelalter aufsuche. Nun die Antwort ist recht einfach: In diversen Geschichten, die ebenfalls in solchen Umgebungen spielen (während meiner Jugend gab es solche Literatur), ist die Gleichberechtigung zwischen den Geschlechtern kein Thema. Das soll heißen, dass alle Rollen auch mit weiblichen Charakteren besetzt sind, was wiederum meiner Gesinnung entspricht. Es zählen die Fähigkeiten der agierenden Personen und weniger ihr Geschlecht. Ich bemerke aber, dass ich schon wieder vom eigentlichen Thema abschweife; also rasch zurück in unsere Gedankenwelt:

Schwere Zeiten sind dies, so manch' Böser versucht auf jede erdenkliche, heimtückische Weise sich an das von rechtmäßigen Herrschern Geschaffene heranzumachen. Ja vereinzelt gibt es sogar Zeitgenossen, die nur so aus purer Erfolgssucht versuchen, die Regeln zu umgehen. Und dabei meine ich nicht bloß das Reiten durch die Dörfer mit weit überhöhter Geschwindigkeit. Nein, hauptsächlich geht es diesen unheimlichen Individuen um immaterielle Werte. Obwohl, zugegeben, sehr oft steckt auch Gold und Silber dahinter.

Auf der anderen Seite sind dies auch sehr gute Zeiten. Die einzelnen Dörfer sind nahezu zur Gänze durch gut ausgestatteten Hochgeschwindigkeitstransportwege verbunden, auf denen jedermann (und natürlich auch jede Frau) sich unbegrenzt und fast ohne Zeitverlust frei bewegen kann. Warum dies so wichtig ist? Nun, hauptsächlich um Gold zu bekommen, wobei eigentlich niemand so recht weiß, von wem es kommt oder wer hier das Gold macht. Aber wie wir ja wissen, gibt es genug magische Gestalten, denen es ja kein Problem bedeutet, jede Menge Gold und Silber zu schaffen und dieses auf den Wegen zu vergraben. Und mit diesem Gold kann man dann noch schnellere Wege bauen und die Dörfer noch größer bauen und, und, und. Ach ja, der Einzelne verwendet diese Wege um Nachrichten zu lesen und zu verschicken. Eine negative Verwendung dieses Verkehrsnetzes

gibt es nicht! Obwohl, manchmal, so munkelt man, kann man auch schon Bilder von Goblins (nicht die Teppiche, sondern die ganz hässliche Kreaturen) zufällig am Weg finden. Da diese aber, wie schon erwähnt, extrem hässlich sind, bemerkt die Bilder ja praktisch niemand.

Um die Guten vor den Bösen zu beschützen, ist es üblich, rund um die Dörfer hohe und massive Mauern zu bauen. Und nicht zu vergessen, es gibt immer einen weisen, alten König, der über alle regiert und dafür sorgt, dass alles mit rechten Dingen zugeht. Zugegeben, gleich einen König für jedes Dorf mag übertrieben klingen, aber diese Könige haben wiederum schöne Töchter, welche wiederum... – aber dies gehört in eine andere Geschichte.

Schauen wir uns einmal drei von diesen Dörfern an, oder besser gesagt ihre Strategien das Böse nicht ins Dorf zu lassen. Es handelt sich dabei um durchschnittliche Dörfer, sozusagen Mittelstandsdörfer. Sie liegen an der gleichen Strasse und haben den gleichen undurchdringlichen Wald in Sichtweite. In diesem Wald, so erzählt man, sollen allerlei dunkle Gestalten (und die sind bekanntlich ja alle böse oder bringen zumindest Unheil) und sogar böse Drachen leben. Richtige Drachen, nicht jene, die man in so manchen Familien findet. Die einzelnen Könige hatten schon vor langer Zeit bekannte Berater eingestellt, die sie bei der Errichtung ihrer Schutzmauer unterstützen. Und wie es damals üblich war, halfen diese Berater auch beim Aufbau der Mauern fleißig mit (habe ich schon erwähnt, dass es sich bei der Geschichte um eine reine Fantasie handelt?). Kurz gesagt, die Dörfer hatten sozusagen eine Standard-Schutzmauer gekauft, angepasst und errichtet. Sie entsprach voll und ganz den individuellen Anforderungen der Dörfer. Doch, wer weiß dies nicht, die Zeiten änderten sich und mit ihnen die Anforderungen auch an die Schutzmauern.

Das erste unserer Dörfer hatte anfangs das meiste Glück. Die Bewohner und natürlich auch der König lebten sehr rasch in großem Wohlstand. Doch wie es in solchen Geschichten üblich ist, wendete sich das Schicksal und es breitete sich große Armut aus. Schuld daran, das wusste der König natürlich sofort, waren neidische Zauberer aus dem Wald, die ihre Flüche nächtens über die alte Dorfmauer schleuderten. Der König, natürlich ein weiser Mann, dachte nach, und fand einen Ausweg aus dem Dilemma: Die Mauer wurde erhöht, alle Nebeneingänge kurzerhand zugemauert und das Haupttor entschieden verkleinert. Kurz gesagt, es wurde alles gemacht, um die Ursache, die bösen Flüche, abzuhalten. Als der Wohlstand dennoch nicht zurückkam, erhöhte man die Mauer weiter und verengte das verbleibende Tor noch mehr. Zugegeben, es war schon eine rechte Plage ins Freie zu gelangen, aber es war dadurch auch fast unmöglich unerkannt hinein zu gelangen. Warum nur fast? Nun, irgendwelche dunkle Gestalten schafften es immer wieder ins Dorf zu gelangen und dort ihr Unwesen zu treiben. Und dabei waren die Wachen, es waren gute und gewissenhafte Wachen, praktisch nie daran Schuld. Das hinderte jedoch niemanden, nicht einmal den König, sie als völlig unzureichend zu deklarieren und sie den ganzen Zorn der Bevölkerung spüren zu lassen. Oftmals kamen die Bösen verkleidet,

oder sie gaben sich als Verwandte von Dorfbewohnern aus. Manchmal ließen sie sich sogar, unter großen Mühen der Leidtragenden, von einfacheren Bewohnern hinter die Mauern tragen.

Das zweite unserer Musterdörfer ging einen anderen Weg. Einen langsameren aber dafür stetig steigenden Weg zum Wohlstand. Immer öfters kamen Bitten von Mitbürgern zum König, dass er die Tore doch verbreitern lassen soll, damit der Durchgang mit breiteren Wagen möglich sei. Und da der König von den Qualitäten seiner Torwache überzeugt war (externe Auditoren bestätigten dies regelmäßig), ließ er, mit der notwendigen Sorgfalt, die Eingänge erweitern. Ja, sogar neue Tore wurden geschaffen. Es gab bald spezielle Tore bei denen man nur hinaus aber nicht herein konnte, Tore für Tiertransporte und solche wo nur Spielleute in das Dorf gelangten. Mit der Zeit wurde der Dorfwall mit unzähligen Ein- und Ausgängen versehen. Betrachtete man die Mauer von weitem, so glich sie eher einem Gitter als einer massiven Befestigung. Erst in der Nähe erkannte man die festen Mauerstücke zwischen den unzähligen Toren. Diese überaus positive Entwicklung blieb natürlich nicht ohne negative Folgen. Nachdem es dem König, oder besser gesagt seinen Wachen, immer mehr Mühe und vor allem Gold kostete, diese Tore zu überwachen, ließ er viele Gelehrte kommen, die ihm aus seiner Misere helfen sollten. Einhellig kamen die Weisen zu dem Schluss, dass alle Tore mit Ausnahme von Wenigen, unbedingt notwendigen, geschlossen werden müssten. Nur welche diese Unnötigen sind, konnten oder wollten sie nicht sagen. Wurde nämlich ein vermeintlich unnötiges Tor geschlossen, so erhob sofort eine Bürgergruppe ihre Stimme, dass dieses Tor für die Ausübung ihrer Tätigkeit unbedingt notwendig sei. Dem König blieb also nur der Weg offen, sein beschränktes Mauer-Budget möglichst gleichmäßig aufzuteilen. Manchmal jedoch stellte der König seinen Untergebenen die Frage, ob die Mauer überhaupt notwendig sei. Doch jedes Mal bekam er innerhalb kürzester Zeit unzählige Berichte der Wachen über die große Anzahl der missglückten, illegalen Eindringungsversuche. Und im zugehörigen König-Summary wurde daraus abgeleitet, dass diese Versuche, ohne die vorhandene Kontrolle, innerhalb kürzester Zeit das Dorf zur Gänze vernichten würden.

Und unser drittes Dorf? Nun der König war ein ganz Schlauer. Der studierte ein paar Fach-Pergamente, analysierte das Wachstum und die Entwicklung seines Dorfes und ließ angepasste, magische Tore bauen. Diese waren genau an die Anforderungen seiner Bewohner angepasst und konnten selbsttätig den Zugang zum Dorf erlauben oder verbieten. Zwar gab es nur einige Tore, doch über diese konnten jedoch praktisch alle Arten von Zu- und Abgängen ermöglicht werden. Und weil er keine Wachen benötigte (es waren ja schließlich magische Tore) konnte der König mehr Gold in die Anpassung der Tore investieren. Dies war schließlich auch notwendig, da auch magische Tore einer gewissen Entwicklung unterliegen und mit der Zeit eventuell vorhandene Schwächen von den Bösen entdeckt und ausgenutzt werden konnten. Natürlich hatte dieser schlaue König auch eine Art von täglichem, magischem Berichtswesen eingeführt, um so die Effizienz der Tore jederzeit

überprüfen zu können. Zusätzlich wurden von ihm zum Gehorsam verpflichtete Diebe angestellt, welche regelmäßig versuchten, an den magischen Toren vorbei zu kommen. Auch diese Berichte las der König mit großer Aufmerksamkeit und richtete danach seine Verbesserungen aus. Kurz gesagt, ein ideales System. Der König war stolz auf seine Entwicklung, präsentierte es jedem anderen König, verkaufte es sogar an andere Dörfer und wurde in unzähligen Fach-Pergamenten lobend erwähnt. Allerdings, mit der Zeit fanden sich auch in seinem Dorf vermehrt dunkle, böse Gestalten. Da es ja keine Wachen mehr gab, hatten sich diese mit der Zeit unter großem Aufwand Durchschlupflöcher gegraben. Durch diese konnten sie ohne Kontrolle ins Dorf und wieder unkontrolliert heraus gelangen.

Zurück in unsere Zeit (eigentlich schade, denn ein paar dieser Ritterinnen waren wirklich...)! Wo liegen nun eventuelle Ähnlichkeiten zu unserer Arbeit vor? Gibt es überhaupt Analogien? Kann es überhaupt Parallelen zwischen unserer hoch entwickelten IT-Welt und etwa dem Mittelalter geben? Vorweg möchte ich nochmals darauf hinweisen, dass es keinerlei Ähnlichkeiten mit lebenden... – aber das hatten wir ja schon.

Nehmen wir einmal beispielhaft an, bei den Dörfern handelt es sich um (fiktive) Unternehmen der heutigen Zeit. Dann wäre der König etwa die Unternehmensführung oder vielleicht auch der verantwortliche Sicherheitsmanager. Die Bewohner, egal ob es sich um »normale« Menschen oder um magische Wesen handelt, wären dann alle Mitarbeiter (zu den magischen Wesen müssten sicherlich alle Arten von Assistentinnen zählen, die meistens als einzige den Durchblick durch das betriebliche Chaos haben). Die Wege zwischen den einzelnen Dörfern könnte das Internet sein und die Dorfbefestigung wäre dann (oh, welch ein Zufall) die firmeneigene Firewall. Zugegeben, die Analogie hinkt ein wenig, denn wo findet man im Internet Bilder von Goblins, aber abgesehen von diesem Fehler könnte man noch einige weitere Analogien ableiten:

Bei dem ersten Dorf könnte es sich vielleicht um ein Unternehmen handeln, bei dem alle betrieblichen Prozesse fest eingespielt sind (und schon immer so gemacht wurden). Bei der allgemeinen »neue Medien«-Euphorie am Beginn dieses Jahrtausends (klingt einfach wunderbar) wurde vielleicht versucht, andere, neuere, eventuell bessere Wege zu beschreiten und hat das Internet gemäß den alten Prozessabläufen eingebunden. So wurde vielleicht jeder Mitarbeiter mit eMail und unbeschränktem Web-Zugang ausgerüstet. Nachdem das Unternehmen auch vom berüchtigten Love-Letter-Virus nicht verschont blieb, wurde diese Errungenschaft, soweit dies noch möglich war, wieder zurück genommen. Dort, wo dies aus strategischen Gründen nicht mehr möglich war, wie etwa beim eMail, wurde die Nutzung jedoch dermaßen eingeschränkt, dass man von einer sinnvollen Nutzung kaum mehr sprechen kann. So konnten etwa alle eintreffenden eMail an einen vom restlichen Netzwerk getrennten Rechner gesendet werden, dort ausgedruckt und anschließend wie ein normaler Brief in den Arbeitsprozess einfließen. – Natürlich ist dies reine Hypothese und wird von keinem Unternehmen praktiziert.

Das zweite Dorf könnte ein typisches, innovatives »New Economy« Unternehmen sein. Mit dem Wissen, dass Mitarbeiter nicht nur äußerst verantwortungsbewusst sind, sondern, wenn sie zufrieden sind auch mehr leisten, wird diesen fast alles ermöglicht (fast, da es immer irgendwo jemanden gibt, der die Rechnungen bezahlen muss). Jeder ist sich der Gefahr, welche im Internet lauern kann, bewusst und agiert auch dementsprechend. Auch hier hat natürlich der Love-Letter-Virus zugeschlagen, aber man wurde durch ihn »gescheiter« und hat versucht, die Mitarbeiter durch entsprechende Schulungs- und Weiterbildungsprogramme über die Risiken und notwendige Gegenmaßnahmen zu informieren. Und natürlich gibt es auch den armen Security Manager, welcher auch seinen Job gut machen möchte (und auch macht), der aber immer mehr Durchgänge durch »seinen« Firewall öffnen muss. Und wer kennt nicht die Reaktionen, wenn ein einmal zugestandenes Privileg zurückgenommen werden muss. Seltsamerweise ist es dabei meistens völlig unerheblich, ob dieses Privileg benötigt wird oder nicht – natürlich rein theoretisch!

Schließlich unser drittes Dorf. Mein Lieblingsdorf, in dem es verantwortungsvolle Spezialisten mit einem uneingeschränkten Technik-Vertrauen gibt. Stets bemüht, möglichst innovativ zu sein und dadurch als Vorzeigeunternehmen gelten zu können. Stets bemüht, möglichst alles zu automatisieren um die Personalkosten so gering wie möglich zu halten und immer über die verschiedensten Informationskanäle über alles informiert. Eine kleine Steigerung könnte es noch geben, wenn nämlich der einmal eingeschlagene Weg nicht mehr verlassen oder gar in Frage gestellt werden darf. Schließlich wurde ja alles gründlich überlegt und betrachtet! – Zum Glück gibt es ja auch solche Unternehmen nur in meiner Fantasie.

Und, was soll das alles? Worin kann die Erkenntnis liegen? Wo könnte etwas geändert werden? Oder ist das lediglich wieder so eine Nörgelei eines Wieners (habe ich schon erwähnt, dass ich in Wien lebe?), der mit sich und der gesamten Welt unzufrieden ist? Nun, das Letztere kann ich nicht ganz ausschließen und die »eierlegende Wollmilchsau« habe ich auch nicht gezüchtet. Ich habe da bloß »so eine Idee«, die vielleicht allen Dörflern helfen könnte. Allerdings ist es natürlich ein steiniger und mühsamer Weg von der Idee zur Realität. Aber wie heißt es doch so schön? »Einer für Alle, Alle für Einen«.

Die Sicherheitsüberlegungen von vielen Unternehmen sehen dermaßen aus, dass möglichst viel gemacht wird, um das illegale Eindringen zu unterbinden. Wir bauen also hohe und massive Wände um uns herum; typisches mittelalterliches Gedankengut. Auf der anderen Seite benötigen wir, oder eigentlich unsere Kollegen und Kolleginnen (die Reihenfolge ist hier bewusst gewählt), immer mehr und immer einfachere Wege ins Internet und leider damit verbunden auch den Weg vom Internet bis zum Arbeitsplatz. Immer mehr sinnvolle Features werden bei der täglichen Arbeit benötigt. Ja selbst für Chat (etwa über ICQ) oder den Austausch von Programmen kann es sinnvolle Gründe und Notwendigkeiten geben. Dies würde im Extremfall allerdings für die Behandlung wie im zweiten Musterdorf führen und das

war ja auch nicht so ideal. Also doch restriktiv bleiben? Ja und Nein! Wie agieren wir eigentlich tagtäglich? Nehmen wir einmal ein Unternehmen mit einigen hundert Mitarbeitern, an einem zentralen Ort. Das Firmengelände oder Gebäude hat wenige, durch Personal geschützte Eingänge. Während der normalen Arbeitszeit können die Mitarbeiter praktisch ungehindert das Unternehmen verlassen und wieder betreten. Eventuell muss beim Vorbeigehen ein Firmenausweis hergezeigt werden. Die eigentliche Sicherheit liegt jedoch darin, dass der Portier (Pförtner) stichprobenartig genaue Kontrollen durchführt und, was fast noch wichtiger ist, dass jeder schon von weitem erkennen kann, dass der Unternehmensbereich geschützt ist. Kommt dennoch eine unternehmensfremde Person unerlaubt in die inneren Bereiche, so können, auf einfache Weise, von jedem Mitarbeiter entsprechende Sicherheitsmaßnahmen gestartet werden. Dies kann das Begleiten der jeweiligen Person zu dem gewünschten Ziel sein, aber auch die Verständigung einer internen Sicherheitstruppe welche sich um den »Eindringling« kümmert. Außerhalb der normalen Arbeitszeit wird mit erhöhtem Sicherheitslevel gearbeitet, d.h. jeder muss sich beim Verlassen und beim Betreten des Unternehmen identifizieren. Das Wachpersonal macht zusätzlich Rundgänge und kontrolliert jede angetroffene Person.

Wie könnte ein solcher Prozess, der sich offensichtlich im »richtigen« Leben als handhabbar herausgestellt hat, im IT-Bereich umgesetzt werden? Zum Einen, und das wäre ja der einfachste Teil, dürften zu bestimmten Zeiten alle Mitarbeiter von Innen nach Außen Verbindungen aufnehmen. Die Verantwortung obliegt dabei jedem Mitarbeiter, welche Art von Zugriffen er außerhalb des Unternehmens tätigt und wohin er sich bewegt. Lediglich das Wissen, dass diese Bewegungen mitprotokolliert werden, sollte den Mitarbeitern zu einem gewissen Maß an Eigendisziplin »helfen«. Werden während dieser Zugriffe (oder eigentlich »Ausgriffe«) Services auf fremden Rechnern angestoßen, welche ihrerseits Rückverbindungen aufbauen, so ist dies im Regelfall erlaubt. Statistisch sollte beim »auslösenden« Mitarbeiter (automatisch) rückgefragt werden, ob diese Verbindung gewollt ist und daher aufgebaut werden soll. Die Anzahl der Rückfragen könnte dabei abhängig von der Vertrauenswürdigkeit und von der Anzahl der bereits bestätigten Zugriffe des Ausgangssystems sein. Während dieser Zeit könnte, sofern dies notwendig ist, der externen Zugriff auf eingeschränkte, interne Systeme durch eine einmalige, einfache Username/Passwortabfrage ebenfalls ermöglicht werden. Eine derartige Notwendigkeit könnte bei Zugriff von Außendienstmitarbeitern über WebCafe sein. Auch hier könnten, je nach Vertrauenswürdigkeit der Quelle und des Zielsystems, ebenfalls statistisch verteilte genauere Erkennungsverfahren zur Anwendung kommen. Alle diese Vereinfachungen müssten die Mitarbeiter jedoch mit einer erhöhten Aufmerksamkeit für »ungewöhnliche« Ereignisse erkaufen. Was als ungewöhnliches Ereignis gelten könnte, obliegt sicher in einem großem Ausmaß dem »gesunden« (IT)-Hausverstand des Mitarbeiters. So könnte etwa ein unmotivierter Zugriff auf die lokale Festplatte ein solches ungewöhnliches Ereignis sein; allerdings könnte aber auch ein regelmäßig laufender automatischer Viren-Scan eine mögliche Ursache dafür sein. Auf jeden

Fall sollte man Vorkehrungen schaffen, damit auch der IT-Laie solche Ereignisse »analysieren« und gegebenenfalls automatisch melden kann. Wurde das Ereignis als »normal« erkannt, so sollte darüber der Benutzer informiert werden, da sich dieser dadurch auch über die Wichtigkeit seiner Wahrnehmung bewusst wird. Sollte es sich tatsächlich um einen Zugriff von Außen handeln, so müssten (automatisch) entsprechende Ausforschungs- und Gegenmaßnahmen angestoßen werden. Ebenfalls automatisch sollten »Wächter« unregelmäßig die vorhandenen Prozesse und Ressourcen überprüfen und bei eventuellen gravierenden Abweichungen ebenfalls Alarm schlagen. Eine solche Abweichung könnte etwa ein Prozess eines nicht »registrierten« Programms sein (z.B. Login auf WebServer). Außerhalb der normalen Arbeitszeit wären Zugriffe nach Innen nur mehr sehr beschränkt möglich, d.h. etwa automatisch aufgebaute Rückverbindungen von beliebigen Quellen wären nicht mehr möglich. Zusätzlich würden die »Wächter« intensiver nach außergewöhnlichen Ereignissen suchen. Wenn etwa auf einen Server 100 Prozesse einer bestimmten Art aktiv sind, kann bei einer Abweichung von schon einem einzigen Prozess ein Alarm ausgelöst werden, wobei natürlich vor dem eigentlichen Auslösen die Ursache (es könnte ja ein rechtmäßiger Vorgang sein) verifiziert werden müsste. Es zeigt sich dabei, dass Qualität (Verfügbarkeit) und Sicherheit Hand in Hand arbeiten. Parallel dazu sollte natürlich die Tatsache der praktisch ständigen Kontrolle, gezielten Ausforschung und rechtlichen Ahndung bei Übertretung der legalen Zugriffsmechanismen, publiziert werden.

Man sieht hier, dass eine praktisch ständige Überwachung notwendig sein wird. Auf der anderen Seite gilt natürlich, dass, je schneller Erkennungs- und Gegenmaßnahmen aktiv werden können, desto weniger komplexe Schutzmechanismen benötigt werden. Dies lässt sich auch als Analogie im täglichen, nicht IT-Leben finden: Kaum jemand glaubt wirklich daran, dass unsere Banken einbruchssicher sind, also auch bei genügend vorhandenen Ressourcen wie Zeit und Geld, es nicht möglich ist mehr oder weniger gewaltsam einzudringen. Es wird »lediglich« der illegale Zugriff, also der Einbruch, solange verzögert, bis geeignete Gegenmaßnahmen aktiv sind und der oder die Täter ausfindig und dingfest gemacht werden können. Im täglichen Leben kennen wir für diese Art von Schutz unzählige Sicherheitseinrichtungen, angefangen von Glasbruch-Detektoren über Trittsensoren, Raumüberwachung mittels Laser, Wärmesensoren oder Bewegungsmelder. Alleine innerhalb unserer IT-Landschaft gibt es noch kaum geeignete Sensoren. Dabei hat es ja schon vor Jahren einen sehr guten »Lehrfilm« über die Möglichkeiten der Erkennung und Abwehr von Eindringlingen innerhalb des IT-Umfeldes gegeben (»Tron« von Walt Disney). Gut, zugegeben, dieser Vergleich hinkt ein wenig, da ja dort der Eindringling eigentlich von der guten Seite war. Aber was sagt das Sprichwort: Nicht alles was hinkt ist ein Vergleich; aber es ist zumindest ein Indiz.

Wenn mir jetzt nochmals die Bilder des am Anfang beschriebenen, zukünftigen Mittelalter vor Augen kommen und ich mir etwas von den dort vorhandenen Feen wünschen könnte, dann würde ich gerne in unserer IT-

Landschaft mehr Leben entdecken. Wir haben uns daran gewöhnt, dass es normal ist, dass der PC piepst, quakt oder sonstig unangebrachte Laute kombiniert mit unverständlichen Meldungen von sich gibt, sobald wir uns nicht, in seinem Sinne, richtig verhalten. Kaum jemand kommt heute mehr auf die Idee, dass eigentlich alles einmal nur als Hilfsmittel gedacht war. Ja wir waren sogar einmal der Meinung, dass die Roboter, und dazu kann man mit gutem Gewissen durchaus auch unsere PC zählen, sich an uns und unsere Eigenheiten anpassen würden und nicht wir uns an diese elektronischen Zauberschachteln. Wir sollten auch bei all den Möglichkeiten, welche uns diese Schachteln bieten nicht vergessen, dass es außerhalb des Siliziums auch noch ein Leben gibt, ein gutes, eines mit einigen Millionen Jahre alten Erfahrungen, mit etablierten Prozessen und Verhaltensmustern. Manchmal kann es recht nützlich sein (zumindest für mich ist es), wenn man seine (IT) Gedanken, Probleme und Lösungen etwas abstrahiert und anschließend alles wie im normalen Leben betrachtet. Und wenn man viel Glück hat, bemerkt man dann, dass die Probleme gar nicht vorhanden sind.

Ach ja, was ich wohl vorhin vergessen habe zu erwähnen: In allen Dörfern gab es Wesen von der Guten und der weniger guten Seite. Und bei Beiden gab es welche, die von Außerhalb, auch vom undurchdringlichen Wald kamen. Manchmal aber, so erzählt man sich, waren es aber auch die eigenen Leute, die dazu beitrugen, dass nicht alles glatt und in Wohlwollen ablief. In diesem Sinne wünsche ich uns allen noch viele Drachen, die wir gemeinsam besiegen können.

14 E-Signatur

Oliver Berndt

Thomas Krampert

14.1 Einleitung

14.1.1 Geschäftsverkehr in Zeiten des Internet

Obwohl der Geschäftsverkehr – speziell zwischen Unternehmen – zunehmend elektronisch erfolgt und es kaum noch einen Büroarbeitsplatz ohne PC gibt, spielt das Papier immer noch eine wesentliche Rolle in der Geschäftswelt.

Die Notwendigkeit für rechtsverbindliche Unterschriften ist eine wichtige Ursache. In einer Zeit zurückgehender Zahlungsmoral, zunehmendem Outsourcing und steigender »Freude« an Rechtsstreitigkeiten kann auf die Beweiskraft einer Unterschrift nicht verzichtet werden.

Speziell bei Käufen im Internet besteht ein dringender Bedarf für eine solche Regelung. Einerseits kennen sich Käufer und Verkäufer nicht, andererseits ist eine Initiierung eines Kaufs im Internet, der dann über einen intensiven Papieraustausch abgewickelt wird, weder sinnvoll noch von den Abnehmern akzeptiert. Internet-Händlern bleibt daher nur die Lösung einer Inkaufnahme des erhöhten Risikos oder den Kunden von einer Registrierung zu überzeugen und dann evtl. einem (Online-)Scoring *[1]* zu unterwerfen.

Im Internet-Handel gilt dies nicht nur für die rechtliche Gültigkeit und Nachvollziehbarkeit der Transaktion, sondern auch für die Sicherheit des Zahlungseingangs. Teilweise haben sich Verfahren etabliert, bei denen der Kunde die erste Lieferung nur auf Nachnahme erhält. Wird diese Lieferung korrekt bezahlt, so ist beim nächsten Mal die Bestellung gegen Rechnung möglich. Dass dieses Verfahren auch nicht optimal ist, zeigt die bereits seit Jahren geführte Diskussion um unterschiedliche Internet-Zahlungsverfahren ohne das sich ein Verfahren hätte durchsetzen können. Andererseits weiß jeder Internet-Händler über mangelnde Zahlungsmoral, Scheinbestellungen etc. zu berichten.

Eine Online-Bestellung, die anschließend einen regen Papieraustausch in Form von zu unterschreibender Papierbestellung, Auftragsbestätigung, Lieferschein und Rechnung erfordert, führt nicht nur zu erhöhten Abwicklungszeiten, sondern verursacht auf beiden Seiten auch erheblichen Aufwand für Erstellung und Versand sowie Verwaltung dieser Papiere.

Da Papier für die elektronische Abwicklung, speziell in Zeiten des Internet, eine große Behinderung bei der Optimierung der Abläufe darstellt, gibt es schon seit geraumer Zeit Bestrebungen konventionelle Unterschriften durch eine elektronische Alternative zu ersetzen.

Wichtig ist daher, dass die elektronische Signatur *[2]* (E-Signatur) mittlerweile auch rechtlich der traditionellen Unterschrift gleichgesetzt ist. Damit sind elektronisch unterschriebene Dokumente (oder E-Mails) verbindlich.

14.1.2 Bedeutung der Unterschrift

Um die notwendige Komplexität der E-Signatur nachvollziehen zu können, ist es hilfreich, zunächst zu beleuchten, welchen Zweck Unterschriften erfüllen.

Unterschriften dienen

- der **Willensbekundung** des Unterschreibenden (z.B. eine Bestellung oder eine Vereinbarung zu tätigen),
- der **Identifikation** des Unterschreibenden,
- dem Nachweis der **Echtheit** (d.h. die Willensbekundung wurde nicht manipuliert),
- der **Nachvollziehbarkeit** der Willensbekundung.

Anders formuliert kann über die Unterschrift nachvollzogen werden, wer was wann gewollt hat. Damit dies auch elektronisch möglich ist, ist ein Verfahren erforderlich, welches die gleichen Anforderungen erfüllt. Das Kopieren einer eingescannten Unterschrift in ein elektronisches Dokument ist dazu nicht geeignet, denn dies ist auch für einen Fremden sehr leicht möglich und damit manipulierbar.

14.1.3 Bedeutung der elektronischen Signatur

Die E-Signatur gleicht eher einer Prüfsumme *[3]* aller Buchstaben eines Textes (Bestellung, Vertrag o.ä.), die über einen personenbezogenen Code verschlüsselt werden. Damit erhält man eine einmalige E-Signatur, die sowohl vom Text als auch von der erstellenden Person abhängig ist. Diese E-Signatur wird elektronisch mit dem Text verknüpft und versiegelt ihn damit. In mehrerer Hinsicht entspricht die E-Signatur somit eher dem Siegel des Mittelalters als der Unterschrift wie wir sie heute kennen. Wichtig ist jedoch einzig und allein, dass

- die Willensbekundung des Unterschreibenden über den Text geäußert wird,
- die Identifikation des Unterschreibenden für den Empfänger aus der Signatur entnehmbar und auch überprüfbar ist,

- der Nachweis der Echtheit durch das zugrundeliegende mathematische Verfahren garantiert wird und
- der ganze Vorgang nachvollziehbar ist.

Da gleichzeitig die rechtliche Anerkennung gegeben ist, können auf dieser Basis Geschäfte sowohl mit anderen Firmen als auch mit Privatpersonen abgewickelt werden. Bei einer Auseinandersetzung mit den Details stellt sich sogar die Frage, ob die E-Signatur nicht deutlich sicherer als eine traditionelle Unterschrift ist.

14.2 Vorteile der elektronischen Signatur

Da eine elektronische Signatur nicht papiergebunden erfolgt, sondern durch softwaregesteuerte Verfahren, die auf Verschlüsselung, Geheimcodes und/oder biometrischen Merkmalen basieren, umgesetzt wird, ist die papierfreie Geschäftsabwicklung realisierbar. Dies gilt vor allem dort, wo es sich um den Austausch von immateriellen Gütern handelt wie den Kauf von Software, Daten, Informationen, Rechten etc. Lediglich wenn Güter physisch zu transportieren sind, wird es noch Lieferscheine geben, obwohl auch diese durch eine mobile Datenerfassung ersetzt werden können. Selbst wenn es noch Lieferscheine gibt, so haben diese – wie auch heute – nur bei Problemfällen eine Bedeutung. Der generelle Ablauf der Transaktion wird durch diese Papiere nicht beeinflusst oder behindert. Die rechtssichere Vereinbarung mit unbekannten Kunden kann papierlos nur über E-Signatur erfolgen.

Die Vorteile sind:

- es ist keine manuelle Posteingangsbearbeitung notwendig,
- es sind keine Papierablagen und -archive mit ihren Handlings- und Platzproblemen notwendig,
- die Reduktion »Geistiger Rüstzeiten« (soll heißen erneutes Hineindenken in die Sachlage) aufgrund Papierhandling oder aufwändiger Nachfrageaktionen,
- es ist kein aufwändiger Papiertransport, z.B. für Unterschriftseinholung notwendig.

Insgesamt ergeben sich dadurch erheblich schnellere Durchlauf- und auch Reaktionszeiten, was sowohl der unternehmensinternen Effizienz als auch dem besseren und schnelleren Kundenservice dient. In vielen Fällen kann durch die Zeitersparnis auch die Zeit für Vorfinanzierungen reduziert werden, was unmittelbar zu monetären Erlösen führt.

Bei entsprechender Gestaltung lassen sich die Antrags- und Beschaffungstransaktionen innerhalb des Unternehmens oder mit externen Partnern komplett automatisieren, ohne dass manueller Aufwand innerhalb des ein-

zelnen Vorgangs entsteht. Lediglich periodische Kontrollen der Ergebnisse, z.B. Auftragsentwicklung, Zahlungseingang etc. und die Behandlung von Problemfällen erfordern manuelle Tätigkeiten.

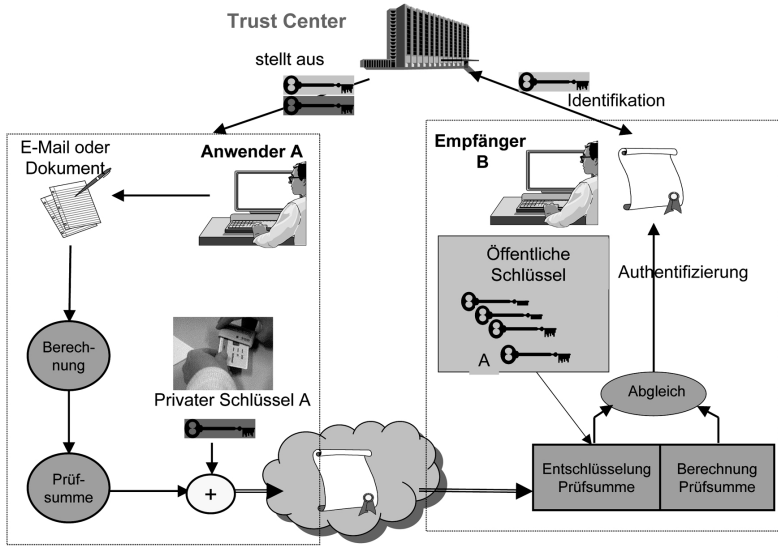
Damit fallen eine Reihe von Arbeitsschritten weg, was zu direkten Einsparungen führt. Natürlich ergeben sich weitere Einsparungen durch verringerte Ablageflächen, günstigere Archivierung und geringere Aufwändungen für Büromaterial. Entscheidend sind jedoch die Effizienzsteigerungen im Prozess.

Die Erschließung dieser Potenziale hat jedoch – wie immer – ihren Preis. Dabei ist weniger an die notwendigen Hard- und Software-Investitionen gedacht, die sich in Anbetracht der Einsparungsmöglichkeiten meist rechtfertigen lassen ***[4]***. Nicht zu unterschätzen ist jedoch der Aufwand für die organisatorische Gestaltung und die Anpassungen der bestehenden Applikationen.

14.3 Ablauf des Signierens

Über Details des Funktionsprinzips der elektronischen Signatur liegen unzähligen Abhandlungen vor ***[5]***. Hier wird daher lediglich der Ablauf aus Nutzersicht beschrieben.

Abbildung 14.1: Prinzip der elektronischen Signatur



Nachdem ein Brief oder eine E-Mail fertiggestellt wurde, nicht mehr verändert und unterschrieben werden soll, ist der Befehl zur Unterschrift anzuklicken. Der Benutzer wird daraufhin aufgefordert den Unterschriftsschlüssel, das ist der so genannte private Schlüssel (private key) einzugeben.

Dieses »Zertifikat« kann prinzipiell an einem beliebigen Ort gespeichert sein. Aus Sicherheitsgründen ist üblicherweise an eine Signaturchipkarte gedacht, die in ein entsprechendes Lesegerät eingeschoben wird. Um die Zugehörigkeit der Person zur Chipkarte sicherzustellen, ist im Allgemeinen noch eine sechsstellige PIN (Personal Identification Number) – analog zum Geldautomat – einzugeben. Alternativ können an dieser Stelle auch biometrische Merkmale, wie z.B. der Fingerabdruck überprüft werden.

Nun erfolgt intern die Berechnung einer einmaligen Prüfsumme des Textes, der sogenannte »Hashwert« sowie die Verschlüsselung dieser Prüfsumme mit dem Unterschriftschlüssel ohne weiteres Zutun des Benutzers.

Das Resultat wird als elektronische Signatur mit dem Text elektronisch verbunden und zum Empfänger übertragen. Der Text selbst kann, muss aber nicht verschlüsselt übertragen werden.

Auf der Empfangsseite erfolgt die Verifikation der E-Signatur automatisch. Dass heißt der Text wird angezeigt, auf Modifikation hin überprüft und es wird der Absender überprüft, indem die Entschlüsselung mit dem passenden (öffentlichen) Schlüssel erfolgt. Dazu muss dem Rechner lediglich der Fundort des öffentlichen Schlüssels bekannt sein.

Um sicherzustellen, dass der Absender auch wirklich der ist, der er vorgibt zu sein, kann eine automatische Anfrage bei dem ausstellenden Trust Center (Zertifizierungsinstanz) erfolgen. Das Trust Center kann eine öffentlich akkreditierte Institution sein. Im Falle eines Unternehmens lässt sich diese Funktionalität aber auch auf einem Intranet-Server implementieren. Sämtliche Überprüfungen laufen automatisch im Empfangsrechner ab. Der Benutzer wird lediglich über das Ergebnis informiert.

14.4 Anwendungsbereiche

Bei den Anwendungen muss generell differenziert werden zwischen

1. dem Aufbau von **Infrastrukturen zur Verschlüsselung** (Public Key Infrastructure, PKI),
2. dem Einsatz von elektronische **Signaturen zwischen IT-Systemen** und
3. dem Einsatz von **personenbezogenen Signaturen**, die auch die Person eindeutig identifizieren sollen (z.B. in Form von Chipkarten) ***[6]***.

Eine PKI ist im allgemeinen Vorraussetzung, um E-Signatur einzusetzen. Zur Anwendung der E-Signatur sind weitere Maßnahmen zu ergreifen, wie z.B. Erstellung, Zuordnung, Verteilung, Verwaltung und Prüfung der Signaturschlüssel. Die erste Stufe und teilweise auch die zweite Stufe wird in Pilotimplementierungen und im Produktiveinsatz, z.B. in Intranet- oder in B2B (Business to Business) -Anwendungen heute schon in vielen Unternehmen praktiziert.

Erst die dritte Stufe ermöglicht die eindeutige Personenbindung. In der zweiten Stufe sind es lediglich Maschinen (gewöhnlich PCs), die identifiziert werden. Die Verbindung zur Person über Login und Passwort ist zwar möglich, unterliegt aber den Sicherheitsmängeln dieser Systeme. Organisatorisch ist die dritte Stufe jedoch deutlich aufwändiger, weil jede Person mit einem Speichermedium und einem entsprechenden Lesegerät ausgestattet werden muss *[7]*.

Erstellung, Zuordnung, Verteilung, Verwaltung und Prüfung personenbezogener Schlüssel ist somit deutlich komplexer. Neben dieser »Roll-out«-Problematik (und den resultierenden Investitionen) sind organisatorische Vorkehrungen für Verlust, Diebstahl, Ausscheiden, Ablauf etc. zu treffen. Das heißt, es sind entsprechende Abläufe zu implementieren und aufbauorganisatorisch zu integrieren.

14.4.1 Freie Wirtschaft

Während die Wirtschaft durchaus begonnen hat, zunehmend PKI aufzubauen, finden sich heute kaum produktive Anwendungen, die bereits die dritte Stufe umsetzen. Es fehlt die »Killer-Applikation«, die den Aufwand rechtfertigt.

Ein technischer Lösungsansatz um PKI-Investitionen zu reduzieren, besteht im Outsourcing und in webbasierten Lösungen. Da es sich jedoch um hochsensible Informationen handelt, müssen sich diese Varianten noch im Markt beweisen.

Gesundheitswesen

Personenbezogene elektronische Signaturen, wie sie im Signaturgesetz (SigG) vorgesehen sind, eignen sich somit primär für Einsatzbereiche, in denen maximale Sicherheit benötigt wird. Es gibt daher einige Ansätze und Pilotinstallationen im Gesundheitswesen. Dazu gehören einerseits unspektakuläre Applikationen wie z.B. die Online-Bestellung von Medikamenten durch Apotheken, aber auch wirklich sensible Anwendungen wie das elektronische Rezept und die Abrechnung von Leistungen zwischen Krankenkassen und Leistungserbringern. Gerade die letztgenannten Applikationen befinden sich jedoch maximal in einer Pilotphase.

Finanzdienstleister

Ähnlich gestaltet sich die Situation im Bankenumfeld. Obwohl es sehr nahe liegt auf den ohnehin vorhandenen (allerdings meist unintelligenten) Karten eine E-Signatur aufzubringen, sind bisher lediglich bei der HypoVereinsbank und der Commerzbank ernsthafte Angebote zu verzeichnen. Bereits seit langem wird zwar in Bankenkreisen über den flächendeckenden Einsatz von Chipkarten diskutiert, eine definitive Entscheidung war aber bisher nicht zu erreichen. Der Misserfolg der Geldkarte hat die Skeptiker bestärkt, ohne sich allzu intensiv mit Ursachen und deren Vermeidung zu beschäftigen.

Da für Banken der Nutzen durch weitere Automatisierung jedoch offensichtlich und auch quantifizierbar ist, übernehmen sie weiterhin eine Schlüsselfunktion bei der Erschließung des Massenmarktes. Soweit es sich um B2B-Applikationen ohne die direkte Personenbindung (Stufe 1 und 2) handelt, existieren bereits eine Reihe von Lösungen und Lösungsansätzen.

Die Unternehmensberatung A.T. Kearney hat weiterhin Bedarf in der Zusammenarbeit von Versicherungen und Rückversicherungen festgestellt, da hier ebenfalls sehr sensible Informationen ausgetauscht werden.

E-Billing

Eine Anwendung, die zumindest im B2B-Geschäft das Potenzial zur »Killer-Applikation« hat, ist E-Billing, also der rein elektronische Austausch von Rechnungen. Mit den zum 01.01.2002 in Kraft getretenen Änderungen des Umsatzsteuergesetzes (UstG §4, Abs. 4) sind elektronische Rechnungen dann rechtsgültig, wenn sie eine personenbezogene elektronische Signatur tragen. Nur in diesem Fall ist der Vorsteuerabzug erlaubt, auf den kein Unternehmen verzichten kann.

Das Problem liegt nun daran, dass Rechnungserstellung und -versand hauptsächlich dann einen nennenswerten Kostenblock darstellt, wenn es massenweise erfolgt. Genau dann ergeben sich große Einsparpotenziale, aber genau dann ist die manuelle Signierung jeder einzelnen Rechnung nicht tragbar. Die Firma Authentidate hat dafür eine Lösung entwickelt, bei der die Rechnungen am zentralen E-Mail-Server mit der personenbezogenen elektronischen Signatur des Verantwortlichen, z.B. dem Leiter der Debitorenbuchhaltung, versehen wird.

Obwohl das Rechnungshandling in den Unternehmen verschieden ist, so entstehen im konventionellen Verfahren für Ausdruck, Kuvertierung, Versand und Archivierung Kosten, die in der Größenordnung von 2,50 € pro Rechnung geschätzt werden. Noch höhere Aufwändungen sind im allgemeinen auf der Empfängerseite zu sehen, weil dort sehr komplexe Rechnungsprüfungsprozesse ablaufen können *[8]*. Bei angenommen 1000 Rechnungen pro Monat á 2,50 € entstehen bereits Kosten von 2.500 € und bei 10.000 Rechnungen entsprechend 25.000 € pro Monat. Durch das oben geschilderte Verfahren lassen sich diese Kosten für den Versand drastisch und für den Rechnungsempfang immer noch nennenswert reduzieren.

Exakte Zahlen können nur im Einzelfall ermittelt werden, aber ein intensiver Blick auf das gesamte Rechnungshandling im eigenen Unternehmen macht das enorme Potenzial schnell transparent.

14.4.2 Öffentliche Verwaltung

Bei der Etablierung der elektronischen Signatur wird es nicht zuletzt auf die Verwaltungen ankommen, die hier eine Vorbildfunktion zu erfüllen haben. Die prinzipielle Pflicht zur Gleichstellung von eigenhändiger Unterschrift und der qualifizierten elektronischen Signatur besteht auch im Verwaltungs-

recht. Berührt wird damit sowohl die Schnittstelle zwischen Verwaltung und Bürger (G2C = Government to Citizen) als auch die Kommunikation zwischen verschiedenen Behörden (G2G = Government to Government). Die Verwaltung kann aber entscheiden, wo sie die Verwendung ermöglicht. Umfassende Anpassungen des Verwaltungsrechts auf Bundes- und insbesondere Länderebene sind erforderlich und in Arbeit *[9]*.

Die öffentliche Verwaltung (ÖV) ist sich ihrer Vorreiterrolle bewusst. Über diverse Projekte wurden Erfahrungen gesammelt und noch vorhandene technologische Schwächen aufgedeckt. Zu diesen Projekten gehörten u.a.:

- MEDIA@Komm

  Nutzung des Internets für kommunale Verwaltung und Interaktionen mit Bürgern

- DOMEA

  Verwaltungsinterne Vorgangsunterstützung über Dokumenten-Management und Workflow

- SPHINX

  Verbesserung der E-Mail-Sicherheit

- Haushaltswirtschaft Niedersachsen

  12.000 Nutzer qualifizierter Signaturen bilden das bisher größte Projekt in Deutschland bzgl. E-Signatur

Im Rahmen der vom Bundesinnenministerium gestarteten Initiative BundOnline2005 sollen bis 2005 ca. 350 Vorgänge durch E-Government unterstützt werden. Das Budget beträgt 1,65 Mrd. €. Die E-Signatur spielt dabei eine wesentliche Rolle. Dies wird auch dadurch unterstrichen, dass die Bundesregierung am 16.01.02 einen Beschluss zur »Sicherheit im elektronischen Rechts- und Geschäftsverkehr in der Bundesverwaltung« gefasst hat.

Darin wird verlangt, dass der Austausch von E-Mails und Dokumenten zwischen Bundesbehörden und von Bundesbehörden zu Unternehmen über E-Signatur gesichert wird. Die entsprechenden Kosten sind in dem Budget für BundOnline2005 bereits berücksichtigt. Weitere Ideen, wie z.B. die E-Signatur auf dem Personalausweis, wurden und werden diskutiert, sind aber derzeit politisch nicht durchsetzbar.

Natürlich gibt es weitere Ideen zu Vorleistungen, welche die Verwaltung erbringen könnte. Es sollte jedoch anerkannt werden, dass im Fall der E-Signatur erhebliche Anstrengungen unternommen wurden und der Staat mehr als nur die Randbedingungen geschaffen hat.

14.4.3 Initiativen

Erfreulicherweise agieren Wirtschaft und Verwaltung nicht völlig unkoordiniert, sondern versuchen bereits seit längerem gemeinsame Initiative zu zeigen. Neuester Ansatz ist das auf den Signaturtagen 2002 durch das Bundesministerium des Innern (BMI) und Bundesministerium für Wirtschaft und Technologie (BMWI) angebotene Bündnis für elektronische Signaturen. Zugrunde liegt die Idee gemeinsamer Signaturkartenangebote zwischen Wirtschaft und Verwaltung. Der Dialog schließt gleichzeitig technische und rechtliche Fragen sowie ein konzentriertes Vorgehen bei der Standardisierung mit ein.

Gerade bei Technik und nationaler wie internationaler Standardisierung besteht Handlungsbedarf, denn einfach handhabbare, kompatible und stabile Produkte sind unabdingbare Voraussetzung für einen Erfolg der E-Signatur.

In diesem Zusammenhang haben sich bisher lediglich Herstellerinitiativen hervorgetan. Besonders hervorzuheben ist dabei die Initiative »Teletrust« (*www.teletrust.de)*, die über den ISIS-MTT-Standard (Industrial Signature Interoperability Specification – Mailtrust) die Kommunikation zwischen den zwei primären Signaturverfahren vereinheitlicht hat. Weiterhin gibt es einige Herstellervereinigungen aus dem Umfeld der Mobilelektronikanbieter, weil sich diese Geräte naturgemäß sehr gut als persönliche »Signaturerstellungseinheiten« eignen.

Mit »Identrus« existiert im Finanzsektor bereits seit 1997 eine Vereinigung, die sich bezüglich verwendeter Technologien und Standards austauschen, Kompatibilität herstellen und gegenseitig ihre Zertifikate anerkennen. Der Fokus von »Identrus« liegt eindeutig auf B2B-Aktivitäten via Internet. In »Identrus« sind weltweit über 60 Banken vertreten. Die deutschen Großbanken sind alle dabei!

14.5 Rechtliche Anerkennung

14.5.1 Historie E-Signatur

Bereits 1997 hat die Bundesregierung das Signaturgesetz als Teil des gemeinhin als Multimediagesetz bekannten Informations- und Kommunikationsdienste-Gesetz (IuKDG) verabschiedet. Damit wurde europaweit erstmalig eine gesetzliche Regelung für die elektronische Unterschrift geschaffen. In der IT-Industrie keimte mit der Verabschiedung des Gesetzes 1997 die Hoffnung auf, dass das papierlose Büro doch noch Wirklichkeit werde und die IT-Sicherheit in Unternehmen durch das Setzen verbindlicher Standards beflügelt wird. Zudem wurde ein großer Markt für Trust Center vorhergesagt.

Die großen Erwartungen, die an dieses Gesetz geknüpft waren, konnte es jedoch nicht erfüllen. Das Signaturgesetz hatte nämlich gleich mehrere Geburtsfehler:

1. Ein extrem hoher technischer und organisatorischer Sicherheitsstandard war Voraussetzung, um als Trust Center zugelassen zu werden. Siebenstellige Beträge waren zu investieren.
2. Der Alleingang des deutschen Gesetzgebers verschaffte Deutschland zwar international eine Vorreiterrolle auf diesem Gebiet, doch ohne zumindest europaweite komplementäre Regelungen hatte das Signaturgesetz von vornherein nur den Charakter einer nationalen Besonderheit, die im Geschäftsverkehr mit dem Ausland keinerlei Geltung für sich beanspruchen konnte.
3. Digital signierte Dokumente hatten nicht den Beweiswert einer Urkunde und besaßen dort, wo der Gesetzgeber die Schriftform fordert, keine rechtliche Verbindlichkeit.

Gerade das Fehlen jeglicher rechtlicher Konsequenzen, die mit der Signaturgesetzgebung hätten verknüpft werden können ***[10]***, rechtfertigt die Frage, wozu von allen beteiligten Stellen und insbesondere den Endanwendern Aufwand in das Angebot und den Einsatz digitaler Signatur betrieben werden sollte.

14.5.2 EU-Richtlinie und deutsche Umsetzung

Der nationale Alleingang Deutschlands, der sich nicht zuletzt auch im europäischen Ausland den Vorwurf der Überregulierung gefallen lassen musste, brachte einen wichtigen Diskussionsprozess in Gang, der zur Verabschiedung der »EU-Richtlinie zur elektronischen Signatur« geführt hat. Dabei wurde nicht nur der Begriff »digital« durch »elektronisch« ersetzt, sondern es sind eine Reihe weiterer relevanter Veränderungen im Vergleich zum ersten Signaturgesetz festgehalten.

Mit dem Ziel der europaweiten Vereinheitlichung der Regelungen zu elektronischen Signaturen und deren allgemeiner Gleichstellung mit der handschriftlichen Unterschrift trifft die EU-Richtlinie im Wesentlichen folgende Aussagen:

- Deregulierung, d.h. eine größere Offenheit bezüglich der technischen und organisatorischen Standards
- Rechtsverbindlichkeit auch im Bereich gesetzlicher Schriftformerfordernisse
- Volle beweisrechtliche Anerkennung

Die Implementierung der Richtlinie ins nationale Recht der Mitgliedstaaten musste bis zum 19.07.2001 erfolgen.

14.5.3 Neues Signaturgesetz (SigG) in Deutschland

Das neue Signaturgesetz macht weniger technische Vorgaben und sieht zudem Vereinfachungen für Trust Center (also Zertifizierungsanbieter oder auch Certification Authority) vor. Das SigG ist seit Mai 2001 und die Änderungen in BGB (Bürgerliches Gesetzbuch) und ZPO (Zivilprozessordnung) sind seit August 2001 in Kraft.

Die elektronische Signatur soll ein äquivalentes Substitut der handschriftlichen Unterschrift werden, d.h. überall dort, wo der Gesetzgeber die Schriftform zwingend vorschreibt, kann eine bestimmte Form der elektronischen Signatur eingesetzt werden. Zudem wird als neue Form die sogenannte »Textform« eingeführt, die auf Vereinbarungen etwa via E-Mail oder Fax abzielt und für weniger sensible Vorgänge gedacht ist.

Hervorzuheben für die beweisrechtliche Seite ist: Nach den Änderungen in der ZPO ist die freie richterliche Beweiswürdigung nicht mehr nur bei der Urkunde, sondern auch bei elektronisch signierten Dokumenten eingeschränkt.

Eine Zertifizierung der Trust Center durch die Regulierungsbehörde für Telekommunikation und Post (RegTP) ist für sie nicht mehr verpflichtend; eine Akkreditierung kann auf freiwilliger Basis erfolgen. Um dennoch ein hohes Maß an Sicherheit zu erhalten, müssen Trust Center für Schäden aufkommen, die Dritten durch Vertrauen auf ein ausgestelltes Zertifikat entstehen. Trust Center müssen sich gegen dieses Risiko mit mindestens 250.000 € versichern.

14.5.4 Varianten der E-Signatur

Aufgrund der Historie in den unterschiedlichen Ländern findet sich in der EU-Richtlinie eine Dreiteilung, die zwischen (einfachen) elektronischen Signaturen, fortgeschrittenen Signaturen und qualifizierten Signaturen unterscheidet. Qualifizierte Signaturen werden in Deutschland noch einmal danach differenziert, ob sie von einem akkreditierten Anbieter stammen oder nicht.

Leider trägt diese Differenzierung, die bis heute auch in Insiderkreisen zu Diskussionen über die »bessere« bzw. die »notwendige« Signatur führt, überhaupt nicht zur Einfachheit und Klarheit bei.

Entsprechend viele und teilweise auch falsche Interpretationen des Gesetzes finden sich in den verschiedenen Ausführungen zur E-Signatur. Wir werden uns daher hier zunächst direkt am Gesetzestext orientieren. In §2 des Signaturgesetz steht ***[11]***:

Im Sinne dieses Gesetzes sind:

- (Einfache) Elektronische Signatur

  »Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen"

(§ 2 Nr. 1 SigG)

- Fortgeschrittene Signatur

  »elektronische Signaturen nach Nummer 1, die
  a) ausschließlich dem Signaturschlüsselinhaber zugeordnet sind,
  b) die Identifizierung des Signaturschlüsselinhabers ermöglichen,
  c) mit Mitteln erzeugt werden, die der Signaturschlüsselinhaber unter seiner alleinigen Kontrolle halten kann, und
  d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann"

(§ 2 Nr. 2 SigG)

- Qualifizierte Signatur

  »elektronische Signaturen nach Nummer 2, die
  a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
  b) mit einer sicheren Signaturerstellungseinheit erzeugt werden"

(§ 2 Nr. 3 SigG)

- Qualifizierte Signatur mit Anbieter-Akkreditierung

  »Mit diesem wird der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen ... zum Ausdruck gebracht.«

(§ 15 Abs. 1 Satz 4)

Die »einfache« elektronische Signatur wird damit im Gesetz lediglich definiert als ein elektronisches Siegel, das den Aussteller erkennen lässt und mit den anderen Daten verknüpft ist. Es werden keinerlei Anforderungen definiert und es gibt keine Zertifizierung.

Dies gilt prinzipiell auch für die fortgeschrittene Signatur. Über die Definition erhält die fortgeschrittene Signatur jedoch insofern eine andere Qualität als sie

- einen Signaturschlüsselinhaber zugeordnet ist,
- eine eindeutige Identifizierung dieser Zuordnung ermöglicht und
- Manipulationserkennung voraussetzt.

Bereits die fortgeschrittene Signatur ist damit eindeutig personenbezogen.

Die qualifizierte Signatur hat als zusätzliche Merkmale:

- einen Gültigkeitszeitraum sowie
- Anforderungen an die Sicherheit der »Signaturerstellungseinheit« (Signaturspeicher, im allgemeinen Chipkarte).

In Deutschland wird innerhalb BGB und ZPO lediglich die qualifizierte Signatur als gleichwertig zum Beweiswert traditioneller Dokumente betrachtet.

Hinzu kommt eine Differenzierung in Abhängigkeit davon, ob der Herausgeber (Trust Center) eine Akkreditierung vorweisen kann.

Akkreditierte Trust Center müssen nachweisen, dass sie eine Vielzahl von technischen und organisatorischen Sicherheitsmaßnahmen erfüllen und es wird die Überprüfbarkeit dieser Signaturen über 30 Jahre sichergestellt.

14.5.5 Zeitsignatur

Nahezu gleich gestellt zur elektronische Signatur ist die Zeitsignatur. Dabei wird die zu signierende Datei (z.B. ein Text) mit einer Zeitangabe versehen und ebenfalls mit einer Signatur verschlüsselt. Sie erhält so einen elektronischen – nicht veränderbaren – Zeitstempel. Dazu signiert das Trust Center selber die Nachricht mit einem speziellen Zeitstempelschlüssel, um erkennbar zu machen, dass die Zeitangabe von einem lizenzierten Trust Center stammt.

Damit kann der eindeutige Nachweis erbracht werden, dass eine Datei mit diesem Inhalt zu diesem Zeitpunkt vorgelegen hat. Nachträgliche Manipulationen werden ebenfalls erkannt.

Prinzipiell stellt das Signaturgesetz an die Zeitsignatur die gleichen Anforderungen. So gibt es auch hier »qualifizierte« Zeitsignaturen. Der wesentliche Unterschied ist lediglich, dass Zeitsignaturen nicht personengebunden sind.

Was zunächst wie ein Nachteil aussieht, ist in der täglichen Praxis ein Vorteil, da automatisch über eine (statt eine pro Mitarbeiter) Signatur »gestempelt« werden kann. Sowohl organisatorisch als auch technisch sind solche Lösungen deutlich einfacher zu implementieren. Hinzu kommt, das im Bedarfsfall beide (zeit- und personengebundene) Signaturen kombiniert verwendet werden können.

14.6 Organisation

14.6.1 Analyse und Konzeption

Wie immer bei der Einführung einer neuen Technologie dürfen jedoch die organisatorischen Konsequenzen nicht außer Acht gelassen werden. Werden Dokumente nur noch in elektronischer Form vorgehalten, muss entsprechende Vorsorge für eine ausreichende organisatorische und technische Sicherheit getroffen werden, denn es entsteht eine neue, nicht zu unterschätzende Abhängigkeit von der Technik. Eine gut durchdachte Konzeption ist daher Voraussetzung für einen erfolgreichen Einsatz der E-Signatur. Aus solchen Überlegungen können sich dementsprechend vielfältige Einflüsse auf die Ablauforganisation und – in Randbereichen – auch auf die Aufbauorganisation ergeben.

Es wird – speziell international – auf absehbare Zeit mehrere unterschiedliche Verfahren für die elektronische Signatur geben, bei denen Aufwand bzw. Komforteinbußen und Sicherheit bzw. Anerkennung unterschiedlich ausgeprägt sind. Für die interessierten Unternehmen bedeutet dies, dass man sich intensive Gedanken machen muss über:

- die zu unterstützenden Vorgänge

  (Art und Anzahl externer Austauschpartner)

- die beteiligten Partner (offener oder geschlossener Benutzerkreis)

- die benötigten Sicherheitsstufen

  (z.B. abhängig von internen vs. externen Vorgängen, involvierte Kosten etc.)

- die Akzeptanz durch die Unternehmensführung und die Mitarbeiter

- die benötigten Arten elektronischer Signatur

  (»einfache« vs. »fortgeschrittene« vs. »qualifizierte« vs. »akkreditierte« Signatur)

- die benötigten Verschlüsselungsverfahren

  (z.B. mit/ohne Public Key, Schlüssellänge)

- die benötigten Identifikationsverfahren

  (z.B. SmartCard&PIN, diverse biometrische Verfahren)

- das benötigte Authentifizierungsverfahren

  (z.B. mit/ohne Trust-Center und eigenes, unabhängiges oder akkreditiertes Trust Center)

- die Organisation der Schlüssel (Erstellung, Verwaltung, Verteilung, Verifizierung) und von Maßnahmen bei Verlust, Diebstahl, Ausscheiden, Ablauf, Attributänderung

- die Gestaltung der technischen Umsetzung, inkl. Anpassung der Applikationen und Roll-Out der Client-Hard- und -Software

Dabei kann es durchaus sinnvoll sein, die unterschiedlichen Vorgänge in verschiedene Sicherheitsstufen zu kategorisieren und mit unterschiedlichen Ausprägungen der elektronischen Signatur zu unterstützen. Die Bewilligung eines Urlaubsantrages benötigt nicht die gleiche Sicherheit wie der Kauf eines Hochleistungscomputers und muss daher auch nicht gleichermaßen abgesichert werden.

Andererseits erhöht sich durch diese Differenzierung wieder die Komplexität der Lösung, so dass auch diesbezüglich eine Abwägung erfolgen muss. E-Signaturen sollten daher als Teil eines gesamtheitlichen Sicherheitskonzeptes gesehen und eingeführt werden.

14.6.2 Erwerb der elektronischen Signatur

Die von den verschiedenen Anbietern bereitgehaltenen Lösungen unterscheiden sich zum Teil ganz erheblich, nicht zuletzt in verschiedenen Bezeichnungen für dieselben Systeme. So wird das Angebot einmal nach Class-0 bis Class-4-Zertifikaten differenziert, einmal gar nicht, und ein weiteres Mal ist etwa von X.509-Zertifikaten die Rede.

Wichtig sind dabei letztlich folgende Punkte:

1. Einige Anbieter haben eine Genehmigung (Akkreditierung) von der RegTP zum Betrieb einer Zertifizierungsstelle, andere nicht bzw. noch nicht. Genehmigte Anbieter arbeiten signaturgesetzkonform und können Produkte anbieten, die neben voller Beweisbarkeit vor Gericht auch den Bereich gesetzlicher Schriftformerfordernisse weitgehend abdecken.
2. Nicht jeder benötigt eine Signatur, die den gesetzlichen Höchstanforderungen genügt und einen Anbieter, der diese erfüllt. Ein Zertifikat muss mitunter nur belegen, dass die angegebene E-Mail-Adresse existiert, nicht aber, dass der Unterzeichner tatsächlich der ist, für den er sich ausgibt.
3. Elektronische Signaturen, so wie sie der Gesetzgeber versteht – als Ersatz für die handschriftliche Unterschrift – können nur von natürlichen Personen beantragt und verwandt werden. Produkte, die etwa der Identifikation eines Internetservers dienen, gehören daher nicht zu dem hier beschriebenen Bereich.

Wer nur einen relativ niedrigen Sicherheitsstandard verwirklichen will, der hat unter den vorhandenen Anbietern die freie Wahl. Der Anbieter prüft je nach Zertifikatsklasse, ob die angegebene E-Mail Adresse existiert oder er lässt sich z.B. eine Kopie des Personalausweises vorlegen. Eine weitergehende Prüfung erfolgt in aller Regel nicht, und die gesamte Prozedur lässt sich vom heimischen PC aus erledigen.

Wer sich jedoch im gesetzeskonformen Bereich bewegen möchte, muss auf einen der genehmigten Anbieter ***[12]*** zurückgreifen. Dies waren zunächst vor allem Telesec (Deutsche Telekom) und Signtrust (Deutsche Post) sowie eine Reihe weiterer Anbieter, die z.T. die Infrastruktur von Telesec bzw. Signtrust nutzen. Signtrust hat sich mittlerweile aus diesem Geschäftsfeld zurückgezogen, es gibt aber derzeit noch 15 weitere Trust Center.

14.6.3 Antragstellung

Geschäftskunden beantragen die Signaturen direkt bei dem Trust Center und können dort im allgemeinen auch weitere Dienstleistungen beauftragen. Die Einführung von E-Signaturen ist ein komplexes – und meist erstmaliges – Projekt, bei dem man sich auch externer Partner bedienen sollte, um von deren Erfahrungen zu profitieren.

Die Antragstellung verläuft für Privatanwender folgendermaßen:

1. Der Erwerber füllt über die Homepage des Anbieters ein Online-Formular aus. Dies wird dann jedoch in aller Regel nicht online abgeschickt, sondern am heimischen PC ausgedruckt und unterschrieben.
2. Mit diesem unterschriebenen Formular begibt man sich zur nächstgelegenen Postfiliale oder zum Büro des Anbieters selbst. In der Postfiliale ist der Personalausweis persönlich vorzulegen, anhand dessen die Identifizierung des Antragstellers erfolgt. Das unterschriebene Formular wird an den Anbieter weitergeleitet. Unter Umständen muss auch noch eine unterschriebene Kopie des Personalausweises beigefügt werden.
3. Der Anbieter kann erst jetzt die sogenannte Zertifizierung vornehmen, wonach das an den Kunden ausgegebene Schlüsselpaar bestehend aus privatem und öffentlichem Schlüssel dem Kunden als Inhaber zugeordnet wird.
4. Es folgt die persönliche Auslieferung. Die PIN erhält man in der Regel in zwei Teilen. Erst dann ist der Gebrauch der Signatur möglich.

14.6.4 Weitere Funktionen beim Gebrauch der Signatur

Das Signieren einer E-Mail bzw. eines elektronischen Dokuments erfolgt nach dem oben beschriebenen Schema. Die Anbieter stellen darüber hinaus jedoch eine Reihe von Diensten zur Verfügung, die hier kurz erläutert werden sollen.

1. »Testzertifikat"

   Bei den Anbietern werden in der Regel Zertifikate zu Testzwecken ausgegeben. Hierbei handelt es sich um reine Software-Lösungen mit einer Gültigkeit von meist 30 Tagen. Die – online – angegebenen Daten werden jedoch keinerlei Prüfung unterzogen. Sie sind entsprechend auch ausschließlich zu Testzwecken nutzbar.

2. Verzeichnisdienst

   Die Anbieter betreiben Verzeichnisdienste, bei denen der Empfänger einer signierten Nachricht abfragen kann, ob das der elektronischen Signatur zugrunde liegende Zertifikat existiert und gültig ist.

3. Sperrdienst

   Bei Diebstahl oder Verlust der Chipkarte lässt sich diese wie eine EC-Karte sperren. Das ausgegebene Schlüsselpaar lässt sich zwar nach wie vor verwenden, da aber die Sperrung an den Verzeichnisdienst weitergegeben wurde, führt die Abfrage durch den Empfänger stets zu der Auskunft, dass das Zertifikat gesperrt wurde.

4. Gültigkeit

   Die Gültigkeitsdauer der ausgegebenen Zertifikate hängt vom jeweiligen Anbieter ab und beträgt ca. 3-5 Jahre. Dies hängt damit zusammen, dass die Anbieter (und der Gesetzgeber) wegen der voranschreitenden technischen Entwicklung ein bestimmtes Verfahren nur für eine gewisse Zeit als sicher einstufen können. Ändert sich jedoch das angewandte Verfahren, so lassen sich bestehende Zertifikate übernehmen.

   Von der Gültigkeitsdauer zu unterscheiden, ist die Nutzungsdauer der erworbenen Signatur. Die Anbieter verlangen nämlich neben der für den Ersterwerb anfallenden Kosten eine jährliche Nutzungsgebühr, ohne die sie ein Zertifikat nicht länger verwalten.

5. »Attribute«

   Teilweise besteht die Möglichkeit für Kunden, besondere Informationen mit den Zertifikaten zu verbinden. Dazu gehören z.B. Vertretungsmacht und -beschränkungen, Zugehörigkeit zu einem Unternehmen usw. Solche Zusatzinformationen werden bei der Zertifikatsabfrage durch den Empfänger übermittelt.

   Während über diese Funktionen neue organisatorische Möglichkeiten erschließbar sind, muss auch erwähnt werden, dass bisher eine Abbildung eines Mitzeichnungsverfahrens mit mehreren Unterschriften meist nicht vorgesehen ist. Lösungen dazu sind eher als »Labormuster« zu bezeichnen und in dem Signaturgesetz nicht berücksichtigt.

14.6.5 Biometrie

Ein bisher nicht zufriedenstellend gelöstes Problem ist der Verlust/Diebstahl der elektronischen Signatur, die üblicherweise auf einer Chipkarte gespeichert wird, welche wiederum über eine PIN geschützt ist. Verliert die PIN ihre Vertraulichkeit, kann ein Dritter mit diesem Wissen versuchen, in den Besitz der Karte zu kommen, um die elektronische Signatur zu missbrauchen. Der Gesetzgeber denkt daher zukünftig ausdrücklich an den Einsatz von biometrischen Verfahren, die als zusätzliche Hürde neben der PIN potenziellem Missbrauch vorbeugen können.

Unter biometrischen Verfahren versteht man dabei die Erkennung von eindeutig mit der Person verbundenen Merkmalen. Bekanntestes Beispiel ist der Fingerabdruck, aber auch das Scannen der Iris oder die Aufnahme der charakteristischen Druckverläufe beim Schreiben (z.B. einer konventionellen Unterschrift) gehören in diese Kategorie.

Die Sicherheit, dass es sich bei der Signatur um die richtige Person handelt und die Willensbekundung echt ist, wird dadurch deutlich erhöht. Bei der Aufnahme der Druckverläufe beim Schreiben ist sogar sichergestellt, dass die Person nicht im Rausch handelt. Allerdings erfordern die meisten Verfahren spezielle Hardware, was zunächst einem flächendeckenden Einsatz

entgegenwirkt. Sofern entsprechende Sensoren jedoch in Standard-Hardware einfließen oder beispielsweise zusammen mit den Kartenlesern implementiert werden, erbringen sie einen wesentlichen Sicherheitsgewinn.

14.6.6 Umsetzung

Laut A.T. Kearney ist kurzfristiges Marktvolumen lediglich im Bereich Business to Employer (B2E) zu erwarten, weil keine externe Abhängigkeiten zu berücksichtigen sind. B2B-Anwendungen sind mittelfristig zu erwarten, weil sie aufgrund bekannter Partner kontrollierbar sind, erhebliche Nutzenpotenziale erschließen und Kundenservice verbessern können. Der Business to Citizen (B2C)-Bereich wird sich erst langfristig entwickeln, dann aber zu großen Volumina führen.

Die Etablierung von Pilotprojekten im B2E-Bereich ist generell sinnvoll. Anwendungen mit Sicherheitsanforderungen sind beispielsweise bei der Beschaffung und Rechnungsprüfung zu sehen. Soweit sensible Informationen ausgetauscht werden, ist aber auch ein Ansatz bei Querschnittsapplikationen wie E-Mail und Dokumentenaustausch empfehlenswert.

Dies ist vor allem im Bereich Personal sowie Forschung und Entwicklung, aber teilweise auch bei Marketing und Vertrieb oder in der Buchhaltung der Fall. Sicherheitsexperten sind sich einig, dass die größte Gefahr von internen Mitarbeitern ausgeht. B2E-Anwendungen sollten somit nicht unterschätzt werden.

A.T. Kearney hat folgende Erfolgsfaktoren als Ergebnis mehrerer Studien für den E-Signatur- Einsatz definiert:

- Kosten von PKI senken
- Komplexität verringern für Administrator, Unsichtbarkeit/leichte Handhabung für Enduser erreichen
- Gewöhnung der Kunden an PKI, indem z.B. nur bestimmte Funktionalitäten angeboten werden
- Konzept um Anfangsinvestitionen für Kunden niedrig zu halten und um ROI (Return of Investment, d.h. die Amortisierung) aufzuzeigen
- Kritische Masse bei Anwendern erreichen
- Interoperabilität mit Hauptstandards sicherstellen
- Anpassung der Produkte an Regeln, Visionen und Notwendigkeit von geschlossenen Trustcommunities

Im Bereich der generellen Sicherheitsanalyse und -konzeption können bewährte Verfahren, wie das des BSI (Bundesamt für Sicherheit in der Informationstechnik) eingesetzt werden, das u.a. auch von C_sar bei der Erstellung von Sicherheitskonzepten angewandt wird.

Eine detaillierte Darstellung des Vorgehensmodells für die Einführung von E-Signaturen sprengt den hier vorgegeben Rahmen. Es sind die Prozesse, die sonstigen organisatorischen und technischen Randbedingungen, aber auch sozioökonomische Faktoren auf Seiten der Mitarbeiter und der Geschäftspartner zu berücksichtigen.

Auch ohne Betrachtung der restlichen Sicherheitsmaßnahmen ist für die Einführung der E-Signatur von einem Realisierungszeitraum nicht unter einem halben Jahr auszugehen.

14.7 Kritische Betrachtung

Es muss festgestellt werden, dass die E-Signatur noch eine geringe Akzeptanz genießt. Die Ursachen sind vielfältig. Teilweise resultieren Akzeptanzprobleme aus der bisher rein technisch dominierten Diskussion. Hashverfahren, asymmetrische Verschlüsselung und Kryptografie sind Begriffe mit denen nur Fachleute umgehen können.

Dabei scheint es sinnvoll sich zunächst mal einige »Grundweisheiten« vor Augen zu halten:

1. In Deutschland sind mündliche Verträge voll wirksam. »Schriftform« wird im BGB nur für wenige Rechtsgeschäfte vorgeschrieben. Entscheidend ist die Beweisfähigkeit und damit die Rechtsicherheit.
2. Die Beweiskraft einer traditionellen Unterschrift ist allgemein bekannt, sie ist einfach zu nutzen und sehr günstig (wenn man die prozessbedingten Folgekosten nicht betrachtet).
3. Die Akzeptanz einer neuen Technologie setzt folgendes voraus:
   - ausreichender Nutzen, um Verhaltensänderung zu initiieren,
   - einfachste Handhabung (vergleichbar mit bisherigem),
   - vertretbare Kosten (speziell für Privatkunden).

Vor allem 2. und 3. behandelt sozioökonomische Faktoren, die in der bisherigen Diskussion unzureichend berücksichtigt wurden. Neue Karten, Lesegeräte und PINs sind nicht nur unhandlich, sondern für Privatpersonen bzw. im breiten Einsatz bei Geschäftskunden auch kostenintensiv. Wirtschaftlichkeit kann daher nicht angenommen, sondern muss durch geschickte Lösungskonzeption im Einzelfall nachgewiesen werden. Hinzu kommen Kompatibilitätsprobleme der benötigten Produkte. Da der Nutzen nicht ausreichend kommuniziert wurde, muss sich jeder potenzielle Anwender fragen, warum er/sie die E-Signatur einsetzen soll.

Ohne massive Verbesserungen bei diesen Aspekten droht die E-Signatur zur Totgeburt zu werden, was sich niemand wünschen kann, denn eine effiziente Abwicklung des elektronischen Geschäftsverkehrs ist ohne E-Signatur

nicht möglich. Wie die Beispiele zu Online-Bestellungen und E-Billing gezeigt haben, wird täglich im großen Stil Geld verschenkt, weil die Nutzenpotenziale der E-Signatur nicht ausgeschöpft werden.

Bezüglich Kompatibilitätsproblemen sind vor allem die Hersteller gefordert. Einfache Handhabung ist eine Anforderung, die von dem Eingabe- und Speichersystem für die E-Signatur zu erfüllen ist. Primär ist an die Hersteller von Kartensystemen gedacht, aber es gilt auch für die diversen biometrischen Erfassungssysteme.

Software-Applikationen, die die E-Signatur nutzen, sind bisher kaum etabliert. Lediglich im E-Mail-Bereich und für SAP kann auf diverse Drittprodukte zurückgegriffen werden. Wie meist bei neuen Technologien handelt es sich um ein Henne-Ei-Problem, denn die Anpassung von Applikationen an Signaturprodukte muss kurz- bis mittelfristig einen ROI erwirtschaften.

Bei der einfachen Handhabung ist vor allem Kreativität bzgl. der Verwendungsmöglichkeiten von vorhandenen Verfahren gefragt. Warum können beispielsweise bestehende Kartensysteme nicht genutzt werden oder warum kann die E-Signatur-Infrastruktur nicht auch für andere Zwecke, z.B. Zugangskontrolle im Geschäftsbereich genutzt werden?. Bereits heute gibt es Firmenkreditkarten, Zugangskontrollsysteme, Kundenkarten und vieles mehr, was sich gut mit einer E-Signatur kombinieren ließe. Diese Kreativität ist nicht nur auf Anbieterseite gefragt. Dort gab es entsprechende Ansätze. Jedoch ist die gedankliche Auseinandersetzung auf Anwenderseite noch nicht weit genug fortgeschritten.

Die bestehende Probleme sind typisch für neue Technologien und Lösungen für rein technische Probleme sind kurzfristig zu erwarten. Für Piloteinsätze im B2E-Bereich sind sie zumeist irrelevant oder lassen sich gut kompensieren. Piloteinsätze sind aber genau das, was jetzt gefordert ist, um erste Einsparungen zu realisieren, Erfahrungen zu sammeln sowie Zukunftsfähigkeit und Produktreife voran zu treiben.

Organisatorische Konzeption ist unternehmensspezifisch, komplex und zeitintensiv, aber – auch bei E-Signatur – unabdingbar. Hier müssen sich die Anwender mit der neuen Technologie vertraut machen.

14.8 Fazit

Trotz der derzeitigen Ernüchterung im E-Business ist der elektronische Geschäftsverkehr zweifellos auf dem Vormarsch. E-Business ohne elektronische Signatur ist auf Dauer nicht vorstellbar. Der Übergang von der derzeitigen Experimentierphase des E-Business in den »Mission-critical«-Bereich wird nicht zuletzt an der Etablierung der elektronischen Signatur gemessen werden können.

Zusammenfassend bleibt festzuhalten, dass mit der neuen elektronischen Signatur erstmalig Rechtssicherheit ohne Anwendung der herkömmlichen Unterschrift erreicht wird. Auch bei dieser Technologie ist die effektive und

effiziente Lösung jedoch nicht einfach durch die Installation von Soft- und Hardware, sondern nur über ein stimmiges Gesamtkonzept zu erhalten. Unstrittig ist die neue Signaturgesetzgebung ein großer Schritt nach vorn, so dass der Einsatz der elektronischen Signatur in der Praxis möglich ist. Dafür ist die Zeit jetzt reif.

Erläuterungen. *[1]* Bewertung Zahlungsmoral bzw. Kreditwürdigkeit über entsprechende Anbieter.

[2] Zumindest die »Qualifizierte E-Signatur« (siehe Signaturgesetz).

[3] Diese Formulierung stellt natürlich eine starke Vereinfachung des wirklichen Verfahrens dar, vermeidet aber eine Erläuterung der für Laien unverständlichen mathematisch-technischen Details. Weiteres dazu im Kapitel über Kryptografie.

[4] Immer wieder geführte Diskussionen über die mangelhafte Wirtschaftlichkeit der Technik verkennen entweder die Einsparungspotenziale oder es mangelt an kreativen Lösungsansätzen. Ist der Nutzen klar quantifiziert und kommuniziert, ist Wirtschaftlichkeit meist eine Frage geschickter Lösungskonzeption.

[5] Eine relativ verständliche Beschreibung des Funktionsprinzips findet sich unter *www.teletrust.de* und eine animierte Darstellung unter *http://www.ti.fhg.de/ti-trust_center/digsig-visualisierung.html*

[6] Streng genommen wird natürlich eine Chipkarte und keine Person identifiziert.

[7] Eine Frage geschickter Konzeption ist natürlich, inwieweit bestehende Infrastrukturen (speziell in Unternehmen) genutzt werden können.

[8] Die Gartner Group hat beim B2B-Rechnungsempfänger $ 7,25 errechnet.

[9] Ein entsprechender Entwurf wurde im April 2002 durch den Bundestag verabschiedet.

[10] Die Konstruktion wurde damals bewusst gewählt, weil zunächst Erfahrungen gesammelt werden sollten. Leider war das Einsatzhemmnis so groß, dass bis heute wenig nennenswerten Praxiserfahrungen vorliegen.

[11] Layout und Text in ( ) durch Autor ergänzt.

[12] Die Liste der akkreditierten Trust Center findet man unter *http://www.regtp.de/tech_reg_tele/start/fs_06.html*

15 Sicherheitsrisiko E-Business?

Dr. Sachar Paulus

15.1 Umfassende Sicherheitsrichtlinien schaffen eine solide Basis für elektronische Geschäftsprozesse

Mit dem »Going Web« sind für Unternehmen eine Vielzahl von Risiken in Bezug auf die Datensicherheit verbunden. In der Regel werden vollständige Prozesse auf Internettechnologie verlagert; die dabei verarbeiteten vertraulichen Daten dürfen jedoch unter keinen Umständen in die Hände der Konkurrenz fallen. Aus diesem Grund müssen Sicherheitsrisiken rechtzeitig erkannt und entsprechende Maßnahmen ergriffen werden. In vielen Ländern ist dies sogar gesetzlich festgeschrieben, etwa durch das deutsche KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich). Mit diesem Gesetz, seit 1998 in Kraft, werden Unternehmen in Deutschland unter anderem verpflichtet, ein Überwachungssystem zur frühzeitigen Erkennung existenzgefährdender Entwicklungen einzurichten. Unternehmensweites Risikomanagement wird zur – häufig ungeliebten – Pflicht.

Informationen sind wertvoll – nicht nur für das Unternehmen selbst, sondern auch für seine Mitbewerber. Vier Faktoren sind ausschlaggebend für die Sicherheit sensibler Daten: Integrität (Daten können nicht manipuliert werden), Authentizität (der Urheber der Daten ist zweifelsfrei nachweisbar), Vertraulichkeit (Daten sind nur für die »richtigen« Adressaten zugänglich) und Verfügbarkeit (Daten sind zugänglich, wenn man sie benötigt). Sicherheit im E-Business bedeutet, diese Eigenschaften zu erhalten.

Doch nicht um jeden Preis. Bevor Maßnahmen ergriffen werden, gilt es, eine Risikoanalyse durchzuführen, um den Wert der zu schützenden Daten und die Wahrscheinlichkeit eines Schadens zu ermitteln. Damit steht eine Kenngröße für akzeptable Investitionen in Schutzmechanismen zur Verfügung. Im Anschluss an die Risikoanalyse sollten die in Frage kommenden Schutzmechanismen untersucht werden, insbesondere unter dem Aspekt der Durchführbarkeit. Nach Ausarbeitung eines Vorschlags empfiehlt es sich, die Geschäftsführung in die Entscheidung mit einzubeziehen, damit auch auf oberster Ebene die meist unvermeidbaren Auswirkungen auf die Geschäftsabläufe mitgetragen werden. Die Untersuchungen sollten in regel-

mäßigen Abständen wiederholt werden, um Kontinuität im Datenschutz zu erreichen. Ergebnis dieses Prozesses ist eine möglichst detaillierte Sicherheitsrichtlinie (Security Policy) .

Die Sicherheitsrichtlinie muss alle sicherheitsrelevanten Bereiche eines Unternehmens abdecken, denn nur durch ein lückenloses Konzept können die im E-Business erforderlichen Vertrauensbeziehungen aufgebaut werden. Die dokumentierten Prozesse sollten in einer umfassenden Sicherheitsarchitektur unter Berücksichtigung von vier zentralen Aspekten umgesetzt werden: einer effizienten Benutzer- und Rollenverwaltung, sicherem Systemmanagement, der Abbildung von Vertrauensbeziehungen und den Sicherheitsmechanismen auf Anwendungsebene.

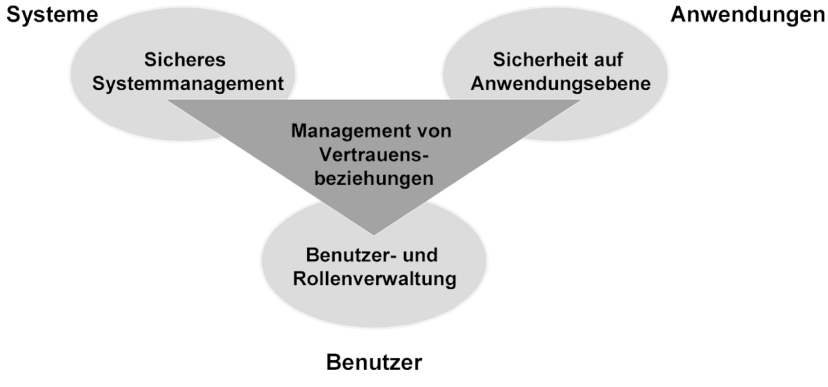


Abbildung 15.1: Vertrauen im E-Business

15.1.1 Benutzer- und Rollenverwaltung

Neue Geschäftsprozesse im E-Business bieten Unternehmen vielfältige Möglichkeiten, Kunden und Partner nahtlos in ihre Geschäftsabwicklung zu integrieren und auch den eigenen Mitarbeitern mehr Verantwortung für Prozesse und Abläufe zu übertragen. Doch wie lässt sich zuverlässig sicherstellen, dass interne und externe Benutzer tatsächlich nur auf die Informationen zugreifen können, die für ihre Augen bestimmt sind? Und wie können Rollen und Berechtigungen für die Mitarbeiter sicher, effizient und anwendungsunabhängig verwaltet werden?

Vor dem Hintergrund der Internetwirtschaft, in der elektronische Geschäftsprozesse komplexe Systemlandschaften erfordern und Unternehmensnetze zunehmend nach außen geöffnet werden, ändern sich auch die Anforderungen an die Benutzer- und Berechtigungsverwaltung. Einfache, zentralisierte Administrationsprozesse, die Integration externer Benutzer in das eigene Berechtigungswesen, ein universelles Rollenkonzept für alle im Unternehmen eingesetzten Anwendungen sowie die Integration von Verzeichnisdiensten über Unternehmensportale stehen dabei im Vordergrund.

In vielen Systemlandschaften liegen Benutzerinformationen in unterschiedlichen Systemen vor: E-Mail-, Telefon- und Anwendungssysteme sind typische Beispiele. Die Benutzerdaten werden meist in eigenen Verzeichnissen (Directories) abgelegt; oft enthalten die verschiedenen Verzeichnisse eines Unternehmens daher gleiche oder ähnliche Daten. Um eine redundante Datenhaltung zu vermeiden, können die einzelnen Verzeichnisse in einem zentralen Unternehmens- oder Metaverzeichnis zusammengeführt werden, das die Benutzerdaten direkt aus dem Human-Resource (HR)-System bezieht und an alle angeschlossenen Systeme – z.B. Messaging-, Telefon- oder Anwendungssysteme – weitergibt. Auch Rollen- und Zuständigkeitsinformationen können hier gespeichert werden. Mit dem Einsatz eines Verzeichnisdienstes erhält die Benutzerverwaltung einen »Single Point of Administration«, der durch die Minimierung redundanter Datensätze und eine Zentralisierung der Administrationsprozesse ein Höchstmaß an Effizienz und Sicherheit bietet.

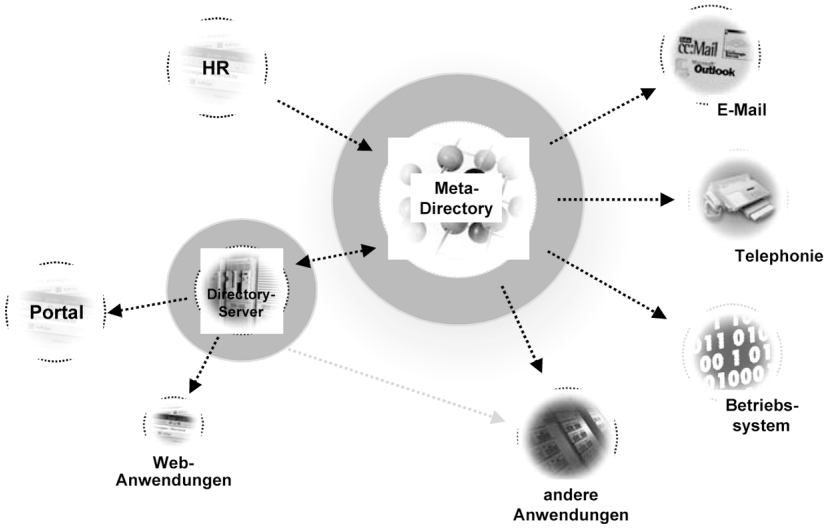


Abbildung 15.2: Benutzerverwaltung mit Verzeichnisdienst

Das Rollenkonzept sollte eine klare Trennung von Rollen und Berechtigungen vorsehen, um eine anwendungsübergreifende Anwendbarkeit zu gewährleisten und die Administration zu vereinfachen. Eine Rolle besteht aus einer Reihe logischer Services, die zum Tätigkeitsprofil des Mitarbeiters gehören, beispielsweise das Anlegen von Kundenaufträgen oder die Fakturierung von Bestellungen. Diese logischen Services werden physischen Services, etwa dem Zugriff auf entsprechende Transaktionen oder Berichten in einem Anwendungssystem, zugeordnet. Rollen werden demnach auf der Basis der ausgeübten Tätigkeiten, d.h. »Bottom-up«, und auf Abteilungsebene definiert. Enthalten sie zugleich die Berechtigungen für den Mitarbeiter, führt dies zu einem sehr aufwändigen Administrationsprozess, da Berechtigungen üblicherweise »Top-down« unter Berücksichtigung der

Organisationsstruktur und Position des Benutzers im Unternehmen festgelegt werden. Zudem werden sie meist an zentraler Stelle, etwa im HR-Organisationsmanagement, oder in den einzelnen Anwendungen, z.B. im Controlling oder im Finanzwesen, vergeben.

15.1.2 Systeme sichern

Die Kunst einer sicheren Netzwerkkonfiguration – etwa Netzwerksegmente zu definieren und Firewalls zu konfigurieren – ist seit langer Zeit bekannt. Da sich die Unternehmensnetze zunehmend nach außen öffnen, wird es jedoch immer schwieriger, alle Sicherheitslücken zu schließen. Das Netzwerk sollte über verschiedene Sicherheitszonen und wenige, durch Firewalls geschützte, Übergänge zwischen diesen Zonen verfügen. Insbesondere für die externen Zugänge zum Unternehmensnetz werden sogenannte demilitarisierte Zonen (DMZ) durch Kombination einer externen und einer internen Firewall geschaffen. Dies stellt sicher, dass nur aus bestimmten Zonen und nur über zuvor festgelegte Dienste und Protokolle Zugriff auf die Informationssysteme besteht.

Wenn nun noch Mechanismen zur Authentifizierung der Systemkomponenten und Verschlüsselung der Kommunikation zwischen Servern hinzu kommen, besteht bereits eine gute Absicherung. Für die Internet-Kommunikation wird deshalb der grundsätzliche Einsatz von HTTP über das Standard-Internetprotokoll Secure Sockets Layer (HTTPS = HTTP über SSL) empfohlen. HTTPS wird inzwischen von allen gängigen Web-Servern und Web-Browsern auch mit starker Verschlüsselung weltweit unterstützt. Darüber hinaus ist es möglich Intrusion-Detection-Systeme (IDS), die ungewöhnliche Aktivitäten aufzeichnen und unbefugtes Eindringen erkennen können, in das Systemmanagement zu integrieren.

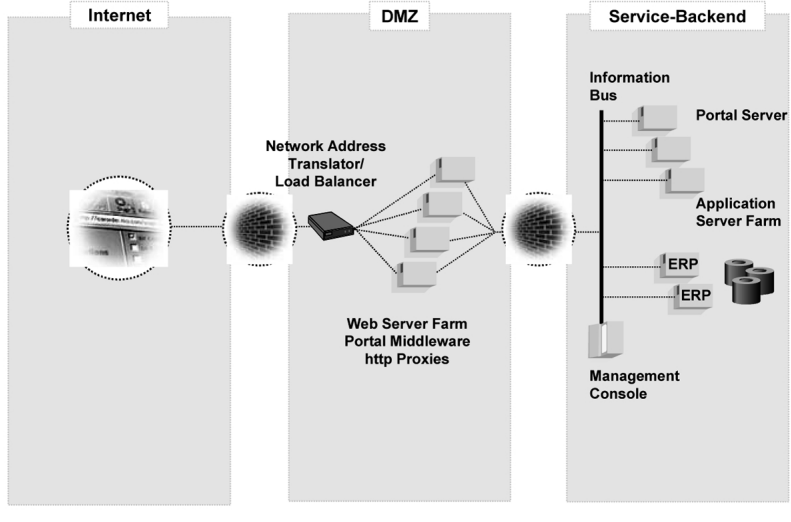


Abbildung 15.3: Sichere Netzwerkarchitektur

15.1.3 Vertrauen schaffen durch zuverlässige Authentifikation

In einer komplexen E-Business-Systemlandschaft werden die verschiedenen Authentifikationsmechanismen immer unübersichtlicher. Bei der Vielzahl von Systemen kann sich kaum ein Anwender alle Passwörter merken. Deshalb sind Verfahren wie Single Sign-On und Authentifikationsdelegation unabdingbar für eine E-Business-Landschaft.

Die Systeme sollen zunehmend sowohl von innen, d.h. von den eigenen Mitarbeitern, als auch von außen, also von Kunden und Partnern, genutzt werden. Aus diesem Grund muss der Mechanismus, über den sich die Anwender anmelden und zweifelsfrei identifizieren, ebenso sicher wie einfach verwendbar sein. Digitale Zertifikate, die von einem anerkannten Trust Center ausgestellt werden, bieten durch standardisierte Authentifikationsprozesse ein Höchstmaß an Sicherheit bei der elektronischen Geschäftsabwicklung. Anwender registrieren sich bei einer vertrauenswürdigen Registration Authority, die im Idealfall direkt in die Benutzerverwaltung integriert ist und die Benutzerdaten an das Trust Center weitergibt. Das Trust Center stellt die Verbindung zwischen der Person und einer »digitalen Identität« her. Diese besteht aus einem Schlüsselpaar mit einem öffentlichen und einem geheimen Schlüssel. Das Zertifikat enthält den Namen des Inhabers sowie den öffentlichen Schlüssel der digitalen Identität; den geheimen Schlüssel kennt nur der Inhaber des Zertifikats. Zertifikate dienen beispielsweise der Authentifikation an Portalen oder virtuellen Marktplätzen.

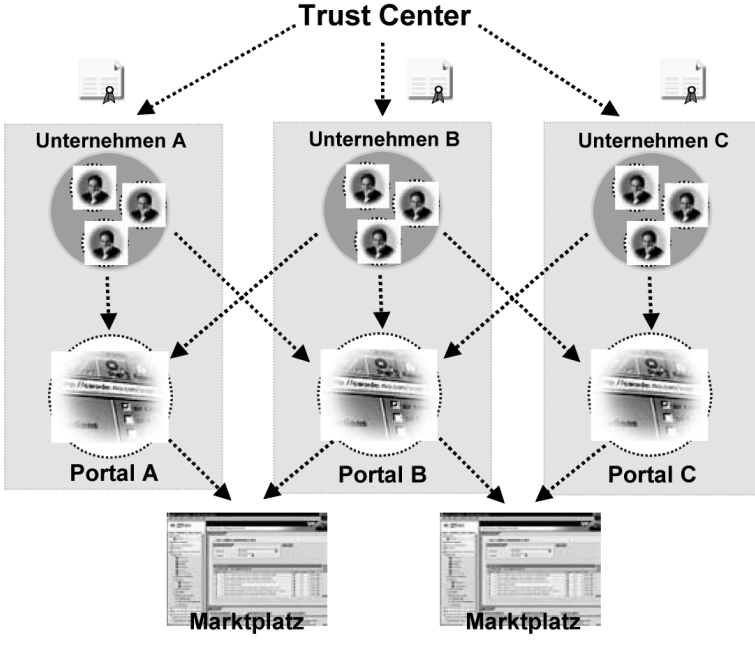


Abbildung 15.4: Sicherer Zugriff auf externe und interne Web-Sites

15.1.4 Sicherheitsmechanismen auf Anwendungsebene

Geschäftsprozesse werden heute häufig über mehrere, miteinander verzahnte Systeme abgewickelt. Eine revisionssichere Umgebung ist daher nicht mehr allein durch eine detaillierte Berechtigungsadministration zu erreichen. Wenn Prozesse in Systemlandschaften verteilt ablaufen, muss die Verbindlichkeitsinformation an die Daten selbst gekoppelt werden, damit der Nachweise für eine korrekte Verwendung der Daten geführt werden kann. Dies erfolgt über elektronische Signaturen. Sie statten unternehmensübergreifende Transaktionen mit elektronischen Merkmalen aus, mit deren Hilfe über einen langen Zeitraum hinweg sowohl Authentizität als auch Integrität der Daten nachgewiesen werden können.

Die hierfür erforderliche Technologie kann jedoch nicht zentral bereitgestellt werden, sondern ist in den jeweiligen Anwendungsprozess integriert. Durch die elektronische Signatur werden Daten, beispielsweise eine Online-Bestellung, mit zusätzlichen Informationen versehen, die der Nicht-Abstreitbarkeit der Transaktion dienen. Alle Systeme, die diese Daten verarbeiten und über entsprechende Funktionen für die Verifizierung elektronischer Signaturen verfügen, können die Informationen überprüfen. Die Überprüfung erfolgt auf mehreren Ebenen. So kann beispielsweise die Art des Zertifikats oder das ausstellende Trust Center ausschlaggebend für die Akzeptanz der Signatur sein; zudem wird die Gültigkeit des Zertifikats zum Zeitpunkt der Signatur geprüft. Geschäftsprozesse, deren Transaktionen elektronisch signiert werden, müssen über eine entsprechende Konfiguration zum Abbruch der Transaktionen bei negativ verlaufener Verifizierung verfügen.

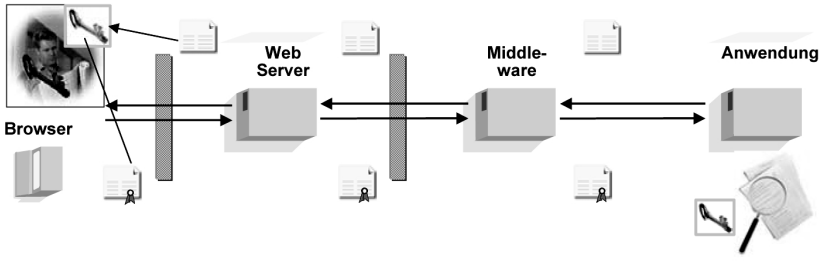


Abbildung 15.5: Transaktionssicherheit durch digitale Signaturen

Auch in anderen Bereichen trägt die Anwendung selbst die Verantwortung für die Sicherheit, etwa bei gesetzeskonformen elektronischen Signaturen für Ausschreibungen und Verträge, elektronischen Bezahlverfahren, E-Mail-Verschlüsselung oder Kryptografie.

15.1.5 Herausforderung Sicherheit

Mit der zunehmenden Nutzung des Internets wird der Schutz unternehmenseigener Systeme und Daten, schon in Zeiten geschlossener Systemlandschaften keine einfache Aufgabe, zur Herausforderung. Sicherheitsmechanismen, die zuvor systemorientiert implementiert wurden, müssen nun in zunehmendem Maße auf Transaktionsebene umgesetzt werden. Doch wenn die Sicherheitsrichtlinie eines Unternehmens die vier Bereiche der Sicherheitsarchitektur in angemessenem Maße berücksichtigt, können die vielfältigen Möglichkeiten des E-Business ausgeschöpft werden – ohne unnötige Sicherheitsrisiken einzugehen.

16 Eine typische Anwendung: Sichere E-Mail

Uwe Krieger

16.1 Einleitung

Nachdem die Kryptografie bis vor noch vor nicht allzu langer Zeit hauptsächlich Gegenstand von militärischem Interesse war, hat sie heute durch die zunehmende Verbreitung der Informationstechnologie Einzug in eine Vielzahl von Anwendungen gefunden. Neben der klassischen Verschlüsselung von Daten gibt es zahlreiche weitere Einsatzmöglichkeiten: Erstellung elektronischer Signaturen als Äquivalent zur handschriftlichen Unterschrift, Authentisierungsdienste im Bereich der Zugangs- und Zugriffskontrolle, Protokolle für sicheres elektronisches Bezahlen oder für die Durchführung von Wahlen im Internet, Anonymisierungsdienste (auf Seiten von Servern und von Clients), Lösungen der Copyright-Problematik und vieles mehr.

Das hier betrachtete Beispiel ist die Absicherung einer der beliebtesten Anwendungen im Internet, der Übermittlung elektronischer Nachrichten. Folgende Ziele sollen dabei erreicht werden:

- Wahrung der Vertraulichkeit: Nur der rechtmäßige Empfänger einer Nachricht soll in der Lage sein diese zu lesen.
- Sicherung der Authentizität: Der Empfänger sollte sich vergewissern können, dass eine Nachricht wirklich vom vorgegebenen Absender stammt.

Eine konsequente Verwendung von Programmen, welche dies gewährleisten sollen, ist aber nicht die Regel (obwohl solche Programme zum Teil sogar kostenlos erhältlich sind). Beispielsweise ist es nicht einfach, in Firmennetzen einen gesicherten Nachrichtenaustausch zu gewährleisten. Selbst bei relativ einfach erscheinenden Anwendungen stößt man ab und zu auf erstaunliche Probleme.

Ein einfaches Beispiel: Üblicherweise werden Firmennetze heutzutage mit aufwändigen Maßnahmen gegen drohende Angriffe von außen geschützt. Standard in diesem Bereich sind Schutzmaßnahmen wie der Aufbau von Firewall- und zentralen Virenschutz-Systemen. Was aber passiert nun, wenn solch ein System mit einer gesicherten, in diesem Fall verschlüsselten Mail für einen Mitarbeiter konfrontiert wird? Eine Prüfung der Inhalte auf potenzielle Schädlinge, eigentlich die Aufgabe der Virenschutzprogramme, ist aufgrund der Verschlüsselung ja nicht möglich. Wie soll in solch einem Fall vorgegangen werden?

Die interessante Beobachtung ist, dass dort die verschiedensten Dinge passieren können: Manchmal wird die Zustellung der Nachricht verweigert (da sie aufgrund der Verschlüsselung nicht auf potenzielle Schädlinge geprüft werden kann), manchmal wird sie problemlos weitergeschickt (da bei einer Prüfung der verschlüsselten Inhalte natürlich keine Viren entdeckt werden konnten).

Dies geht inzwischen so weit, dass man mittlerweile von manchen Kommunikationspartnern direkt aufgefordert wird, beispielsweise PowerPoint-Präsentationen oder Excel-Tabellen lieber verschlüsselt zuzusenden. »Die werden wegen der ganzen Makros nicht mehr durchgelassen; schicken Sie es doch einfach mit PGP verschlüsselt, dann ist es kein Problem«. So einfach ist das für den »normalen« Nutzer, wenn die Sicherheitssoftware Inhaltsüberprüfung und E-Mail-Verschlüsselung nicht integriert. Quasi wird das eine Sicherheitssystem genutzt, um ein anderes zu umgehen. Dies ist ein erhebliches Risiko, da man hiermit auf die funktionierenden (und vor allem stets zu aktualisierenden) zusätzlichen Virenschutzprogramme auf dem Client angewiesen ist. In der Tat kann es sein, dass schädliche Inhalte das Gateway des Unternehmens passieren, obwohl man dort eigentlich die notwendigen Schutzmaßnahmen vorgesehen hat.

16.2 Sicherheitsanforderungen

An sichere elektronische Dienstleistungssysteme werden Anforderungen aus den verschiedensten Bereichen gestellt; von der technischen Seite sind dies vor allem die Einhaltung von Standards, Anbindung an evtl. vorhandene Infrastrukturen oder die Modularität von Lösungen. Aber natürlich gibt es eine Reihe von anderen wichtigen Gesichtspunkten. Lösungen im kommerziellen Umfeld müssen ökonomisch sein, Profitabilität, Time-to-Market und Investitionsschutz sind zu gewährleisten. Dazu kommen gerade im Bereich der IT-Sicherheit eventuell auch politische Aspekte. Nationale oder internationale Gesetzgebung sind zu berücksichtigen, in speziellen Anwendungsbereichen (z.B. im Bankenumfeld) sind zusätzliche Vorgaben von Institutionen zu beachten.

Im Folgenden werden eine Reihe von Aspekten, die im Umfeld der sicheren E-Mail eine Rolle spielen, näher beleuchtet. Nach einer Betrachtung der vorliegenden Situation und einer kurzen Darstellung der zugrunde liegenden Techniken erfolgt eine genauere Betrachtung des eingangs erwähnten Beispiels: Wie erstellt man ein sinnvolles Konzept für die gemeinsame Nutzung verschiedener, in ihrer Funktion teilweise widersprüchlich erscheinender Mechanismen (in diesem Fall eine Kombination aus Virenschutz, der Verwendung von Firewalls und eben dem gesichertem Nachrichtenaustausch)?

16.3 Der Stand heute

Trotz des Booms, den das World-Wide-Web (WWW) in den letzten Jahren erlebt hat, ist E-Mail nach wie vor einer der meistgenutzten Internetdienste. Aus vielen Kommunikationsbeziehungen ist sie aufgrund der Einfachheit und Schnelligkeit des Informationsaustausches nicht mehr weg zu denken. Dass Sicherheit gerade bei dieser Anwendung eine wesentliche Rolle spielt, sollte eigentlich offensichtlich sein: Im Gegensatz zum Web, bei dem es größtenteils um im Prinzip öffentlich zugängliche HTML-Seiten geht, wird E-Mail eher für den Austausch von als vertraulich angesehenen Informationen genutzt.

Trotzdem sind Verschlüsselungsstandards wie SSL (Secure Socket Layer) oder IPSec (IP Security Protocol) im WWW auch heutzutage noch etablierter als Programme für die Absicherung der E-Mail: in diesem Bereich werden die zur Verfügung stehenden bestehenden Mechanismen oder Programme momentan noch kaum genutzt. Einem Großteil der Benutzer ist anscheinend noch nicht klar, dass diese Art der elektronischen Kommunikation eben nicht mit einem normalen (also verschlossenen) Brief zu vergleichen ist, sondern eher einer für alle einsehbaren Postkarte entspricht.

Was sind die Gründe für diese mangelnde Akzeptanz? Neben dem erwähnten mangelnden Problembewusstsein sind dies sicherlich zum Teil auch »politische« Aspekte: Bislang sorgten sich üblicherweise staatliche Stellen um die Vertraulichkeit (Brief-, Post- bzw. Fernmeldegeheimnis) übermittelter Informationen. Nun hat der Anwender erstmalig Methoden zur Verfügung, die Vertraulichkeit von Daten in eigener Verantwortung sicher zu stellen. Er entzieht mit dieser Vorgehensweise natürlich aber übergeordneten Instanzen die Kontrollmöglichkeit. Die Folge ist, dass vertrauliche (also verschlüsselte) E-Mail von einigen Stellen immer noch als suspekt angesehen wird. Solche Vorbehalte sind vielleicht der Grund dafür, dass man erstaunlich häufig auf Reaktionen trifft wie: »Warum soll ich meine Nachrichten verschlüsseln, ich habe doch nichts zu verbergen?«

Auf der anderen Seite gibt es sicher auch eine Reihe von technischen Gründen für die geringe Verbreitung: In der Vergangenheit waren eine Vielzahl der angebotenen Lösungen einfach zu kompliziert, um sich durchsetzen zu können. Ein Benutzer erwartet heute, dass solch eine Anwendung eben nicht nur für Spezialisten verwendbar ist, sondern für jedermann mit ein oder zwei Klicks unter der ihm vertrauten Oberfläche zur Verfügung steht. Die Akzeptanz der Benutzung verschlüsselter Nachrichten lässt sich deshalb vor allem durch die Verfügbarkeit von transparenten – d.h. für den Benutzer unsichtbaren – und einfach zu bedienenden Lösungen steigern (das Problem, wie es mit der Akzeptanz von Lösungen besteht, die nicht kontrolliert werden können und deren Ausfall nicht bemerkt werden würde, wird dabei erst einmal nicht weiter berücksichtigt).

16.4 Standards und Anwendungen

Bei einer Applikation für E-Mail-Sicherheit handelt es sich um einen Ansatz, bei dem die Sicherheitsfunktionen nicht auf der Transportebene, sondern auf der Anwendungsschicht realisiert werden. Dies hat (neben der Tatsache, dass man sich bei der Definition der Protokolle nicht unbedingt auf den kleinsten gemeinsamen Nenner einigen muss) auch den Vorteil, dass die Funktionalität im Allgemeinen nicht an bestimmte Plattformen gebunden ist. Für den Austausch von Nachrichten zwischen Rechnernetzen vollkommen unterschiedlicher Architekturen ist dies natürlich eine wesentliche Eigenschaft.

Als Vorreiter von Programmen in diesem Bereich ist PGP (*Pretty Good Privacy*) von Phil Zimmermann anzusehen. PGP war Anfang der neunziger Jahre eines der ersten Programme, mit welchem Verschlüsselungstechnologien einem größeren Anwenderkreis zur Verfügung gestellt wurden; mit dieser Anwendung begann die eigentliche Verbreitung der Public-Key-Kryptografie.

Im kommerziellen Umfeld haben inzwischen Anwendungen auf Basis offener Standards (wie z.B. Zertifikate gemäß ANSI X.509) die größere Relevanz. Beispiele hierfür sind Verschlüsselungsstandards wie S/MIME (*Secure/Multipurpose Internet Mail Extensions*) oder der ältere PEM-Standard (*Privacy Enhanced Mail*). Die Funktionsweise dieser Protokolle bzw. Programme ist aber in allen Fällen vergleichbar: Üblicherweise wird eine Kombination aus klassischen, symmetrischen Verschlüsselungsmethoden und aus asymmetrischen (Public-Key-) Verfahren eingesetzt:

- Das symmetrische Verfahren wird zur Verschlüsselung der übertragenen Nachrichten eingesetzt.
- Mit dem asymmetrischen Verfahren wird einerseits die Übertragung des für die Entschlüsselung notwendigen, bei jeder Nachricht unterschiedlichen Sitzungsschlüssels abgesichert, andererseits ist man mit dieser Klasse von Verfahren auch in der Lage, elektronische Signaturen zu erzeugen.

Daneben gibt es eine überschaubare Anzahl von Zusatzfunktionen, welche hauptsächlich das Schlüsselmanagement (also das Erzeugen und Verwalten der kryptografischen Schlüssel) betreffen.

Die Verschlüsselungskomponenten waren noch vor einiger Zeit eigenständige Programme. Inzwischen ist die Funktionalität üblicherweise in Form eines Plug-In in gängige Mail-Clients (wie MS Outlook oder Lotus Notes) integriert. Wie später noch zu sehen sein wird, treten häufig aber gerade an dieser Schnittstelle zwischen eigentlicher Anwendung und Verschlüsselungskomponente Schwachstellen zutage.

16.5 Notwendige Infrastrukturen

Wer schon einmal mit Programmen wie PGP gearbeitet hat, wird es am eigenen Leib erlebt haben: Das eigentliche Problem liegt in der Verwaltung der Schlüssel von Kommunikationspartnern. Zu Beginn ist zu gewährleisten, dass die notwendigen Schlüssel auf sichere Art und Weise ausgetauscht werden. Gerade bei größeren Benutzergruppen ist es nicht trivial sicherzustellen, dass man nicht einen falschen Schlüssel untergeschoben bekommt oder veraltete Informationen benutzt.

Um diese Probleme in den Griff zu bekommen, bedient man sich üblicherweise des Konzeptes der Trustcenter. Als vertrauenswürdige Dritte haben diese die Aufgabe, durch die Ausstellung von Zertifikaten, die kryptografischen Schlüssel der Benutzer zu beglaubigen oder auch zu erzeugen. Dies hat den Vorteil, dass jeder Kommunikationspartner für die sichere Beschaffung von Schlüsseln auf eine zentrale Instanz zurückgreifen kann.

Gerade mit der Verabschiedung des deutschen Signaturgesetzes im Jahre 1997 machten sich zahlreiche Firmen die Hoffnung, mit dem Betrieb eines Trustcenters Erfolg am Markt erzielen zu können. Bisher wurden diese Hoffnungen jedoch enttäuscht und erste Anbieter haben sich bereits wieder vom Markt zurückgezogen. In vielen Bereichen werden damit immer noch Verschlüsselungssysteme eingesetzt, die auf Trustcenter-Zertifikate verzichten.

16.6 Virenschutz vs. Verschlüsselungstechnologien

Kommen wir zurück zu dem eingangs erwähnten Beispiel des Konflikts zwischen E-Mail-Verschlüsselung und der Notwendigkeit den Inhaltsüberprüfung eingehender E-Mails. Einerseits gehören heute aufwändige Firewalls und die Inhaltsüberprüfung eingehender E-Mails auf potenziell schädliche Inhalte zum Standard. Andererseits wird ein oft noch kleiner, aber wichtiger Teil der Unternehmenskommunikation verschlüsselt durchgeführt. Häufig werden dabei lokal installierte E-Mail-Plugins eingesetzt. Eine zentrale Kontrolle dieser E-Mails ist aufgrund der Verschlüsselung der Nachrichten damit nicht mehr möglich. Die Systemverantwortlichen stecken damit in einem Dilemma: Erst haben sie ein komplexes Firewall-System mit Virenscan aufgebaut, und nun entziehen sich immer mehr Nutzer der Kontrolle.

Um sich einer möglichen Gefahr durch Inhalte von verschlüsselten Mails kategorisch zu entziehen, haben einige Unternehmen Sicherheitsrichtlinien, nach der eine verschlüsselte Mail beim Eintreffen im System grundsätzlich an den Absender zurückgeschickt wird. In diesem Fall erreicht die Mail den Empfänger überhaupt nicht. Dieses Vorgehen stellt keine Lösung, sondern lediglich eine Problemverlagerung dar, zumal man ja davon ausgehen muss, dass gerade verschlüsselte E-Mails eine höhere Priorität besitzen. Es können

bei diesem Vorgehen zwar Adressen von Absendern definiert werden, deren Mails auch in verschlüsselter Form das Gateway passieren dürfen. Dieses bedeutet jedoch einen Mehraufwand für den Administrator und verringert nur das erwähnte Sicherheitsrisiko am Client, ohne wirklich Sicherheit zu garantieren.

Das Wachstum von E-Commerce und E-Government wird aber zwangsläufig zu einer Zunahme verschlüsselter E-Mails führen. Vor diesem Hintergrund dienen die Sicherheitsrichtlinien lediglich der bestmöglichen Schadensbegrenzung. Eine einheitliche Lösung, die für den Umgang mit verschlüsselten Inhalten in einem Firewall-System wirkliche Sicherheit garantiert und langfristigen Investitionsschutz gewährt, ist anzustreben.

Die bestehenden Ansätze für die Koexistenz von Inhaltsüberprüfung und Verschlüsselung von E-Mails lassen sich nach technischen Gesichtspunkten wie folgt unterscheiden:

A) Client-zu-Client-Verschlüsselung mit lokaler Inhaltskontrolle

Die einfachste Möglichkeit besteht darin, übliche Verschlüsselungs-Plugins in die E-Mail-Clients zu integrieren und die Verschlüsselung damit durch den Anwender selbst durchführen zu lassen. Der grundsätzliche Nachteil ist dabei, dass so nur noch eine lokale Kontrolle verschlüsselter E-Mails möglich ist. Damit muss die Software zur Inhaltskontrolle lokal installiert werden. Die Nachteile liegen dabei auf der Hand: wie erwähnt kann der Anwender lokal die Software zur Inhaltskontrolle außer Funktion setzen. Darüberhinaus ist eine zentrale Konfigurationskontrolle nicht einfach zu etablieren und noch schwerer aufrechtzuerhalten.

B) Client-zu-Client-Verschlüsselung mit zentrale Inhaltskontrolle

Hier wird ebenfalls eine Ende-zu-Ende-Verschlüsselung bis zum Empfänger durchgeführt, die E-Mail wird jedoch zusätzlich mit dem öffentlichen Schlüssel der prüfenden Instanz (also einem firmeneigenen Schlüssel) chiffriert. Damit kann die E-Mail an zentraler Stelle entschlüsselt und eine Inhaltskontrolle durchgeführt werden. E-Mails, die diese zusätzliche Verschlüsselung nicht aufweisen, werden nicht durchgelassen. Vorbedingung ist damit, dass alle Kommunikationspartner dieses System unterstützen; das ist damit auch das größte Problem bei der Einführung eines solchen Systems.

C) Hinterlegen der Anwenderschlüssel für die Inhaltskontrolle

Dieses Modell sieht vor, die privaten Schlüssel aller Anwender zusätzlich zentral zu speichern, um für die Inhaltskontrolle darauf zugreifen zu können. Die Anwender können dabei ihre üblichen, lokalen Verschlüsselungsprogramme weiter nutzen. Hier stellt die Sicherheit der Schlüsselverwaltung ein großes Problem dar: Ein Angriff auf diese Datenbank würde auf einen Schlag sämtliche Schlüssel kompromittieren. Außerdem ist die Verwendung üblicher Sicherheitstoken hier nicht möglich. Aus diesen Geräten, die darüber definiert sind, dass ein Benutzer sie pro-

blemlos bei sich tragen kann und die für ihn bestimmte, sicherheitskritische Aufgaben übernehmen (typisches Beispiel ist eine Smartcard), kann der private Schlüssel üblicherweise nicht ausgelesen werden.

D) Reine Server-zu-Server-Verschlüsselung

Anderer Lösungsweg: Die Verwendung von E-Mail-Proxies, welche als eine Art Filter z.B. zwischen den Mail-Servern arbeiten und alle übermittelten Nachrichten verschlüsseln bzw. elektronisch signieren. Damit ist eine E-Mail auf ihrem Weg über das Internet geschützt, außerdem ist als Vorteil zu nennen, dass für den Benutzer diese Vorgehensweise natürlich vollkommen transparent ist. Andererseits sind die Nachteile offensichtlich: Zum einen ist keine echte Ende-zu-Ende-Sicherheit erreicht, zum anderen lässt sich solch eine Lösung nur schwer in offenen Systemen realisieren. Für die Umsetzung in geschlossenen Benutzergruppen, wie z.B. die sichere Anbindung verschiedener Firmenstandorte, mag ein solcher Ansatz aber sehr wohl ein vernünftiger Kompromiss sein. Es ist allerdings zu akzeptieren, dass die Kommunikation innerhalb der jeweiligen Firmennetzwerke nicht gesichert ist.

E) Client-zu-Client-Verschlüsselung, Bereitstellung des Transferschlüssels

Bei diesem Ansatz wird eine verschlüsselte E-Mail zwischengespeichert und dem Empfänger eine Anfrage zur Übersendung des Schlüssels für die Inhaltsüberprüfung gesandt. Da übliche E-Mail-Verschlüsselungen auf hybriden Verfahren basieren, kann der Empfänger seinen privaten Schlüssel selbst hochsicher auf einer Smartcard gespeichert haben. Er entschlüsselt damit den Transferschlüssel, mit dem die eigentliche E-Mail geschützt war, und leitet ihn weiter, so dass die E-Mail zentral entschlüsselt und überprüft werden kann. Ist er mit der Inhaltsüberprüfung nicht einverstanden, kann die Mail gelöscht oder weitergeleitet werden.

16.7 Einschätzung der Alternativen

Alles in allem hängt eine Entscheidung für den einen oder anderen Ansatz natürlich von vielen Einflussfaktoren ab. Möglichkeit (A) wirft grundsätzliche Probleme wegen des rein lokalen Ansatzes auf und sollte daher vermieden werden. Die Ansätze (C) und (D) sind bei nicht allzu hohen Sicherheitsanforderungen einsetzbar, ansonsten jedoch aus den bereits erwähnten Gründen problematisch. Werden in einem Unternehmen bereits sogenannte PSE (*Personal Security Environment*) wie z.B. Smartcards genutzt und sollen diese auch für die E-Mail-Verschlüsselung eingesetzt werden, bleiben die Verfahren (B) und (E) übrig. Die zusätzliche Verschlüsselung für die Inhaltskontrolle (B) ist für den Empfänger transparent – für ihn ändert sich nichts. Allerdings müssen sich alle Absender an das System anpassen und eine zusätzliche Verschlüsselung durchführen, so dass in der Praxis Probleme bei der Abstimmung mit Kommunikationspartnern zu befürchten sind.

Bei der Anwender-Entschlüsselung des Transferschlüssels für die zentrale Inhaltskontrolle (E) sind die Lasten anders herum verteilt: der Absender bleibt unbeeinflusst, und der Empfänger muss einen zusätzlichen Schritt (die Entschlüsselung des Transferschlüssels) durchführen. Bis auf diesen erhöhten Bedienungsaufwand auf Empfängerseite bietet dieser Ansatz aber nur Vorteile, deshalb hier die etwas genauere Darstellung des möglichen Vorgehens:

- Eine hybrid verschlüsselte E-Mail erreicht das Gateway und wird auf dem Server zwischengespeichert. Die verschlüsselte E-Mail setzt sich unter anderem aus der mit dem Transferschlüssel symmetrisch verschlüsselten E-Mail und aus dem mit einem Public-Key-Verfahren verschlüsselten Transferschlüssel zusammen. Der verschlüsselte Transferschlüssel wird innerhalb des Firewall-Systems identifiziert, abgetrennt und mit einer entsprechenden Anfrage an den Empfänger geschickt.
- Dieser kann nun entscheiden, ob die E-Mail vom System analysiert werden soll. Die Firewall wird die Mail bei diesem Verfahren auf keinen Fall ungeprüft passieren lassen; man kann dem Empfänger aber an dieser Stelle die Möglichkeit geben, beispielsweise eine alternative Adresse wie einen privaten E-Mail-Account anzugeben, an welche die Mail weiter zu leiten ist.
- Üblicherweise gibt der Empfänger jedoch seine Zustimmung und entschlüsselt den für die Nachricht verwendeten Transferschlüssel. In der Praxis könnte dies z.B. bedeuten, dass der Empfänger auf eine Anfrage hin seine Smartcard in ein Lesegerät einlegt und die Aktion mit der Eingabe seiner PIN bestätigt. Anschließend wird der Transferschlüssel zurückgesandt. Dieser Versand des entschlüsselten Transferschlüssels kann mit einer einfachen Verschlüsselung versehen werden.
- Danach ist der Server in der Lage, mit Hilfe des nun verfügbaren Transferschlüssels die verschlüsselte E-Mail entschlüsseln. Nach Überprüfung des Inhaltes und anschließender Freigabe kann die ursprüngliche, verschlüsselte E-Mail an den Empfänger weitergeleitet werden. Im Falle von Auffälligkeiten kann sie wegen gefährdender Inhalte direkt gelöscht oder an einer besonderen Stelle zwecks weiterer Bearbeitung gespeichert werden. In diesem Fall erhält der vorgesehene Empfänger lediglich eine Information über den Vorgang.

Die zu leistende Integrationsarbeit für die Nutzung dieses Verfahrens ist allerdings nicht zu unterschätzen. Es werden zwei Module benötigt: eines auf Serverseite, sowie ein Modul für den Client, das üblicherweise in das Mailprogramm integriert ist. Diese Module müssen an die im System vorhandene Mail-Software auf Server und Client angepasst sein. Außerdem ist die korrekte Kommunikation mit dem verwendeten Virenscan-System zu gewährleisten.

Beim Absender hingegen sind für die Anwendung des Systems keinerlei Änderungen notwendig. Er kann seine übliche S/MIME- oder PGP-konforme Verschlüsselungssoftware weiter nutzen.

16.8 Stichwort Key Recovery

Sichere, also elektronisch signierte oder verschlüsselte E-Mails haben sicherlich eine Reihe von Vorzügen, es ergeben sich dadurch aber auch einige zusätzliche Dinge, die zu beachten sind. Eine Standardfrage ist beispielsweise die, was zu tun ist, falls die Informationen, die zum Entschlüsseln einer chiffrierten Nachricht notwendig sind, verloren gegangen sind? Heutzutage wird immer mehr dazu übergegangen, private Schlüssel zum Schutz vor Attacken nicht auf dem PC zu speichern, sondern in den bereits erwähnten PSEs. Bekannteste Beispiele sind SmartCards oder sogenannte USB-Token, allesamt Gegenstände, welche schon von ihrer Größe her ideal dafür geeignet sind, sie zu verlegen oder zu verlieren. Was ist, wenn damit der Zugang zum eigenen Posteingang temporär oder auf Dauer nicht mehr möglich ist, weil alle gespeicherten Nachrichten nur verschlüsselt vorliegen?

In diesen Fällen sollen Mechanismen zum *Key Recovery* oder auch *Key Escrow* weiter helfen. Hierunter versteht man Methoden, kryptografische Schlüssel oder verschlüsselte Nachrichten auch ohne die eigentlich notwendigen Informationen verfügbar zu machen. Zu unterscheiden sind dabei auf jeden Fall:

- *Key Recovery*: Der Zugriff auf den privaten Schlüssel eines Benutzers.
- *Data Recovery*: Der Zugriff auf dauerhaft gespeicherte verschlüsselte Daten.
- *Message Recovery*: Der Zugriff auf verschlüsselte Inhalte, ohne den eigentlichen Schlüssel eines Benutzers zu kompromittieren.

Als Grundsatz kann man davon ausgehen, dass *Key Recovery* im Allgemeinen überflüssig ist, wenn ein Signaturschlüssel, d.h. der geheime Teil eines für die Erstellung elektronischer Signaturen verwendeten Schlüsselpaares verloren gegangen ist. Bis zum Zeitpunkt des Verlustes erstellte Signaturen können weiterhin mit Hilfe des immer noch verfügbaren öffentlichen Schlüssels verifiziert werden, es können lediglich keine neuen Signaturen mehr erstellt werden. In solch einem Fall ist es einfacher und auch sicherer, für die Erstellung künftiger Signaturen den verlorenen Schlüssel nicht zu rekonstruieren, sondern stattdessen besser ein neues Schlüsselpaar zu erzeugen.

Data Recovery ist dagegen im kommerziellen Einsatz als legitimes Interesse der Beteiligten anzusehen, hat aber wenig Berührungspunkte mit der eigentlichen Nachrichtenübermittlung, da in der Regel wohl kaum die eigentlichen E-Mails archiviert werden. Ansonsten muss ein hierfür gedachtes Konzept natürlich sorgfältig geplant werden und gleichermaßen die Interessen einer Firma am Zugriff auf archivierte Daten und evtl. Persönlichkeitsrechte von Mitarbeitern berücksichtigen. Der naheliegendste und einfachste Ansatz besteht darin, bei einer Verschlüsselung für den zu speichernden Inhalt nicht nur personen-gebundene Schlüssel zu verwenden, sondern auch geeignete firmeneigene Schlüssel.

Es bleibt der Fall von *Message Recovery*, also in diesem Fall die Möglichkeit, ohne Beteiligung des eigentlichen Empfängers auf verschlüsselte Nachrichten zugreifen zu können. Lösungen in diesem Bereich sind zumindest als zwiespältig anzusehen, der Einbau entsprechender Mechanismen weckt natürlich zu Recht die Befürchtung, dass derartigen »Hintertüren« auch unberechtigt genutzt werden könnten. Nachdem in PGP entsprechende Funktionalität eingebaut wurde, bekam der Vertreiber der kommerziellen Versionen von PGP die Bedenken der Anwender deutlich zu spüren.

16.9 Archivierungsprobleme

Probleme mit der Archivierung von Mails sind natürlich eng mit dem zuletzt behandelten Thema verknüpft. Will man im Nachhinein (evtl. Jahre später) auf gespeicherte Nachrichten zurückgreifen, ist nicht unbedingt gewährleistet, dass sie sich auch zu diesem Zeitpunkt noch entschlüsseln lassen, bzw. dass elektronische Signaturen noch überprüfbar sind.

Auch hier ist der Themenbereich der elektronischen Signatur eigentlich wieder einfacher abzuhandeln. Der Verlust öffentlicher Schlüssel stellt keine ernst zu nehmende Gefahr dar, da diese beliebig dupliziert werden können. Um auch Jahre später die Authentizität zu gewährleisten, ist die Re-Signierung von Daten eine Möglichkeit. Hierbei werden vor Ablauf des Gültigkeitszeitraumes eines Zertifikats die Datenbestände bzw. Nachrichten erneut signiert.

Das Verfahren hat aber natürlich eine prinzipielle Schwäche: Der Zeitpunkt, wann eine elektronische Signatur unüberprüfbar wird und deswegen durch eine neue Signatur zu ergänzen bzw. zu ersetzen ist, kann nicht immer im voraus bestimmt werden. Das Zertifikat läuft zwar zu einem eindeutig bestimmten Zeitpunkt ab, ausgeschlossen ist aber nicht, dass es durch eine Kompromittierung des Schlüssels schon vorher ungültig wurde. Damit entsteht eventuell das Problem, dass eine Signatur nicht rechtzeitig aktualisiert wurde und damit die Kette unterbrochen ist.

Als einfachste Lösung für das Problem des Zugriffs auf verschlüsselte Nachrichten kann der Hinweis gelten, den Posteingang nicht als Archiv zu missbrauchen. Dauerhaft zu speichernde Daten sind zu extrahieren und separat zu speichern. Das Problem beim späteren Zugriff auf Informationen stellt sich damit in dieser Form nicht.

16.10 Trojanische Pferde

Die vorhergehenden Abschnitte beschäftigten sich hauptsächlich mit technischen oder organisatorischen Schwierigkeiten bei der Einbindung von gesicherter E-Mail. Hier geht es nun hauptsächlich um die Darstellung einiger möglicher Angriffe und – soweit möglich – entsprechender Gegenmaßnahmen.

Geht man einmal davon aus, dass eine Signatur üblicherweise auf dem Rechner (PC) des Anwenders erzeugt wird, so ist klar, dass an diesem Punkt Angriffe möglich sind. Der für die Erstellung von Signaturen notwendige private Schlüssel mag sogar üblicherweise zum Schutz vor Attacken in verschlüsselter Form auf dem PC gespeichert sein; zu einem bestimmten Zeitpunkt (nämlich während der Erstellung der Elektronischen Signatur) liegt er aber unverschlüsselt im Hauptspeicher.

Das Problem ist nun, dass alle gängigen Betriebssysteme im Prinzip zulassen, dass andere, zeitgleich auf dem PC laufende Anwendungen diesen Prozess beobachten (zum Erspähen des privaten Schlüssels) oder verfälschen (um an die Signatur unter anderen als den eigentlich gewünschten Daten zu erlangen). Die größte Gefahr geht dabei von sogenannten Trojanischen Pferden aus, also Programmen, die unter Vorspiegelung einer nach außen sichtbaren Funktionalität versteckte schädliche Funktionen aufweisen.

Selbst wenn der Signaturschlüssel besonders gesichert ist, was typischerweise durch Speicherung und Anwendung auf einer Smartcard gewährleistet ist, lassen sich immer noch Attacken finden. Zum einen kann der für die Freischaltung des Schlüssels notwendige Zugriffscode (üblicherweise eine PIN) abgefangen werden, zum anderen verbleibt natürlich das Problem der Verfälschung zu signierender Daten.

16.11 WYSIWYS: What You See Is What You Sign

Die naheliegende Möglichkeit, sich gegen diese Art von Attacken zu schützen, ist natürlich die komplette Abschottung des verwendeten Rechners gegenüber der feindlichen Umgebung (üblicherweise dem Internet). Solch ein Ansatz mag innerhalb von Firmen oder Institutionen durch die Umsetzung strenger Sicherheitsrichtlinien sogar umsetzbar sein, für einen privaten Anwender ist diese Vorgehensweise aber unrealistisch.

Notwendig wäre stattdessen eine sichere Anzeigeeinheit, welche zu signierende Daten verlässlich darstellt und dafür Sorge trägt, dass nur diese dem Signierprozess unterworfen werden. Zwar gibt es zahlreiche Versuche, diese Funktionalität in Form einer Softwarelösung zur Verfügung zu stellen, aufgrund der geschilderten generellen Schwachstellen von Betriebssystemen dürfte diesem Ansatz aber kein Erfolg vergönnt sein.

Einzig Erfolg versprechender Weg ist, Anzeige- und Signiereinheit enger aneinander zu koppeln. Nur so wäre gewährleistet, dass vorhandene »Schädlinge« nicht in der Lage sind, die Kommunikation zwischen diesen Komponenten zu verfälschen. Existierende Designstudien integrieren deshalb die dazu notwendigen Komponenten in den Monitor: Enthält dieser zusätzlich einen Smartcard-Leser sowie eine kleine Recheneinheit, welche in der Lage ist, bestimmte Dokumentenformate (z.B. PDF; bitte aber ein Format

ohne Makrofähigkeit!) anzuzeigen, so schiene das Problem erst einmal gelöst. Zu signierende Daten könnten z.B. über den USB-Anschluss an das Gerät übermittelt werden. Danach würden alle Vorgänge nur noch auf dieser Einheit ablaufen. Theoretisch könnte man sie sogar vom eigentlichen PC trennen.

16.12 Weitere Fallstricke

Das eine Kette nur so stark anzusehen ist wie ihr schwächstes Glied, ist allgemein bekannt. Insbesondere wenn man ein komplexeres System aus mehreren Modulen zusammen setzt, muss man dem natürlich Rechnung tragen, indem man darauf achtet, dass alle Bestandteile die geforderten Eigenschaften in Bezug auf die Sicherheit haben.

Man sollte sich aber bewusst sein, dass gerade im Bereich der IT-Sicherheit etliche Fallstricke lauern. IT-Sicherheit gibt es nicht als »Baukasten«; Hauptproblem ist normalerweise der Übergang zwischen den einzelnen Bestandteilen.

Auch hierzu gibt es natürlich Beispiele aus dem Bereich der E-Mail-Sicherheit. Ein besonders deutliches bezieht sich auf einen »Optimierungsversuch« bei MS Outlook, welcher vor einiger Zeit Aufmerksamkeit erregt hat. Das Problem entstand dadurch, dass versucht wurde, die Reaktionszeit beim Versenden von Nachrichten mit (evtl. sehr großen) Attachments (Anhängen) spürbar zu verringern. Lösungsansatz war, diese Attachments schon vorab (also nachdem sie auf eine noch im Entwurf befindliche Nachricht gezogen wurden, aber bevor der Knopf zum Versenden betätigt wurden) an einen evtl. vorhandenen Exchange-Server zu übersenden. Auch wenn der Absender den festen Willen hat, die Inhalte nur verschlüsselt zu übersenden, auf dem Server sind die Informationen durch diese Vorgehensweise trotzdem in unverschlüsselter Form vorhanden.

Ob dies ein Problem darstellt oder nicht, muss von Fall zu Fall entschieden werden (der Exchange-Server befindet sich ja üblicherweise im Firmennetz). Hauptproblem ist, dass die Problematik für den Anwender normalerweise nicht erkennbar ist. Ist solch eine Problem erst einmal erkannt, so kann es – wie auch in diesem Fall durch die Anbieter der Verschlüsselungskomponenten geschehen – relativ schnell gelöst werden.

16.13 Evaluierung im Bereich der IT-Sicherheit

Um Problemen in Bezug auf die Sicherheit von Anwendungen oder Systemen entgegen zu wirken, gibt es allerdings auch Mechanismen. Ähnliche »Gütesiegel« wie man sie aus dem Bereich Qualitätsmanagement kennt kann man im Bereich der IT-Sicherheit erwerben. Dies betrifft als direktes

Äquivalent zu einer Zertifizierung nach ISO 9000 z.B. den Themenbereich Sicherheitsmanagement: Der Standard BS 7799 bzw. ISO 17799 beschreibt, welche Anforderungen zu erfüllen sind, um beispielsweise als Firma nachzuweisen, dass man auch in diesen Bereichen die notwendigen Anforderungen erfüllt.

Wichtiger in Bezug auf das Thema hier ist aber, dass es ähnlich wie die Hauptuntersuchung eines Kfz beim TÜV oder ähnlichen Institutionen auch für Produkte aus dem IT-Sicherheitsbereich ein Siegel zur Bestätigung der Sicherheit gibt. Gängige sind die europaweit entwickelten Kriterien nach ITSEC (*Information Technology Security Evaluation Criteria*) oder nach CC (*Common Criteria*).

Aber auch hier lauern Fallstricke, die zu beachten sind. Ein Knackpunkt ist beispielsweise der erste Schritt, die Erstellung der sogenannten Sicherheitsvorgaben. Gegen dieses normative Dokument wird im Rahmen der weiteren Evaluierung geprüft, die dort beschriebenen Eigenschaften (und eben nur diese) werden beurteilt. Werden in diesem Dokument bestimmte Angriffsszenarien nicht berücksichtigt, so kann es sein, dass ein Produkt den Stempel zur Bestätigung der Sicherheit erhält, obwohl es in der Praxis angreifbar ist.

Die von der Systematik ansonsten den ITSEC sehr ähnlichen Common Criteria (CC) tragen diesem Problem Rechnung: Ein Schutzprofil (*Protection Profile, PP*) beschreibt ein typisches IT-Sicherheitsproblem inkl. einer allgemeinen, CC-konformen Lösung. Aus solch einem Schutzprofil können verschiedene Sicherheitsvorgaben (*Security Target, ST*) mit relativ geringem Aufwand abgeleitet werden, ohne dass deren Konsistenz neu geprüft werden müssen. Da solche Schutzprofile selbst im Sinne der CC evaluiert werden müssen, ist gewährleistet, dass sie in sich geschlossen, sinnvoll und widerspruchsfrei ist. Erst damit wird ein Schutzprofil potenziell für eine größere Anzahl von Produkten und Systemen anwendbar und der Nutzen des Konzeptes sichtbar.

Ein typisches Beispiel für ein PP ist das von mehreren großen Halbleiterherstellern definierte PP für Smartcard-Prozessoren; Ähnliche Meilensteine für reine Software-Produkte, wie z.B. eine E-Mail Applikation, sind aber noch nicht vorhanden.

16.14 Fazit

Es gibt einige von der technischen und von der organisatorischen Seite praktikable Möglichkeiten, wie mit Sicherheitsanforderungen bei verschlüsselten Mails umgegangen werden kann. Sie variieren jedoch erheblich in dem gegebenen Maß an Sicherheit und Vertraulichkeit. Welche Lösung im konkreten Fall praktikabel ist, wo Prioritäten gesetzt werden und welche rechtlichen Grundlagen eingehalten werden müssen, muss jeder Anwender bzw. Administrator vor Ort entscheiden. Bei ständig steigender Kommunikation über das Internet werden die Anforderungen an die Komplexität und der Abstimmung der einzelnen Sicherheitstools immer wichtiger. Der Abbruch

der Kommunikation aus Sicherheitsgründen kann nur das letzte Mittel sein das System zu schützen. Schließlich erhält der Adressat die Daten überhaupt nicht – kein probates Mittel, besonders vor dem Hintergrund eines wachsenden Kryptografiebedarfs.

Literatur. [CC] Common Criteria for Information Technology Security Evaluation, Version 1.0, 1996

[ITSEC] ITSEC: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik – Information Technology Security Evaluation Criteria

[IPSEC] RFC 2401, »Security Architecture for the Internet«, November 1998, *http://www.ietf.org/rfc/rfc2401*

[PEM] RFC 1421-1424, »Privacy Enhancement for Internet Electronic Mail«, Februar 1993, *http://www.ietf.org/rfc/rfc1421 ff*

[S/MIME] RFC 2633, »S/MIME Version 3 Message Specification«, Juni 1999, *http://www.ietf.org/rfc/rfc2633*

[SSL] RFC 2246, »The TLS Protocol Version 1.0«, Januar 1999, *http://www.ietf.org/rfc/rfc2246*

17 Sicherheit von Online-Banking: Anspruch und Wirklichkeit

Frank Schipplick

17.1 Einleitung

Das Online-Banking ist hinsichtlich seiner Sicherheit in den letzten Jahren mehrfach durch verschiedene Medienberichte in Verruf gekommen. Bei der Masse der Laien hat sich dadurch trotz unseriöser Pauschalisierungen ein negativer Eindruck bezüglich Sicherheitsfragen bei Internet-Technologien gebildet.

Die wohl spektakulärste Meldung im letzten Jahr war der erfolgreiche Angriff auf den Web-Server der HypoVereinsbank, den Hacker im Auftrag des ARD-Magazins »Ratgeber Technik« durchgeführt haben. Die Angreifer gelangten so an die Daten von 1,5 Millionen Kunden – Kontostände, Überweisungsdaten, Dispositionskredite etc. – da diese unverschlüsselt auf dem Web-Server abgelegt waren. Diese Daten wurden dann auszugsweise in der besagten Fernsehsendung veröffentlicht.

Am nächsten Tag sank der Aktienkurs der HypoVereinsbank um 5%. Ob der gesamte Kursverlust auf diesen Fernsehbeitrag und die anschließenden sehr negativen Pressemeldungen zurückzuführen war, ist zwar nicht eindeutig nachweisbar. Allerdings war der Imageschaden für die HypoVereinsbank immens. Über die daraus entstandenen finanziellen Schäden wurde natürlich »der Mantel des Schweigens« gelegt.

Im vorliegenden Artikel werden die zur Zeit gängigen Online-Banking-Verfahren – PIN/TAN-Lösungen und HBCI (Homebanking Computer Interface) – hinsichtlich ihrer Sicherheit beleuchtet. Dabei werden nicht nur die theoretischen Sicherheitslücken herausgestellt, sondern auch ihre praktische Relevanz beschrieben. Denn die absolute Sicherheit gibt es nicht und Sicherheit bewegt sich immer im konkurrierenden Dreieck zwischen Benutzerfreundlichkeit und Kosten. Der Leser soll in die Lage versetzt werden, die Risiken und die Vorteile des Online-Banking für sich selbst abschätzen und zukünftige Meldungen über Sicherheitslücken richtig einordnen zu können.

Dazu werden zunächst die möglichen Angriffsszenarien allgemein beschrieben. Im nächsten Schritt erfolgt eine Darstellung des Schutzbedarfs für Online-Banking-Systeme. Anschließend werden dann die verschiedenen Verfahren beschrieben, die Unterschiede zwischen ihnen herausgestellt und sicherheitstechnisch bewertet.

17.2 Angriffsszenarien

Die größte Gefahr für die IT-Sicherheit besteht zur Zeit darin, dass die Werkzeuge und Methoden für die meisten Angriffe **für Millionen Menschen** über das Internet frei verbreitet werden und nicht mehr nur ausgesprochenen Computerspezialisten zur Verfügung stehen. Nahezu jede Computerzeitschrift bietet auf beiliegenden CDs eine Sammlung höchst effektiver Programme zum Selbstbau von Viren oder zur Penetration fremder Rechnersysteme an. Zwischen Medienvertretern und Hackern ist zudem ein Wettlauf um das nächste Opfer mit bekanntem Namen entbrannt, so dass sich zu Kriminellen, die bereit sind, zur eigenen Bereicherung das Risiko hoher Strafen auf sich zu nehmen, eine große Anzahl von Personen gesellt, die »für den guten Zweck«, zur Steigerung ihres Bekanntheitsgrades oder zur Selbstverwirklichung **systematisch** Firmen und Institutionen angreift. Für Hacker gibt es neben staatlichen Institutionen kaum ein begehrteres Ziel als namhafte Banken, weil nicht nur die Möglichkeit besteht, große Summen zu stehlen, sondern die Bewunderung, die einem für einen erfolgreichen Hackversuch in der Szene und der Öffentlichkeit entgegengebracht wird, besonders groß ist.

17.2.1 Angriffe auf den Client

Der Client befindet sich unter der Kontrolle des Kunden, so dass das Einbringen von Schadsoftware nur durch den Kunden selbst verhindert werden kann. Letztendlich muss hier ein Risiko in Kauf genommen werden. Aber die Sicherheitsarchitektur von Bankanwendungen kann das Schadensausmaß eines erfolgreichen Angriffs und den Aufwand für die Sperrung des Zugangs des Angreifers und/oder den Weiterbetrieb bestimmen.

Die Sicherheit von Bankanwendungen ist insbesondere betroffen, wenn

- falsche Transaktionsdaten erzeugt werden bzw. Transaktionsdaten gefälscht oder verfälscht werden,
- die Software Aktionen vorspiegelt, die gar nicht stattfinden und/oder
- private oder geheime Schlüssel entwendet werden.

Die Entwendung von Schlüsseln stellt hierbei die größte Gefahr dar. Mit den gestohlenen Schlüsseln kann der Angreifer in die Rolle des berechtigten Kunden schlüpfen und Transaktionen »in dessen Namen« ausführen.

Diese Art von Sicherheitslücken ist zu unterscheiden von der Verwendung schwacher Kryptografie oder zu kurzer Schlüssel. Da er die Schlüssel einfach »stehlen« kann, muss der Angreifer keine aufwändige Kryptoanalyse durchführen, um die Schlüssel aus aufgefangenen Nachrichten abzuleiten.

Diebstahl von Geheimnissen durch Angriffe auf den Client

Besonders sensibel sind immer individuelle Autorisierungsdaten, die zur Anmeldung eines Nutzers für einen bestimmten Dienst oder zur Autorisierung einer Transaktion notwendig sind. Durch Schadsoftware (wie z.B. »Trojanische Pferde«) können im Extremfall Schlüssel, Zertifikate und – während der Eingabe – auch Nutzerkennung und Passwörter ausgespäht werden. Ein Angreifer kann diese Daten nutzen, um der Bank gegenüber in der Identität des Kunden aufzutreten (»Maskerade-Angriff«). Abgehört werden können sowohl die Tastatureingabe als auch der Inhalt des Bildschirms.

Das Schadenspotenzial eines Diebstahls von Autentifizierungsmerkmalen wie Zertifikaten und/oder Schlüsseln unterscheidet sich stark abhängig davon, ob benutzerspezifische Autentifizierungsmerkmale oder für alle Nutzer (= Nutzergruppe) gleiche Merkmale eingesetzt werden. Mit dem Besitz eines einzelnen Merkmals kann der Angreifer nur in der Rolle eines einzelnen Kunden agieren und der Schaden bleibt auf diesen Kunden beschränkt. Mit einem unspezifischen Merkmal kann der Schaden prinzipiell auf den gesamten Bereich ausgedehnt werden.

Sicherheitsrisiko Internetbrowser und Betriebssystem

Immer wieder erscheinen Berichte über lückenhafte Implementierungen von Sicherheitsmaßnahmen in Browsern: Die Bereiche, in denen Java Script, Applets oder ActiveX ablaufen, sind unzureichend gegen andere (schutzwürdige) Bereiche des PCs abgeschottet. Ebenso zahlreich sind Berichte über Schwachstellen in Betriebssystemen (insbesondere Microsoft-Produkte). Ein Angreifer kann ihm bekannte Lücken für Angriffe ausnutzen, insbesondere um Daten oder Programme abzurufen, zu löschen und/oder zu verändern bzw. das Verhalten von Programmen zu verändern.

Dabei existieren die folgenden Risiken:

- Jede neue Version eines Browsers oder des Betriebssystems, z.B. nach Leistungserweiterungen, kann neue Lücken enthalten.
- Bekannte Lücken werden nicht geschlossen, weil die Anwender aus Mangel an Wissen oder Sicherheitsbewusstsein weiterhin ältere Versionen benutzen.
- Nutzer machen Fehler in der Konfiguration des Browsers oder des Betriebssystems, so dass nicht alle zur Verfügung stehenden Sicherheitsfunktionen optimal genutzt werden.

17.2.2 Abhören von Daten bei der Übertragung

Daten, die ungesichert über das Internet geschickt werden, können ohne großen Aufwand und ohne tieferes Fachwissen abgehört und/oder geändert werden.

17.2.3 »Man In The Middle«-Attacke

Das hier beschriebene Angriffsszenarium zielt auf die Authentifizierung des Servers. Ein Kunde (Client) wählt die Webseite seiner Bank an, wird aber auf die Seiten eines Angreifers umgeleitet, der dem Kunden die Identität der Bank vorspiegelt.

Um für den Namen einer Website die IP-Adresse zu erhalten, werden im Internet sogenannte Domain Name Server (DNS) betrieben. Durch eine gefälschte Eintragung im Verzeichnis eines DNS werden angeforderte HTML-Seiten von anderen Servern abgerufen. Angriffe dieser Art sind bereits bekannt geworden. Es geht aber auch einfacher: Wenn das Betriebssystem eine Konfigurationsdatei vorsieht, in der Web-Adressen die entsprechenden IP-Adressen zugeordnet werden, kann einfach durch einen zusätzlichen Eintrag in diese Datei der Web-Adresse der Bank eine beliebige IP-Adresse zugeordnet werden. Web-Adressen, die in der Konfigurationsdatei aufgeführt sind, werden nicht mehr bei einem Name-Server nachgefragt und ungeprüft zum Aufbau einer TCP/IP-Verbindung verwendet.

Beim Aufruf von durch SSL geschützten Seiten weist der Browser auf das Zertifikat hin und führt nach Bestätigung die Initialisierung und später die Verschlüsselung selbständig durch. Das Zertifikat sieht der Nutzer aber nur auf Anforderung. **Da die meisten Nutzer dieses Zertifikat nicht jedes Mal prüfen, fällt eine Umleitung auf die Website eines Angreifers nicht auf.** Bei der Verwendung von Signed Java Applets tritt dieses Problem nicht auf, weil vom Applet jedes Mal eine Signaturprüfung erzwungen wird.

Mit der Umleitung auf seine Webseiten erfährt der Angreifer die beabsichtigten Transaktionen des Kunden. Der Angreifer kann gleichzeitig eine Verbindung zur Bank aufbauen und die Transaktionen dorthin weiterleiten. Er kann aber die Transaktionen auch beliebig filtern und/oder verändern.

Falls keine starke Authentifizierung des Clients vorgesehen ist (Client-Zertifikate), kann der Angreifer gegenüber der Bank in der Rolle des Kunden auftreten, da er in der Initialisierung die Authentifizierungsmerkmale (z.B. Kennung und Passwort) des Kunden erfährt oder die Authentifizierungsaufforderung des Servers an den Kunden weiterleitet. Denkbar ist auch, dass Applets des Angreifers die Merkmale ausspähen, wenn Sicherheitsfunktionen des Browsers abgeschaltet sind oder nicht in der erforderlichen Stärke implementiert wurden.

Der Einsatz identischer Zertifikate für alle Nutzer erleichtert auch in diesem Szenario einen Angriff. Der Angreifer braucht Schlüssel und Zertifikat nicht unbedingt beim Kunden selbst auszuspähen. Er besitzt sie, weil er selbst Kunde ist oder war, oder sie bei einem anderen Kunden ausgespäht hat bzw. das Zertifikat weitergegeben wurde.

17.2.4 Denial-of-Service-Angriff

Eine Denial-of-Service (DoS)-Attacke ist die gewollte Überlastung eines Netzwerkdienstes oder eines ganzen Netzwerkes durch einen Datenstrom, der zu einer Überlastung oder sogar Ausfall des Dienstes/Netzwerks führt. Normalerweise verursacht ein solcher Angriff keinen direkten Schaden auf dem angegriffenen System. Ein Schaden entsteht durch die Störung der Kommunikation, wenn beispielsweise Kunden über einen längeren Zeitraum hinweg nicht den Online-Zugang zu ihrem Konto oder Depot nutzen können. DoS-Attacken lassen sich zur Zeit kaum wirksam bekämpfen. Auch die Urheber des Angriffs sind nur schwer auszumachen. Ziel von Sicherheitsmaßnahmen muss es daher sein, den Schaden durch eine Kommunikationsstörung so gering wie möglich zu halten.

17.2.5 Angriffe auf das Netz der Bank

Auch wenn die Netzgrenze der Bank durch eine Firewall abgesichert ist, bietet dies keinen vollständigen Schutz des internen Netzes, da verschiedene Schwachstellen existieren.

Produktspezifische Schwachstellen und Fehler

In der Vergangenheit sind immer wieder gravierende Sicherheitsprobleme mit Firewallprodukten verschiedener Hersteller aufgetreten. Hacker tauschen diese Kenntnisse über das Internet meistens schneller aus als die Hersteller mit Lösungen aufwarten können.

Beispielsweise wurden im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sechs der bekanntesten Firewalls (Application-Gateways) auf ihre Performance und Sicherheit untersucht. Das Ergebnis war eine 29-seitige tabellarische Auflistung der gefundenen Schwachstellen.

Nicht nur die Firewalls selbst können Schwachstellen haben. Auch Betriebssysteme, Protokolle, Anwendungsprogramme und Hardwareprogramme sind nie völlig fehlerfrei.

Prinzipielle Schwachstellen

Selbst wenn eine Firewall fehlerfrei programmiert ist, kann sie nicht gegen alle Angriffe schützen. Nicht alle Protokolle und Dienste lassen sich zur Zeit mit einem Application-Gateway sichern. Selbst wenn ein Application-Gateway für ein bestimmtes Protokoll angeboten wird, kann nicht mit Sicherheit ausgeschlossen werden, dass bereits alle Angriffsmethoden bekannt sind. Firewalls schützen auch nicht vor allen Denial-of-Service-Attacken.

Fehler in der Konfiguration/Administration

Die größte Gefahr stellt immer noch der Mensch dar. Die derzeit angebotenen Firewall-Produkte sind derart komplex aufgebaut, dass Administration und Change-Management äußerst schwierige Aufgaben darstellen, bei denen es

sehr leicht zu Fehlern kommen kann, die dann zu Funktionseinbußen führen können. **Nach Untersuchungen von Experten sind über 50% aller Firewalls fehlerhaft konfiguriert.**

Manipulationen durch Insider

Mitarbeiter, die Administratorrechte besitzen oder zumindest Zugriff auf Maschinen und Konsolen haben, könnten ihr Wissen missbrauchen, um Systeme und Konfigurationen bewusst zu manipulieren.

17.2.6 Replay-Attacken

Mit Replay-Attacken ist das Wiedereinspielen von abgehörten oder aufgezeichneten Daten gemeint. Wenn sich ein Hacker Transaktionsdaten eines Geschäftsvorfalls durch Abhören des Client-Rechners oder der Datenübertragung vom Kunden zur Bank beschafft, kann beispielsweise eine Aktienorder mehrfach ausgeführt werden, was einen erheblichen Schaden verursachen kann. Das Wiedereinspielen von Autorisierungsdaten ist ein weiterer denkbarer Angriff.

17.3 Schutzbedarf

Um die Frage zu beantworten, welche Sicherheitsanforderungen ein Online-Banking-System erfüllen muss, sind die folgenden drei Systembereiche zu betrachten:

- Daten und Transaktionen,
- Netzübergänge sowie
- Backend-Systeme (inkl. Firewall) und Clientrechner.

17.3.1 Daten und Transaktionen

Im ersten Schritt ist es sinnvoll, die zu übertragenden Daten nach verschiedenen Datengruppen zu unterscheiden. Denn je nach Datengruppe sind die Anforderungen bezüglich Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit unterschiedlich hoch. Generell lassen sich die Daten wie folgt klassifizieren:

1. Daten für anonyme Benutzer. Dies sind allgemeine Informationsdaten, die die Bank über ihre Homepage jedem Benutzer kostenlos zur Verfügung stellt (z.B. Informationen über die eigenen Produkte und Dienstleistungen, allgemeine Wirtschaftsinformationen).
2. Informationsdaten für geschlossene Benutzergruppen, bei denen man sich also vorher registrieren muss. Dies können z.B. spezielle Wertpapieranalysen sein, die man nur seinen eigenen Kunden zur Verfügung stellen möchte.

3. Kunden- und transaktionsbezogene Daten. Dies sind insbesondere auch alle Vertragsdaten der Kunden (Name, Kontonummer, etc.).

Für die drei Datengruppen ergibt sich aus den Projekterfahrungen der C_sar AG die in der nachfolgenden Tabelle dargestellte Anforderungsbewertung bezüglich Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit der Daten:

Daten-gruppe	Vertraulich-keit	Integrität	Verfüg-barkeit	Verbindlich-keit
1	keine	niedrig – mittel	gering	keine
2	niedrig – mittel	mittel	mittel	mittel
3	hoch	hoch	hoch	hoch

Tab. 17.1: Anforderungs-bewertung der Datengruppen

Daraus lassen sich folgende Anforderungen an die umzusetzenden kryptografischen Schutzmaßnahmen für die einzelnen Datengruppen ableiten:

Datengruppe 1

Eine Verschlüsselung sowie eine Authentisierung ist nicht notwendig. Für die Integritätssicherung werden die Daten signiert übertragen. Die dazu verwendeten Kryptosysteme müssen die Anforderungen der Klasse I (siehe nachfolgende Definition) erfüllen.

Datengruppe 2

Die Transaktions- sowie die Authentisierungsdaten (z.B. Schlüssel oder Passwörter) werden verschlüsselt übertragen. Für die Integritätssicherung gelten die gleichen Anforderungen wie bei der Datengruppe 1. Alle verwendeten Kryptosysteme müssen die Anforderungen der Klasse I (siehe nachfolgende Definition) erfüllen.

Datengruppe 3

Die Transaktionsdaten sind mittels Kryptosystemen der Klasse II (siehe nachfolgende Definition) verschlüsselt zu übertragen. Die Authentisierungsdaten sind über Challenge- und Response-Verfahren zu überprüfen. Für die Integritätssicherung sind die Daten mit starken asymmetrischen Kryptoverfahren (Klasse II) zu signieren. Damit werden auch die hohen Anforderungen zur Gewährleistung der Verbindlichkeit erfüllt.

Kryptosysteme der Klasse I. Die verwendeten Schlüssel müssen durch die Kryptosysteme in einer gesicherten Systemumgebung erzeugt werden können. Darüber hinaus müssen Schlüssel durch kryptografische Verfahren gesichert, gespeichert und transportiert werden. Bei asymmetrischen Kryptosystemen sollte der Einsatz von Zertifikaten zur Schlüsselverteilung von

öffentlichen Schlüsseln unterstützt werden. Das Schlüsselmanagement kann durch den Anwender, den Sicherheits-Administrator oder eine vertrauenswürdige externe Stelle (Zertifizierungsstelle) erfolgen.

In der Klasse I sind auch schwache Kryptoverfahren zugelassen.

Kryptosysteme der Klasse II (starke Kryptoverfahren). Die verwendeten Schlüssel müssen in einer gesicherten Systemumgebung erzeugt werden und besonders gesichert an die jeweiligen Kommunikationspartner gelangen. Dazu müssen Schlüssel mittels starker Kryptoverfahren sicher gespeichert bzw. transportiert werden können.

Bei asymmetrischen oder hybriden Kryptosystemen ist der Einsatz von Zertifikaten zur Schlüsselverteilung von öffentlichen Schlüsseln zu unterstützen. Dabei sollten vertrauenswürdige Zertifizierungsdienste eine Zertifizierung von öffentlichen Schlüsseln übernehmen können, so dass ein gesicherter Austausch dieser Schlüssel gewährleistet ist. Das Schlüsselmanagement und die Zertifizierung von Schlüsseln erfolgt durch vertrauenswürdige interne (Sicherheits-Administration) oder externe Stellen (Zertifizierungsstellen).

Es müssen Mechanismen zur zeitnahen Schlüsselsperrung und Schlüsselvernichtung von symmetrischen und asymmetrischen Schlüsseln definiert sein. Darüber hinaus müssen Funktionen für ein Key-Backup und die Key-Archivierung von geheimen Schlüsseln (symmetrisch) und öffentlichen Schlüsseln (asymmetrisch) unterstützt werden. Für bestimmte Einsatzzwecke (statische Speicherung von chiffrierten Daten) müssen Mechanismen für ein Key-Recovery von Chiffrierschlüsseln bereitstehen. Private Signaturschlüssel dürfen im Falle des Verlustes nicht durch administrative Stellen oder zentrale Zertifizierungsstellen wiederherstellbar sein.

17.3.2 Netzübergänge

Die beim Online-Banking genutzten Dienste und Protokolle sollten aus Sicht der Sicherheitsexperten die folgende Sicherheitsfunktionalität bereitstellen:

Identifikation und Authentisierung der Kommunikationspartner

Die behauptete Identität ist durch ein Frage-Antwort-Verfahren (Challenge & Response) zu Beginn der Kommunikationsbeziehung zu prüfen. Aus abgehörten Authentisierungsdurchläufen dürfen sich keine Rückschlüsse für den nächsten Authentisierungsprozess ziehen lassen.

Datenflusskontrolle

Die Datenflusskontrolle muss auf Anwendungsebene erfolgen. Teilnetze sind durch ein Application Gateway zu trennen. Die Dienstnutzung sollte benutzerbezogen erfolgen.

Beweissicherung

Alle Verbindungen sind mit Datum, Uhrzeit, Benutzer-ID des Initiators, Name des Kommunikationspartners (Rechner, Prozess oder Benutzer) und den Verbindungsparametern zu protokollieren. Die übertragenen Datenmengen sind zu bestimmen und aufzuzeichnen.

17.3.3 Backend-Systeme (inkl. Firewall) und Clientrechner

Sicherung der Firewall

Für den Netzübergang Internet zum internen Netz einer Bank sind die folgenden architektonischen sowie technischen und organisatorischen Anforderungen zu erfüllen:

- Serversysteme, die aus externen Netzen erreicht werden müssen, sind in einer Demilitarized Zone (DMZ) zu installieren. Eine DMZ ist ein abgesichertes (Zwischen-) Netz, das im Allgemeinen zwischen zwei zu trennenden Netzwerken platziert wird, um eine zusätzliche Schutzzone zur Absicherung der Netzkopplung zu erhalten. Innerhalb der DMZ werden dann die sicherheitsrelevanten Systeme platziert, die zur Kommunikation mit externen Netzen benötigt werden. Hierdurch wird ein direkter Zugriff auf das zu schützende Netz verhindert.
- Zur Sicherung der Systeme einer Bank wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Firewall mit einem Paketfilter und einem Application Gateway empfohlen. Einige Experten fordern sogar eine 3-stufige Trenneinrichtung (Paketfilter – Application Gateway – Paketfilter).
- Der Übergang zwischen Serversystemen im lokalen Netz und den Systemen in der DMZ muss gesichert erfolgen.
- Es müssen gut sicherbare Protokolle eingesetzt werden.
- Die Administration der Firewall muss von einem gesicherten Terminal aus erfolgen.
- Alle Eingriffe eines Administrators in die Konfiguration einer Firewall müssen durch das Vier-Augen-Prinzip abgesichert werden.
- Die Firewall muss ständig funktionstüchtig sein und dem neuesten Stand der Technik entsprechen.
- **In der externen DMZ sollten prinzipiell keine Daten aus der Datengruppe 3 im Klartext verarbeitet werden.**
- Alle wesentlichen Komponenten der Internet-Architektur/Firewall sind redundant auszulegen, so dass im Fall eines Ausfalls einer Komponente keine Betriebsstörung für den Kunden spürbar ist.

Allgemeine Architektur-Anforderungen

- Um die Auswirkungen einer Denial of Service-Attacke so gering wie möglich zu halten, müssen alle Dienste so implementiert werden, dass sie zur Not bewusst deaktiviert werden können, ohne dass andere Dienste oder Systeme der Bank davon betroffen werden.
- Wichtige Systeme und Hardwarekomponenten sind redundant auszulegen, so dass bei einem Ausfall die Verfügbarkeit des Online-Zugangs gewahrt bleibt.

Client-Rechner

Der Client-Rechner befindet sich im Einflussbereich des Kunden. Eine Bank hat keine unmittelbare Kontrolle über ihn und kann auf die Administration nur sehr eingeschränkt – in Form von Beratung – Einfluss nehmen. Trotzdem gibt es Anforderungen an die Sicherheit des Client-Rechners, die erfüllt sein müssen, damit eine Bank ihn für die Durchführung von Online-Transaktionen akzeptieren kann.

- Nur solche Kundenrechner dürfen als Kommunikationspartner akzeptiert werden, die über einen Internetbrowser verfügen, der nach dem Stand der Technik als sicher gilt. Bei der Verwendung von SSL kann z.B. geprüft werden, welche Verschlüsselungsfunktionen verwendet werden.
- Wenn für das Online-Banking ein Chipkartenleser einsetzt wird (wie bei HBCI), so sollte dieser unabhängig vom PC arbeiten, um das Risiko, dass die Tastatureingaben auf dem PC abgehört werden, auszuschalten (Klasse-II-Leser). Ein idealer Leser zeigt dem Nutzer alle Daten vor dem Signieren an, so dass ein Virus auf dem PC keine Zugriffsmöglichkeiten auf die Transaktionsdaten mehr hat (Klasse-III- oder Klasse-IV-Leser). Allerdings sind diese Chipkartenleser aus Kostengründen zur Zeit kaum vermarktbar.

17.4 Online-Banking-Verfahren

17.4.1 PIN/TAN-Lösungen

Das am meisten genutzte Verfahren für Online-Banking ist das PIN/TAN-Verfahren. Dabei existieren unterschiedliche Varianten bzw. Lösungen für die Umsetzung einer Authentifikation über PIN/TAN. Beim »klassischen« PIN/TAN-Verfahren wählt der Kunde in seinem Browser die Adresse seiner Bank, woraufhin eine SSL-Verbindung (über Port 443) aufgebaut wird. Die Authentifikation des Kunden erfolgt über die Eingabe von Kontonummer und Geheimzahl (PIN). Jede Transaktion wird mit einer nur einmal benutzbaren Transaktionsnummer (TAN) vom Kunden bestätigt. Die typische Architektur einer solchen PIN/TAN-Lösung ist in der nachfolgenden Abbildung dargestellt:

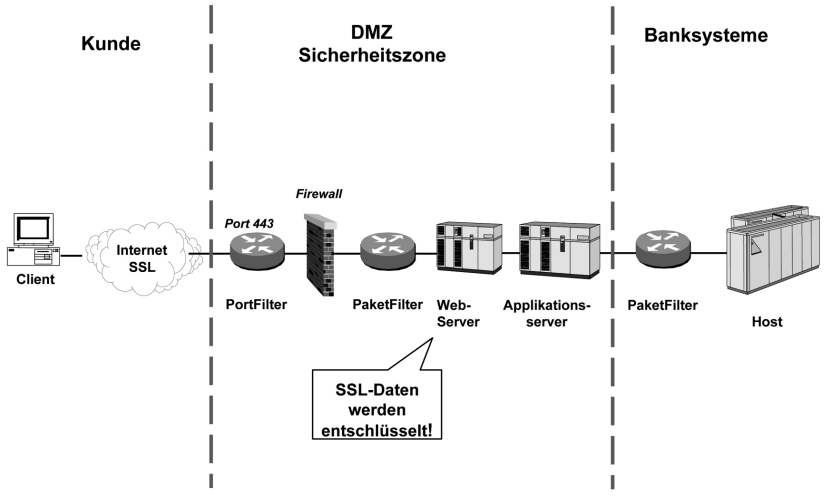


Abbildung 17.1: Architektur einer PIN/TAN-Lösung

Sehr weit verbreitet sind auch Lösungen, die auf herstellerspezifischen Transaktionsservern basieren. Das bekannteste Beispiel dafür ist das Produkt Twister der Firma Brokat. Die Firma selbst existiert zwar inzwischen nicht mehr, das Produkt ist aber immer noch in vielen Online-Banking-Systemen im Einsatz. Darüber hinaus haben die Lösungen von Konkurrenzunternehmen eine vergleichbare Architektur. Der Zugriff erfolgt ebenfalls über den Web-Browser mittels einer SSL-Verbindung. Die Authentifikation des Kunden erfolgt wie beim oben beschriebenen Verfahren (PIN, Kontonummer und TAN). Zusätzlich benutzt der Client aber noch Signed Java Applets, die der Kunde beim Aufruf der entsprechenden Internetseite seiner Bank vom Web-Server erhält. In der nachfolgenden Grafik ist der Aufbau einer Online-Banking-Lösung auf Basis eines Transaktionsservers dargestellt:

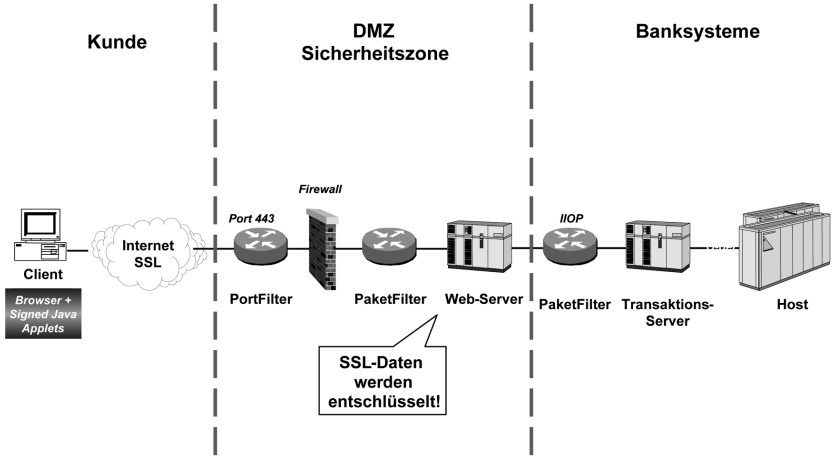


Abbildung 17.2: Online-Banking-Lösung auf Basis eines Transaktionsservers

Sicherheitsbewertung

Beim Vergleich mit den in Abschnitt 17.3 aufgestellten Sicherheitsmaßnahmen, ergeben sich zwei wesentliche Angriffspunkte auf PIN/TAN-Lösungen. Zum einen betrifft dies den Client (vor der Verschlüsselung der Daten) und zum anderen den Web-Server der Bank.

Die meisten publizierten Angriffe auf Online-Kundenzugänge von Banken haben Schwächen der SSL-Architektur beim Client ausgenutzt. Insbesondere hat sich gezeigt, dass der Diebstahl von PINs und TANs vom Kunden-PC kein großes Problem für findige Hacker darstellt. Teilweise wurden die PIN und die TAN-Listen von zu sorglosen Kunden auf der Festplatte des PCs gespeichert. Diese durch eine entsprechende Schadsoftware auszulesen, stellt kein großes Hindernis dar. Aber auch bei einem ordnungsgemäßen Umgang des Kunden mit seiner PIN und den TANs, ist es Angreifern gelungen, diese bei der Eingabe über die PC-Tastatur abzufangen. Der PC wurde durch einen Trojaner dann direkt nach Eingabe der TAN zum Absturz gebracht, so dass der Kunde die geplante Transaktion nicht mehr ausführen konnte. Der Angreifer war damit im Besitz der PIN und einer noch nicht »verbrauchten« TAN, so dass er eine Transaktion mit der Identität des Kunden durchführen konnte.

Die zweite große Schwachstelle von PIN/TAN-basiertem Online-Banking, die aber bisher bei den Sicherheitsverantwortlichen wenig Berücksichtigung gefunden hat, besteht dann, wenn die mit SSL verschlüsselten Daten in der DMZ entschlüsselt werden, um die Autorisierungsinformationen zu prüfen – **was in der Regel der Fall ist!** Nach der Entschlüsselung liegen alle Daten im Klartext vor, so dass ein Angreifer, der die Firewall überwinden konnte, vollen Zugriff auf vertrauliche Daten (Daten der Gruppe 3) erhalten kann. Dabei macht es aus sicherheitstechnischer Sicht keinen Unterschied, ob diese Daten auf dem Web-Server gespeichert oder nur von diesem weitergeleitet werden. Auch Daten, die weitergeleitet werden, können von einem Angreifer, der Zugang zum Web-Server hat, selbst mitgeschnitten und über das Internet an ihn geschickt werden. Das Führen von Log-Dateien mit Zugangsdaten der Kunden auf dem Web-Server ist in diesem Zusammenhang ein besonders schwerwiegendes Sicherheitsrisiko.

Bei der HypoVereinsbank ist genau dieser Angriff erfolgreich durchgeführt worden, indem ein Fehler auf dem Microsoft Web-Server von Hackern ausgenutzt wurde. Das Führen einer Log-Datei mit Zugangsdaten der Kunden auf dem Web-Server hat es den Hackern besonders leicht gemacht, mit dem Diebstahl nur einer einzigen Datei 1,5 Millionen Kontoverbindungen zu erhalten.

Die Entschlüsselung der mit SSL übertragenen Daten stellt daher ein prinzipielles Sicherheitsproblem dar. Dabei sind beide oben dargestellten Architekturen in dieser Hinsicht sicherheitstechnisch gleich zu bewerten.

17.4.2 Homebanking Computer Interface (HBCI)

Der HBCI-Standard beschreibt eine flexible und gesicherte Kommunikation zwischen zwei Systemen. Der Standard wurde so entwickelt, dass die Kommunikation beliebiger (auch nicht-bankfachlicher) Anwendungen mit HBCI abgesichert werden kann. HBCI verwendet das Kommunikationsprotokoll TCP mit fest zugeordneten Portadressen (für HBCI ist Port 3000 registriert). Als Kryptoverfahren für die elektronische Signatur und die Datenverschlüsselung sind symmetrische (Triple DES, 128 bit) und asymmetrische Verfahren (RSA) spezifiziert, die bezüglich elektronischer Signatur alternativ eingesetzt werden können.

Auf der Kundenseite wird eine spezielle HBCI-Client-Software für den Zugriff auf den HBCI-Server benötigt. Dies kann entweder eine Software zur Installation auf dem Kunden-PC sein (Offline-Client) oder dem Kunden wird bei jedem Aufruf über den Web-Browser die notwendige Software mittels Signed Java Applets geladen (Online-Client).

Als Sicherheitsmedium wird eine Chipkarte eingesetzt, auf der die kryptografischen Schlüssel gespeichert sind. Wird für die elektronische Signatur das asymmetrische Kryptoverfahren eingesetzt, ist auch die Verwendung einer Diskette als Sicherheitsmedium möglich. Die meisten Banken geben aber aus Sicherheitsgründen eine Chipkarte aus. Die Authentifikation des Kunden gegenüber der Chipkarte erfolgt über eine PIN.

Nachfolgend ist der Aufbau einer HBCI-Architektur dargestellt, bei der der HBCI-Server auf dem Hostrechner des Banksystems integriert ist. Wenn der HBCI-Server ein Unix-System ist, kann er auch als Application-Server in der DMZ stehen. Die hier dargestellte Architektur ist aber die bei den Banken üblichste Realisierung.

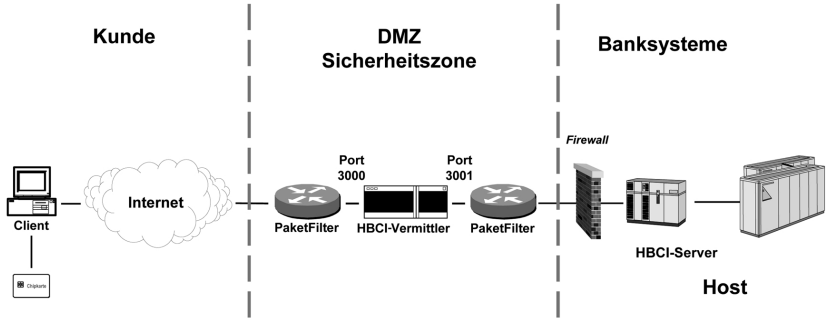


Abbildung 17.3: Aufbau einer HBCI-Architektur

Sicherheitsbewertung

Auch bei HBCI besteht die Gefahr, bei Verwendung von Klasse-I-Lesern (einfache Chipkartenleser ohne Tastatur und Display), dass die Tastatureingaben auf dem PC durch das Einbringen einer Schadsoftware sehr leicht

abgehört werden können. Dies wurde in der Vergangenheit von Hackern bereits zum Abhören der PIN ausgenutzt. Der Chaos Computer Club hat einen solchen Angriff demonstriert.

Allerdings kann ein Angreifer mit der HBCI-PIN alleine nichts anfangen. **Er muss zusätzlich noch in den physischen Besitz der HBCI-Chipkarte kommen!** Dies wird in der Regel in Pressemeldungen über einen erfolgreichen Angriff auf die HBCI-PIN nicht erwähnt. Auch ist die in diesem Zusammenhang oft getroffene Aussage, dass das HBCI-Verfahren »geknackt« sei, falsch! Der oben beschriebene Angriff ist nur ein Angriff auf den Client, nicht auf das HBCI-Verfahren selbst. Mit dem Angriff wird also lediglich demonstriert, dass ein Client-Rechner unsicher ist, was aber keine neue Erkenntnis darstellt.

Zur Abwehr des oben beschriebenen Sicherheitsrisikos kann man Klasse-II-Leser (Chipkartenleser mit integrierter Tastatur, die unabhängig vom PC arbeiten) einsetzen. Einige Banken geben bereits solche Lesegeräte aus, insbesondere im höherwertigen Firmenkundensegement. Klasse-II-Leser sind jedoch deutlich teurer als einfache Chipkartenleser.

Ein weiteres – wenn auch kleines – Risiko, besteht darin, dass ein Schadprogramm gefälschte Daten vom PC an den Chipkartenleser zum Signieren überträgt. Ein derartiger Angriff müsste jedoch auf den lokal installierten Treiber für die Chipkartenleser (z.B. CTAPI oder PC/SC) erfolgen und ist nur schwer durchzuführen, weil Spezialwissen über die Schnittstelle zum Leser erforderlich ist und die Transaktionsdaten, die an den Kartenleser übertragen werden, durch einen Hashwert gesichert sind. Ein solcher Angriff könnte nur durch einen idealen Chipkartenleser, der unabhängig vom PC alle Transaktionsdaten im Klartext vor dem Signieren auf dem Display des Lesers anzeigt, abgewehrt werden. Zur Zeit gibt es aber kein Produkt, das diese Ansprüche erfüllt. Auch sind die Kosten für einen solchen Chipkartenleser immer noch so hoch, dass er zur Zeit nicht vermarktbar ist.

Beim Vergleich der beiden alternativen Client-Software-Arten (Online- und Offline-Client) ist festzuhalten, dass der Online-Client, der Signed Java Applets verwendet, sicherer ist als der Einsatz einer festinstallierten Software (Offline-Client: z.B. StarMoney, WISO Mein Geld) auf dem Kundenrechner. Jede dieser Software benutzt einen HBCI-Kernel, dessen Spezifikationen öffentlich zugänglich sind. Die HBCI-Schnittstelle (API/Kernel) ist in Windows-Systemen in Form einer Dynamic Link Library (DLL) eingebunden. Diese Datei kann von einem Angreifer, der sich Zugang zum PC des Kunden verschafft hat, leicht ersetzt oder manipuliert werden. Transaktionsdaten könnten vor der Berechnung des Hashwertes von einen Angreifer verändert werden. Bei der Verwendung von Java Applets befinden sich dagegen keine Dateien auf dem Kundenrechner, auf die ein Angreifer zugreifen könnte. Des Weiteren sind Java Applets, die auf der aktuellen Java-Version beruhen, noch nie nachweisbar von einem Schadprogramm verändert worden.

Aus Sicht der Backend-Systeme ist die oben dargestellte HBCI-Architektur wesentlich sicherer als die PIN/TAN-Lösungen, da die Transaktionsdaten erst im Host entschlüsselt werden. Der HBCI-Vermittler kontrolliert und prüft die formale Syntax des HBCI-Datenstroms (soweit möglich) ohne die Nachricht zu entschlüsseln. Ein Angreifer müsste also nicht nur eine, sondern mehrere Firewalls gleichzeitig überwinden, um an vertrauliche Daten zu gelangen. Es ist jedoch sehr wahrscheinlich, dass ein Intrusion Detection System das Eindringen in der ersten Firewall bemerkt, bevor die letzte Barriere überwunden ist. Damit kann der Angriff dann abgewehrt werden, bevor ein Schaden entsteht.

17.5 Fazit

Die meisten in der Vergangenheit publizierten Angriffe auf Online-Banking-Verfahren betrafen den Client-Rechner, in dem die PINs und TANs ausgespäht wurden. Dabei lag der Fokus auf den PIN/TAN-Verfahren. Dies liegt daran, dass diese wesentlich verbreiteter als HBCI und auch leichter angreifbar sind. Die Angriffe haben in der Praxis jedoch den Bankkunden keine nennenswerten finanziellen Schäden zugefügt. Denn auch wenn ein Angreifer in den Besitz der PIN und einer gültigen TAN kommt und damit im Namen des Bankkunden Transaktionen durchführen kann, dürfte es ihm sehr schwer fallen, sich dadurch einen finanziellen Vorteil zu verschaffen. Würde er Geld des Bankkunden auf sein eigenes oder ein für ihn verfügbares Bankkonto überweisen, verliert er seine Anonymität. Durch die internationale Verflechtung der Banksysteme sind elektronische Transaktionen leicht verfolgbar und auch stornierbar.

Die Motivation der Angriffe liegt also nicht in der persönlichen Bereicherung – wie bei Betrügereien mit der ec-Karte, wo der Angreifer anonym bleiben kann – sondern eher in medienwirksamen Gründen.

Das bedeutet aber, dass man mit den Sicherheitsrisiken des Client-Rechners aus ökonomischer Sicht der Bank durch die Implementierung eines vernünftigen Risikomanagements durchaus »leben« kann. Den Client-Rechner selbst wird man nicht mit einem vertretbaren Kosten-Nutzen-Aufwand ausreichend absichern können.

Das viel größere Sicherheitsrisiko – auch wenn viele Bankvorstände dies nicht so richtig wahrhaben wollen – liegt in den Banksystemen beim Einsatz der beschriebenen PIN/TAN-Lösungen, die aus Kosten- und Bequemlichkeitsargumenten oft gegenüber dem sichereren HBCI-System bevorzugt werden. Dass ein Web-Server trotz Firewall erfolgreich ausspioniert werden kann, hat das Beispiel HypoVereinsbank gezeigt und ein grundlegendes Problem illustriert: Eine perfekte Firewall kann und wird es nicht geben. Firewalls sind überaus kompliziert zu administrieren, fehleranfällig und einige Dienste und Protokolle lassen sich prinzipiell nur mangelhaft sichern.

Der Imageschaden und die damit verbundenen finanziellen Einbußen, die durch ein »gehacktes« Banksystem entstehen, können immense Auswirkungen für ein Kreditinstitut haben.

Es bleibt also die geschäftspolitische Entscheidung, ob man »mit der Masse leichter sterben« oder etwas mehr in Sicherheit investieren will, auch wenn man damit grundsätzlich keine 100%ige Sicherheit erzielen kann.

18 Bürgerfreundliches E-Government. Das Projekt OSCI-XMeld

Frank Steimke

18.1 Übersicht

Das novellierte Melderechtsrahmengesetz bietet weitreichende Möglichkeiten, wichtige Geschäftsvorfälle zukünftig schneller, bürgerfreundlicher und kostengünstiger umzusetzen. Um dieses optimal nutzen zu können, sind in der 1. Bundesmeldedaten-Übermittlungsverordung (1. BMeldDÜV) Vorgaben für ein einheitliches Nachrichtenformat sowie für die Technik der Datenübermittlung erforderlich. Die bereits jetzt vorhandene Möglichkeit der bilateralen Einigung ist nicht ausreichend, ohne verbindliche Vorgaben für diese beiden Fragestellungen wird man die erhofften Ziele nicht erreichen können.

Die OSCI-Leitstelle erarbeitet im Auftrag der öffentlichen Verwaltung Lösungen für solche Fragestellungen. Sie kann für beide oben genannten Aufgaben fertige Antworten anbieten: für die Technik der Datenübermittlung das Transportprotokoll OSCI-Transport, für das einheitliche Nachrichtenformat die Ergebnisse des Projektes OSCI-XMeld. Da beide Projektergebnisse im Auftrag der öffentlichen Verwaltung erstellt worden sind, stehen sie zur unentgeltlichen Nutzung zur Verfügung.

Die Ergebnisse wurden durch Fachleute erarbeitet, durch einen anderen Personenkreis qualitätsgesichert, und durch den Auftraggeber KoopA-ADV abgenommen. Sie sind vollständig und umfangreich dokumentiert.

Dieses Papier beschreibt unsere Projektergebnisse in einer nicht-technischen Form. In dem Abschnitt *Handlungsbedarf durch das novellierte Melderechtsrahmengesetz* wird erklärt, weshalb es trotz eines (bundeseinheitlichen) Datensatzes für das Meldewesen *(DSMeld)* überhaupt Handlungsbedarf gibt. Der Abschnitt *Festlegung von Standards für die öffentliche Verwaltung* stellt die Aufgabe der OSCI-Leitstelle dar, unter deren Leitung die Ergebnisse erarbeitet wurden.

Im Abschnitt *Das Projekt OSCI-Xmeld 1.0* wird an drei kleinen Beispielen dargestellt, welche Ergebnisse in diesem Projekt erarbeitet wurden, und in welcher Form diese dokumentiert sind.

Für die Technik der Datenübermittlung schlagen wir das MEDIA@Komm Projektergebnis OSCI-Transport vor. Im Abschnitt *OSCI-Transport für die sichere Nachrichtenübermittlung* wird dieses Protokoll kurz dargestellt.

18.1.1 Handlungsbedarf durch das novellierte Melderechtsrahmengesetz

Durch die Novellierung des Melderechtsrahmengesetz sind die gesetzlichen Grundlagen geschaffen worden, um Geschäftsvorfälle des Meldewesens zukünftig effizienter, schneller und bürgerfreundlicher gestalten zu können. Neben qualitativen Verbesserungen erwartet man sich dadurch auch erhebliche Kostensenkungen, insbesondere bei den Personalkosten in den Meldeämtern.

Dem automatisierten und schnellen Rückmeldeverfahren kommt dabei eine Schlüsselrolle zu. Folgerichtig ist eine Novellierung der 1. BMeldDÜV im Jahr 2003 geplant.

Gleichzeitig planen schon jetzt viele Betreiber von EWO-Verfahren eine Verbesserung ihres Dienstleitstungsangebotes auf Basis des novellierten Melderechtsrahmengesetzes. Wegen des hohen wirtschaftlichen Potenzials werden die einfache Melderegisterauskunft nach §21 Abs. 1a sowie die Datenübermittlung an andere Behörden nach §18 Abs. 4 häufig als erstes realisiert.

18.1.2 Auswirkungen auf Meldeämter

Für die DV-Verfahren in den Meldeämtern sind erhebliche Auswirkungen offensichtlich. Während bisher die Rückmeldungen per Briefpost vorgenommen werden, erzwingt das novellierte Melderechtsrahmengesetz die länderübergreifende Vernetzung der Meldeverfahren. Bei der hohen Zahl von Meldeämtern, dem großen Kommunikationsvolumen, und schließlich der inhomogenen DV-Ausstattung in den Kommunen ist diese Vernetzung eine große Herausforderung.

Den geplanten Einsparungen in den Meldeämtern steht ein Investitionsbedarf in bisher unbekannter Höhe für DV-Verfahren gegenüber. Das Interesse des Bundes, der Länder und der Kommunen muss es sein, gemeinsam ein optimales Kosten-/Nutzenverhältnis zu ermitteln und die technische Umsetzung der Vernetzung an diesem Ziel auszurichten.

Dabei sind unterschiedliche Voraussetzungen in verschiedenen Kommunen zu berücksichtigen. In großen Datenverarbeitungszentralen wird man andere Anforderungen an Verfügbarkeit und Leistungsfähigkeit erfüllen können, als in kleinen Meldebehörden.

18.1.3 Verbindliche Festlegungen sind erforderlich

Für einen reibungslosen Datenaustausch zwischen Meldebehörden und ihren Kunden (bzw. den anderen Meldebehörden) sind verbindliche Festlegungen bezüglich der zu übermittelnden Daten und der technischen Infrastruktur unerlässlich. Die Hersteller der Einwohner-Meldewesen (EWO)-Verfahren benötigen klare Vorgaben, unter welchen Umständen sie welche Daten in welcher Form an den Empfänger zu senden haben.

18.1.4 Der DSMeld reicht nicht aus

Dieser Klärungsbedarf besteht, obwohl mit dem DSMeld ein bundeseinheitlicher Datensatz existiert. Doch der DSMeld ist hauptsächlich für die Zwecke der *Erfassung* und *Speicherung* nützlich, also für die Anwendung *in* den Meldeämtern. Für die Übermittlung *zwischen* Meldeämtern und anderen benötigt man weitergehende Festlegungen.

Welcher Regelungsbedarf über den DSMeld hinaus noch besteht, zeigt ein Vergleich mit der 2. BMeldDÜV, in der die automatisierte Datenübermittlung an öffentliche Stellen (Kreiswehrersatzämter, Bundesanstalt für Arbeit etc.) beschrieben wird.

18.1.5 Festlegung der Nachrichtenformate

Es bedarf verbindlicher Vorgaben, wie die zu übertragenen Daten zu formatieren und darzustellen sind. Wie kennzeichnet man Beginn und Ende von Datenfeldern? Wie werden Wiederholungen dargestellt? Wie differenziert man zwischen Pflichtfeldern und optionalen Feldern? Wo stehen Angaben über *Absender* und *Empfänger* der Nachricht?

In der 2. BMeldDÜV wird pro Empfänger das Datenformat exakt und verbindlich in den Anlagen zu §6 (2) festgeschrieben. In der 1. BMeldDÜV fehlen solche Festlegungen.

Darüber hinaus ist auch der Datenumfang festzulegen. Unter welchen Umständen müssen (und dürfen) welche Daten an wen übermittelt werden? In der 2. BMeldDÜV ist dies pro Empfänger exakt und abschließend festgelegt. In der 1. BMeldDÜV ist dies ebenfalls für die Rückmeldung erfolgt (in §2 und §3). Diese verbindliche Festlegung fehlt jedoch im Falle der Fortschreibung des Melderegisters nach §4, denn es gibt *diverse Anlässe*, das Melderegister fortzuschreiben (zum Beispiel: *Wegzug aus einer Gemeinde, Aufhebung einer bestehenden Lebenspartnerschaft, Änderung des Geburtsnamens auf Grund einer Adoption* und so weiter). Aus Gründen des Datenschutzes dürfen nur solche Daten übermittelt werden, die für die Erfüllung der Aufgabe unterlässlich sind. Es gibt in der 1. BMeldDÜV oder anderen Verordnungen jedoch keine abschließende Aufzählung der Datenfelder pro Anlass.

18.1.6 Technik der Nachrichtenübermittlung

Das technische Übertragungsprotokoll muss den Kommunikationspartnern vorgegeben werden. In dem sensiblen Bereich der Meldedaten haben Fragen des Datenschutzes und der Datensicherheit eine besonders hohe Bedeutung. Darüber hinaus muss es möglich sein, den Nachrichtenversand mit Sende- und Empfangszeitpunkten sicher nachvollziehen zu können, um gegebenenfalls den Nachweis der Fristwahrung führen zu können.

Das Melderechtsrahmengesetz erzwingt bei vielen Geschäftsvorfällen, die Privatkunden betreffen, den Einsatz der qualifizierten elektronischen Signa-

tur. Für die Übertragung zwischen Meldebehörden ist dies nicht der Fall, dort wird die fortgeschrittene Signatur lediglich nahegelegt (in der Begründung zu §17).

In der 2. BMeldDÜV werden ab §7 verschiedene Verfahren der Datenübermittlung mittels automatisierter Verfahren beschrieben, inklusive der Vorkehrungen zur Sicherung der Integrität, Authentizität und Vertraulichkeit.

In der 1. BMeldDÜV wird von der schriftlichen Form der Datenübermittlung ausgegangen. Eine automatisierte Datenübermittlung setzt voraus, dass sich Sender und Empfänger jeweils bilateral bezüglich der Modalitäten geeinigt haben. Vorgaben des Gesetzgebers fehlen. Genau das ist der Grund für hohe Personalkosten in den Meldeämtern, die bei der manuellen Bearbeitung schriftlich übermittelter Rückmeldungen anfallen.

In der Tabelle 18.1 werden die Regelungen der 2. BMeldDÜV dem aktuellen Stand und unserem Vorschlage bezüglich der 1. BMeldDÜV gegenübergestellt.

Tab. 18.1: Vergleich mit der 2. BMeldDÜV

Regelungsbedarf	2. BMeldDÜV	1. BMeldDÜV	
		aktuell	zukünftig
Technik der Datenübermittlung	§7 ff	In der Regel Briefpost, bilaterale Einigung ist möglich	OSCI-Transport
Nachrichtenformat	Spezifisch pro Empfänger in den Anlagen zu §6	Ohne Vorgabe	OSCI-XMeld

18.1.7 Festlegung von *Standards*, nicht Produkten

Die verbindliche Vorgabe für die oben angesprochenen Fragestellungen darf nicht auf der Ebene von zu nutzenden Produkten stattfinden. Dadurch würde sich automatisch eine Herstellerabhängigkeit ergeben, dies kann nicht im Interesse der öffentlichen Verwaltung sein. Vielmehr sind Standards festzuschreiben, die von allen potenziellen Kommunikationspartnern zu erfüllen sind. Mit welchen Produkten sie dies tun, ist unerheblich.

In der 2. BMeldDÜV werden beispielsweise in den Anlagen zum §6 nur die Datenformate beschrieben. Es werden keine Produkte für deren Verarbeitung vorgeschrieben. Die Hersteller von EWO-Verfahren werden lediglich beauftragt, Daten in diesen Formaten zu verarbeiten.

18.1.8 Es müssen *beide* Fragen verbindlich geregelt werden

Um eine Infrastruktur für den Datenaustausch zwischen Meldebehörden zu etablieren, ist es zwingend erforderlich, dass *beide* oben genannten Fragestellungen für die Kommunikationsbeteiligten verbindlich vereinbart werden.

Eine einvernehmliche Festlegung auf ein Nachrichtenformat nützt überhaupt nichts, wenn die Übermittlung der Nachrichten zwischen den Meldebehörden auf Grund nicht kompatibler Übermittlungsverfahren oder unterschiedlicher Sicherheitssoftware scheitert.

Ebensowenig hilfreich wäre eine Einigung auf eine einheitliche Technik der Datenübermittlung inklusive elektronischer Signaturen und Quittungsmechanismen, wenn der Nachrichteninhalt vom Empfänger nicht verstanden oder nicht automatisiert verarbeitet werden kann.

Wenn es nicht gelingt, auf *beiden* Ebenen zu praktikablen Lösungen zu kommen, wird man das Ziel der Kostenreduktion durch die automatisierte Übermittlung von Rückmeldungen nicht erreichen.

18.1.9 Regelungsbereich: der *länderübergreifende* Datenaustausch

Da die Realisierung der Rückmeldung mittels automatisierter Datenübermittlung ein hohes wirtschaftliches Potenzial bietet, sind in einzelnen Bundesländern bereits Lösungsansätze entstanden. Diese sind untereinander nicht kompatibel, außerdem in der Regel integraler Bestandteile bestimmter EWO-Produkte.

Die 1. BMeldDÜV regelt nur den Datenaustausch »zwischen Meldebehörden verschiedener Länder«. Daher lässt eine Vorgabe der zu nutzenden Technik solche, bereits in den Ländern existierenden Lösungen, unberührt. Innerhalb der Bundesländer wäre eine Übernahme technischer Vorgaben aus der 1. BMeldDÜV ebenso möglich, wie die Weiterentwicklung bestehender Techniken. Es könnten *Clearingstellen* eingerichtet werden, welche für die Umsetzung eines landesspezifischen Datenformats in die von der 1. BMeldDÜV vorgeschriebenen Formate zuständig sind. In Abb. 18.1 sind mögliche Realisierungsformen mit und ohne Clearingstelle dargestellt.

18.1.10 Für beide Fragestellungen gibt es fertige Lösungen

Die OSCI-Leitstelle koordiniert im Auftrag der öffentlichen Verwaltung die Entwicklung von Standards für den Bereich des E-Government. Nach der Novellierung des Melderechtsrahmengesetzes ist das Meldewesen der erste große Bereich, in dem E-Government flächendeckend eingeführt werden kann. Die OSCI-Leitstelle kann fertige Lösungen für beide Bereiche anbieten:

- Für die *Festlegung der Nachrichtenformate* die Ergebnisse des Projektes OSCI-XMeld 1.0.

  In der 1. BMeldDÜV sollte – analog zu den Anlagen des §6 der 2. BMeldDÜV – auf die XML-Schema-Dateien verwiesen werden, die als Projektergebnis entstanden sind. In diesen werden die Nachrichtenformate für die verschiedenen Geschäftsvorfälle des Meldewesens exakt und eindeutig definiert.

  XML hat sich als eine Beschreibungssprache für Datenaustauschformate inzwischen weltweit durchgesetzt. Da XML für die automatisierte Verarbeitung optimiert, aber für Menschen schwer lesbar ist, hat die OSCI-XMeld Projektgruppe zusätzlich eine umfangreiche Dokumentation erstellt.

- Für die *Technik der Nachrichtenübermittlung* das Protokoll OSCI-Transport.

  OSCI-Transport wurde speziell für die sichere und nachvollziehbare Abwicklung von Geschäftsvorfällen des E-Government entwickelt. Über elektronische Signaturen und Verschlüsselungsmechanismen hinaus bietet OSCI-Transport auch Quittungen und Zeitstempel, um den Nachweis der Fristwahrung führen zu können.

  Die Eignung von OSCI-Transport für das E-Government aus sicherheitstechnischer Sicht ist durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt worden. OSCI-Transport ist ein *empfohlener Standard* in der (*SAGA)*-Architektur des Bundes (SAGA: Standards und Architekturen für E-Government-Anwendungen).

  Daher sollte die 1. BMeldDÜV – analog zu den §§7 ff. der 2. BMeldDÜV – das Protokoll OSCI-Transport zur verbindlichen Vorgabe für die Technik der Datenübermittlung zwischen Meldebehörden verschiedener Bundesländern machen.

18.1.11 Übernahme von Lösungen ohne Produktabhängigkeit

In beiden Fällen handelt es sich um Standards, *nicht um Produkte*, die im Auftrag der öffentlichen Verwaltung entwickelt wurden. Die Ergebnisse wurden jeweils durch Fachleute (des Meldewesens bzw. der Sicherheitstechnik) erarbeitet. Sie stehen der öffentlichen Verwaltung unentgeltlich zur Verfügung. Der KoopA-ADV hat die Ergebnisse abgenommen und ihre Verwendung in E-Government-Projekten empfohlen (Beschlüsse 1-12-09 und 1-12-10 des KoopA-ADV).

Die Aufgaben der OSCI-Leitstelle, unter deren Leitung beide Ergebnisse erarbeitet wurden, sowie die Ergebnisse OSCI-XMeld sowie OSCI-Transport werden auf den folgenden Seiten genauer beschrieben.

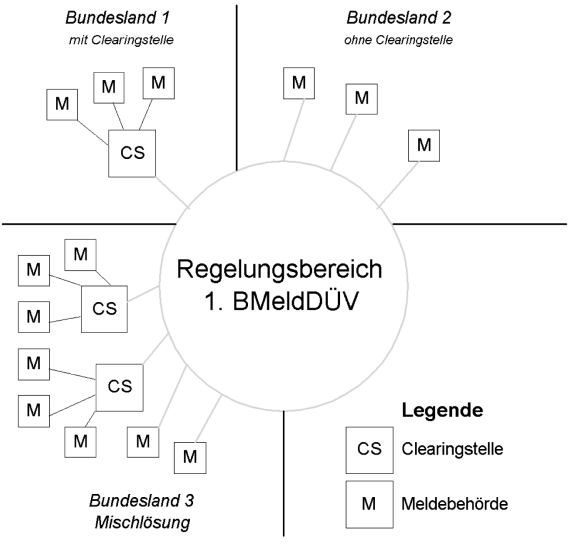


Abbildung 18.1: Realisierungsvarianten in den Bundesländern

18.1.12 Festlegung von Standards für die öffentliche Verwaltung

Der Bedarf an einer stärkeren Vernetzung von Organisationseinheiten der öffentlichen Verwaltung mit dem Ziel, Geschäftsprozesse schneller, effizienter, kostengünstiger und bürgerfreundlicher zu gestalten, ist nicht auf das Meldewesen beschränkt. Das Internet hat im Bereich des *E-Business* bereits zu einer drastischen Veränderung geführt. Lange Zeit konnte dies in der öffentlichen Verwaltung nicht nachvollzogen werden, weil hier besondere Anforderungen an die Sicherheit und die Nachvollziehbarkeit der Kommunikation gestellt werden.

Erst mit der Verfügbarkeit neuester Sicherheitstechniken, insbesondere der elektronischen Signatur, können besonders sensible Geschäftsprozesse der öffentlichen Verwaltung umgesetzt werden. Seitdem diese Techniken zur Verfügung stehen, werden Projekte initiiert, um die Vernetzung in der Praxis nutzbringend anzuwenden. An vielen Stellen finden Pilotprojekte statt.

18.1.13 Die Aufgabe der OSCI-Leitstelle

Im Rahmen des Bundesprojektes MEDIA@Komm finanziert die Bundesregierung anteilig die OSCI-Leitstelle. Deren Aufgabe ist es, für die öffentliche Verwaltung Standards in den Bereichen der sicheren Datenübermittlung sowie der Datenformate und -repräsentation zu entwickeln. Die Leitstelle befindet sich in Bremen und ist derzeit mit zwei Personen besetzt.

18.1.14 Auftraggeber: KoopA-ADV

Die Leitstelle ist nicht kommerziell orientiert. Der Auftraggeber für die Standardisierungsprojekte ist der KoopA-ADV, denn in der Regel sind von E-Government-Projekten Bund, Land und der kommunale Bereich betroffen. Die genaue Beschreibung der Aufgaben der OSCI-Leitstelle und ihrer Vorgehensweise sind in einem Organisationskonzept festgelegt, welches gemeinsam mit dem Bundesministerium für Wirtschaft und Technologie (BMWi), dem Bundesministerium des Innern (BMI), den MEDIA@Komm-Städten, dem Deutschen Städtetag und weiteren Beteiligten entwickelt wurde.

18.1.15 Sicherheit und Datenformate müssen gemeinsam betrachtet werden

Bei der Umstellung der Geschäftsprozesse auf einen neuen *Vertriebskanal Internet* kann die Frage der Sicherheit nicht separat betrachtet werden. Am Beispiel des Meldewesens wird deutlich, dass die Vorgaben des Gesetzgebers die Nachrichteninhalte ebenso bestimmen wie die Sicherheitsmechanismen.

Prozesse müssen so modelliert werden, dass die *richtigen Inhalte* den Empfänger *sicher* erreichen. Ob rechtsverbindliche Zeitstempel und Quittungen benötigt werden, ergibt sich aus den Rechtsnormen.

Aus diesem Grunde ist es Auftrag der OSCI-Leitstelle, sich sowohl um die Inhalte, als auch um die Technik der Datenübermittlung zu kümmern.

18.1.16 Ergebnisse sind unentgeltlich

Die von der OSCI-Leitstelle erarbeiteten Ergebnisse werden im Auftrag der öffentlichen Verwaltung erarbeitet. Sie sollen dort möglichst breitflächig eingesetzt werden. Sie stehen der öffentlichen Verwaltung unentgeltlich zur Verfügung.

Dies gilt selbstverständlich auch für OSCI-XMeld 1.0 und OSCI-Transport.

18.1.17 Die OSCI-Leitstelle vertreibt keine Produkte

Die Aufgabe der OSCI-Leitstelle endet dort, wo für die Verwaltung und gegebenenfalls gemeinsam mit Software-Herstellern Spezifikationen für Standards erarbeitet worden sind. Bevor diese Ergebnisse konkret genutzt werden können, müssen sie in Produkten implementiert werden.

Die Erstellung und der Vertrieb von Produkten, die Spezifikationen in Technik umsetzen, ist nicht mehr die Aufgabe der Leitstelle. Hier kann es ganz unterschiedliche Situationen geben. Kommerzielle Firmen können die frei verfügbaren Spezifikationen ebenso implementieren und anschließend auf dem Markt anbieten, wie dies für Kommunal- oder Landesrechenzentren möglich ist.

Die technische Umsetzung der Ergebnisse von OSCI-XMeld kann beispielsweise durch die Anpassung bestehender Schnittstellen, oder auch durch den Zukauf von Standardkomponenten erfolgen. Welche dieser Alternativen kostengünstiger ist, muss im Einzellfall durch den jeweiligen Auftraggeber entschieden werden.

Aus Sicht der Verwaltung ist es sicher wünschenswert, wenn es mehrere Produkte gibt, welche die Standards der öffentlichen Verwaltung erfüllen. Die Wettbewerbssituation führt in der Regel zu geringeren Kosten und eröffnet Wahlmöglichkeiten.

18.1.18 Die Ergebnisse sind hersteller- und produktneutral

Die Erarbeitung unserer Ergebnisse erfolgt gemeinsam mit Fachleuten der Verwaltung aus unterschiedlichen Bundesländern. In der Regel werden fachlich versierte Mitarbeiter von DV-Herstellern und aus Landes- oder Kommunalrechenzentren ebenfalls im Projekt beteiligt. Dies war sowohl bei OSCI-XMeld, als auch bei OSCI-Transport der Fall. Dadurch wird sichergestellt, dass es keine versteckten Produkt- oder Herstellerabhängigkeiten in den jeweiligen Projektergebnissen gibt.

Für die erste Version von OSCI-Transport wurde zu Recht der Vorwurf erhoben, dass es Abhängigkeiten von Produkten der Firma *bremen online services* gäbe. In der aktuellen Version 1.2 von OSCI-Transport wurde die Produktneutralität durch ein QS-Gremium bestätigt, zu dem unter anderem die drei MEDIA@Komm-Städte, die Anstalt für kommunale Datenverarbeitung (AKDB) und die Firma SAP gehören.

18.2 Das Projekt OSCI-XMeld 1.0

18.2.1 Pilotprojekt *Online-Ummeldung* in Bremen

Die Stadt Bremen hat im Rahmen des MEDIA@Komm Projektes die *Online Ummeldung* umgesetzt (also Umzug *innerhalb der Gemeinde*). Vor dem Hintergrund der anstehenden Novellierung des Melderechtsrahmengesetzes hat die OSCI-Leitstelle im Frühjahr 2001 mit den Planungen für ein bundesweites Projekt begonnen, in denen die in diesem Pilotprojekt gemachten Erfahrungen zu einem bundesweit abgestimmten Datenaustauschformat führen sollten.

Die Projektorganisation

In dem Projekt wurden drei Gremien eingerichtet:

Die Arbeitsgruppe. In der *Arbeitsgruppe* haben Fachleute aus Meldeämtern und kommunalen Rechenzentren, Datenzentralen sowie Hersteller kommunaler Software gemeinsam die Fachinhalte erarbeitet.

Die Abstimminstanz. Vorliegende Ergebnisse wurde in einer *Abstimminstanz* qualitätsgesichert. Dieses Gremium war besetzt durch Meldereferenten, den Bundesbeauftragten für den Datenschutz, einen Vertreter des Deutschen Städtetages sowie die drei MEDIA@Komm-Städte. Darüber hinaus waren auch hier Vertreter von Datenzentralen, Rechenzentren und Herstellern vertreten.

Die Entscheidungsinstanz. In der *Entscheidungsinstanz* wurden die strategischen Ziele festgelegt und die qualitätsgesicherten Ergebnisse abgenommen. Die Entscheidungsinstanz war besetzt durch Vertreter des KoopA-ADV.

Die Projektleitung

Die Projektleitung lag bei der OSCI-Leitstelle. Wir wurden durch externe Methodenberater von der Firma MSI unterstützt.

Das Projekt wurde in drei Phasen durchgeführt und dauerte von August 2001 bis März 2002. Der Aufwand betrug rund 150 MT (ohne den Aufwand der Projektleitung).

Ergebnis: Exakte Vorgaben für Nachrichtenformate

Die Projektergebnisse bestehen in einer Beschreibung der Nachrichtenformate für die wichtige Geschäftsvorfälle des novellierten Melderechtsrahmengesetz. Es handelt sich somit um genaue Vorgaben für ein Datenaustauschformat, so wie es in der 2. BMeldDÜV durch die Anlagen zum §6 geregelt wird. Allerdings bedienen wir uns im Projekt OSCI-XMeld der wesentlich moderneren Beschreibungssprache XML, um Nachrichtenformate exakt und unmissverständlich festzulegen.

Die Beschreibung erfolgt in XML

Bei XML handelt es sich um eine moderne Methode, um genau zu definieren, welche Struktur Nachrichten haben müssen, wenn sie zwischen Sendern und Empfängern auszutauschen sind. Unter anderem wird festgelegt:

- welche Datenfelder Nachrichtenbestandteil sein können;
- in welcher Reihenfolge sie zu senden sind;
- ob Felder zwingend, optional oder wiederholbar sind;
- welches Format die Felder haben dürfen (Zeichensatz, ggfs. Feldlänge etc.)

XML hat sich als Beschreibungssprache weltweit durchgesetzt.

XML ist automatisiert zu verarbeiten ...

Ein wesentlicher Vorteil von XML gegenüber frei erstellen Vereinbarungen (wie sie als Anlagen der 2. BMeldDÜV genutzt werden) ist, dass XML automatisiert verarbeitet werden kann. Man kann mit sehr geringem Aufwand

eine Software erstellen, die automatisch prüft, ob eine Nachricht zwischen zwei Meldeämtern den Formatvorgaben der OSCI-XMeld-Gruppe entspricht.

... aber für Menschen schwer lesbar

Dieser große und ökonomisch wichtige Vorteil wird jedoch mit dem Nachteil erkauft, dass eine in XML vorliegende Beschreibung erlaubter Nachrichtenformate (eine so genannte *Schema-Datei)* für Menschen schwer lesbar ist.

Aus diesem Grunde wurde im OSCI-XMeld-Projekt neben dem eigentlichen Arbeitsergebnis (drei XML Schema-Dateien) eine sehr umfangreiche Dokumentation erstellt. Sie hat vor allem das Ziel, dem Leser den Inhalt der Schema-Dateien nahe zu bringen. Darüber hinaus werden in dieser Dokumentation Entwurfsprinzipien erläutert und das Verhältnis zwischen jedem DSMeld-Feld und den OSCI-XMeld-Nachrichten dargestellt.

In diesem Papier beschreiben wir zwei Beispiele der OSCI-XMeld Projektergebnisse in Form von Bildern, wie sie sich auch in der von uns erstellten Dokumentation befinden.

Drei Bereiche wurden erfolgreich abgeschlossen

In der oben dargestellten Projektlaufzeit konnten drei Bereiche vollständig abgeschlossen werden. Es liegen abgestimmte und qualitätsgesicherte XML Schema-Definitionen vor für:

- Die Rückmeldung nach Zuzug oder nach Statuswechsel inklusive der Auswertung einer Rückmeldung, entsprechend §§2,3 der 1. BMeldDÜV.
- Insgesamt rund 50 Nachrichtenformate für Ereignisse, die zu einer Fortschreibung des Melderegisters entsprechend §4 der 1. BMeldDÜV führen.
- Die einfache Melderegisterauskunft an private (Einzelauskunft) oder gewerbliche (Sammelauskünfte) Kunden nach §21 Abs. 1a des novellierten Melderechtsrahmengesetzes.

Ein Beispiel: Tod des Ehegatten

Am Beispiel der Nachricht *Tod des Ehegatten* wird das Arbeitsergebnis des OSCI-XMeld-Projektes dargestellt.

Verstirbt der Ehegatte des Betroffenen, so ist dies den Meldeämtern aller Gemeinden, in denen der Betroffene (Neben-) Wohnungen unterhält, im Rahmen der Fortschreibung des Melderegisters nach §4 Abs. 1 der 1. BMeldDÜV mitzuteilen.

Welche Daten werden übermittelt?

Da die Einzelfälle der Fortschreibung in der 1. BMeldDÜV nicht geregelt sind, wurden die erforderlichen Daten zunächst durch die Fachleute des Meldewesens in der Projektgruppe ermittelt. Die für diesen Spezialfall erforderlichen Datenfelder wurden in ein allgemein anwendbares Schema eingefügt, welches generell bei der Fortschreibung des Melderegisters anzuwenden ist.

Daten für jede Fortschreibung ...

So muss bei jeder Fortschreibung des Melderegisters sichergestellt werden, dass eine eindeutige Identifikation des Betroffenen in der empfangenden Gemeinde gewährleistet wird.

... und spezifische Daten pro Anlaß

Für den speziellen Fall der Fortschreibung des Melderegisters aus Anlass des *Todes des Ehegatten* kommt hinzu, dass Angaben zum neuen Familienstand des Betroffenen benötigt werden, außerdem nähere Angaben zum Sterbefall.

Das Ergebnis ist in der Abbildung 18.2 dargestellt.

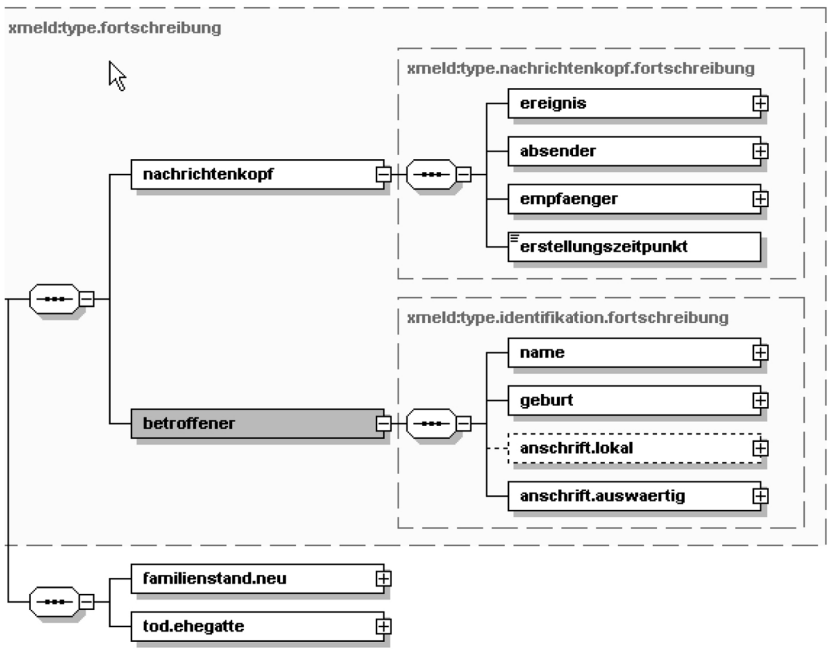


Abbildung 18.2: Nachrichtenstruktur im Falle des Todes eines Ehegatten

Diese grafische Darstellung wurde für den menschlichen Leser erstellt. Die verbindliche Beschreibung selbst ist in XML formuliert und Bestandteil der mit OSCI-XMeld 1.0 ausgelieferten XML Schema-Dateien.

Einfache Nachrichtenerstellung durch *Bausteine*

Alle Nachrichten des Meldewesens beziehen sich auf stets wiederkehrende Strukturelemente wie zum Beispiel *Anschrift*, *Meldebehörde*, *Familienstand*, *Nachweisdaten* und so weiter. Tatsächlich bildete die Erarbeitung dieser »Bausteine« auf Basis eines formal beschriebenen Informationsmodells die Hauptarbeit der OSCI-XMeld-Arbeitsgruppe. Die Komposition neuer Nach-

richtenformate, etwa für die Datenübermittlung zwischen Behörden nach §18 Melderechtsrahmengesetz, gestaltet sich durch den Rückgriff auf diesen Baukasten relativ einfach.

Ein Beispiel: der Familienstand

Einer der Bausteine, auf die bei der Nachricht zum Tod des Ehegatten zurückgegriffen wird, ist der *Familienstand*. Die Projektgruppe hat gemeinsam festgelegt, welche Datenfelder des DSMeld im Zusammenhang mit der Übermittlung eines Familienstandes (des Betroffenen oder eines Familienangehörigen) übermittelt werden können. Das Ergebnis der Überlegungen mündete in eine Datenstruktur, die ebenfalls in den XML-Schema-Dateien zu finden ist. Abbildung 18.3 zeigt die entsprechende grafische Beschreibung.

Die von der Projektgruppe erstellte Dokumentation besteht zu einem überwiegenden Anteil aus der Beschreibung der gemeinsam entwickelten Bausteine.

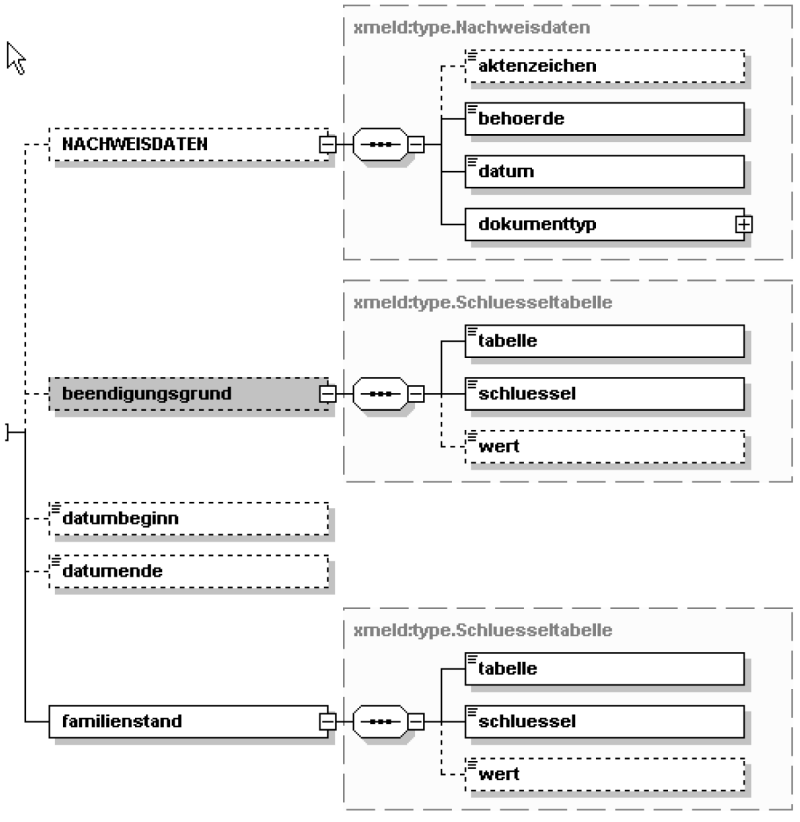


Abbildung 18.3: Der Nachrichtenbaustein »Familienstand«

Ein Baukasten für das Meldewesen

Die XML-Schema-Datei »xmeld-baukasten.xsd« umfasst derzeit rund 30 solcher Bausteine für Nachrichten des Meldewesens. Neben dem oben als Beispiel dargestellten *Familienstand* haben die Fachleute des Meldewesens unter anderem folgende Strukturen erarbeitet: *Anschrift*, *Auskunftssperre*, *Ausweisdokument*, *Einwohnerschaft*, *Unionsbürgerschaft* und weitere. So ist durch eine gründliche Erarbeitung des Informationsmodells die Fortführung des Projektes mit dem Ziel, weitere Nachrichtenstrukturen zu erarbeiten, gut vorbereitet worden.

Der DSMeld bildet das Fundament von OSCI-XMeld

Letztendlich werden nahezu alle Bestandteile der OSCI-XMeld-Strukturen auf den DSMeld zurückgeführt. Die inhaltlichen Definitionen des DSMeld werden durch OSCI-XMeld nicht angetastet. In OSCI-XMeld hat lediglich eine Erweiterung für solche Datenfelder stattgefunden, die spezifisch sind für die *Übermittlung* von Nachrichten. Dazu gehören zum Beispiel Angaben zur adressierten Meldebehörde im Rahmen der Rückmeldung, aber auch Angaben zum Kunden im Rahmen der einfachen Melderegisterauskunft nach §21 Abs. 1a.

In Abb. 18.4 ist dargestellt, dass OSCI-XMeld-Nachrichten aus OSCI-XMeld-Bausteinen zusammengesetzt sind. Diese werden durch den DSMeld definiert.

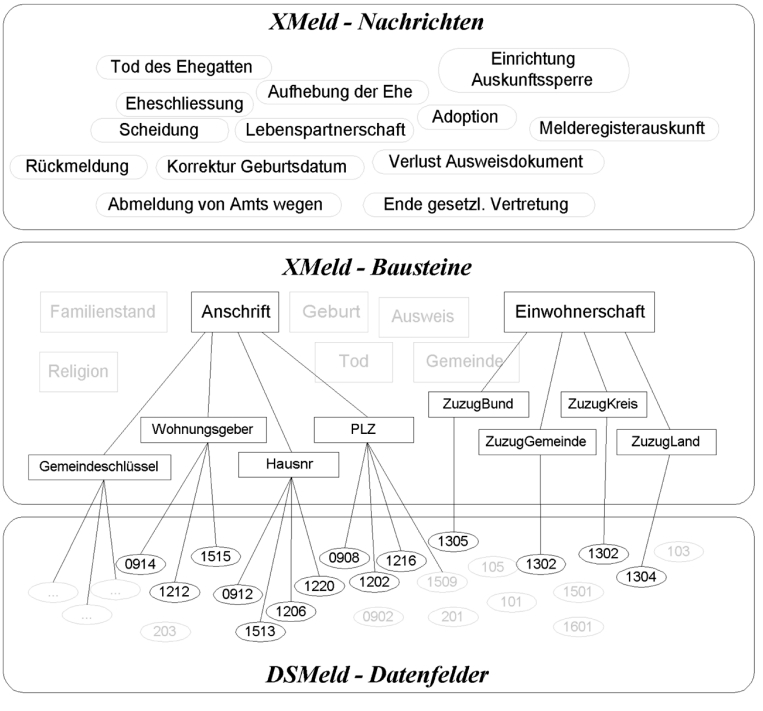


Abbildung 18.4: Nachrichten, Bausteine und der DSMeld

So bildet der DSMeld als *Vorgabe für die Erfassung und Speicherung* von Daten in Melderegistern auch die Basis für die OSCI-XMeld-Nachrichten. Die dazwischen liegende Hierarchiestufe der »Bausteine« sichert die leichte Erweiterbarkeit und Wartbarkeit der OSCI-Xmeld-Nachrichtenstrukturen.

Projektende im März 2002

Das Projekt OSCI-XMeld 1.0 wurde im März 2002 mit der Abnahme aller Ergebnisse durch die Entscheidungsinstanz termingerecht abgeschlossen. Die Entscheidungsinstanz hat dabei die OSCI-Leitstelle aufgefordert, mit den Planungen für ein Folgeprojekt OSCI-XMeld 1.1 zu beginnen, in dem weitere Geschäftsvorfälle des Meldewesens abzudecken sind.

Die Projektergebnisse (also die XML-Schema-Dateien und die zugehörige Dokumentation) stehen – wie alle Spezifikationen der OSCI-Leitstelle – unentgeltlich zur Verfügung.

18.2.2 OSCI-Transport für die sichere Nachrichtenübermittlung

Für den automatisierten Nachrichtenaustausch zwischen Meldebehörden ist die verbindliche Festlegung von Nachrichtenformaten nicht ausreichend. Es wird außerdem verbindliche Vorgaben über die Technik der Nachrichtenübermittlung geben müssen, ansonsten ist der reibungslose Nachrichtenaustausch trotz einer Einigung über die Inhalte nicht gewährleistet.

Sichere Nachrichtenübermittlung als Querschnittsaufgabe

Die Frage nach einer Methode für den sicheren und nachvollziehbaren Datenaustausch wird sich in sehr vielen Projekten des E-Government stellen. Die meisten Geschäftsvorfälle stellen hohe Anforderungen:

- an den Datenschutz (weil personenbezogene Daten übermittelt werden),
- an die elektronische Signatur (als Ersatz der eigenhändigen Unterschrift),
- und an die Nachvollziehbarkeit der Datenübermittlung (zum Nachweis der Fristwahrung).

Anders als im *E-Business* hat die öffentliche Verwaltung nicht die Möglichkeit, ihre Sicherheitsmechanismen anhand einer Risikoanalyse und anschließenden Wirtschaftlichkeitsbetrachtungen selbst festzulegen. Die Entwicklung eines Transportprotokolls, welches speziell für diese besonderen Anforderungen geeignet ist, ist somit eine *Querschnittsaufgabe* im Rahmen des E-Government.

OSCI-Transport: ein MEDIA@Komm-Ergebnis

Der Bedarf an einem solchen Protokoll ist von der Verwaltung früh erkannt worden. Deshalb ist die OSCI-Leitstelle im Rahmen des MEDIA@Komm-Projektes damit beauftragt worden, hier einen Entwurf vorzulegen und diesen innerhalb der öffentlichen Verwaltung abzustimmen.

Ende 2000: Version 1.0

Die OSCI-Leitstelle hat Ende 2000 die erste Version von OSCI-Transport vorgelegt. Seitdem wird OSCI-Transport in vielen E-Government-Projekten produktiv eingesetzt

Aktuell: Version 1.2

Die Erfahrungen aus der Praxis führten zu neuen Anforderungen. Diese wurden durch die OSCI-Leitstelle gesammelt und priorisiert. Im März diesen Jahres wurde das Projekt »OSCI-Transport 1.2« begonnen. Unter der Projektleitung der OSCI-Leitstelle erarbeiteten Fachleute der Verwaltung (drei MEDIA@Komm-Städte und Stadt Hagen) und der Wirtschaft (Firmen ppi, SAP, *bremen online services*, datenschutz nord) gemeinsam die neue Version. Die Anforderungen wurden vor dem Projektbeginn mit dem BSI abgeglichen.

Aufgrund des hohen Engagements aller Beteiligten konnte die neue Version 1.2 bereits im Juni diesen Jahres vom Auftraggeber KoopA-ADV abgenommen werden. Seitdem steht OSCI-Transport in der neuen Version der öffentlichen Verwaltung unentgeltlich zur Verfügung.

Bestandteil des BSI-Handlungsleitfadens ...

Die Eignung von OSCI-Transport für die Anforderungen des E-Government wurde mit Fachleuten aus der Verwaltung immer wieder diskutiert. Mit der Arbeitsgruppe »Kommunikation und Sicherheit« des KoopA-ADV wurde das Einsatzszenario für OSCI-Transport beschrieben. Als Ergebnis dieses Diskussionsprozesses wurde OSCI-Transport in den »Handlungsleitfaden für die Einführung der elektronischen Signatur und Verschlüsselung in der Verwaltung« aufgenommen.

... und »empfohlener Standard in SAGA«

In dem Dokument »SAGA: Standards und Architekturen für E-Government Anwendungen« bewertet der Bund verschiedene Techniken und Methoden, die im E-Government zur Anwendung kommen können. OSCI-Transport hat dort die Einstufung als *empfohlener Standard* erhalten. Es wird darauf hingewiesen, dass »nach sicherheitstechnischer Bewertung durch das BSI und der Unterstützung durch geeignete Produkte ... diese Standards den Status obligatorisch erlangen [können]«. In diesem Fall würde OSCI ein verbindlicher Standard im Rahmen von *Bund Online 2005*. Die entsprechende sicherheitstechnische Bewertung nimmt das BSI auf Grund eines Erlasses des BMI derzeit vor.

OSCI-Transport schafft eine einheitliche Transportbasis

Die Technologien für den Umgang mit elektronisch unterschriebenen Dokumenten und Nachrichten sind noch recht jung. Mit den auf dem Markt vorhandenen Produkten kann man elektronisch signieren und Zeitstempel

erzeugen, aber es mangelt oft an der Interoperabilität. Das bedeutet, man kann sich nicht darauf verlassen, dass der Empfänger einer unterschrieben und verschlüsselten Nachricht diese auch öffnen und lesen kann – wenn Sender und Empfänger unterschiedliche Sicherheitsprodukte (Signaturkarten, Kartenleser oder Software) einsetzen, sind Probleme zu befürchten.

Im Meldewesen muss es einheitliche Lösungen geben

Für den Regelungsbereich der 1. BMeldDÜV ist eine verbindliche Vorgabe von Übertragungsverfahren nicht akzeptabel, wenn dies faktisch den Zwang zur Nutzung eines einzigen Produktes als Konsequenz hat. Aus diesem Grunde haben alle Projektbeteiligten stets betont:

- Eine Einigung auf einheitliche Standards für die Technik der Datenübermittlung ist sinnvoll und notwendig.

  Eine Wettbewerbssituation *auf der Ebene der Standards* ist unsinnig und verhindert effiziente, flächendeckende Lösungen.

- Die alternativen Umsetzungsmöglichkeiten in Ländern und Kommunen müssen erhalten bleiben.

  Eine Wettbewerbssituation *auf Hersteller- und Produktebene* ist sinnvoll und führt in der Regel zu einer ökonomisch günstigeren Situation für die Verwaltung.

OSCI-Transport ist Hersteller- und Produktneutral

Die Spezifikation von OSCI-Transport ist überall dort, wo es möglich war, an international anerkannten Standards und Projekten ausgerichtet. Die in der Version 1.0 noch vorhandenen Abhängigkeiten von konkreten Implementierungen (also Produkten) der Firma *bremen online services* wurden in der Version 1.2 vollständig entfernt. Dies wurde durch das QS-Gremium bestätigt (Arbeitsgruppe *Transport und Verpackung* des Deutschen Institut für Normung (DIN) im Rahmen der MEDIA@Komm-Begleitforschung).

18.2.3 OSCI-XMeld und OSCI-Transport sind Lösungen für den Einsatz im Meldewesen

Durch den gemeinsamen Einsatz von OSCI-XMeld und OSCI-Transport kann ein hersteller- und produktneutraler Informationsverbund zwischen den Meldeämtern der Bundesrepublik aufgebaut werden. Dann regelt:

- OSCI-XMeld das verbindliche Nachrichtenformat, so wie es in der 2. BMeldDÜV durch die Anlagen zum §6 geschieht; und
- OSCI-Transport bestimmt die Technik der Nachrichtenübermittlung, so wie es in der 2. BMeldDÜV in §7 ff gemacht wird. Dabei sichert OSCI-Transport die Einhaltung der hohen Anforderungen an Datenschutz und Datensicherheit ebenso zu, wie die Nachvollziehbarkeit der Datenübermittlung.

Bei beiden Spezifikationen handelt es sich um Arbeitsergebnisse, die im Auftrag der öffentlichen Verwaltung erstellt wurden und unentgeltlich genutzt werden können.

Zustimmung durch Bürger- und Meldeamtsleiter

Nach dem Abschluss des Projektes OSCI-XMeld 1.0 wurden die Ergebnisse dem *Arbeitskreis der Bürger und Meldeamtsleiter im Deutschen Städtetag* vorgestellt. Diese Gruppe von Fachleuten schloss sich der Argumentation zu Gunsten von OSCI-XMeld sowie OSCI-Transport an und fordert, die Novellierung der 1. BMeldDÜV auf dieser Basis zu betreiben.

Die Verwaltung bestimmt ihre Standards selbst

Von besonderer Bedeutung für diese Entscheidung der Fachleute des Meldewesens war dabei die Tatsache, dass die Entwicklung sowohl von OSCI-XMeld, als auch von OSCI-Transport, im Auftrag der öffentlichen Verwaltung erfolgt und auch durch diese kontrolliert wird. Einer Herstellerabhängigkeit müsse bei dem Aufbau eines Informationsverbundes im Meldewesen unbedingt entgegengewirkt werden, dies war die übereinstimmende Auffassung aller Teilnehmer.

19 Die Chipkarte der Zukunft: Java Card und konkurrierende Interpreter-Konzepte

Frank Schipplick

19.1 Einleitung

Chipkarten, die auf Interpreterkonzepten basieren, gewinnen in den verschiedenen Anwendungsbereichen (z.B. Telekommunikation oder Kreditwirtschaft) immer mehr an Bedeutung. Langfristig werden sie die derzeit noch dominierenden proprietären Chipkartenbetriebssysteme verdrängen. Zur Zeit gibt es vier verschiedene konkurrierende Interpreterkonzepte:

- Java Card,
- Multos,
- Windows für Smart Card und
- die BasicCard.

Einem Applikationsbetreiber ist es jedoch im Wesentlichen egal, wie das Betriebssystem seiner Karte heißt und mit welchen Tools seine Applikationen entwickelt werden. Ihn interessiert vielmehr:

- die Sicherheit der Karte,
- die Flexibilität bei der Applikationsentwicklung,
- die Interoperabilität mit weiteren Applikationen,
- die Download-/Upgradefähigkeit im Feld,
- die Kompatibilität der Karte,
- die Verfügbarkeit der Karte,
- und der Preis je Karte.

Im vorliegenden Kapitel werden diese Fragestellungen eingehender beleuchtet. Dabei liegt der Fokus auf der Java Card, da sie das bedeutendste Interpreterkonzept ist.

19.2 Technischer Vergleich der Interpreterkonzepte

19.2.1 Multos

Die Multos-Entwicklung ist ursprünglich durch Mondex gestartet worden und obliegt nun dem MAOSCO Konsortium mit insgesamt 11 Mitgliedern, unter denen neben Herstellern wie Fujitsu, Giesecke & Devrient, Hitachi und Infineon auch Europay International, Mastercard International und American Express vertreten sind.

Multos basiert auf einem Interpreter mit einer assemblerähnlichen Sprache MEL. Sprachen wie C und Java können durch einen Cross-Compiler nach MEL übersetzt werden und somit auch genutzt werden. Da Multos eine Trennung zwischen dem eigentlichen Betriebssystem Multos und dem MEL Interpreter vorsieht, ist es möglich auch eine Java-Implementierung parallel zu MEL auf einer Chipkarte zu implementieren.

Als einziges Betriebssystem mit Interpreter verfügt Multos über eine Zertifizierung ITSEC E6 hoch (siehe www.itsec.gov.uk). Damit auch die jeweiligen Implementierungen von Multos durch den Chiphersteller (Hitachi, Motorola und Infineon) diesen Anforderungen genügt, muss dieser seinerseits die Implementierung sowie den Chip entsprechend ITSEC E6 hoch evaluieren und zertifizieren lassen.

MAOSCO vermarktet neben den Multos-Lizenzen im Wesentlichen die PKI und die Zertifikate, die zur Aktivierung der Karten sowie zum Laden und Löschen von Applikationen auf der Karte notwendig sind. Durch diese starre Linzenzpolitik kommen auf einen Kartenherausgeber erhebliche Kosten beim Kartenmanagement zu.

19.2.2 Windows for SmartCard

Ab 1997 hat auch Microsoft massiv die Entwicklung eines eigenen Chipkartenbetriebssystems vorangetrieben. Diese Entwicklung des Betriebssystems für Chipkarten, damals noch unter dem Namen »SmartCards for Windows«, war Bestandteil der Strategie, für jedes elektronische Gerät das passende Windows Betriebssystem anbieten zu können. Auch Windows CE hat in dieser Strategie seinen Ursprung.

Das Konzept von »Windows for SmartCard« sieht vor, dass der Entwickler über ein komfortables Entwicklungskit die Zusammenstellung seines Chipkartenbetriebssystems selber gestalten kann. So kann er an einer grafischen Oberfläche durch einfaches Anklicken konfigurieren, mit welchem Protokoll seine Karte betrieben wird (T=0/T=1) oder welche kryptografischen Funktionen unterstützt werden.

Die Entwicklung der eigentlichen Applikation erfolgt dann in einer speziellen Entwicklungsumgebung mittels Basic. Alle notwendigen Tools werden dabei kostengünstig von Microsoft angeboten, sind jedoch nur für Windows Plattformen erhältlich. Bestandteil der Produktfamilie rund um das Software Development Kit (SDK) für »Windows for SmartCards« sind auch die notwendigen Chipkarten und Chipkartenterminals. Mit PC/SC hat Microsoft zudem parallel die notwendige Infrastruktur/Treiberarchitektur entwickelt, um auf Chipkarten über einen Chipkartenleser auch in den größeren Windowsbetriebssystemen zugreifen zu können.

Das Betriebssystem wurde von Microsoft auch bei größeren Stückzahlen je Karte verkauft.

Nachdem es Anfang 2001 um die weitere Entwicklung des Betriebssystems sehr ruhig geworden ist, hat sich Microsoft Mitte 2001 entschlossen, die Lizenzpolitik zu ändern. Seitdem ist es für Anbieter und Hersteller möglich, die Entwicklungsumgebung und das eigentliche Betriebssystem im Quellcode zu lizenzieren. Parallel hierzu hat Microsoft den Quellcode als Standardisierungsvorschlag bei ETSI (European Telecommunications Standards Institute) eingereicht.

Das Betriebssystem ist in drei unterschiedlichen Varianten zur Zeit verfügbar:

- Windows for SmartCards 1.0/Netzwerksicherheit
- Windows for SmartCards 1.1/GSM
- Windows for SmartCards 2.0/Bankanwendungen

Eine Zertifizierung des Betriebssystems gemäß ITSEC ist bisher nicht erfolgt, sie ist jedoch durch Offenlegung des Quellcodes (Mai 2001) möglich geworden.

19.2.3 Zeitcontrols BasicCard

Die BasicCard und die zugehörige Entwicklungsumgebung wird durch die mittelständische Firma Zeitcontrol vermarktet. Die Vermarktung der BasicCard ist jedoch erst in den letzten 3-4 Jahren vorangetrieben worden. Im Gegensatz zu anderen Interpreterkonzepten zielt die Vermarktung der BasicCard nicht primär auf bedeutende Absatzmärkte wie etwa GSM-Karten für Mobilfunkprovider oder Kunden- und Bankenkarten, sondern vielmehr auf die Vermarktung im Projektgeschäft oder sogar direkt an den Endanwender.

Um diese Marktfelder erfolgreich bedienen zu können, bietet Zeitcontrol fertig konfektionierte Produkte mit Entwicklungsumgebung, Chipkartenleser, Dokumentation und den notwendigen BasicCards an. Aufgrund der einfachen Handhabung wird die BasicCard mittlerweile in vielen Demonstrations- oder Lehrprojekten bei der Realisierung exemplarischer Chipkartenprojekte verwendet.

Die Karte unterstützt einen eigenen Basic-Dialekt, der durch einen Compiler in einen Bytecode, den sogenannten P-Code übersetzt wird. Auch hier wird somit, wie bei der Java Card, ein Teil des Interpreters (bzw. der Virtuellen Maschine) Off-Card abgearbeitet.

Im Gegensatz zu aufwändigen Personalisierungskonzepten, etc. wird die BasicCard in einem »offenen« Zustand ausgeliefert. Das bedeutet, dass es beliebig möglich ist, Applikationen in die Karte zu laden, mit diesen zu arbeiten und diese auch wieder zu löschen. Einen Schutz bietet die Karte für die gespeicherten Applikationen und Daten erst dann, wenn die Karte »abgeschlossen« worden ist. Ein erneutes »Öffnen« ist danach jedoch nicht mehr möglich.

Einem Einsatz in sicherheitskritischen Bereichen steht neben fehlenden Angaben zur Sicherheit der Karten zudem entgegen, dass die BasicCard nicht über alle Funktionen verfügt, die für sicherheitskritische Anwendungen notwendig sind. Ein »echter« Zufallsgenerator in Hardware steht nicht zur Verfügung. Auch das Ladeverfahren entspricht weder den funktionalen noch den sicherheitsrelevanten Anforderungen, die für einen breiten Einsatz im Bereich Banken, Telekommunikation etc. notwendig sind. Eine Zertifizierung gemäß ITSEC ist bisher nicht angestrebt.

Durch die einfache Programmierung kann die BasicCard jedoch ohne großen Aufwand (inkl. Einarbeitung) zur Realisierung einfacher Chipkartenprojekte herangezogen werden.

19.2.4 Java Card

Mit zunehmender Verbreitung der Java-Technologie hat Sun festgestellt, dass eine einzige Java Virtual Machine (VM) mit all ihren Bibliotheken, APIs und Tools nicht allen Anforderungen genügen kann. Aus dieser Überlegung heraus sind nun drei unterschiedliche Editionen entstanden, für die Entwicklungsumgebungen, Dokumentationen und Tools zur Verfügung gestellt werden:

- Java 2 Plattform, Enterprise Edition
- Java 2 Plattform, Standard Edition
- Java 2 Plattform, Micro Edition

Die einzelnen Editionen unterscheiden sich im Wesentlichen durch einen von der Enterprise bis hinunter zur Micro Edition abnehmenden Funktionsumfang der verfügbaren Java-Klassen, wobei jedoch die Kernfunktionalität aller Editionen gleich und vor allem kompatibel geblieben ist.

Die Java 2 Micro Edition ist speziell für den umfangreichen Markt der Konsumergeräte wie etwa Mobiltelefone, Pager, Set-Top Boxen und auch Chipkarten, entwickelt worden.

Darauf aufbauend wurde die aktuelle Version der Java-Card-Spezifikation (Version 2.1.1 vom 18. Mai 2000) entwickelt. Wie bereits die vorhergehende Version besteht diese aus den drei Teilen:

- Definition der Laufzeitumgebung

  (Java CardTM 2.1.1 Runtime Environment (JCRE) Spezification),

- Definition der API

  (Java CardTM 2.1.1 Application Programming Interface) sowie die

- Definition der Virtuellen Maschine

  (Java CardTM 2.1.1 Virtual Machine Specification).

Der aktuelle Standard Java Card 2.1.1 hat ein sehr stabiles Stadium erreicht, große Änderungen sind nicht mehr zu erwarten.

Bereiche, die bisher noch nicht standardisiert sind, werden auch nach wie vor im Gebiet der herstellerspezifischen Funktionen zu finden sein. In diesem Sektor ist jedoch auch das Interesse an einer Standardisierung gering.

Unabhängig von der Java-Card-Technologie wird es jedoch weitere Standards geben, wie sie etwa im Bereich des Mobilfunks durch 3GPP (3. Generation-Partnership-Projekt) und ETSI (European Telecommunication Standard Institute) spezifiziert werden. Unabhängig von der Technologie des Kartenbetriebssystems können diese weitere Funktionen standardisieren. Ein ähnlicher Standard, der die Funktionalität der Java Card maßgeblich beeinflusst, von dem Standard Java Card jedoch unabhängig ist, existiert mit Open Platform (bzw. 3GPP Open Platform).

Open Platform

Das Projekt Open Platform wurde 1998 noch unter dem Namen »Visa Open Platform« durch Visa gestartet, um einheitliche Voraussetzungen für die Verwendung einer Chipkarte mit mehreren Kartenapplikationen (Multi-Applikation) und das hierfür notwendige Laden bzw. Verwalten dieser Applikationen zu schaffen. Speziell mit den aufkommenden Interpreterkarten und den immer leistungsfähigeren Chips, die über einen großen Speicherbereich verfügen, wurde deutlich, dass sich zunehmend mehrere Applikationen auf einer Karte befinden werden. Die Idee von Open Platform ist es, die Zugriffsrechte auf die Karte zu standardisieren. Dabei sind insbesondere die Vorgänge beim Laden und Löschen von Applikationen und Datenstrukturen, das Personalisieren sowie die Abläufe im Terminal standardisiert worden.

Um eine deutlich bessere Evaluierbarkeit gemäß ITSEC oder Common Criteria zu erreichen, sieht Open Platform eine klare Trennung der Applikationen in sogenannten »Security Domains« vor. Zugriffsrechte auf diese Domains und auch die Rechte innerhalb einer Domain werden durch das Kartenbetriebssystem sichergestellt. Zugriffe mit unzureichenden Rechten werden so geblockt und durch das Betriebssystem protokolliert.

Auch Interpreterkonzepte wie etwa Java Card unterstützen unterschiedliche Zugriffsrechte, die durch die Interpreter überwacht werden. Der Interpreter selbst ist jedoch in den meisten Fällen auf ein minimales Chipkartenbetriebssystem aufgesetzt. Open Platform erhöht somit die Sicherheit und führt eine klar strukturierte Trennung ein, die zudem noch einen direkten Bezug zu Security Domains und somit zu unterschiedlichen Applikationsbetreibern hat.

Obwohl Open Platform nicht eindeutig auf die Verwendung von Java Cards als Kartenplattform abzielt und auch Windows for SmartCards als mögliche Betriebssystemvariante erwähnt wird, ist Java Card doch eindeutiger Favorit. Nicht zuletzt bieten alle namhaften Kartenhersteller mittlerweile Java Cards basierend auf der Spezifikation Java Card 2.1 und Open Platform 2.0 an. Der Standard Java Card 2.1.1 wird zur Zeit implementiert und ist noch nicht bei allen Herstellern verfügbar. Auch Open Platform wird noch nicht in der aktuellsten Version unterstützt. Die aktuelle Spezifikation ist in drei Teile aufgeteilt:

- Die »Open Platform Card Specification«, Version 2.1, Juni 2001 sowie zugehörig zu dieser die Spezifikation des Java Card Export Files für Open Platform vom November 2001.
- Die »Visa Open Platform Card Implementation Specification« bestehend aus den Teilen »Multiple Application Smart Card Management Systems GlobalPlatform Functional Requirements« in Version 3.4 vom Mai 2001 sowie »Card Configuration and Script Builder Specification« in Version 2.0.2 vom November 2002.
- Die »Open Platform Terminal Specification« in Version 1.5 von November 1999 sowie eine Referenz Implementierung der API.

Die nachfolgende Beschreibung konzentriert sich auf den für Java Card wesentlichen kartenspezifischen Anteil der Spezifikation.

So beschreibt die »Open Platform Card Specification« die Kommunikation zwischen Karte und Terminal sowie die Kommunikation zwischen den einzelnen Applikationen. Einerseits wird so die Entwicklung von Kartenapplikationen ermöglicht, auf der anderen Seite jedoch auch der »on card«-Anteil der Ladeinfrastruktur der Karte spezifiziert. Über einzelne Befehlssequenzen lässt sich der gesamte Lebenszyklus der Karte (Produktion, Personalisierung, Aktivierung, Sperren und Einzug) abbilden.

Wesentliche Komponenten der Open Platform Architektur auf der Karte sind:

- Runtime Environment
- Open Platform API
- Kartenmanager
- Kartenapplikationen (Applets bei Java Cards)
- Security Domains

Die nachfolgende Zeichnung verdeutlicht den Aufbau der Open Platform Architektur und die Einbettung in ein Interpreterbetriebssystem wie Java Card.

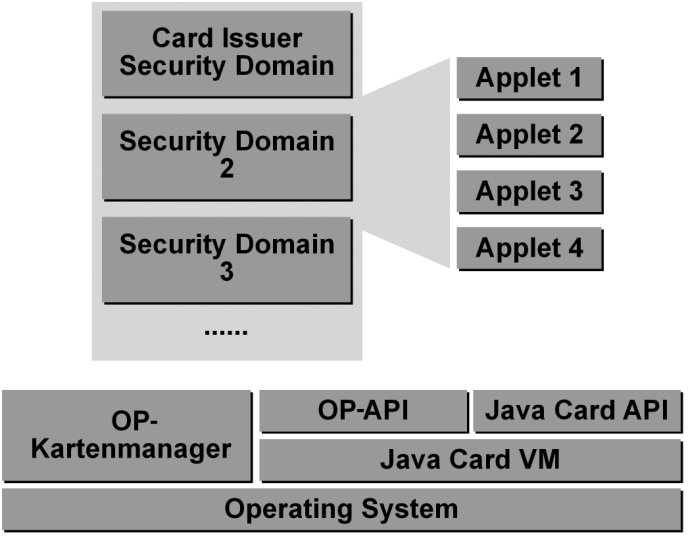


Abbildung 19.1: Open-Platform-Architektur

Eine wesentliche Komponente der Open Platform Architektur ist der Kartenmanager, der die Interessen des Kartenherausgebers auf der Karte vertritt. Er verhindert die unberechtigte Nutzung und protokolliert alle Zugriffe. Alle Zugriffe auf die Karte werden über einen Kommandoverteiler entgegengenommen und an eine zugeordnete Kartenapplikation (Applet) weitergeleitet. Neben den Dateninhalten der Karte werden auch die Zugriffsrechte auf die Karte bzw. von Applikationen in der Karte verwaltet. Diese Funktionalitäten sind in das Chipkartenbetriebssystem integriert und somit immer aktiv, sie zu umgehen ist nicht möglich.

Auf jeder Karte ist immer mindestens die »Security Domain« des Kartenherausgebers vorhanden. Weitere mögliche Sicherheitszonen können für Applikationsbetreiber eingerichtet werden, die nicht mit dem Kartenherausgeber identisch sind oder die organisatorisch bzw. technisch getrennt eingerichtet werden sollen. Die unterschiedlichen Sicherheitszonen ermöglichen es, Applikationen und Daten vor den Zugriffen anderer Sicherheitszonen zu schützen. Somit sind in diesem Modell die Sicherheitscharakteristiken von Java Card oder einem anderem Kartenbetriebssystem durch zusätzliche Barrieren erhöht. Das Management der Schlüssel, um somit auf einzelne Daten bzw. Applikationen zuzugreifen, obliegt jeder einzelnen Sicherheitszone bzw. dem Applikationsbetreiber. Es ist nicht möglich, eine neue »Security Domain« ohne den Kartenherausgeber einzurichten. Entsprechende Rechte müssen über die »Issuer Domain« und den Kartenmanager konfiguriert werden.

Mit Hilfe der »Security Domains« ist es möglich, gemeinsame Sicherheitsrichtlinien domainübergreifend zu definieren, so etwa eine einheitliche globale PIN, die von unterschiedlichen Applikationen mit einem übergreifenden Fehlbedienungszähler zentral vor Missbrauch geschützt wird. In den einzelnen Sicherheitszonen »Security Domains« können jedoch auch eigene Policies mit applikationsspezifischen PINs definiert werden.

19.3 Einsatzgebiete und Verbreitung

19.3.1 Multos

Als zertifiziert »sichere« Plattform ist Multos für den Einsatz im Bankbereich oder aber auch als SIM-Karte sehr gut geeignet. Europay International hat sogar in einem Vergleichstest mit Java Card und »Windows for SmartCards« zudem bewiesen, dass die Anforderungen einer Kartenapplikation an Speicher und Rechenzeit mit Multos am geringsten sind. Dennoch findet man Multos in Europa in nahezu keiner Chipkarte wieder.

Der Hauptabsatzmarkt der Multos Karten liegt, nach eigenen Angaben von MAOSCO, mit 65% im asiatischen Raum (jeweils durch Lizenznehmer von Master Card International und JCB). Auf Europa und America fallen jeweils nur rund 10%. Insgesamt sind bisher circa 7 Mio. Multos Karten in Umlauf gebracht worden.

Haupteinsatzgebiet der Multos-Karten ist der Bankenbereich. Dies nicht zuletzt durch die MAOSCO Mitglieder Mastercard und American Express. In der Öffentlichkeit ist dabei das »Blue Card« Projekt von American Express in den USA am bekanntesten. Obwohl jedoch die ersten Blue-Karten mit dem Multos Betriebssystem ausgeliefert worden sind, werden derzeit alle neueren Karten ausschließlich mit Java-Card-Technologie ausgestattet.

Neben dem Bankenbereich wird Multos in vielen mittleren Projekten mit 10.000 bis 200.000 Karten eingesetzt, darunter befinden sich auch zahlreiche Firmenausweis- und Kundenbindungssysteme. Für Projekte in dieser Größenordnung bietet die verfügbare PKI einen deutlichen Mehrwert, da sich hier eine eigene PKI nicht immer rechnet.

Im Telekommunikationssektor sowie auch im Gesundheitswesen wird Multos nahezu nicht eingesetzt. Ein Grund hierfür sind insbesondere die hohen Lizenzgebühren.

19.3.2 Windows for SmartCards

Alleine durch Microsoft polarisiert das Interpreterbetriebssystem Windows for SmartCards die möglichen Zielgruppen stark. Besonders im Fokus steht dabei die Sicherheit der Karte und der durch das Betriebssystem zu schützenden Daten und Programme. Entsprechende Sicherheitslücken der Desk-

top- und Serverbetriebssystemen von Microsoft sind in der Branche weitestgehend bekannt und werden als Vorbehalt angeführt. Da bis Mitte 2001 eine Offenlegung des Betriebssystems und der Quellcodes nicht geplant war, konnte eine Überprüfung oder Zertifizierung des Betriebssystems nicht erfolgen. Die entsprechenden Vereinbarungen mit den Lizenznehmern sahen sogar eine Haftungsübernahme durch die Hersteller der Karten vor.

Seitdem diese Hürde gefallen ist, steht einer Evaluierung nichts mehr im Wege, dennoch sind die Vorbehalte geblieben. So ist man bei Microsoft letztendlich auf einen einzigen Hersteller des Betriebssystems angewiesen. Entsprechende Verfahren in den USA und auch Erwägungen der Europäischen Kommission belegen zudem eine eindeutige Machtposition, wenn nicht gar Monopolstellung von Microsoft im Bereich der Desktop-Betriebssysteme. Eine ähnliche Entwicklung im Bereich der Chipkarte ist von keinem Kartenherausgeber gewollt. Betrachtet man den immensen Aufwand mit dem Microsoft dieses Produkt in der Einführungsphase vermarktet hat, so fällt auf, dass es in der letzten Zeit um Microsofts Windows for SmartCards sehr ruhig geworden ist. Auf der Homepage von Microsoft ist dieses Betriebssystem nahezu nicht mehr zu finden. Pressemitteilungen bezüglich Windows for SmartCards sind durch Microsoft schon seit Ende 2000 kaum mehr veröffentlicht worden. Einzig die Änderung der Lizenzpolitik im Mai 2001 ist somit zu vermerken und könnte als Indiz gewertet werden, das Produkt nach einer verfehlten Markteinführung nun über eine geänderte Lizenzpolitik durch Partnerunternehmen vermarkten zu lassen.

Größere Projekte, basierend auf diesem Betriebssystem sind nicht bekannt. Es steht zu vermuten, dass Microsoft dieses Produkt langfristig in dieser Art nicht weiter vermarkten wird.

19.3.3 Zeitcontrols BasicCard

Haupteinsatzbereich der BasicCard ist das Projektgeschäft sowie das Endkundensegment mit geringen Kartenstückzahlen.

Da die Karten den Sicherheitsanforderungen größerer Projekten nicht genügen, wird auch zukünftig der Einsatz im Banken-, Telekommunikations- oder Gesundheitswesen ausgeschlossen sein. Die Karte eignet sich somit eher für kleinere Projekte bei denen ein Ingenieurbüro oder ein Softwarehaus individuelle Kundenprojekte realisiert. Als größtes Projekt ist derzeit der Einsatz der BasicCard in einigen Spielkonsolen geplant, um zusätzliche Spielfiguren getrennt vom Spiel zusätzlich vermarkten zu können.

Bereits heute wird die BasicCard von vielen Hobbyisten und Bastlern eingesetzt. Es gibt jedoch keinen großflächigen Einsatz der BasicCard.

19.3.4 Java Card

Java Cards werden bereits von zahlreichen Netzbetreibern als GSM-Karten genutzt. In der Vergangenheit war dabei die eigentliche SIM-Applikation noch im proprietären Prozessorcode geschrieben und die Java Card Virtuelle Maschine wurde nur für die nachladbaren Applikationen genutzt. Dies hat sich mit der gesteigerten Performance und zunehmendem Speicher gewandelt.

Erste Java Cards wurden bereits 1997 durch die Swisscom eingesetzt. Bis heute sind durch die Swisscom über 2 Mio. Java Cards als SIM eingesetzt worden. Durch Telecom Italia Mobile (TIM) sind über 5 Mio. Java Cards ausgegeben worden. Weitere GSM-Netzbetreiber wie France Telecom, Telefonica, Orange, Hong Kong Telecom and China Mobile setzten ebenfalls auf die Java Card.

Die Entwicklung der USIMs (SIM-Karte des UMTS-Netzwerkes) läuft bei allen Mobilfunkbetreibern sogar komplett auf Basis von Java Cards.

Im Vergleich zu den vorgenannten Interpreterkonzepten bietet die Java Card eine Reihe von Vorteilen. Direkte Nachteile, die einem Einsatz der Karte langfristig entgegenstehen, sind nicht bekannt.

Vorteile der Java Card:

- Die Java Card Technologie ist durch ein Konsortium von Chipkartenherstellern in Zusammenarbeit mit SUN spezifiziert und frei veröffentlicht worden. Eine Abhängigkeit von einem einzelnen Hersteller oder Lizenzgeber ist somit nicht gegeben.
- Java Cards werden von allen bedeutenden Kartenherstellern angeboten. Die Java-Lizenzen müssen durch den Hersteller bezahlt werden und sind Bestandteil des Kartenpreises.
- Die Performance der heutigen Prozessorkarte reicht zunehmend aus, um die Anforderungen auch anspruchsvoller Kartenanwendungen zu erfüllen. Der Einsatz der Java Card als SIM-Karte für große GSM-Mobilfunkprovider belegt, dass dieses Betriebssystem in der Kosten-/Nutzenanalyse mit den herkömmlichen Prozessorkarten bereits gleichwertig ist.
- Eine starre PKI Infrastruktur besteht nicht. Die Integration der Karte in die bestehenden Kartenverwaltungssysteme wie auch in die Personalisierungsprozesse ist somit deutlich einfacher. Entsprechende Standards, wie etwa Open Platform, sind zur Zeit in Vorbereitung bzw. bereits veröffentlicht.
- JAVA und auch die daraus abgeleitete Java Card sind unter dem Aspekt der Sicherheit entwickelt worden. Der Kartenhersteller Gemplus bietet inzwischen auch eine nach den ITSEC zertifizierte Java Card an. Des weiteren erfolgte Ende 2001 eine Zertifizierung zweier Java-Chips gemäß Federal Information Processing Standards (FIPS) des National Institute

of Standard and Technology, nämlich FIPS 140-1 Level 2 und FIPS 140-1 Security Level 3 durch die US-Regierung. Diese Chips werden für den Ausweis des US-Militärs eingesetzt (4,3 Millionen Ausweise).

Nachteile der Java Card:

- Obwohl Java Card ein klar definiertes Betriebssystem darstellt, definiert die aktuelle Java Card Spezifikation nicht den vollständigen Funktionsumfang der heutigen Karten. Somit liefert jeder Kartenhersteller einen eigenen Satz kartenspezifischer Funktionen. Da jedoch darunter vor allem auch die kryptografischen Funktionen zu finden sind, sind die Kartenapplikationen zur Zeit nur bedingt kompatibel.
- Als Sprache ist Java im Vergleich zu Multos und Windows for Smart-Cards deutlich komplexer und somit schwerer zu zertifizieren. Demgegenüber stehen jedoch die Vorteile eines modernen Sprachkonzeptes.

Betrachtet man die wenigen Nachteile, so wird deutlich, dass diese im Wesentlichen durch weitere Standarisierungsbemühungen ausgeglichen werden können. Da dies im Interesse aller Kartenherausgeber ist, steht zu erwarten, dass die fehlenden Standards bereits kurzfristig zur Verfügung stehen.

19.4 Verfügbarkeit von Java-Card-Produkten

Alle großen Chipkartenhersteller – Gemplus, Giesecke & Devrient, Oberthur, Orga und SchlumbergerSema – bieten Java Cards und entsprechende Entwicklungstools in unterschiedlichen Ausprägungen an. Dabei unterscheiden sich die Hersteller technisch nicht sehr stark. Der Schwerpunkt der Entwicklungen liegt bei allen Herstellern aber derzeit – aufgrund der Nachfrage – im Mobilfunkbereich und zwar bei der USIM-Entwicklung. Für die USIM werden zur Zeit die größten und damit auch teuersten Chips eingesetzt. Die typischen Speichergrößen dieser Chips liegen bei 128 K ROM und 64 K EEPROM.

Für den Bankenbereich bieten alle Hersteller im Augenblick noch deutlich kleinere Java Cards an. Die typischen Speichergrößen liegen hier bei 16 K bis 32 K EEPROM und 48 K bis 96 K ROM. Diese Karten sind bei allen Herstellern kompatibel zur Java Card Spezifikation, Version 2.1 und zur Open Plattform Spezifikation, Version 2.0. Die erste Umsetzung der neuesten Spezifikationen (Java Card 2.1.1, Open Plattform 2.1) ist durch Gemplus und Oberthur erfolgt, Orga hat dies für das laufende Jahr angekündigt. Die anderen Hersteller haben hierzu noch keine definitiven Aussagen getroffen.

Die Preise für Java Cards liegen zur Zeit bei ca. 8 bis 15 € für weiße (unbedruckte) Karten, je nachdem, ob es sich um eine 16 K oder 32 K EEPROM-Karte handelt. Genauere Preisangaben kann man erst angeben, wenn die

exakte Abnahmemenge und die Lieferkonditionen feststehen. Preise für die Java Cards, die für die USIM-Entwicklung eingesetzt werden, sind derzeit noch nicht erhältlich.

Entwicklungstoolkits (Entwicklungssoftware inklusive Kartenleser und Testkarten) kosten zwischen 1.500 und 2.000 € pro Stück bei kleinen Abnahmemengen.

19.5 Fazit

Mit Hilfe von Java Cards wird es möglich sein, dass nicht nur Daten, sondern auch ablauffähige Programme selbst auf bereits ausgegebene Karten nachgeladen werden können. Die Vorteile, die sich daraus ergeben würden, sind:

1. Größere Flexibilität und Innovationsmöglichkeiten bei der Einführung neuer Funktionalitäten

   In der heutigen Situation muss man bei Änderungen von Chipkartenbetriebssystemen auch die Laufzeit bzw. die Gültigkeitsdauer der Karten und der darauf befindlichen Anwendungen berücksichtigen. Jede Modifikation des Chipkartenbetriebssystems bedingt die Ausgabe neuer Karten. Um Kosten zu sparen, werden daher notwendige Änderungen mit den Austauschzyklen korreliert, insbesondere in der Kreditwirtschaft. Mit dem Einsatz von Java Cards sind jederzeit, ohne Rücksichtnahme auf irgendwelche Austauschzyklen, funktionale Änderungen der Betriebssysteme möglich, da die Modifikationen auf bereits ausgegebene Karten nachgeladen werden können. Damit ist es möglich, schneller auf innovative technische Entwicklungen zu reagieren.

2. Plattform-Unabhängigkeit

   Für Java Cards gilt das »write once, run anywhere«-Prinzip: eine Anwendung muss als Applet nur einmal programmiert werden und kann dann auf die Java Cards von unterschiedlichen Kartenherstellern geladen werden. Einzige Voraussetzung ist, dass diese Java Cards alle die jeweils aktuelle Java Card Spezifikation – zur Zeit Version 2.1.1 – unterstützen bzw. neuere Versionen abwärtskompatibel sind.

   Die jeweilige Anpassung der Anwendung an alle Kartenlieferanten, wie derzeit notwendig, entfällt damit.

3. Multifunktionsfähigkeit

   Java Cards bieten die Möglichkeit, mehrere frei programmierte Java Card Applets gleichzeitig auf eine Karte zu laden. Durch die Nachladbarkeit von Anwendungen in Form von Daten und insbesondere Java Card Applets können darüberhinaus nachträglich – auf bereits ausgegebene Karten – weitere Funktionen/Applikationen auf die Karte gebracht werden. Dabei wird die Sicherheit der einzelnen Applikationen durch soge-

nannte »Security Domains« gemäß dem Standard Open Platform gewährleistet. Herkömmliche Chipkarten und Chipkartenbetriebssysteme stellen nur eine eingeschränkte Multifunktionalität zur Verfügung: es können nur spezifische Datenstrukturen für zusätzliche Anwendungen nachträglich auf den Karten angelegt werden. Eine Abschottung der Applikationen ist nur indirekt – nicht jedoch technisch durch eine Trennung von Betriebssystem und Applikationen – gegeben.

4. Einfache und kostengünstigere Programmierung der Anwendungen

   Mit der Programmierbarkeit in Java ergibt sich eine deutlich kürzere Entwicklungszeit für die Anwendungen. Zur Erstellung können handelsübliche Entwicklungstools für Java benutzt werden. Fertige Applets können bereits im Vorfeld an Simulatoren getestet werden. Spezifisches Know-how über den Chip, seine Interna und seine Programmierung in Native-Code ist nicht mehr notwendig. Damit wird der Anwendungsentwickler auch unabhängig von der Unterstützung des Chipkartenlieferanten.

5. Größere Gestaltungsmöglichkeiten für Zusatzanwendungen

   Bei der Entwicklung von Zusatzanwendungen ist man nicht mehr ausschließlich an vordefinierte Zusatzanwendungen – wie z.B. bei der ec-Karte mit Chip bzw. SECCOS (Secure Chipcard Operating System durch den zentralen Kreditausschuss (ZKA)) – gebunden. Damit ergibt sich ein weitaus größerer Gestaltungsspielraum, um mit innovativen neuen Anwendungen den Kunden zur vermehrten Nutzung seiner Chipkarte (z.B. Bankkarte) zu bewegen und ihn damit auch enger an das jeweilige kartenausgebende Institut zu binden.

Das oben dargestellte Optimierungspotentials ist sicherlich unbestritten, dennoch sind Java Cards keine Wunderkarten. Denn Java Cards ermöglichen zwar eine einfachere Programmierung von Anwendungen, das Erstellen einer **sicheren** Anwendung wird jedoch nicht leichter. Ebenso wird die notwendige Logistik beim Kartenherausgeber (Personalisierung und Auslieferung der Karten, Key Management etc.) mit Java Cards nicht einfacher. Durch die organisatorische und räumliche Trennung von Kartenproduktion und Appleterstellung kann jedoch an anderer Stelle ein höheres Sicherheitsniveau erreicht werden

20 Von der IT-Sicherheitsanforderung zum Service Level Agreement

Rolf-Dieter Köhler

Thomas Krampert

Edzard van Hülsen

20.1 Einleitung

Informationstechnologie ist in vielen Unternehmen unverzichtbarer Bestandteil der Wertschöpfung. Ohne automatische Übertragung und Verarbeitung von geschäftsrelevanten und -kritischen Informationen kommen zentrale Abläufe der Unternehmen zum Stillstand. Im Extrem führen Ausfälle der IT in wenigen Tagen zur Insolvenz.

Der Einsatz neuer Technologien in den Unternehmen nimmt rasant zu, verbunden mit immer kürzeren Perioden für die Erweiterung und Erneuerung solcher Technologien. Die Wettbewerbsfähigkeit zwingt die Unternehmen dazu, mit dieser Entwicklung Schritt zu halten.

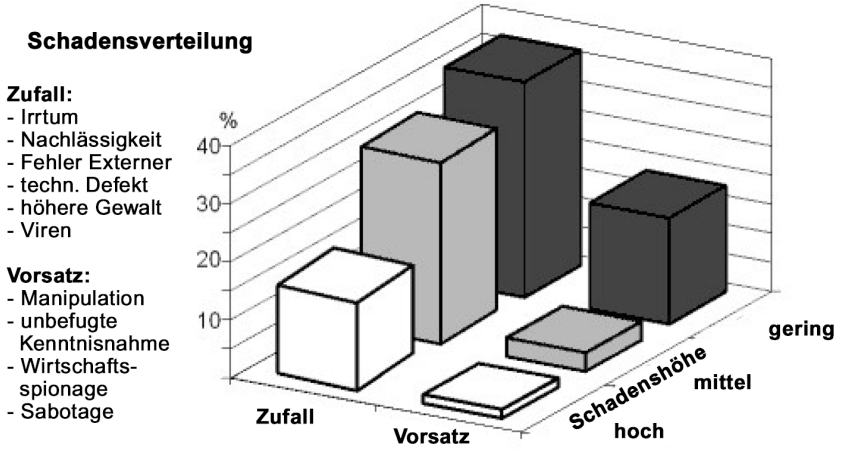


Abbildung 20.1: Alltag der IT-Sicherheit, Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Hinzu kommt, dass der IT-Bereich nicht mehr als IT-Servicelieferant in einer geschlossenen organisatorischen Einheit gesehen werden kann, sondern die IT durchdringt zunehmend alle Fachbereiche eines Unternehmens als flä-

chendeckende, unternehmensweite Einrichtung zur Unterstützung der originären Geschäftsprozesse. Der dadurch bedingte Datenstrom über teilweise nicht beeinflussbare Netzeinrichtungen sowie durch die dezentrale Speicherung von Geschäftsdaten stellt ein hohes Risiko sowohl für eine technisch bedingte Beschädigung als auch für einen gezielten Angriff durch Unberechtigte auf diese Daten dar.

Die sich daraus ableitenden Anforderungen an die Sicherheit aller geschäftsrelevanten Daten erfordern ein unternehmensweites durchgängiges IT-Sicherheitskonzept.

20.2 Begrifflichkeiten

Der Begriff IT-Sicherheit umfasst folgende Komplexe, die im Bereich von Kommunikationsnetzwerken eine starke Rolle spielen:

- Systemverfügbarkeit

  Bereitstellung von Anwendungen an die Arbeitsplätze der Nutzer nach vorgegebenen zeitlichen Parametern wie Servicezeiten, Antwortzeitverhalten, Ausfall- und Wiederherstellungszeiten. Spezifikation von Kritikalitätsklassen entsprechend der Anforderungen an die Anwendungen nach zeitkritischen Gesichtspunkten.

- Datensicherheit

  Schutz von Daten durch unberechtigten Zugriff auf Daten sowohl von innen als auch durch Angriffe von außen (Zutritt- und Zugriffsberechtigungen, Rechte-Vergabe, Firewalls, Virenschutz, u.a.).

- Datensicherung

  Archivierung und Wiederherstellbarkeit von Daten nach vorgegebenen zeitlichen und qualitativen Aspekten (Archivierungs- und Wiederanlaufverfahren, K-Fall Konzept).

20.3 Allgemeine Anforderungen an die IT-Sicherheitseinrichtungen

Einrichtungen zur Sicherstellung von Daten und Anwendungen erfordern immer ein Zusammenspiel von organisatorischen Maßnahmen wie z.B. Zutritts- und Zugriffsregeln und der Implementierung technischer Komponenten wie z.B. Kontrollmechanismen für Datenzugriff und IT-Komponenten. Dabei ist die Anwendungsverfügbarkeit der maßgebende Faktor.

Die Gestaltung der Sicherheitseinrichtungen darf nicht für jeden der genannten Komplexe isoliert ausgelegt werden, sondern ist immer in einer ausgewogenen Balance aller Komplexe zu konzipieren. Eine Überdimensionierung eines Komplexes kann durchaus negative Auswirkungen auf einen anderen

Komplex haben, z.B. kann eine »bombensichere« Archivierung zwar höchsten Archivierungsschutz gewährleisten, die Wiederherstellbarkeit von derart archivierten Daten für die Anwender möglicherweise aber zu lange dauern; ebenso kann eine sehr sichere zentrale Datenhaltung einem dezentral arbeitenden Börsenhändler nicht den notwendigen Handelsspielraum geben.

Der Ausgangspunkt aller Bestrebungen, die IT-Sicherheit »wasserdicht« zu gestalten, ist eine detaillierte Schwachstellenanalyse. Als Basis für eine solche Analyse müssen alle Anforderungen der drei Komplexe bekannt sein. In der Regel sind diese Anforderungen nicht hinreichend spezifiziert und sind oft die erste Aufgabe in der Analyse. Dabei nimmt die Evaluierung möglicher Angriffsszenarien auf Geschäftsdaten bei verteilten Anwendungen einen besonderen Stellenwert ein.

20.4 Systemverfügbarkeit

Die Funktionsfähigkeit einer IT-Infrastruktur stellt einen wichtigen Produktionsfaktor in den Unternehmen dar. Eine Nichtverfügbarkeit der IT-Infrastruktur bedeutet in vielen Unternehmen ein Produktionsverlust und kann den Unternehmen u.U. enorme Geschäftsverluste und damit auch Wettbewerbseinbußen zufügen.

Sicherheit im Sinne von Verfügbarkeit sagt etwas über die Stabilität der Arbeitsweise, also der Verfügbarkeit einer Komponente oder eines komplexen Systems, aus.

Somit sind Lösungen erforderlich, bei denen die Störung einzelner Komponenten nicht zu einem Totalausfall des Systems führen dürfen, sondern die Beeinträchtigungen des Systems müssen sich innerhalb definierter Grenzen halten, die vorher bestimmt werden.

Typische Verfügbarkeitsangaben eines IT-Systems werden immer noch in Prozentangaben des störungsfreien Betriebes eines zentralen Rechnersystems (Host) angegeben und bewegten sich oft zwischen 99,0% bis 99,9%. Diese Angabe stammt aus der Zeit der klassischen Datenverarbeitung und diente als Nachweis für die Verfügbarkeit, da die IT-Anwendungen ausschließlich von Bildschirmen in den Fachabteilungen auf einem Zentralrechner betrieben wurden. Da außer den Bildschirmsteuereinheiten keine weiteren leistungsbeeinträchtigenden Komponenten beteiligt waren, hatte diese Zahl durchaus ihre Berechtigung als Messgröße für die Verfügbarkeit und wurde vom RZ-Leiter als Verfügbarkeitsnachweis präsentiert.

Mit dem Wandel der IT zu einer dezentralen Architektur ist diese Zahl jedoch nicht mehr die maßgebende Verfügbarkeitsgröße, da sie ausschließlich die Verfügbarkeit einer IT-Komponente, dem Zentralrechner, angibt. Alle weiteren Komponenten in der Elementenkette von einem dezentralen Arbeitsplatz bis zum Anwendungssystem sind dabei unberücksichtigt. Diese haben jedoch einen wesentlichen Einfluss auf die Verfügbarkeit der Anwendungen und müssen bei der Berechnung der Verfügbarkeit für die Endbenutzer mit herangezogen werden.

Mit dieser Berechnung wird allerdings ausschließlich ein wahrscheinlicher Komplettausfall von Anwendungen ermittelt. In einem überwiegend dialogorientierten IT-Betrieb ist für die Endbenutzer jedoch die Leistungsfähigkeit der Anwendungen von größerem Interesse, die von den Anwendern durch das Antwortzeitverhalten wahrgenommen wird.

Hierzu gilt es, entsprechende Messverfahren und Berichtswesen zu implementieren.

Die Verfügbarkeitseinschränkung einer Anwendung für den Endbenutzer während einer Service-Periode wird durch die Summe der Verfügbarkeiten aller Komponenten bestimmt (Abbildung 20.2).

Abbildung 20.2: Beispiel einer Nichtverfügungsbestimmung

	Arbeitsplatz	Router	Router	Host	Datenbankserver	Storage
Verfügbarkeit	98%	98,5%	99%	99%	98,5%	99%
Nichtverfügbarkeit	2%	1,5%	1%	1%	1,5%	1%
(Beispieldaten)						

Im o.a. Beispiel sind der Einfachheit halber zeitlich sich nicht überlappende Ausfälle angenommen. Da aber mit zeitlich überlappenden Ausfällen gerechnet werden muss, kann die effektive Nichtverfügbarkeit mit Hilfe der Wahrscheinlichkeitsrechnung ermittelt werden. Hierzu können die MTBFs (meantime between failure) der einzelnen Komponenten herangezogen werden.

Die Festlegung hoher Verfügbarkeiten und den damit entsprechend verbundenen Konsequenzen muss anwendungsspezifisch sehr genau analysiert werden, da hierbei hohe Aufwändungen entstehen können, die durch den Nutzen gerechtfertigt sein müssen.

20.4.1 Hochverfügbare Systeme

Hochverfügbare Systeme basieren auf einem »no single point of failure«-Konzept. Ein Ausfall bedeutet einen hohen direkten wirtschaftlichen Verlust für das Unternehmen und beeinflusst maßgeblich den Geschäftserfolg oder verletzt gesetzliche Auflagen. Die Anwendungen sind zeitkritisch und nicht substituierbar.

Für solche Systeme müssen die wichtigen Komponenten redundant ausgelegt sein. Der Ausfall solcher Komponenten darf keine gravierenden negativen Einflüsse auf die Gesamtverfügbarkeit haben.

Dabei ist es unerheblich, ob eines der installierten Systeme aktiv und das andere passiv ist, oder ob beide Systeme z.B. mit geteilter Last (Load-Sharing) arbeiten. Diese Spezifikationen werden erst beim konkreten Design wichtig.

Eine Parallelisierung von funktional gleichen Komponenten erhöht somit die Systemverfügbarkeit. Verfügen die Komponenten über die Option redundanter Baugruppen (z.B. redundante Stromversorgung), so sollten auch diese redundant installiert werden.

Zusätzlich werden meist proprietäre Protokollunterstützungen für die Steuerung der Komponenten geboten.

20.4.2 Verfügbarkeit einer Funktion

Gegenüber der eben beschriebenen Systemverfügbarkeit greift die Betrachtung der Verfügbarkeit einer Funktion aber wesentlich weiter.

Das folgende Szenario verdeutlicht den typischen Ablauf einer Dialoganwendung.

Ein Anwender startet mit anwendungstypischen Eingabeparametern ein Anwendungsprogramm, das nach der Verarbeitung das Ergebnis in der gewünschten Qualität liefert.

Der Ablauf der gesamten Transaktion einschließlich der Teilkomponenten und Randbedingungen sieht folgendermaßen aus:

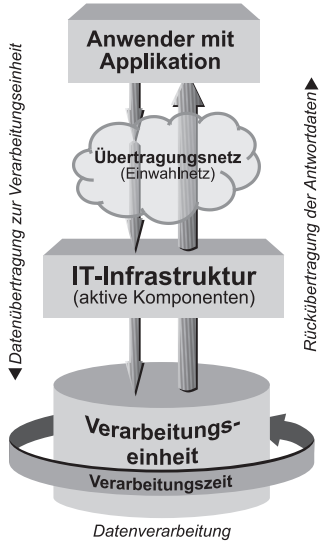


Abbildung 20.3: Übersicht über eine vollständige Transaktion

Für die Verfügbarkeit einer Funktion sind somit **alle** beteiligten Komponenten des Verarbeitungsprozesses zu betrachten und nicht nur die Komponenten der technischen IT-Infrastruktur.

20.5 Datensicherheit

Das Thema der Datensicherheit ist ein sehr sensibles Thema, da hier sehr differenzierte Betrachtungsweisen existieren, die unterschiedlichen Umgangsformen damit oft sehr kontrovers diskutiert werden und dieses Thema für sich den Umfang dieses Buches sprengen würde.

Die Sicherheit auf Datenebene sollte auch dahingehend analysiert werden, was überhaupt darunter zu verstehen ist:

- Die Daten sollten deshalb erst einmal klassifiziert werden.
- Es sollte entschieden werden, wer überhaupt auf die Daten zugreifen darf.
- Die Art des Datenzugriffes muss bestimmt werden (lesen, schreiben, manipulieren...).

20.5.1 Zugriffsberechtigung auf (elektronische) Daten

Ehe von Datenzugriffen im Firmennetz in irgendeiner Form gesprochen werden kann, ist es erforderlich, die betreffenden Personen zu erfassen und Regeln festzulegen, ob und wie sie Zugriff in das Firmennetz erhalten.

In den meisten Unternehmen werden zielgruppenorientierte Sicherheitsrichtlinien aufgestellt, die meist unter organisatorischen Aspekten wie z.B.

- unterschiedliche Benutzergruppen bzw. -profile für abgestufte Datenzugriffe,
- Zutrittsregelungen zu den Rechnerräumen etc.

erstellt werden.

Eine möglichst eindeutige Erkennung der Benutzer (z.B. durch Einsatz von Directory-Services) ist besonders in größeren Nutzergruppen wichtig, da nicht nur eindeutiges Single-Sign-On auf unterschiedlichen Wegen möglich wird, sondern eine Vielzahl firmenspezifischer Prozesse davon profitieren können.

20.5.2 Differenzierung des Datenzugriffs

Die Daten eines Unternehmens müssen den unterschiedlichen Personen mit entsprechenden Berechtigungen zur Verfügung gestellt werden. Die Art des Zugriffes (erstellen, lesen, modifizieren, löschen) wird in der Regel durch die spezielle Arbeitsaufgabe der Bearbeiter festgelegt und unterliegt firmeninternen Vorgaben. Dieser Umgang mit den Daten stellt den Regelfall dar.

Es ist aber auch erforderlich, die Art von unerlaubten Datenzugriffen zu ermitteln, um entsprechende Gegenmaßnahmen treffen zu können. Daten können

- abgehört,
- manipuliert oder auch
- vernichtet

werden.

Werden Daten durch unbefugte Personen **abgehört**, gelesen, kopiert etc., so überträgt sich auf den neuen (unrechtmäßigen) Besitzer das damit verbundene Geheimnis, das er zu seinem Vorteil auswerten kann. Der ursprüngliche (Geheimnis-)Besitzer merkt u.U. von diesem Diebstahl nichts. Auf alle Fälle verliert er sein Know-how an einen Fremden, der u.U. sein Geschäftskonkurrent ist.

Manipulierte Daten bergen eine enorme Brisanz. Werden firmeninterne Daten z.B. für eine Entscheidungsfindung herangezogen und sind diese (geschickt) manipuliert, kann das der Firma einen enormen Schaden zufügen, u.U. sogar den Ruin bedeuten. Deshalb ist es sehr wichtig, die Authentizität der Daten zu gewährleisten. Das betrifft aber nicht nur gespeicherte Daten, sondern auch solche, die von einem Partner übertragen wurden. Hier ist es zwingend erforderlich, die Identität des Absenders eindeutig zu erkennen. In der IT wird hier oft der Begriff »Man-in-the-Middle«-Angriff als Möglichkeit dargestellt, wobei sich eine dritte Person in eine Kommunikation zwischen zwei Parteien einschleicht und als der scheinbare Absender ausgibt.

Eine weitere geschäftsgefährdende Art der Datenmanipulation stellt deren **Vernichtung** dar. In der heutigen Zeit sollte diese Art des Datenzugriffs durch Unbefugte oder bedingt durch technische Fehler eigentlich keinem ordentlich geführten Unternehmen wirklichen Schaden zufügen. Voraussetzung ist allerdings, dass regelmäßig Back-Ups durchgeführt werden und eine Recovery-Strategie definiert ist. Zielgerichtete Datenvernichtung stellt allerdings eine plumpe Art der Datenmanipulation dar, da der Betroffene diesen Schaden unmittelbar erkennen und Gegenmaßnahmen einleiten kann.

20.5.3 Datenschutz und Privatsphäre

Sicherheit im Umgang mit den Daten in einem Unternehmen bedeutet letztendlich auch für den Mitarbeiter in gewisser Weise einen potenziellen Eingriff in seine Privatsphäre. Deshalb müssen hier auch Gesetzesgrundlagen beachtet werden und die Sicherheitspolicies z.B. mit dem Betriebsrat abgestimmt werden.

20.5.4 Datenschutzmöglichkeiten

In der Praxis ist es oft so, dass Teildaten, die einem Objekt zugeordnet sind, an unterschiedlichen Stellen mit differenzierten Berechtigungen benutzt und in unterschiedlichem Umfang verfügbar gemacht werden. Das trifft z.B. bei Personaldaten zu. Diese werden in der Personalabteilung, an den Arbeitsstationen für das User-Login, für Zutrittssysteme etc. benötigt.

20.5.5 Vertraulichkeit der Daten

Leider ist in vielen installierten Systemen zu bemerken, dass »einfach« bestimmte Daten speziellen Bereichen zugeordnet sind. Damit wird zwar erreicht, dass mittels Berechtigungseinschränkungen auf User-Ebene die Vertraulichkeit bestimmter Daten gewährleistet wird, aber eine eindeutige Datenverwaltung so nicht möglich ist.

Typischerweise werden Daten somit mehrfach vorgehalten und eine konsistente Datenpflege ist fast nicht realisierbar.

20.5.6 Schutz der Daten während der Übertragung

Werden Daten über entsprechende LAN-, MAN- oder WAN-Verbindungen übertragen, so ist auch hier eine Analyse hinsichtlich des Schutzbedarfs notwendig.

Daten können vor ihrer Übertragung z.B. durch die Applikation selbst so modifiziert werden, dass es einem Angreifer erschwert wird, diese Daten für seine Bedürfnisse zu verwenden.

Die Übertragungswege selbst können so abgeschottet werden, dass ein Zugriff auf die Daten erschwert wird. Dies geschieht gegenwärtig mit IP-VPN-Techniken (VPN: Virtual Private Network). Dabei gibt es verschiedene Möglichkeiten, die von Fall zu Fall verifiziert werden müssen ***[1]***.

Aber auch Techniken wie SSL (Secure Socket Layer) oder TLS (Transport Layer Secure), wie sie häufig bei Internetübertragungen zur Anwendung kommen, können u.U. ausreichenden Schutz bieten.

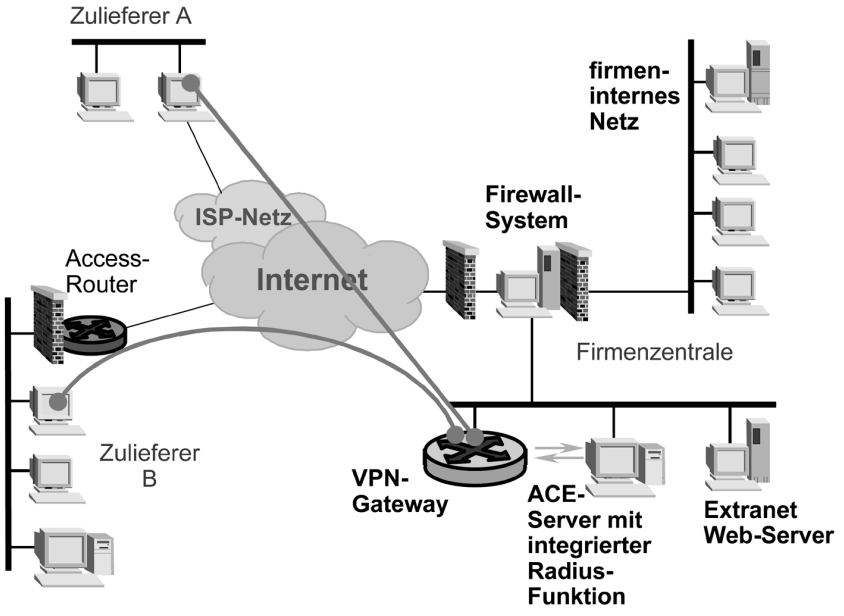


Abbildung 20.4: Mittels VPN geschützte Verbindungswege

In Zeiten der drahtlosen Netze (IEEE 802.11; IEEE802.15/Bluetooth) ist dem Schutz der Übertragungswege besondere Aufmerksamkeit zu widmen. Besonders die WLAN-Techniken (WLAN: Wireless LAN) werden in der Praxis leider sehr oft ohne ausreichende Sicherheitstechniken eingesetzt und die Daten werden jedem »Teilnehmer« am drahtlosen Datenverkehr quasi auf dem silbernen Tablett präsentiert.

Innerhalb von LAN-Netzwerken werden die verschiedensten Techniken angeboten, um einen ausreichenden Datenschutz zu bieten. So werden neben MAC- bzw. Port-basierenden Zugriffssteuerungen auch VLAN-Techniken (Virtual LAN) empfohlen. Ein einfaches Für oder Wider für die einzelnen Techniken kann pauschal nicht ausgesprochen werden. Diese Techniken bieten teilweise nur scheinbaren Schutz bzw. basieren auf proprietären Ansätzen, die den Anwender in eine Herstellerabhängigkeit zwingen können. Das ist sicherlich nicht im Interesse des Unternehmens.

20.5.7 Definition der Schutzräume

Selbstverständlich ist es das Bestreben eines jeden Unternehmens, seine Daten vor Außenstehenden prinzipiell abzuschotten. Dies erfolgte in der Vergangenheit vornehmlich durch Routertechniken in Verbindung mit entsprechenden RAS-Technologien (Remote Access Service) für definierte Einwahlaccounts. Um die wahre Identität der firmeninternen Adressräume nicht preiszugeben, wurde mittels Adressumsetzung die wahre Identität des firmeninternen Kommunikationsteilnehmers verschleiert. – Technologisch genügt dies nicht mehr den aktuellen Anforderungen.

NAT (Network Address Translation) wird zwar auch heute noch eingesetzt, aber unter dem Aspekt, Teile der Firmendaten ausgewählten Partnern effektiver und sicherheitstechnisch abgestuft zur Verfügung zu stellen, müssen zusätzliche Sicherheitstechniken eingesetzt werden.

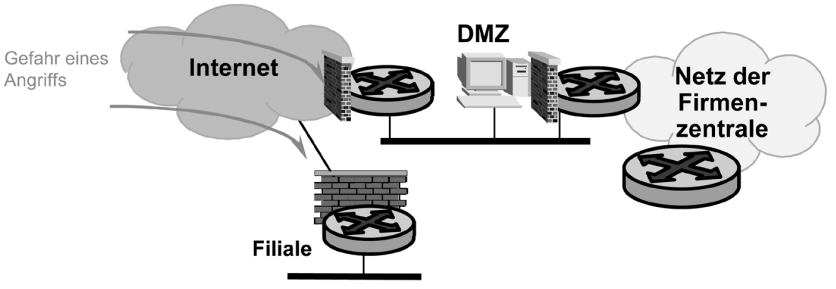


Abbildung 20.5: Abschottung der Filiale bzw. Firma mittels (einfacher) Firewall und DMZ

Aus diesem Grund haben sich in den letzten Jahren Firewall-Techniken etabliert. Mit diesen ist ein Unternehmen prinzipiell in der Lage, ein abgestuftes Sicherheitskonzept zwischen dem internen Firmennetz und dem äußeren Einwahlnetz zu realisieren. Eine hierbei häufig realisierte Sicherheitszone (DMZ: Demilitarisierte Zone) fungiert als »Schutzraum« bzw. »Pufferzone« für den Datenaustausch zwischen dem äußeren und firmeninternen Nutzerkreisen.

Um potenzielle Angriffer von außen zu erkennen, können noch zusätzlich sogenannte IDS (Intrusion Detection System) installiert werden. Diese sollen schon den Versuch eines unerlaubten Zugriffes von außen erkennen und verhindern helfen. Solche Systeme sind relativ komplex und eignen sich gegenwärtig fast nur für größere Firmen.

Die IDS-Gruppe (*http://www.intrusion-detection-system-group.co.uk/*) bietet hierzu eine Fülle von Informationen und Systemen an.

Trotz alledem darf nicht übersehen werden, dass die erwähnten Techniken prinzipiell gegen Angriffe von außen schützen sollen. Die meisten unerlaubten Zugriffe auf Daten geschehen aber immer noch innerhalb der Netzwerke.

20.6 Datensicherung

Die Datensicherung kann auf technischer Ebene durch unterschiedlichste Lösungen durchgeführt werden. Als Beispiel seien hier einige wenige stellvertretend für die Vielfalt der möglichen Lösungen erwähnt:

- Installation redundanter Komponenten zur Weiterleitung der Daten (Router, Switches etc.) inklusive der dazu erforderlichen Steuerungsprotokolle.
- Verwendung eines redundanten Verkabelungssystems im Primär- und Sekundärbereich.

- Verwendung von fehlerredundanten Speichersystemen wie z.B. durch den Einsatz von RAID-Systemen.
- Redundant installierte Serversysteme (z.B. durch Cluster-Techniken).
- Absicherung wichtiger Komponenten gegen Stromausfall bzw. -störungen z.B. durch die Installation von USV-Anlagen (USV: Unterbrechungsfreie Strom-Versorgung).

20.6.1 Behebung von Störungen

Die Behebung von Störungen muss entsprechend den gewählten Lösungen erfolgen. Da diese sehr differenziert sein können, ist die jeweilige Aktion sehr unterschiedlich in der Reaktionszeit und den damit verbundenen finanziellen Aufwändungen.

- Wird z.B. ein hoher Aufwand in die Installation redundanter Komponenten investiert, so ist das System im Fehlerfall immerhin noch arbeitsfähig und die Anstrengungen zur Wiederherstellung der vollständigen Redundanz verlangen in der Regel keinen extremen logistischen Kraftakt. Somit können auch die finanziellen Belastungen z.B. hinsichtlich teurer Wartungsverträge oder Ersatzteilhaltung reduziert werden.
- Wird dagegen keine Fehlertoleranz implementiert, so steht u.U. das System und es muss innerhalb eines definierten Zeitfensters alles unternommen werden, um dieses wieder in einen funktionstüchtigen Zustand zu bringen. In der Zeit der Nicht-Verfügbarkeit des Systems entstehen dem Unternehmen entsprechende Verluste bzw. Aufwändungen, die u.U. sehr hoch sein können.

Die Palette der Möglichkeiten ist hierbei sehr breit gefächert und muss deshalb durch eine entsprechende Analyse ermittelt und spezifisch zugeschnitten werden. Dabei ist auch zu unterscheiden, ob es sich um eine Beeinträchtigung des Systems durch eine fehlerhafte Teilfunktion oder u.U. um einen Totalausfall des Systems und seiner Wiederinbetriebnahme (Disaster Recovery) handelt.

Es ist auf alle Fälle eine möglichst genaue Aufwand-Nutzen-Betrachtung erforderlich, um genau »die richtige Lösung« für den jeweiligen Anwendungsfall zu ermitteln.

20.6.2 Lokalisierung der Daten

Und es darf auch nicht vernachlässigt werden, wo sich die Daten befinden.

- Da können einmal die Daten firmenintern und zentral für die Mitarbeiter (im weitesten Sinn) zur Verfügung gestellt werden.
- Die Daten können dezentral auf den Rechnern der Mitarbeiter abgelegt sein.

- Die Daten können aber auch Partnern, Interessenten etc. mittels externer Zugriffe (z.B. über Internet) extern verfügbar gemacht werden.

Mischformen davon sind möglich.

Ist es unter spezifischen Gesichtspunkten unumgänglich, dass Daten an unterschiedlichen Orten »parallel« abgelegt werden, so ist es zwingend erforderlich, dass eine einzelne Stelle definiert wird, an der die Daten modifiziert werden dürfen.

Es ist in so einem Fall dafür zu sorgen, dass die Ursprungsdaten an den unterschiedlichen Verfügbarkeitsorten regelmäßig aktualisiert werden. Die Daten werden somit eindeutig (im Sinne von unikat), damit Fehlinterpretationen durch unterschiedliche Dateninhalte vermieden werden können. – Dies ist aber definitiv eine aufwändige und fehlerbehaftete Möglichkeit, die möglichst vermieden werden sollte.

20.7 IT-Management

Um ein komplexes Netz mit allen seinen Komponenten richtig zu managen, müssen die einzelnen Ebenen des Netzwerkmanagements (NM) klar definiert werden. Aber schon hier können sich »die Geister scheiden«. Nach welchem Modell soll überhaupt das Management erfolgen?

Diese Diskussion verdeutlicht sehr passend, wie weit bei unterschiedlichen Betrachtungsweisen die Meinungen auseinandergehen können, obwohl doch jeder mit seinem Blickwinkel »richtig« liegt. Einige NM-Ansätze werden nachfolgend kurz diskutiert.

Vorher aber noch ein Hinweis, der leider oft übersehen wird: Das NM ist mit der günstigste Ort für einen potenziellen Angreifer, sich Zugang zu Daten zu verschaffen. Immer häufiger werden WEB-basierte NM-Lösungen eingesetzt und eine Fernwartung von Netzen realisiert. Gelingt es einem Angreifer, auf die NM-Ebene zu gelangen, so kann er sich nicht nur einen hervorragenden Überblick über das System verschaffen und das Ziel seines Angriffes relativ leicht lokalisieren, er kann u.U. die Administratoren ausschalten und somit absolute Hoheit erlangen.

Der Managementprozess lässt sich prinzipiell in Etappen unterteilen.

1. Die erste Etappe erfasst die Parameter (Monitoring).
2. Die folgende Etappe bearbeitet die Werte (Ereignisbehandlung).
3. In der dritten Etappe werden die Parameter ausgewertet und entsprechende Reporte generiert (Reporting) bzw. Ereignisse aktiviert.

Das ISO-7-Schichten-Modell

Im Netzwerkbereich wird häufig das ISO-7-Schichten-Modell zur Zuordnung von Protokollen bzw. Diensten herangezogen. Dies ist allerdings sehr technisch orientiert und für eine globale Sichtweise nicht geeignet.

Hier kommen sehr häufig NM-Systeme zum Einsatz, die ausschließlich die aktiven Komponenten eines Netzes überwachen und steuern.

Funktionsbereiche des ISO/OSI-Netzwerkmanagements

Die ISO/OSI legt fünf Funktionsbereiche für das Netzwerkmanagement fest, die als FCAPS-Managementfunktionen bekannt sind:

- **F: Fault Management** (Entdecken, Analysieren und Beheben von Fehlern (Unterstützung durch Trouble Ticket Systeme).
- **C: Configuration Management** (Einrichtung, Inbetriebnahme, Aufrechterhaltung des Betriebs, Modifikation bzw. Deaktivierung von Konfigurationen der Infrastruktur-Ressourcen).
- **A: Accounting Management** (Erfassung, Archivierung und Reporting von Zugriffen und Verbindungen und in Anspruch genommenen Netzwerkdienstleistungen und Abrechnung entsprechend einer festgelegten Tarifierung oder einer Service-Level-Vereinbarung).
- **P: Performance Management** (Bereitstellen von Informationen über die Ressourcenauslastung anhand von Leistungskenngrößen, Analyse, Auswertung und Tuning zum Ziel der Erhöhung der Netzwerkleistungsfähigkeit).
- **S: Security Management** (Überwachung und Erkennen von Sicherheitsangriffen auf das Netz. Schutz gegen Beeinträchtigung von außen als auch gegen interne Sicherheitsgefahren, Verwaltung von Benutzerkonten).

Das TMN-Modell (nach ITU-T)

Das TMN-Modell (Telecommunications Management Network) wurde von der ITU (ITU: International Telecommunication Union) entwickelt und basiert auf dem OSI-Modell, verfolgt allerdings einen objektorientierten Ansatz:

- Business-Management-Schicht: Umsetzung des Geschäftkonzeptes inklusive betrieblicher und geschäftlicher Prozesse, Erreichen des ROI (ROI: Return on Investment), Umsatz- und Ergebnisziele, Zielgruppenorientierung.
- Service-Management-Schicht: Realisierung der vereinbarten Service-Level, Dienstgüten und Kosten etc.
- Netzwerk-Management-Schicht: Mit Verbindungen, Systemen und Anwendungen, die solche Dienste bereitstellen.

- Element-Management-Schicht: Im Netz (Übertragungs- und Zugangsnetz) mit dem Ziel, Ausfallzeiten zu minimieren sowie den Durchsatz zu erhöhen, um insgesamt eine hohe Verfügbarkeit und Leistungsqualität zu garantieren.

Die Aufzählung der unterschiedlichen Sichtweisen macht deutlich, dass in den einzelnen Betrachtungsweisen und -ebenen spezifische Aufgaben bestehen, die durch entsprechende Hilfsmittel umgesetzt und realisiert werden müssen.

Günstiger erscheint beim Thema NM das ITU-Schichtenmodell. Während in der untersten Schicht die rein technischen Aspekte anzutreffen sind, werden die höheren Schichten dahingehend abstrahiert, dass in ihnen logische Dienste/Services anzutreffen sind. Das gipfelt letztendlich in der obersten Schicht, in der sich der logische Ablauf bzw. die zentralen Dienste eines Unternehmens widerspiegeln.

In dem sich also in der obersten Ebene z.B. die Sicherheitsregeln für den Umgang mit den Unternehmensdaten wiederfinden, werden in der untersten Ebene diese Anforderungen im Sinne der technischen Umsetzung wie Verschlüsselungstechniken, Passwortrestriktionen etc. umgesetzt.

In der Netzschicht (Ebene des Gerätemanagements) wird die gesamte Infrastruktur betrachtet. Zu dem Aufgaben, die hierbei zu erfüllen sind, zählen u.a.:

- Accounting-Management
- Asset-Management
- Change-Management
- Konfigurations-Management
- Netzwerk-Management
- Performance-Management
- Problem-Management
- Security-Management
- Software-Management
- Storage-Management
- User-Management
- Workload/Batch-Management

Im Bereich der IT-Infrastruktur werden die beiden unteren Ebenen (Netzwerktechnik und -dienste) betrachtet.

In der untersten Ebene (Netzwerktechnik) sind die Komponenten installiert, die die eigentliche Kommunikationsinfrastruktur bieten und deren einwandfreie Funktion die Systemverfügbarkeit realisieren. Diese werden verkörpert durch:

- Netze (Aktive Netzkomponenten wie z.B. Router, Switches)
- Übertragungswege (Kabelstrecken innerhalb des LAN, aber auch Kommunikationsstrecken im WAN wie z.B. das Telefonnetz oder auch die Internetdienste)
- Server (Server-Plattformen mit Internettechnologie-Diensten)
- Datenbanken (Zentrale Datenbank für Business-Daten)
- Firewallsysteme
- Applikationen (Zentrale Applikation für die Business-Logik)

20.8 Service Level Management

Service-Level-Management (SLM) ist ein in sich geschlossenes System von Maßnahmen, mit denen zweierlei erreicht wird:

- IT und Fachabteilungen analysieren gemeinsam die Anforderungen, die die Geschäftsprozesse der Anwender an die IT-Versorgung stellen und vereinbaren die »Lieferung« entsprechender IT-Services.
- Die tatsächlichen Leistungen der IT, egal ob gut oder verbesserungsbedürftig, werden sichtbar und objektiv messbar.

Wesentliche Bestandteile von SLM sind z.B.

- Zentraler Servicekatalog
- Servicebeschreibungen und Service Level Agreements (SLAs)
- Service Pricing
- Mess-, Reporting- und Reviewverfahren für die IT-Leistung
- Account Management
- Contracting

Für ein erfolgreiches Service-Level-Management sind die von der IT erbrachten Leistungen in Form von standardisierten IT-Services zusammenzufassen. Dieser »zentrale Servicekatalog« stellt die Grundlage für die nachfolgenden Serviceverhandlungen dar.

Alle IT-Services sind in ihrem Umfang und Inhalt detailliert zu beschreiben: Was stellt die IT bereit, welche Aktivitäten sind in dem Service enthalten, für welche Aspekte des Service ist der Anwender verantwortlich?

Nur wenn die zu erbringende Leistung anhand eindeutiger Merkmale zweifelsfrei definiert ist, kann später festgestellt werden, ob die Ziele auch erreicht wurden.

Innerhalb des SLM-Rahmenwerks wird für jeden Service ein Servicepreis verbindlich festgelegt (natürlich unter Einbeziehung der jeweiligen Servicequalität). Dies gibt Anwendern und IT Planungssicherheit und macht die IT-Leistung auch kostenmäßig mit der Leistung von externen Anbietern vergleichbar.

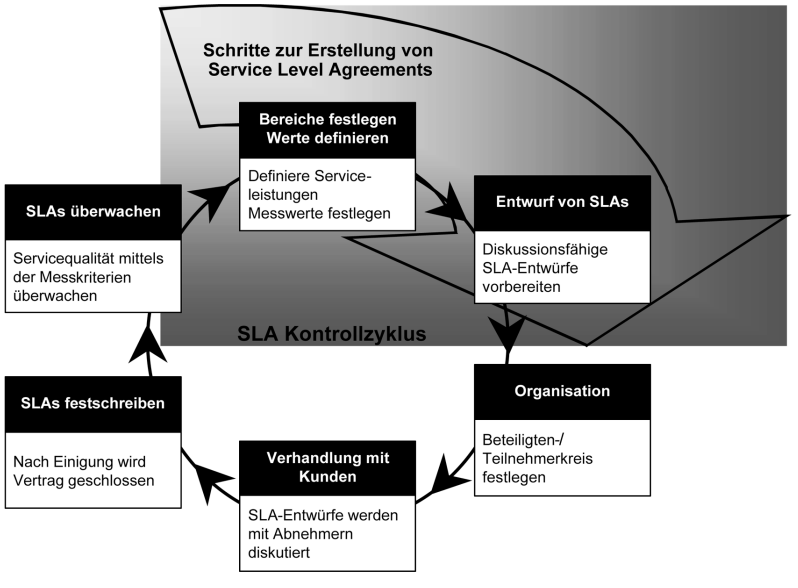
Die Einhaltung der getroffenen Service Level Vereinbarungen ist regelmäßig zu überprüfen; so wird ein Prozess der kontinuierlichen Verbesserung in Gang gesetzt. Sowohl für die Erhebung der Ist-Zahlen als auch für die laufende Kommunikation zwischen IT und Anwendern, stellt das SLM verbindliche Verfahren bereit.

Ebenso wie Leistungsanbieter regelmäßige Kundengespräche führen, sollte die interne IT ihre Beziehung zu ihrem internen »Kunden« aktiv führen und sich so als Geschäftspartner der Fachabteilung positionieren.

20.9 Service Level Agreement

Service Level Agreements (SLAs), also die Festschreibung der Leistungsinhalte und -qualitäten, sind eine wesentliche Komponente des Service Level Managements – aber eben nur ein Schritt zum Erfolg: Wenn SLAs nicht in einen ganzheitlichen Rahmen unter Beteiligung des Anwenders und des Unternehmensmanagements eingebunden sind, wird die gut gemeinte Initiative verpuffen.

Abbildung 20.6: SLA-Kontrollzyklus



Ein Service Level Agreement (SLA) stellt einen Vertrag zwischen zwei Partnern dar. In diesem wird der Umfang und die Güte eines Dienstes, den ein Dienstleistungsgeber gegenüber seinem Kunden zu erbringen hat, beschrieben und die Vertragsbedingungen schriftlich geregelt.

20.9.1 Begriffe und Inhalte

Service Level Agreements (SLA)

SLA verkörpern die Verträge zwischen einem Serviceanbieter und seinem Kunden. Dabei werden

- Art und Umfang der Dienstleistung,
- deren Dienstgüte (Güteparameter, messbare Kriterien, Qualitätserwartungen, Vorgehen bei Unterschreitungen der Dienstgüte etc.) und
- die Vertragsbedingungen

schriftlich fixiert und vertraglich geregelt.

Ein SLA besteht aus einer spezifizierten Vielzahl von Einzeldefinitionen zu Messgrößen und deren -methoden bzw. -verfahren, Erhebungszeiträumen und projektbezogenen Definitionen.

Die Messgrößen eines SLA bestehen meist aus

- den Verfügbarkeitsquoten,
- den Zeiteinheiten, in denen vereinbarte Parameter erfasst werden,
- den Dienstespezifikationen als Gegenstand der Vereinbarung,
- den Angaben zu Wartungs- und Serviceintervallen definierter Dienstleistungen etc.

Typische Parameter für einen IT-Dienst sind z.B. garantierte Antwortzeiten, oder auch Bandbreite und Verfügbarkeit von Systemen oder Funktionalitäten.

Durch die abgeschlossenen SLAs werden Verbesserungen für die Nutzung der IT-Strukturen wie z.B.

- klare Anforderungen an den Dienstleister (Zielvereinbarungen),
- eindeutige Verantwortlichkeiten und
- Qualitätssteigerung des IT-Service

angestrebt. Dadurch wird für die Vertragsbeteiligten eine klare Planungsgrundlage für die Zukunft möglich.

Die Beschreibung der SLA-Inhalte sollte sich dabei nicht nur auf die »technischen« Aspekte begrenzen. Wichtiger für den Servicenehmer ist dagegen die Formulierung der Serviceprozesse und der Servicequalität.

Die (technische) Umsetzung der Servicevereinbarung ist Aufgabe des Serviceanbieters und sollte mit geeigneten Mitteln erfolgen.

Service Level Requirement (SLR)

Ehe ein SLA ausgehandelt werden kann, muss der Dienstleistungsnehmer seine Anforderungen spezifizieren. Dies erfolgt mittels der Service Level Requirements (SLR).

Auch sollten in den SLR in der Regel höhere Anforderungen auf Seiten des Dienstleistungserbringers formuliert, als in einer später abgeschlossenen SLA vertraglich fixiert werden.

Service Level Target (SLT)

Ein professioneller Dienstleister ist bemüht, zur Erfüllung der vereinbarten SLA sich intern Ziele zu deren Erfüllung zu setzen. Diese sollten (zumindest in definierten Bereichen) höher als die eigentlich vereinbarten Leistungen sein. Dies sollte in den sogenannten Service Level Targets (SLT) fixiert werden.

20.9.2 Service Level und SLA-Inhalt

Nach erfolgter Definition der zu erbringenden Leistung kann daraus ein SLA abgeleitet werden. Die in einem SLA zu erbringenden Leistungen durch den Dienstleister müssen klar spezifiziert sein. Dadurch ist die Bestimmung der Servicequalität bzw. des Servicelevels einfacher möglich.

Ein SLA muss gemessen werden können. Die erbrachten Leistungen müssen durch den Serviceanbieter nachweisbar sein und der Kunde muss diesen Nachweis bei Bedarf ausgehändigt bekommen. Üblicherweise stellt dieser schriftliche Nachweis eine zusätzliche Leistung dar, die im SLA nicht definitiv enthalten ist. Deshalb sollte der Kunde explizit darauf hingewiesen werden, dass dies eine kostenpflichtige Position darstellt.

Im Bereich der technischen Unterstützung müssen die betroffenen Systemkomponenten identifiziert, deren Betrieb, ihre Konfiguration und die Zuständigkeiten für definierte Aufgaben festlegt werden.

Die unterschiedlichen SLA-Verträge müssen auf der Basis der verschiedensten Anforderungen durch die Kunden differenziert werden. Dazu ist eine Klassifizierung der SLA erforderlich, die den Gegenstand der zu erbringenden Dienstleistung beschreiben.

Mögliche Inhalte und Unterscheidungsmerkmale können dabei sein:

- Welche Dienste werden beansprucht (Lieferbedingungen beschreiben)?
- Festlegung der Service-Level inklusive deren Schwellwerte (Performance, Verfügbarkeit (99,x%), Latenzzeiten etc.)
- Festlegen der Garantie-Level (Gerätegarantie, Funktionsgarantie etc.)
- Formulierung der Funktionsfähigkeit geschäftskritischer Applikationen oder Systeme
- Festlegung des Hard- und Software-Equipments bei beiden Vertragspartnern

- Festlegung der Vergütungspflichten (wann?, wieviel?, in welcher Form?)
  - Verfügbarkeit bestimmter Dienste
  - Entstör- oder auch Reaktionszeit
  - Übertragungsqualität
  - Einbeziehung der Sicherheitsaspekte (Security-Policy des Unternehmens)
  - Festlegung von Messgrößen und -verfahren
  - Festlegung des effektiven Datendurchsatzes oder auch der minimalen Verlustrate

Weiterhin ist eine Differenzierung nach unterschiedlichen Erfüllungsebenen (Level) erforderlich, in denen die spezifischen Leistungen fixiert sein müssen. Diese Leistungen können z.B.

- nach Zeitzonen für die Dienstleistungserfüllung (siehe Tabelle 20.1),
- nach Reaktionszeiten (z.B. 30 Minuten),
- nach dem Grad der Erfüllung (Analyse der Fehlermeldung, Wiederherstellung der Arbeitsfähigkeit ggf. auch mit verminderten Leistungskriterien, Wiederherstellung des vollständigen Ausgangszustandes vor dem Fehlereignis etc.)

differenziert sein.

Tab. 20.1: Mögliche SLA-Kategorien nach Servicezeiten

Servicezeit		
Kategorie A	Montag bis Freitag	07.00-18.00Uhr
	Samstag	07.00-14.00Uhr
Kategorie B	Montag bis Freitag	18.00-07.00Uhr
	Samstag	14.00-24.00Uhr
	Sonntag, Feiertag	00.00-07.00Uhr
Wartungsfenster	Systemwartungsarbeiten können außerhalb der sonstigen Servicezeiten durchgeführt werden (nach vorheriger Absprache)	
Systemreboot	Zu vertraglich geregelten Zeiten wird das System neu gestartet, um das Risiko für ungeplante Ausfälle zu minimieren.	

Die Abnahmekriterien der erbrachten Leistung müssen definiert werden wie z.B. erfüllt, minder erfüllt, nicht erfüllt.

Weiterhin sind neben der Formulierung des finanziellen Vertragsangebotes auch die Ansprüche des Dienstleistungsnehmers bei Nichterfüllung zu formulieren (Regressansprüche).

Es ist eine Notfallplanung und die Festlegung von Eskalationsmechanismen zu realisieren. Für die unterschiedlichen SLA werden zunehmend die verschiedenen Formen des Reportings durch den Auftragnehmer wichtig. Diese müssen definiert und kontrolliert werden.

Zusätzlich ist die Festlegung einer Leistungsverrechnung erforderlich.

Die nachfolgende Tabelle bietet einen kleinen Überblick über verschiedene SLM-Anbieter.

Tab. 20.2: Einige Anbieter von SLA- und SLM-Produkten

Anbieter	Adresse
BMC Software Inc.	*http://www.bmc.com*
Cisco	*http://www.cisco.com/warp/public/cc/pd/wr2k/svmnv1/prodlit/_de_slm_ds.htm*
ClarITeam	*http://www.susanne-schulze.de/01.htm*
Contix	*http://www.contix.de/homepage/docs/leist-slm.htm*
Debis	*http://www.debis.at/6/6311i.htm*
Education Helpdesk	*http://www.edu-helpdesk.ac.at/it-manag.htm*
ete-hager AG	*http://www.ete-hager.ch/ete_neu/deutsch/about_mf_d.htm*
Everest	*http://www.clearview.de/whitepapers/index.html*
GENERELL COMPUTER AG	*http://www.generell.com/serviceCtr.html*
Infovista	*http://www.indigo.at/indigoCS/lecturelunch/infovista/sld001.htm*
Intellivision Networks AG	*http://www.intellivision.de/*
Intus Datadesign AG	*http://www.intusdata.ch/unser/Dienstleis-tungen.htm*
IS Management Group GmbH	*http://www.ismgroup.ch*
PS'SOFT Inc. USA	*http://www.pssoft.net/deutsch/easy_de.htm*
Restorage gmbh	*http://www.restorage.ch/sla.htm*
Siemens	*http://w3.siemens.de/solutionlife/_online_lexikon/3/f009833.htm*
Simac	*http://www.simac.de/news_d/html/news.html*
Swiss Warehouse	*http://www.swiss-warehouse.ch*
Trikom	*http://www.trikom.de/slm.htm*
TSG – The Sourcing Group	*http://www.tsgag.com/vebs/3.shtml*
Visual Networks	*http://www.visualnetworks.com*

Literatur. *[1]* Jörg Buckbesch, Rolf-Dieter Köhler: VPN-Virtuelle Private Netze, Sichere Unternehmenskommunikation in IP-Netzen; Fossil-Verlag Köln; 2001; ISBN: 3-931959-34-1.

A Abkürzungen

3GPP	3. Generation Partnership Projekt
ACK	Acknowledge
AES	Advanced Encryption Standard
AFIS	Automatisches Fingerabdruck Identifizierungssystem
AGB	Allgemeine Geschäftsbedingungen
API	Application Program Interface
ASCII	American Standard Code for Information Interchange
b2b	Business to Business
b2c	Business to Customer
BAFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
Bit	Binary Digit
BKA	Bundeskriminalamt
BMeldDÜV	Bundesmeldedaten-Übermittlungsverordnung
BMI	Bundesministerium des Innern
BMWI	Bundesministerium für Wirtschaft und Technologie
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authorities
CC	Common Criteria
CERT	Computer Emergency Response Team
CoP	Code of Practice
CRC	Column-Row-Checksum
CRM	Customer Relationship Management
CSI	Computer Security Institute
CSO	Chief Security Officer
DB	Datenbank
DES	Data Encryption Standard
DIN	Deutsches Institut für Normung

DLL	Dynamic Link Library
DMZ	Demilitarisierte Zone
DNS	Domain Name Service
DoS	Denial-of-Service
DSMeld	Datensatz für das Meldewesen
DV	Datenverarbeitung
E	Elektronisch
EDV	Elektronische Datenverarbeitung
EN	Europäische Norm
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
EW	Eintrittswahrscheinlichkeit
EWO	Einwohner-Meldewesen
FBI	Federal Bureau of Investigation
FCAPS	Fault-, Configuration-, Accounting-, Performance-, Security-Management
FIPS	Federal Information Processing Standards
G2C	Government to Citizen
G2G	Government to Government
GSHB	Grundschutzhandbuch
GSM	Global Systems for Mobile communications
HBCI	Homebanking Computer Interface
HR	Human Ressource
HTTP	Hypertext Transport Protocol
HTTPS	HTTP über SSL (Secure-Socket-Layer)
I	Immateriell
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection Systems
IEC	International Electronical Commission
IPSec	IP Security Protocol
ISIS-MTT	Industrial Signature Interoperability Specification-Mailtrust
ISMS	Informationssicherheits-Managementsystem
ISO	Internationale Organisation für Standardisierung
IT	Informationstechnologie
ITU	International Telecommunication Union
IuKDG	Informations- und Kommunikationsdienste-Gesetz

KontraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KoopA-ADV	Kooperationsausschuss Automatisierte Datenverarbeitung Bund, Länder, Kommunaler Bereich
KWG	Gesetz über das Kreditwesen
LAN	Local Area Network
M	Materiell
MD5	Message Digest 5
MK	Mechanismusklassen
MMS	MultiMedia Services
MPL	Maximum Possible Loss
MSA	Maximale Schadenshöhe
MTBF	mean-time between failure
NAT	Network Address Translation
NBS	National Bureau of Standards
NIST	National Institute of Standards and Technology
NM	Netzwerkmanagement
NSA	National Security Agency
OP	Open Platform
OSCI	Online-Services-Computer-Interface
OSPF	Open Shortest Path First
ÖV	Öffentliche Verwaltung
P	Personell
PDA	Personal Digital Assistant
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PIN	Personal Identifikation Number
PKI	Public Key Infrastructure
PML	Probable Maximum Loss
PP	Protection Profile
PSE	Personal Security Environment
QM	Qualitätsmanagement
QMS	Qualitätsmanagementsystem
RAP	Risk Activity Plan, Risiko Aktivitäten Plan
RAS	Remote Access Service
RBAC	Role Based Access Control
RegTP	Regulierungsbehörde für Telekommunikation und Post

RIP	Router Information Protocol
ROI	Return on Investment
RSA	Verschlüsselungsverfahren nach Rivest, Shamir, Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAGA	Standards und Architekturen für E-Government Anwendungen
SDK	Software Development Kit
SECCOS	Secure Chipcard Operating System
SECMAN	Security Manager
SigG	Signaturgesetz
SigV	Signaturverordnung
SIM	Subscriber Identity Module
SLA	Service Level Agreement
SLM	Service Level Management
SLR	Service Level Requirement
SLT	Service Level Target
SSL	Secure-Socket-Layer
ST	Security Target
SYN	Synchronization
TAN	Transaction Number
TCP/IP	Transmission Control Protocol/Internet Protocol
TIM	Telecom Italia Mobile
TLS	Transport Layer Secure
TMN	Telecommunications Management Network
USIMs	SIM-Karte des UMTS-Netzwerks
USV	Unterbrechungsfreie Strom-Versorgung
VLAN	Virtual LAN
VM	Virtual Machine
VPN	Virtuale Private Network
WAN	Wide Area Network
WLAN	Wireless LAN
WWW	World-Wide-Web
XML	eXtensible Markup Language
ZKA	Zentraler Kreditausschuss
ZPO	Zivilprozessordnung

B Autorenprofile

B.1 Herausgeber

Walter Gora

Walter Gora, Jahrgang 1960, beendete sein Studium der Informatik und der Betriebswirtschaftslehre an der Universität Erlangen-Nürnberg im Jahre 1984, war anschließend als wissenschaftlicher Mitarbeiter tätig und promovierte dann als Dr.-Ing. mit einer Arbeit zum Netzmanagement. Für die Philips Kommunikations Industrie war er von 1988 bis 1990 tätig und baute dort die Abteilung »Consulting« auf. Danach wechselte er zur Diebold Deutschland GmbH, wo er zuletzt einen Fachbereich leitete. Seit 1993 ist Dr. Gora geschäftsführender Gesellschafter von Gora, Hecken & Partner (GHP) und in Projekten mit den Schwerpunkten Organisation und Informations- und Kommunikationstechnik tätig. Nach dem Merger von GHP mit der CITAG AG im April 2002 wurde er Vorstand bei der jetzigen C_sar – Consulting, solutions and results AG, einer Management- und Technologieberatung mit Hauptsitz Frankfurt am Main.

Thomas Krampert

Dipl.-Ing. Thomas Krampert, Jahrgang 1964, war nach seinem Studium der Feinwerktechnik von 1991 bis 1995 als selbständiger Ingenieur für verschiedene Industrieunternehmen beratend tätig. Danach wechselte er für zwei Jahre zu einem Systemhaus und Funknetzbetreiber einer deutschen Konzerngruppe, wo er für den Vertriebssupport zuständig zeichnete. Seit 1997 ist Thomas Krampert als Leiter des Competence-Centers »IT-Sicherheit« bei der damaligen Management- und Technologieberatung Gora, Hecken & Partner (GHP) in Projekten mit den Schwerpunkten Kommunikation und Netze tätig. Nach dem Merger von GHP mit der CITAG AG im April 2002 wurde er Partner bei der jetzigen C_sar – Consulting, solutions and results AG. In seiner Funktion hat er zahlreiche IT-Sicherheitskonzepte und -projekte verantwortet. Er ist weiterhin lizenzierter IT-Grundschutz-Auditor des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

B.2 Autoren

Astrid Albrecht

Astrid Albrecht, Volljuristin, befasst sich seit mehreren Jahren im Querschnittsbereich von Recht und Technik mit modernen Informations- und Kommunikationstechnologien. Sie ist beim Bundesamt für Sicherheit in der Informationstechnik für die Bereiche Biometrie und elektronische Signaturen zuständig. Zuvor hat sie in rechtlicher und gesellschaftspolitischer Hinsicht für den Verbraucherzentrale Bundesverband dessen Beteiligung am Projekt BioTrusT geleitet. Sie ist Vorsitzende der Arbeitsgruppe 6 »Biometrische Identifikationsverfahren« des TeleTrusT e.V. Astrid Albrecht hat zahlreiche Beiträge zu rechtlichen Fragen der Informationsgesellschaft veröffentlicht, darunter ein Gutachten für den Deutschen Bundestag zu rechtlichen und verbraucherpolitischen Aspekten der Biometrie. Sie wird regelmäßig als Referentin zu nationalen wie internationalen Konferenzen und Workshops eingeladen.

Oliver Berndt

Dipl.-Wirtsch.-Ing. Oliver Berndt, Jahrgang 1958, studierte zunächst Elektronik und Wirtschaft und schloss dann ein weiteres Studium an der Universität of New Mexico, USA an. Von 1984 bis 1989 war er bei NCR und Siemens in Support und Produktplanung tätig. 1989 begann die Beratungslaufbahn bei der Diebold Unternehmensberatung. In den nachfolgenden sechs Jahren hat er mehrere Unternehmensberatungen als selbständiger Berater im Bereich Netzwerke, Dokumenten-Management und neue Technologien unterstützt. Seit 1999 arbeitet Oliver Berndt als Chefberater und jetzt als Partner bei der C_sar – Consulting, solutions and results AG bzw. dem Vorgängerunternehmen GHP. Er ist Leiter des Geschäftsbereiches »Utilities« und berät mit den Schwerpunkten branchenspezifische Prozesse, E-Business, Dokumenten-Management, E-Signatur und Workflow.

Frank Bourseau

Dr. math. Frank Bourseau, Jahrgang 1963, war nach seinem Studium der Mathematik und anschließender Promotion von 1995 bis 1998 als Berater und Senior-Berater im Anwendungsentwicklungsbereich mit Spezialisierung auf Datenbanken tätig. Danach wechselte er in den IT-Sicherheitsbereich des Informatikzentrums der Sparkassenorganisation (SIZ) in Bonn, wo er von 1998 bis 2001 als Referent und Teamleiter verantwortlich für den Themenbereich Sicherheitstechnologie war. Seit 2002 ist er IT-Security Manager

bei der dvg mbH in Hannover mit den Schwerpunkten Sicherheitsmanagement und Policies. Er ist weiterhin Lead-Auditor für den Informationssicherheitsstandard BS 7799 der British Standards Institution (BSI).

Ulrich Falke

Ulrich Falke, Jahrgang 1956, ist Freier Journalist in Berlin und arbeitet seit zwei Jahren auch für die C_sar AG, zuvor Gora, Hecken & Partner Management- und Technologieberatung GmbH. Zudem lehrt er seit einigen Jahren als Mentor Politikwissenschaft am Fernstudienzentrum der Humboldt-Universität zu Berlin. Mit Beginn seines Studiums der Publizistik, Politologie und Philosophie an der Freien Universität Berlin und an der University of Arkansas, USA, Ende der 70er Jahre bewegt er sich in dem Bereich der Kommunikation. Seine bisherigen beruflichen Stationen sind neben seinen journalistischen Tätigkeiten für verschiedene Redaktionen bei Presse und Rundfunk: Redenschreiber für die Berliner Bürgermeisterin und Senatorin Ingrid Stahmer, Berater im Präventionsprojekt »Aids in der Arbeitswelt« der Berliner Gesundheitsverwaltung, PR-Redakteur und Leiter der Öffentlichkeitsarbeit der OSB Sportstättenbauten GmbH. Heute publiziert er vor allem in Fachzeitschriften und Titeln wie Computerwoche, c't, Netzwert (Handelsblatt), Mittelstandsmagazin oder Behörden Spiegel.

Christian Friberg

Dr. rer. nat. Christian Friberg, Jahrgang 1968, studierte von 1989 bis 1994 Informatik und Mathematik an der Christian Albrechts Universität zu Kiel. Während seiner anschließenden Promotion spezialisierte er sich auf Sicherheitsverfahren im Bereich Netzwerke und Betriebssysteme und schrieb seine Arbeit über rollenbasierte Zugriffskontrolle in Mehrbenutzerbetriebssystemen. Seit 1999 arbeitet er bei der PPI Financial Systems GmbH und ist dort Projektleiter für die bankseitige Implementierung von HBCI (Home Banking Computer Interface) und interne Projekte über Sicherheit und Wissensmanagement.

Carsten Gerhardt

Carsten Gerhardt, Jahrgang 1974, ist Student am Lehrstuhl von Professor Luttenberger und beendet sein Studium der Ingenieursinformatik mit seiner Diplomarbeit über Einsatzmöglichkeiten des BSI-GSHBs bei der PPI Financial Systems GmbH. In mehreren Tätigkeiten als Werkstudent beschäftigte er sich mit der Implementierung von Verfahren zur Qualitätssicherung nach ISO 9000 und workflow-unterstützenden Kommunikationssystemen mit Webinterface.

Walter Hammerschmid

Ing. Walter Hammerschmid, Jahrgang 1958, war nach der Ausbildung zum Nachrichtentechniker an der Höheren Technischen Bundes Lehr- und Versuchsanstalt zu (Wien) und von 1977 bis 1981 im Biotechnischen Labor des Ludwig Bolzman Institut (Wien) als freier Mitarbeiter beschäftigt. Bei den Projekten »Künstliches Herz« und »Reaktivierung des Bewegungsapparates von Querschnittsgelähmten« konnte er die ersten praktischen Hard- und Software-Erfahrungen mit Mikroprozessor- Steuerungen machen. Danach lag der berufliche Schwerpunkt im Bereich Software-Entwicklung. Bei einem Personal Leasing Unternehmen (IVM) sowie bei Alcatel Österreich wurden von ihm unter anderem ein Zugsüberwachungsprogramm für die ÖBB Tauernstrecke und halbautomatische Prüfplätze im Bereich Telefonie entwickelt. Von 1991-1999 war Walter Hammerschmid bei den Österreichischen Lotterien tätig, wobei er dort den Bereich IT-Security gründete und leitete. Danach wechselte er zu einem Internet Provider, bei dem er ebenfalls für die Sicherheit verantwortlich war. Seit 2001 ist er beim Projekt »elektronischer Krankenscheinersatz« des Hauptverbandes der österreichischen Krankenkassen für alle Sicherheits- und kryptografischen Belange verantwortlich.

Hansjörg Höltkemeier

Hansjörg Höltkemeier, geboren 1964, ist Managing Director »EDS Solutions Consulting« und Partner des EDS-Tochterunternehmens »C_sar Consulting - solutions and results AG«. Dabei begleitet er sowohl traditionelle (Groß-) Unternehmen und Behörden als auch innovative Start-Up-Companies bei der Entwicklung und Implementierung von innovativen Strategien und Systemen für eine erfolgreiche Positionierung und Marktbehauptung in der Digital Economy. Vorangegangen waren – ebenfalls im Umfeld des Internet – leitende Tätigkeiten bei der gedas GmbH (Leiter Neue Medien) und in der Contact Consulting Services (Inhaber, Partner mit Schwerpunkt Medien). Seit 1995 beschäftigt sich Herr Höltkemeier zudem parallel auch wissenschaftlich und in der Lehre mit den Auswirkungen des Internet auf Marketing und Management. Seine berufliche Laufbahn begann er zuvor im Marketing, wo zunächst als Consultant und späterer Berliner Niederlassungsleiter der debis Marketing Services GmbH sowie nachfolgend als Marketingleiter der Q-Bus GmbH tätig war.

Rolf-Dieter Köhler

Dipl.-Ing. Rolf-Dieter Köhler, Jahrgang 1955, studierte bis 1981 an der heutigen TU Chemnitz (damals: TH Karl-Marx-Stadt) Informationstechnik. Nach einigen Jahren als Mitarbeiter in der Forschung und Entwicklung für die Steuerungsentwicklung und rechnergestützte Produktionsprozesse arbeitete er von 1989 bis 2000 als Support-Ingenieur und als Senior Network Consultant vornehmlich an der Konzipierung und Überwachung mehrerer Großprojekte. Seitdem ist Rolf-Dieter Köhler als Seniorberater bei der damaligen Management- und Technologieberatung Gora, Hecken & Partner (GHP) - jetzigen C_sar – Consulting, solutions and results AG für die strategische Restrukturierung großer Netzwerke verschiedener Unternehmen verantwortlich. Weiterhin hat er bisher sechs Fachbücher sowie ca. 35 Fachartikel veröffentlicht.

Henryk Konhäuser

Henryk Konhäuser, 47 Jahre alt, befasst sich sowohl praktizierend wie auch beratend seit mehr als 25 Jahren mit der Professionalisierung und Optimierung des Risiko-Management-Prozesses. So übernahm er nach seinem Berufsstart im Staatsdienst, bereits 1976 Aufgaben im Sicherheitsmanagement, Personenschutz und in der Revision der Tengelmann-Gruppe. Nach seiner zweijährigen Qualifikation zur Führungskraft für Betriebs- und Wirtschaftssicherheit, konzipierte er ab 1984 für den Schweizer ADIA-Konzern neue Dienstleistungen rund um das Thema Risiko- und Sicherheitsmanagement und führte diese in der Region Deutschland ein. Im Jahre 1990 wechselte er zum schwedischen Sicherheitskonzern SECURITAS, um dort als Berater den Geschäftsbereich Risikomanagement gesamtverantwortlich aufzubauen. Seine heutige Tätigkeit bei authentos, einem internationalen Authentifizierungskonzern, begann 1996. Hier war er zunächst mit dem Aufbau eines Sicherheits-Management-Systems für die Chipkarten produzierende ORGA-Gruppe betraut. Es folgte die Einführung eines Risiko-Management-Systems und die verantwortliche Übernahme der Abteilung Konzernrisikomanagement bei authentos. Die Integration ständig evaluierter Risiko-Management-Elemente in komplexe Managementsysteme gehört zu seinen Spezialgebieten. Richtungsweisende Terminologien, Prozessorientierung und Praxisbezug prägen seine heutige Risk Management Methodology.

Uwe Krieger

Uwe Krieger, Jahrgang 1963, ist Mitglied der Geschäftsleitung sowie Leiter des Bereiches Research bei der cv cryptovision GmbH in Gelsenkirchen, für die er seit 1999 tätig ist. Er ist verantwortlich für das kryptografische Know-how der Firma und damit zuständig für den Wissenstransfer und die Unterstützung der verschiedensten Bereiche des Unternehmens. Als Diplom-Mathematiker, der seit Mitte der neunziger Jahre im Bereich der Kryptografie arbeitet, legt er seinen Schwerpunkt auf die mathematischen Grundlagen der Kryptografie, speziell im Bereich der Public Key Verfahren.

Luttenberger, Norbert

Prof. Dr.-Ing. Norbert Luttenberger studierte Elektrotechnik an der TU Braunschweig. Von 1977 bis 1984 arbeitete er im Bereich Automatisierungstechnik der Siemens AG in Erlangen. 1984 wechselte er an den Lehrstuhl für Rechnerarchitektur und Verkehrstheorie (Prof. Dr. U. Herzog) der Universität Erlangen-Nürnberg, wo er zum Dr.-Ing. promoviert wurde. Danach war er am Europäischen Zentrum für Netzwerkforschung der IBM in Heidelberg in den Bereichen Multimedia-Kommunikation und Mobile Datenkommunikation tätig. Von 1995 bis 2000 war er Professor für Datenübertragung und Netzwerke im Fachbereich Informatik der Fachhochschule Gelsenkirchen. Seit Oktober 2000 bekleidet er die Professur für Kommunikationssysteme am Institut für Informatik und Praktische Mathematik der Christian-Albrechts-Universität zu Kiel. Seine Forschungsgebiete sind Mobilität und Sicherheit sowie Datenschutz.

Thomas Mai

Dipl.-Ing. Thomas Mai, Jahrgang 1964, hat nach seinem Studium des Bauingenieurwesens noch einen Abschluss im Fach TQM (Total Quality Management) erworben. In den Jahren 1994 bis 2001 war er in einigen Unternehmen speziell mit dem Aufbau und der Weiterentwicklung des jeweiligen QM-Systems beauftragt. Seit 2001 ist Thomas Mai als Consultant bei der damaligen Management- und Technologieberatung Gora, Hecken & Partner (GHP) - jetzigen C_sar – Consulting, solutions and results AG für die Erarbeitung von IT-Sicherheitskonzepten verantwortlich. Thomas Mai ist seit 2000 geprüfter DGQ-Auditor.

Isabel Münch

Dipl.-Math. Isabel Münch war nach ihrem Studium der Mathematik mit Nebenfach Informatik an der Universität Bonn von 1990 bis 1993 Mitarbeiterin beim debis Systemhaus GEI in der Abteilung IT-Sicherheit. 1994 ist sie als Referentin im Bundesamt für Sicherheit in der Informationstechnik (BSI) eingestiegen. Seit 2002 ist Isabel Münch Referatsleiterin für Systemsicherheit und IT-Grundschutz im BSI. Ihre Arbeitsschwerpunkte sind die Weiterentwicklung des IT-Grundschutzhandbuchs (Standardsicherheitsmaßnahmen für IT-Systeme), die Leitung und Koordination von IT-Sicherheitsanalysen und IT-Sicherheitsberatung mit Schwerpunkten Bankenbereich und E-Commerce. Außerdem vertritt sie das BSI in verschiedenen nationalen und internationalen Gremien mit dem Schwerpunkte IT-Sicherheitsmanagement. Neben dem IT-Grundschutzhandbuch zeichnet sie noch für zahlreiche andere Veröffentlichungen verantwortlich, z.B. die Werke »IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft« und »Sicherheitsaspekte bei Electronic Commerce«.

Harald Niggemann

Dr. Harald Niggemann, geboren 1970, Diplom-Physiker, ist stellvertretender Leiter des Referats Systemsicherheit und Grundschutz im Bundesamt für Sicherheit in der Informationstechnik (BSI). Er ist unter anderem zuständig für den Bereich IT-Sicherheitsanalyse von Gesamtlösungen und ist Mitglied des IT-Grundschutz-Teams im BSI. Seine aktuellen Tätigkeitsschwerpunkte umfassen die Einführung des Zertifizierungsschemas für IT-Grundschutz sowie die Fortschreibung der technischen und nicht-technischen Kapitel des IT-Grundschutzhandbuchs und weiterer Kriterienwerke im Bereich IT-Sicherheit. Auch die Abstimmung der beiden BSI-Werkzeuge USEIT und GS-TOOL mit den Vorgaben des IT-Grundschutzhandbuchs gehört - wie auch die Durchführung von Schulungsveranstaltungen der IT-Grundschutz-Auditoren - zu seinen Aufgaben.

Sachar Paulus

Dr. Sachar Paulus ist Leiter des Produktmanagements für Sicherheit der SAP AG. Sein Team koordiniert Sicherheitstechnologie, sichere Entwicklung und die Bearbeitung von Sicherheitsvorfällen für alle SAP Applikationen. Bevor er zur SAP gekommen ist, war er als Consultant für SECUDE GmbH and KOBIL Systems GmbH tätig, sowie wissenschaftlicher Assistent am Institut für Experimentelle Mathematik in Essen und am Institut für Theoretische Informatik an der TU Darmstadt. Herr Dr. Paulus hat in Zahlentheorie promoviert; er ist seit 1990 im Bereich der Kryptografie aktiv und hat zahlreiche

Veröffentlichungen in internationalen Magazinen und auf Konferenzen zu den Themen Kryptografie und Datensicherheit. Seine Hauptinteressen liegen in den Bereichen PKI und SmartCards sowie Geschäftsmodelle für IT-Sicherheit und IT-Riskmanagement.

Thomas Probst

Dr. Thomas Probst studierte Mathematik und Physik in Braunschweig und Kiel. Nach seiner Dissertation im Bereich der Numerischen Mathematik beschäftigt er sich seit 1999 beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein in Kiel mit Fragen datenschutz-freundlicher Technikgestaltung und der Validier- und Auditierbarkeit datenschutzgerechter Produkte. Einen Schwerpunkt bildet der Fragenkomplex »Datenschutz und Biometrie«, den er im Rahmen des Projekts BioTrusT bearbeitet. Er ist Autor und Co-Autor von Veröffentlichungen und Vorträgen zum Themenkreis (datenschutz)rechtlicher und -technischer Fragen biometrischer Verfahren.

Frank Schipplick

Dipl.-Math. Frank Schipplick, Jahrgang 1963, war nach seinem Studium zunächst als Versicherungsmathematiker bei der Europa Versicherung tätig. Von 1991 bis 1995 war er als Projektleiter im Bereich Informationssicherheit des Instituts für Informationstechnik der RWTÜV Anlagentechnik für die Evaluierung von Sicherheitsprodukten nach den europäischen Sicherheitskriterien (ITSEC) verantwortlich. Danach wechselte er für knapp drei Jahre zur Schlumberger Technologies GmbH. Dort war er als Produkt Marketing Manager und Area Sales für Chipkarten und Chipkartenterminals tätig. Von 1998 bis Juli 2002 war Frank Schipplick bei der Beratungsgesellschaft Eutelis Consult als Management Consultant für das Kompetenzzentrum »Chipkarten, elektronische Bezahlsysteme und IT-Sicherheit« verantwortlich. In dieser Position hat er diverse Sicherheitsuntersuchungen sowie zahlreiche technische und vermarktungsunterstützende Projekte in den Bereichen Chipkartenanwendungen und Biometrie erfolgreich durchgeführt. Seit August 2002 ist Frank Schipplick Executive Consultant bei der C_sar – Consulting, solutions and results AG mit den Schwerpunkten IT-Sicherheit, Chipkartenanwendungen und elektronische Bezahlsysteme beschäftigt.

Detlef Schumann

Dipl.-Wirtsch.-Ing. Detlef Schumann, Jahrgang 1960, begann seine berufliche Laufbahn als Einrichter für Automatisierungsanlagen. Während seines Studiums zum Ingenieur für Automatisierungstechnik machte er die erste Bekanntschaft mit der EDV im Jahr 1988 als Organisationsprogrammierer. Danach schlossen sich von 1992 bis 2000 weitere Tätigkeiten als Systemadministrator, EDV-Leiter und DV-Koordinator bei verschiedenen Wirtschaftsunternehmen an, wobei seine Schwerpunkte bei den Betriebssystemen UNIX und Windows NT sowie den Einsatz von ERP-Lösungen in mittelständischen Unternehmen lagen. In dieser Zeit absolvierte er ein Studium zum Diplom-Wirtschaftsingenieur. Sein Wechsel in den Consulting-Bereich erfolgte vor zwei Jahren; seit 2001 ist Detlef Schumann als Consultant bei der damaligen Management- und Technologieberatung Gora, Hecken & Partner (GHP) – jetzigen C_sar – Consulting, solutions and results AG tätig.

Frank Steimke

Dipl.-Inf. Frank Steimke, Jahrgang 1962, war nach seinem Studium der Informatik in einem großen kommunalen Krankenhaus für den Aufbau der DV-Abteilung zuständig. Während dieser Tätigkeit entwickelte sich sein besonderes Interesse für die Standardisierung der Schnittstellen unterschiedlicher DV-Anwendungen. Er war Mitglied des technischen Komitees der »HL7 Benutzergruppe« Deutschlands und hat an der Übertragung dieses amerikanischen Standards auf deutsche Verhältnisse aktiv mitgearbeitet. Seit 1999 entwickelt er als Leiter der »OSCI – Leitstelle« Protokollstandards für die öffentliche Verwaltung, die insbesondere für die Nutzung im E-Government Bereich geeignet sind. Hierzu gehören Querschnittsaufgaben wie die sichere Übermittlung elektronisch signierter Dokumente zwischen Bürgern und der Verwaltung. Ein fachlicher Schwerpunkt ist die Umsetzung E-Government im Meldewesen durch das standardisierte Datenaustauschformat »XMeld«.

Edzard van Hülsen

Dipl.-Ing. Edzard van Hülsen, Jahrgang 1944, trat nach seinem Studium der Elektrotechnik von 1966 bis 1969 als Projekt Ingenieur in das IBM Werk Mainz ein, wo er für die Qualitätssicherung von Test- und Fertigungseinrichtungen für Großrechner verantwortlich war. Ab 1973 trug er als Program Manager und Projektleiter Verantwortung für zahlreiche IBM Projekte. Er war 1990 Mitbegründer und Leiter des Service Geschäft des IBM Technischen Außendienstes für systemnahe IT Services. Bei der IBM Europa in Paris war er mehrjährig als Program Manager für die Entwicklung und Koordination

des Service Geschäfts in Zentraleuropa verantwortlich und war danach in Hamburg als Market Manager für das Service Management Geschäft verantwortlich. Seit 2000 ist Edzard van Hülsen als Seniorberater bei der damaligen neu gegründeten Consulting, Innovation und Technology AG (CITAG) eingesetzt mit den Schwerpunkten Bewertung und Optimierung von Systems Management Prozessen in Großrechenzentren. Nach dem Merger von Management- und Technologieberatung Gora, Hecken & Partner (GHP) mit der CITAG AG im April 2002 hat er in dieser Position bei der jetzigen C_sar – Consulting, solutions and results AG als Projektleiter zahlreiche Projekte geleitet, die den Kunden wertvolle Empfehlungen für Optimierungsmaßnahmen im IT Umfeld aufgezeigt haben.

Frank Wiltner

Dipl.-Inform. Frank Wiltner, Jahrgang 1969, hat nach seinem Studium der Informatik mit den Schwerpunkten Betriebssysteme und Netzwerke von 1997 bis 2000 als Consultant IT Security bei einem Dienstleistungsunternehmen für IT-Sicherheit gearbeitet. In den folgenden zwei Jahren war er bei der EDS Systematics AG als Senior Consultant und Gruppenleiter IT-Sicherheit vor allem bei der Konzeption und Einrichtung von Firewall-Systemen für diverse Unternehmen eingesetzt. Seit 2002 ist Frank Wiltner als Senior Consultant bei C_sar – Consulting, solutions and results AG mit den Schwerpunkten IT-Beratung, Sicherheits- und Risikomanagement und Konzeption von Sicherheitslösungen tätig.

Daniel Wirth

Diplom-Physiker Daniel Wirth, Jahrgang 1972, war während seines Studiums an der Universität Freiburg studentischer Mitarbeiter der Fakultät für Physik und des Rechenzentrums der Universität. Nach studienbegleitenden Tätigkeiten in der Systemadministration und der Anwenderberatung war er von 2000 bis 2002 als Senior Consultant IT-Sicherheit für die EDS Systematics AG tätig, wo er vor allem für die Konzeption und Realisierung von verschiedenen Sicherheitssystemen sowohl im Industrie- und Bankenbereich als auch im Behördenbereich zuständig war. Seit 2002 beschäftigt sich Daniel Wirth als Consultant bei C_sar – Consulting, solutions and results AG mit den Schwerpunkten IT-Beratung sowie der Analyse und der Konzeption von Sicherheitslösungen.

Stichwortverzeichnis

Copyright

Zusatzdaten

Möglicherweise liegt dem gedruckten Buch eine CD-ROM mit Zusatzdaten bei. Die Zurverfügungstellung dieser Daten auf der Website ist eine freiwillige Leistung des Verlags. Der Rechtsweg ist ausgeschlossen.

Hinweis

Dieses und andere eBooks können Sie rund um die Uhr und legal auf unserer Website

(http://www.informit.de)

herunterladen