Juli/August/September 2009
www.TecChannel.de
€ 14,90 Österreich € 16,40
Benelux € 17,15 · Schweiz SFR 29,80

TECCHANNEL COMPACT

IT EXPERTS INSIDE

Alles sicher!

- Web-Anwendungen vor Angriffen schützen
- Netzwerk abschotten
- Ausfallsicherheit erhöhen
- Schutzschild für Smartphones
- Tools & Tipps für mehr IT-Sicherheit
- Rundumschutz für Windows-Server & PCs

Editorial

Trügerische Sicherheit

Ende des 15. Jahrhunderts wurden Burganlagen nutzlos. Was jahrhundertelang als Bollwerk gegen Angreifer diente, war den damals aufkommenden Kanonen schutzlos ausgeliefert. Ähnliches vollzieht sich derzeit, von vielen noch unbemerkt, bei der Absicherung von Firmennetzen. Durch eine Firewall glaubt man, vor Angreifern von außen gesichert zu sein. Doch diese greifen längst zu neuen Waffen und attackieren Web-Applikationen, Online-Shops und E-Commerce-Lösungen. Technologiebedingt bieten diese Systeme interaktive Eingabemöglichkeiten nach außen hin an. Intern müssen sie aber auf Geschäftsprozesse und Datenbanken zugreifen, die mitten im Herz der Firma liegen.

Die klassische Firewall hilft hier gar nichts mehr. Nur eine Kenntnis der typischen Schwachstellen von Web-Anwendungen, sicher entwickelte Web-Applikationen und WAFs (Web Application Firewalls) als letzter Verteidigungsring schützen heutzutage vor unkontrolliertem Datenverlust. Mit all diesen Themen beschäftigt sich das erste und auch umfangreichste Kapitel dieses TecChannel-Compacts.

Aber der Feind kommt nicht immer direkt von außen. Manipulierte oder bösartige Webseiten können Schadcode enthalten, den sich ein Mitarbeiter unbemerkt beim Surfen einfängt. Virenscanner sind dagegen ebenso nutzlos wie die eingangs erwähnten Firewalls. Dann aber erfolgt der Angriff von innen durch einen mit allen nötigen Rechten ausgestatteten Client aus dem eigenen Netzwerk. Daher widmet sich ein weiteres Kapitel dieses Compacts der Absicherung von Clients und speziell von Windows und dem Internet Explorer.

Ist auch dieser Schutzwall durchbrochen, gilt es, den Angriff so schnell wie möglich zu bemerken und den Schaden zu minimieren. Unsere Beiträge zu Intrusion Detection und zum Schutz der Server und des Rechenzentrums geben Ihnen das dafür nötige Know-how.

Ich wünsche Ihnen nun viele neue Erkenntnisse beim Lesen dieses TecChannel-Compacts und hoffe, dass Sie das Wissen aus dem Beitrag zum richtigen Verhalten nach IT-Angriffen nie benötigen werden.

Albert Lauchner

Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)
Stellv. Chefredakteur / CvD: Albert Lauchner
Redaktion TecChannel:
Lyonel-Feininger-Straße 26, 80807 München,
Tel.: 0 89/3 60 86-897, Fax: -878
Homepage: www.TecChannel.de,
E-Mail: feedback@TecChannel.de
Autoren dieser Ausgabe: Wolfgang Aigner, Johann Baumeister, Manfred Bremmer, Hans-Christian Dirscherl, Jürgen Donauer, Matthias Fraunhofer, Katharina Friedmann, Bernhard Haluschak, Wolfgang Herrmann, Peter Höpfl, Thomas Hruby, Moritz Jäger, Magnus Kalkuhl, Albert Lauchner, Stefan Marx, Walter Mehl, Harald Philipp, Ramon Schwenk, Christian Vilsbeck, Christoph Wolfert, Sebastian Wolfgarten, Max Ziegler
Verlagsleitung: Michael Beilfuß

Grafik und Layout:
stroemung GmbH (Michael Oliver Rupp, Oliver Eismann), Multimedia Schmiede, Twentyfirst Communications: B. Maier-Leppla
Titelbild: iStockphoto

Anzeigen: Anzeigenleitung: Sebastian Woerle
Tel.: 0 89/3 60 86-628
Ad-Management: Edmund Heider (Ltg.) (-127)
Anzeigenannahme: Martin Behringer (-554)
Druck: Sachsendruck GmbH, Paul-Schneider-Strasse 12, 08525 Plauen
Gesamtvertrieb: Josef Kreitmair
Produktion: Heinz Zimmermann (Ltg.) (-157)
Jahresbezugspreise:
Inland: 49,20 EUR, Studenten: 43,80 EURAusland: 52,20 EUR, Studenten: 46,80 EUR
Haftung:
Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Veröffentlichungen in TecChannel-Compact erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt. Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleiniger Gesellschafter der IDG Business Media GmbH ist die IDG Communications Media AG, München, eine 100-prozentige Tochter der IDG Inc., Boston, Mass., USA.
Verlag:
IDG Business Media GmbH, Lyonel-Feininger-Straße 26, 80807 München
Tel.: 0 89/3 60 86-0, Fax: -118
Website: www.idgmedia.de
Handelsregisternummer: HR 99187
Umsatzidentifikationsnummer: DE 811257800
Geschäftsführer: York von Heimburg
Mitglied der Geschäftsführung: Michael Beilfuß
Vorstand: York von Heimburg, Keith Arnot, Bob Carrigan
Aufsichtsratsvorsitzender: Patrick J. McGovern

TecChannel ist Mitglied der IDG Business Media GmbH und somit ein Teil der IDG-Verlagsgruppe. Darin erscheinen unter anderem auch folgende Zeitschriften:

COMPUTERWOCHE · ChannelPartner · PC WELT · Digital World
Macwelt · GameStar · CIO · GamePro

Abonnement, Einzel- und Nachbestellung, Umtausch defekter Datenträger:
TecChannel Kundenservice, Postfach 81 05 80, 70522 Stuttgart, Tel: (+49) 07 11/72 52-276, für Österreich 1/21 95 560, für Schweiz, 0 71/3 14 06-15, Fax: (+49) 07 11/72 52-377, E-Mail: shop@TecChannel.de

Inhalt

1 Schutz von Webservern

Bei der Absicherung von Webservern soll in erster Linie ein direkter Zugriff aus dem Internet über die Webserver auf vertrauliche Daten verwehrt werden. Authentisierungsmethoden, Web-Application-Firewalls und richtige Einstellungen sowie auf Sicherheit optimierte Web-Anwendungen bieten Schutz vor Angriffen.

1.1 Grundschutz für Web-Applikationen

Klassische Firewalls und Intrusion-Detection/Prevention-Systeme (IDS/IPS) können Web-Anwendungen nicht vor Hackern abschirmen. Web Application Firewalls (WAFs) sollen Angreifern auf Anwendungsebene einen Riegel vorschieben.

Der direkte Zugang in interne Firmennetze ist Hackern inzwischen weitestgehend verbaut. Firewalls und Intrusion Detection wehren die früher noch erfolgreichen Angriffe sicher ab. Doch Web-Anwendungen bieten den Hackern zunehmend die Chance, an sensible Daten zu gelangen.

Die für das Internet konzipierten Anwendungen bieten jede Menge an Angriffsfläche. Oft genügen dem Angreifer schon das Einschleusen von SQL-Kommandos über frei zugänglich Formularfelder oder die simple Manipulation von Parametern in der URL, um an interne Daten zu gelangen. Mit komplexeren Angriffsmethoden wie beispielsweise Cross-Site-Scripting und Session-Hijacking nutzen Kriminelle gezielt Problemzonen in der Web-Applikation selbst aus. Klassische, auf die Absicherung der Transportschichten konzentrierte Schutzvorkehrungen wie Firewalls und Intrusion-Detection/Prevention-Systeme (IDS/IPS) greifen hierbei nicht. Experten führen das Gros der Schwachstellen in Web-Anwendungen darauf zurück, dass das http-Protokoll nicht für die heute üblichen Applikationen konzipiert wurde. So müssen etwa aufgrund des zustandslosen Übertragungsprotokolls Sessions beziehungsweise Zustände der Anwendungen eigens definiert und sicher implementiert werden. Zusätzliche Angriffsflächen, so die mit dem Thema Web Application Security (WAS) befasste Non-Profit-Community „Open Web Application Security Project“ (Owasp, www.owasp.org), entstehen durch die Komplexität der Web-Script-Sprachen und Application-Frameworks.

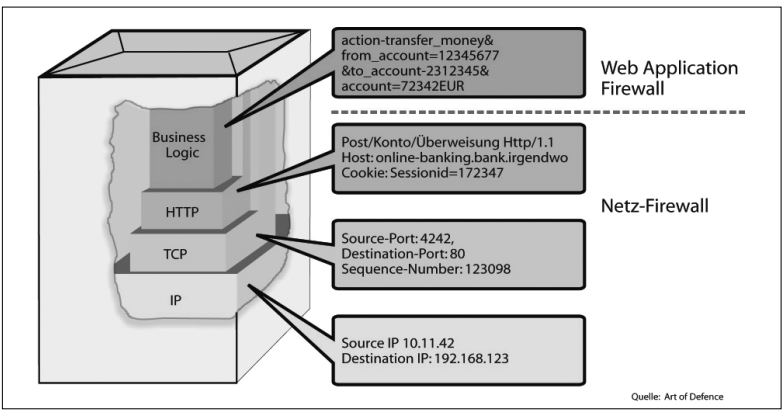
Grundsätzlich sollte die Absicherung einer Web-Anwendung bereits in der Design- beziehungsweise Entwicklungsphase beginnen. Worauf es dabei ankommt, versucht das Owasp Web-Entwicklern unter anderem mit seiner jährlich aktualisierten Liste „The Ten Most Critical Web Application Security Vulnerabilities“ (computerwoche.de Quicklink 582260) nahezubringen. Doch „sichere“ Programmierung allein reicht nicht.

„Natürlich ist es immer erstrebenswert, durch sichere Entwicklung Fehler von vornherein zu vermeiden – ganz auszuschließen sind Schwachstellen jedoch nie“, gibt Stefan Strobel, Geschäftsführer des auf Applikationssicherheit spezialisierten

Unternehmens Cirosec, zu bedenken. Aber auch regelmäßige Sourcecode-Audits, um Fehler in bereits bestehenden Anwendungen aufzuspüren und zu beheben, sind nach Erfahrung des Experten kein Allheilmittel. „Wir haben in Bankenapplikationen im Zuge von Audits Schwachstellen gefunden, deren Behebung im Endeffekt bis zu einem Dreivierteljahr in Anspruch genommen hat – unter anderem, weil sich dabei wieder neue Fehler eingeschlichen haben“, beschreibt der Berater. Während dieser Zeit ist die Anwendung angreifbar.

1.1.1 Proaktiver Schutz mit WAFs

Web Application Firewalls (WAFs) sollen auf Anwendungsebene, ganz ohne Eingriff in die Web-Applikation, dafür sorgen, dass Hacker keine Chance haben. Hauptaufgabe der WAFs ist laut Owasp, durch Penetrationstests oder Sourcecode-Audits aufgespürte Sicherheitslücken in produktiven Web-Anwendungen möglichst schnell abzudichten. Eine WAF arbeitet damit vollkommen anders als die Netzwerk-Firewall, die primär nur analysiert, woher Datenpakete kommen und wohin sie geschickt werden. Eine WAF, die auf sämtliche vom Browser an den Web-Server geschickten Daten zugreifen kann, interpretiert hingegen den Datenfluss. So kann sie Anfragen mit verdächtigem Inhalt unterbinden.



Sicherheitsstruktur: Einbindung einer Web Application Firewall (WAF)

Suspekte Aktionen erkennt eine WAF ähnlich wie Virenscanner mittels Regeln, Signaturen oder auch integrierten heuristischen Verfahren. Mittlerweile arbeiten auch WAFs meist nicht mehr nur mit einer Blacklist, die anhand bekannter Angriffsmuster nachweislich bösartige Anfragen unterbindet. Sie nutzen auch Positivlisten, mit deren Hilfe alles abgelehnt wird, was das Regelwerk nicht explizit erlaubt. So kann sie auch unbekannte Attacken abwehren.

Verschiedenste Lernmodi, die es ermöglichen sollen, die aufwändige Pflege der Whitelists weitgehend zu automatisieren, sind zumindest bei führenden Anbietern im WAF-Segment wie Citrix, Barracuda Networks (nach der Übernahme von Netcontinuum) oder auch F5 mittlerweile Standard. Diese Hersteller vereinen in ihren Gateways WAFs mit Funktionen wie Load-Balancing und Caching. „Es gibt sowohl statische Lernfunktionen, die den Administrator vor der Inbetriebnahme schützen, als auch dynamische Modi, die während der Laufzeit die individuelle Benutzer-Session verfolgen und Zustände zu vorhergehenden Zeiten mit Zuständen zu nachfolgenden Zeiten vergleichen", so Security-Spezialist Strobel.

1.1.2 Links überprüfen

Die Dynamik lässt sich beispielsweise über eine Statustabelle im Hauptspeicher der WAF erzielen, die sich alle aus der zu schützenden Web-Anwendung ausgehenden Links beziehungsweise URLs „merkt" und nur die registrierten zulässt. Der Schweizer WAF-Anbieter Visonys (www.visonys.com) wiederum realisiert dies in seinem als Software-Appliance konzipierten Produkt „Airlock" mittels URL-Verschlüsselung.

Dabei analysiert Airlock alle aus der Web-Applikation kommenden HTML-Dokumente auf dem Weg zum Benutzer und chiffriert die darin befindlichen Links, so dass sie nicht mehr modifizierbar sind. „Man muss also nur einen einzigen unverschlüsselten Einstiegspunkt definieren – in der Regel die Startseite. Alle weiterführenden Links, Dokumente sowie sämtliche Navigationspfade innerhalb der Web-Anwendung sind dann verschlüsselt -und zwar nicht nur auf Verbindungsebene wie bei einer SSL-Verschlüsselung, sondern die URL beziehungsweise die in der Browser-Zeile sichtbare Adresse selbst", erläutert Daniel Estermann, Geschäftsführer bei der Visonys Deutschland GmbH, das Funktionsprinzip.

Laut Thomas Schreiber, Geschäftsführer bei der auf Web-Applikationssicherheit spezialisierten Securenet GmbH, lassen sich mittels URL-Verschlüsselung gleich mehrere Übel an der Wurzel packen und eine ganze Klasse von Angriffsformen auf die Session-ID, etwa Session-Hijacking, -Fixation,- Denial-of-Service sowie -Riding, verhindern helfen. Auch könnten damit die Möglichkeiten der URL-Parameter-Manipulation, die Angreifern etwa dazu dienen können, sich höhere Zugriffsrechte zu verschaffen, deutlich eingeschränkt werden.

1.1.3 Best-of-Breed statt All-in-one

Dieses Feature hat mittlerweile auch Art of Defence (www.artofdefence.com) seiner WAF-Lösung „Hyperguard" spendiert. Die Schutzsoftware des Regensburger Unternehmens stellt in gewisser Weise einen Exoten unter den in der Regel vor den Web-Servern platzierten, als Softwarelösungen oder Hardware-Appliances konzipierten WAFs dar: Das Host-basierende Hyperguard lässt sich als Plug-in di-

rekt im Web-Server installieren, kann aber auch in anderen Wirtssystemen wie Load Balancern (ZXTM von Zeus Technology), Reverse Proxys (etwa Microsoft ISA-Server) oder als Add-on in Netz-Firewalls (Genuscreen von Genua) sitzen. „Wir versuchen, das Thema Web Application Security als Best-of-Breed-Lösung für den Kunden dort abzubilden, wo er es haben möchte", beschreibt Georg Heß, CEO bei Art of Defence, den WAF-Ansatz seines Unternehmens.

Ziel sei es, den sehr unterschiedlichen Ausgangssituationen und Zukunftsvisionen in den Unternehmen gerecht zu werden. Als Vorteile des Plug-in-Prinzips insbesondere für schnell wachsende, verteilte Infrastrukturen hebt Heß die einfache Installation sowie hohe Skalierbarkeit von Hyperguard hervor. Zudem soll es das „Application Defence Center" der WAF ermöglichen, sämtliche, selbst nicht inhouse befindliche, sondern auf Rechenzentren verschiedener Partnerunternehmen verteilte Hyperguard-Instanzen zentral zu überwachen und zu verwalten. „Dies ermöglicht es Unternehmen, den Überblick über dezentrale Strukturen zu bewahren und ihre Web-Applikationen separat im Blick zu behalten."

Neben dem grundsätzlichen Schutz gegen Hacker-Attacken auf Anwendungsebene bieten heutige WAFs auch applikationsübergreifende Sicherheitsdienste wie beispielsweise Single-Sign-on-Möglichkeiten (SSO) mit vorgelagerter Authentifizierung – so etwa Visonys Airlock. Die Integration der Authentifizierung in die WAF ermögliche neben zusätzlicher Sicherheit Kosteneinsparungen bei der Applikationsentwicklung, da diese nicht mehr jeweils eigens implementiert werden müsse, so Visonys' Deutschland-Chef Estermann. Als weiteres Beispiel für Aufgaben, die sich zentral an eine WAF delegieren lassen, nennt Securenet-Experte Schreiber die Abwehr so genannter Data-Mining-Angriffe, sprich: den Schutz vor dem ungewünschten Auslesen der gesamten Datenbank durch das Senden Tausender Requests mit jeweils variierendem Parameter.

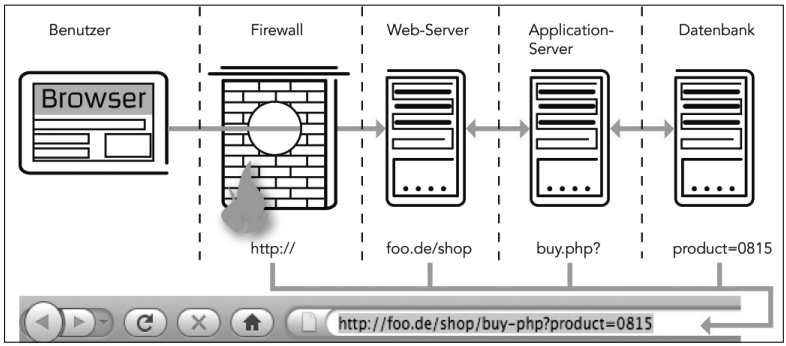
Katharina Friedmann

Katharina Friedmann ist Redakteurin mit Schwerpunkt IT-Sicherheit bei unserer Schwesterpublikation Computerwoche, von der wir diesen Beitrag übernommen haben.

TecChannel-Links zum Thema	Webcode	Compact
Grundschutz für Web-Applikationen	1785530	S.10
Sicherheitsrisiko Web-Anwendung	1785212	–
Angriffe auf Web-Anwendungen erkennen und abwehren	1784364	–
Schutz von Webshops und E-Commerce-Lösungen	1817630	S.37
Network Access Control für mehr Netzwerksicherheit	2018468	S.54

1.2 Die größten Schwachstellen in Web-Anwendungen

Über die Jahre hat sich die statische Web-Seite zu einer komplexen dynamischen Anwendung gewandelt, die dem Internet-Nutzer viele Funktionen bereitstellt. Dazu ist eine Vielzahl von Technologien erforderlich, deren Implementierung und Betrieb nicht immer trivial sind. Parallel zum technischen Fortschritt sind neue Schwachstellen in den Anwendungen entstanden. Nach einer Statistik des Web Application Security Consortium (www.webappsec.org/projects/statistics/) lassen sich mittels Penetrationstests in 96,85 Prozent aller Web-Anwendungen kritische Sicherheitslücken identifizieren.



Adressübergabe: Beim Aufruf einer Web-Seite im Browser werden die einzelnen URL-Segmente an die entsprechenden Server der Web-Anwendungen weitergereicht.

Um Qualität und Sicherheit von Anwendungen zu verbessern, wurde das Community-Projekt „Open Web Application Security Project" (owasp.org) ins Leben gerufen. Innerhalb des OWASP gibt es verschiedene Teilprojekte, so etwa das „OWASP Top Ten Project", das regelmäßig die jeweils zehn kritischsten Schwachstellen von Web-Applikationen beschreibt (letzter Stand: 2007). Ziel ist es, Entwickler, Designer, Architekten und Unternehmen für potenzielle Schwachstellen zu sensibilisieren und aufzuzeigen, wie sich diese vermeiden lassen. Die folgenden „OWASP Top Ten" stellen unter Web-Sicherheitsexperten einen anerkannten Konsens dar, was die derzeit kritischsten Lücken in Web-Anwendungen betrifft:

1.2.1 Cross Site Scripting (XSS)

Cross Site Scripting (XSS) ist die mit Abstand am weitesten verbreitete Schwachstelle – sie betrifft nahezu jede Web-Anwendung (siehe auch „Schwachstellen in Web-Seiten", BSI-Lagebericht 2009, Seite 38, www.bsi.bund.de/literat/lagebe

richt/Lagebericht2009.pdf). XSS-Lücken treten dann auf, wenn eine Anwendung von einem Benutzer übermittelte Daten an den Browser zurückgibt, ohne zu prüfen, ob die Zeichen codiert dargestellt werden müssen. Das ermöglicht einem Angreifer, beispielsweise Javascript-Code im Browser eines Opfers zur Ausführung zu bringen. Dieser bösartige Code kann im Browser auf alle Informationen der betroffenen Website zugreifen. Hierzu zählen Session-Informationen, die in Cookies gespeichert sind, aber auch in Eingabefelder eingegebene Informationen wie Passwörter. Durch Javascript lassen sich auch Bestandteile einer Web-Seite modifizieren oder identisch nachbilden. Im Falle einer Login-Maske werden die eingegebenen Login-Daten zunächst an einen Angreifer weitergeleitet, und erst dann erfolgt der eigentliche Login-Vorgang. Die XSS-Schwachstelle dient oft als Werkzeug für den als „Phishing" bekannt gewordenen Angriff, bei dem Web-Nutzer verleitet werden sollen, sensible Daten preiszugeben.

1.2.2 Injection Flaws

Injection-Fehler sind in Web-Anwendungen sehr verbreitet. Sie entstehen, wenn die Web-Applikation an sie übermittelte Daten ungeprüft als Programmcode verwendet. Injection-Schwachstellen gibt es in mehreren Ausprägungen – etwa Webscript Injection, OS Command Injection oder SQL-Injection (Webcode **402351**). Letztere tritt am häufigsten auf: Dabei übermittelt ein Angreifer innerhalb eines Parameters (etwa eines Formularfelds) gültigen SQL-Code an die Web-Anwendung, die ihn dann ausführt. Das ermöglicht ihm, auf Daten in der Datenbank zuzugreifen, sich diese anzeigen zu lassen, zu manipulieren oder sogar zu löschen. Viele Datenbanken erlauben zudem das Ausführen von Systemkommandos, was die Gefahr einer feindlichen Übernahme des Datenbanksystems erhöht. Oft wird außer Acht gelassen, dass Datenbank-Server im Inneren einer IT-Landschaft stehen. Eine Injection-Schwachstelle ermöglicht es einem Angreifer somit, ein internes System anzugreifen – an vielen Sicherheitsmaßnahmen vorbei.

1.2.3 Malicious File Execution

Bei Web-Anwendungen besteht die Möglichkeit, Schaddateien auf den Web-Server zu laden und zur Ausführung zu bringen. Häufig werden Dateien einfach entgegengenommen und auf dem Web-Server gespeichert, ohne vorab die Gültigkeit zu prüfen. Möglich werden entsprechende Angriffe oft durch Upload-Funktionen innerhalb der Web-Applikation. Bleibt eine hinreichende Prüfung der hochgeladenen Dateien aus, kann ein Angreifer bösartigen Code auf dem Server der Anwendung platzieren. Schadcode wird dabei in die Datei eingebettet und durch einen anschließenden Aufruf zur Ausführung gebracht. Die Auswirkungen einer solchen Attacke sind unterschiedlich und hängen stark von der Konfiguration des Web-Servers ab: Es besteht die Gefahr einer Server-Übernahme, auch ein Angriff auf die Benutzer der Web-Anwendung ist möglich.

1.2.4 Insecure Direct Object Reference

Bei der Entwicklung von Web-Anwendungen werden oft Objektreferenzen verwendet, um auf ein bestimmtes internes Implementierungsobjekt zu verweisen. Dabei kann es sich um Dateien, Verzeichnisse, Datenbankeinträge oder digitale Schlüssel handeln. Bei einer Insecure-Direct-Object-Reference-Lücke ist die Objektreferenz auf diese Objekte manipulierbar. Ein Angreifer kann durch geschicktes Manipulieren unautorisiert auf Dateien und Inhalte zugreifen. Vor allem wenn Applikationen mit sensiblen Daten arbeiten, sind diese Attacken gefährlich. Konkret verwenden Angreifer meist manipulierte IDs oder Pfadangaben, um etwa fremde Datensätze aus der Datenbank auszulesen oder unautorisiert auf Dateien des Web-Servers zuzugreifen.

1.2.5 Cross Site Request Forgery (CSRF)

Bei dieser Angriffsvariante wird der rechtmäßig angemeldete Benutzer zum „Bauernopfer", indem – ohne sein Wissen – von seiner authentisierten Web-Anwendungs-Session eine Anfrage durchgeführt wird. Möglich ist das beispielsweise, wenn sich der bei einer Web-Anwendung angemeldete User beim Verlassen derselben nicht abmeldet und beim weiteren Surfen auf eine vom Angreifer präparierte Seite gelangt. Der dort platzierte bösartige Code löst über die autorisierte Sitzung des Nutzers einen Angriff aus, indem er beispielsweise im Namen des Opfers, jedoch ohne sein Wissen eine Funktion (etwa eine Überweisung) in Gang setzt. Solche Attacken zu erkennen oder nachzuweisen ist extrem schwierig. CSFR (Webcode **1993878**) ist die Variante von Angriffen auf Web-Anwendungen, die derzeit am schnellsten zunimmt.

1.2.6 Information Leakage and Improper Error Handling

Web-Applikationen können unbeabsichtigt detaillierte Informationen etwa zum Aufbau der Anwendung oder zu verwendeten Softwareversionen preisgeben – beispielsweise über technische Fehlermeldungen, die direkt im Browser des Benutzers angezeigt werden. Solche Fehler kann ein Angreifer bewusst provozieren.

Jedes System produziert eigene Fehlermeldungen, die Rückschlüsse auf Funktionsweisen und Eigenschaften der Web-Anwendung ermöglichen, aber ausschließlich den Entwicklern vorbehalten sein sollten. Besonders verbreitet ist die Identifikation aktuell verwendeter Softwareversionen: Wenn ein Angreifer über sie Bescheid weiß, kann er unter Umständen auch ihre Sicherheitslücken ausnutzen. Für den Betreiber einer Web-Anwendung ist diese Schwachstelle riskant, weil sich darauf basierend weiterführende Angriffe lancieren lassen.

1.2.7 Broken Authentication and Session-Management

Wenn in einer Web-Anwendung Zugangsdaten ausgetauscht werden, ist besondere Vorsicht geboten. Zugangs- und Sitzungsinformationen (Session-Tokens) sind oft nicht hinreichend vor Angreifern geschützt. Für Letztere sind Session-Tokens vor allem interessant, weil sie den Zugang zu gesperrten Bereichen unter dem Namen und mit den Rechten eines legitimen Benutzers ermöglichen. Schwachstellen im Standard-Authentisierungsmechanismus sind dabei nicht immer der einfachste Angriffspunkt. Vielmehr konzentrieren sich Hacker auf Sicherheitslücken in zusätzlichen Authentifizierungsfunktionen wie Logout-Funktion, Passwort-Erinnerung oder „Secret Questions", um an Zugangsinformationen zu gelangen. Beim fehlerhaften Umgang mit Session-Tokens kann der Angreifer mittels XSS oder Man-in-the-Middle-Attacken in Besitz des Session-Tokens gelangen und so die Sitzung übernehmen (Session-Hijacking). Benutzer und Betreiber sind hiervon gleichermaßen betroffen, da sich neben Benutzer- auch Administratorenkonten kompromittieren lassen.

1.2.8 Insecure Cryptographic Storage

In vielen Web-Anwendungen fehlen kryptografische Funktionen oder sind schlecht implementiert. Dabei sind die Verschlüsselung schützenswerter Daten wie Zugangs- und Kreditkarteninformationen oder die Nicht-Vorhersagbarkeit etwa von Session-Tokens wichtige Mechanismen zur Absicherung einer Web-Applikation. Allerdings gewährleisten kryptografische Funktionen nicht zwingend, dass Daten und Tokens auch wirklich geschützt sind. Mitunter werden eigenentwickelte, schwache (etwa SHA-1 oder MD5) oder fehlerhaft implementierte Algorithmen verwendet, die gebrochen werden können und somit keinen Schutz bieten. Zudem werden die kryptografischen Schlüssel häufig an unsicheren Stellen (etwa in der Anwendung herunterladbar) aufbewahrt, wodurch die Sicherheit des gesamten Verschlüsselungsmechanismus aufgehoben wird.

1.2.9 Insecure Communications

Bei dieser Art von Schwachstelle werden sensible Daten über einen unsicheren Kommunikationskanal im Klartext oder nur teilweise beziehungsweise unsicher verschlüsselt übertragen. In diesen Fällen kann ein Angreifer durch passives Mitlesen oder eine Man-in-the-Middle-Attacke auf die transferierten Daten zugreifen. Vor allem bei der Übermittlung vertraulicher Informationen wie Zugangs-, Zahlungs- oder Kundendaten ist es notwendig, die Datenkommunikation zu verschlüsseln. Jedoch gibt es Web-Anwendungen, die nur den Austausch der Login-Informationen über einen sicheren Übertragungskanal abwickeln und die anschließende Kommunikation unverschlüsselt lassen. Dabei wird häufig vergessen, dass auch bei den folgenden Anfragen sicherheitsrelevante Authentifizie-

rungsinformationen wie Session-Tokens übertragen werden. Das ermöglicht dem Angreifer, unverschlüsselte Tokens mitzulesen und sich mit der fremden Identität bei der Web-Anwendung zu authentisieren.

1.2.10 Failure to Restrict URL Access

Kritische Informationen in einer Web-Anwendung werden häufig lediglich dadurch geschützt, dass die entsprechende URL einem unautorisierten Benutzer nicht angezeigt wird oder nicht bekannt ist. Für eine Attacke lässt sich das ausnutzen, indem die URL direkt angesprochen wird. Die bekannteste Angriffsmethode, die diese Lücke missbraucht, nennt sich „Forced Browsing“: Der Angreifer versucht, durch systematisches „Ausprobieren“ ungeschützte Seiteninhalte oder Anwendungsfunktionen zu identifizieren und darauf zuzugreifen. Das Ziel ist häufig, versteckte Dateien oder URLs ausfindig zu machen, die bei der Implementierung der Berechtigungen übersehen wurden. Für den Betreiber einer Web-Anwendung sind solche Schwachstellen besonders brisant, da ein Angreifer Informationen über deren Aufbau und Struktur gewinnt oder sogar Zugriff auf administrative Funktionen der Seite erhält.

1.2.11 Fazit

Die OWASP Top Ten liefern einen umfassenden Überblick über die aktuell gefährlichsten Schwächen in Web-Anwendungen. Zu den einzelnen Sicherheitslücken gibt es auf der Web-Seite der Organisation (www.owasp.org) neben detaillierten Beschreibungen Bewertungen der jeweiligen Gefahren sowie einen entsprechenden Maßnahmenkatalog. OWASP, das sein Top-Ten-Projekt primär als „Aufklärungs-Dokument“ definiert, rät, Sicherheitsfragen beim Entwickeln einer Web-Anwendung von Beginn an zu beachten. Dazu stellt die Gruppe weitere unterstützende Projekte bereit (etwa Development Guide, Code Review Guide, Testing Guide). Sämtliche Informationsmaterialien und Tools, die von OWASP zur Verfügung gestellt werden, sind unter anerkannten Free-and-Open-Source-Software-Lizenzen veröffentlicht und somit für jeden frei zugänglich.

Christoph Wolfert

Christoph Wolfert ist Security-Consultant bei OneConsult Deutschland. Sein Fokus liegt im Bereich Network Security, Web-Application Security Testing und Software Development. Er ist Experte auf dem Gebiet der Netzwerkdatenanalyse sowie Netzwerkdatenvisualisierung.

1.3 Den Lücken in Web-Anwendungen auf der Spur

Web-Applikationen sind aus dem heutigen vernetzten Leben nicht mehr wegzudenken: Ob es darum geht, Bücher online einzukaufen, Bankgeschäfte zu erledigen oder auch das lang ersehnte Wunschauto zu konfigurieren – längst sind Web-Anwendungen das Mittel der Wahl. Plattformunabhängige Browser ermöglichen es, von fast jedem Endgerät und von überall aus auf eine Web-Applikation zuzugreifen. Doch ist nicht alles rosig im Online-Umfeld. Oft gibt es einen straffen Zeitplan, wenn es darum geht, ein neues Release einer Applikation zu veröffentlichen. Wenn es eilt, können sich Fehler einschleichen, die von böse gesinnten Anwendern ausgenutzt werden, um Informationen, Ansehen oder Geld herauszuschlagen. Aber auch gut informierten und erfahrenen Programmierern ohne Zeitdruck können Fehler unterlaufen, die eventuell ernste Folgen nach sich ziehen – im schlimmsten Fall lassen sich Befehle auf den zugrundeliegenden Systemen ausführen oder vertrauliche Daten aus der Datenbank auslesen. Grundsätzlich gilt: Je früher solche Sicherheitslücken in der Entwicklungsphase erkannt werden, desto leichter sind sie zu beheben. Um diese Schwachstellen rechtzeitig auszumerzen, empfehlen sich zwei Herangehensweisen. Zum einen handelt es sich dabei um die statische (Quellcode-)Analyse, die auf Basis des produzierten Codes versucht, den Datenfluss zu erkennen und Fehler in Logik und Datenverarbeitung aufzudecken. Zum anderen gibt es die dynamische Überprüfung an einer lauffähigen Applikation, mit der sich dieser Beitrag schwerpunktmäßig befasst.

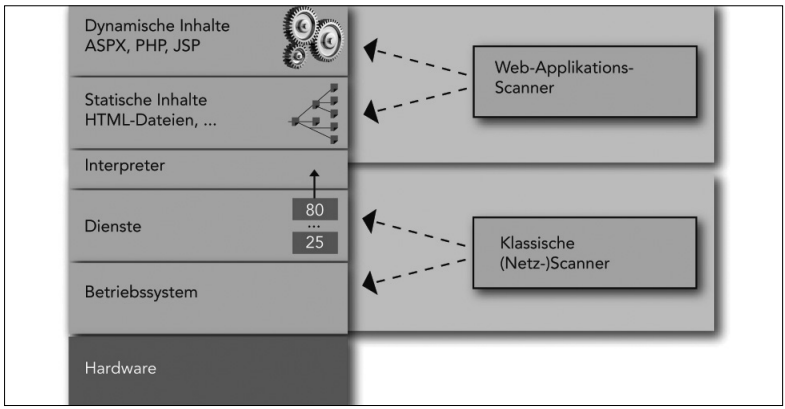
1.3.1 Das Web-Audit

Die dynamische Überprüfung, das klassische „Web-Audit“, umfasst aufwändige manuelle Aufgaben, lässt sich aber auch ein Stück weit automatisieren: Unterstützung leisten hier Web-Applikations-Scanner, mit deren Hilfe viele Schwachstellen in einer Anwendung effizient aufgespürt werden können. Anders als klassische Netzscanner wie beispielsweise „Nessus“ oder „Retina“, die auf Betriebssystem- und Dienstebene nach Schwachstellen suchen, setzen diese Spezial-Tools auf einer höheren Ebene an und interagieren – ähnlich wie ein Browser – nur über den HTTP(S)-Kanal mit der Anwendung.

1.3.2 Wie Scanner arbeiten

In der Regel arbeitet ein Web-Applikations-Scanner in zwei aufeinander aufbauenden Schritten: Zunächst werden die Struktur und sämtliche Seiten innerhalb einer Anwendung erfasst. Für das so genannte Crawlen muss der Scanner in der Lage sein, Links zu weiteren Seiten zu folgen, auch wenn sie dynamisch, beispielsweise in Form eines Javascript-Menüs, erzeugt werden. Außerdem hat das Tool zu erken-

nen, wann es in einen Zyklus läuft, sprich: die gleiche Seite wieder und wieder besucht. Für schwierige Fälle bieten die meisten Produkte einen manuellen Crawl-Modus an: Der Auditor kann mit einem Browser selbst durch die Applikation klicken und so definieren, welche Seiten und Bereiche vom Scanner überprüft werden sollen. Im zweiten Schritt des Scan-Vorgangs erfolgt die eigentliche Schwachstellensuche. Jede Seite, die der Scanner während des Crawl-Vorgangs erfasst hat, wird einzeln und wiederholt untersucht. Dazu werden alle Formularfelder und Parameter innerhalb dieser Seite mit bestimmten Angriffsmustern vorbelegt und anschließend an die Web-Applikation geschickt, um deren Reaktion auf die Angriffsmuster auszuwerten. An der Antwort lässt sich beispielsweise anhand des HTTP-Statuscodes (etwa: „200 OK“ oder „500 Internal Server Error“) oder durch Fehlermeldungen im HTML-Body erkennen, ob die Applikation auf den Angriff „hereingefallen“ ist.



Ansatzpunkte: Netz-Scanner setzen auf OS- und Dienste-Ebene an, Web-Applikations-Scanner arbeiten auf Applikationsebene via HTTP(S). (Quelle: Cirosec)

Mit guten Produkten können nicht nur Web-Applikationen, sondern auch Web-Services auf Schwachstellen überprüft werden. Das Vorgehen ist ähnlich, allerdings entfällt der erste Schritt des Crawlings, da sich die zur Verfügung stehenden Funktionen aus der Web-Service-Definition, der WSDL-Datei, entnehmen lassen. Die Schwachstellen hingegen können bei Web-Services die gleichen Auswirkungen haben wie bei Web-Applikationen.

1.3.3 Manuelle Aufgaben

Neben einem automatisierten Scan überprüfen spezialisierte Dienstleister die komplette Web-Applikation manuell. Notwendig ist diese aufwändige Inspektion, weil es Schwachstellen gibt, die von einem Scanner nicht gefunden oder auch nicht

korrekt interpretiert werden. In der Regel werden sämtliche Parameter auf jeder Seite einzeln betrachtet und, ähnlich wie beim Scanner, verschiedene Angriffsmuster ausprobiert. Dieser Schritt erfordert das größte Know-how im gesamten Web-Audit. Grundsätzlich brauchte es Erfahrung und Hintergrundwissen, um ein Audit sinnvoll und mit bestmöglichem Ergebnis betreiben zu können. Hilfe versprechen hierzulande viele Firmen, die eine Prüfung von Web-Applikationen anbieten. Methoden, Werkzeuge und Erfahrung sollten im Einzelfall jedoch hinterfragt werden, denn nur wenige Sicherheitsunternehmen sind tatsächlich darauf spezialisiert und bringen das erforderliche Know-how mit.

Doch auch ohne tief greifende Kenntnisse und in Eigenregie können Unternehmen mit einem Web-Applikations-Scanner mitunter gute Ergebnisse erzielen. Einige Produkte wie etwa der „Acunetix Web Vulnerability Scanner" lassen sich einfach bedienen und liefern für kleines Geld bessere Resultate als ein falsches Gefühl von Sicherheit beim billigsten externen Anbieter.

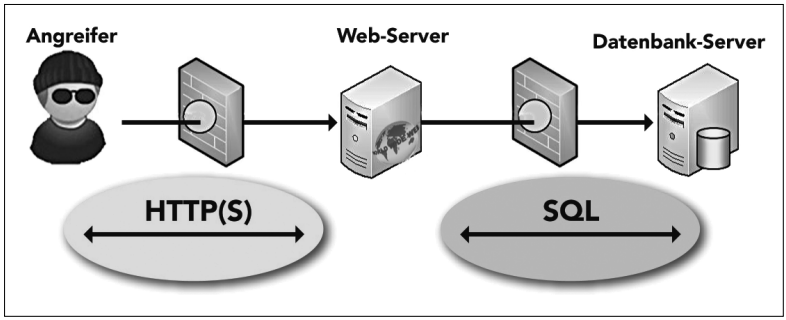
1.3.4 Der Markt

Wer den Kauf eines Web-Applikations-Scanners zu diesem Zweck in Erwägung zieht, sollte die Produkte im Vorfeld allerdings sorgfältig evaluieren, da alle im Umgang mit bestimmten Techniken oder Session-Mechanismen Stärken und Schwächen aufweisen. Die beiden bekanntesten Tools auf dem Markt sind „HP WebInspect" (vormals SPI Dynamics) und „IBM Appscan" (früher Watchfire). Beide bieten neben vielen Konfigurationsmöglichkeiten und Angriffsmustern praktische Hilfsmittel zur manuellen Nachüberprüfung aufgespürter Schwachstellen. Ein ebenfalls mächtiges Produkt ist „Cenzic Hailstorm", das aufgrund seiner Komplexität allerdings ein gewisses Maß an technischem Know-how erfordert. Obwohl noch nicht lange am Markt, erzielen der „Acunetix Web Vulnerability Scanner" und „NT Objectives NTO Spider" gute Ergebnisse und lassen sich auch von Einsteigern relativ einfach bedienen.

1.3.5 Weitere Vorteile von Scannern

Unabhängig von der Wahl eines konkreten Produkts gibt es aber auch eine Reihe von Prüfungen, bei denen ein automatisierter Scanner hilfreich sein kann. Auch wenn er die manuelle Überprüfung durch einen erfahrenen Auditor nicht ganz ersetzen kann, lassen sich damit einige Arten von Schwachstellen effizient aufdecken. Beispielsweise kann ein Scanner in kürzester Zeit prüfen, ob in einer Applikation bestimmte URLs vorhanden sind. Durch einfaches Anhängen und Ausprobieren von URLS wie „/admin", „/administrator", „/phpmyadmin" oder „/webmin" lässt sich schnell kontrollieren, ob neben der Anwendung eventuell noch weitere interessante Seiten auf dem Web-Server existieren („Forceful Browsing"). Auch variieren die gängigen Produkte die Datei-Endungen von aufgerufenen Seiten, um – mit ein bisschen Glück – Backup-Dateien einer Seite aufzuspü-

ren. Wird nämlich statt der Seite „login.jsp“ einfach „login.bak“ angefragt und existiert diese Datei auf dem Web-Server, wird sie wegen der unterschiedlichen Datei-Endung nicht vom Web-Server interpretiert beziehungsweise ausgeführt. Lediglich der Quellcode der „.bak“-Datei wird als Text ausgegeben, aus dem sich möglicherweise interessante Details über den Login-Vorgang herauslesen lassen.



Strukturiert: Web-Audits erfolgen meist aus der Perspektive eines Angreifers, der durch eine Firewall vom Web-Server getrennt ist. Über einige Anwendungen ist jedoch ein unberechtigter Durchgriff bis zur Datenbank möglich. (Quelle: Cirosec)

Über die Prüfung auf Applikationsebene hinaus wird in der Regel auch auf bestimmte Schwachstellen in der Konfiguration des Web-Servers getestet. So werden beispielsweise Verzeichnisse auf mögliche Schreibrechte geprüft. Diese Aufgabe kann auch ein Scanner erfüllen oder dabei unterstützen. Durch einen Upload mit der HTTP-Methode „PUT“ prüft das Tool für jedes einzelne Verzeichnis, ob der Web-Server eine auf diese Weise hochgeladene Datei annimmt.

1.3.6 Qualitätsmerkmale und Hürden

Die Qualität eines Scanners lässt sich jedoch nicht nur daran festmachen, wie viele und welche Prüfungen er bietet, sondern vor allem daran, wie gut er komplexe und dynamische Seiten crawlen und mit Login-Mechanismen umgehen kann.

Web-Applikationen sind heute weit komplexer als noch vor fünf oder zehn Jahren. Waren damals eher statische HTML-Seiten mit einer fest vorgegebenen Abfolge von Request und Response die Regel, sind heute mit Ajax, Flash und Silverlight hochdynamische Applikationen verfügbar, bei denen ein Scanner mit dem Erfassen und Ordnen der Website-Struktur häufig überfordert ist. So basiert die Technik Ajax darauf, dass jederzeit im Hintergrund Anfragen an eine Web-Seite gestellt werden können – sogar ohne jegliche Benutzerinteraktion. Auch wenn sich viele aktuelle Scanner darauf eingestellt haben und mehr oder weniger in der Lage sind, Ajax-Requests und Links zu parsen – das Erkennen und Verfolgen derselben ist bei automatisierten Tools nach wie vor ein wunder Punkt.

Zu den größten Herausforderungen für Web-Applikations-Scanner zählen das Session-Handling und der Umgang mit dem Login-Mechanismus einer Applikation. Das Tool muss selbständig erkennen können, ob es bei der Applikation angemeldet ist oder sich anmelden muss.

1.3.7 Tücken bei der Anmeldung

Am weitesten verbreitet ist die HTML-Form-basierende Anmeldung mit einem Benutzernamen und Passwort. Damit sich der Scanner selbständig bei der Applikation anmelden kann, wird in der Regel ein so genanntes Login-Makro aufgenommen: Der Auditor nimmt manuell im Browser eine Anmeldung an der Applikation vor, während der Scanner diesen Vorgang und sämtliche Eingabewerte des Auditors, also auch Benutzername und Passwort, im Hintergrund mitschneidet.

Dieses Login-Makro wird vom Scanner jedes Mal ausgeführt, wenn er eine Abmeldung beziehungsweise die Ungültigkeit seiner Session erkennt. Hier liegen die Tücken im Detail, da die Erkennung des Logouts von Applikation zu Applikation sehr unterschiedlich ausfallen kann. Am einfachsten sind Meldungen wie „Sie wurden abgemeldet“ oder „Ihre Session ist abgelaufen“ als Logout-Signatur zu verwenden. In schwierigeren Fällen kann es erforderlich sein, weitere Parameter wie HTTP-Statuscode, URL, Header-Variablen oder Cookie-Status hinzuzunehmen, um einen Logout zu erkennen.

Die meisten Applikationen halten den Session-Status in Cookies, die vom Anwender beziehungsweise Scanner bei jeder Anfrage mitgeschickt werden. Seltener trifft man noch Session-IDs in der URL, also als GET-Parameter, an. Beide Fälle stellen für den Scanner üblicherweise kein Problem dar. Schwieriger wird es, wenn – wie häufig etwa bei SAP-basierenden Anwendungen – die Session-ID in den URL-Pfad selbst als eine Art „virtuelles Verzeichnis“ eingebettet ist. Hier müssen die meisten Scanner passen und gehen bei jeder neuen Session-ID davon aus, dass ein neues Verzeichnis vorliegt. Solche Grenzfälle zeigen, dass sich nicht jede Applikation mit jedem Scanner erfolgreich überprüfen lässt und grundsätzliche manuelle Tests und entsprechendes Know-how hilfreich sind.

1.3.8 Die Grenzen der Scanner

Einige Schwachstellen sind ausschließlich durch eine manuelle Überprüfung aufzuspüren. So können Scanner beispielsweise keine Logikfehler erkennen, da sie nicht fähig sind, die Bedeutung von Parametern und URLs zu interpretieren: Ein Scanner weiß nicht, dass normale Benutzer Administrationsseiten nicht aufrufen dürfen. Daher wird er keine Schwachstelle feststellen, wenn er – im Kontext eines normalen Benutzers – unberechtigt Zugriff auf administrative Bereiche erhält. Ein weiteres simples Beispiel wäre eine Überweisung, bei der die Zielkontonummer als URL-Parameter übermittelt wird. Ein Scanner kann nicht wissen, dass die Appli-

kation eigentlich verhindern sollte, dass dieser Parameter beispielsweise von „zielkonto=12345“ in „zielkonto=67890“ geändert wird. Neben Logikfehlern stehen Scanner auch Plausibilitätsprüfungen einer Applikation hilflos gegenüber. Wenn eine Anwendung an einer bestimmten Stelle erst die Eingabe einer gültigen Kundennummer oder die Einhaltung einer vorgegebenen Abfolge von Eingabemasken erfordert, damit der nächste Schritt erfolgen kann („Wizards“), gibt es derzeit keine Möglichkeit zur automatisierten Überprüfung.

1.3.9 Fazit

Unterm Strich tragen automatisierte Tools trotz ihrer Grenzen wesentlich dazu bei, die Effizienz von Sicherheitsüberprüfungen zu erhöhen und ohne viel Aufwand im Rahmen der 80/20-Regel einen großen Teil der Risiken zu identifizieren. Unter diesem Aspekt können Unternehmen Scanner auch in Eigenregie als hilfreiches Werkzeug nutzen. Automatisierte Scanner empfehlen sich auch, wenn eine Vielzahl von Applikationen in möglichst kurzer Zeit auf die gröbsten Schnitzer hin untersucht werden soll. Direkt vor dem Rollout einer Applikation, nach größeren Änderungen und vor allem bei geschäftskritischen Anwendungen sollte ein professionelles Audit mit einer manuellen Komponente jedoch nicht fehlen. Denn selbst gute Scanner haben ihre Grenzen und können mit der Erfahrung und dem Detailwissen eines Auditors nicht mithalten.

Max Ziegler

Max Ziegler ist Senior Berater bei Cirosec in Heilbronn. Hier führt er Sicherheitsüberprüfungen von IT-Systemen, Netzen und Web-Applikationen durch.

TecChannel-Links zum Thema	Webcode	Compact
Den Lücken in Web-Anwendungen auf der Spur	2019854	S.19
Grundschutz für Web-Applikationen	1785530	S.10
Die größten Schwachstellen in Web-Anwendungen	2019842	S.14
Web Application Firewalls in der Praxis	2019855	S.25
Web-Anwendungen sicher entwickeln	2019856	S.32
Schutz von Webshops und E-Commerce-Lösungen	1817630	S.27
10 Tipps zur Sicherheitsoptimierung von Apache	2018831	S.41

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

1.4 Web Application Firewalls in der Praxis

Das Firmennetz wird durch eine Netz-Firewall gesichert – doch schützt dies auch den Internet-Auftritt? Der dazugehörige Web-Server steht zwar in einer demilitarisierten Zone (DMZ) – doch wo liegen die Benutzer- und Transaktionsdaten des Shops, der zunehmend mehr Umsätze macht? Der Datenbank-Server, auf dem alle wichtigen Unternehmensprozesse zusammenlaufen, befindet sich meist im internen Netz. Genau das ermöglicht es Angreifern, über Schwachstellen in Internet-Auftritten bis in das Innerste von Firmennetzen vorzudringen. Mit Hilfe spezieller Techniken nutzen sie die zwingend erforderlichen Kommunikationspfade zwischen Internet, Web-Server und Datenbank aus, um Daten zu manipulieren und Zugriff auf vertrauliche Informationen zu erlangen.

Beinahe täglich werden neue Schwachstellen in viel genutzten Applikations-Frameworks bekannt, ergeben sich neue Manipulationsmöglichkeiten in verbreiteten Web-Applikationen, hört man von Datendiebstahl in großem Stil. Um so mehr verwundert es, dass so mancher für einen (verwundbaren) Internet-Auftritt Verantwortliche nachts noch Ruhe findet.

1.4.1 Aber die Firewall?

Eine klassische Netz-Firewall kann vor dieser Bedrohung nicht schützen. Sie kann lediglich anhand von Port-, Quell- und Zielinformationen einer Anfrage entscheiden, ob der Datenfluss erlaubt ist oder blockiert werden soll. Eine http-Anfrage aus dem Internet an den Web-Server ist natürlich erwünscht, und allein anhand der Quelladresse und des Protokolls ist nicht erkennbar, ob sie „böse“ ist. Der Inhalt der Anfrage wird von Netz-Firewalls nicht untersucht. Das ist Aufgabe einer Web Application Firewall, kurz: WAF. Eine WAF untersucht die Anfragen an den Web-Server im Kontext der angefragten Applikation aufs Genaueste und blockiert Angriffe wie zum Beispiel SQL-Injection oder XSS-Attacken, bevor sie überhaupt zum Web-Server gelangen können. Darüber hinaus werden die als Antwort ausgelieferten Web-Seiten auf sensible Daten hin untersucht, die nicht nach außen gelangen sollen.

1.4.2 Die Integration

Eine WAF lässt sich auf mehrere Arten in eine bestehende Netzumgebung integrieren. Grundsätzlich gibt es die beiden Betriebsmodi „Reverse Proxy“ und „Bridge“. Bei der Integration als Bridge wird die WAF wie ein Switch einfach in die Netzverbindung eingeschleift. Hierbei sind keine Änderungen am Routing, der Konfiguration der Firewall oder des Netzes erforderlich. Die WAF liest den Netzverkehr passiv mit. Meist erfolgt die Integration einer WAF allerdings als Reverse Proxy. Dabei wird die direkte Verbindung zwischen dem Browser des Benutzers

und dem Web-Server aufgebrochen. Statt mit dem Web-Server spricht der Browser direkt mit der Web Application Firewall. Nach Überprüfung der Anfrage baut Letztere eine eigene Verbindung zum Web-Server auf und liefert die erhaltenen Antwortseiten an den Browser aus.

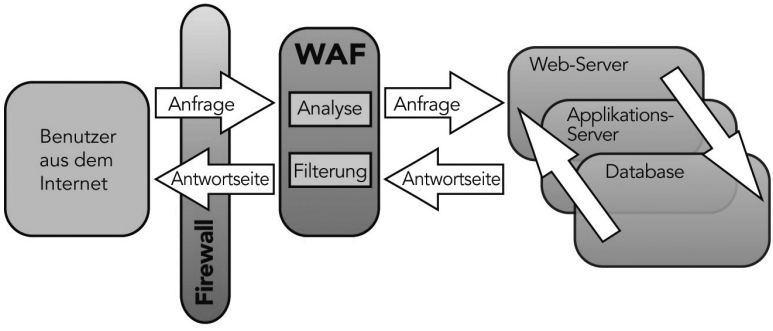
1.4.3 Die Grundfunktionen einer WAF

Benutzereingaben in eine Web-Applikation werden vom Web-Browser in Form von GET- oder POST-Parametern an den Web-Server übermittelt. Hierzu zählen auch Auswahlfelder oder Parameter, die von der Applikation als so genannte Hidden-Parameter gesetzt werden. Alle diese Parameter können von Angreifern manipuliert und missbraucht werden. Zu den Grundfunktionen einer WAF zählt, diese Angriffe zu erkennen und zu blockieren und die übermittelten Parameter vor Manipulationen zu schützen. Des Weiteren verhindert sie, dass Daten gestohlen beziehungsweise ausgespäht werden. Einige WAF-Produkte bieten zusätzlich an, die Benutzerauthentisierung einer Web-Applikation zu übernehmen.

1.4.4 Wie eine WAF Angriffe erkennt

Die Angriffserkennung erfolgt in mehreren Schritten: Zunächst werden alle übermittelten Daten „normalisiert", sprich: sämtliche Codierungen, die einen Angriff tarnen könnten, werden aufgelöst.

In einem nächsten Schritt folgt dann die Filterung durch verschiedene Listen – im Idealfall zuerst anhand einer Whitelist. Dabei handelt es sich um eine Liste, in der für jeden Parameter und jede URL der Web-Applikation die jeweils gültigen Werte hinterlegt sind, was auch als „positives Sicherheitsmodell" bezeichnet wird: Demnach ist alles verboten, was nicht explizit erlaubt ist.



Abgeschottet: Die WAF inspiziert Anfragen an den Web-Server und blockiert Angriffe, bevor sie zu diesem gelangen. (Quelle: Cirosec)

Ergänzend filtern alle WAFs die Anfragen durch Blacklists. Das sind Listen mit bekannten Angriffsmustern, die auf die übermittelten Parameter angewendet werden. Tritt eines dieser Angriffsmuster in einer Anfrage auf, wird diese blockiert. Diese Art der Filterung nennt sich „negatives Sicherheitsmodell": Was nicht explizit verboten wird, ist erlaubt. Im Unterschied zu einem IDS/IPS (Intrusion Detection/Prevention System) untersucht die WAF hierbei nicht nur den Datenstrom als Ganzes, sondern analysiert auch das zugrunde liegende HTTP (Hypertext Transfer Protocol) und prüft die einzelnen Bestandteile der Anfrage bezogen auf jedes einzelne Formular oder sogar Feld. Die WAF taucht demnach wesentlich tiefer in die Kommunikation ein und ist so in der Lage, viele bekannte Angriffe zu erkennen. Da die Attacken stets auf denselben Grundlagen basieren, müssen diese Muster nur selten erneuert werden. Für eine erfolgreiche SQL-Injection muss zum Beispiel gültiges SQL eingesetzt werden. Dieser Standard ist seit vielen Jahren unverändert. Die zugehörigen Angriffsmuster sind also nur bei einer Änderung des SQL-Standards anzupassen.

1.4.5 Schutz vor Manipulation

Grundsätzlich gibt es zwei Arten von Objekten, die es vor Manipulationen zu schützen gilt: Das sind zum einen die vom Browser des Benutzers an die WebApplikation übermittelten Parameter, deren Inhalt aus Benutzereingaben in Formulare oder aus Auswahlfeldern stammt. Zum anderen übermittelt die Web-Applikation ein oder mehrere Cookies an den Browser, in denen sensible Daten wie Session-Informationen oder Authentisierungs-Tokens gespeichert sein können.

Es gibt Web Application Firewalls, die zum Schutz dieser Objekte anbieten, die tatsächlichen Werte von Auswahlfeldern oder Cookies durch verschlüsselte Werte zu ersetzen und so einer Manipulation vorzubeugen. Ein Angreifer kann nun die Werte dieser Objekte nicht mehr nach Belieben verändern. Weil er den geheimen Schlüssel nicht kennt, kann er den manipulierten Inhalt nicht so chiffrieren, dass die WAF dies akzeptieren würde.

Verschlüsselung wird zudem von manchen Herstellern als Schutz vor „Forceful Browsing" eingesetzt – dabei handelt es sich um das Ausspähen von Daten durch die direkte Eingabe von URL-Pfaden beziehungsweise Dateinamen, die normalerweise nicht über Hyperlinks der Web-Applikation erreichbar wären. Um dem entgegenzuwirken, werden alle in einer HTML-Seite vorhandenen Hyperlinks durch verschlüsselte Varianten ersetzt. Die WAF akzeptiert nur noch Seitenaufrufe, die durch Aufruf eines solchen Links erfolgen. Ohne den geheimen Schlüssel kann ein Angreifer keine URL mehr direkt aufrufen oder Dateinamen erraten.

Sollte es einem Angreifer trotz der genannten Maßnahmen gelingen, die Web-Applikation zu manipulieren, um Daten zu stehlen, kann die WAF dennoch eingreifen: Auch die ausgehenden Daten werden auf bestimmte Muster untersucht. Die Auslieferung sensibler Daten wie etwa Kreditkartennummern lässt sich so blockieren oder in der ausgelieferten Seite maskieren.

Durch das Filtern ausgehender Seiten lässt sich aber auch verhindern, dass möglicherweise wichtige Details ausgespäht werden. Fehlerseiten von Applikations- oder Web-Servern enthalten häufig detaillierte, für Angreifer wertvolle Informationen über die darunterliegende Infrastruktur. Daher werden diese Seiten von der WAF durch eigene Seiten ersetzt oder auf unverfängliche Seiten umgeleitet.

1.4.6 Authentisierung via WAF

Viele WAF-Produkte lassen sich auch als zentrale Authentisierungsinstanz für Web-Applikationen einsetzen. Die Möglichkeiten reichen hier von einer herkömmlichen „Basic-Auth" mit einer in der WAF gepflegten Benutzerdatenbank über die Authentisierung mit Client-Zertifikaten bis hin zu Single-Sign-on-Portalen mit Unterstützung für komplexe Benutzerdatenbanken (beispielsweise Host-Anbindung oder Kerberos-Token).

1.4.7 SSL-verschlüsselte Anfragen

Eine WAF kann auch per SSL verschlüsselte Anfragen inspizieren. Das originäre Server-Zertifikat samt Schlüssel wird dabei auf der WAF eingespielt, die (im Reverse-Proxy-Modus) dann die SSL-Verbindungen terminiert. Nach der Untersuchung der Anfrage kann die Verbindung zum eigentlichen Web-Server erneut verschlüsselt werden oder – je nach Anforderung – auch unchiffriert erfolgen. Für den Betrieb im Bridge-Modus wird SSL transparent inspiziert.

1.4.8 Das WAF-Regelwerk

Um ihren Zweck erfüllen zu können, benötigt eine WAF eine Policy, die möglichst gut an die zu schützende Applikation angepasst ist. Eine solche Policy lässt sich auf unterschiedliche Weise erstellen. Auch können unter Umständen mehrere sich ergänzende Schutzmechanismen in einer Policy parallel verwendet werden.

1.4.9 Black- und Whitelists

Die Blacklists der Hersteller müssen lediglich aktiviert werden, um wirksam zu werden. Anspruchsvoller ist die Erstellung von Whitelists, da diese genau an die jeweilige Applikation und die dort verwendeten Parameter anzupassen sind. Bei vielen WAFs lässt sich ein Lernmodus aktivieren. Aus gültigen Anfragen werden dann die zulässigen Parameterwerte und URLs extrahiert und in die Policy übernommen. Bei Web-Applikationen, die sich oft ändern, stößt dieses Verfahren allerdings schnell an seine Grenzen. Hier werden dann dynamisch erstellte Policies oder ein generisches Regelwerk angewendet, das die Parameter eher mit regulären

Ausdrücken beschreibt, als konkrete Werte vorzugeben. Durch geschickte Kombination von Blacklists und relativ generischen Whitelists lässt sich in der Praxis ein hohes Sicherheitsniveau erreichen und der Aufwand für die Pflege des Regelwerks dennoch gering halten.

1.4.10 False Positives

Bei der Erstellung einer Policy handelt es sich meist um einen iterativen Prozess, bei dem anfangs noch Fehlalarme – so genannte False Positives – auftreten können. Dabei werden an sich legitime Anfragen als Angriff eingestuft und blockiert. Abhilfe schafft hier ein Feature, das sich „One-Click-Refinement" nennt: Aus dem Logviewer der WAF heraus können mit nur einem Mausklick Ausnahmen für solche Requests erstellt werden. Eine weitere Hilfe zur Erkennung und Behebung von False Positives ist ein passiver Betriebsmodus, der in der ersten Zeit der Inbetriebnahme eingeschaltet werden kann. In diesem Modus wird nicht blockiert, sondern nur ein Eintrag im Logfile generiert.

1.4.11 Marktübersicht

In der Entwicklung des WAF-Markts lässt sich seit einiger Zeit ein Trend beobachten: Kleinere hochspezialisierte Anbieter von WAF-Lösungen werden von den großen Playern übernommen. Die akquirierten WAF-Lösungen werden dann in vorhandene und etablierte Plattformen integriert. Daraus ergibt sich auch der Trend zu Appliance-Lösungen. Lösungen auf Modulbasis oder reine Software-Lösungen spielen eine immer geringere Rolle. Einige gibt es aber noch.

Zu den größeren Herstellern zählen etwa F5, Citrix und Barracuda, die auf ihren etablierten Plattformen Features wie SSL-Beschleunigung und Load Balancing mit den WAF-Techniken kombinieren. Damit decken sie ein breites Spektrum an Anforderungen ab, die vor einer Web-Server-Farm gefragt sind. Allen gemein sind hier Hardware-Appliances, die in verschiedenen Ausbaustufen angeboten werden. Die WAF-Technik lässt sich dabei häufig durch einfaches Nachlizenzieren auf bereits vorhandenen Plattformen freischalten. Auch die spezialisierteren und kleineren Hersteller vertreiben ihre Lösung oft als Appliance, bieten daneben aber auch andere, sehr flexible Möglichkeiten an, ihre Produkte einzusetzen.

Der einzige reine Appliance-Hersteller in diesem Umfeld ist Imperva mit „SecureSphere". Im Gegensatz dazu ist Protegrity als der einzige reine Softwarehersteller zu nennen, der mit „Defiance TMS" eine Stand-alone-Software für verschiedene Betriebssystem-Plattformen anbietet. Zwischen diesen beiden Playern gibt es eine Reihe von Herstellern, die WAF-Technik neben einer vorkonfigurierten Appliance als Modul für verschiedene Web-Server anbieten. Art of Defence hat Plug-ins für Apache beziehungsweise Microsofts IIS oder ISA Server im Programm, lässt sich aber auch auf Plattformen wie dem „ZEUS Loadbalancer" oder der „Ge-

NUScreen Firewall“ einsetzen. Breach wiederum offeriert neben seinen beiden Appliance-Serien kommerziellen Support für „ModSecurity“, dessen Hauptentwickler das Unternehmen letztes Jahr angestellt hat. Sehr flexibel ist DenyAlls „rWeb“, das sich auf Hardware verschiedenster Hersteller einsetzen lässt – unter anderem als Modul für die Blade-Plattform von Crossbeam.

WAF-Hersteller – ein Überblick

Hersteller	Art	Herkunft/Plattform
F5	Hardware-Appliance	Übernahme von Magnifire (2005); Integration in BigIP Plattform als ASM
Barracuda	Hardware-Appliance	Übernahme von NetContinuum (2007)
Citrix	Hardware-Appliance	Übernahme von Teros (2005); Integration in NetScaler-Plattform
Cisco	Hardware-Appliance	Übernahme von Reactivity (2007); Integration als WAF-Modul im ACE-XML-Gateway
DenyAll	Hardware-Appliance	Eigenentwicklung (seit 2002); Produktlinie rWeb, Integration in Apache Webserver
Imperva	Hardware-Appliance	Eigenentwicklung (seit 2001); Produktlinie SecureSphere
Phion	Soft-Appliance	Übernahme von Visonys (2008); noch keine Integration
Art of Defence	Modul	Eigenentwicklung (seit 2006); Produktlinie Hyperguard; Modul für diverse Web-Server
ModSecurity	Modul	Eingeschränkte OpenSource-Lösung, Modul für Apache Webserver beziehungsweise Zeus-Loadbalancer
Breach	Hardware-Appliance	Zwei Produktlinien: - Eigenentwicklung WebDefend - Kommerzielle Appliance basierend auf Übernahme von ModSecurity (2008)
Protegrity	Software	Übernahme von KaVaDo (2005); Softwarelösung für die Plattformen Linux, Solaris und Windows

Immer mehr Hersteller entdecken zudem die Möglichkeit, ihre WAF als virtuelle Maschine für VMWares ESX Server anzubieten. Als Beispiel wären hier Phion mit „Visonys Airlock“, das als Image für physische Hardware sowie als VMware-Image verfügbar ist, und Art of Defence zu nennen, das ebenfalls ein Image für diese Plattform bereitstellt. Offen bleibt hier natürlich, inwiefern eine virtualisierte Plattform mit ihren Angriffspunkten die richtige Umgebung für eine Sicherheitsinstanz wie eine Firewall darstellt.

1.4.12 Die Stolpersteine

So komplex Integration und Betrieb einer WAF zunächst erscheinen mögen, hält sich der Aufwand doch erfreulich in Grenzen – wenn man einige Grundsätze beachtet. Nach der Entscheidung, ob die WAF als Bridge oder Reverse Proxy integriert wird, gilt es, eine hinreichend lange Testphase einzuplanen, in der die Policy erstellt und optimiert wird. In dieser Phase kommt es darauf an, die richtige Balance zwischen erreichbarem Sicherheitsniveau und vertretbarem Administrationsaufwand zu finden. Das erfordert sicher einige Erfahrung. Wird diese Aufgabe sorgfältig erledigt, verläuft der Übergang vom Test- zum Produktionsbetrieb jedoch ohne nennenswerte Probleme. In der Regel wird die WAF als „Firewall" organisatorisch der für das Netz zuständigen Administratorengruppe zugeordnet. Der Betrieb der WAF stellt dieses Umfeld vor nicht allzu große Herausforderungen, da für den Betrieb einer WAF – entgegen der Ausrede mancher Administratoren – keine Softwareentwicklungskenntnisse nötig sind. Grundkenntnisse in Sachen http oder zur Schreibweise von URLs sind jedoch erforderlich.

1.4.13 Fazit

Die Auswahl und die anschließende Integration einer WAF sind keine alltäglichen Aufgaben. Wurden diese Anfangshürden jedoch überwunden, hat sich die Sicherheit der Web-Applikationen um ein Vielfaches verbessert – ohne dass sich der Administrationsaufwand in gleichem Maße erhöht. Nicht zuletzt ist dies auch ein positives Signal für den potenziellen Anwender oder Kunden: Hier wird das Thema Sicherheit verantwortungsvoll behandelt und proaktiv umgesetzt.

Stefan Marx

Stefan Marx ist ein auf Applikationssicherheit spezialisierter Berater bei der Cirosec GmbH in Heilbronn.

TecChannel-Links zum Thema	Webcode	Compact
Web Application Firewalls in der Praxis	2019855	S.25
Grundschutz für Web-Applikationen	1785530	S.10
Die größten Schwachstellen in Web-Anwendungen	2019842	S.14
Den Lücken in Web-Anwendungen auf der Spur	2019854	S.19
Web-Anwendungen sicher entwickeln	2019856	S.32
Schutz von Webshops und E-Commerce-Lösungen	1817630	S.37
10 Tipps zur Sicherheitsoptimierung von Apache	2018831	S.41

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

1.5 Web-Anwendungen sicher entwickeln

Geschäftsprozesse überschreiten immer häufiger Firmengrenzen und erlauben den direkten Zugriff Dritter auf Unternehmensdaten. Der Verlust an Integrität, Vertraulichkeit und Verfügbarkeit kann – je nach Prozess – großen Schaden anrichten. Die Datenverarbeitung erfolgt durch Anwendungen, die eine geforderte Geschäftslogik abbilden und – vor allem im Fall von Web-Applikationen – Schnittstellen für den Benutzer bereitstellen. Sichere Anwendungen werden für Geschäftsprozesse daher immer wichtiger. Dabei gilt es, Applikationssicherheit stets ganzheitlich zu betrachten – sowohl auf den verschiedenen technischen Ebenen als auch im Hinblick auf den Entwicklungsprozess.

Im Folgenden wird der Entwicklungsprozess einer Anwendung mit den relevanten Sicherheitsaspekten beschrieben, da er alle technischen und organisatorischen Ebenen umfasst. Der Hauptfokus liegt jedoch auf den Sicherheitsprinzipien beim Design und bei der Programmierung einer Web-Applikation.

1.5.1 Sicherheit im Entwicklungsprozess

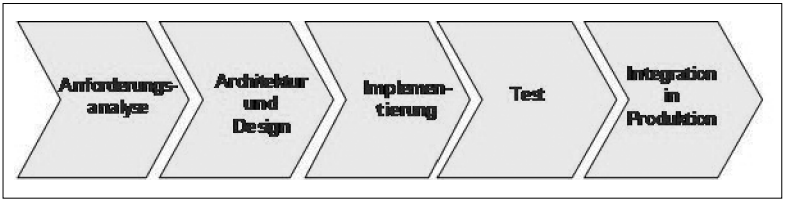
Unabhängig davon, welches Entwicklungsmodell ein Unternehmen favorisiert (etwa das V-Modell oder agiles Programmieren) – stets werden die Phasen „Anforderungsanalyse", „Architektur und Design", „Implementierung", „Test", „Integration in Produktion" durchlaufen. In allen Schritten sind Sicherheitsaspekte zu berücksichtigen, die hier als ein erster Überblick über die Materie skizziert werden. Als Beispielanwendung dient ein einfacher Webshop, der unter anderem Funktionen wie das Speichern von Kontodaten beziehungsweise Kreditkarteninformationen für registrierte Benutzer bereitstellt.

1.5.2 Anforderungsanalyse

In der Anforderungsanalyse, auch Requirements Engineering genannt, sind nicht nur funktionale, sondern auch sicherheitsrelevante Anforderungen zu definieren. Letztere lassen sich mit Hilfe etwa von Threat Modelling sowie Risiko- und Abuse-Cases-Analyse sowie aus Firmenrichtlinien und gesetzlichen Vorgaben ermitteln. Das Ergebnis der Anforderungsanalyse muss im Hinblick auf Sicherheit bereits so belastbar sein, dass Architektur und Design der Anwendung in der Folgephase möglich werden.

Bei unserem Webshop werden zunächst die gesetzlichen Anforderungen ermittelt. Aufgrund der Speicherung beziehungsweise Verarbeitung personenbezogener Daten kommt das Bundesdatenschutzgesetz (BDSG) zum Tragen. Da Kreditkarteninformationen gespeichert werden, muss die Anwendung zudem PCI-Compliance erreichen. Ferner gilt es zu berücksichtigen, dass es sich bei dem eingesetzten Server um einen Multiprojekt-Server handelt, sprich: die Kompromittierung einer

Anwendung kann auch andere Applikationen betreffen. Aus der Risikoanalyse ergibt sich außerdem ein hoher Schutzbedarf für die personenbezogenen Daten – vor allem für Kontoinformationen. Der größtmögliche Schaden ist hier ein Imageverlust für den Fall, dass Schwachstellen des Webshops bekannt werden.



Generischer Prozess: In jeder Phase der Entwicklungsarbeit an der Anwendung sind die Sicherheitsaspekte zu beachten. (Quelle: Secaron)

1.5.3 Architektur und Design

In der Architektur- und -Designphase werden die wesentlichen Komponenten der Anwendung mit ihren Funktionen beschrieben. Außerdem gilt es, die Schnittstellen zwischen den Komponenten zu spezifizieren und den Datenfluss zu modellieren. Ferner werden alternative Lösungsvarianten aufgezeigt und anhand einer Wirtschaftlichkeitsbetrachtung bewertet. Folgende sicherheitsrelevante Aufgaben sind in dieser Phase zu erledigen:

- Bedrohungs-, Schwachstellen- und Restrisikoanalyse;
- risikosenkende Maßnahmen müssen definiert und spezifiziert werden;
- Architektur- und Designvorschläge sind zu erstellen – unter Berücksichtigung von Best Practices (Security Design Patterns) beispielsweise zur Umsetzung des fachlichen Berechtigungskonzepts;
- Architektur- und Design-Reviews – auch im Hinblick auf die identifizierten Sicherheitsanforderungen;
- Tests zur Überprüfung der Sicherheitsfunktionen müssen spezifiziert werden.

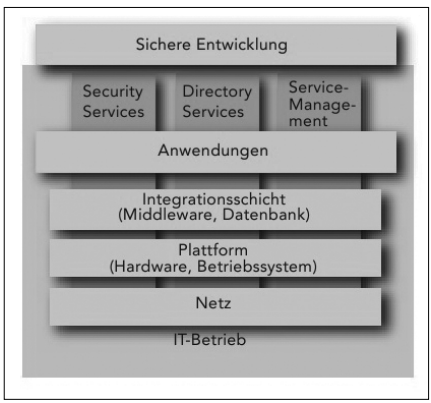
In unserem Beispiel wird für Authentisierung, Autorisierung und Session-Management auf Security Design Patterns zurückgegriffen. Eine Zwei-Faktor-Authentisierung mittels SMS-Bestätigung soll Phishing- oder Trojaner-Attacken erschweren. Für eine komfortable Administration wird ein einfaches Rollenkonzept mit normalen Benutzern und Administratoren eingeführt.

Als zusätzlicher „Defense-in-Depth"-Ansatz sollen Zugriffe mehrfach, an verschiedenen Layern der Applikation, geprüft werden. Die erste Schutzschicht auf Ebene der Requests prüft, ob für den Zugriff auf eine spezielle URL ausreichende Rechte vorhanden sind. Die zweite Schutzschicht auf dem Service-Layer stellt sicher, dass auch für den Aufruf einer bestimmten Servicefunktion entsprechende

Rechte vorliegen. Die dritte Schutzschicht auf Datenebene sorgt dafür, dass beim Zugriff auf das DAO (Data Access Object) nur Daten zurückgeliefert werden, auf die rechtmäßig zugegriffen werden darf. Eingaben von Benutzern werden so streng wie möglich validiert. Beispiel Postleitzahlenfeld: Da nur Kunden in Deutschland unterstützt werden, wird geprüft, ob die angegebene Nummer fünf Stellen hat. Um gegen Injection-Angriffe gefeit zu sein, werden im Vorfeld alle integrierten Interpreter ermittelt und zentrale Maskierungsfunktionen für den jeweiligen Kontext zur Verfügung gestellt. Beispiel: HTML- oder Javascript-Code wird durch spezielle JSTLs (Javaserver Pages Standard Tag Library) maskiert.

1.5.4 Implementierung

Das eigentliche Coding der Anwendung erfolgt in der Implementierungsphase, in der die Vorgaben aus den vorangegangenen Phasen zu realisieren sind. Unterstützt wird die Implementierung durch Frameworks und Programmierumgebungen, die mit bereits definierten Sicherheits-Features konfiguriert sind oder die Programmierung bestimmter Sicherheitsfunktionen erleichtern. Zudem sollten Programmierrichtlinien den Entwicklern klare Vorgaben für die verwendeten Frameworks, Programmierumgebungen und -sprachen an die Hand geben. Die bereits definierten Sicherheitstests sind weiter zu verfeinern oder zu ergänzen. In dieser Phase werden auch Installations- und Betriebshandbücher unter Berücksichtigung von Sicherheitsanforderungen für die Betriebsumgebung (etwa Härtungsvorgaben für Server) erstellt.



Implementierung: Sichere Anwendungen müssen ganzheitlich geschaffen werden. (Quelle: Secaron)

Für unseren Webshop werden Muster für die Einbindung von Interpretern erarbeitet. Beispiele hierfür sind die Ausgabe von HTML oder Javascript, die Anbindung einer Datenbank mittels JPA (Java Persistence API) und die Anbindung an einen LDAP-Service. Sicherheitskritische Funktionen wie die Nutzung von Securi-

ty Design Patterns und das Aufrufen von Interpretern werden mittels Sourcecode-Reviews geprüft und gegebenenfalls korrigiert. Ferner sollen in den Build-Prozess integrierte Tools wie „Findbugs“ und „Checkstyle“ die Codequalität verbessern und Programmierfehler (auch sicherheitsrelevante) reduzieren.

1.5.5 Test

Wichtig ist, die Anwendung nicht nur funktional zu testen. In einem Testplan sind die zuvor definierten Sicherheits-Checks zu verfeinern oder zu ergänzen, auszuführen und zu dokumentieren. Nach der Fehlerbereinigung muss erneut geprüft werden. Dabei sind nicht nur Checks vorzunehmen, die sich direkt auf die bereinigten Fehler beziehen, sondern auch mögliche Nebeneffekte der am Code vorgenommenen Änderungen zu berücksichtigen. Die Security-spezifischen Tests sollte ein Sicherheitsverantwortlicher überprüfen oder besser: abnehmen.

Bei unserem Webshop wird ein Teil der Tests, die sich leicht automatisieren lassen, in eine Suite fachlicher Checks integriert. Die restlichen Überprüfungen sind vor jedem Release als Testplan manuell vorzunehmen. Inhalte sind unter anderem das Rollenkonzept, einfache Injection-Flaws und die strenge Eingabevalidierung der Daten. Ein externer Sourcecode-Review sorgt für PCI-Compliance. Parallel dazu erfolgt ein Penetrationstest, der einer Attacke eines qualifizierten Angreifers entspricht. Zudem prüft der Tester auch unkonventionelle Vorgänge, auch die Produktions- beziehungsweise Integrationsumgebung wird getestet. Die Ergebnisse der Tests werden in einer Restrisikoanalyse bewertet und das verbleibende Risiko eingeschätzt.

1.5.6 Integration in Produktion

Selbst eine Anwendung ohne ein einziges Sicherheitsproblem lässt sich nicht sicher betreiben, wenn die Produktionsumgebung nicht hinreichend abgesichert ist. Mangelhafte Abstimmung zwischen Entwicklung und Betrieb verursacht häufig schwerwiegende Schwachstellen für die Applikation. Schwerpunkte in der sicheren Produktion sind die Härtung von Systemen, hinreichendes Patch-Management sowie sichere Administration. Noch mehr Abstimmung ist beim Einsatz einer Web Application Firewall (WAF) notwendig, da sich damit auch Schwachstellen in der Applikation absichern lassen. Eine WAF mit voreingestelltem Regelwerk erhöht zwar das Sicherheitsniveau, reicht als Schutz vor gezielten Angriffen (auf eine unsichere Anwendung) jedoch nicht aus. Das erfordert spezielle, auf die jeweilige Applikation zugeschnittene Policies. Idealerweise bildet die WAF eine zweite Schutzschicht – vor einer sicher entwickelten Anwendung.

Für unseren Webshop gilt es darüber hinaus, sichere Verschlüsselungsalgorithmen für SSL/TLS zu konfigurieren und unsichere Protokolle wie SSLv2 zu deaktivieren. Der Application-Server wird in der demilitarisierten Zone (DMZ) betrie-

ben, und vom Internet her ist nur der Port für SSL (443) freigegeben. Die Administration der Anwendung, des Application-Servers und des Betriebssystems ist nur über ein spezielles Administrationsnetz im internen LAN möglich.

1.5.7 Fazit

Sicherheit erst im Betrieb zu integrieren funktioniert in der Praxis nicht. Alle relevanten Sicherheitsaspekte müssen bereits während der Entwicklung einer Web-Applikation berücksichtigt werden. Dabei gilt: Je später sicherheitsrelevante Fehler in der Entwicklungsphase entdeckt werden, desto aufwändiger ist es, sie zu beheben. Eine sichere Online-Anwendung führt in der Regel auch zu besserer Codequalität und Wartbarkeit. Eventuell höhere Investitionen in die Entwicklung können sich schnell amortisieren, wenn Imageschäden und finanzielle Verluste dadurch vermieden werden.

Wolfgang Aigner

Wolfgang Aigner ist Security-Consultant bei Secaron in Hallbergmoos.

TecChannel-Links zum Thema	Webcode	Compact
Web-Anwendungen sicher entwickeln	2019856	S.32
Grundschutz für Web-Applikationen	1785530	S.10
Die größten Schwachstellen in Web-Anwendungen	2019842	S.14
Den Lücken in Web-Anwendungen auf der Spur	2019854	S.19
Web Application Firewalls in der Praxis	2019855	S.25
Schutz von Webshops und E-Commerce-Lösungen	1817630	S.37
10 Tipps zur Sicherheitsoptimierung von Apache	2018831	S.41

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

1.6 Schutz von Webshops und E-Commerce-Lösungen

Webshops und Web-Applikationen sind ein zentrales Element zur Kommunikation mit Kunden. Doch da die frei zugänglichen Webseiten im Hintergrund auf sensible Geschäftsdaten zugreifen, stellen sie ein lohnendes Ziel für Hacker dar.

Mit direkten Angriffen über das Netzwerk haben Hacker heute nur noch bei Home-Anwendern eine Chance. Zugriffe auf interne Firmendaten werden über Firewalls, Intrussion Prevention und eine Kapselung der Netzwerke zuverlässig verhindert. Aber mit Webshops und Web-Applikationen bieten Firmen neue Angriffsflächen. Meist greifen die Web-Anwendungen auf Datenbanken wie den Kundenstamm samt Bankverbindung und Kreditkartennummer zu. Gelingt es einem Angreifer, über Schwachstellen im Browser oder in der Anwendung in die Datenbank einzudringen, ist nicht nur der Imageschaden groß.

1.6.1 Phishing

Das Versenden von Phishing-Mails zählt zu den populärsten Methoden, um vertrauliche Daten in E-Commerce-Infrastrukturen und Online-Bezahlsystemen auszuspionieren – und zu missbrauchen. Vor allem Mittelständler, die über keine dedizierte IT-Sicherheitsabteilung verfügen, geraten zunehmend ins Visier von Betrügern. Der Begriff Phishing umfasst den Versand betrügerischer E-Mails mit dem Ziel, den Empfänger zur Preisgabe persönlicher Informationen zu bewegen.

Häufig sind E-Mails mit falschen Absenderadressen in ihrer Aufmachung elektronischen Nachrichten von vertrauenswürdigen Unternehmen täuschend ähnlich und enthalten einen Link, der meist direkt auf eine gefälschte Internet-Seite führt. Abgefischt werden neben aktuellen Zugangs- und Transaktionsdaten Informationen zur Identität – etwa Geburtsdatum, Anschrift und Führerscheinnummern – sowie Konto- und Kreditkartendaten. Phishing-Versuche sind nicht mehr so leicht zu erkennen wie früher – sich ständig wandelnde Angriffstechniken der Datendiebe erschweren es, zwischen Legitimem und Gefälschtem zu unterscheiden.

Der beste Schutz vor Phishing besteht darin, grundsätzlich allen E-Mails zu misstrauen, die persönliche Daten fordern. Seriöse Firmen verlangen niemals die Eingabe von Zugangs- oder Kontodaten. Zudem sollten Mails von unbekannten Absendern nicht beantwortet und beigefügte Anhänge nicht geöffnet werden.

1.6.2 Was ist Cross Site Scripting (XSS)?

Das so genannte Cross Site Scripting ist eine zunehmend verbreitete Methode, Web-Applikationen anzugreifen. Dabei manipuliert ein Angreifer die Web-Anwendung so, dass sie schädlichen Skriptcode in die dem Besucher angezeigte Seite

einbettet. Der Browser verarbeitet den eingeschmuggelten Code dann so, als sei es ein legitimer Inhalt der Web-Seite – mit allen entsprechenden Sicherheitsfreigaben. Ferner droht Unternehmen im Fall eines Server-Absturzes und dem damit verbundenen Datenverlust erheblicher Schaden. Denn oft fehlt ein ausgearbeiteter Krisenplan im Hinblick auf ein verlässliches Ersatzsystem zur Datensicherung, was die zeitnahe Wiederherstellung von Daten erschwert.

1.6.3 Was hilft gegen XSS-Attacken?

Sämtliche Informationen, die per Formulareingabe oder URL-Parameter (Uniform Resource Locator) an den Server übermittelt werden, sind zunächst auf Schadcodes zu überprüfen. Gibt ein User zur Registrierung auf einer Website etwa als Benutzernamen `<script type='text/javascript'> alert(,hallo');</script>` ein, dürfte nach dem Senden der Formulareingabe in keinem Fall ein Dialogfenster „Hallo" statt des Benutzernamens erscheinen. Dies wäre ein eindeutiges Indiz für eine nicht geprüfte und folglich für Cross Site Scripting und eventuell sogar SQL-Injection anfällige Web-Seite.

Gerade Schwachstellen in einem Online-Eingabefeld wie dem Suchformular ermöglichen es Angreifern, Inhalte auszutauschen oder schädlichen Programmcode auszuführen, um den Benutzer zu täuschen und so an seine Zugangsdaten oder Kontoinformationen zu gelangen. Mit einem Web-Scanner lassen sich Web-Seiten einfach auf XSS-Lücken abklopfen.

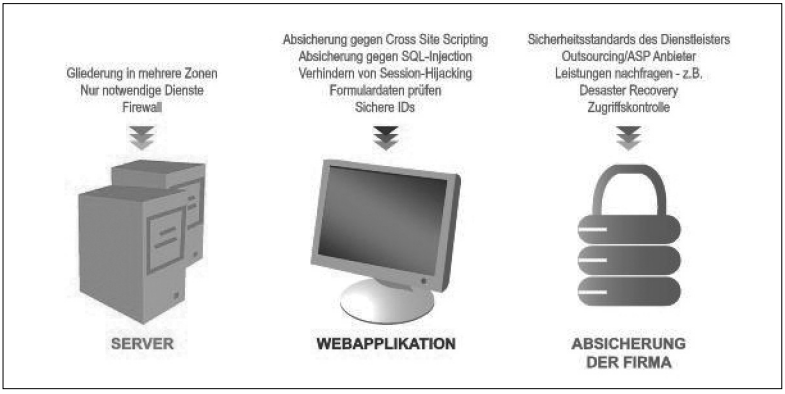
1.6.4 Wie lassen sich Session-Hijacking und SQL-Injection verhindern?

Viele Web-Applikationen arbeiten mit Sessions, um den Nutzer nach dem Einloggen zu identifizieren. Hier hat sich der Gebrauch von GUIDs (Globally Unique Identifiers) bewährt. Dabei handelt es sich um eine 32-stellige alphanumerische Zeichenkette, die das Identifizieren der Session-ID durch Ausschnüffeln (Session-Hijacking) praktisch unmöglich macht.

Ein großer Teil der Web-Anwendungen greift auf eine SQL-Datenbank zurück. Das als SQL-Injection bezeichnete Einschleusen oder Manipulieren von SQL-Kommandos ist derzeit die von Hackern am häufigsten genutzte Angriffstechnik auf Anwendungsebene. Besonders anfällig sind fehlerhaft konzipierte Websites, deren Datenbankschnittstellen unnötig Informationen preisgeben. Solche Schwachstellen finden sich vor allem in Anmeldeformularen oder Formularen zur Anforderung vergessener Passwörter. Um SQL-Injection vorzubauen, sollten sämtliche Zugriffe auf die Datenbank von der Web-Anwendung aus nur über so genannte Prepared Statements oder besser Stored Procedures erfolgen. Der direkte Einsatz von SQL-Befehlen hingegen sollte möglichst vermieden werden.

1.6.5 Welche grundsätzlichen Schutzmaßnahmen gibt es?

Ein Großteil denkbarer Angriffsszenarien lässt sich allein durch die richtige Konfiguration der Skripting-Umgebung abwehren. Dabei ist zu beachten: Je weniger Rechte und Funktionen eine Applikation voraussetzt beziehungsweise erhält, desto weniger kann schiefgehen. Im Idealfall sollte eine Webshop-Applikation auf Basis der „Secure Coding Guidelines" entwickelt sein und regelmäßig daraufhin überprüft werden. Durch Setzen einiger Optionen und Parameter lassen sich gefährliche Funktionen abstellen beziehungsweise im Ernstfall der Schaden begrenzen. So schützt zum Beispiel das Arbeiten mit „Doppel-Opt-ins" bei der Online-Registrierung über eine E-Mail-Adresse vor Missbrauch. Hierbei erhält der Nutzer nach der Anmeldung per Mail die Aufforderung, die angegebenen Daten zu bestätigen – erst dann wird sein Account akzeptiert.



Anspruchsvolle Konzepte betrachten Sicherheit als andauernden Prozess und basieren auf den drei Säulen: Sicherheit innerhalb der Server-Plattform, die Absicherung der Web-Anwendung selbst sowie der Umgang mit Daten innerhalb der Firma. Quelle: Atrada

Ferner sollten Sicherheitsvorkehrungen wie das Filtern von Javascript-Codes beziehungsweise XSS, der Gebrauch von GUIDs sowie Schutzmaßnahmen gegen SQL-Injection getroffen und in alle Web-Applikationen integriert werden.

1.6.6 Wie Web-Bedrohungen nachhaltig abwehren?

Um Web-Bedrohungen effektiv entgegenwirken und im entscheidenden Moment schnell reagieren zu können, sollte das Thema Sicherheit als andauernder Prozess behandelt werden und – zum optimalen Schutz der Lösung, aber auch aus Kostengründen – bereits in die Planung von E-Commerce-Projekten einfließen. Umfassende Konzepte basieren auf drei Säulen: Sicherheit innerhalb der Server-Platt-

form, Absicherung der Web-Anwendungen selbst sowie der sichere Umgang mit Daten innerhalb des Unternehmens. Im Hinblick auf eine umfassende Sicherheit im System gilt es darüber hinaus, fremden Daten prinzipiell zu misstrauen, da sich nie ausschließen lässt, dass sie manipuliert sind. Neben der Implementierung gängiger Sicherheitsstandards und gesundem Misstrauen spielt letztendlich erhöhte Wachsamkeit, sprich: fortwährende Überwachung, eine tragende Rolle.

1.6.7 Was ist bei der Absicherung der Server-Plattform zu beachten?

Die Sicherheit von Server und Netz bilden das Sicherheitsfundament einer Web-Anwendung. Grundsätzlich gilt es, die Server-Plattform in mehrere Zonen aufzuteilen – und selbstverständlich eine Firewall einzusetzen. Dabei sollten nur Web-Applikations-Server direkt mit dem Internet verknüpft werden. Bei allen anderen Systemen, die nicht unmittelbar vom User angesprochen werden – beispielsweise dem Datenbank-Server – ist eine Web-Verbindung zu vermeiden. Nur so lässt sich das Angriffsrisiko verringern. Gelangt ein Angreifer beispielsweise an Login-Daten eines Datenbank-Servers, sind sie für ihn wertlos, solange er nach der Devise der geringsten Privilegien keinen Zugriff auf den Server erlangt. Darüber hinaus gelten heute regelmäßige Software-Updates als unabdingbarer Standard, um sich vor Angriffen von außen zu schützen. Auch sollten auf den eingesetzten Systemen nur für den Betrieb zwingend erforderliche Dienste laufen: Je weniger „Default"-Anwendungen aktiviert sind, desto kleiner die potenzielle Angriffsfläche.

1.6.8 Inwieweit sind die eigenen Mitarbeiter gefordert?

Der richtige Umgang mit sicherheitsrelevanten Themen im Unternehmen selbst wird oft vernachlässigt, ist zum eigenen Schutz jedoch unabdingbar. Daher gilt es, die Zugriffsberechtigung auf Kundendaten für jeden Mitarbeiter klar zu regeln – und zwar nach der Devise: „Weniger ist mehr". Je weniger Personen hier Einblick haben, desto eher sind die Informationen vor unbefugtem Zugriff geschützt. Vor diesem Hintergrund empfiehlt es sich zum einen, einen Zugriffsschutz von innen zu installieren, zum anderen, die erfolgten Zugriffe mit Hilfe von Spezialsoftware zu protokollieren. Auf diese Weise lassen sich Änderungen in den Bestandsdaten jederzeit nachvollziehen.

Peter Höpfl

Peter Höpfl betreute seit 1999 die Weiterentwicklung verschiedener eCommerce-Plattformen bevor er 2001 die IT-Leitung innerhalb der Atrada AG übernahm. Sein Tätigkeitsfeld umfasst die Bereiche Softwareentwicklung und IT-Infrastruktur.

1.7 Apache-Sicherheitsoptimierung

Der Webserver Apache verwendet bereits in der Standardinstallation eine verhältnismäßig sichere Konfiguration. Mit zehn einfachen Regeln können Sie die Sicherheit des Apache Webservers aber nochmals deutlich steigern. Auf diese Weise schützen Sie sich wirkungsvoll vor Angriffen und Ausfällen.

Die folgenden Vorschläge und Anmerkungen sind Hinweise, die die Konfiguration des Apache sicherheitstechnisch optimieren sollen. Aber Achtung: Durch diese Optimierungen entsteht keineswegs eine vollkommen sichere Konfiguration. Die Tipps dienen dazu, auf Fehler und notwendige Konfigurationsarbeiten des Administrators nach der Installation des Apache sowie auf mögliche Gefahrenquellen allgemeiner Natur aufmerksam zu machen. Wie Sie Ihre Installation des Apache zusätzlich absichern, lesen Sie in den weiteren Teilen unserer neuen Artikelserie.

Vor diesem Hintergrund bieten sich zur ersten Sicherheitsoptimierung der Apache Grundkonfiguration die auf den folgenden Seiten gezeigten Möglichkeiten an. Einige Problemfälle treten in der Standardkonfiguration der aktuellen Apache-Version 2.2 nicht mehr auf, können sich dort allerdings durch die Übernahme der *httpd.conf*-Datei einer älteren Version eingeschlichen haben. Eine Überprüfung ist daher in jedem Fall sinnvoll. Beachten Sie bitte, dass die angegeben Zeilennummern für Apache 2.2 keine Gültigkeit mehr haben.

1.7.1 Tipp 1: Listen-Anweisungen

Standardmäßig lauscht der Apache nach der Installation durch die Anweisung `Listen 80` (*httpd.conf*, Zeile 218) auf Port 80 aller verfügbaren IP-Adressen des Systems. Dadurch besteht die Gefahr, dass ein unachtsamer Administrator dafür sorgt, dass der Apache über eine IP-Adresse angesprochen werden kann, über die normalerweise kein Zugriff auf das System möglich sein sollte.

Es ist daher ratsam, die IP-Adressen, über die ein Zugriff auf das lokale System möglich sein soll, explizit durch eine Listen-Anweisung in der Konfigurationsdatei des Apache zu definieren. Ein Beispiel:

```
Listen 192.168.0.6:80
```

Durch diese Anweisung wird der Apache nur auf Port 80 der Netzwerkschnittstelle gebunden, der die IP-Adresse 192.168.0.6 zugeordnet ist. Bitte beachten Sie außerdem, dass der Server auch über den TCP-Port 443 (HTTPS) auf allen Netzwerkkarten ansprechbar ist, sofern SSL aktiviert ist.Die Ursache dafür liegt darin, dass die Datei conf/ssl.conf durch den Apache ebenfalls geladen wird (*httpd.conf*, Zeilen 1040-1042) und dort eine entsprechende Listen-Anweisung vorhanden ist. Die oben gemachten Aussagen bezüglich der Gefahr einer universellen Anweisung treffen selbstverständlich auch für SSL zu.

1.7.2 Tipp 2: User nobody

Nach der Installation des Apache ist es die Aufgabe des Administrators, die Konfigurationsdatei des Apache durchzuschauen und dort verschiedene Änderungen der Grundkonfiguration vorzunehmen. Eine wichtige Änderung ist die Korrektur der in den Zeilen 266-267 enthaltenen Definition der Benutzer- und Gruppenkennung, mit der der Apache betrieben werden soll.Standardmäßig sieht diese Konfiguration aus Gründen der Kompatibilität wie folgt aus:

```
User nobody
Group #-1
```

Der Benutzer nobody wird hier verwendet, da dieser bereits auf einer Vielzahl von Systemen existiert und dort gerne für das Ausführen von Systemdiensten mit nicht privilegierten Rechten benutzt wird. Aus Sicherheitsgründen sollten Sie einen separaten Benutzer für die Ausführung des Servers erstellen und dessen Benutzerkennung in die Konfigurationsdatei des Apache eintragen. Die aus Kompatibilitätsgründen standardmäßig verwendete Gruppenkennung *#-1* ist sehr interessant, da diese streng genommen ungültig ist und dafür sorgt, dass der Apache mit einer falschen und in der Regel nicht existierenden Gruppenkennung ausgeführt wird (z.B. 4294967295). Erzeugen Sie deshalb für die Ausführung des Apache eine separate Gruppe oder stellen Sie durch Eingabe des Befehls *id nobody* die korrekte Kennung der Gruppe fest, der der Benutzer *nobody* angehört und korrigieren Sie den Wert der Gruppenkennung in der Datei *httpd.conf*. Sie können unter anderem durch die folgenden Befehle eine separate Gruppe und einen Benutzer für die Ausführung des Apache erstellen:

```
# groupadd wwwuser
# useradd -g wwwuser -d /nonexistent -s /bin/false wwwuser
```

Ändern Sie nun in der Datei *httpd.conf* die User- und Group-Anweisung:

```
User wwwuser
Group wwwuser
```

1.7.3 Tipp 3: Optionen für das Wurzelverzeichnis

In den Zeilen 316-319 der Datei *httpd.conf* werden Konfigurationsoptionen für das Wurzelverzeichnis »/« des Dateisystems festgelegt. Die besagte Stelle der Konfigurationsdatei sieht wie folgt aus:

```
<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>
```

Ich persönlich sehe keinen Grund dafür, dass der Apache, hervorgerufen durch die Angabe der Option *FollowSymLinks*, standardmäßig symbolischen Links folgt. Dieses Verhalten ist insbesondere deshalb fragwürdig, da durch diese Standardkonfiguration ebenfalls solche Links beziehungsweise Verweise verfolgt werden, bei denen die Zieldatei bzw. das Zielverzeichnis nicht demselben Benutzer gehören, dem der eigentliche Link gehört. Dadurch ist es einem potenziellen Angreifer prinzipiell möglich, auf Dateien zuzugreifen, die außerhalb des als *DocumentRoot* definierten Verzeichnisses gespeichert sind. Aus diesem Grunde halte ich folgende Konfiguration für sinnvoller:

```
<Directory />
Options None
AllowOverride None
</Directory>
```

Falls Sie dennoch auf symbolische Verweise im Wurzelverzeichnis nicht verzichten können, sollten Sie das Verfolgen von symbolischen Links wenigstens auf solche beschränken, bei denen der Besitzer der Zieldatei beziehungsweise des Zielverzeichnisses mit dem Besitzer des Verweises identisch ist:

```
<Directory />
 Options SymLinksIfOwnerMatch
 AllowOverride None
 </Directory>
```

Die vorherige Variante ist dennoch wahrscheinlich die sicherere. Des Weiteren ist es aus sicherheitstechnischer Sicht sinnvoll, den Zugriff auf die Wurzel des Dateisystems (»/«) ebenfalls an dieser Stelle zu beschränken. Die beste Konfiguration an dieser Stelle der Datei *httpd.conf* ist deshalb wohl:

```
<Directory />
Options None
AllowOverride None
Order deny,allow
Deny from all
</Directory>
```

Mit Hilfe dieser Konfiguration lassen sich unter anderem so genannte Directory Traversals, das heißt mutwillige Durchstöberung des gesamten Verzeichnisbaums eines Servers, verhindern.

1.7.4 Tipp 4: Optionen für htdocs anpassen

Weiterhin werden in den Zeilen 331-360 der Konfigurationsdatei *httpd.conf* Optionen für das als DocumentRoot bezeichnete Dokumentenverzeichnis *htdocs* der lokalen Apache-Installation (z.B. */usr/local/apache2/htdocs*) definiert. Gekürzt sieht die Passage wie folgt aus:

```
<Directory »/usr/local/apache2/htdocs«>
Options Indexes FollowSymLinks
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

Auch hier halte ich es aus sicherheitstechnischen Gründen nicht für ratsam, automatisch Verzeichnislistings zu erzeugen und symbolischen Verweisen zu folgen. Durch Verzeichnislistings werden die Inhalte eines Verzeichnisses in einer Übersicht präsentiert, sofern in dem jeweiligen Verzeichnis keine Indexdatei vorhanden ist. Dadurch besteht die Gefahr, dass Verzeichnisinhalte ungewollt veröffentlicht beziehungsweise von außen eingesehen werden können. Des Weiteren existiert durch die vorhandene FollowSymLinks-Anweisung die Möglichkeit, dass ein Angreifer durch einen symbolischen Verweis auf Dateien und Verzeichnisse zugreift, die außerhalb des als DocumentRoot definierten Verzeichnisses gespeichert sind. Ich empfehle daher folgende Konfigurationsänderung (gekürzt):

```
<Directory »/usr/local/apache2/htdocs«>
Options None
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

Sollten Sie die genannten Funktionen für ein bestimmtes Verzeichnis benötigen, sollten Sie diese explizit zum Beispiel mit Hilfe einer Directory-Anweisung für das entsprechende Verzeichnis, aktivieren.

1.7.5 Tipp 5: Die ServerTokens-Anweisung

Der Apache 2 bietet durch die ServerTokens-Anweisung die Möglichkeit, den Umfang der an den Client übermittelten Informationen (so genannte »*Banner*«) bezüglich zu der eingesetzten Version, der vorhandenen Erweiterungen und dem zugrunde liegenden Betriebssystem im Kopf (Header) einer Antwort des Servers zu definieren. Standardmäßig werden jedoch alle vorhandenen Informationen veröffentlicht, wodurch meiner Meinung nach zu viele sensible Daten über die allgemeine Serverkonfiguration an die Öffentlichkeit gelangen.

Ein Beispiel einer großen deutschen Universität:

```
Apache/2.0.39 (Unix) mod_ssl/2.0.39 OpenSSL/0.9.6b DAV/2
```

Ein nicht sonderlich versierter Anwender mag dieser Zeile vielleicht wenig Bedeutung beimessen, aber für einen Angreifer liefert sie wichtige Informationen. Für die auf dem Server installierte Version des Apache 2 existiert eine Schwachstelle, die in der entfernten Ausführung von beliebigem Code resultieren kann.

Außerdem existiert bereits seit dem 21. Dezember 2001 eine überarbeitete Version (0.9.6c) der OpenSSL-Bibliothek, da verschiedene Schwachstellen in dem Programm entdeckt worden sind, wobei momentan die OpenSSL-Version 0.9.7c aktuell ist. Ferner ist es ein Kinderspiel festzustellen, dass auf dem entsprechenden Server Sun Solaris 8 läuft.

Aus diesen und anderen Gründen empfehle ich durch folgende Konfiguration den Umfang der veröffentlichten Informationen auf ein Minimum zu reduzieren:

```
ServerTokens Prod
```

Dadurch identifiziert sich der Server nur noch mit der Kennung Apache und lässt somit keine direkten Rückschlüsse auf das verwendete Betriebssystem und die vorhandenen Erweiterungen (z.B. OpenSSL) zu. Die Identifikation als eine beliebige Software (z.B. Microsoft IIS 5) ist ebenfalls durch eine Manipulation des Quellcodes des Apache möglich, obgleich es sich dabei um eine Spielerei handelt.

Selbstverständlich ist mir bekannt, dass derartige Maßnahmen oft abwertend als »*Security by obscurity*« (etwa »*Sicherheit durch Verschleierung*«) bezeichnet werden und die aktive Sicherheit des eigenen Systems (wenn überhaupt) nur minimal erhöhen. Trotzdem denke ich, dass man aus Sicherheitsgründen einem potenziellen Angreifer nicht alle Informationen in mundgerechten Stücken präsentieren sollte, denn wie heißt es so schön: Gelegenheit macht Hacker :-)

1.7.6 Tipp 6: Fehlermeldungen

Der nächste Optimierungsvorschlag betrifft dasselbe Problem, da der Apache im Falle eines aufgetretenen Fehlers (z.B. Datei nicht gefunden) eine entsprechende Meldung präsentiert, in der unter anderem auch eine Signatur enthalten ist, die Informationen über die verwendete Software (inklusive Versionsangaben) und eventuell vorhandene Erweiterungen beinhaltet. Ein Beispiel:

```
Apache/2.0.44 (Unix) mod_ssl/2.0.44
➥ OpenSSL/0.9.6b PHP/4.3.0
```

Auch diese Fehlermeldungen können einem Angreifer wichtige Informationen über ein potenzielles Ziel liefern. Diese lassen sich jedoch mit Hilfe der *ServerSignature*-Anweisung unterbinden:

```
ServerSignature Off
```

Alternativ können Sie im Falle eines aufgetretenen Fehlers durch folgende Einstellung nur die E-Mailadresse des Administrators anzeigen lassen:

```
ServerSignature Email
```

1.7.7 Tipp 7: /icons/ löschen

Direkt nach der Installation des Apache befindet sich in den Zeilen 549-556 der Datei *httpd.conf* eine *Alias*- und *Directory*-Anweisung, die die im Unterverzeichnis icons der lokalen Installation des Apache enthaltenen Icons als Verzeichnis */icons/* auf Ihrer Internetseite veröffentlicht. Dies bedeutet generell kein Sicherheitsrisiko, aber das Vorhandensein eines solchen Verzeichnisses gibt in der Regel Aufschluss auf den Konfigurationsstand des Servers. Da für dieses Verzeichnis das Erzeugen eines Verzeichnisindizes standardmäßig eingeschaltet ist, empfehle ich, diese Funktion zu deaktivieren oder das Verzeichnis inklusive der genannten Konfigurationsanweisungen vollständig zu entfernen, sofern Sie dieses nicht benötigen.

1.7.8 Tipp 8: /manual/ löschen

Dasselbe Problem wird durch die Konfigurationsanweisungen in Zeile 596-615 der *httpd.conf* erzeugt, die durch eine *AliasMatch*- und eine *Directory*-Anweisung das Handbuch des Apache als Verzeichnis */manual/* auf Ihrem Server veröffentlichen. Dabei handelt es sich nicht direkt um ein Sicherheitsrisiko, aber auch hier gibt das Vorhandensein eines solchen Verzeichnisses Aufschluss über den allgemeinen Konfigurationsstand des Servers. Außerdem ist für dieses Verzeichnis ebenfalls das automatische Erzeugen von Verzeichnisindizes eingeschaltet, weshalb ich dazu rate, diese Funktion zu deaktivieren oder das Verzeichnis inklusive der genannten Konfigurationsanweisungen vollständig zu entfernen.

1.7.9 Tipp 9: Test-Skripte löschen

Zu Testzwecken befinden sich im Verzeichnis *cgi-bin* Ihrer lokalen Apache-Installation zwei Skripte, die die Umgebungsvariablen des Servers ausgeben. Dadurch können Details der Serverkonfiguration (z.B. Datei- und Verzeichnispfade) veröffentlicht werden, die eigentlich nur den Administrator des Servers etwas angehen.

Das Vorhandensein dieser Skripte ist ein sehr deutlicher Hinweis auf den allgemeinen Konfigurationsgrad des Servers, insbesondere wenn solche Skripte später über eine Suche bei der Suchmaschine Google gefunden werden. Löschen Sie daher direkt nach der Installation des Apache die Skripte *test-cgi* und *printenv* aus dem Unterverzeichnis *cgi-bin*.

1.7.10 Tipp 10: Hilfsprogramme löschen

Viele Hersteller bieten fertige Installationspakete für den Apache an. Diese enthalten meist zusätzliche Konfigurationsanweisungen und Programme (z.B. htdig, sdbsearch, info2html), die beispielsweise das Durchsuchen des lokalen Hilfesystems der jeweiligen Distribution ermöglichen.

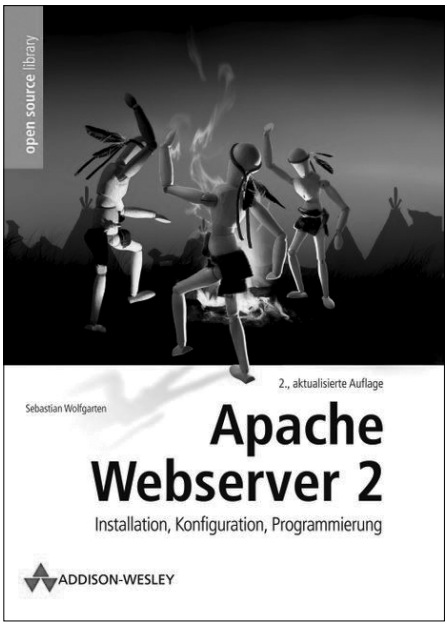
Aufgrund der Tatsache, dass diese Erweiterungen in der Vergangenheit mehrfach die Ursache von Sicherheitsproblemen waren (siehe http://lists.insecure.org/lists/bugtraq/2001/Aug/0028.html) und darüber hinaus Informationen über den allgemeinen Konfigurations- und Wartungsstand des Systems liefern, sollten Sie derartige Hilfsprogramme vollständig aus Ihrem System entfernen.

1.7.11 Fazit

Die genannten Vorschläge und Erfahrungswerte sind Hinweise, die die eigene Konfiguration des Apache sichern und darüber hinaus Einblicke in beliebte Konfigurationsmängel geben sollen. Sie sind keineswegs vollständig und führen nicht zur absoluten Sicherheit eines Systems, sondern sollen vielmehr als Hilfe zum sicheren Aufbau einer eigenen Konfiguration des Apache verstanden werden.

Sebastian Wolfgarten

Dieser Beitrag basiert auf Kapitel 9 des Buchs „Apache Webserver 2 – Installation, Konfiguration, Programmierung“ von Sebastian Wolfgarten. Dieses Standardwerk über den Apache Webserver mit über 900 Seiten können Sie als eBook in unserem Partnerbuchshop Informit.de für 19,95 Euro downloaden.



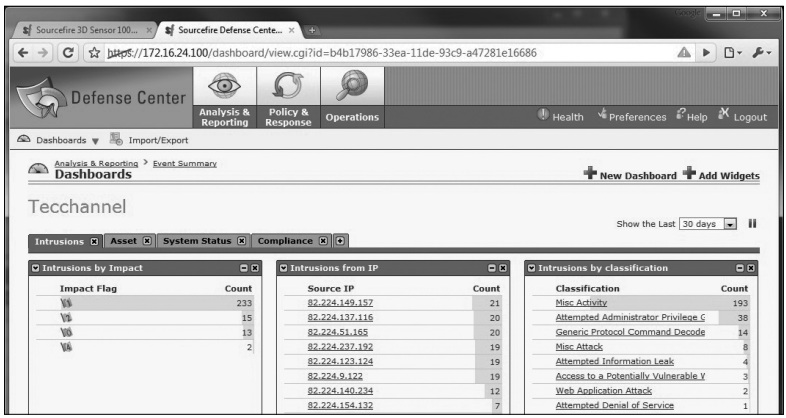
2 Netzwerksicherheit

Sicherheit in der Informationstechnik bedeutet in erster Line die Absicherung von Netzwerkinfrastrukturen. In diesem Kapitel erläutern wir aktuelle, praxisrelevante Ansätze zur Einbruchserkennung im LAN und WLAN.

2.1 Sourcefire: Intrusion Detection in der Praxis

Intrusion Detection ist eine der wichtigsten Komponenten für den Schutz eines Netzwerks. Sensoren analysieren den Netzwerk-Traffic und schlagen bei potentiell gefährlichen Aktivitäten Alarm. TecChannel nimmt die IDS/IPS-Lösung von Sourcefire in einem Praxistest unter die Lupe.

Nicht nur legitime Daten fließen durch Firmennetzwerke, auch Malware und Hacker-Attacken nutzen die vorhandene Infrastruktur. Systeme zur Intrusion Detection verfolgen kontinuierlich den Traffic und informieren, wenn sie ein Angriffsmuster oder ein verdächtiges Verhalten wahrnehmen. Kombiniert mit Intrusion Prevention können solche Systeme auch Gegenmaßnahmen einleiten.

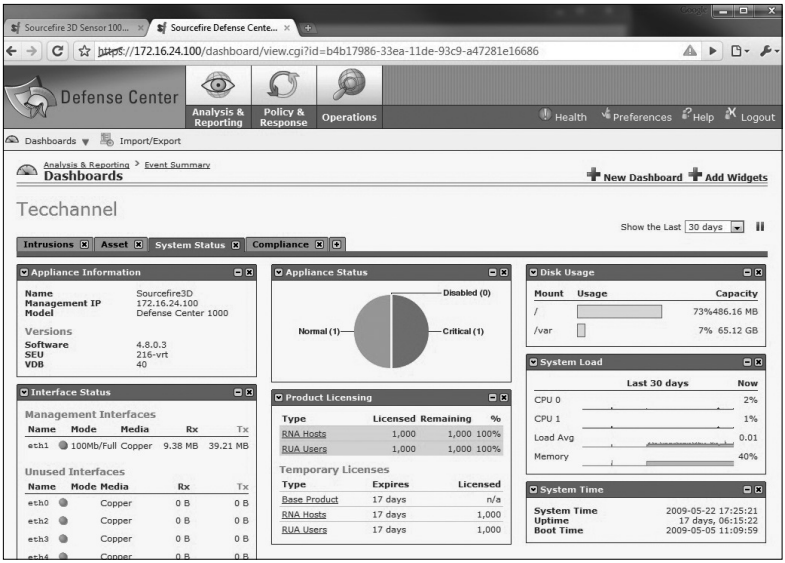


Dasboard: Die Widgets von Sourcefire stellen die jeweiligen Informationen aus dem Netzwerk da und lassen sich beliebig erweitern und durch den Administrator anpassen.

Für unseren Praxistest haben wir uns ein Überwachungssystem von Sourcefire (sourcefire.com) vorgenommen. Der Gründer von Sourcefire Martin Roesch ist in der Sicherheits-Szene kein Unbekannter. Er ist geistiger Vater von Snort, einem der bekanntesten Open-Source-Intrusion-Prevention-Systeme.

2.1.1 Test-Szenario und Aufbau

Unsere Testumgebung besteht aus einem Minimal-Setup. Dazu verwendeten wir ein Defence Center DC1000 (www.sourcefire.com/products/3D/defense_center) als Management-Server sowie einen Sensor vom Typ 3D1000 (www.sourcefire.com/products/3D/sensor). Theoretisch lässt sich der Sensor auch alleine betreiben, allerdings verliert man dann einiges an Komfortfunktionen. Der Sensor wurde per One Time Password am Defence Center angemeldet, anschließend ließ sich eine erste Policy erstellen und auf das System ausrollen.



Zustandsanzeige: Das Defense Center von Sourcefire verwaltet sämtliche an das IDS angeschlossenen Sensoren. Bis zu 100 sind maximal möglich.

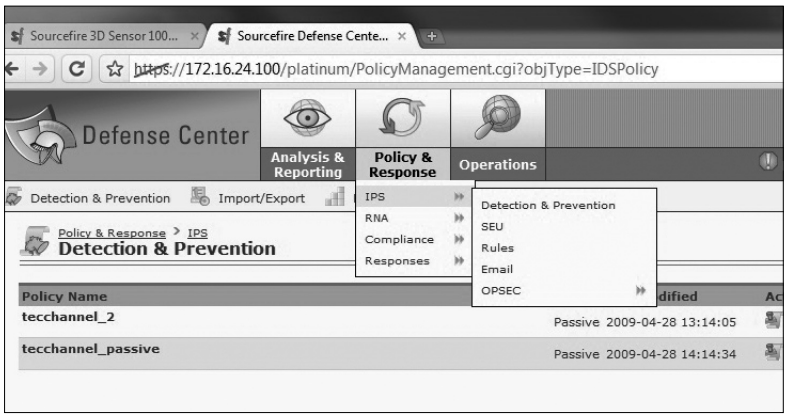
Da der reguläre Netzwerk-Traffic nur für wenig interessante Zwischenfälle gesorgt hätte, bespielten wir den Sensor mit zuvor aufgezeichnetem Datenverkehr, der auch mehrere Attacken und Exploit-Versuche enthielt.

Sind der oder die Sensoren platziert und mit dem Defense Center verbunden, lassen sie sich bequem steuern und auswerten. Ein weiterer Vorteil ist, dass die einzelnen Sensoren selbst nur wenig Speicherplatz benötigen, da das Defense Center die Informationen zentral verwaltet. Dadurch zeigen die Statistiken ein komplettes Bild der Vorgänge im Netzwerk. Außerdem kann man dadurch verhindern, dass Angreifer den Speicher der Sensoren gezielt vollschreiben, um ihre eigenen Spuren zu verdecken. Die Sensoren selbst müssen natürlich so platziert werden, dass sie jeden Verkehr im Netzwerk mitschneiden können. Dazu eignen sich etwa Mirror-

Ports, auf die der gesamte Verkehr des LANs gespiegelt wird. Etwas komplexer wird es, wenn eine größere virtuelle Infrastruktur überwacht werden soll: Der virtuelle Traffic lässt sich nur sehr schwer auf ein physikalisches Gerät spiegeln. Hier fehlen meist noch passende Lösungen, kommende Generationen von Virtualisierungssoftware, etwa VMware vSphere, wollen dieses Problem aber angehen.

2.1.2 In der Praxis

Das Interface des Defense Centers wirkt aufgeräumt. Im oberen Bereich finden sich die drei Menüpunkte Analys & Reporting, Policy & Response und Operations. Den größten Teil des Bildschirms belegt das Dashboard. Widgets, die sich beliebig anordnen lassen, zeigen eine Auswahl von Informationen an. Alle Widgets und Ansichten lassen sich nahezu beliebig verändern, umsortieren und anpassen.



Policy ausrollen: Die jeweiligen Sensoren lassen sich mit unterschiedlichen Richtlinien bestücken.

Sobald die Geräte im Netzwerk aktiv sind, beobachten sie den Traffic. Bevor sie allerdings sinnvolle Ergebnisse liefern, sollte eine Policy angepasst und ausgerollt werden. Sourcefire liefert fünf verschiedene Grund-Policies mit. Man kann diese wahlweise direkt verwenden oder sich neue Policies auf dieser Grundlage erstellen. Selbstredend kann man auch sie dahingehend einstellen, wann und wie ein Zuständiger alarmiert werden soll.

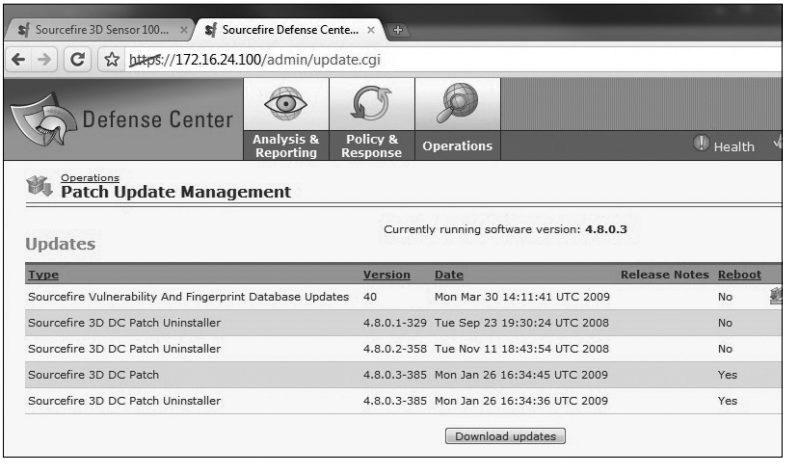
Zum Anpassen der jeweiligen Policy sollte man aber einiges an Zeit einplanen. Nahezu jedes vorhandene Protokoll lässt sich anpassen, einschränken oder freigeben. In jedem Fall ist es sinnvoll, das IDS zunächst in einem passiven Lauschmodus arbeiten zu lassen, um sich einen Überblick über das LAN zu verschaffen. Aus den jeweiligen Ergebnissen lassen sich anschließend passende Policies erstellen oder bestehende Richtlinien abändern.

Genauere Ergebnisse dank RNA

Für die Optimierung der Warnungen ist besonders das Feature Real-time Network Awareness, kurz RNA (www.sourcefire.com/products/3D/rna), interessant. Der separat lizenzierte Dienst legt nach und nach eine Übersicht an, welche Dienste, Betriebssysteme und Server im Netzwerk vorkommen. Das hilft zum einen bei der Inventarisierung und verfolgt zum anderen noch einen weiteren Zweck: Sobald sich RNA einen Überblick über das Netzwerk verschafft hat, können registrierte Angriffe deutlich besser bewertet und zugeordnet werden. Oder einfacher gesagt: In einer Linux-Only-Umgebung ist ein hoch kritisches Windows Server Exploit kein Grund für einen Alarm. Über diesen Dienst kann Sourcefire das Hintergrundrauschen sowie die False/Positive-Rate deutlich verringern.

Signatur- und Firmware-Updates

Wie bei einem Antivirensystem benötigt auch die Sourcefire IDS Signaturen, um Angriffe zuverlässig erkennen zu können. Allerdings variieren die Attacken deutlich weniger als bei Malware. Für das IDS kommen die gleichen Updates wie bei Snort zum Einsatz. Sourcefire aktualisiert die Datenbanken in regelmäßigen Abständen. Zunächst erhalten Abonnenten die neuen Signaturen, nach einiger Zeit stehen die Informationen allen zur Verfügung (www.snort.org/vrt/). Die Dateien lassen sich zentral herunterladen und anschließend auf die angeschlossenen Geräte per Push-Befehl verteilen.



Aktualisierung: Neue Firmware und neue Signaturen lassen sich zentral verwalten und ausrollen.

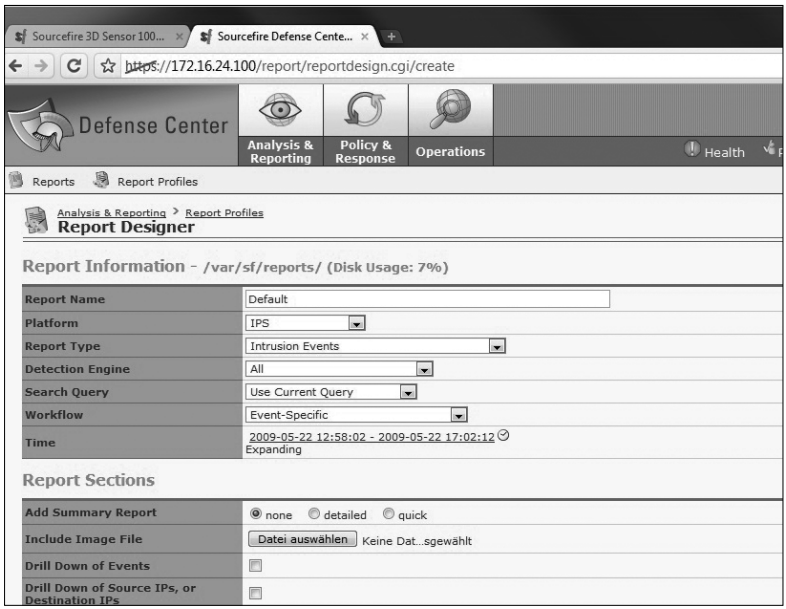
Neben VRT-Updates erhalten Anwender auch immer wieder Updates für die Firmware der eingesetzten Geräte. Praktischerweise lassen sich die Aktualisierungen sowohl beim Defense Center als auch bei den Sensoren direkt über das

Web-Interface herunterladen und einspielen. Außerdem ist es möglich, zu einer früheren Version zurückzukehren. Sollte der Internetzugriff nicht vorhanden sein, etwa wegen einer gegenwärtigen Attacke auf das Netzwerk, können Updates auch direkt auf das Defense Center und die Sensoren eingespielt werden.

2.1.3 Reports: Übersichtlich und anpassbar

Ebenso flexibel wie die Policies sind die Auswertungen. In den Widgets lässt sich so ziemlich jeder Wert aus der Sourcefire-Datenbank auslesen und darstellen. Das Dashboard selbst kann durch Tabs erweitert werden, sodass man die Übersichten thematisch aufbereiten kann. Diese Vielfalt hat sowohl Vor- als auch Nachteile. Denn zum einen kann man hoch spezialisierte Übersichten über das Netzwerk und die aktuellen Vorgänge schaffen, zum anderen sind ist das Erstellen mitunter aber zeitaufwendig, und im schlimmsten Fall verzettelt man sich in Einzelansichten und verliert damit den Überblick.

Im Test hat auch die sehr gute Benutzerverwaltung gefallen. Die Dashboards können für jeden Nutzer separat abgespeichert und eingerichtet werden. Damit ist sichergestellt, dass jeder die für ihn relevanten Daten erhält und sich seine Informationen nicht mühsam aus einem großen Dashboard zusammensuchen muss.



Flexibel: Reports lassen sich mit allen Werten der Datenbank bestücken und automatisch generieren.

Der gute Eindruck der Dashboards setzt sich bei den einzelnen Reports fort. Auch hier kann man detailliert einstellen, welche Informationen in welcher Form in welchem Report landen. Das Erstllen und Versenden der Reports lässt sich weitgehend automatisieren. Gut auch, dass die Daten in verschiedenen Formaten aufbereitet werden können; zur Auswahl stehen PDF, HTML oder CSV.

2.1.4 Fazit

Sourcefire ist nichts für kleine Netzwerke und „Nebenbei-Admins". Dazu ist die Lösung zum einen zu mächtig, zum anderen muss der Administrator die Zeit und das Wissen haben, die notwendig sind, um die Funktionen an seine Bedürfnisse anpassen zu können. Allein die vielfältigen Konfigurationsmöglichkeiten der Policies verwirren auf den ersten Blick, Fehlkonfigurationen sind da nahezu programmiert. In den Händen eines gut geschulten und fähigen Administrators dagegen wird das Sourcefire IDS eine mächtige Schutzkomponente im Netzwerk. Gerade durch die granularen Einstellungsmöglichkeiten lassen sich Bedrohungen gezielt erkennen, die sonst im Rauschen untergehen. Gerade hier hilft die Kombination mit der Real-Time-Network-Awareness-Komponente. Dadurch kann das System aktuelle Angriffe deutlich besser klassifizieren und dem Admin so viel Zeit ersparen. Besonders gut gefallen auch die vielfältigen Auswertungsmöglichkeiten. Sourcefire schafft es nicht nur, die Daten sinnvoll auswerten, sondern kann die einzelnen Reports auch für Nicht-ITler verständlich aufbereiten. Dadurch wird es deutlich einfacher, Argumente für Sicherheit im Unternehmensnetz vorzubringen und das notwendige Budget zu rechtfertigen.

Moritz Jäger

Moritz Jäger arbeitet als Redakteur im Software-Ressort bei TecChannel. Neben Themen rund um Open-Source, Virtualisierung und Sicherheit liegt sein Fokus auf Anwendungen, Lösungen und Tools für die mobile Arbeitswelt. Egal ob Push-Mail, Übertragungstechnologien, USB-Anwendungen oder Endgeräte und deren Absicherung – Jäger verlässt sich nicht auf die Herstellerangaben, sondern stellt die Testobjekte im praktischen Einsatz auf die Probe.

TecChannel-Links zum Thema	Webcode	Compact
Sourcefire: Intrusion Detection in der Praxis	2019109	S.48
Netzwerk-Überwachung mit Snort	431413	–
Schwachstellen aufspüren mit dem Nessus-Scanner	431420	–
Network Access Control für mehr Netzwerksicherheit	2018468	S.54

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

2.2 Network Access Control für mehr Netzwerksicherheit

Der Netzwerkzugang und das LAN müssen zuverlässig geschützt werden – besonders wegen gesetzlicher Mindestanforderungen. Einen praktischen Ansatz dazu bietet NAC. TecChannel sagt Ihnen, welche grundlegenden Anforderungen eine Network Access Control-Lösung erfüllen muss.

Netzwerke sind die Lebensadern modernen Firmen. Nahezu alle Informationen laufen heutzutage durch LANs. Doch sind Daten dort auch sicher? Wie wird beispielsweise sichergestellt, dass Nutzer keine unerlaubten Wireless Access Points einklinken oder dass Notebooks auch wirklich virenfrei von der Geschäftsreise zurückkommen? Mögliche Lösungen für diese Probleme sind unter der Abkürzung NAC für Network Access Controll oder Network Admission Control zusammengefasst. Diese Technologien sollen sicherstellen, dass nur genehmigte und ungefährliche Hosts Zugang zum Netzwerk erhalten. Damit wird nicht nur den jeweils bestehenden Policies genüge getan, NAC ist auch in wichtiger Bestandteil der meisten Compliance-Anforderungen.

Nach der Installation identifiziert die NAC alle im Netz angeschlossenen Geräte und prüft sie gegen die Sicherheitsanforderungen. Besteht ein Host den Test, erhält er Zugang zum Netz. Fällt das Testsubjekt durch die Prüfung, können die Geräte automatisch in ein Quarantäne-Netz aussortiert werden und erhalten eine entsprechende Behandlung. Des Weiteren ermöglicht NAC das Erstellen und Verwalten individueller Richtlinien und Rollen für verschiedene Nutzergruppen, beispielsweise für Gäste, die keinen Vollzugriff erhalten sollten.

2.2.1 Viel Nutzen, viel Aufwand

Obwohl die Vorteile klar auf der Hand liegen, scheuen sich viele Firmen davor, ein NAC-Projekt zu realisieren – nicht zuletzt aufgrund der hohen Kosten. Zudem sind viele NAC-Lösungen teuer, komplex oder lassen sich leicht umgehen. Einfache Plug-and-Play-Lösungen gibt es nicht; stattdessen ist ein hohes Maß an Konzeption im Vorfeld erforderlich.

In diesem Zusammenhang verfolgen Hersteller verschiedene Ansätze. Viele davon erfordern die Anschaffung einer komplexen Netzwerkarchitektur, die nicht selten auf Komponenten basiert, die in absehbarer Zeit überholt sein werden. Des Weiteren gibt es Lösungen, die nicht alle Teilbereiche eines Netzwerks berücksichtigen und beispielsweise ältere Komponenten außer Acht lassen, so dass weiterhin gefährliche Sicherheitslücken bestehen. Da jede NAC-Lösung zunächst eine Prozedur zur Netzwerkerkennung durchläuft, bei der viele manuelle Eingaben erfolgen müssen, gestaltet sich der Implementierungsprozess oft kompliziert und langatmig. Das gilt insbesondere, wenn Geräte erkannt werden müssen, die sich hinter Firewalls befinden oder nicht zentral administrierbar sind. Zudem wirft der Ein-

griff in Fremdrechner, etwa von Gast-Usern, rechtliche Fragen auf, beispielsweise bei der Installation spezieller Clients. Die Quintessenz: Der Markt ist verunsichert, und in Unternehmen bleiben erhebliche Sicherheitslücken.

Trotz aller Schwierigkeiten ist eine vollständige und verlässliche NAC, die im Rahmen des jeweiligen Security-Budgets bleibt und sich in das bereits vorhandene Netzwerk-Setup einfügen lässt, realisierbar und lohnenswert. Dazu sind aber einige Punkte zu berücksichtigen.

2.2.2 Transparenz ist der Schlüssel

Wie kann ein Netzwerk gegen Zugriffe von Fremdgeräten gesichert werden, wenn es nicht imstande ist, diese zu erkennen? Fakt ist, dass es mit lediglich partiellen Kenntnissen eines Netzwerks praktisch unmöglich ist, dieses sicher zu gestalten. Demnach müssen als Basis immer die Sichtbarkeit sowie die Identifizierung der Netzwerkkomponenten in Echtzeit gewährleistet sein. Ist dies nicht der Fall und werden lediglich bereits bekannte Geräte überwacht, ist das Netzwerk offen für Schädlinge, die sich von Fremd- oder nicht überprüften Rechnern einspeisen.

Network Access Control: Mit mobilen Endgeräten werden leicht digitale Schädlinge ins eigene Netz eingeschleppt, wenn keine Kontrolle stattfindet.

Daher ist es von zentraler Bedeutung, dass eine NAC-Lösung ein vollständiges Inventar aller im Netzwerk vertretenen Geräte anlegt und regelmäßig aktualisiert. Dabei sollte ebenfalls für Hardware-Firewalls und nicht verwaltbare beziehungsweise virtuelle Systeme ein ausführliches Profil angelegt werden. Zur Sichtbarkeit zählt auch, dass eine akkurate physikalische Karte des Netzwerks erstellt wird, um die vollständige IT-Infrastruktur abzubilden. Sie dient IT-Verantwortlichen als Grundlage für die zu ergreifenden Sicherheitsmaßnahmen.

2.2.3 Audit und Compliance

Das Einhalten von Sicherheitsrichtlinien wird durch verschärfte Gesetze zur Pflicht. Unternehmen müssen nachweisen können, dass sie alles in ihrer Macht Stehende tun, um einen wirksamen Schutz ihrer beziehungsweise der Kundendaten zu gewährleisten. NAC kommt dabei eine gewichtige Rolle zu, da es für jedes Gerät ein Profil erstellt, welches nach jeder Sicherheitsprüfung (Audit) aktualisiert wird. Darin enthalten sind User-Informationen, Funktionen und die eingesetzte Soft- und Hardware. Die Profile fungieren als Basis für die Entscheidung, ob ein Gerät den bestehenden Anforderungen durch Policies entspricht und ihm der Zugang zum Netz gewährt wird oder nicht. Hierbei ist es wichtig, dass wiederum sämtliche Systeme erfasst werden. Im Zuge der regelmäßigen Überprüfung identifizieren Audits Geräte, die nicht-konform, ungemanagt oder bösartig sind, noch bevor sie mit der Netzzugangskontrolle in Berührung kommen.

Des Weiteren werden jegliche Änderungen an einem System – seien es beispielsweise von Mitarbeitern installierte Programme auf Software- oder der Anschluss fremder Datenträger auf Hardwareebene – durch die Audits erkannt und gemeldet. Die jeweiligen Sicherheitsprüfungen werden in Form von Berichten gespeichert und bieten somit bei Compliance-Prüfungen die erforderlichen Nachweise über die Sicherheitsbemühungen eines Unternehmens.

2.2.4 Anforderungen an eine NAC-Lösung

Jede Netzwerkzugangskontrolle muss in Echtzeit operieren. Nur so lässt sich sicherstellen, dass sämtliche neu angeschlossenen Geräte sofort erkannt und in den NAC-Prozess mit einbezogen werden. Ohne Echtzeitkontrolle haben Angreifer eine große Auswahl an Möglichkeiten, ein Netzwerk zu attackieren und Schadcode einzuschleusen. Aus diesem Grund wird für unbekannte oder bei einer Prüfung aufgefallene Geräte eine Quarantänefunktion verwendet, die einen wichtigen Puffer vor dem eigentlichen Netzwerk bildet und mit diesem keine gemeinsame infrastrukturelle Basis haben darf. Daher sollte eine übergreifende Security Policy die Behandlung von Fremdgeräten für das gesamte Unternehmen einheitlich regeln, so dass es nicht in bestimmten Abteilungen zu Ausnahmefällen komm

Innerhalb der Quarantäne müssen standardisierte Sicherheits-Checks vorgenommen werden. Hierbei analysiert die NAC beispielsweise, ob aktuelle Service Packs, Patches, Updates oder eine aktive Antivirussoftware auf dem jeweiligen System installiert sind. Zutritt zum Netzwerk wird erst dann gewährt, wenn ein Check vollständig erfolgreich ausfällt. Rechner, bei denen die NAC nicht Policy-konforme Änderungen feststellt, müssen dieselbe Prozedur durchlaufen. Anhand der gespeicherten Profile sollte eine Lösung auch erkennen, ob zum Beispiel die MAC-Adresse eines Rechners missbraucht wird, um ein Fremdgerät ins Netzwerk zu schmuggeln. Von Vorteil ist für den Benutzer eine transparent agierende NAC. Das bedeutet, dass das System lediglich im Falle eines Verstoßes gegen die beste-

henden Sicherheitsrichtlinien bemerkt wird, da es den Benutzer aus dem Netzwerk ausschließt. Konforme User werden ohne eine gesonderte Anmeldeprozedur völlig unauffällig durch den NAC-Prozess geleitet.

Soll die Möglichkeit gegeben werden, dass auch Besucher Zutritt zum Unternehmensnetz erhalten, steigen die Anforderungen an die Flexibilität eines NAC-Systems immens. Da die Gäste nicht von der NAC gemanagt werden, bedürfen sie einer Sonderbehandlung, bei der sichergestellt wird, dass keine Schädlinge ins Netzwerk hinein- beziehungsweise keine vertraulichen Daten hinausgelangen. Dementsprechend muss die NAC sie identifizieren und automatisch nur für ein im Vorfeld festgelegtes, mit starken Einschränkungen verbundenes Benutzerprofil autorisieren. Geht es um die Einhaltung von Policies, bedingen viele NAC-Lösungen ein blindes Handeln der Benutzer. Die Konsequenzen der umgesetzten Richtlinien lassen sich oftmals nicht vorhersagen, so dass eventuell fehlerhafte Policies einen erheblichen Schaden in der IT-Infrastruktur eines Unternehmens anrichten. Eine gute Netzzugangskontrolle beinhaltet daher die Möglichkeit, das Umsetzen bestimmter Richtlinien im Vorfeld zu simulieren. Zuletzt sollte eine NAC-Lösung das gesamte Spektrum eines Netzwerkes abdecken.

2.2.5 Fazit

Network Access Control sollte als Sicherheitsmethodik betrachtet werden. Eine NAC-Lösung lohnt sich nur dann, wenn sie im ersten Schritt das Netz grundlegend überprüft. Dazu erstellt sie Profile von jeglichen Geräten, die mit dem Netzwerk verbunden sind, und erkennt dabei die nicht konformen, unbekannten und unautorisierten Geräte, noch bevor die NAC-Prozesse aktiviert werden.

Ferner sollte eine Netzwerkzugangskontrolle in hohem Maße skalierbar sowie relativ einfach in die gesamte IT-Infrastruktur zu implementieren sein, um sich schnell zu rentieren. Eine Lösung, die alle oben genannten Punkte erfüllt, bietet beispielsweise der Hersteller Insightix an. Hierbei handelt es sich um eine umfassende Zugangskontrolle in Echtzeit, wobei garantiert ist, dass nur autorisierte sowie Compliance-konforme Geräte Zugriff auf das Netzwerk erhalten beziehungsweise in diesem operieren dürfen.

Thomas Hruby

TecChannel-Links zum Thema	Webcode	Compact
Network Access Control für mehr Netzwerksicherheit	2018468	S.54
Grundschutz für Web-Applikationen	1785530	S.10
Sicheren Gastzugang für LAN und WLAN realisieren	1768961	–
Sicherheitslücke Roadwarrior	402189	–
Sourcefire: Intrusion Detection in der Praxis	2019109	S.48

2.3 Ports scannen mit Nmap & Co.

Ohne Ports und Portnummern wäre eine Kommunikation über die im Internet üblichen Protokolle Transmission Control Protocol (TCP) und User Datagram Protocol (UDP) nicht möglich. Doch offene Ports sind potenzielle Einfallstore für Angreifer. Für die richtige Konfiguration von Abwehrmaßnahmen wie Firewalls ist ein tiefergehendes Verständnis daher unerlässlich.

Der Löwenanteil der Internetkommunikation zum Browsen und für E-Mails läuft über das TCP- und das UDP-Protokoll ab. Jeder Anwendung, die mit dem Internet in Verbindung steht, weisen die Protokolle TCP und UDP eine Portnummer zu. So „weiß" jedes Datenpaket, zu welcher Anwendung es gehört, der Port ist sozusagen die Adresse für einen bestimmten Typ von Internet-Daten. Ein HTTP-Paket für den Browser landet also nicht im Mailprogramm und ein Paket mit Mail findet den Weg in Ihren Mailclient und landet nicht im Browser, jedes Datenpaket erreicht dank der Portnummern sein richtiges Ziel.

2.3.1 Sockets sind die Adressen von PC und Servern

Komplettiert wird die Adresse eines Datenpaketes mit der IP-Adresse des Zielrechnerns. Die Kombination aus IP-Adresse des Zielrechners und Portnummer der Zielanwendung auf dem Zielrechner nennt man Socket. Zwei Sockets definieren eine Verbindung, einer für den Ausgangs- und einer für den Zielrechner. Dank des Sockets landet jedes Datenpakt auf dem richtigen Rechner in der richtigen Anwendung. Umgekehrt gibt es natürlich auch auf dem Server, der die Daten bereit stellt, die Sockets, sprich: Auch dort müssen die entsprechenden Ports geöffnet sein. Womit wir wieder beim Thema wären.

Der für eingehende Mails zuständige POP3-Server arbeitet beispielsweise am Port 110, ein Webserver lauscht am Port 80. Soll es ein andere Port sein, weil Sie zum Beispiel zwei Webserver gleichzeitig betreiben, müssen Sie das ausdrücklich so festlegen, beispielsweise bei Apache in dessen Konfigurationsdatei.

Jedes Datenpaket weiß also, an welchen Port es gerichtet ist. Dafür wird ihm nämlich im Header des Datensegments die Absender- und Ziel-Portnummer hinzugefügt. Das gilt sowohl für das TCP- als auch für das UDP-Protokoll.

Serverprozesse haben immer statische Portnummern, Clientanfragen bekommen dagegen bei jeder Anfrage eine dynamische Portnummer zugewiesen. Ein eindeutiges Socket für eine Anfrage an einen Webserver mit der IP-Adresse 192.168.1.18 kann beispielsweise folgendermaßen aussehen: 192.168.1.18:80. Und wenn der anfragende Clientrechner die IP-Adresse 192.168.100.12 hat, dann würde das Socket für die ausgelieferte Website folgendermaßen aussehen: 192.168.100.12:49152 – wobei letzteres der dynamisch zugeteilte Port für die Antwort wäre.

2.3.2 Well known und registrierte Ports

Bei Portnummern unterscheidet man grundsätzlich drei Gruppen: Well Known (0-1023) Ports, registrierte Ports (1024-49151) und dynamische/private Ports (49152-65535). Die so genannten Well Known Ports umfassen bekannten Nummern für gängige Dienste wie HTTP, IMAP, POP3, SMTP, Telnet, FTP, um nur einige Beispiele zu nennen. TCP und UDP verwenden oft, aber nicht immer, die gleichen Portnummern, einige Portnummern kommen auch nur unter einem der beiden Protokolle zum Einsatz.

Einige Beispiele für Well Known Ports

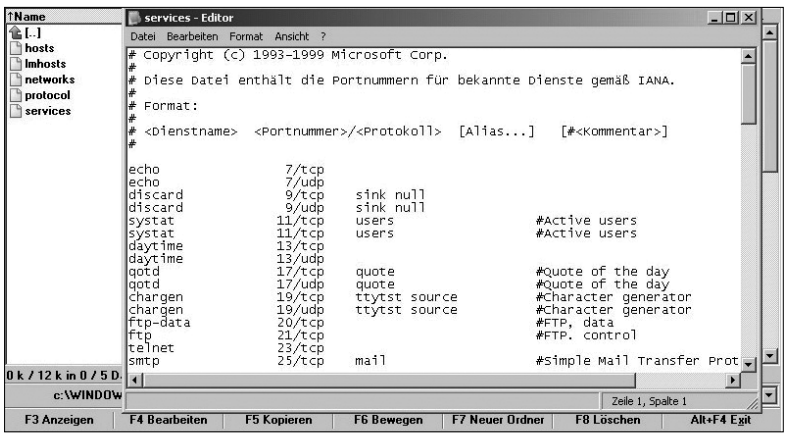
Port	Einsatz
7	Echo
20	FTP-Datentransfer vom Server zum Client
21	FTP-Steuerbefehle durch den Client
23	Telnet-Kommunikation (unsichere Verbindungsmethode aus den Urzeiten des Internets, weil sie Daten unverschlüsselt überträgt)
25	SMTP-Mail-Versand
43	DNS-Auflösung von Domainnamen in IP-Adressen
80	http-Webserver
110	POP3-Client-Zugriff für Mail-Server
143	IMAP
194	IRC
389	LDAP
443	HTTPS
531	AIM, ICQ
666	DOOM-Online-Spiel
901	SWAT
989	FTPS-Daten
990	FTPS-Steuerbefehle

Registrierte Ports gibt es für bestimmte Anwendungen von Herstellern, die ein Benutzer selbst installiert. Proxy-Server sind hierfür ein Beispiel oder SIP mit dem Port 5060 (SIP findet bei vielen VoIP-Diensten Verwendung). Den Port 3306 nutzen MySQL-Datenbanken, 8080 und 8008 sind ebenfalls relativ bekannte Portnummern, weil sie als Alternative für 80 genommen werden. Die ist sinnvoll, wenn zwei Webserver gleichzeitig auf einem System laufen, beispielsweise ein Apache und ein IIS, oder man einen zusätzlichen Webserver zu Testzwecken betreiben.

```
 7 # Updated from http://www.iana.org/assignments/port-numbers and other
 8 # sources like http://www.freebsd.org/cgi/cvsweb.cgi/src/etc/services .
 9 # New ports will be added on request if they have been officially assigned
10 # by IANA and used in the real-world or are needed by a debian package.
11 # If you need a huge list of used numbers please install the nmap package.
12
13 tcpmux          1/tcp                           # TCP port service multiplexer
14 echo            7/tcp
15 echo            7/udp
16 discard         9/tcp           sink null
17 discard         9/udp           sink null
18 systat          11/tcp          users
19 daytime         13/tcp
20 daytime         13/udp
21 netstat         15/tcp
```

Übersicht: Portliste auf einem Linuxsystem.

Die Port-Liste eines Linuxrechners findet man unter *etc/services.* Bei Windows XP liegt diese Übersicht unter *%WINDIR%\system32\drivers\etc\services.* Die dynamischen/privaten Ports sind keiner Anwendung fest zugewiesen und werden je nach Bedarf eingesetzt. Eine Liste der gängigen Portnummern finden Sie hier bei der IANA (www.iana.org/assignments/port-numbers).



Auswertung: Portliste auf einem Windowssystem.

2.3.3 Ports schließen oder absichern

Damit ein Rechner mit dem Internet kommunizieren kann, müssen also zwingend einige Ports offen sein. Jeder offene Port ist aber ein potenzielles Einfallstor für Angreifer, wenn die an dem Port lauschende (also bereit stehende) Anwendung eine Sicherheitslücke aufweist. Um absolute Sicherheit zu bekommen, müsste man alle Ports schließen, doch dann ist keine Internetverbindung mehr

möglich. Ergo müssen einige Ports offen bleiben. Somit gilt die Faustregel: So viele Ports wie nötig und so wenige wie möglich freischalten. Konkret bedeutet das, dass man Dienste, die man nicht benötigt, einfach abschaltet, bevor ein Angreifer diese zum Eindringen in Ihr System ausnutzt.

Der Anwender sollte aber wissen, welche Ports aktuell auf seinem Rechner tatsächlich erreichbar sind und welche Anwendungen an welchen Ports „lauschen". Ports für Dienste, die man benötigt, beispielsweise für Mails, für das Surfen, für Instant Messaging oder weil man Filesharing macht, sollten zumindest überwacht werden. Beispielsweise durch einen Sniffer, der aufzeichnet, wann welche Datenpakete über welchen Port an welche Zieladresse abgingen beziehungsweise eintrafen. Wireshark (Webcode **431415**) ist hierfür ein geeignetes Tool .

Dienste, die Sie benötigen und deshalb nicht abschalten können, sollten Sie möglichst so konfigurieren, dass nicht von jedem beliebigen Rechner der Zugriff darauf möglich ist, sondern nur von bestimmten Rechnern, beispielsweise nur von PCs aus Ihrem Intranet. Unter Linux können Sie den Zugriff auf bestimmte Dienste ergänzend auch via TCP-Wrapper steuern (hosts.deny und hosts.allow). Zudem sollten Sie Ihre Firewall so restriktiv konfigurieren, wie es nur irgendwie möglich und sinnvoll ist. Für jedes Betriebssystem existieren einige einfache Tools, mit denen Sie in wenigen Sekunden ermitteln können, welche Ports auf Ihrem System geöffnet sind. Diese Tools sollten Sie kennen und zumindest eines davon regelmäßig nutzen, um Ihren Rechner oder Ihr Heim- beziehungsweise Firmennetzwerk auf Einfallstore zu scannen, bevor das ein Angreifer macht.

2.3.4 So spüren Sie offene Ports auf

Der einfachste Weg um offene Ports anzuzeigen, sind die Bordmittel der Betriebssysteme. Mit dem unter Windows und Linux gleichermaßen verfügbaren Kommandozeilenbefehl `netstat` ermitteln Sie, welche Netzwerkverbindungen Ihr PC aufgebaut hat. Unter Windows Vista öffnen Sie etwa über *Start, cmd* eine DOS-Box, in die den Befehl `netstat -an` eintippen. Daraufhin zeigt Ihnen Windows alle Netzwerkverbindungen auf einer Maschine an, laufende Serverdienste sind mit *Listen*, *Listening* oder *Abhören* gekennzeichnet. Mit der Option `-o` wird zu jedem Port die Prozess-ID PID des dazu gehörigen Prozesses angezeigt.

```
C:\Dokumente und Einstellungen\strategos>netstat -ano

Aktive Verbindungen

  Proto  Lokale Adresse          Remoteadresse          Status          PID
  TCP    0.0.0.0:135            0.0.0.0:0              ABHÖREN         924
  TCP    0.0.0.0:445            0.0.0.0:0              ABHÖREN         4
  TCP    0.0.0.0:56089          0.0.0.0:0              ABHÖREN         1532
  TCP    127.0.0.1:1031         0.0.0.0:0              ABHÖREN         3716
  TCP    127.0.0.1:1041         127.0.0.1:1042         HERGESTELLT     3240
  TCP    127.0.0.1:1042         127.0.0.1:1041         HERGESTELLT     3240
  TCP    127.0.0.1:1048         127.0.0.1:1049         HERGESTELLT     3240
  TCP    127.0.0.1:1049         127.0.0.1:1048         HERGESTELLT     3240
  TCP    127.0.0.1:5152         0.0.0.0:0              ABHÖREN         1560
```

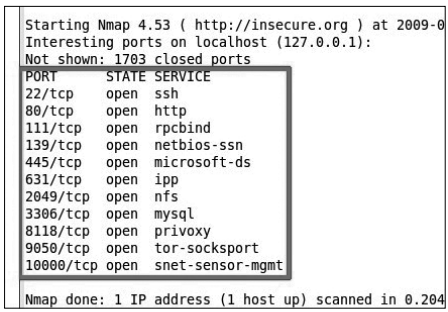
Offene Ports finden: Netstat unter Windows.

Ein beliebtes Hilfsmittel zum Erkennen offener Ports sind jedoch Portscanner, die viel differenzierte Möglichkeiten für das Scannen von Ports bieten und mit denen sich unter Umständen sogar die komplette Struktur eines Netzwerks anzeigen lässt. Ein Portscan ist ganz besonders dann unverzichtbar, wenn Sie auf Ihrem Rechner neue Anwendungen installiert oder neue Dienste gestartet haben. Machen Sie dann einen Portscan Ihres Systems um sich zu vergewissern, ob dadurch neue Ports geöffnet wurden.

Wichtiger rechtlicher Hinweis: Die hier vorgestellten Werkzeuge sind für jeden Anwender, der sich professionell mit seinem Netzwerk oder seinem Internet-PC beschäftigen und Sicherheitslücken entdecken und schließen will, unverzichtbare und im Praxiseinsatz bei Unternehmen und Behörden vielfach erprobte Werkzeuge. Da die Gesetzeslage in der Bundesrepublik Deutschland aber in Bezug auf derartige Sicherheits-Werkzeuge nicht unproblematisch ist, verzichten wir auf eine direkte Download-Verlinkungen zu diesen Tools und auf Schritt-für-Schritt-Anleitungen. Setzen Sie Portscanner und Sniffer nur in Ihrem eigenen Netzwerk ein und nur, wenn Sie Ihr Netzwerk alleine nutzen. Scannen Sie keine Ports von fremden Netzwerken und lesen Sie keinen fremden Netzwerk-Traffic mit.

2.3.5 Mit Nmap offene Ports erkennen und analysieren

Der quelloffene und kostenlose Portscanner Nmap (Network Mapper) eignet sich hervorragend um offene Ports in Ihrem Netzwerk zu entdecken. Nmap unterstützt alle gängigen und auch weniger bekannte Betriebssysteme wie beispielsweise FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS und Amiga. Für die jeweiligen Betriebssysteme stehen eigene Downloadpakete zur Verfügung (außerdem steht der Quellcode für Anwender bereit, die Nmap selbst kompilieren wollen). Für Windows greifen Sie am besten zum selbstextrahierenden ZIP-Archiv. Darin ist nicht nur der eigentliche Portscanner (also das Kommandozeilentool), sondern auch die grafische Bedienoberfläche Zenmap enthalten, mit der sich Nmap wie eine normale Windows-Anwendung bedienen lässt. Zu Zenmap lesen Sie später mehr.



```
Starting Nmap 4.53 ( http://insecure.org ) at 2009-0
Interesting ports on localhost (127.0.0.1):
Not shown: 1703 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
2049/tcp  open  nfs
3306/tcp  open  mysql
8118/tcp  open  privoxy
9050/tcp  open  tor-socksport
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 0.204
```

Port-Analyse: Nmap unter Linux.

Nmap gehören für jeden Netzwerkbetreiber zu den unverzichtbaren Werkzeugen. Sie können damit ganz einfach das Antwortverhalten Ihres Netzwerks nach außen hin überprüfen. Wenn der Scanner installiert ist, können Sie beispielsweise unter Linux mit Rootrechten und dem Befehl `nmap localhost` Ihr System auf geöffnete Ports hin überprüfen. Beim Portscan werden sowohl TCP als auch UDP unterstützt. Typischerweise wird Nmap von der Kommandozeile aus gestartet, ganz einfach geht das mit folgendem Befehl: `nmap -v -A targethost`. Bei targethost geben Sie die IP-Adresse des zu überprüfenden Rechners ein. Doch Nmap besitzt noch viel mehr Optionen für den professionellen Einsatz, die Sie auf der Kommandozeile mit angeben können. Wenn Sie beispielsweise nur Ports für TCP-Verbindungen suchen, sollten Sie `nmap –sT` eingeben. Eine Liste der Optionen finden Sie auf dieser Seite http://nmap.org/book/man-briefoptions.html .

2.3.6 Fingerprinting: Betriebssysteme identifizieren

In Zusammenhang mit Portscans sollte auch das OS-Fingerprinting erwähnt werden. Jedes Betriebssystem hinterlässt seinen eigenen Fingerabdruck im Internet, beispielsweise anhand der TCP/IP-Stack-Implementation. Diesen Vorgang nennt man OS-Fingerprinting. Ein Portscanner kann versuchen, anhand dieses Fingerabdrucks das Betriebssystem zu identifizieren. Da das auch die Vorgehensweise von Hackern ist, sollten Sie selbst auch einmal Ihr System daraufhin überprüfen, wie es sich nach außen hin zu erkennen gibt.

Man unterscheidet zudem zwischen aktiver und passiver Betriebssystemerkennung. Bei der aktiven wird dem gescannten Rechner quasi ein Datenpaket als Köder geschickt. Das Analyseprogramm schickt selbst Datenpakete an den zu untersuchenden Rechner. Der Zielrechner antwortet auf dieses Paket, aus der Antwort kann dann versucht werden, das System zu identifizieren. Dieses aktive Vorgehen liefert exaktere Ergebnisse, kann aber von einem Administrator auch leichter erkannt werden. Wenn Sie nur Ihr eigenes Netzwerk scannen, stellt das kein rechtliches Problem dar: Ihre eigenen Systeme dürfen Sie scannen, versuchen Sie also ruhig die aktive Methode. Bei der passiven Methode liest das Scannerprogramm nur den Traffic an den überwachten Rechner mit. Hier bleibt der Scannende zwar gut getarnt, weil er nur Pakete analysiert, die für den überwachten Host gedacht sind, dafür bekommt man aber auch weniger exakte Ergebnisse. Ein aktiver Versuch zur Identifizierung des Betriebssystems des Zielrechners mit abgeschickten TCP-Paketen sieht beispielsweise so aus: `nmap -sT -O Clientname` (wenn man den Scanvorgang beschleunigen will, kann man zusätzlich mit „-p“ auch noch gezielt den Port angeben, an den Nmap das Datenpaket schicken soll). Das „-O“ steht für „Enable OS detection“. Schutzmaßnahmen gegen Fingerprinting bestehen etwa darin, dass der Zielrechner so konfiguriert ist, dass er keine Informationen über sich preis gibt oder dass er sogar falsche Informationen sendet um den Angreifer zu verwirren. Admins können einen Portscan unter Umständen mit Intrusion Detection Systemen erkennen. Nmap kann deshalb so konfiguriert wer-

den, das er verborgen scannt und einen Stealth-Scan durchführt. Nmap und das auf der nächsten Seite erklärte Zenmap sind für die Betriebssystemerkennung aber nicht ohne Konkurrenz. Ähnliche Aufgaben übernimmt zum Beispiel Xprobe2. Auch p0f scannt Ports und versucht das Betriebssystem zu ermitteln.

2.3.7 Zenmap: Grafische Oberfläche für Nmap

Nmap besitzt eine Fülle von Optionen, die Sie auf der Kommandozeile eintippen müssen. Kryptisch anmutende Kommandozeilenbefehle mit komplizierten Options- und Parameterfolgen sind nicht jedermanns Sache. Das gilt besonders für Windows-Anwender. Doch es gibt Abhilfe: Zenmap, eine grafische Bedienoberfläche (GUI) für Nmap. Zenmap stellt zudem zusätzliche Funktionen zur Verfügung. Mit Zenmap wird der Netzwerkscan deutlich vereinfacht. Geben Sie einfach die zu scannende IP-Adresse (oder den IP-Adressbereich) oder den Hostnamen und die Art des Scans ein. Der Benutzer kann bei Zenmap unter unterschiedlich umfangreichen Scans wählen. Beispielsweise ein kompletter Scan (mit oder ohne UDP), ein schneller Scan für die gängigsten TCP-Ports oder ein reiner Ping-Scan, um die Verfügbarkeit eines Rechners zu testen und sich erst einmal einen Überblick über die in einem bestimmten Adressraum verfügbaren Rechner zu verschaffen. Je nach Umfang des Scans erscheinen schon nach wenigen Sekunden oder erst nach einigen Minuten die Resultate. Die von Zenmap zur Auswahl gegebenen Scanprofile lassen sich nach Belieben anpassen und ergänzen.

```
TRACEROUTE (using port 3389/tcp)
HOP RTT   ADDRESS
1   0.00  192.[redacted]
2   0.00  idg-fw-1-berlin.idgmuc.idg ([redacted])
3   16.00 217.111.81.2
4   16.00 irl.ber.network.bln.de.colt-isc.net (62.96.179.33)
5   0.00  gel-1-4-cr3.BER.router.colt.net (212.74.74.226)
6   31.00 ge0-1-prl.muc.router.colt.net (212.74.75.143)
7   31.00 inxs.core01.muc01.atlas.cogentco.com (194.59.190.33)
8   15.00 tel-2.ccr01.nue01.atlas.cogentco.com (130.117.1.246)
9   31.00 tel-2.ccr01.drs01.atlas.cogentco.com (130.117.2.54)
10  32.00 neue-medien.demarc.cogentco.com (130.117.21.210)
11  31.00 dd2330.kasserver.com (85.[redacted])
```

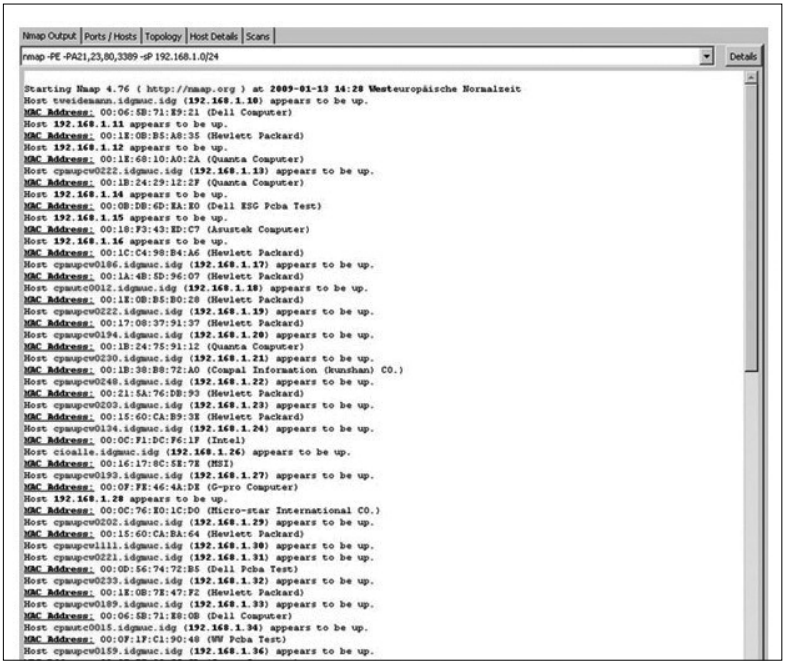
Traceroute-Ergebnis von Nmap

Routenverlauf: Traceroutergebnis mit Nmap.

Der Abschluss der kompletten Scans kann Zeit in Anspruch nehmen. Im rechten Ausgabefenster dokumentiert Nmap daher seine Arbeitsschritte: Welche Ports überprüft werden, welche Art von Scan gerade erfolgt und wie die Ergebnisse aussehen. Geschlossene Ports werden nicht separat angezeigt, zu den geöffneten Ports gibt es dagegen Detailinformationen wie „offen“ oder „gefiltert“, welcher Dienst konkret an einem offenen Port lauscht und welche Softwareversion des jeweiligen Dienstes Nmap zu erkennen glaubt. Wenn der Port 80 offen ist, weil ein Webser-

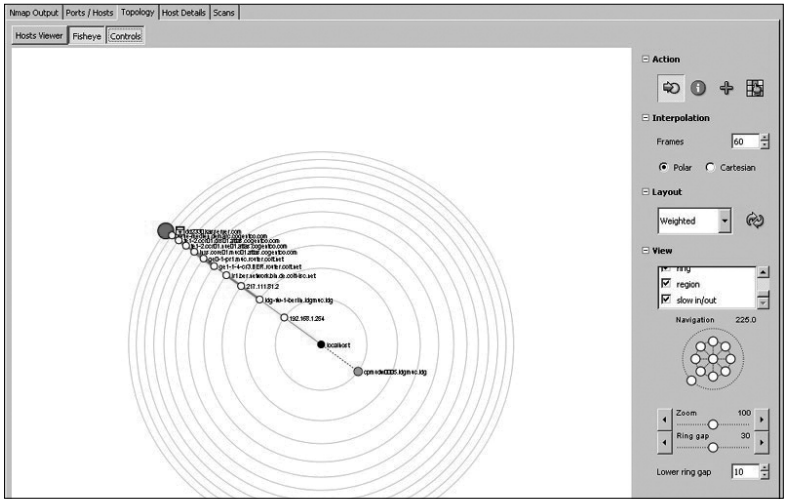
ver auf dem gescannten System läuft, dann liefert Nmap beispielsweise die Angabe, welche Apacheversion er entdeckt zu haben glaubt. Oder welche MySQL-Datenbankversion auf dem Server ihre Dienste verrichten soll. Und welcher Mailserver vermutlich die Post zustellt.

Zudem gibt Nmap an, wieviele Hops (also Sprünge von einem Netzknoten zum nächsten) nötig sind, bevor das Datenpaket vom Ausgangsrechner aus den Zielrechner erreicht hat. Nmap liefert auch gleich die Route dafür mit, sprich: die Ergebnisse der Netzwerk-Befehle `Traceroute/tracert`. Auch bei Zenmap versucht Nmap herauszubekommen, welches Betriebssystem vermutlich auf dem Zielrechner installiert ist – hierfür wird die oben beschriebene Fingerprintmethode eingesetzt. Die OS-Erkennung soll nicht nur mit typischen PC-Systemen wie Windows (einschließlich Vista mit SP1), Linux und MacOS, sondern auch mit Wii-Konsolen und iPhones klappen. Die Scanergebnisse können zur späteren Analyse bequem in Dateien gespeichert werden.



Antwort ermitteln: Einfacher Ping-Scan.

Wenn Sie gleich mehrere Rechner auf einmal scannen wollen: Kein Problem, bei Target können Sie auch IP-Ranges eingeben. Wenn Sie dabei aber „intense Scan“ wählen, kann der Scanvorgang sehr lange dauern.



Übersichtlich: Zenmap erstellt die Netzwerk-Topologie.

In Nmap ist seit Version 4.75 Radialnet integriert. Damit lassen sich die Netzwerke visuell darstellen. So entsteht quasi eine Karte des Netzwerks, auf der die geöffneten Ports pro Host angezeigt werden. Jeder Kreis stellt einen PC dar, Farbe und Größe eines solchen Punktes hängen von der Zahl der offenen Ports ab. Router werden als Quadrate dargestellt.

Hans-Christian Dirscherl

Hans-Christian Dirscherl ist Redakteur bei unserer Schwesterpublikation PC-WELT, von der wir diesen Beitrag übernommen haben.

TecChannel-Links zum Thema	Webcode	Compact
Ports scannen mit Nmap & Co.	2019857	S.S.58
Ports im Überblick	401852	–
So funktionieren TCP/IP und IPv6	401211	–
Rootkit-Detection	431416	–

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

2.4 Millionen DSL-Router hochgradig gefährdet

Cross Site Request Forgery als Angriffsvektor wurde lange unterschätzt. Doch jetzt ist es TecChannel gelungen, über einfache CSRF-Attacken DSL-Router von A wie AVM Fritz!Box bis Z wie ZyXEL über das Internet von außen anzugreifen. Surft man mit dem PC auf eine manipulierte Website, kann die komplette Konfiguration der DSL-Router unbemerkt modifiziert werden.

Bislang gelten Cross Site Scripting und Injection-Angriffe als Haupteinfallsvektor für erfolgreiche Attacken auf Web-Server. Doch in der aktuellen Liste der gefährlichsten Fehler, die regelmäßig von der OWASP (Open Web Application Security Project) herausgegeben wird, hat sich Cross Site Request Forgery (CSRF) inzwischen auf Platz fünf hochgearbeitet.

Wie gefährlich dieser bislang unterschätzte Angriffsweg tatsächlich ist, zeigen aktuelle Sicherheitstests von TecChannel. Im Folgenden erläutern wir zunächst die gar nicht so schwierige Theorie hinter CSRF. Anschließend demonstrieren wir zwei Angriffe auf unserer eigene Site TecChannel.de, die einige harmlose CSRF-Schwachstellen enthält. Aber dann geht es ans Eingemachte:

Über CSRF-Attacken ist es uns gelungen, die Konfiguration der AVM Fritz!Box (www.avm.de), des Cisco/Linksys WAG 160 N (www.linksysbycisco.com) und eines ZyXEL P-660HW (www.zyxel.de) beliebig zu modifizieren. Aber auch die meisten anderen DSL-Router dürften gefährdet sein. Für den Angriff genügt es, dass der Anwender eine präparierte Website besucht. Diese kann dann Konfigurationsarameter, die über die Web-Oberfläche des DSL-Routers zu erreichen sind, beliebig ändern. Ein Besuch einer manipulierten Seite, und alle Telefonate laufen bei einem Router mit Telefoniefunktion über eine teure 0900er-Vorwahl.

Der Passwortschutz der Router erwies sich dabei als nicht ausreichend. Welches Gefahrenpotenzial sonst noch in dem CSRF-Angriff steckt und was man gegen Attacken auf die DSL-Router unternehmen kann, lesen Sie am Ende dieses Beitrags.

2.4.1 Angriffsvektor CSRF (XSRF oder Session Riding)

Die Non-Profit-Organisation OWASP veröffentlicht alle zwei Jahre eine Liste der gängigen Angriffe auf Web-Anwendungen (www.owasp.org/index.php/Top_10_2007). Ziel ist es, Web-Entwickler, Web-Designer und Firmen mit Web-Anwendungen für die aktuellen Gefahren zu sensibilisieren.

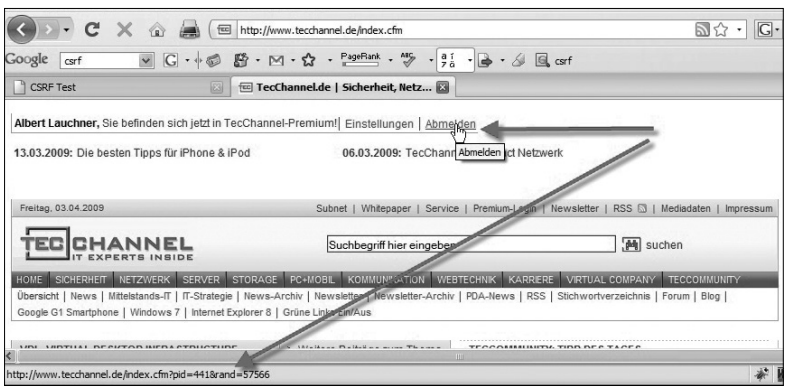
Seit Jahren belegen die inzwischen hinlänglich bekannten Cross Site Scriptings und Injections die vorderen Plätze. Bei diesen Attacken schreibt der Angreifer ausführbaren Code in Eingabefelder von Web-Anwendungen. Wird die Eingabe nicht sauber gefiltert und umcodiert, führt beim Cross Site Scripting der Browser bösartigen Code aus. Bei Injections hingegen gelangt der Code bis zu den Servern. Bei

SQL-Injections etwa schleust man so SQL-Anweisungen zur Datenbank durch und kann dann Daten entwenden oder zerstören. In der Regel ist der Angreifer beim Cross Site Scripting oder bei Injections selbst aktiv und gibt den kritischen Code über seinen Browser ein. Cross Site Request Forgery wählt einen ganz anderen Weg. Hierbei wird ein nichtsahnender Surfer als Mittelsmann für den Angriff missbraucht. Eine bösartige Website nutzt die Vertrauensstellung des PCs oder Browsers des Mittelsmanns gegenüber einer anderen Seite aus.

Ein ganz einfacher Fall ist ein in das Intranet einer Firma eingeloggter Anwender. Surft dieser in einem zweiten Browserfenster eine präparierte Seite irgendwo im Netz an, so kann ein darin enthaltener Schadcode mit den legitimen Rechten des Anwenders auf das Intranet zugreifen. Ist der Login auf das Intranet gar über ein Cookie automatisiert, muss der Anwender nicht einmal aktiv eingeloggt sein, um über diesen Weg einen Angriff zu starten.

2.4.2 CSRF-Logout-Button-Attacke

Zum besseren Verständnis dazu gleich ein einfaches Praxisbeispiel, das aber nur Abonnenten von TecChannel-Premium selbst live testen können: Geschütze Bereiche, die nur nach einem Login erreichbar sind, findet man überall im Web. Ob ein Forum, ein Intranet oder eine Web-Anwendung, stets ist ein Login nötig. Und wo ein Login ist, da sollte es auch einen Logout geben. Oftmals ist dieser Logout nur ein einfacher Link, der sich hinter einem Text oder einem Icon verbirgt. Wird dieser Link, wie auch im Premium-Bereich von TecChannel umgesetzt, aufgerufen, beendet der Web-Server die Session und loggt den User aus.



Logout-Link: Der Logout aus TecChannel-Premium erfolgt durch den Aufruf einer speziellen Seite.

Im Fall von TecChannel Premium genügt ein Aufruf der URL *http://www.tecchannel.de/index.cfm?pid=441&rand=57566* für die Abmeldung. Meldet man sich öfter

an und ab, erkannt man, dass sich der hintere Parameter „&rand=xxxx“ zwar stets ändert. Gibt man die URL zum Test manuell ein und lässt den hinteren Parameter ganz weg oder benutzt einen bereits benutzen Wert, so wird man aber dennoch ausgeloggt. Somit genügt ein stets gleicher Link für den Logout. Jetzt stellt sich die Frage, wie man dies für einen Angriff nutzen kann.

Angriff über das <img> Tag

Rein technisch gesehen gibt es so etwas wie den Aufruf eines Links für einen Web-Server gar nicht. Das Klicken mit der Maus auf einen Link behandelt ja der Browser. Der Browser erkennt, dass der User einen Link geklickt hat. Daraufhin fordert er vom Web-Server die Daten für die gewünschte URL an. Der Web-Server von TecChannel.de erhält also vom Browser bei einem Kick auf den Logout-Text einfach nur die Aufforderung, die Daten der Seite *http://www.tecchannel.de/index.cfm?pid=441&rand=57566* an den Browser zu senden. Diese Seite gibt es aber gar nicht. Der Seitenaufruf wird lediglich als Kommunikationsmittel genutzt. Erhält der Web-Server eine Anfrage dieser Seite, interpretiert er dies als Wunsch zum Logout und schickt die normale TecChannel-Homepage an den Browser.

Nun gibt es aber weitere Möglichkeiten, Daten vom Web-Server anzufordern. Besonders einfach geht dies über das Image-Tag, mit dem normalerweise Bilder in Seiten eingebunden werden. Findet der Browser im Quelltext einer Seite ein Element wie `<img src=http://www.tecchannel.de/img/tecchannel_logo.gif>`, so fordert er diese Daten vom Server an. Technisch gesehen nutzt der Browser beim Anfordern sowohl einer HTML-Seite als auch eines Bildes das HTTP-Kommando GET mit der gewünschten Adresse als Parameter.

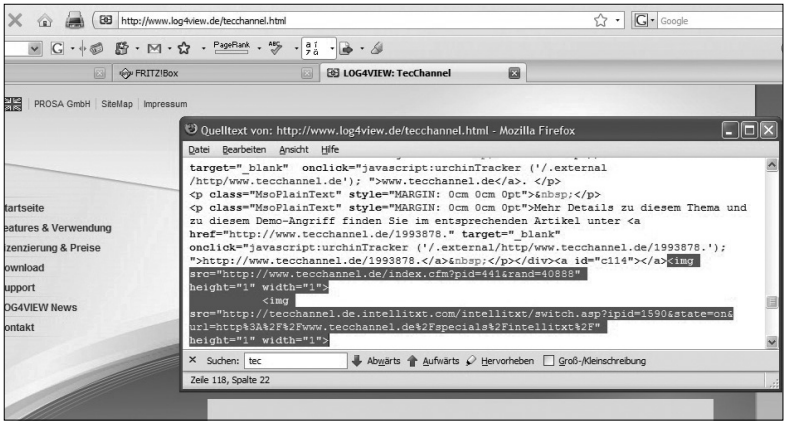
Für die harmlose XSRF-Attacke auf den Logout nutzt man jetzt aus, dass

- das Bild auch von einem anderen Server und Domain kommen kann
- das Bild keine passende Dateiendung wie .gif , .png oder .jpg haben muss
- bei fehlerhaft zurückgelieferten Daten der Browser an der Stelle des Bilds nichts anzeigt.

Datenverkehr im Detail

Somit genügt es, auf einer beliebigen Website, die gar nichts mit TecChannel zu tun hat, das Element `<img src=http://www.tecchannel.de/index.cfm?pid=441&rand=57566>` einzufügen. Surft ein eingeloggter Premium-Anwender die so präparierte Seite an, fordert der Browser von TecChannel die vermeintlichen Bilddaten an und loggt den User dadurch aus.

Zum Test haben wir unter www.log4view.de/tecchannel eine dementsprechend präparierte Seite eingerichtet, sodass Premium-User den Angriff live testen können. Beim Aufruf erfolgt dann auch gleich noch die nächste Stufe eines CSRF-Angriffs, die Manipulation von Cookies. Dies können alle Leser von TecChannel.de live ausprobieren.



Demo-Seite: Auf der harmlos aussehenden Seite, die mit der Domain TecChannel.de nichts zu tun hat, sind die beiden Angriffs-Images eingebettet.

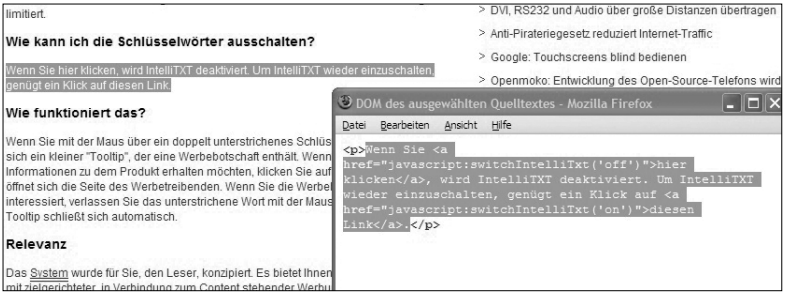
2.4.3 Cookie-Manipulation mit CSRF

Das nächste Beispiel eines CSRF-Angriffs ist schon etwas hinterhältiger. Ist beim Logout-Angriff die Auswirkung sofort zu sehen, manipulieren wir nun ein Cookie. Damit wird eine Eigenschaft dauerhaft verändert, und die Auswirkung zeigt sich eventuell erst viel später. Zunächst ein paar Worte zur „Versuchsumgebung". Wie hier auf TecChannel beschrieben (www.tecchannel.de/specials/intellitxt/), nutzen wir als spezielle Werbeform IntelliTXT. Dabei werden bestimmte Schlüsselwörter mit grünen Werbe-Links hinterlegt.

IntelliTXT: Der Anwender kann die IntelliTXT-Werbeform optional ein- und ausblenden.

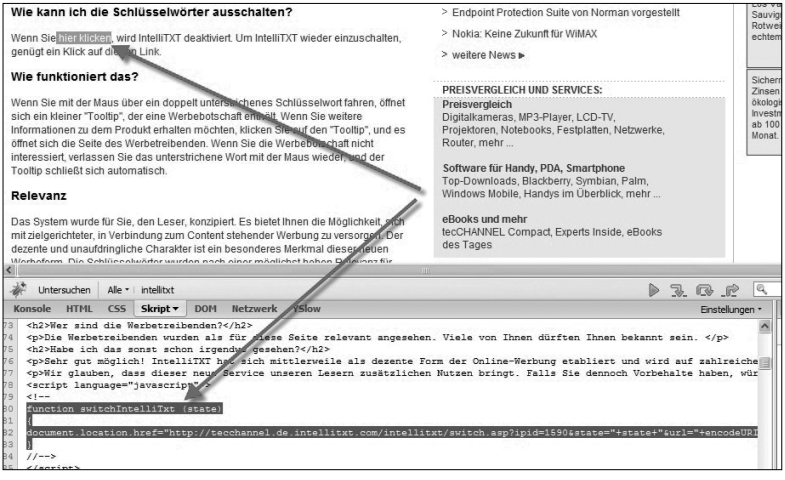
Diese Werbeform kann vom Leser ein- und ausgeschaltet werden. Sieht man sich den Sourcecode der Seite an, erfolgt die Auswahl über einen Link, der ein Ja-

vascript aufruft. Um dies zu analysieren, ist aber ein wenig Aufwand nötig, da es nicht in den HTML-Code eingebettet ist, sondern nachgeladen wird.



Javascript: Die Auswahl erfolgt normalerweise über ein Javascript-Element, das man erst noch in einer externen Library suchen muss.

Die Analyse des Sourcecodes erleichtern zwar Debugging-Tools wie Firebug. Aber es geht auch viel einfacher.

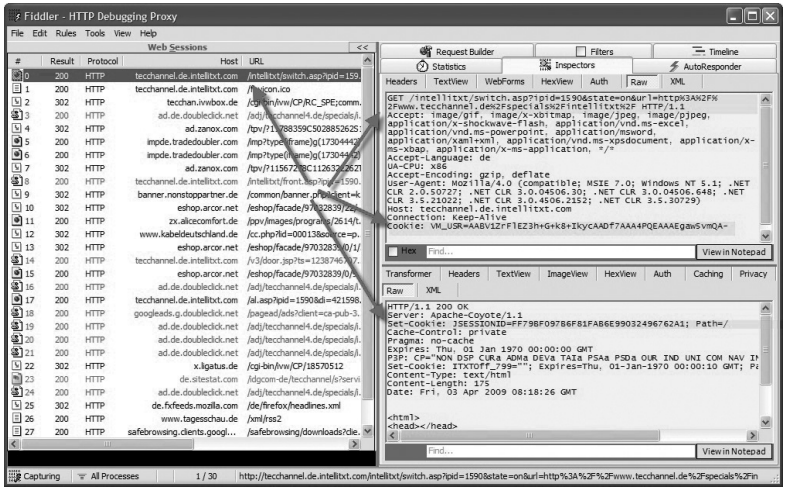


Add-on: Mit der Firefox-Erweiterung „Firebug" kann man das IntelliTXT-Script aufspüren.

Analyse mit dem Debugging Proxy

Zum Test der IntelliTXT-Funktionen klemmen wir uns zunächst in den Datenverkehr zwischen Browser und Server. Ideal für diesen Zweck ist die Freeware Fiddler, mit der man HTTP-Pakete mitschneiden, analysieren und sogar modifizie-

ren kann. Klickt man auf TecChannel.de den Link zum Einschalten von IntelliTXT, so sieht man im oberen Bereich von Fiddler (www.fiddler2.com/fiddler2/), dass im Prinzip nur wieder eine bestimmte URL auf intellitxt.com aufgerufen wird (GET). Wie im unteren Bereich des Screenshots zu sehen, liefert der Server von IntelliTXT daraufhin ein Cookie zurück, in dem der Browser die Erlaubnis zum Anzeigen der Werbung speichert.



Debugging Proxy: Fiddler zeigt das zum Aktivieren gesendete Paket und die Antwort des Servers an.

Fügt man nun wieder den mit Fiddler gefundenen Link als Image mit `<img src=„http://tecchannel.de.intellitxt.com/intellitxt/switch.asp?ipid=1590&state=on&url=http%3A%2F%2Fwww.tecchannel.de%2Fspecials%2Fintellitxt%2F“ height=“1“ width=“1“>` auf eine beliebige Website ein, wird bei deren Besuch IntelliTXT auf TecChannel.de aktiviert.

Das Frappierende daran ist das Management des Cookies, das wir wieder anhand unserer Demo-Seite aufzeigen:

- Das nichtsahnende Opfer greift auf die Seite www.log4view.de/tecchannel zu.
- Diese Seite ruft nun über ein manipuliertes Image eine Adresse auf intellitxt.com auf. Wie die URL tecchannel.de.intellitxt.com vermuten lässt, ist im vorderen Teil kodiert, für welche Domain die Werbung bei IntelliTXT freigeschaltet werden soll.
- Der Server von IntelliTXT interpretiert den Seitenaufruf nun als einen Klick auf den Link zum Einschalten der Werbung auf TecChannel.
- Wie im unteren Teil des Fiddler-Screenshots zu sehen, sendet er nun ein Cookie zurück, in dem er sich diese Erlaubnis merkt.

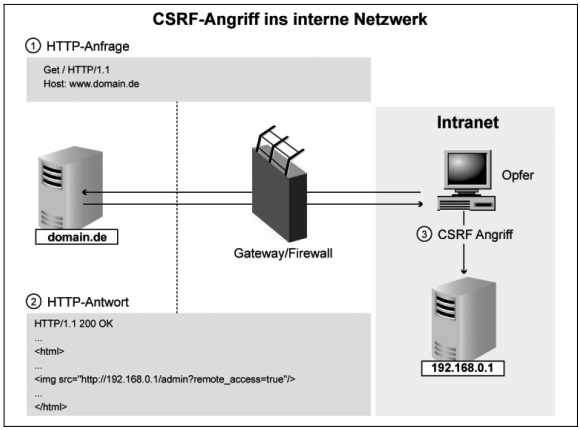
Das Opfer war während der ganzen Zeit nicht auf TecChannel.de. Doch wenn er das nächste Mal TecChannel.de besucht, wird er die IntelliTXT-Werbung in den Artikeln sehen.

> Noch ein Anmerkung zum Test: Diese Werbeform ist generell nur in Artikeln und nicht auf der Homepage oder den Übersichtsseiten aktiviert.

2.4.4 CSRF-Angriff auf das interne Netz

Die bislang demonstrierten Sicherheitslücken waren gegen Server gerichtet, die sich im frei zugänglichen Internet befinden. Das Hinterhältige an einem CSRF-Angriff ist jedoch, dass die Aktion immer vom Browser eines unwissenden Opfers ausgeht und somit dessen Rechte besitzt. Dadurch sind von außen gesteuert jederzeit Angriffe auf Rechner im Intranet möglich. Diese sind normalerweise weniger geschützt, da die Administratoren davon ausgehen, nur interne Mitarbeiter hätten darauf einen Zugriff und die normale Firewall würde externe Attacken abblocken.

Durch die Firewall: Da das Opfer hinter der Firewall sitzt, ist auch ein Angriff auf das interne Netz möglich.



Wie das Diagramm zeigt, ändert sich am prinzipiellen Vorgehen beim CSRF-Angriff auf das interne Netzwerk gar nichts. Der Firmenmitarbeiter an seinem Arbeitsplatz greift auf eine manipulierte externe Seite zu. Darin ist ein Image mit einer Adresse eines firmeninternen Servers eingebunden. Beim Laden des vermeintlichen Bildes löst der Browser dann Aktionen auf dem Server, der eigentlich durch die Firewall von außen gar nicht zugänglich ist.

Jetzt stellt sich natürlich die Frage, woher ein externer Angreifer Details wie lohnende Server, deren darauf laufende Web-Anwendung und zudem noch die IP-Adresse im internen Netz kennen sollte. Eine Möglichkeit ist die Rache eines entlassenen Mitarbeiters, der sein Insiderwissen preisgibt oder ausnutzt.

Ein weitaus einfacheres Ziel ist aber ein DSL-Router. Die Fritz!Box beispielsweise steht millionenfach in deutschen Haushalten und kleinen Büros, ist im internen Netz immer unter fritz.box erreichbar, und die darauf laufende Web-Anwendung ist für jeden einfach analysierbar.

Im Folgenden dienen die AVM-Router lediglich als Beispiel, da diese in Deutschland weit verbreitet sind. Selbstverständlich sind auch alle anderen DSL-Router, die per Web-Interface konfiguriert werden, potenzielle Opfer – sofern die Hersteller keinen wirksamen Schutz implementiert haben. In unseren Tests konnten wir beispielsweise den Cisco/Linksys WAG 160 N und einen ZyXEL P-660HW über den gleichen Weg angreifen.

2.4.5 Sicherheitsrisiko DSL-Router

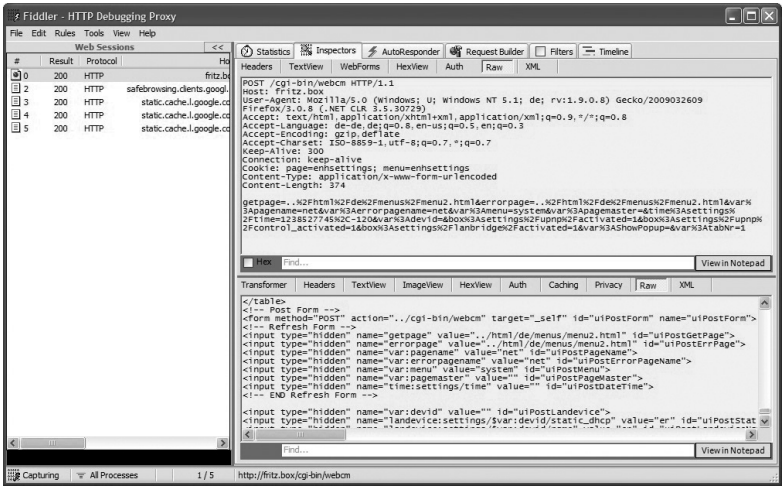
Die komplette Konfiguration der Fritz!Box erfolgt wie bei den meisten DSL-Routern über ein Web-Interface. Auf der Fritz!Box läuft ein einfacher Web-Server, der HTML-Seiten mit Formularfeldern ausliefert. Die im Bild dargestellte WLAN-Konfiguration ist ein HTML-Formular, das ein paar Checkboxen, ein paar Dropdown-Felder und einige Textfelder enthält.

Web-Formular: Im Prinzip besteht die Konfiguration nur aus einem einfachen Formular.

Der User kann in diesem Formular die Werte verändern. Klickt er auf „Übernehmen“, sendet der Browser die Daten zur Fritz!Box, die dann die Werte übernimmt. Dabei erfolgt keine weitere Sicherheitsabfrage. Gelingt es, über einen CSRF das Senden der Formulardaten zu simulieren, kann ein kleines Code-Fragment in einer externen Website die Fritz!Box beliebig umkonfigurieren.

2.4.6 AVM bestätigt Angriff

TecChannel ist der CSRF-Angriff auf die komplette Konfiguration der Fritz!Box relativ schnell gelungen. Da die Fritz!Box im deutschen Markt die größte Verbreitung hat, wurde AVM über das Sicherheitsrisiko sofort informiert und hat dieses inzwischen auch bestätigt. Um Missbrauch zu vermeiden, haben wir uns jedoch entschlossen, weder den genauen Angriffsweg noch den Code zu publizieren. Deshalb werden wir auch keine entsprechende Testsite live zur Verfügung stellen.



Kommunikation über POST: Ein simpler POST an den Web-Server der Fritz!Box des Herstellers AVM genügt zum Verändern von Daten.

Aufmerksam wurde TecChannel auf diesen Angriffsvektor durch eine kleine Randbemerkung auf den TrendTagen der Sicherheitsexperten von cirosec (www.cirosec.de). Dieser IT-Dienstleister hat sich schon vor Jahren auf die Verwundbarkeitsanalyse und den Schutz von Web-Anwendungen spezialisiert. Mehrmals im Jahr hält cirosec kostenlose Veranstaltungen zu aktuellen Sicherheitsthemen ab.

2.4.7 Das Passwort allein schützt nicht

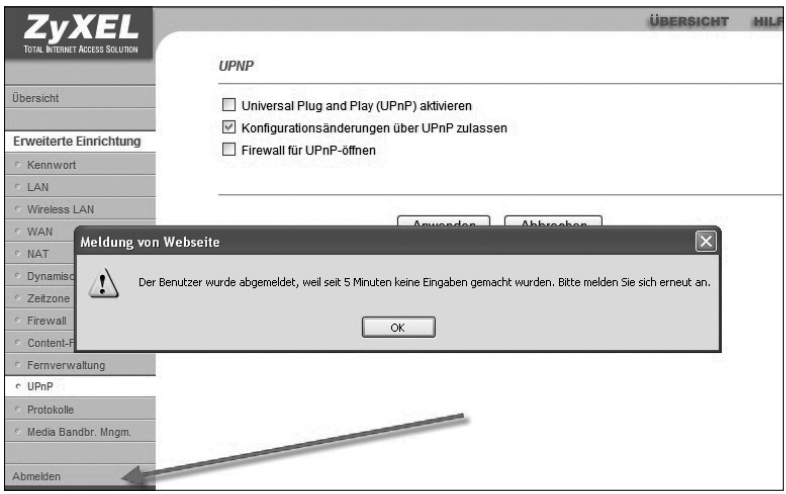
Beim Angriff gibt es eine einzige Hürde: Das Web-Interface der DSL-Router ist meist über ein Passwort geschützt, an dem auch ein simulierter „POST“ nicht ohne Weiteres vorbeikommt. Da sich AVM des Sicherheitsrisikos seit geraumer Zeit bewusst ist, wird man bei der ersten Konfiguration der Fritz!Box über den Web-Browser seit einigen Firmware-Revisionen eindringlich zur Vergabe eines Passwortschutzes gedrängt. Bei einigen anderen Router-Herstellern ist der Pass-

wortschutz sogar zwingend erforderlich und kann gar nicht deaktiviert werden. Aber um es gleich vorwegzunehmen: Der Schutz der Web-Oberfläche durch das Passwort ist mitunter wirkungslos und der CSRF-Angriff gelingt dennoch.

Außerdem zeigt die Erfahrung, dass viele Anwender immer noch auf ein Passwort verzichten oder die Werkseinstellungen nicht verändern. Aus dem internen Netz vermuten sie keine Angriffe, hinter der Firewall fühlen sie sich mit ihren privaten IP-Adressen sicher. Auch das Argument einer Gefährdung durch ein WLAN gilt seit der sicheren Verschlüsselung mit WPA nicht mehr, sodass man aus Bequemlichkeit den Kennwortschutz nicht nutzt.

Aber selbst wenn ein Kennwort gesetzt ist: Wer beim Browsen mehrere Fenster geöffnet hat und in einem davon auf dem DSL-Router eingeloggt ist, ist von allen anderen Fenstern aus komplett ungeschützt. Bei Zugriffen auf einen Server nutzt der Browser trotz mehrerer Tabs nämlich immer nur eine Session. Alle Zugriffe auf den DSL-Router erfolgen in diesem Fall mit den Rechten des legal eingeloggten Browser-Tabs. Dabei ist es auch kein Schutz, wenn Browser wie Chrome oder der IE8 für jedes Tab einen eigenen Prozess starten. Daher werden CSRF-Angriffe oft auch als Session Riding bezeichnet.

Aber es kommt noch schlimmer: Das Web-Interface der Fritz!Box beispielsweise kennt keinen Logout. Wie uns AVM auf Nachfrage bestätigt hat, hält die Fritz!Box nach einem Zugriff die Session noch fünf Minuten lang geöffnet. Auch Linksys und ZyXEL verwenden wie die meisten DSL-Router ein derartiges Zeitfenster. Erst wenn mehrere Minuten lang keine User-Aktion mehr stattfand, loggen die DSL-Router den Besucher automatisch aus.



Lobenswert: ZyXEL bietet neben dem automatischen Logout nach fünf Minuten Inaktivität auch einen Menüpunkt zum sofortigen Abmelden vom Web-Interface an.

Auch wenn man den Browser-Tab mit der Fritz!Box-Konfiguration also längst geschlossen hat, kann man innerhalb dieses Zeitfensters mit einem CSRF-Angriff ohne weitere Passwortabfrage die Konfiguration der Fritz!Box beliebig modifizieren. Schafft es ein Angreifer, den Schadcode in einem Fritz!Box-affinen Umfeld wie einem DSL-Forum oder einem Workshop zur Fritz!Box zu platzieren, hat er gute Chancen auf einen Erfolg.

2.4.8 Potenzielle und reale Gefahren für DSL-Router

Was könnte ein Angreifer nun eigentlich machen, wenn er die Konfiguration eines DSL-Routers manipuliert? Eine Möglichkeit, die laut AVM bereits aktiv genutzt wurde, ist das Umändern der Wahlregeln. Damit leitet der Angreifer alle Anrufe über seine teure 0900er-Vorwahl um und bereichert sich so. Zumindest bei der Fritz!Box soll dieser Angriff laut AVM inzwischen nicht mehr möglich sein.

Durch das Freischalten von Ports kann der Angreifer auch Löcher durch die Firewall des DSL-Routers bohren und eine Weiterleitung auf bestimmte Rechner einrichten. So hat er dann Zugriff auf die PCs im Netzwerk und kann diese in einem zweiten Schritt attackieren. Mit ein bisschen Aufwand kann man bei der Fritz!Box das Web-Interface zum Zugriff per https aus dem Internet freischalten. Dann reicht ein einmaliger einfacher Angriff zum Freischalten, den Rest erledigt man dann „ganz offiziell" direkt über das Internet. Hierzu muss man jedoch neue Passwörter vergeben, sodass dies dem rechtmäßigen Anwender auffällt, wenn er wieder auf seine Fritz!Box zugreifen will.

Digitale Signatur: Die Fritz!Box erkennt eine modifizierter Firmware.

Interessant ist auch das Umleiten des Traffics zur Analyse der Daten. Der Angreifer kann einen VPN-Tunnel von der Fritz!Box zu sich aufbauen. Dann routet er den ganzen Datenverkehr oder auch nur Anfragen auf bestimmte IP-Adressen zu

sich und kann als Man-in-the-Middle alles manipulieren. Kreditkartenzahlungen sind hierdurch besonders gefährdet. Fängt der Angreifer Zugriffe zum Router-Hersteller selbst ab, droht der Mega-GAU: Er kann ein neues Firmware-Update vortäuschen und dann dem Opfer eine modifizierte Software unterschieben. Dann könnte er aus den infizierten DSL-Routern ein gefährliches Bot-Netz aufbauen: rund um die Uhr online und keinerlei Virenscanner oder andere Sicherheits-Tools, die auf den Bots laufen. Zudem hat der Besitzer des DSL-Routers keine Chance zu erkennen, was er am Ausgang in das öffentliche Netz alles verschickt.

AVM hat die Gefahr einer modifizierten Firmware aber nach eigenen Angaben schon seit Langem gebannt. Die Downloads besitzen eine digitale Signatur, sodass eine Fremd-Firmware bei der Installation auffällt. Allerdings haben nicht alle Router-Hersteller ein derartiges Sicherheits-Feature implementiert.

2.4.9 Schutzmaßnahmen

AVM ist sich der Gefahr durch CSRF-Angriffe seit Längerem bewusst. Doch bislang kann man keinen wirklich sicheren Schutz davor anbieten. Denn egal ob man beispielsweise Session-IDs oder Tokens in die Konfigurationsformulare mit einbettet: Nach Meinung von AVM könnte man diese Daten per Skript auswerten und passend wieder zurückschicken.

Die einzig sichere Lösung derzeit besteht daher aus drei Maßnahmen, die nur in ihrer Kombination helfen. TecChannel rät

- Ein Passwort für das Web-Interface der Fritz!Box vergeben
- Während des Zugriffs auf das Web-Interface der Fritz!Box keine weiteren Browser-Tabs geöffnet haben
- Nach dem Schließen des Web-Interfaces mindestens fünf Minuten lang keine andere Website besuchen und am besten den Browser beenden. Falls das Web-Interface des DSL-Routers einen manuellen Logout zulässt, sollte man diesen auch stets nutzen.

AVM will die Gefährdung jetzt mit hoher Priorität aus der Welt schaffen. Dabei will man sich nicht nur auf eine Risikominimierung etwa mittels eines Logout-Buttons beschränken. Im Extremfall könnte man beispielsweise den kompletten Internetverkehr eines PCs blockieren, wenn dieser auf den Konfigurationsseiten eingeloggt ist. Bis zur technischen Lösung setzt man auch auf die Abschreckung durch das Gesetz, da es eine strafbare Handlung sei, in fremde Computersysteme einzudringen, vor allem wenn es dazu einer gewissen kriminellen Energie bedarf.

Sicherheitsspezialisten für Web-Anwendungen wie Stefan Strobel von der cirosec GmbH sind der Meinung, dass es auch etablierte und einfach umzusetzende technische Möglichkeiten gibt, um das Problem zu lösen. Hier setzt man darauf, dass Anfragen, die etwa die Konfiguration ändern, nicht statisch und somit nicht vorhersagbar sein dürfen. Zufällige Tokens würden diesen Zweck erfüllen, sofern die Anwendung nicht auch noch eine Cross-Site-Scripting-Schwachstelle hat.

2.4.10 Fazit

CSRF oder auch Session Riding steigt nicht ohne Grund in der Rangliste der Web-Gefährdungen immer weiter nach oben. Zahlreiche Web-Anwendungen sind dadurch angreifbar. Neuentwicklungen müssen unbedingt auf entsprechende Schwachstellen hin untersucht werden. Für bestehende Systeme in großen IT-Umgebungen bieten sich Web Application Firewalls (WAFs) an, um nachträglich einen Schutzschild zu installieren. Mehr dazu demnächst in einem Artikel zu diesem Thema. Entwickler von einfachen Web-Interfaces zur Konfiguration von Peripheriegeräten stehen vor einem Problem und sollten ihre Software auf derartige Schwachstellen hin überprüfen.

Keinesfalls soll hier der Eindruck entstehen, das Problem existiere nur bei AVM, Cisco/Linksys und ZyXEL. Wer bei anderen Routern, Netzwerkdruckern und kleinen NAS-Systemen nach Schwachstellen im Web-Interface sucht, wird fündig. Allerdings ist bei AVM das Problem wegen der millionenfachen Verbreitung der Fritz!Box-DSL-Router besonders gravierend. Dem Anwender kann man nur raten, Schutzmaßnahmen wie Passwörter überall zu nutzen. Das Arbeiten mit mehreren Tabs sollte man beim Zugriff auf geschützte Seiten vermeiden. Und wie die Falle mit dem offenen Zeitfenster zeigt, nutzt man, falls vorhanden, immer den Logout-Button, um eine Session zu beenden. Existiert kein geregelter Logout, wartet man nach dem Schließen der Web-Anwendung eine angemessene Zeit. Unkritisch ist es in diesem Fall, mit einem anderen Browser weiterzuarbeiten. Mit IE, Firefox, Chrome und Safari hat man ja inzwischen genügend Auswahl.

Albert Lauchner

Albert Lauchner ist seit November 1999 stellv. Chefredakteur bei TecChannel. Er ist für redaktionelle Qualität, den Auftritt von TecChannel und das Redaktionssystem verantwortlich. Zuvor arbeitete der Diplom-Physiker neun Jahre beim Computermagazin Chip als Leiter des Testlabors und der Hardware.

TecChannel-Links zum Thema	Webcode	Compact
Millionen DSL-Router hochgradig gefährdet	1993878	S.67
Grundschutz für Web-Applikationen	1785530	S.10
Schutz von Webshops und E-Commerce-Lösungen	1817630	S.37
Sicherheitsrisiko Web-Anwendung	1785212	–

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

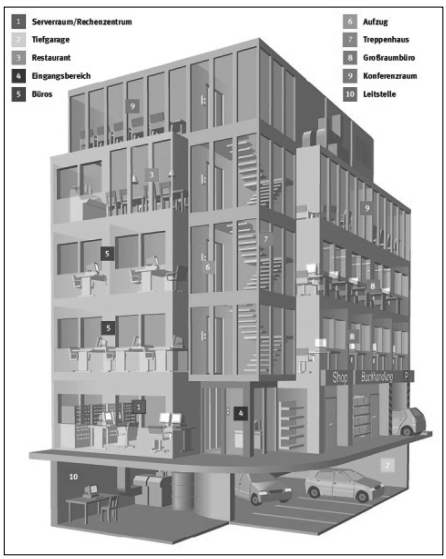
3 Schutz für Server

Serverräume mit Datenbank-, File-, Mail- und Anwendungs-Servern bilden das Herzstück jeder IT-Infrastruktur. Um die Ausfallsicherheit zu maximieren gilt es, potentielle Gefahren zu reduzieren. Ansätze sind der Zugangsschutz zu Serverräumen, Fernwartung und der Einsatz geeigneter Systemkomponenten.

3.1 Serverräume wirkungsvoll vor unbefugtem Zutritt schützen

Die Angst vor Datenverslust durch externen und internen Diebstahl ist groß. Deshalb sichern Unternehmen sensible Bereiche wie etwa Serverräume speziell ab. Wie eine wirkungsvolle Zugangskontrolle aussehen kann, beschreibt unser Praxisartikel anhand von Beispielen.

Die IT bildet das Herzstück eines jeden Unternehmens. Diese muss der Betreiber besonders gut schützen, um Angriffe sowohl von außen als auch von innen zu verhindern. Denn nicht alle Personen oder Gäste, die in einem Unternehmen arbeiten oder es besuchen, sind diesem wohlgesinnt. Hinzu kommt, dass die Firmen im Rahmen von Compliance-Vorgaben verpflichtet sind, IT-Security-Management-Systeme auf Basis von ITIL (Webcode **1751293**) oder Basel II zu implementieren.



All-in-One: Ein optimaler Zutrittsschutz beinhaltet alle wichtigen Räume und Gebäudeteile eines Unternehmens. (Quelle: Novar)

Deshalb sollten unternehmenskritische Bereiche wie etwa Serverräume mit einer wirksamen Zutrittskontrolle abgesichert werden. Diese besteht heute üblicherweise aus einer konventionellen mechanischen oder digitalen Schließanlage. Aber mehr und mehr kommen in diesen Bereichen Sicherheitsverfahren wie Biometrie (Webcode **402320**) oder RFID (Webcode **431196**) zum Einsatz. Eine zusätzliche Absicherung der beiden Zutrittsverfahren durch Kombination eines Ausweismediums oder PIN-Code-Eingabe ist in der Praxis üblich. Im Hochsicherheitsbereich können auch Zutrittsschleusen zum Einsatz kommen.

In unserem Beitrag erläutern wir praxisnahe Beispiele, wie eine wirksame Zutrittskontrolle aussehen kann. Will ein Unternehmen einen zuverlässigen Zugangsschutz, so kommt nur eine Kombination aus mehreren Sicherheitstechnologien in Frage. Diese arbeiten in Verbindung mit einem ausgeklügelten zentralen IT-basierten Sicherheitssystem zusammen.

3.1.1 Authentifizierung, Identifizierung und Verifizierung

Um eine sichere biometrische Zutrittskontrolle zu gewährleisten, müssen Personen, die ein Unternehmen beziehungsweise Gebäude betreten wollen, von einem System eindeutig erkannt werden. Häufig fallen Begriffe wie Authentifizierung, Identifizierung und Verifizierung.

- Bei der **Identifizierung** werden die biometrischen Erkennungsmerkmale mit mehreren oder allen im biometrischen System gespeicherten biometrischen Referenzen verglichen.
- Dagegen bedeutet eine **Verifizierung**, dass die biometrischen Erkennungsmerkmale mit einer im biometrischen System gespeicherten biometrischen Referenz verglichen werden.
- Unter **Authentifizierung** versteht man ein Verfahren zur Feststellung der Identität einer Person, um zum Beispiel den Zugang zu technischen Systemen oder Gebäuden zu ermöglichen beziehungsweise zu kontrollieren.

3.1.2 Traditionelle Absicherung und Überwachung von Serverräumen

Der Markt bietet eine Fülle von Produkten für die Absicherungen von Serverräumen und Datenzentren. Die klassische Form der Zugangskontrolle erfolgt mit einem Schlüssel inklusive Schließanlage. Moderne Schließanlagen besitzen elektronisch kodierte Schlüssel und Schließzylinder, die über eine zentrale computergestützte Leitstelle verwaltet werden. Allerdings bieten diese Möglichkeiten keinen sicheren Schutz gegen den Zutritt von unbefugten Personen, die sich durch Diebstahl den Schlüssel angeeignet haben, da keine Authentifizierung der Personen erfolgt. Das Gleiche gilt für elektronische Schlüssel, wie etwa RFID-basierte Firmen-

ausweise oder Zugangskarten mit Magnetstreifen. Eine weitere, oft genutzte Zutrittskontrolle ist die PIN-Code-Eingabe per Tastenfeld. Aber auch diese Methode bietet keinen hinreichenden Zutrittsschutz, da keine Authentifizierung der Personen stattfindet und das Verfahren anfällig für das Ausspähen der PIN-Nummer ist. So können beispielsweise Personen mit einer versteckten Videokamera den Zutrittsberechtigten bei der PIN-Eingabe beobachten und somit in den Besitz der Ziffernkombination geraten.

Um Personen gezielt in einem Gebäude oder Raum zu überwachen, werden digitale Videokameras verwendet. Diese Systeme arbeiten autark ohne Personaleinsatz und zeichnen sämtliche Aktivitäten auf. Solche Videoeinrichtungen werden üblicherweise zusammen mit Bewegungsmeldern, Öffnungssensoren für Rack- und Raumtüren, Glasbruchsensoren oder Vibrationssensoren betrieben.

3.1.3 Raumüberwachung per Videokameras

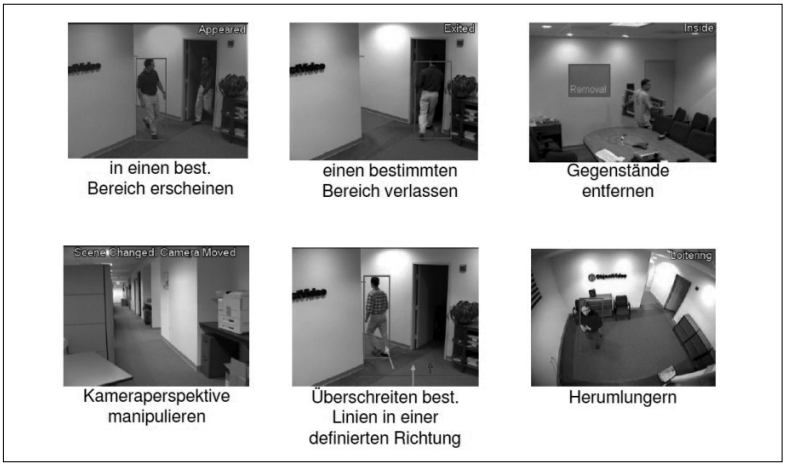
Die traditionelle Videoüberwachung mittels eines Videobeobachters ist heute noch ein probates Mittel, Serverräume zu überwachen. Dabei werden per Videokameras alle sicherheitsrelevanten Räume beziehungsweise Bereiche ständig auf einer Multivisionswand kontrolliert. Allerdings ist diese Methode sehr personalintensiv und damit teuer. Darüber hinaus haben Untersuchungen von IMS Research ergeben, dass nach zirka 22 Minuten die Konzentration eines Bildschirmbeobachters so stark sinkt, dass er bis zu 95 Prozent der Aktivitäten auf den Bildschirmen nicht mehr wahrnimmt. Damit ist diese Art der Zutrittskontrolle auf unübersichtlichen Monitorwänden obsolet.

3.1.4 Intelligente Videoüberwachung

Diese Überwachungsmethode basiert auf einer modularen Architektur, die aus dem digitalen Audio- / Bildaufzeichnungssystem sowie hochwertigen Kameras, Mikrofonen, Lautsprechern und Zutrittskontrollsystemen besteht. Die einzelnen Komponenten werden speziell nach Ihren Anforderungen (Einsatzort, Wetterbedingungen) ausgewählt, damit sie immer einsatzbereit sind.

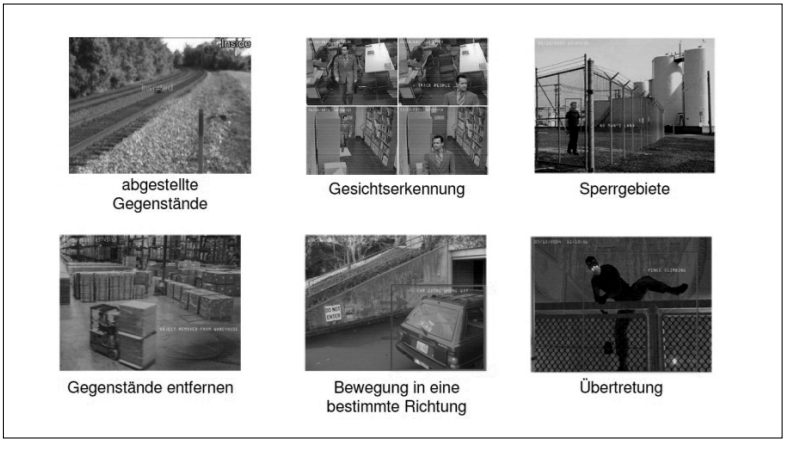
Alle Aufzeichnungssysteme sind an eine zentrale Überwachungsstation (bei mehreren Standorten oder Gebäudeteilen) angeschlossen, welche die Bilder von den verschiedenen Standorten überwacht und für die Informationsverarbeitung an das Netzwerk weiterleitet.

Die moderne Videoüberwachung ist dank ausgefeilter Software in der Lage, verschiedene Gefahrensituationen zu erkennen und entsprechend einen Alarm auszulösen. In Innenräumen können so zum Beispiel Sicherheitsbereiche definiert werden, zu denen Personen keinen Zutritt haben oder in denen keine Gegenstände abgestellt werden dürfen. Moderne Videokameras erkennen mittlerweile selbstständig, wenn Unbefugte diese manipuliert beziehungsweise verstellt haben.



Raumüberwachung: Moderne Videosysteme können vordefinierte Gefahrensituationen erkennen und einen entsprechenden Alarm auslösen. (Quelle: Unisys)

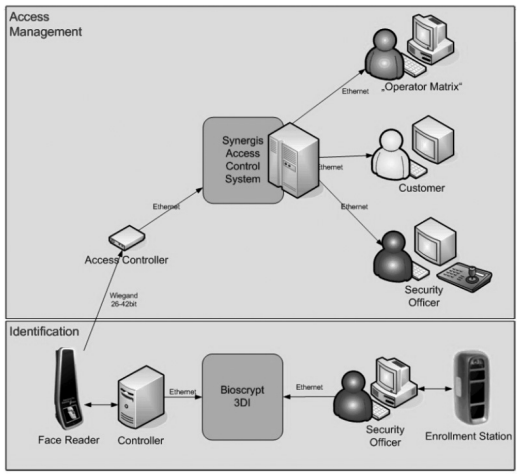
Die Kontrolle der Videosysteme kann dezentral von jedem berechtigten Bedienplatz in einem Netzwerk erfolgen und erfordert somit keinen festen Überwachungsplatz. Jede Kamera kann einzeln oder gleichzeitig mit anderen Kameras Bereiche überwachen. Darüber hinaus werden die aufgezeichneten Bilder beziehungsweise Videos automatisch auf einem zeitlimitierten Backup-System zur eventuellen Überprüfung zwischengespeichert.



Alles im Blick: Das elektronische Auge der Überwachungsanlage registriert sämtliche ungewöhnlichen Bewegungen und schlägt Alarm. (Quelle. Unisys)

3.1.5 Praxisnaher Einsatz biometrischer Zutrittssysteme

Biometrische Zutrittssysteme bringen sowohl für mittelständische Unternehmen als auch für große Firmen und sogar für Privathaushalte eine Vielzahl von Vorteilen mit sich. Ein solches System besteht im Allgemeinen aus Lesegeräten, einer zentralen IT sowie einer speziellen Software für die Verwaltung der Datensätze und der dazugehörigen Zutrittsberechtigungen. Das können Systeme sein, mit denen innerhalb eines Unternehmens unterschiedliche Zutrittsbereiche verwaltet werden können. Die Daten werden zentral erfasst und organisiert, um entsprechende Sicherheitsbereiche abzugrenzen. Darüber hinaus ist ein solches Kontrollsystem standortübergreifend einsetzbar.



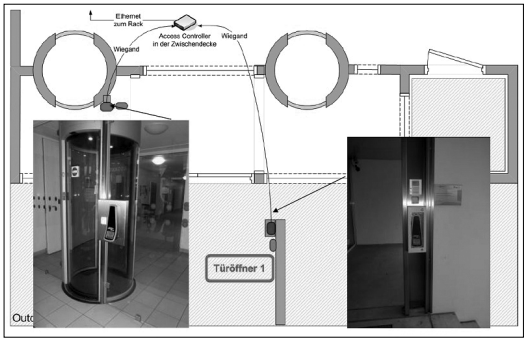
Zutrittssystem: Ein biometrisches Zugangskontrollsystem besteht aus mehreren unterschiedlichen Komponenten. (Quelle: Unisys)

Die Funktionsweise der biometrischen Zugangskontrolle wird am besten an einem Beispiel deutlich: Ein neu eingestellter Mitarbeiter bekommt weder einen Schlüssel noch eine Zutrittskarte oder einen Code. Stattdessen wird an seinem ersten Arbeitstag sein Gesicht über einen biometrischen 3D-Gesichtsscanner (Enrollment Station) eingelesen. Dabei werden die biometrischen Daten des Gesichts nicht als Foto, sondern als binärer Code im System gespeichert. Ab diesem Zeitpunkt ist sein Gesicht der Eintrittsschlüssel. Gleichzeitig werden durch einen Administrator die entsprechenden Zutrittsbereiche innerhalb des Unternehmens festgelegt.

Das bedeutet: Ab diesem Zeitpunkt hat neben den entsprechenden IT-Verantwortlichen auch der neue Mitarbeiter Zutritt zum Serverraum, da dieser über einen Gesichts-Scan die Authorisierung für das Betreten des Serverraumes erhalten hat. Für jede Berechtigung kann zudem eine bestimmte Uhrzeit definiert werden. So könnte zum Beispiel die Reinigungskraft das Büro nur zwischen 17 und 20 Uhr betreten dürfen.

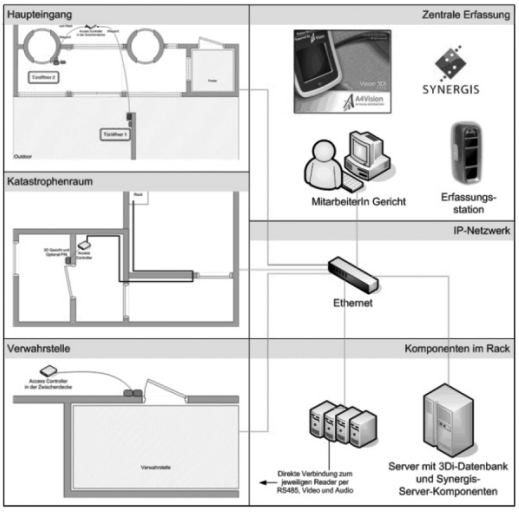
3.1.6 Personenvereinzelung und 3D-Gesichts-Scan

Personenvereinzelungsanlagen mit einem integrierten 3D-Gesichts-Scan verhindern, dass sich Unbefugte Zutritt zum Serverraum oder Rechenzentrum verschaffen. In einem nächsten Schritt gilt es zu überlegen, wie man den Zutritt zum Gebäude entsprechend wirkungsvoll absichert.



Bitte eintreten: Personenvereinzeler und ein 3D-Gesichts-Scan verhindern den Zutritt von unerwünschten Besuchern. (Quelle: Unisys)

So empfiehlt es sich zusätzlich, einen Empfangsbereich einzurichten, der ebenfalls durch Vereinzelungsschleusen von den technischen Bereichen abgetrennt ist. Darüber hinaus sollten Namen und Anwesenheitszeiten von Besuchern vom Sicherheitspersonal erfasst werden.

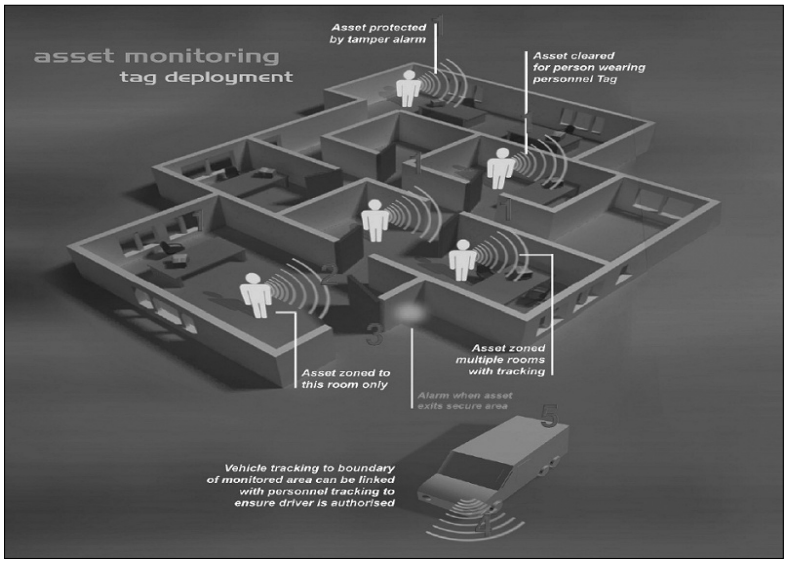


Kein Zutritt: Nur berechtigte Personen erhalten den Zutritt in die entsprechenden Räume. (Quelle: Unisys)

Zudem ist der Zutritt zu den Technikräumen, den Verwahrstellen und den einzelnen Serverschränken über geeignete Zutrittssysteme nochmals separat abzusichern. Dies ist aus Sicherheitsaspekten besonders dann wichtig, wenn ein Unternehmen Dienstleistungen über eine externe Firma in Anspruch nimmt.

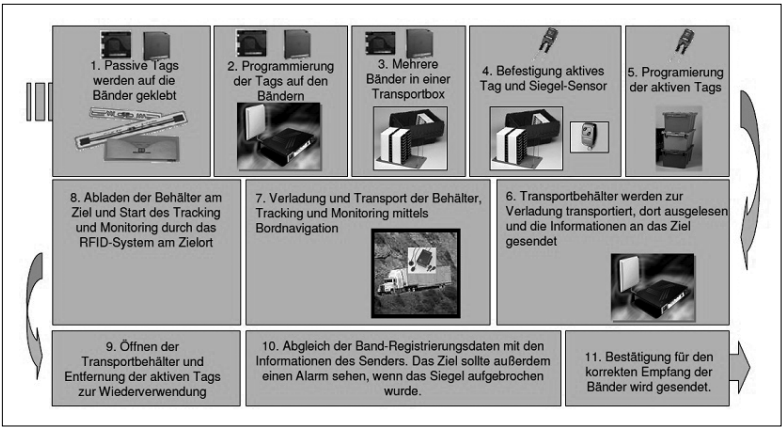
3.1.7 Zutrittskontrolle und Überwachung mit RFID-Technologie

In den vergangenen Jahren setzten Unternehmen verstärkt RFID-Technologie ein. Diese werden hauptsächlich in geschlossenen Kreisläufen wie Überwachung von Personen in Gebäuden oder im Materialfluss verwendet.



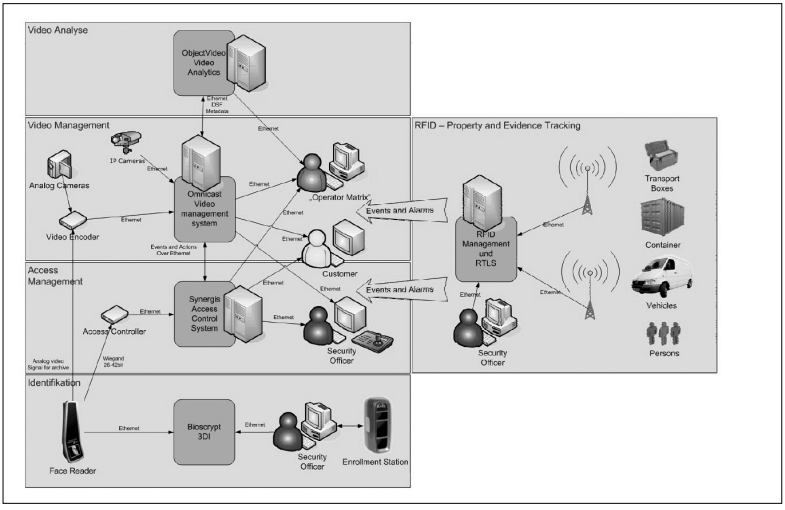
RFID-Spion: Mithilfe der RFID-Technologie lassen sich Bewegungen von Personen, Geräten und Fahrzeugen kontrollieren. (Quelle: Unisys)

Besonders hilfreich und effektiv erweist sich die RFID-Technologie für die Lokalisierung und Inventarisierung von Backup-Bändern, Beweisstücken, PCs, Laptops, Dokumenten und sonstigen Werten im Gebäude. Mithilfe von RFID-Lesegeräten an den Ein- und Ausgängen im Gebäude kann ein Unternehmen jederzeit feststellen, wo sich bestimmte Gegenstände oder Personen befinden. Dabei ist die Verfolgbarkeit eines zum Beispiel mit einem Transponder ausgestatteten Behälters durch vollständiges Tracking und Aufzeichnung aller Bewegungen des RFID-Tags dokumentiert und jederzeit abrufbar.



Tracking: Ein Backup-Band, versehen mit einem RFID-Tag, kann jederzeit lokalisiert und identifiziert werden. (Quelle: Unisys)

Wertvolle Gegenständen können sogar mittels kombinierter RFID- und GPS-Technologie zwischen Gebäuden oder Unternehmen versendet werden. Die Integrität dieser Pakete kann der Anwender zusätzlich durch manipulationssichere Siegel mit der sogenannten Cellular-Alert-Technologie sicherstellen.



Maximale Sicherheit: Die Kombination aus RFID-Technologie und biometrischer Zutrittskontrolle ergibt einen maximalen Schutz vor unbefugten Besuchern. (Quelle: Unisys)

Für größtmögliche Sicherheit sollte der Verantwortliche idealerweise die biometrische Zugangskontrolle mit der RFID-Technologie in einem geschlossenen System kombinieren.

3.1.8 Fazit

Im Rahmen des Datenschutzes muss sichergestellt werden, dass personenbezogene Daten sicher vor Missbrauch aufbewahrt werden. Einen wichtigen Beitrag hierzu leistet die Zutrittskontrolle. Sie stellt sicher, dass Einrichtungen wie Datenzentren oder Serverräume entsprechend ihrer Bedeutung geschützt sind.

Das Gros der Unternehmen schützt besonders den zentralen Serverraum, da dort hochkritische Daten verarbeitet werden. Er ist nicht nur vor Feuer und Vandalismus zu schützen, sondern auch vor missbräuchlichem Eindringen zu sichern. Die Zutrittskontrolle bezieht sich aber nicht nur auf die IT-Anlage. Sie betrifft auch andere Räumlichkeiten, in denen personenbezogene oder gar sensible Forschungsdaten aufbewahrt werden, wie etwa Archivräume.

In Unternehmen mit elektronischen und kodierten Schließsystemen ist unter Zuhilfenahme biometrischer Authentifizierung mittels 3D-Gesichts-Scans die Zutrittskontrolle – wie unsere Praxisbeispiele zeigen – die beste Lösung. Außerdem gewährleistet sie eine hohe Benutzerakzeptanz, da sie berührungslos arbeitet. Auch beinhaltet diese Form des kombinierten Zugangsschutzes einen sehr hohen Sicherheitsstandard. Zu berücksichtigen sind aber die hohen Kosten der Sicherheitsanlage, doch müssen diese relativiert werden, wenn die Anlage in das Sicherheitskonzept des gesamten Gebäudes einfließt.

Bernhard Haluschak

Bernhard Haluschak ist als Hardware-Redakteur bei TecChannel tätig. Der Dipl. Ing. (FH) der Elektrotechnik / Informationsverarbeitung blickt auf langjährige Erfahrungen im Server-Umfeld und im Bereich neuer Technologien zurück. Vor seiner Fachredakteurslaufbahn arbeitete er in Entwicklungslabors, in der Qualitätssicherung sowie als Laboringenieur in namhaften Unternehmen.

TecChannel-Links zum Thema	Webcode	Compact
Serverräume wirkungsvoll vor unbefugtem Zutritt schützen	1780627	S.80
Sicherheit in Server-Räumen	468234	–
IT-Sicherheit: Das sind die Herausforderungen 2009	1780729	–
IT-Security 2008: Viren, Spam, Herausforderungen, Innovationen	1779521	–

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

3.2 Server-Fernwartung effizient einsetzen

Ständige Verfügbarkeit und das Überwachen der unternehmenseigenen IT-Infrastruktur gehören zu den zentralen Aufgaben einer IT-Abteilung. Der steigende Kostendruck zwingt IT-Abteilungen, ihr Infrastruktur-Management ständig zu optimieren. Ein effizientes Remote-Management eine Lösung.

Moderne Server-Räume und Rechenzentren von heute sind hochkomplexe IT-Steuerungs- und Verwaltungsumgebungen. Dabei müssen die IT-Mitarbeiter mit jeglichen Gerätetypen wie beispielsweise Servern, Routern oder Switches vertraut sein. Außerdem sind die IT-Verantwortlichen für die Wartung an mehreren Standorten mit beschränkten Ressourcen zuständig. Die Kosten sind dabei so niedrig wie möglich zu halten.

Bei einem Ausfall der IT-Infrastruktur können die finanziellen Konsequenzen für Unternehmen verheerend sein. Neben den entgangenen Geschäften führt ein solches Desaster oft auch zu einem Vertrauensverlust der Benutzer, Arbeitskosten für problematische Reparaturen sowie Bußgeldern, die in Dienstverträgen (Service Level Agreements) mit internen oder externen Kunden vereinbart wurden. Je nach Branche können sich die Kosten für einen Ausfall der IT-Infrastruktur auf Hunderte bis Millionen von Euros pro Stunde belaufen. Verschiedene Remote-Management-Technologien (Webcode **441753**) können den IT-Verantwortlichen vor solchen Katastrophen schützen.

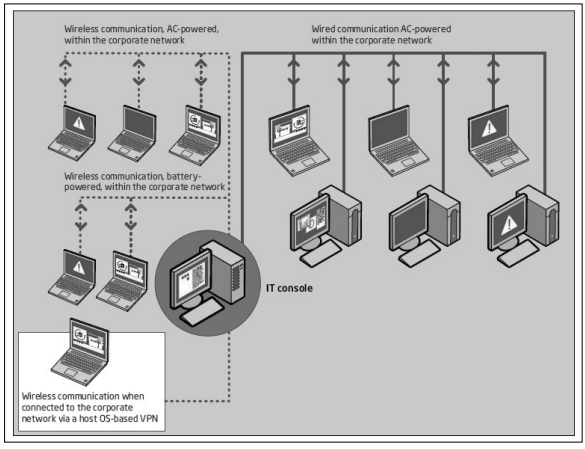
Die Anforderungen an ein ideales Server-Fernwartungs-Konzept bestehen dabei aus einigen zentralen Eigenschaften. In erster Linie sollte die Lösung dem Anwender erlauben, seine Server aus der Ferne zu bedienen, sowie die volle Integration von Tastatur, Bildschirm und Maus ermöglichen, wodurch der Systemverwalter zum Beispiel nach einem Neustart das BIOS-Setup aus der Ferne aufrufen kann. Neben spezieller Management-Software bieten Hersteller auch verschiedene hardwarebasierte Managementlösungen an.

3.2.1 Grundlagen des Remote-Managements

Um das reibungslose Funktionieren der Server- und auch Client-Systeme im Netzwerk zu gewährleisten, kommt es auf drei Schritte an: die Erkennung der vorhandenen Hard- und Software, die Wiederherstellung der Systeme im Falle eines Fehlers und den Schutz der Systeme vor Gefahren. Dieser Dreiklang aus Inventarisierung, Fernwartung und Security-Management muss jederzeit gegeben sein – egal in welchem Zustand sich das einzelne System aktuell befindet.

Die meisten Remote-Tools für diese Aufgaben des IT-Managements leiden jedoch an einem entscheidenden Manko: Damit die Management-Tasks ausgeführt werden können, muss auf den aus der Ferne zu administrierenden Systemen ein funktionstüchtiges Betriebssystem installiert sein und tatsächlich laufen, weil sonst der Agent nicht arbeiten kann.

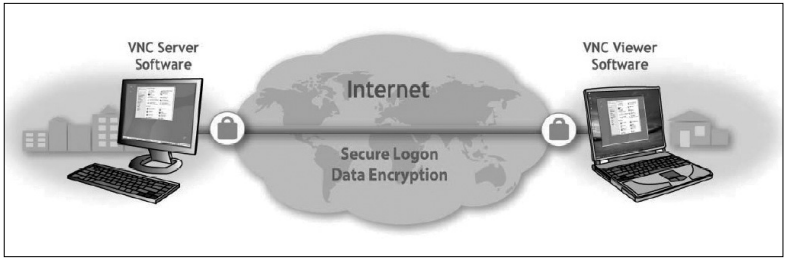
Schwierigkeiten unterhalb dieser Schranke lassen sich nur durch Besuche vor Ort und die komplette Festplattenformatierung sowie Neuinstallation beheben. Darüber hinaus lässt sich nicht immer zweifelsfrei feststellen, welche Systeme tatsächlich gerade im Netzwerk in Betrieb sind.



Steuerzentrale: Bei einem Systemproblem kann der Systemadministrator per IT-Management-Konsole jederzeit auf den „defekten" Rechner zugreifen und gegebenenfalls den Fehler beheben oder Diagnoseroutinen aufrufen. (Quelle: Intel)

3.2.2 Remote-Management- und Client-Software

Diese Art von Lösung ermöglicht IT-Administratoren den Zugriff auf den Desktop sowie auf Anwendungen des Ziel-Servers. Ein deutlicher Nachteil von Remote-Verwaltungs-Software wie zum Beispiel den Programmen VNC (www.realvnc.com), Enteo (www.enteo.com/de) oder Radmin (www.radmin.de) besteht darin, dass sie nur verwendet werden kann, wenn das Zielbetriebssystem verfügbar ist. Reagiert das Betriebssystem nicht mehr oder ist es abgestürzt, ist der Zugriff auf den Server nicht möglich.



Remote-Management: Für die Nutzung einer Remote-Softwarelösung muss der Anwender auf dem Quell- und Zielsystem jeweils ein entsprechendes Remote-Programm installieren. (Quelle: RealVNC)

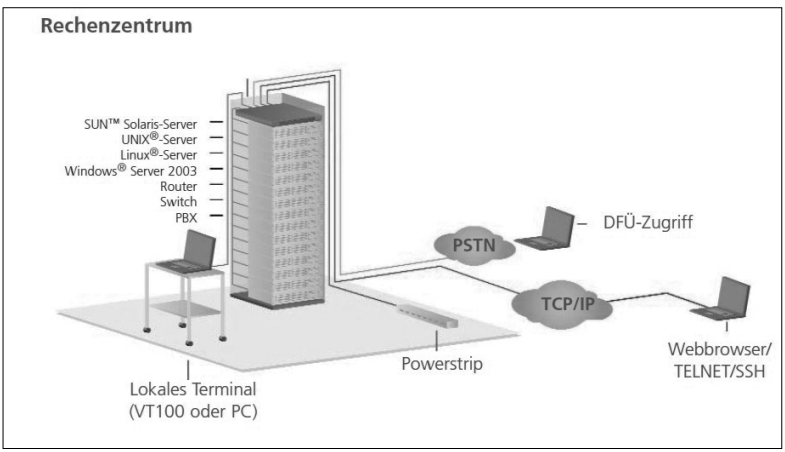
Darüber hinaus sind diese Softwarelösungen von einer Verbindung mit der Netzwerkkarte des Ziel-Servers abhängig. Auch dabei gilt: Ist das Netzwerk nicht verfügbar, lässt sich das Server-Problem nicht beheben, und es muss ein Techniker vor Ort eingesetzt werden.

Für den Zugriff auf Geräte mit serieller Schnittstelle wie Router, Switches oder Server werden häufig Telnet und SSH verwendet. Ebenso wie bei der Remote-Verwaltungs-Software ist diese Zugriffsmethode nur bei vorhandener Netzwerkverbindung effektiv. Sollte ein Problem mit dem WAN vorliegen, muss sich möglicherweise ein IT-Techniker vor Ort damit auseinandersetzen.

Zudem werden zum Beispiel die Nebenstellen eines Unternehmens aufgrund dieser Wartungsschnittstellen anfälliger für Angriffe in das Netzwerk. Grund: Diese Schnittstellen können besonders einfach von Hackern zum Stehlen von Daten sowie zum Einschleusen von Viren verwendet werden.

3.2.3 Sichere Konsolen-Server (SCS)

Den gemeinsamen Nenner aller IT-Systeme in einem dezentralen Unternehmen bildet das Netzwerk, für das üblicherweise ein Router, ein Switch und eine Firewall benötigt werden. Fällt eine dieser Komponenten an einem Remote-Standort



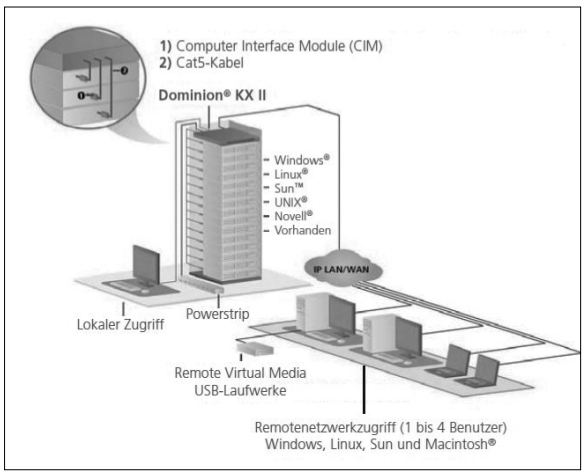
Steuermann: Bei sicheren Konsolen-Servern (SCS) benötigt der Administrator nur eine Online-Verbindung, um überall auf Netzwerkgeräte wie Server oder Switches zuzugreifen. (Quelle: Raritan)

aus, kann sich dies negativ auf das Unternehmen auswirken. Die Mehrzahl der Netzwerkgeräte verfügt über eine serielle Schnittstelle, und für den Zugriff und die Wartung wird – wie bereits erwähnt – üblicherweise auf SSH und Telnet gesetzt. Beim Auftreten eines Problems mit dem Netzwerk lassen sich diese Zugriffs-Tools

jedoch nicht verwenden. Sichere Konsolen-Server (Secure Console Servers, SCS) nutzen die serielle Management-Schnittstelle und bieten über SSH / Telnet sowie den Webbrowser Remote-Zugriff auf verwaltete Server und andere serielle Geräte. Bei dieser seriellen Zugriffsart des SCS handelt es sich auch um einen standarisierten zentralen Zugriffs- und Steuerungspunkt für WAN- und Netzwerkgeräte sowie für Geräte zur Stromverteilung. Ein weiterer Vorteil von SCS besteht darin, eine DFÜ-Verbindung herzustellen für den Fall, dass das WAN nicht verfügbar sein sollte. Dadurch muss sich der IT-Techniker nicht extra an den Remote-Standort begeben, was wiederum eine schnellere Reparatur ermöglicht und Kosten spart. Darüber hinaus kann die Auswahl eines geeigneten SCS dazu beitragen, zum Beispiel die Zweigniederlassung mit zusätzlichen Sicherheitsebenen zu versorgen und somit dem Diebstahl sensibler Unternehmens- oder Kundendaten durch Hacker vorzubeugen.

3.2.4 KVM-over-IP-Switch

Aktuelle und moderne KVM-Switch ermöglicht mehreren Benutzern das Herstellen einer Verbindung mit mehreren Servern beziehungsweise Netzwerkgeräten über eine jeweils eigene, vom KVM-Switch unterstützte Konsole. Bei KVM-over-IP-Switches ist die Anzahl der Benutzer, die gleichzeitig auf einen KVM-Switch arbeiten können, begrenzt. Zum Umgehen solcher Beschränkungen können Server, auf die besonders häufig zugegriffen wird, auf mehrere KVM-über-IP-Switches aufgeteilt werden. Einer der Vorteile der KVM-over-IP-Lösung liegt darin, dass für diese Lösung nur relativ wenige Cat5-Kabel benötigt werden. Dadurch stellen sie für Umgebungen, in denen nur begrenzte Verkabelungsmöglichkeiten gegeben sind, eine gute Remote-Alternative dar.



Management mit Komfort: Ein KVM-over-IP-Switch stellt den sicheren Zugriff auf die Server von jedem Standort innerhalb und außerhalb des Rechenzentrums bereit. Erweiterte Modelle bieten zudem eine hohe Videoqualität und eine gute Maussynchronisation. (Quelle: Raritan)

Ein Beispiel für eine solche Umgebung wäre die Erweiterung eines bereits vorhandenen Rechenzentrums. Dabei ist zu beachten: Je mehr Kabel in einem Server-Rack verlegt werden, desto stärker sind die Auswirkungen auf die Luftzirkulation, was zu zusätzlichen Hitzeproblemen führen kann.

Analoge KVM-Switches

Die beste Maus- und Videosynchronisierung lässt sich mit einem analogen KVM-System erzielen, das lokal und über ein eigenes Netzwerk als Out-of-Band-Lösung betrieben wird. Abhängig vom Netzwerkverkehr und von der Entfernung zwischen Benutzer und Switch können bei KVM-over-IP-Switches eine geringe Verzögerung sowie eine gewisse Verschlechterung der Bildqualität auftreten.

Bei einem analogen KVM-System wird die Verbindung mit Servern und Konsolen über ein dediziertes und vor Ort befindliches Netzwerk hergestellt. Da die Informationen nicht über ein IP-Netzwerk gesendet werden, bietet ein analoges KVM-System höchstmögliche Sicherheit; es bestehen jedoch Beschränkungen hinsichtlich der Entfernung, und der Remote-Zugriff ist auf den Standort des Rechenzentrums beschränkt.

Sicherheit von KVM-over-IP-Switches

KVM-over-IP-Switches werden über ein IP-basiertes Netzwerk eingebunden. Das bedeutet, dass der Datenverkehr für jedermann verfügbar ist. Allerdings lässt sich der Datenverkehr für nahezu jeglichen auf Sicherheit bedachten Endbenutzer mithilfe geeigneter Verschlüsselungs-, Authentifizierungs- und Autorisierungsanwendungen ausreichend schützen.

So verfügen intelligente KVM-over-IP-Systeme über eine sichere Verschlüsselung wie etwa 256-Bit-AES und unterstützen branchenübliche Authentifizierungs- und Autorisierungssysteme wie LDAP-S (Webcode **401872**), Active Directory (Webcode **443285**) und RADIUS (Webcode **465711**). Das Informieren der IT-Mitarbeiter und Endbenutzer über anstehende Veränderungen und Ausfälle umfasst nicht nur die einfache Benachrichtigung, sondern oftmals auch das Erstellen von Dokumentationen sowie das Durchführen von Schulungsmaßnahmen in verschiedensten, von der jeweiligen Zielgruppe abhängigen Bereichen.

3.2.5 Baseboard Management Controller (BMC)

Gute Administrierbarkeit ist ein dediziertes Auswahlkriterium für Server, deshalb sollten diese Systeme grundsätzlich mit einem sogenannten Baseboard Management Controller (BMC) ausgestattet sein. Der BMC ermöglicht den Fernzugriff auf den Server über das Netzwerk ohne eine serielle Verbindung. Administratoren können damit den Server auch von einem entfernten Standort aus überwachen, verwalten und bei Bedarf sogar herunterfahren und neu starten.

Der BMC übernimmt die proaktive Überwachung und gibt eine Warnung aus, sobald das System benutzerdefinierte Schwellenwerte für eine Reihe kritischer Funktionen erreicht. Die Verwaltung des BMC erfolgt unabhängig vom Betriebssystem und vom Status des Servers. Der Administrator kann also auch dann noch über das Netzwerk auf den Server zugreifen, wenn dieser ausgefallen ist, um zum Beispiel das BIOS zu überprüfen.

Wichtig dabei ist: Der BMC sollte kompatibel zu IPMI (Intelligent Platform Management Interface, www.intel.com/design/servers/ipmi/) sein. IPMI ist ein branchenübergreifender Industriestandard, mit dem die Verwaltung von Servern unterschiedlicher Hersteller verbessert werden soll. Standardisiert wurden dabei Verwaltungshardware, Überwachung, Warnfunktionen und Kommunikation. Das kommt vor allem größeren Unternehmen zugute, weil sie ihre Server über eine gemeinsame Oberfläche verwalten können. Administratoren sind damit produktiver, weil sie mit weniger Tools auskommen.

3.2.6 Fazit

KVM-Fernzugriff ist ein einfaches und zugleich leistungsstarkes Konzept. Zwar gibt es keinen adäquaten Ersatz für einen vor Ort befindlichen IT-Experten, der die Systeme am Laufen hält, doch ist dies ein Luxus, den sich nur die wenigsten Unternehmen leisten können.

Die zweitbeste Lösung besteht in der Verwendung geeigneter Tools zur Ausdehnung der Reichweite der am Hauptsitz tätigen IT-Mitarbeiter auf die Remote-Standorte eines Unternehmens. Während einige dieser Tools derzeit scheinbar sehr günstig oder gar kostenlos zu haben sind, ergeben sich die Kosten bei diesen Produkten durch Abstriche bei Verfügbarkeit und Sicherheit.

Das Ergebnis sind möglicherweise unerwartete Reisekosten und Ausfallzeiten, also eben jene Aspekte, die durch den Einsatz von Remote-Zugriffs-Lösungen vermieden werden sollen. So hängt die richtige KVM-Entscheidung vom jeweiligen Bedürfnis eines Unternehmens ab und ermöglicht den IT-Mitarbeitern einen reaktionsschnellen, sicheren, flexiblen, einfachen und preisgünstigen Zugriff auf die IT-Geräte ihres Unternehmens, um diese verwalten zu können. Dabei stehen dem IT-Verantwortlichen unterschiedliche technische Lösungen zur Verfügung.

Bernhard Haluschak

Bernhard Haluschak ist als Hardware-Redakteur bei TecChannel tätig. Der Dipl. Ing. (FH) der Elektrotechnik / Informationsverarbeitung blickt auf langjährige Erfahrungen im Server-Umfeld und im Bereich neuer Technologien zurück. Vor seiner Fachredakteurslaufbahn arbeitete er in Entwicklungslabors, in der Qualitätssicherung sowie als Laboringenieur in namhaften Unternehmen.

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

3.3 Test – Hochverfügbarkeit mit Server-Cluster

In Unternehmen mit kritischen Anwendungen muss die IT hochverfügbar ausgelegt sein. Neben ausfallsicheren Servern sind Server-Cluster eine probate Lösung. Wir haben ein Cluster-System auf Basis der Avance-Software von Stratus in Hinblick auf Installation und Management sowie High Availability (HA) getestet.

Kleine und mittelständische Unternehmen, die extrem von der IT abhängig sind, können sich Server-Ausfälle nicht leisten. Doch dem Crash eines Servers kann man vorbeugen. Es gibt hierzu verschiedene technische Ansätze. So können etwa kritische Hardwarekomponenten in einem System redundant ausgelegt sein oder fehlertolerante Technologien eingesetzt werden. Dazu zählen zum Beispiel beim Storage die RAID-Funktionen (Webcode **401665**) oder beim Hauptspeicher die ECC oder Mirroring-Technologie (Webcode **402181**).

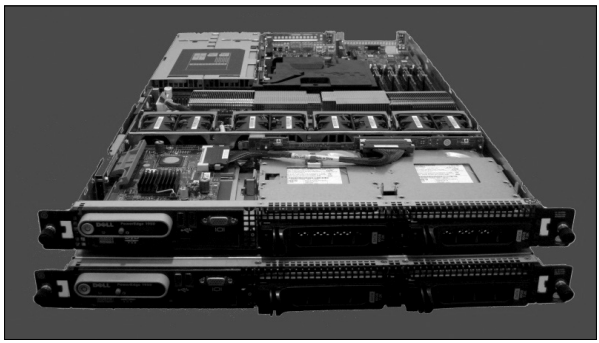
Noch mehr Ausfallsicherheit bieten redundante Server-Systeme wie etwa Hochverfügbarkeits-Cluster (Webcode **456463**). Diese bestehen in der Regel aus mindestens zwei identischen Servern, die miteinander verschaltet sind. Alle Funktionen und Anwendungen laufen simultan ab, und jedes System kann im Notfall autark weiterarbeiten. Ist das defekte System wieder betriebsbereit, synchronisieren sich die Server automatisch und arbeiten anschließend wieder parallel weiter. Dazu gehört neben der Hardware auch eine entsprechende Steuersoftware.

Wir haben die Cluster-Lösung „Avance“ von Stratus (www.stratus.de) unter die Lupe genommen und diese detailliert untersucht. Dieses System soll extrem fehlertolerant und besonders für SMB-Unternehmen geeignet sein. Unser ausführlicher Test informiert über Funktionsweise, Installation und Handhabung sowie die Ausfallsicherheit des Cluster-Systems.

3.3.1 Testsystem: 2x Dell PowerEdge 1950

Unser Server-Cluster-Testsystem besteht aus zwei 1HE-Rack-Servern von Dell (www.dell.de), die miteinander „verschaltet“ sind. Bei den Systemen handelt es sich um identische PowerEdge-1950-Server. Laut Stratus sind diese Geräte für die Avance-Software zertifiziert und eignen sich somit für unseren Test. Da die zwei Systeme identisch aufgebaut sind, beschränkt sich unsere Hardwarebeschreibung auf ein Gerät. Für die Rechenleistung unserer Testkandidaten sorgen zwei Dual-Core-Xeon-Prozessoren des Typs E5140 mit 2,33 GHz und je vier MByte L2-Cache. Als Unterbau fungiert das Server-Mainboard S5000PAL von Intel. In den insgesamt acht DIMM-Slots unseres Testgeräts steckt mit vier je 1-GByte-FB-DIMM nur die Minimalkonfiguration an Hauptspeicher. Um Systemabstürze durch Speicherfehler zu vermeiden, beherrscht der Server die Memory-Security-Funktionen (Webcode **402181**) ECC, Memory Mirroring und Memory Spare.

Mit zwei Steckkartenplätzen für PCI-Riser-Module lässt der Server einen ausreichenden Spielraum für Erweiterungen. Um den Server in ein Netzwerk einzubinden, verfügt dieser über zwei Gigabit-Onboard-Controller samt ausgeführten Schnittstellen. Für den Anschluss externer Geräte stehen dem User auf der Rückseite zwei USB-2.0-Ports sowie zwei serielle Schnittstellen zur Verfügung. Zusätzlich kann der Anwender zwei USB-2.0-Schnittstellen an der Frontseite benutzen. Darüber hinaus ist je ein Display-Anschluss auf der Rück- und Vorderseite verfügbar. Einen Remote-Management-Controller zum Managen des Servers besitzt das System nicht – dieser ist aber optional erhältlich.



Systemdetails: Das Cluster-Testsystem besteht aus zwei identischen PowerEdge-1950-Servern von Dell.

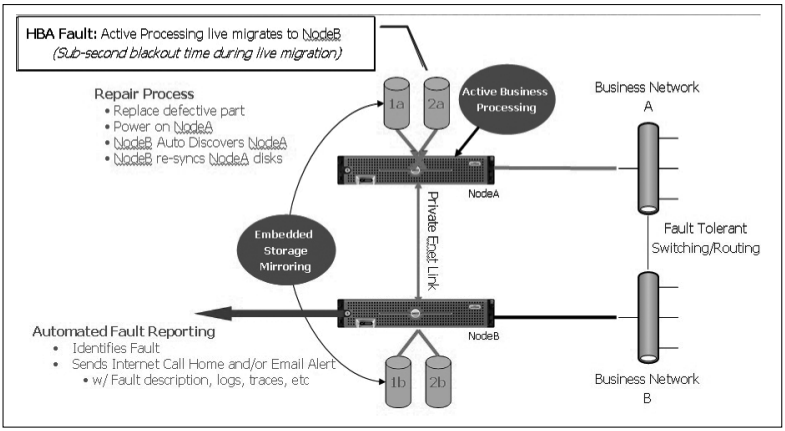
Unser Testsystem ist mit zwei 80 GByte großen SATA-II-Festplatten von Seagate ausgestattet, die nicht als RAID-Verbund arbeiten. Die Verwaltung der HDDs übernimmt der Onboard-SATA-II-Controller. Die Laufwerkskonfiguration des Servers rundet ein Slim-DVD-ROM ab. Um die Temperatur im Inneren des Server-Gehäuses möglichst gering zu halten, besitzt der Server redundante Lüfter. Ebenfalls Hotswap-fähig und redundant sind die zwei 670-Watt-Netzteile.

3.3.2 Funktionsweise des Avance-HA-Cluster

Bei der Avance-Cluster-Lösung von Stratus handelt es sich um ein auf Citrix XenServer (www.citrix.de/produkte/schnellsuche/xenserver/) basierendes Hochverfügbarkeits-Cluster. Im Allgemeinen besteht ein Cluster aus mindestens zwei Servern, den sogenannten Knoten. Fällt ein Knoten aus, übernimmt automatisch der zweite Knoten die Arbeit (Failover). Zusätzlich können Wartungsarbeiten am System durchgeführt werden, ohne dass die Verfügbarkeit der laufenden Dienste darunter leidet. Stratus Avance macht aus zwei Standard-x86-Servern ein hochverfügbares System. Dabei installiert die Avance-Software auf beiden Servern jeweils einen „logischen" Server auf Basis der Open-Source-Virtualisierungssoftware Citrix XenServer. Darauf lassen sich beliebig viele virtuelle Server einrichten, auf denen Anwendungs-Server und Applikationen unter Windows oder Linux betrie-

ben werden können. Sobald die VMs eingerichtet sind, repliziert sie Avance auf die andere Node im System; ein gemeinsamer Speicher über iSCSI oder Fibre-Channel SAN ist nicht notwendig.

Die beiden Rechner werden über eine Netzwerkverbindung gekoppelt und durch Avance permanent überwacht und synchronisiert. Beim Ausfall eines Servers kann der jeweils andere den Betrieb automatisch übernehmen.



Funktionsübersicht: Der schematische Aufbau des Stratus-Clusters verdeutlicht die Funktionsweise des Systems. (Quelle: Stratus)

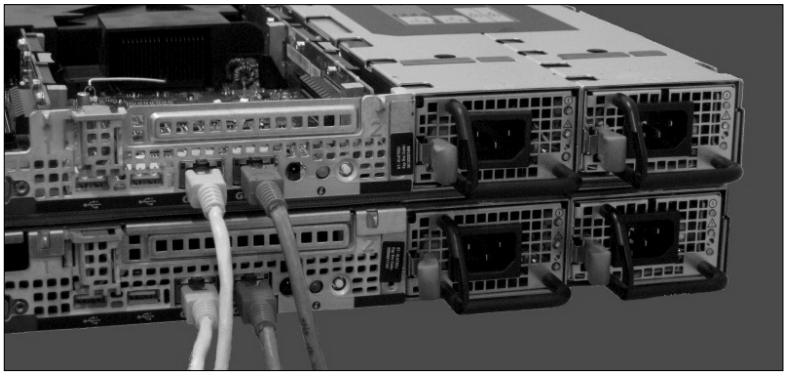
Die Software kann von einer Managementkonsole aus gesteuert werden. Die Lösung verfügt über integrierte Prognosewerkzeuge, die die meisten Hardware- und Softwareprobleme schnell identifizieren. IT-Personal kann die virtuellen Maschinen, die physikalischen x86-Server und die Netzwerkschnittstellen aus der Ferne überwachen und verwalten. Damit eignet sich Avance auch für den Einsatz an entfernten Standorten ohne Fachpersonal vor Ort.

3.3.3 Installation der Avance-Cluster-Software

Für die schnelle und einfache Inbetriebnahme beziehungsweise Konfiguration des Hochverfügbarkeits-Clusters offeriert Stratus dem Anwender einen *Installation and Configuration Guide* und einen *User Guide*. Diese Anleitungen erklären Schritt für Schritt die Hardwareinstallation und die Netzwerkkonfiguration sowie die Funktionsweise der Avance-Software.

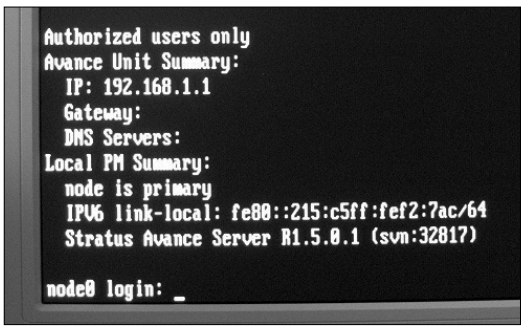
Vor dem Starten des Clusters müssen die beiden Server-Einheiten über ein direktes Netzwerkkabel (Direkt Link) miteinander verbunden werden. Zusätzlich benötigt das System eine Verbindung ins „externe“ Netzwerk. Diese Kommunika-

tionspfade dienen dem Cluster-Manager zur Überwachung der beiden Cluster-Knoten. Darüber hinaus ist eine Web-Konsole in Form eines Client-PCs (Managementkonsole) erforderlich; sie übernimmt die Ansteuerung und Kontrolle des Clusters über das Netzwerk.



Rückseite: Die beiden Server-Nodes des Clusters sind direkt über eine Netzwerkverbindung (dunkles Netzwerkkabel) miteinander verbunden.

Vor der Installation von Avance muss der Anwender das Server-BIOS entsprechend den Stratus-Vorgaben modifizieren. Dazu ist zwingend erforderlich, dass im CPU-Setup die Funktionen *Execute Disable* und die Option *Virtualization Technology* auf Enable gestellt werden. Zusätzlich muss die Boot-Sequenz des Servers mit dem integrierten NIC1 beginnen, dann folgen die Festplatte und das CD-ROM-Laufwerk. Darüber hinaus sollten das Datum und die Zeit korrekt eingestellt sein sowie kein System-Passwort vergeben sein. Wichtig vor dem ersten Boot-Vorgang ist die Onbaord-Storage-Konfiguration des Servers. Diese sollte zwei logische Laufwerke enthalten, und zwar unabhängig von der „internen" Konfiguration der physikalischen Festplatten.

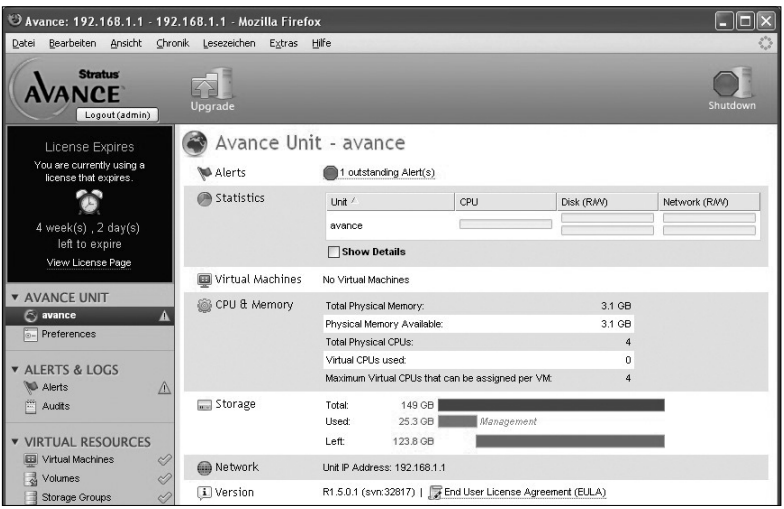


Fertig: Die beiden Server des Cluster sind betriebsbereit und können jetzt über eine Managementkonsole im Netzwerk angesprochen werden.

Die Installation von Avance erfolgt explizit über das CD-ROM-Laufwerk von einem der beiden Node-Server. Hierzu sind ein Monitor und eine Tastatur am Server erforderlich. Per PXE-Option lässt sich die Avance-Software zurzeit noch nicht installieren, so der Hersteller. Nach dem Boot-Vorgang von der Avance-CD verlangt der Server die Eingabe des *Install*-Kommandos inklusive der anwenderspezifischen Netzwerkvorgaben. Unser Testsystem initialisierten wir mit dem Eingabe: *install ip=192.168.1.1/24*. Danach startete der Installationsvorgang.

Nach zirka zehn Minuten führt der Installations-Server einen selbstständigen Reboot durch, und nach weiteren acht Minuten konnten wir den Node-Server erstmals über eine entsprechend konfigurierte Konsole (http://192.168.1.1) erreichen. Jetzt muss der User grundlegende Konfigurationen wie Lizenzierung der Software, Anlegen eines User-Accounts sowie Einstellen des Datums und der Uhrzeit durchführen. Anschließend bootet das System erneut, und nach acht Minuten erscheint auf der Managementkonsole zum ersten Mal der Login-Bildschirm. Damit ist die Installation des ersten Node-Servers abgeschlossen.

Nach dem Login wird der zweite Node-Server automatisch installiert. Während dieser Zeit kann noch keine virtuelle Maschine konfiguriert werden. Dieser Vorgang dauerte in unserem Test rund 17 Minuten und muss vom Anwender mit dem Umschalten des Nodes vom Maintenance- in den Running-Mode mit dem Finalize-Button abgeschlossen werden. Erst jetzt, nach insgesamt etwa 45 Minuten, ist der Server Cluster für die Installation von VMs und den entsprechenden Applikationen bereit.

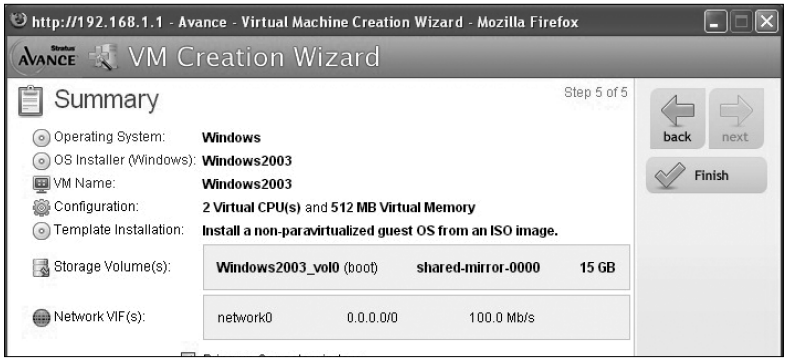


Steuerzentrale: Die Verwaltung des Server-Systems vereinfacht der webbasierte Cluster-Manager. Dieser unterstützt den Anwender bei der Konfiguration und Wartung. Zusätzlich informiert er den Anwender über den Status des Clusters.

Die Bedienerführung der Avance-Cluster-Software ist intuitiv und leicht verständlich. Sind alle Grundeinstellungen vorgenommen worden und alle notwendigen Netzwerkparameter bekannt, lässt sich die Installationsprozedur auch ohne tiefgreifendes technische Know-how problemlos bewältigen.

3.3.4 Installation und Verwaltung von virtuellen Maschinen

Die Virtualisierungssoftware Avance bietet die Möglichkeit, über ISO-Images isolierte Virtual Machines (VMs) auf dem Cluster-Server zu installieren. Die Stratus-Lösung unterstützt dabei alle gängigen Windows- und Linux-Betriebssysteme außer Windows Server 2008. Dieser Support soll erst in der Avance-Version 1.6 integriert werden. Die einzelnen unabhängig voneinander agierenden VMs arbeiten als selbstständige virtuelle Server. Aktuell unterstützt der Hersteller maximal zwei virtuelle Prozessoren pro physischen CPU-Kern. Diese können als virtuelle Prozessoren (vCPU) auf eine oder auf mehrere virtuelle Maschinen verteilt werden. Die Anzahl der maximal unterstützten virtuellen Maschinen ist 16. In unserem Test (2x Dual-Core-CPUs) können nicht mehr als acht Instanzen (VMs) auf unserem Testsystem installiert werden.



Zusammenfassung: Das Avance-Tool unterstützt den Nutzer bei der Erstellung virtueller Maschinen.

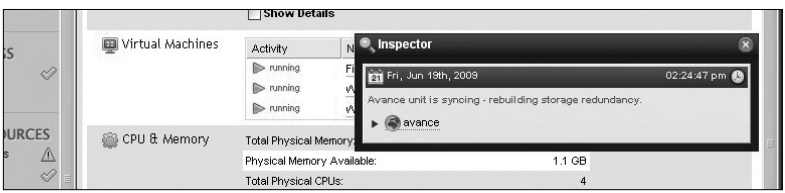
Das Erstellen einer VM auf dem Avance-Cluster-System ist denkbar einfach. Der Anwender wechselt dafür in die *Virtual Resources* der Avance-Software und betätigt den *Create-Button*. Die selbsterklärende Menüführung leitet den User dann durch die Installation. So wird im ersten Schritt nach dem Betriebssystem der zu installieren VM gefragt (Linux oder Windows) und der Quell-Ort des ISO-Images festgelegt. Ein Manko der Avance-Software ist, dass es explizit nur ISO-Images verarbeitet und diese nur über das Netzwerk oder direkt vom Cluster-Server-CD-ROM-Laufwerk (Node0) installiert werden können. Eine IDE-Redirect-Funktion auf das lokale Laufwerk der Managementkonsole fehlt.

Nach Festlegung des VM-Namens, der virtuellen CPUs und des Hauptspeichers erfolgen die Definition des Storage-Systems und die Konfiguration des Netzwerks. Vor dem Start der VM-Installation kann der Anwender in einer Übersicht die Einstellungen nochmals überprüfen. Danach geht der Vorgang den gewohnten Weg einer standardmäßigen Betriebssysteminstallation – allerdings ohne die paravirtuellen Treiber. Diese müssen noch, nach der Erstellung der VM, in einem zweiten Durchgang nachinstallierte werden. Erst dann steht die VM fehlerfrei zur weiteren Nutzung auf dem Cluster zur Verfügung. Der gesamte Vorgang der VM-Installation dauerte auf unserem Testsystem etwa 21 Minuten. Um weitere VMs zu installieren, muss die oben beschriebene Verfahrensweise wiederholt werden. Eine Kloning-Funktion für VMs bietet die Avance-Software leider noch nicht.

3.3.5 Praxistests: Ausfallsicherheit

Um die Hochverfügbarkeit des Clusters zu testen, integrieren wir die Geräte in unser abgeschlossenes Labornetzwerk. Darin befinden sich drei Windows-Clients sowie ein Domänen-Controller. Die Clients sind an einem Gbit-Switch angeschlossen: Das getestete Cluster verwendet für jeden Knoten jeweils einen Gbit-Link zum Switch. Wie lang der Cluster bei einem provozierten Ausfall wie Ziehen des Netzsteckers oder des Netzwerkkabels, Ausfall einer Festplatte und Totalausfall eines Servers benötigt, um eine VM auf den sicheren Knoten zu migrieren, haben wir detailliert getestet:

Das Ergebnis: Der Server-Cluster benötigt beim Ausfall eines Netzteils oder eines Netzwerkkabels des aktiven Nodes wenige Sekunden, bis die VM wieder funktionsfähig auf dem "sicheren" Node arbeitet. In unserem Test ermittelten wir einen Wert von 20 Sekunden. In dieser Zeit migriert die Avance-Software im laufenden Betrieb alle VMs von dem "defekten" Server auf den Ersatz-Node. Nach dem Austausch des Netzteils benötigt das System weitere 27 Sekunden, bis das Cluster wieder seine Redundanz erreicht hat.



Storage-Problem: Nach einem Festplattenausfall synchronisiert das System mittels des Inspectors die Storage-Laufwerke und stellt die Redundanz des Storage-Subsystems auf dem Cluster wieder her.

Alle Fehler, die nur den Node1 betreffen, haben auf die Funktion der VMs auf dem „aktiven" Node keinen Einfluss. Allerdings wird das ganze System in einen Warnmodus versetzt, der den Administrator informiert, dass er das Cluster

schnellstmöglich instandsetzen soll. Eine Hochverfügbarkeit ist in diesem Modus nicht mehr gewährleistet. In unserem Test benötigte ein Festplattenausfall auf dem passiven Node etwa 18 Minuten – inklusive eines Reboots, um das System wieder in den ursprünglichen redundanten Zustand zu bringen.

3.3.6 Fazit

Das Hochverfügbarkeits-Cluster-System Avance von Stratus ist zwar nicht in 15 Minuten vollständig installiert, wie dies der Hersteller suggeriert, doch es erfüllt die Anforderungen an ein HA-System, das eine Ausfallsicherheit von 99,99 Prozent verspricht. Den zentralen Bestandteil der Cluster-Lösung von Stratus bildet die Avance-Software. Sie hat der Hersteller für bestimmte Server-Modelle zertifiziert, und nur auf diesen Geräten garantiert Stratus auch eine sichere Funktion. Vorerst unterstützt Avance 1.5 nur gängige Server von Dell und HP, weitere Hersteller sollen mit den nächsten Updates dazukommen.

Die Installation der Avance-Software ist, wie der Hersteller versprochen hat, sehr einfach und problemlos durchzuführen. In unserem Test benötigten wir bis zur vollständigen Lauffähigkeit des Avance-Systems auf der vorgegebenen Hardware rund 45 Minuten. Erst dann können die entsprechenden VMs für die Anwendungen installiert werden. Die getestete Stratus-Lösung der Version 1.5 unterstützt pro installierter VM maximal zwei virtuelle Prozessoren sowie insgesamt nur acht Instanzen. Darüber hinaus bietet Avance zurzeit keinen Support für Nehalem-Prozessoren (Webcode **2019750**) sowie Windows Server 2008; diese werden erst mit der Version 1.6 unterstützt.

Die Ausfallszenarien in unserem Test bewältigte das Cluster-System rasch und fehlerfrei. Je nach Systemfehler und Node bemerkt der Anwender den Systemausfall gar nicht oder er muss auf seine Applikation nur wenige Sekunden warten. Allerdings können bis zur vollständigen Wiederherstellung der Ausfallsicherheit – abhängig vom Fehler – mehrere Minuten vergehen.

In puncto Funktionalität und Handhabung bietet die Stratus-Lösung umfangreiche Features, die dem Administrator die Arbeit und die Überwachung des Systems erleichtern. Ein Preis von 4000 Euro für ein 2-x-2-Wege-System oder 5000 Euro für ein 2-x-4-Wege-System sind für das Avance-HA-Cluster-System angemessen. Es fallen aber noch zusätzliche Kosten in Höhe von 960 Euro für Support und Updates pro Jahr an. Darüber hinaus muss der Anwender die entsprechenden Hardwarekosten auch noch extra dazurechnen

Bernhard Haluschak

Bernhard Haluschak ist als Hardware-Redakteur bei TecChannel tätig. Der Dipl. Ing. (FH) der Elektrotechnik / Informationsverarbeitung blickt auf langjährige Erfahrungen im Server-Umfeld und im Bereich neuer Technologien zurück. Vor seiner Fachredakteurslaufbahn arbeitete er in Entwicklungslabors, in der Qualitätssicherung sowie als Laboringenieur in namhaften Unternehmen.

3.4 Intel: Nehalem EX greift RISC-CPUs an

Intel gibt neue Details zu seinem ersten 8-Core-Prozessor Nehalem EX bekannt. Der Xeon MP für Mehrwegesysteme soll den größten Performance-Sprung gegenüber dem Vorgänger in Intels CPU-Historie machen. Neue RAS-Features sorgen für Hochverfügbarkeit auf RISC-Niveau.

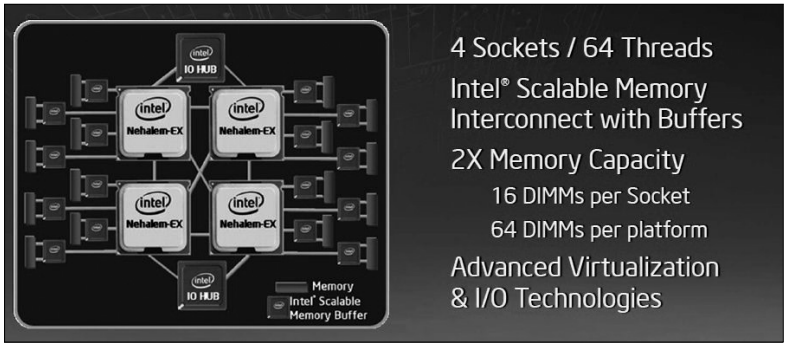
Der Nehalem EX wird Intels nächste Generation der Xeon-MP-Serie für Server mit vier und mehr Sockeln. Aktuelles Topmodell für die Mehrwege-Server ist der Xeon X7460 Dunnington (Webcode **1771836**). Der 6-Core-Prozessor basiert auf der 45-nm-Core-Architektur und verwendet die Xeon-MP-Plattform Caneland (Webcode **1728728**). In der zweiten Jahreshälfte 2009 schwenkt Intel dann auch bei den Xeons für Mehrwegesysteme auf die Nehalem-Architektur um. Für Desktop-PCs gibt es seit November 2008 die Core-i7-CPUs mit Nehalem-Architektur (Webcode **1775602**). Im März 2009 folgte dann die Xeon-5500-Serie für 2-Sockel-Systeme (Webcode **1979997**). Der Xeon MP mit dem Codenamen „Nehalem EX" wird Intels erster 8-Core-Prozessor sein. Alle acht Kerne sind auf einem Siliziumplättchen vereint. Laut Intel benötigt der Nehalem EX 2,3 Milliarden Transistoren. Der aktuelle Xeon X7460 mit sechs Kernen und 25 MByte Cache (9M L2-Cache, 16M Shared L3-Cache) besteht aus 1,9 Milliarden Transistoren.

Intel (www.intel.de)wird den Nehalem EX weiterhin im 45-nm-Prozess fertigen. Die Puffergröße beziffert Intel mit „24 MByte Shared Cache". Zwar detailliert Intel einzelnen Caches des Nehalem EX nicht weiter, allerdings wird es sich dabei um den Shared L3-Cache handeln. Wie bei der Nehalem-Architektur üblich, besitzt jeder Kern einen dedizierten 256 KByte fassenden L2-Cache.

Intels Nehalem EX kann durch sein zusätzliches Hyper-Threading pro Kern insgesamt 16 Threads parallel abarbeiten. In einem 4-Sockel-Server sieht das Betriebssystem somit insgesamt 64 virtuelle Prozessoren. Die Turbo-Technologie zum Steigern der Taktfrequenz einzelner Kerne integriert Intel im Nehalem EX ebenfalls, wie der Hersteller bekannt gab. Um welchen Faktor die Turbo-Technologie die Taktfrequenz bei einem bis hin zu acht ausgelasteten Cores erhöht, sagt Intel noch nicht.

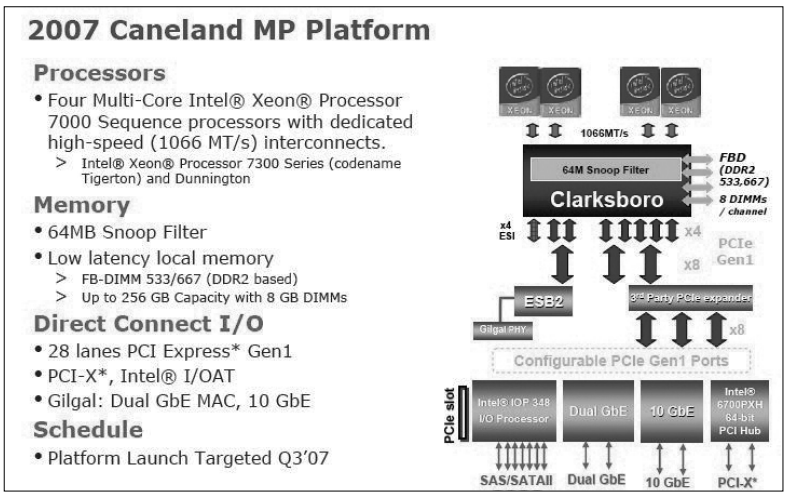
3.4.1 Hohe Skalierfähigkeit

Der Nehalem EX benötigt durch sein QuickPath-Interface und den integrierten Speicher-Controller eine komplett neue Plattform. Das Interface des Nehalem EX soll pro Link 6,4 GT/s ermöglichen. Beim Core i7 975 Extreme Edition arbeitet das QuickPath-Interface ebenfalls mit 6,4 GT/s. Intel spendiert dem Nehalem EX dabei vier QuickPath-Schnittstellen. Damit lassen sich 8-Sockel-Systeme direkt über QuickPath realisieren. Systeme mit mehr als acht Prozessoren sind durch einen zusätzlichen Node-Controller von OEMs möglich. Mehr als 15 Serversysteme mit acht oder mehr Nehalem-EX-Prozessoren sind laut Intel bei den OEMs in Arbeit.



FSB ade: Mit Nehalem EX führt Intel die QuickPath-Architektur in Mehrwegesystemen ein. Jeder Nehalem EX verfügt über vier QuickPath-Schnittstellen und vier integrierte Speicher-Channels. (Quelle: Intel)

Jeder Nehalem EX steuert über vier integrierte Speicher-Controller jeweils einen „Scalable Memory Interconnect with Buffers" an. Voraussichtlich handelt es sich bei den angeschlossenen Speichermodulen um normale DDR3-DIMMs – die Interconnects ersetzen die FB-DIMM-Technologie. Laut Intel sind pro Nehalem EX 16 DIMMs möglich. Jeder der vier Speicher-Channels mit dem „Scalable Memory Interconnect" steuert somit vier DIMMs an. Eine 4-Sockel-Plattform ermöglicht insgesamt 64 DIMMs. Damit verdoppelt sich laut Intel die Speicherkapazität gegenüber der Xeon-7400-Plattform. Die Speicherbandbreite erhöht sich bei einem Nehalem-EX-System um den Faktor 9 gegenüber der Xeon-7400-Plattform.

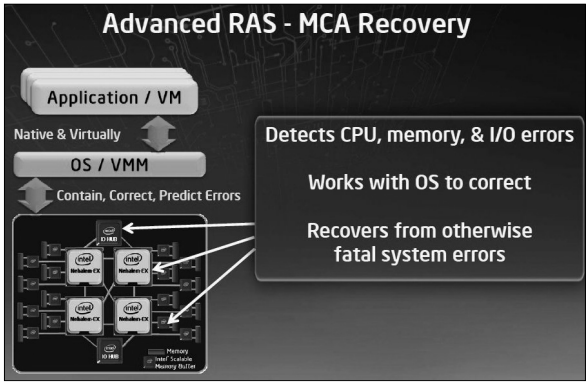


Vorgänger: In der Caneland-Plattform für Xeon-7400-Prozessoren sind die CPUs noch über klassische FSB an den Chipsatz angebunden. Der Chipsatz steuert zudem den Speicher an. (Quelle: Intel)

3.4.2 RAS-Features auf RISC-Niveau

Mit dem Nehalem EX will Intel erstmals die RAS-Features von RISC-Systemen bei x86-Servern anbieten. Möglich machen soll dies das neue Feature „MCA Recovery“ des Nehalem EX. Mit der Machine Check Architecture (MCA) sollen Fehler bei CPU, Speicher und I/O entdeckt und korrigiert werden. Defekte bei diesen Komponenten sollen den Betrieb des Servers nicht stören.

Das Feature „MCA Recovery“ muss von den Betriebssystemen unterstützt werden. Eine Unterstützung wird von den Anbietern entsprechender Enterprise-Betriebssysteme bereits angekündigt. Microsoft unterstützt MCA Recovery mit dem kommenden Windows Server 2008 R2, VMware will künftige Versionen von vSphere anpassen, Novell bereitst sein SUSE Linux Enterprise auf MCA Recovery vor und Red Hat arbeitet ebenfalls an einer entsprechenden Unterstützung.



RISC-Angriff: Mit dem neuem Feature „MCA Recovery“ soll der Nehalem EX im x86-Segment erstmals die RAS-Fähigkeit von RISC-Systemen bieten. (Quelle: Intel)

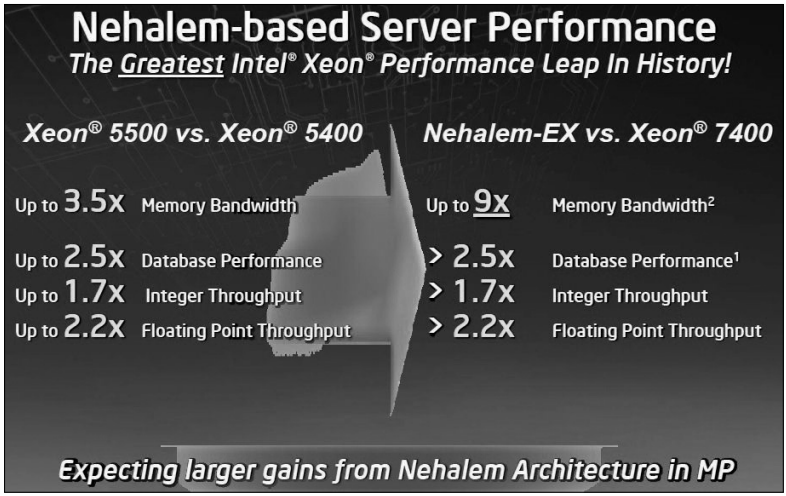
Mit den Hochverfügbarkeits-Features sowie der hohen Skalierfähigkeit des Nehalem EX macht sich Intel zusätzliche interne Konkurrenz zum Itanium 2. Hier pochte Intel bisher stets auf die speziellen RAS-Features für den sicheren Betrieb von Mission-Critical-Workloads. Der Itanium sei laut Intel weiterhin die „ideale Lösung“ für System mit mehr als acht Prozessoren und höchstem Speicherbedarf.

Den Starttermin des lange erwarteten Itanium-2-Nachfolgers „Tukwilla“ verschob Intel kürzlich ein weiteres mal. Der zuletzt Mitte 2009 avisierte Launch-Termin wurde nun auf das erste Quartal 2010 verlegt.

3.4.3 Performance-Angaben

Die Integer-Performance des Nehalem-EX-Systems soll gegenüber der Xeon-7400-Plattform um den Faktor 1,7 steigen. Der Durchsatz bei Fließkommaberechnungen erhöht sich laut Intel um den Faktor 2,2. Vier 6-Core-Xeon-X7460 errei-

chen mit der Benchmark-Suite SPEC CPU2006 einen Integer-Durchsatz von 294 Punkten (SPECint_rate_2006). Ein Nehalem-EX-Server mit vier Prozessoren müsste demnach zirka 500 Punkte bei SPECint_rate_2006 schaffen. Damit läge das Nehalem-EX-System auf dem Niveau von 8-Sockel-Servern mit IBMs Power6 (5 GHz Dual-Core).



Performance-Sprünge: Am deutlichsten steigt bei Nehalem-EX-Systemen die Speicherbandbreite. Damit lassen sich auch die speicherintensiven Floating-Point-Berechnungen in der Performance um den Faktor 2,2 erhöhen. (Quelle: Intel)

Bei Floating-Point-Berechnungen erreichen 4-Sockel-Server mit Xeon X7460 bei CPU2006 eine Performance von 156 Punkten (SPECfp_rate_2006). Vier Nehalem EX sollten durch den angegebenen Faktor 2,2 zirka 343 Punkte bei SPECfp_rate_2006 ermöglichen. Dies entspräche in etwa dem Leistungsniveau eines 8-Sockel-Servers mit IBM Power6 (3,5 GHz Dual-Core).

Eine weitere Performance-Angabe von Intel bezieht sich auf das Leistungsvermögen des Nehalem EX bei Datenbanken. Basierend auf einem OLTP-Workload soll der Nehalem EX um den Faktor 2,5 schneller sein als der Xeon 7400.

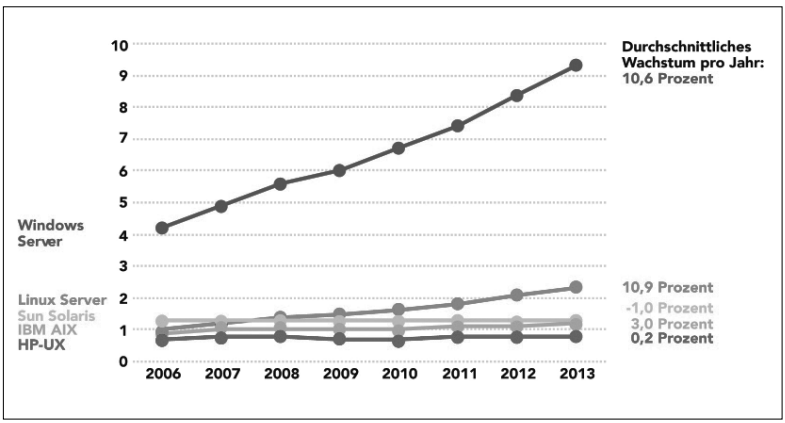
Ausführliche Informationen über die Performance der Multi-Core-Prozessoren von AMD, Intel, IBM, Fujitsu und Sun finden Sie bei TecChannel im Artikel Die schnellsten Prozessoren im Vergleich (Webcode **2016541**). Einen Test von Intels aktueller Xeon-7400-Serie finden Sie im Artikel Test: Erste 6-Core-CPU von Intel (Webcode **1771836**). Wie sich die Nehalem-basierende Xeon-5500-Serie für 2-Sockel-Systeme gegen AMDs Opteron schlägt, zeigt der Artikel CPU-Test: AMD 6-Core-Opteron 2435 und 8435 (Webcode **2019333**).

Christian Vilsbeck

3.5 Standard-x86-Server vs. RISC-Unix-Systeme

Klassische RISC-Unix-Systeme müssen sich im Data Center immer mehr gegen Standard-Server mit x86-Architekturen von AMD oder Intel behaupten. Neben hoher Performance und zunehmenden RAS-Features punkten die x86-Server mit geringeren Kosten und höherer Flexibilität.

Aktuelle Standard-x86-Server verfügen über immer mehr Prozessorleistung bei geringerer Leistungsaufnahme (Webcode **2019333**). So ist es kaum verwunderlich, dass diese "herkömmliche" x86-Server für Rechenzentren immer Interessanter werden. Diesen Trend untermauert auch die Entwicklung der weltweiten Umsätze mit Server-Betriebssystemen. Nach Analysen der Marktforscher von Gartner stagniert der Umsatz mit Unix-Systemen nahezu. In einigen Bereichen sehen die Experten sogar rückläufige Tendenzen, trotz langfristigen Lizenz-, Support- und Wartungsverträgen. Dagegen entwickeln sich Server-Betriebssysteme basierend auf x86-Prozessor-Architektur (Webcode **2019222**) wie Linux- oder Windows prächtig. In diesem Bereich sind zweistellige Wachstumsraten keine Seltenheit und die Marktbeobachter prognostizieren weiterhin eine positive Entwicklung in diesem Segment. So rechnen die Gartner-Analysten bis 2013 für Windows- und Linux-Betriebssysteme mit einem durchschnittlichen jährlichen Umsatzplus von mehr als 10 Prozent. Dagegen muss sich HP-UX (www.hp.com) mit einem Wachstum von 0,2 Prozent begnügen und Sun Solaris rutscht sogar in leicht negative Erwartungen. Einzig IBM (www.ibm.de) mit der Unix-Variante AIX, das auf den selbst entwickelten Power-Prozessoren läuft, verspricht ein mittleres Wachstum von zirka drei Prozent.



Zukunftsaussichten: Während die Umsätze mit Unix-Betriebssystemen nahezu stagnieren, glänzen Windows und Linux auf x86-Servern mit zweistelligen Zuwachsraten. (Quelle: Gartner)

Ebenfalls eine ähnliche Tendenz zeichnet sich im Bereich der Server-Systeme (Hardware und Betriebssystem) ab. In diesem Segment sagen die Gartner-Experten (www.gartner.com) im Zeitraum bis 2014 für alle weltweit verkauften Unix-Server ein mittleres Umsatzminus von etwa 0,3 Prozent pro Jahr voraus. Dagegen können Linux- und Windows-Computer mit einem Umsatzzuwachs von 1,5 beziehungsweise 0,7 Prozent rechnen. Ohne den konjunkturellen Abschwung durch die Wirtschaftskrise 2008/2009, unter dem die x86-Server-Systeme laut den Experten außerordentlich leiden, würden die Zahlen weit aus positiver für die Entwicklung der Standard-Serversysteme ausfallen.

3.5.1 Warum Unternehmen Standard-Server nutzen

Der Aufstieg der x86-Server hat vielfältige Gründe. „Die meisten Unternehmen wollen damit schlicht und ergreifend Kosten sparen", beobachtet Gartner-Analyst Andrew Butler. Dabei hätten sie nicht nur die Anschaffungskosten im Auge, sondern beispielsweise auch die immer wiederkehrenden Wartungsaufwendungen. Michael Homborg, Marketing-Manager bei Fujitsu-Siemens Computers (seit 1. April Fujitsu Technology Solutions), bestätigt diese Einschätzung. Schon seit längerem verzeichne der Hersteller eine stark wachsende Nachfrage nach x86-Systemen. Vor allem Kostenvorteile spielten dabei eine entscheidende Rolle. Homborg: „Das geht jetzt in der Krise erst richtig los."

Standard-Rack-Server: Klassische 86-Server-Systeme dringen in immer anspruchsvollere Anwendungsbereiche vor. (Quelle: Dell)

Auch für IBM ist das x86-Segment trotz der margenstärkeren Unix-Server und Mainframes ein wichtiger Markt geworden, erläutert Ingolf Wittmann, Sales Manager in der Systems & Technology Group. Erst kürzlich hat die deutsche Tochter des IT-Konzerns eine eigene Vertriebsmannschaft für x86-Server aufgestellt. Konkurrent Dell (www.dell.de) buhlt unterdessen mit speziellen Dienstleistungen und Software-Tools um Kunden, „die von einer proprietären Server-Architektur auf eine offene, flexible und standardbasierte Plattform migrieren möchten". Vor allem die angeschlagene Sun Microsystems (www.sun.com), die von Oracle übernommen werden soll, haben die Texaner dabei im Visier.

3.5.2 Technische Gründe für x86-Server

Neben Preisvorteilen spricht das breite Angebot an Servern unterschiedlichster Leistungsklassen für die x86-Plattform. Aufgrund der standardisierten Architektur können Unternehmen ohne größeren Aufwand den Lieferanten wechseln und die Abhängigkeit von einem Hersteller verringern. Doch es gibt auch technische Gründe für das x86-Konzept. Für Butler heißt das schlagende Argument Softwarekompatibilität: Fast alle für die Plattform entwickelten Anwendungen laufen unverändert auf x86-Servern sämtlicher Hersteller, ganz im Gegensatz zu RISC-Unix-Systemen, auf denen Applikationen in der Regel auf bestimmte Kombinationen aus Prozessoren und Betriebssystemen wie beispielsweise Suns Sparc-CPUs (Webcode **451827**) und das Unix-Derivat Solaris zugeschnitten sind.

Immer weniger Anwendungen würden zudem für sehr große Server geschrieben, berichtet der Analyst. So lege etwa Oracle (www.oracle.de) seine Software zunehmend auf mehrere kleine Rechnerknoten aus. Alle Trends in der Softwareentwicklung beförderten die so genannte Scale-out-Strategie, die nicht mehr auf leistungsstarke Multiprozessor-Server („Scale-up"), sondern eine Vielzahl einzelner Systeme im Verbund setzt. Diese Art der Skalierung von IT-Ressourcen passe perfekt zu den x86-Rechnern, so Butler. Das prominenteste Einsatzbeispiel liefert Google mit seinen riesigen Server-Farmen, in denen Tausende x86-Rechner zusammengeschaltet sind.

3.5.3 Virtualisierung beflügelt x86-Serversysteme

Zu den wichtigsten Treibern des x86-Marktes gehört der Trend zur Virtualisierung, darin sind sich Experten einig. Bemerkenswert erscheint diese Entwicklung vor allem deshalb, weil die x86-Architektur im Gegensatz zu den mächtigen Konkurrenten aus dem RISC/Unix-Lager zunächst gar nicht für virtualisierte Umgebungen ausgelegt war. Das aber ändert sich derzeit. Die Prozessorhersteller Intel und AMD (Webcode **2019333**) arbeiten mit Hochdruck an einer verbesserten Unterstützung von Virtualisierungstechniken. Moderne Chipsets und CPUs entlasten beispielsweise die ressourcenhungrigen Hypervisor von VMware (www.vmware.de), Citrix (www.citrix.de) oder Microsoft (www.microsoft.de) von Routineaufgaben und sorgen für eine deutlich höhere Verarbeitungsleistung in virtualisierten Server-Umgebungen. Mit Hilfe von Virtualisierungstechniken können Unternehmen mehrere dezentrale Server jetzt auch auf leistungsstarke x86-Server konsolidieren. Diese Option war lange RISC-Unix- oder Mainframe-Plattformen vorbehalten, die dazu ausgereifte Techniken anboten. Die oberbayerische Alphaform AG (www.alphaform100.de) beispielsweise, ein Komplettanbieter im Bereich Rapid Prototyping und Kleinserien, konsolidierte 14 dezentrale x86-Server auf vier leistungsstärkere SunFire Server mit jeweils zwei Opteron-CPUs von AMD. Sowohl Server- als auch Speichersysteme arbeiten virtualisiert unter dem ESX-Server der EMC-Tochter VMware. Der Energiebedarf des Rechenzentrums sank nach der

Umstellung um 39 Prozent, zugleich benötigt das Unternehmen 60 Prozent weniger Platz für die zentralen Systeme. „Für die x86-Architektur sprach eindeutig der Preis", erläutert IT-Leiter Kai Fahr. Klassische RISC-Unix-Server, wie sie gerade in konsolidierten Umgebungen häufig genutzt werden, kamen für ihn nicht in Frage.

In ganz anderen Dimensionen dachten die IT-Verantwortlichen des Prozesstechnikherstellers Endress+Hauser (www.endress.de). Sie ersetzten rund 250 Dell-Server durch sieben Intel-basierende Highend-Server von IBM. Die Rechner laufen unter Microsoft Windows 2003 und nutzen die Virtualisierungssoftware ESX V3 von VMware. Jeder Server ist mit rund 20 logischen Partitionen konfiguriert. Bei einer Nettoinvestition von 1,2 Millionen Euro ergebe sich ein jährliches Sparpotenzial von 1,4 Millionen Euro, berichten die Verantwortlichen. Das eingesetzte Kapital rentiere sich damit bereits nach zehn Monaten.

3.5.4 Blade-System sparen Energie

Am meisten profitiert die x86-Architektur vom Formfaktor der Blade-Systeme, dem derzeit am schnellsten wachsenden Segment im Server-Markt. Gartner berichtet von jährlichen Steigerungsraten von 18 Prozent bezüglich der verkauften Systeme und 16 Prozent gemessen am Umsatz. Unternehmen sähen in den flachen Servern eine Ergänzung zu den bereits vorhandenen Systemen, erklären die Marktforscher das Phänomen. Sie wollten damit insbesondere Platz und Energie sparen. Immer mehr IT-Manager nutzten x86-basierende Blades (Webcode **1783583**) als strategische Plattform im Rechenzentrum.

Dicht gepackt: Mit Blades lassen sich viele Server auf engstem Raum unterbringen. Die Blade-Systeme bieten dabei eine hohe Rechenleistung bei geringem Platz- und Energiebedarf. (Quelle: FTS)

Dazu beigetragen hat auch die stetig zunehmende Leistung der Prozessoren mit mehreren Rechenkernen (Multicore). Intels kürzlich vorgestellte neue Xeon-Architektur „Nehalem" (Webcode **2019222**) etwa bringt den Rechnern einen weiteren Schub. „Heute erhältliche x86-Server wären im Jahr 2000 noch als Highend-

Systeme für den SAP-Betrieb klassifiziert worden", vergleicht IBM-Manager Wittmann. Dementsprechend drängen x86-Systeme in Anwendungsbereiche vor, die lange Zeit eine Domäne von RISC-Unix-Plattformen oder Großrechnern waren. Wittmann zählt dazu unter anderem ERP-Systeme (Webcode **1779466**), Datenbanken, Business Intelligence und Data Warehousing.

3.5.5 Sieben Aspekte, die für x86-Server sprechen

1. Kostenvorteile durch standardisierte Technik und hohe Stückzahlen.
2. Große Auswahl relevanter Produkte.
3. Problemloser Wechsel des Lieferanten.
4. Einfache Skalierung durch Hinzufügen weiterer Rechner.
5. Softwarekompatibilität: Anwendungen laufen unverändert auf Rechnern unterschiedlicher Hersteller.
6. Zunehmende Unterstützung von Virtualisierungstechniken in Prozessoren und Chipsets.
7. Große Stückzahlen ermöglichen hohe Entwicklungsgeschwindigkeit der CPU-Hersteller.

3.5.6 Zukunftsperspektiven von RISC-Unix-Systemen

An ein baldiges Aussterben der klassischen Rechenboliden glaubt trotzdem kaum ein Experte. „In Sachen Verwaltbarkeit haben die großen Server noch immer die Nase vorn", urteilt Gartner-Mann Butler. Bis die x86-Protagonisten den Vorsprung aufgeholt hätten, werde noch einige Zeit vergehen. Zudem bräuchten klassische RISC/Unix-Nutzer lange, bis sie eine in ihren Augen riskante Migration auf eine andere Plattform wagen. Ganz anders verhielten sich Startup-Unternehmen. Die meisten Cloud-Provider etwa würden x86-Server bevorzugen.

In der Zukunft erwartet Gartner (www.gartner.com) zwei unterschiedliche Typen von Rechenzentren: zum einen „Legacy Data Center", die wegen vorhandener Altsysteme oft gar keine Chance hätten, auf andere Plattformen zu wechseln. Zum anderen so genannte New Generation Data Center, die häufig auf der grünen Wiese entständen und sich nicht um Altanwendungen kümmern müssten. Sie setzten in der Regel strategisch auf x86-Systeme unter Windows oder Linux. Butler: „RISC-Unix wird dort nur noch genutzt, wenn es unbedingt nötig ist.".

Wolfgang Herrmann

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

3.6 Datenaustausch zwischen Linux, Windows 7 und Server 2008 R2

Die neue Generation der Windows-Betriebssysteme steht vor der Tür. Die Zusammenarbeit mit Linux-Systemen ist dabei wichtiger denn je. TecChannel hat Windows 7 und Server 2008 R2 in heterogenen Umgebungen getestet.

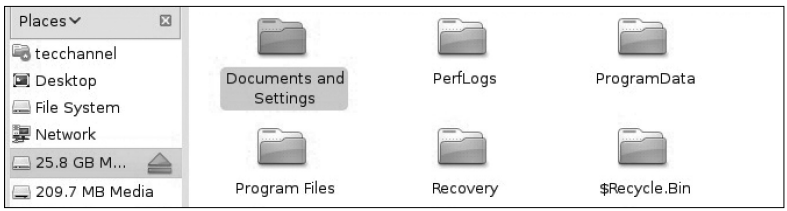
In Firmennetzwerken ist ein reibungsloser Datenaustausch über das Netzwerk heutzutage essentiell. Daten fließen dabei oft heterogen, also zwischen Windows-Systemen und Linux-Installationen. Microsofts neue Betriebssysteme, Windows 7 für Clients und Server 2008 R2, sind dabei, sich als neue Komponenten in diese Netze zu integrieren. In unserem Workshop zeigen wir Ihnen, wie Sie Ihre Linux-Landschaft zur Kooperation mit den neuen Windows-Varianten bringen.

In heterogenen Netzen ist neben NFS oftmals Samba im Einsatz. Daher legen wir Wert darauf, dass sowohl Linux als auch Windows mit beiden Formaten zurechtkommen. Abschließend beschäftigt sich der Artikel mit dem gesicherten Zugriff auf Server mittels SSH. Bevor wir allerdings auf den Server zu sprechen kommen, widmen wir uns einem lokalen Problem. Denn wer Windows und Linux im Desktop im Dual-Boot-Modus einsetzt, der hat oft ein Problem: Gerade benötigte Daten liegen auf der Partition des anderen Betriebssystems. Wir zeigen Ihnen, wie Sie von Linux aus auf NTFS-Dateisysteme zugreifen können und wie Sie unter Windows an Linux-Dateien gelangen.

Für unsere Testumgebung haben wir uns für Kubuntu und Ubuntu Intrepid 8.10 als Linux-Desktops entschieden. Alle Systeme liefen unter VMware 6.5 – gehostet von Ubuntu 8.04 – auf einem Dual-Core-System mit 4 GByte RAM. Alle virtuellen Maschinen wurden mit zwei virtuellen Prozessoren betrieben.

3.6.1 Mit Linux auf Windows-7-Partitionen zugreifen

Hier gibt es außer „Es funktioniert" wenig zu berichten. Unser Ubuntu-Testsystem konnte die NTFS-Partition von Windows 7 Beta dank NTFS-3G einwandfrei einbinden. Auch Lese- und Schreibzugriffe waren problemlos möglich. Ein einfacher Klick auf die Windows-Partition reichte, um vollen Zugriff zu erlangen.



Vollzugriff: Von Linux auf NTFS-Partitionen zugreifen klappt ohne Probleme.

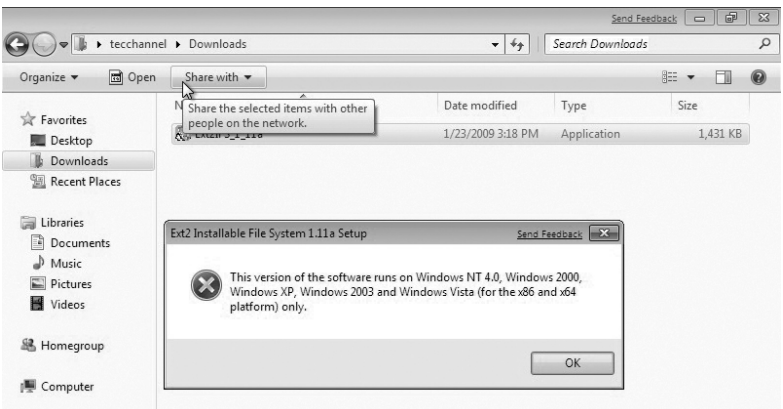
Einzig wenn das Journal von NTFS nicht leer ist, können Schwierigkeiten auftreten. Dies ist jedoch eine Schutzmaßnahme von NTFS-3G, etwa wenn Windows nicht sauber heruntergefahren wurde. Sollte dies der Fall sein, reicht es, Windows 7 einmal zu starten und herunterzufahren. Danach sollte es in der Regel wieder funktionieren. Das war allerdings auch zu erwarten, da sich an NTFS im Gegensatz zu Vista nichts geändert hat.

3.6.2 Umkehrschwung: Windows 7 und Linux-Partitionen

Ein Zugriff von Windows auf Linux-Dateisysteme ist deutlich komplizierter als der Zugriff auf NTFS-Dateisysteme. Dennoch gibt es einige Programme, die dies ermöglichen – zumindest teilweise. Dabei lassen sich Reiser-Dateisysteme – wenn überhaupt – nur lesend einbinden. Bei den dafür entwickelten Werkzeugen hat sich in jüngster Zeit auch nicht mehr viel getan. Das könnte unter anderem daran liegen, dass alle großen Linux-Distributionen nunmehr wieder auf das Dateisystem ext3 oder in Kürze ext4 setzen.

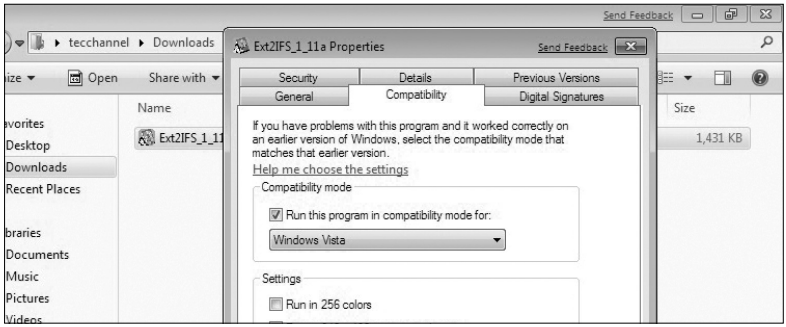
Ext2IFS – Hindernisparcour und kein Erfolg

Ext2IFS (www.fs-driver.org) dürfte eines der bekanntesten Werkzeuge sein, um Zugriff auf ext2 zu erlangen. Das Programm kann ebenfalls mit ext3 umgehen. Hierfür unterliegt es allerdings einigen Einschränkungen. Der Entwickler spricht derzeit von einer Kompatibilität mit Windows NT4.0/2000/XP/2003/Vista/2008. Ein Installationsversuch unter Windows 7 schlägt zunächst auch fehl.



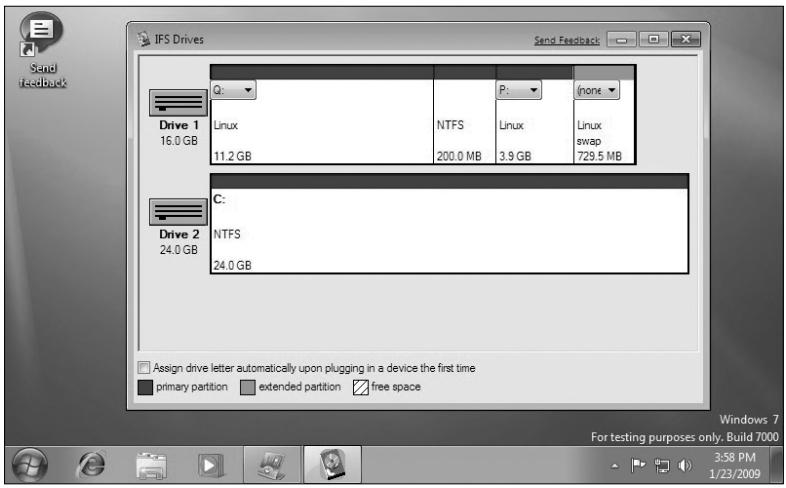
Nicht kompatibel: Ext2IFS verweigert eine Installation unter Windows 7.

Setzt man es allerdings in den Kompatibilitäts-Modus für Windows Vista, erscheint die Fehlermeldung nicht mehr.



Kompatibel zu Vista: Mit diesen Einstellungen lässt sich die Fehlermeldung unterbinden.

Während der Installation können Sie wählen, ob Sie die Software lediglich im "Nur Lesen"-Modus verwenden wollen. Sie können zwar einen Schreibzugriff ermöglichen, allerdings sollten Sie hier aufpassen, wenn Sie Änderungen vornehmen. Dieses Risiko ist nicht unbedingt notwendig, da Linux, wie bereits erwähnt, Vollzugriff auf NTFS hat. Im Test sind wir dieses Risiko nicht eingegangen. Nach der Installation können Sie sofort den Linux-Dateisystemen einen Laufwerksbuchstaben zuweisen.



Zugewiesen: Die Software erkennt die Linux-Laufwerke ohne Probleme.

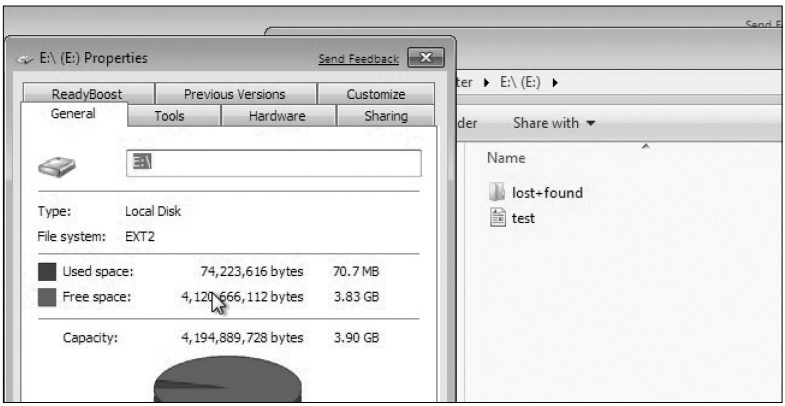
Die neu eingebundenen Laufwerke P (ext2) und Q (ext3) erscheinen anschließend im Explorer. Allerdings gibt es Fehler beim Zugriff. Ein Doppelklick auf die Laufwerke teilt mit, dass man die Laufwerke formatieren müsse, um darauf zugreifen

zu können. Das wollen wir natürlich nicht. Weiteres Herumspielen mit der Dateizugriffskontrolle brachte ebenfalls keine positiven Ergebnisse. Der Versuch mit Ext2IFS ist also gescheitert.

Ext2fsd – Absturzgefahr

Ein Einsatz von Ext2fsd (http://ext2fsd.sourceforge.net) sah zunächst vielversprechender aus. Das Programm ließ sich installieren. Nach der permanenten Zuweisung der ext-Laufwerke forderte Ext2fsd jedoch einen Neustart, der in einem Systemabsturz endete. Bei einem weiteren Startversuch sah es besser aus, und es wurde sogar der freie Speicherplatz der Linux-Laufwerke angezeigt. Das ext2-System funktionierte einwandfrei.

Ein Versuch, auf ext3 zuzugreifen, endete ebenfalls wieder in einem Crash. Der war anscheinend zu viel für die Beta-Version des neusten Microsoft-Betriebssystems. Versuchte Neustarts endeten entweder in einem BSOD oder führten zu Fehlern im Bootvorgang.



Teilerfolg: Mit Ext2fsd funktioniert zumindest das Einbinden von ext2-Dateisystemen.

Nach einer Neuinstallation versuchten wir das ganze Spiel noch einmal, diesmallerdings nur mit einem ext2-Dateisystem. Diesmal hatten wir Erfolg: Das Linux-FS ließ sich lesend und schreibend einbinden. Einen Komplettabsturz gab es nicht mehr. Für den Einsatz mit ext3 eignet sich das Programm aber nicht.

3.6.3 Zwischenfazit und eine Web-Alternative

Mit Linux lässt sich in gewohnter Manier auf das NTFS-Dateisystem zugreifen. Dies hat sich auch mit Windows 7 Beta nicht geändert. Der Reverse-Versuch fiel eher kläglich aus. Lediglich Ext2fsd konnte einen Teilerfolg verbuchen. Damit las-

sen sich zumindest ext2-Dateisysteme einbinden. TecChannel verwendete noch ein drittes Tool: explore2fs (www.chrysocome.net/explore2fs).

Dieser Versuch endete nach wenigen Klicks im Mount-Manager der Software ebenfalls in einem Blue Screen. Da die meisten Linux-Systeme mit ext3 installiert sein dürften, ist ein Datenaustausch zwischen Windows 7 und Linux auf Dateisystemebene somit nicht ohne Weiteres möglich. Derzeit ist also keines der Programme uneingeschränkt zu empfehlen. Die Entwickler der freien Software brauchen wohl noch Zeit, um ihre Programme entsprechend an das neue Betriebssystem anzupassen. Problemloser geht der Austausch von Dateien beispielsweise mit Web-Synchronisierungs-Tools wie Dropbox vonstatten. Der Client lässt sich unter Linux, Windows und Mac OS X installieren. Legt man anschließend Dateien in der Dropbox (www.getdropbox.com) ab, kann man von anderen Systemen aus darauf zugreifen. Allerdings eignet sich die Lösung natürlich nur dann, wenn Sie vorher wissen, welche Daten Sie benötigen.

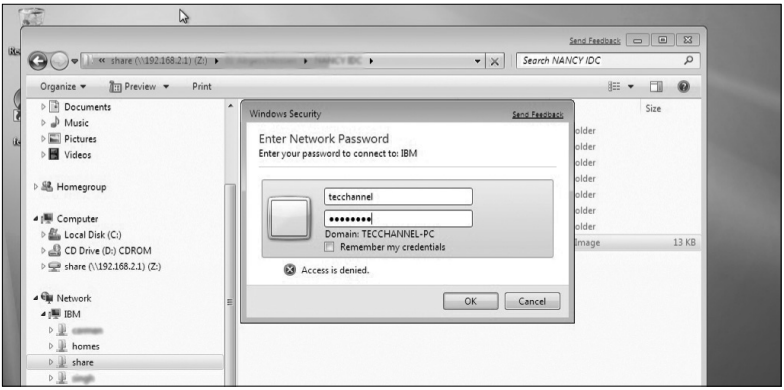
3.6.4 Datenaustausch zwischen Linux und Windows 7 über das Netzwerk

Wer von der lokalen Festplatte ins Netzwerk geht, stößt immer häufiger auf heterogene Umgebungen, in denen Linux-Server fleißig Daten mit der Windows-Welt austauschen. Windows 7 und Windows Server 2008 R2 werden mit dieser Realität klar kommenmüssen, wenn sie sich im Business-Umfeld durchsetzen wollen.

3.6.5 Linux als Samba-Server

Als Linux-Server haben wir uns für Ubuntu 8.04 LTS „Hardy Heron“ (Webcode **1756639**) entschieden. Dies hat einen einfachen Grund: Für die Server-Variante des Betriebssystems gibt es noch vier Jahre Unterstützung – sprich bis 2013. Wichtig ist, dass die Samba-Software einen möglichst aktuellen Stand hat. Denn wie Windows Vista benötigt auch die Beta von Windows 7 eine Samba ab Version 3.0.10. Im Test hinterlässt Microsofts neues Desktop-Betriebssystem einen positiven Eindruck. Der Datenaustausch funktioniert exakt so, wie er soll. Über die Netzwerkschaltfläche sucht man sich den entsprechenden Rechner und klickt ihn an. Sollten Anwendername und Passwort nicht mit dem Windows-7-Rechner übereinstimmen, fordert das System den User auf, die richtigen Kontodaten zu verwenden. Danach können Sie wie gewohnt auf Ihre Daten zugreifen.

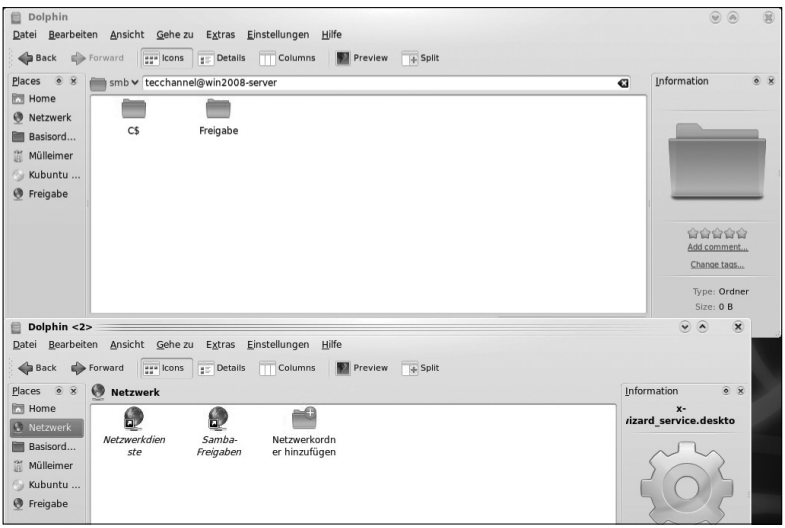
Ein kleines Problem trat dann allerdings doch auch: In der Standard-Einstellung gibt der Samba-Dienst auch Drucker frei. Darin ist auch ein PDF-Drucker enthalten. Will man diese Freigabe unter Windows 7 verbinden, beschwert sich das System über einen fehlenden Druckertreiber. Zur Umgehung des Problems reicht es, einen passenden PostScript-Treiber zu verwenden. Die Linux-Gegenstelle verwendet Ghostscript und erzeugt damit die PDFs.



Klappt: Eine Verbindung von einem Windows-7-Client zu einem Linux-Server ist problemlos möglich.

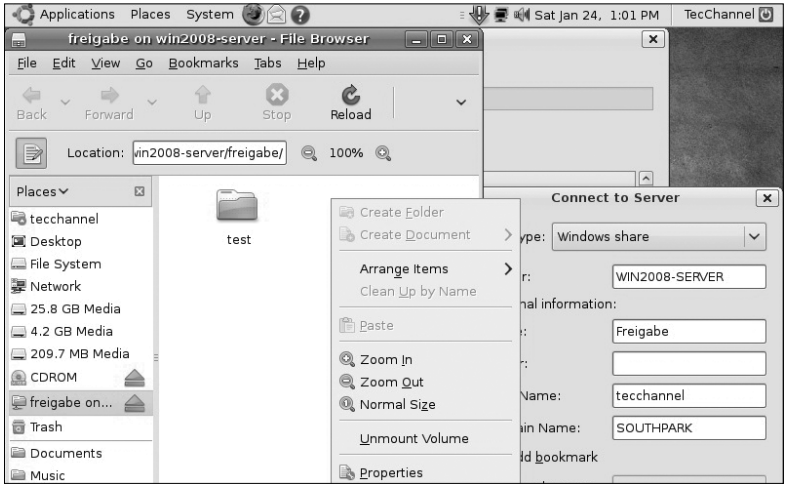
3.6.6 Linux als Samba-Client an Server 2008 R2

Mit Windows 7 auf einen Samba-Server zuzugreifen klappt. Allerdings wollten wir auch wissen, ob ein Linux-Client auf einen Windows Server 2008 R2 zugreifen kann. In erster Linie interessiert uns dabei der simple Dateiaustausch. Dazu haben wir ein einfaches Benutzerkonto erstellt und einen Ordner freigegeben. Im Test erkannten wir dann schnell die Einschränkungen.



Note „Gut“: KDE 4.1 kann mit den Freigaben des Windows Server 2008 R2 gut umgehen.

Sowohl Kubuntu 8.10 als auch Ubuntu 8.10 bringen die notwendigen Tools in KDE (www.kde.org) beziehungsweise GNOME (www.gnome.org) mit sich, um sich zu dem Windows Server zu verbinden. Allerdings funktionieren nicht beide gleich gut. KDE 4.10 schlägt sich im Vergleich eindeutig besser. Hier findet man via „Netzwerk – Samba-Freigaben“ den entsprechenden Rechner. Bei einem Klick auf diesen kommt eine Passwort-Abfrage, und man sieht die entsprechende Freigabe. Mit dieser lässt sich nun ganz normal arbeiten. Sie können Dateien und Ordner löschen, anlegen und so weiter.



Note „Befriedigend“: GNOME weist im Zusammenspiel mit Windows-Freigaben Eigenheiten auf.

Durchstreift man mit GNOME das Netzwerk, findet man den Windows-Server ebenso. Ein Doppelklick auf ihn endet jedoch in einer leeren Suchmaske. Der Dateimanager Nautilus will weder ein Passwort haben, noch zeigt er die Freigabe an. Erst die Verwendung der Schaltfläche “Zu Server verbinden” führte zum gewünschten Ergebnis. Erster Nachteil ist, dass Sie wissen müssen, wie die Freigabe heißt. Zweite Eigenheit: Sie können direkt in der Freigabe weder einen Ordner noch eine Datei erstellen. Ebenso funktionierte rech „kopieren – einfügen“ mit der rechten Maustaste nicht. Ziehen Sie allerdings mit der linken Maustaste eine Datei in den Hauptordner der Freigabe, wird die Datei angelegt. Das Speichern einer Datei aus OpenOffice in den Hauptordner der Freigabe funktionierte ebenfalls – aber erst beim zweiten Versuch. In KDE klappte alles einwandfrei.

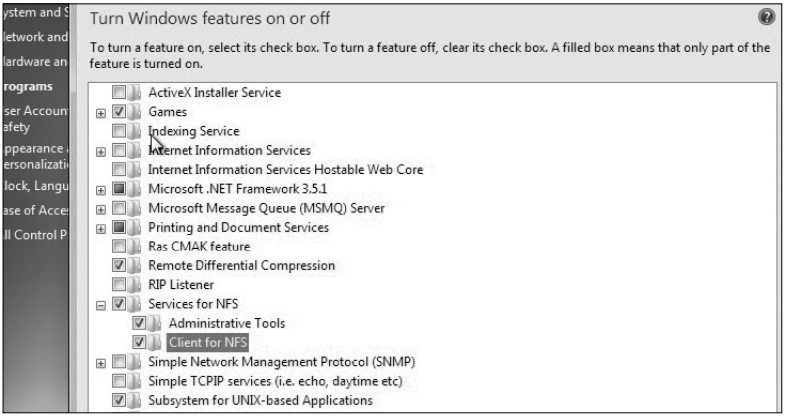
Zuverlässig funktioniert die Kommandozeile:

```
mount -t smbfs -o username=[Windows-Anwender],
➥ password=[Passwort] //[IP-Adresse Windows-Server]/
➥ [Freigabe]/ /[Einbindepunkt]
```

Binden Sie auf diese Weise eine Windows-Freigabe ein, arbeitet auch der GNOME-Dateimanager ohne Probleme damit. Sollten Sie die IP-Adresse des Windows-Rechners nicht wissen, hilft: `nmblookup [Name Windows-Rechner]`. Falls Sie den Namen der Freigabe herausfinden wollen, könnte das Programm smbtree hilfreich sein. Mehr dazu erfahren Sie mit `man smbtree`.

3.6.7 Mit Windows auf Linux-NFS-Server zugreifen

Für ältere Windows-Installationen gibt es die Windows Services for UNIX 3.5 (http://technet.microsoft.com/en-us/interopmigration/bb380242.aspx), die unter anderem einen NFS-Client bereitstellten. Mit dem Erscheinen von Windows Vista wurde das Paket in Services for Unix umbenannt. Die notwendige NFS-Software ist aber nur für Business- oder Ultimate-Varianten verfügbar. Die Beta von Windows 7 entspricht der Ultimate-Version, das Paket ist also mit an Bord. Sie müssen es allerdings erst aktivieren.



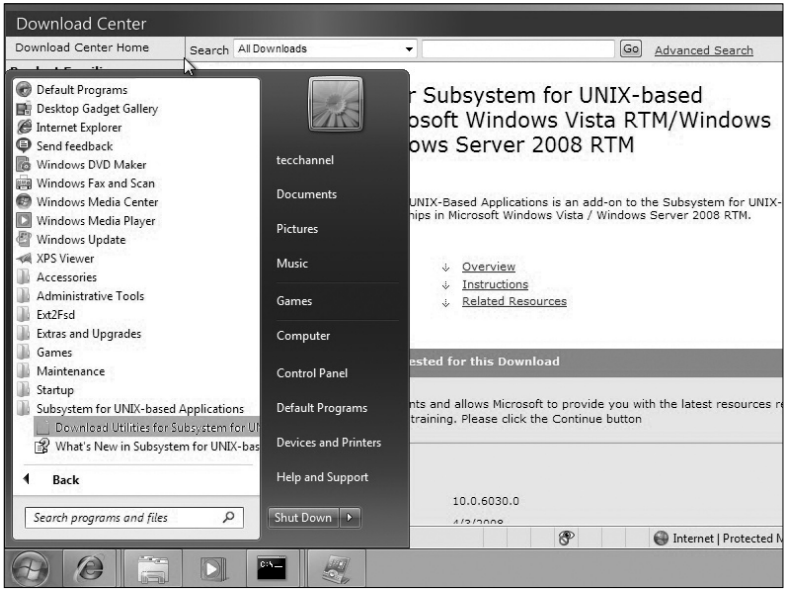
NFS-Client für Windows: Sie müssen die entsprechende Option aktivieren.

Ist dies geschehen, können Sie sich zu NFS-Servern verbinden. Öffnen Sie dazu die Kommandozeile und benutzen den mount-Befehl. Eine Hilfe zu mount bekommen Sie, indem Sie den Befehl ohne weitere Optionen ausführen.

```
mount [Optionen] //[Servername oder IP-Adresse]/[Freigabe]
➥ [Laufwerksbuchstabe]
```

Bei den optionalen Komponenten befinden sich auch die „Services for UNIX“. Nach der Installation finden Sie einen entsprechenden Ordner unter „Alle Programme“. Der Download-Link bringt Sie auf die richtige Seite. Hier können Sie das Subsystem for UNIX-based Applikations (SUA) (http://technet.microsoft.

com/en-us/library/cc779522.aspx) herunterladen. Je nach Architektur ist das Paket zwischen 473 und 484,1 MByte groß. Derzeit steht Windows 7 noch nicht in der Liste der unterstützten Betriebssysteme, aber es funktioniert trotzdem.



Großer Download: Das SUA-Paket ist nicht gerade klein.

3.6.8 Windows Server 2008 R2 als NFS-Server

Windows Server 2008 R2 stellt einen eigenen NFS-Server-Dienst zur Verfügung. Dieser ist per Standard jedoch deaktiviert. Sie müssen die „Dienste für NFS" daher zunächst freischalten.

NFS aktiviert: Zuerst müssen Sie den passenden Dienst in Server 2998 R2 freischalten.

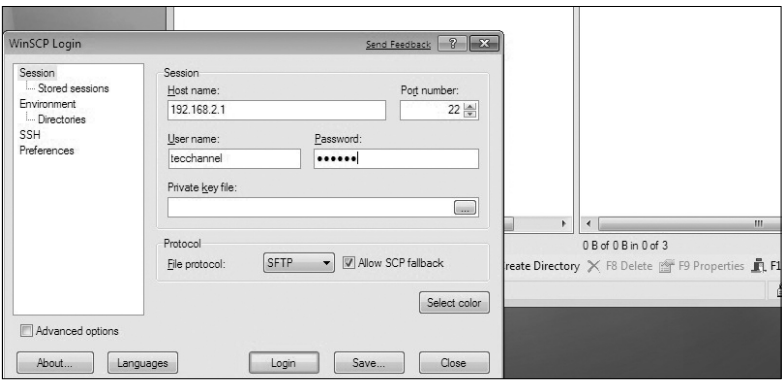
Einen Ordner können Sie nun via Rechtsklick – Eigenschaften – NFS-Freigabe freigeben. Binden Sie diese Freigabe nun unter Linux ein, funktioniert das scheinbar zunächst problemlos.

```
mount [Name Windows Server oder IP-Adresse]:/
➥ [Freigabe] [Mountpunkt]
```

Sobald Sie jedoch auf das Verzeichnis zugreifen wollen, könnten Sie einen Input/Output-Fehler bekommen. Dies ist ein Berechtigungs-Problem. Der berechtigte Anwender und die zugelassene Gruppe unter Linux könnte die Nummer 4294967294 haben. Wenn Windows keine Mapping-Informationen besitzt und Sie als UID/GID -2 ankommen, weist Windows ihnen diese bizarre Berechtigungs-Nummer zu. Sie finden hierzu weitere Informationen im Blog von MSDN „Who's 4294967294" (blogs.msdn.com/sfu/pages/who-s-4294967294.aspx). Abhilfe schafft zum Beispiel der Befehl chown. In unserem Fall gewährte ein `chown tecchannel.tecchannel nfs` Zugriff ohne Fehlermeldung.

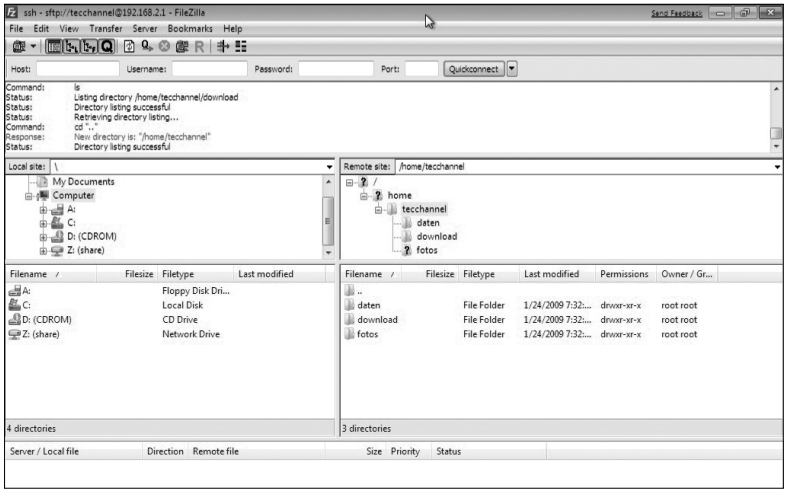
SSH mit Windows 7

Gerade wenn man sein eigenes Netzwerk verlässt, sollten Sie Verbindungen mittels SSH verschlüsseln. Von Windows auf einen OpenSSH-Server zuzugreifen war bereits in der Vergangenheit nicht schwer. Es gibt gute Programme, mit denen ein verschlüsselter Datenaustausch problemlos funktioniert. Simpel, aber übersichtlich und funktionabel ist der SFTP-Client WinSCP (http://winscp.net).



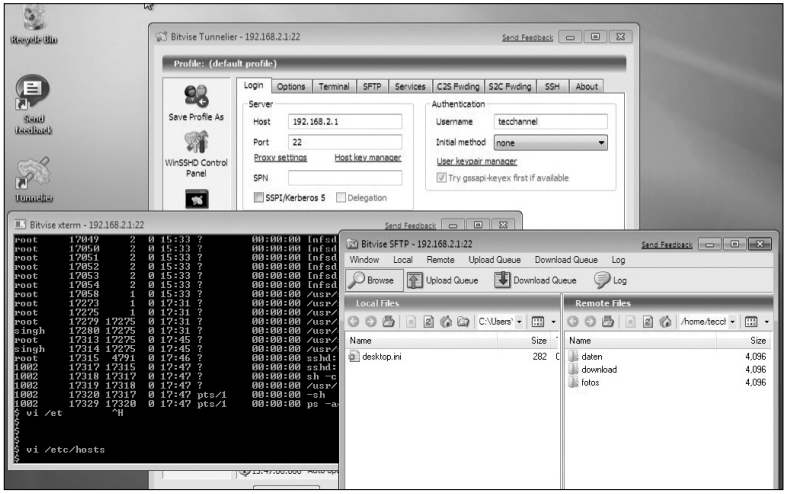
Klein, aber fein: Das Utility WinSCP ist leicht bedienbar und eignet sich hervorragend, um Daten verschlüsselt von einem Linux-OpenSSH-Server abzuholen.

Ein bekannter FTP- und SFTP-Client ist Filezilla (www.filezilla-project.org). Der Transfer-Client ist aufwendiger gestaltet als WinSCP, dafür ein wenig komfortabler in der Handhabung. Filezilla stellt neben SFTP auch „FTP over implicit TLS/SSL" und „FTP over explicit TLS/SSL" zur Verfügung.



Alter Bekannter: Filezilla hat sich zu einem der beliebtesten FTP- und SFTP-Clients gemausert.

Ein weiterer sehr interessanter Vertreter dieses Genres ist Tunnelier (www.bitvise.com/tunnelier) von Bitvise. Für den privaten Gebrauch ist die Software kostenlos. Sie öffnet beim Einloggen nicht nur einen grafischen Dateimanager, sondern bietet auch ein Terminal-Fenster mit an. Somit können Sie auf der Kommandozeile des entfernten Systems arbeiten.



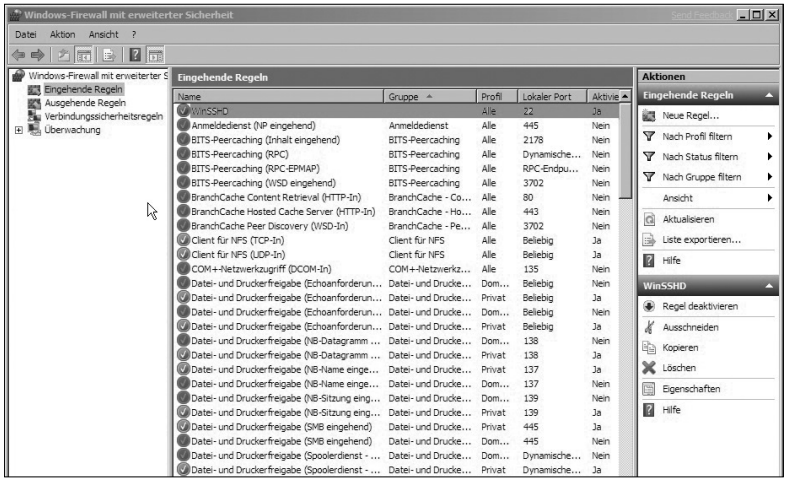
Mehr als ein Dateimanager: Tunnelier stellt auch ein Terminal-Fenster zur Verfügung.

3.6.9 Mit Windows Server 2008 SSH-Dienste zur Verfügung stellen

Auch unter Windows haben Sie die Möglichkeit, Daten verschlüsselt über das SSH-Protokoll anzubieten. Am einfachsten funktioniert das mit der Software WinSSHD (www.bitvise.com/winsshd) von Bitvise. Wie beim bereits erwähnten Tunnelier ist auch hier ein privater Einsatz kostenlos. Die nicht-kommerzielle Version bietet allerdings einige Einschränkungen. Die Installation ist ganz nach Windows-Manier denkbar einfach. Nach der Installation können Sie das Control Panel öffnen, den SSH-Daemon konfigurieren und starten. Für einen kurzen Test reichen die Standard-Einstellungen.

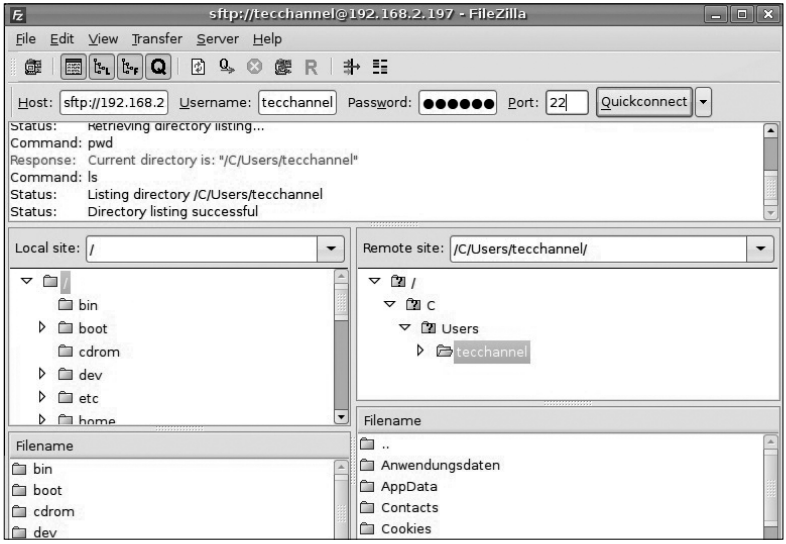
SSH-Daemon für Windows: Die kostenlose Software ist unter Windows schnell und unkompliziert installiert. Mit nur einem Mausklick läuft der Daemon im Hintergrund.

Allerdings bekamen wir bei einer Testverbindung zunächst ein Timeout. Daran ist allerdings nicht WinSSHD schuld, sondern die Windows-Firewall. Diese hat keinen Eintrag für eingehende Verbindungen über Port 22. Unter den erweiterten Einstellungen der Windows-Firewall finden Sie den Punkt „Eingehende Regeln". Dort legen Sie einfach eine neue Regel an und wählen als Regeltyp „Port" aus. Im nächsten Schritt geben Sie als TCP-Port unter „Bestimmte lokale Port" 22 an. Unter „Aktion" müssen Sie diesen Schritt nun zulassen. Im vorletzten Schritt können Sie bestimmen, in welchem Umfang die Regel Anwendung findet: Domäne, Privat oder Öffentlich. Nun brauchen Sie der Regel nur noch einen Namen und optional eine Beschreibung geben.



Einlass bitte!: Sollten Sie die Standardeinstellungen von WinSSHD nicht verändern wollen, müssen Sie für den Datenaustausch den Port 22 der Windows-Firewall öffnen.

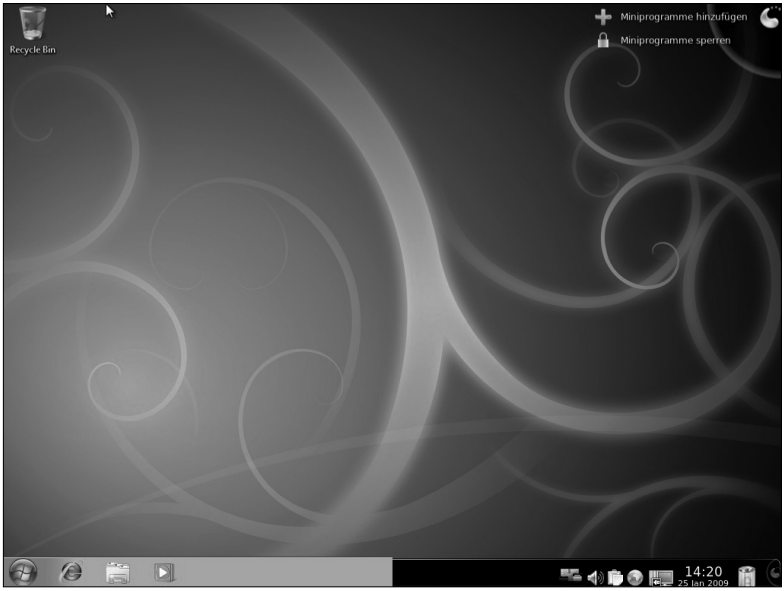
Nachdem Sie die Firewall korrekt konfiguriert haben, können Sie zum Beispiel mit jedem beliebigen SFTP-Client via SSH auf den Windows-Server zugreifen.



Linux nach Windows: Ist alles ordnungsgemäß eingerichtet, können Sie von Linux via SSH-Verbindung leicht Daten des Windows-Servers abholen.

3.6.10 Fazit

Die Koexistenz zwischen Linux und Windows 7 Beta beziehungsweise Windows Server 2008 R2 hat sich gegenüber Vista oder Server 2003 weder verbessert noch verschlechtert. Windows als Client und Linux als Server funktioniert immer noch besser als der andere Weg. Desktop-Linuxer haben aber normalerweise ein dickes Fell und lassen sich von Nichtigkeiten wie fehlenden Treibern oder zusätzlicher Software nicht entmutigen.



Linows oder Windux? Die Kombination unterschiedlicher Systeme wäre wohl die Wunschvorstellung – sie wird aber in absehbarer Zeit nicht in Erfüllung gehen.

Als Quintessenz lässt sich aus diesem Test ziehen, dass Linux und die nächste Generation von Windows durchaus harmonisch miteinander umgehen können. Dem Einsatz in heterogenen Umgebungen steht also wenig entgegen.

Jürgen Donauer

Jürgen Donauer war als Systemadministrator zunächst für Informix und später IBM tätig. Dann verschlug es ihn in das Rechenzentrum von Media-Saturn. Dort kümmerte er sich mitunter um die Webserver, Datenbankanbindung und den Online-Shop. Anschließend war er als Redakteur im Bereich Linux für TecChannel tätig. Derzeit arbeite Jürgen Donauer als freier Autor für TecChannel sowie als Tauchlehrer.

4 Schutz für Clients

Die Bedrohung für Client-PCs auf Windows-, Linux- und Mac-Basis durch Viren und Malware nimmt aufgrund immer neuer Schädlingsvarianten stetig zu. Deshalb ist ein gezieltes Abdichten kritischer Angriffspunkte in den Client-Betriebssystemen sowie der Einsatz geeigneter Abwehr-Software wichtig.

4.1 Tipps und Tools für mehr Sicherheit unter Windows

Windows-Plattformen dienen einer Vielzahl von Firmen als Basis sowohl für Clients als auch für Server. Das und der große Marktanteil auch im Privatanwenderbereich macht sie für Angreifer besonders interessant. Daher gilt es für Unternehmen, in Windows-Umgebungen einige Sicherheitsgrundregeln zu beachten. Sie betreffen die Bereiche Clients und Server sowie das Active Directory als grundlegenden Verzeichnisdienst in Windows-Umgebungen. Dieser Ratgeber liefert einen Einblick, wie sich die eigene Windows-Umgebung – fernab von zugekauften Extras – mit bordinternen Mitteln sicherer gestalten lässt.

Um hierfür die Basis zu schaffen, ist, unabhängig von den betrachteten Systemen, zudem auf folgende Aspekte zu achten: das Patch-Management, proaktive Schutzmaßnahmen, Schulung und Berechtigung der Benutzer.

4.1.1 Die Verfahren – nur bekannt oder auch gelebt?

Selbst wenn es bereits hinlänglich bekannt ist: Updates sind unbedingt zeitnah, flächendeckend und kontrolliert einzuspielen. Als Grund für das oft wochenlange Aussetzen eines Patchs werden häufig fehlende Ressourcen und die Angst vor Betriebsstörungen angeführt. Dabei tritt oft genau das Gegenteil ein, wie die explosive Verbreitung des Conficker-Wurms deutlich machte: Selbst lange Zeit nach dem Erscheinen des Microsoft-Patchs am 23. Oktober 2008, der die von dem Schädling ausgenutzte Windows-Schwachstelle beheben sollte, waren viele Systeme noch nicht aktualisiert und somit angreifbar. Noch Monate später legte Conficker Unternehmen und Behörden lahm und verursachte hohe Schäden – Microsoft-Emea-Sicherheitschef Roger Halbheer bezeichnete dies als „russisches Roulette mit dem Netzwerk".

Als Beispiel, wie aus Zero-Day-Attacken dann „Three-Month"-Attacken werden, verdeutlicht dieser Fall, wie sehr es beim Kampf gegen Sicherheitslücken auf Tempo ankommt. Unternehmen müssen in diesem Kontext auch auf ein lückenloses Auditing der Systeme achten, um durchgängig aktuelle Patches installiert zu haben. Erreichen lässt sich dies mit Hilfe integrierter Systeme wie den „Microsoft

Windows Server Update Services“ (WSUS) oder dem „Software Update Management“ in Microsofts neuem „System Center Configuration Manager“ (SCCM). Erst wenn alle Systeme auf einem angemessenen Versionsstand sind, kommen proaktive Maßnahmen überhaupt zum Tragen.

Was hier nicht fehlen darf, ist ein Virenschutzkonzept für Clients und Server samt umfassender Strategie sowie eine geeignete technische Umsetzung. So sind Malware-Scanner nur so viel wert wie ihre Signaturen. In Kombination bieten sich weitere proaktive Schutzmaßnahmen an – etwa die Konfiguration und Aktivierung der lokalen Firewall über die „Gruppenrichtlinien“.

4.1.2 Balance zwischen Sicherheit und Benutzbarkeit

Sicherheit ist aber nicht nur ein technisches Problem. Häufig ist es der Mensch, der Angriffen Tür und Tor öffnet. Die Gründe hierfür sind mangelndes Bewusstsein für sicheres Verhalten oder Neugier, nicht selten aber auch die Benutzbarkeit der verwendeten Software. Das beste technische Konzept versagt, wenn der Benutzer die Tragweite seiner Aktionen nicht kennt oder mit allzu restriktiven Regeln nicht umgehen kann (Beispiel: das 30-Zeichen-Passwort).

4.1.3 Beachten Sie das Least-Privilege-Prinzip

Auch geschulte Benutzer brauchen klar definierte Grenzen – schließlich soll Malware die Rechte des Benutzers ausnutzen. Ein Wurm mit administrativen Rechten hat gute Chancen, seiner fragwürdigen Bestimmung nachzugehen. Daher ist stets das Least-Privilege-Prinzip anzuwenden: Jeder Benutzer, jeder Dienst und jedes System erhält demnach nur die Rechte, die zur Erfüllung der jeweiligen Aufgaben absolut erforderlich sind. Hier gilt es, besonders strikt vorzugehen, was eine genaue Kenntnis der Arbeitsabläufe und Systeme voraussetzt. Die Umsetzung des Least-Privilege-Paradigmas gehört zu den besten Methoden, ein grundlegendes Fundament für sichere Systeme zu schaffen – allerdings ist es dazu häufig erforderlich, mit alten Gewohnheiten zu brechen. Auch hier ist die Balance zwischen Sicherheit und Benutzbarkeit wichtig: Vistas lärmende User Account Control (UAC) ist ein Beispiel dafür, wie eine gute Idee ins Gegenteil verkehrt wurde.

4.1.4 Zero-Day-Attacks – das Ende Ihres Netzes?

Sind die Rechte erst einmal möglichst restriktiv vergeben, die Systeme aktuell und durch proaktive Maßnahmen abgesichert sowie die Benutzer geschult, müssen weitere Schutzmaßnahmen ergriffen werden. So genannte Zero-Day-Angriffe, sprich: die Ausnutzung noch unbekannter Sicherheitslücken, lassen sich häufig auch mit den beschriebenen Methoden nicht verhindern.

Um diese Art von Attacken effektiv bekämpfen zu können, hat Microsoft (ab Vista) neue Funktionen in seine Betriebssysteme implementiert. Ein Beispiel ist die „Kernel Patch Protection" (auch „PatchGuard" genannt) auf x64-Vista-Systemen: Verändern Treiber einen geschützten Bereich des Kernels, wird das System sofort kontrolliert herunterfahren (BSoD). Da Systemtreiber und Kernel in allen Windows-Betriebssystemen by Design in demselben Kernel-Ring und mit gleichen Berechtigungen laufen, würde ansonsten Attacken aller Art Tür und Tor geöffnet.

Viele Zero-Day-Attacken beruhen auf Buffer Overflows – eine der am häufigsten ausgenutzten Schwachstellen in Betriebssystemen. Vereinfacht ausgedrückt versucht der Angreifer, zu viele Daten in einen zu kleinen reservierten Speicherbereich (Buffer) zu schreiben, um ihn zum Überlaufen zu bringen. Techniken, die dies verhindern sollen, sind in Nicht-Microsoft-Betriebssystemen schon länger im Einsatz. Seit Vista sind solche Schutzmechanismen auch in die Windows-Betriebssysteme für Clients und Server eingebaut.

Ein Beispiel hierfür ist die „Address Space Layout Randomization" (ASLR). Das Funktionsprinzip: Buffer Offerflows nutzen die streng sequenzielle Struktur von Heap, Stack und Co., um Adressen für Angriffe zu berechnen. Durch die zufällige Anordnung von Speicherbereichen (Randomization) wird die Ausnutzung von Overflows schwieriger. In Kombination damit sollte Data Execution Prevention (DEP) eingesetzt werden. Diese Funktion soll das Ausführen von Code aus bestimmten Speicherbereichen verhindern und wird von modernen CPUs in Hardware beherrscht (NoeXecute-Bit). Doch bislang, selbst Jahre nach der Einführung, wird sie nur sehr sporadisch genutzt.

Die wirkliche Schwachstelle – die häufig zu große Angriffsfläche von Systemen – können jedoch auch diese Techniken nicht schließen. Wer ihren Schutz möchte, sollte sie sorgfältig evaluieren und aktivieren, denn aus Gründen der Kompatibilität sind sie meist nicht aktiv.

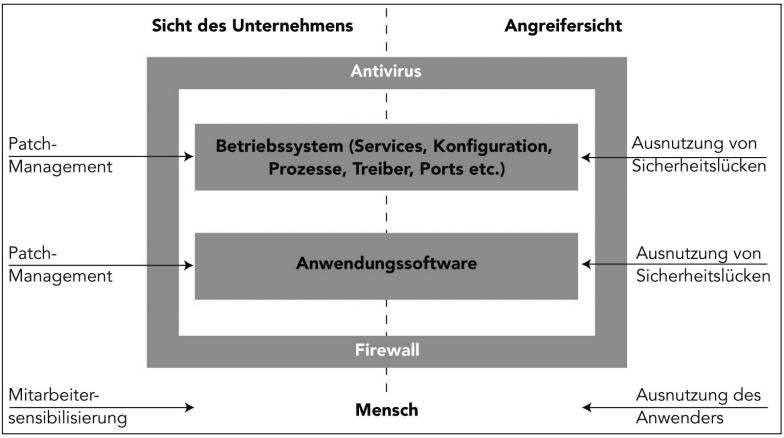
4.1.5 Das Betriebssystem als direkter Angriffspunkt

Techniken wie das beschriebene ASLR sollen auch vor unbekannten Schwachstellen schützen. Deren Anzahl lässt sich in Relation zur Angriffsfläche eines Systems betrachten, die sich im Wesentlichen aus laufenden Prozessen und Diensten, offenen Ports, aber auch der Menge an installierter Software zusammensetzt.

Um dem Angreifer möglichst wenig Ansatzpunkte zu liefern, sollte die Angriffsfläche im Idealfall so minimal sein, dass Techniken wie ASLR und DEP gar nicht erst zum Tragen kommen.

Eine gute Systemhärtung etwa kann viele Angriffe abwehren, da sie die Grundlage für den Angriff entzieht. Aber sie erfordert auch viel Know-how und Zeit.

Ein Beispiel hierfür ist die Core-Installation des Windows Server 2008, die ohne Benutzeroberfläche und sonstige Spielereien auskommen muss und damit eine neue Richtung in Microsofts Politik bedeutet.



Systemabsicherung: Die Angriffsfläche aus Sicht des Unternehmens und des Angreifers.

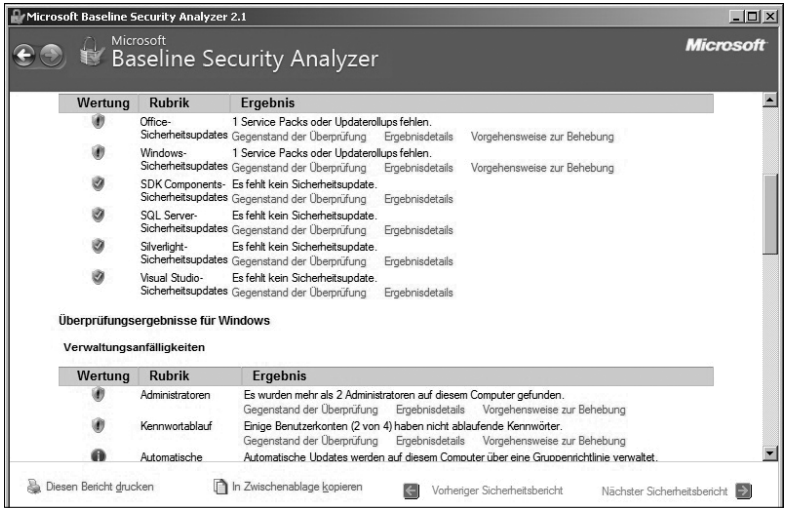
4.1.6 Vorsicht bei der Server-Migration

Microsoft hat seit den ersten Gehversuchen mit Windows NT viel Detailarbeit bei den Einstellungen der neuen Betriebssysteme geleistet. So wurde das Sicherheitsniveau neuer Installationen von Server NT bis Server 2008 stark angehoben. Die Betonung liegt hier auf „neue Installation", denn im Gegensatz dazu ist eine Migration, so vorteilhaft sie für ein Unternehmen auch scheinen mag, aus Sicherheitssicht bedenklich. Durch die Migration von Systemen werden unsichere Einstellungen und mögliche Sicherheitslücken auf das neue System übertragen. Einstellungen wie der berüchtigte LM-Hash (LAN Manager) können durchaus gewünscht sein. Im Gros der Fälle handelt es sich jedoch um Erblasten, die den potenziell sichereren neuen Systemen und Infrastrukturen die Chance nehmen, ihr Potenzial auszuspielen. Ein Server, der seit Jahren immer wieder auf neuere Betriebssysteme migriert wurde, wird nie das Maß an Sicherheit bieten wie ein neues System, dessen Einstellungen bekannt sind.

4.1.7 Durchgängiges Patch-Management – ein Muss

Wichtig ist auch die sichere Bereitstellung eines Servers, die immer offline oder in einem geschützten Segment erfolgen sollte – immerhin ist sie später die Basis für die angestrebte Zielfunktionalität. Auch hier gilt: Handelt es sich um Software von Drittherstellern, ist sie vor dem produktiven Einsatz unbedingt auf die neueste Version zu bringen. Das Patch-Management muss durchgängig sein. Es schadet auch nichts, sich im Vorfeld einen Überblick über die bereits bekannten Sicherheitslücken zu verschaffen.

Wie erwähnt, basiert die Verwundbarkeit eines Servers auf seiner Angriffsfläche. Da die Vielzahl der installierten Funktionen und laufenden Dienste nicht leicht überschaubar ist, bietet Microsoft mit dem „Security Configuration Wizard" (SCW) einen einfach zu bedienenden Assistenten, mit dem sich Sicherheitseinstellungen und Servicekonfiguration eines Servers untersuchen und anhand einer Wissensbasis konfigurieren lassen. Durch die Ausgabe als XML-Datei gehen sowohl die Übertragung auf andere Server als auch die manuelle Nachbearbeitung gut von der Hand. Allerdings ist hier wie bei allen sicherheitsspezifischen Einstellungen Vorsicht geboten, um am Ende nicht vor einem zwar gehärteten, aber funktionsunfähigen System zu stehen.



Patch-Management: Der MBSA liefert einen Überblick etwa zum Patch-Status oder zu Defiziten in Sachen Security-Best-Practises im Unternehmen.

Empfehlenswert für Administratoren kleiner und mittlerer Firmen ist auch der „Microsoft Baseline Security Analyzer" (MBSA), der einen Überblick über eine Fülle von Informationen bietet. So lassen sich damit unter anderem die Versorgung mit Updates und das Einhalten von Best Practices schnell und übersichtlich anzeigen. Gerade Unternehmen mit sehr wenigen Systemen können damit notfalls die teureren Lösungen ersetzen.

4.1.8 Keine Server ohne Clients

Für Clients gelten dieselben Regeln wie für Server: Mehr Dienste, mehr Prozesse und mehr Software führen zu einem höheren Risiko. Die Fülle von Anwendungs-

software, die auf Clients läuft, stellt den größten Teil der Angriffsfläche dar. Hier gilt es, Adobe Reader, Flash, Office und Co. schnell und vor allem sorgfältig mit Security-Patches zu versorgen. Dazu benötigt der Administrator einen umfassenden und detaillierten Überblick über die im Unternehmen eingesetzte Software. Besitzen manche Anwender lokale Administratorrechte (was sie natürlich nicht sollten), müssen sie besonders auf ihre Software achten und regelmäßig Updates einspielen. Was hierbei gerne übersehen wird, sind die Treiber, die ebenfalls Sicherheitslücken aufweisen können und beim Bekanntwerden einer Sicherheitslücke möglichst schnell aktualisiert werden sollten.

4.1.9 Kinderkrankheiten von vorgestern

Die Infrastruktur einer Windows-Umgebung ist grundlegend durch das Active Directory und die bereitstellenden Domain-Controller geprägt. Hier gilt: Ist die Sicherheit eines Domain-Controllers kompromittiert, ist auch die Domäne kompromittiert. Um die Angriffsfläche zu reduzieren, sollten Unternehmen wie auf den Servern auch auf jedem Domain-Controller Microsofts Security Configuration Wizard anwenden.

Gerade bei Einstellungen im Bereich Authentisierung zeigen sich die Tücken der Standardinstallationen. Generell gilt: Kann sich ein Angreifer (oder Malware) gültige Credentials eines Benutzers verschaffen, sind ihm Tür und Tor geöffnet. Besonders leicht wird ihm das gemacht, weil in Windows-Umgebungen grundsätzlich mehrere Authentisierungsvarianten zum Einsatz kommen. Die älteste unter ihnen, das LAN-Manager-Protokoll, wird in den meisten Umgebungen nicht mehr benötigt, jedoch nach wie vor konfiguriert und damit stets in Kombination mit sichereren Verfahren verwendet. Dabei ist das viel zitierte und angesprochene Berechnen von Kennwörtern in den meisten Fällen gar nicht interessant, weil Angreifer die abgefangenen Informationen immer wieder zur Authentisierung benutzen können. Daher sollten Unternehmen beim Aufbau einer sicheren Windows-Infrastruktur ausschließlich auf Kerberos und NTLMv2 setzen. Vor allem im Bereich Active Directory entscheiden sich viele Unternehmen für eine Migration, da die Neuinstallation und das unter Umständen erforderliche Verschieben der DC-Rollen riskant sind. Daher sollten Administratoren, die ihre Domäne schon seit längerem auf neue Versionen aktualisieren, prüfen, ob bestimmte Berechtigungen und Einstellungen noch gewünscht sind. Ein Beispiel hierfür ist die „Prä-Windows-2000-Kompatibilität“, die den anonymen Zugriff auf das Active Directory gestattet. Bei vielen Domänen lässt sich diese Funktion deaktivieren, um die Sicherheit zu erhöhen. Das erfordert wie alle Security-Maßnahmen allerdings viel Sorgfalt und die genaue Kenntnis der eigenen Applikationen und Prozesse. Auch Service-Accounts sind in diesem Kontext erwähnenswert: Ein Service benötigt niemals Domain-Admin- oder Administratorrechte, um die Applikation, für die er verantwortlich ist, auszuführen. Hier darf das Least-Privilege-Prinzip nicht aus Bequemlichkeit gebrochen werden, was allerdings oft geschieht.

4.1.10 Sicherheit auch bei der Administration

Eine sichere Verwaltung durch geschulte Administratoren ist Grundvoraussetzung für eine sichere Infrastruktur. Dabei dürfen Active Directory Service Accounts wie der Domain Admin niemals zur Administration eines Rechners oder Servers verwendet werden. Technisch lässt sich das durchsetzen, indem man das Privileg „Deny logon locally" für diese Accounts auf oberster Ebene der Domäne setzt und alle administrativen Rechner in eine eigene Organisationseinheit verschiebt. Hintergrund ist, dass diese Accounts so weitreichende Berechtigungen besitzen, dass ihre Credentials in keinem Fall auf Systemen landen dürfen, die nicht vollständig kontrollierbar sind. Das nur als Hinweis darauf, dass ein klares Rechtekonzept mit der Aufteilung administrativer Tätigkeiten erforderlich ist und alle Prozesse genau dokumentiert und auch gelebt werden müssen.

4.1.11 Fazit

Natürlich gibt es keinen perfekten Schutz – allerdings auch keinen Grund, nicht mit vertretbarem Aufwand und den angebotenen Windows-Bordmitteln die größtmögliche Sicherheit zu erreichen. Microsoft liefert mit seinen Security Guides und Tools mehr als genug Informationen, um technische Herausforderungen anzupacken. Doch technische Vorkehrungen (und die kleine Untermenge der angesprochenen Maßnahmen) sind keine umfassende Lösung. Für eine umfassende Sicht auf die IT-Security bietet es sich an, Windows-Sicherheit eingebettet in ein Informationssicherheits-Management-System (ISMS) zu betrachten – denn ohne organisatorisch gelebte Sicherheit ist Windows-Security das kleinste Problem im Unternehmen.

Matthias Fraunhofer

Matthias Fraunhofer ist ein auf Windows-Security spezialisierter Berater bei Secaron in Hallbergmoos.

TecChannel-Links zum Thema	Webcode	Compact
Tipps und Tools für mehr Sicherheit unter Windows	2019859	S.126
Gebündelte Sicherheit mittels Forefront	2019860	S.133
Windows – wo die Gefahren lauern	2019861	S1.38
Zehn IE-Einstellungen für sicheres Surfen	2019862	S.178
Conficker – das größte Botnet aller Zeiten	1986704	–
WSUS: Intelligente Update-Verwaltung unter Windows	430834	–

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

4.2 Gebündelte Sicherheit mittels Microsoft Forefront

Unter dem Markennamen „Forefront“ fasst der Software-Hersteller Microsoft seine Tools für den Schutz am Server, an den Clients und an der Firmengrenze zusammen. Zu Microsofts Produktfamilie Forefront gehören im Einzelnen der Internet Security and Acceleration Server (ISA), die Sicherheits-Tools für Desktops, Exchange, SharePoint und den Office Communications Server (OCS) sowie das Intelligent Application Gateway (IAG).

4.2.1 ISA als Schutzwall an der Unternehmensgrenze

Der erste Vertreter der Forefront-Reihe ist Microsofts ISA-Server (Internet Security and Acceleration Server), der vor knapp drei Jahren in der Version ISA 2006 erneuert und mittlerweile um ein Servicepack 1 ergänzt wurde. Bei dem ISA-Server handelt es sich, anders als häufig dargestellt, nicht um eine herkömmliche Firewall – wer lediglich nach einer leistungsstarken Firewall sucht, wird eher zu einer Appliance greifen.

Neben Firewall-Eigenschaften übernimmt der Internet Security and Acceleration Server weitere Aufgaben und Funktionen. Dazu gehören:

- die **Funktion eines Reverse Proxy** sowie die Möglichkeit, firmeninterne Server-Dienste im Web verfügbar zu machen;
- die **Verwaltung von Virtual Private Networks** (VPN), um Zweigstellen über einen gesicherten Kommunikationstunnel an das Firmennetz anzubinden;
- die **Überwachung des ein- und ausgehenden Internet-Traffics**. Dies umfasst den Zugriff der Nutzer aus dem Internet auf die veröffentlichten Web-Server, aber umgekehrt auch den Zugriff der internen Nutzer auf das Internet;
- die **Absicherung des Zugriffs von Mail-Clients** wie Outlook Web Access aus dem Internet auf den Exchange-Server im Firmennetz sowie die Absicherung des Web-Zugriffs auf den SharePoint Portal Server.

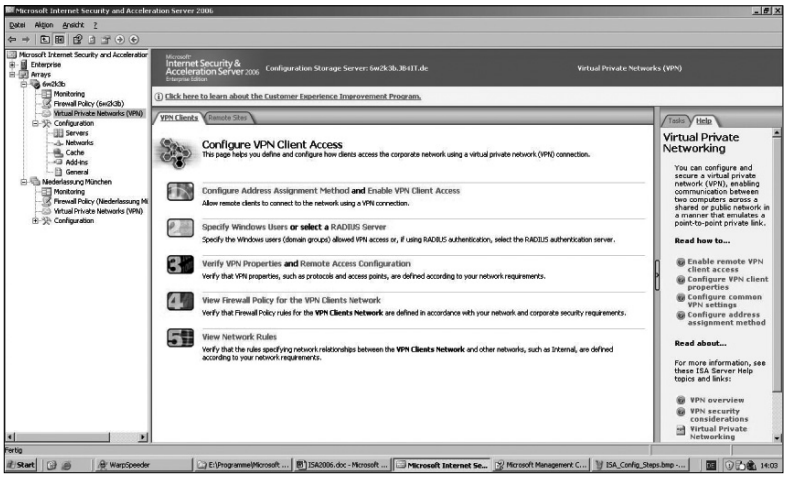
Um die Verwaltung zu vereinfachen, hat Microsoft dem ISA Assistenten zur Seite gestellt. Sie helfen bei der Konfiguration und stehen beispielsweise für den Exchange Web Client Access, Outlook Web Access, allgemeinen Mail-Zugriff oder den Zugriff auf SharePoint-Sites bereit.

Ein weiterer Funktionsbereich des Tools ist die Anbindung von Filialen via VPNs. Als Sicherheitsprotokolle werden der IPsec-Tunnel-Mode und das „Layer Two Tunneling Protocol“ (L2TP) unterstützt. Zur Authentifizierung der Benutzer lässt sich auf einen Radius-Server zurückgreifen. Ferner ist eine Quarantäne-Funktion für RAS-Zugänge (Remote Access Services) implementiert.

4.2.2 Sicherer Internet-Zugang durch das IAG

Bei Microsofts Intelligent Application Gateway (IAG) handelt es sich im Kern um ein SSL-VPN-Gateway. Es ermöglicht und kontrolliert den Zugriff beliebiger Endgeräte auf die Applikationen oder Verzeichnisse im Firmennetz. Dazu werden Zugangsportale eingerichtet, an denen sich der Benutzer anmeldet. Je nach Ergebnis von Authentifizierung und Autorisierung wird ihm ein spezifischer Zugang zum Netz mit den Anwendungen zugewiesen. Die Grundlage für den Zugriff liefert eine ausgefeilte Berechtigungslogik – eine Stärke des IAG. Zu den geprüften Zugangskriterien der Policy-basierenden Authentifizierung und Autorisierung zählen neben dem Benutzernamen unter anderem der Ort, an dem sich der Anwender zu dem jeweiligen Zeitpunkt aufhält, die Uhrzeit sowie der Sicherheitszustand des Geräts, das er verwendet. Aus all diesen Kriterien leitet das IAG die Rechte für den jeweiligen Benutzer oder sein Gerät ab.

Durch Endpoint-Policies wird ferner bestimmt, welche Bedingungen der Client erfüllen muss, damit er eine Applikation aufrufen kann. So kann beispielsweise ein mobiler Mitarbeiter, der sich mit einem als sicher erkannten Firmen-Notebook anmeldet, den vollen Zugriff auf die ihm zugewiesenen Ressourcen erhalten. Ist dieses Gerät jedoch mit Viren verseucht, so wird sein Nutzer vermutlich nur eingeschränkten Zugriff bekommen. Noch weniger Rechte werden dem Benutzer eingeräumt, wenn er sich von einem öffentlichen PC im Internet-Cafe einwählt. Ferner lässt sich festlegen, dass ein prinzipiell berechtigter Benutzer auf fremden Geräten generell keinen Download vornehmen darf. Um die Sicherheit zu erhöhen, kann das Portal zudem die Nutzung von HTTPS erzwingen.



Administration: Die Verwaltung von Microsofts ISA wird durch zahlreiche Assistenten vereinfacht.

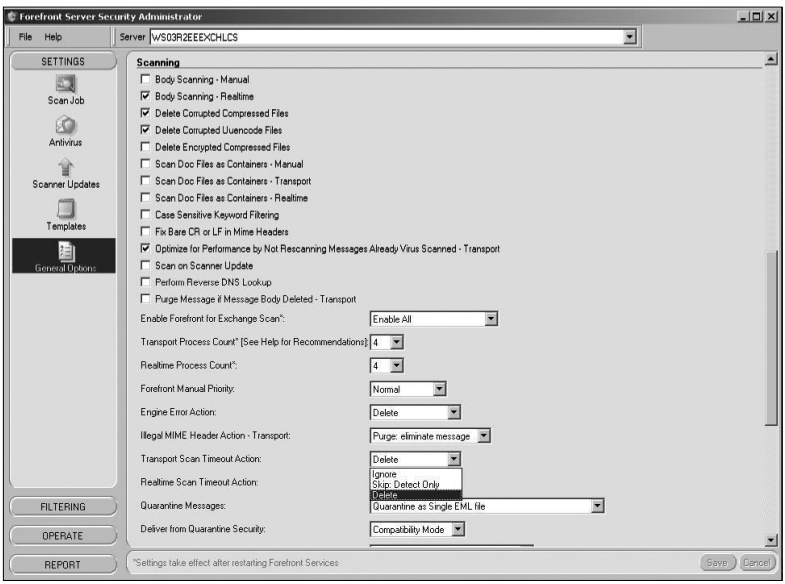
4.2.3 Wichtige Anwendungen schon parat

Um den Aufbau des Portals zu vereinfachen, hat Microsoft die wichtigsten Anwendungen – etwa diverse Domino-, Notes- und Outlook-Zugriffe, Microsoft CRM, SAP, Peoplesoft, Websphere, Sametime, Sharepoint und Citrix sowie die Zugriffe auf Terminal Services, File-Shares und FTP-Dienste – bereits vorbereitet.

Das IAG ist nur als Appliance von Microsoft-Partnern verfügbar, die auch die Konfiguration und die Verknüpfung mit einer dedizierten Hardware vornehmen. Diese Dritthersteller erweitern die Basisfunktionen des IAG meist um bessere Verwaltungsfunktionen. Ein Modul dieser Appliance ist auch der ISA, der allerdings nicht eigenständig in Erscheinung tritt: Er schützt das Gateway vor Angriffen.

4.2.4 Absicherung von Exchange und SharePoint

Der dritte Forefront-Block widmet sich der Absicherung von Microsofts Kommunikations-Servern: „Forefront Security für Exchange“ schützt den Mail-Server Exchange, während „Forefront Security für Sharepoint“ den Sharepoint Server und „Forefront Security für Office Communications“ den Office Communications Server (OCS) absichert.



Forefront für Exchange: In den Scan-Optionen entscheidet der Administrator detailliert, wie das System mit verdächtigen Mails verfahren soll.

Diese ursprünglich von Sybari („Antigen“) stammenden und von Microsoft übernommenen Forefront-Module lassen sich funktional zusammenfassen. Der Grund: Die beiden Server-Systeme Exchange und SharePoint stellen, wenn auch unterschiedlich implementiert, eine Plattform für den Informationsaustausch dar. Da beide aufgrund der Möglichkeit des Informations-Uploads als Datensenke operieren, sind auch beide den gleichen Risiken durch Malware ausgesetzt. Folglich sind die Sicherheitsprinzipien in den Forefront-Modulen für beide Systeme vergleichbar. Die Implementierung in das jeweilige Gastsystem, also Exchange oder SharePoint, ist jedoch naturgemäß unterschiedlich umgesetzt.

Forefront für Exchange beziehungsweise SharePoint sind Frameworks, in die die Drittanbieter ihre Sicherheitsprodukte einklinken können. Forefront fungiert hierbei lediglich als Vermittler zwischen den Sicherheits-Tools der Partner und den eigenen Kommunikations-Servern. Bei diesen Sicherheitssystemen handelt es sich meist um Scanner für Malware oder sonstige Bedrohungen, denen SharePoint oder Exchange ausgesetzt sind. Die eigentliche Logik zur Erkennung der Angreifer, die Scan Engines samt den Signaturdateien zur Erkennung von Malware, stammen nicht von Microsoft selbst, sondern von den Partnern. Sie bestimmen die Qualität der Sicherheitsprüfungen. Um die Sicherheit zu erhöhen, lassen sich bis zu fünf separat konfigurierbare Scan Engines parallel betreiben.

4.2.5 Schutz vor Viren, Trojanern und Co.

Das Modul „Forefront Client Security“ soll Windows-basierende Clients vor Viren, Trojanern, Spyware oder Rootkits schützen, aber auch Server-Systeme ab der Version Windows 2000 vor Malware-Angriffen bewahren. Die Verwaltung dieser Schutzeinrichtung ist allerdings zentralisiert. Dazu baut Forefront Client Security auf einem zentralen Management-Server auf, der auch das Reporting und die Benachrichtigung der Administratoren bei Sicherheitsereignissen übernimmt.

Auf dem zentralen Management-Server werden Security-Policies definiert, die dann auf die zu schützenden Geräte zu verteilen sind. Die Sicherheitseinstellungen umfassen Konfigurationen für den Echtzeitschutz samt Zeitplänen, Maßnahmen für spezifische Bedrohungen sowie Angaben zu Warnmeldungen und für das Reporting. Parallel dazu werden die Vorfälle auf den Clients an den Reporting- und Benachrichtigungs-Server geschickt, der die gesammelten Statusmeldungen dann auswertet und Berichte zum Sicherheitszustand der Systeme generiert.

Die Verteilung der Sicherheits-Policies kann durch die Active Directory Group Policy (Gruppenrichtlinien) oder ein Tool zur Softwareverteilung erfolgen. Malware-Definitionen lassen sich ferner über Microsofts „Windows Server Update Services“ verteilen. Mobile Benutzer wiederum können angewiesen werden, ihre Signatur-Updates direkt über das Microsoft Update zu beziehen.

4.2.6 Integration der Sicherheitsfunktionen in Stirling

Die Forefront-Tools stehen heute überwiegend separat nebeneinander – nicht zuletzt, weil sich die Sicherheitsfunktionen funktional kaum berühren. So hat beispielsweise eine Perimeter-"Firewall" wie der ISA mit einem Schutz für das Endgerät kaum etwas gemeinsam: In dem einen Fall geht es um die Überwachung der Protokolle, des Kommunikationsverhaltens der Benutzer und der Dateninhalte. Beim Endpoint-Schutz der Client Security wiederum steht die Abwehr von Spyware, Viren, Patches oder dergleichen im Fokus. Zwar ließe sich die Untersuchung auf Viren und Trojaner auch direkt in die Perimeter-Firewall verlagern, was diesen Produkten jedoch erheblich mehr Rechenleistung und Intelligenz abfordern würde, als sie heute im Allgemeinen aufweisen. Darüber hinaus müsste auch der Schutz des Clients vor Konfigurationsfehlern und seine Prüfung auf Updates und Sicherheits-Patches nach wie vor beim Client verbleiben.

Die Integration der unterschiedlichen Security-Komponenten kann daher nicht in der Management-Konsole liegen, sondern muss bedeutend tiefer – in der Interaktion der Tools untereinander – ansetzen. Unter dem Codenamen „Stirling" plant Microsoft die stärkere Integration der Produkte, was die heute getrennt operierenden Security-Tools dazu befähigen soll, untereinander Daten und Statusmeldungen auszutauschen.

4.2.7 Konzentrierte Tool-Interaktion geplant

Die Interaktion der Werkzeuge in einem Dynamic Response System soll die Sicherheit der gesamten Infrastruktur erhöhen. Microsoft will diese in der Umsetzung komplexe Interaktion mit der kommenden Version von Forefront (Codename „Stirling") realisieren und dann schrittweise erweitern. Und so könnte das aussehen: Hält beispielsweise ein Client-Rechner eine große Anzahl von TCP-Verbindungen, oder führt er periodisch einen Verbindungsaufbau über Bereiche von IP-Adressen durch (Port Scan), deutet das auf einen Befall des Geräts mit Schadsoftware hin. Wird dies erkannt, kann der Client blockiert werden, oder die Firewall unterbindet den Datenverkehr. Die bereits in der zweiten Betaversion vorliegende Stirling-Konsole soll Anfang 2010 auf den Markt kommen. In die kommende Version 2010 von Forefront soll ferner der „Identity Lifecycle Manager" integriert werden.

Johann Baumeister

Dipl. Inform. Johann Baumeister blickt auf über 25 Jahre Erfahrung im Bereich Softwareentwicklung sowie Rollout und Management von Softwaresystemen zurück und ist als Autor für zahlreiche IT-Publikationen tätig. Sie erreichen ihn unter jb@JB4IT.de

4.3 Windows – wo die Gefahren lauern

Die Zahl der Online-Attacken steigt – vor allem auf Windows-Umgebungen: Nicht nur Security-Experten melden eine dramatische Zunahme, auch Microsoft stellte 2008 einen neuen Rekord beim Schließen von Sicherheitslücken auf. Windows 7, die lang angekündigte und laut Steve Ballmer „beste Windows-Version aller Zeiten", ruft Befürworter und Kritiker gleichermaßen auf den Plan. Acht Jahre nach der Einführung von Windows XP – derzeit das meistgenutzte Betriebssystem der Welt – und zwei Jahre nach der „schmerzvollen" Erfahrung mit Vista sagen viele Experten dem kommenden OS nach ersten Tests jedoch eine mögliche Erfolgsstory voraus. Bis das Gros der Nutzer das neue Microsoft-Betriebssystem in vollem Umfang nutzen und von den verbesserten Sicherheitsbedingungen profitieren kann, wird es aber noch etwas dauern.

Insbesondere in sensiblen Firmenumgebungen sollten Anwender und Netzadministratoren daher zunächst den Sicherheitsrisiken für die aktuellen Windows-Versionen ihre Aufmerksamkeit widmen. Während Microsoft in den ersten sechs Monaten 2008 mit 36 Security-Updates insgesamt 58 Sicherheitslücken in seinen Betriebssystemen schließen musste, waren in der zweiten Jahreshälfte 42 Sicherheits-Updates notwendig, um 97 Schwachstellen zu beheben.

Wichtig ist daher, die Risiken für Windows zu erkennen und einzudämmen. Es handelt sich dabei um naheliegende Gefahren, die auf Anwenderseite jedoch kaum verinnerlicht werden, aber auch um weniger offensichtliche Bedrohungen, die folglich noch weniger Beachtung finden. Aus denselben Gründen, wie private PC-Anwender Windows nutzen, verwenden auch Unternehmen das populäre Betriebssystem: geringe Kosten und hohe Bedienerfreundlichkeit. Doch gerade aufgrund dieser Vorzüge werden die offensichtlichsten Gefahren häufig übersehen.

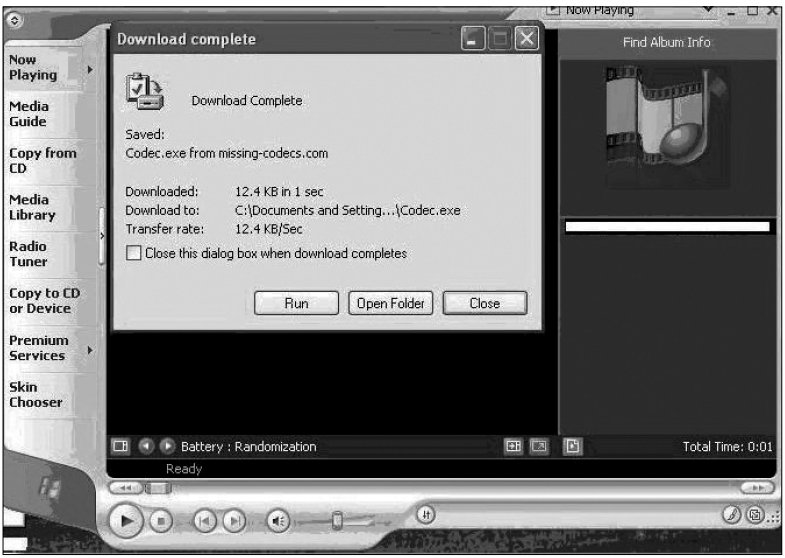
4.3.1 Achillesferse Windows-Update

Ein häufig unterschätztes Sicherheitsrisiko sind Windows-Patches und -Updates beziehungsweise deren Nicht-Installation. Die Anfang 2009 rasant ansteigende Infektionsrate durch den Wurm Conficker (auch Downadup oder Kido genannt) verdeutlichte, wie wenig ausgeprägt das Gefahrenbewusstsein unter Anwendern ist, wenn es darum geht, bekannte Sicherheitslücken durch regelmäßiges Aktualisieren des Betriebssystems zu schließen. Erstmals im November 2008 aufgetaucht, nutzte der Schädling die (von Microsoft bereits seit Oktober gepatchte) MS08-067-Sicherheitslücke im „Windows Server Service" aus, um sich über lokale Netze auszubreiten. Eine Ende Dezember 2008 entdeckte neue Variante des Wurms (Win32.Worm.Downadup.B) wiederum zeigte, dass auch Wechselspeichermedien zu gefährlichen Infektionsmedien werden können: Der Schädling nutzte unter anderem USB-Sticks, um sich zu verbreiten, kopierte sich dann in das Recycler-Verzeichnis des Windows-Papierkorbs und kreierte eine „Autorun.inf"-Datei, um sich auf dem befallenen PC künftig selbst zu starten.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt grundsätzlich das Einspielen neuer Patches, den Einsatz einer Firewall und eines Antivirenprogramms. Angesichts des Trends, dass Malware universelle Verbreitungswege wie Netzfreigaben, Wechseldatenträger oder Server-Dienste nutzt, bleibt dem Anwender hier letztlich keine andere Wahl.

4.3.2 „Eingebaute" Sicherheitslücken

Durch diverse Applikationen, die Microsoft mit seinen Betriebssystemen bündelt, entstehen systemimmanente Schwachstellen (Built-in Vulnerabilities). So wurde beispielsweise der Windows Media Player zum Opfer – oder besser zum Instrument – für die Verbreitung eines der produktivsten Malware-Vertreter: Im April belegte der Schädling „Trojan.Wimad.Gen.1" mit 5,68 Prozent den dritten Platz des monatlich erscheinenden „E-Threat Landscape Report" von BitDefender. Sein Bruder „Trojan.Downloader.WMA.Wimad.N", der im Dezember 2008 auf dem fünften Rang landete, war immerhin für 3,14 Prozent aller weltweit infizierten Systeme verantwortlich. In der Regel via E-Mail verbreitet und als 3,5 MB großes WMA-Sound-File von populären Künstlern getarnt, öffnet der Trojaner einen Web-Browser, um einen angeblich benötigten Codec herunterzuladen. In Wirklichkeit handelt es sich dabei um den Zusatz „Adware.PlayMp3z.A".



Erfüllungsgehilfe für Malware: der Windows Media Player.

Microsofts Media Player ist aber nur ein Beispiel dafür, wie Cyberkriminelle Windows-Applikationen nutzen, um Malware zu verbreiten. Dabei gilt: Nicht nur ausführbare Dateien beherbergen Schadsoftware, vielmehr kann jede Software, sei sie von Microsoft oder Drittanbietern, Malware enthalten und von Hackern dazu missbraucht werden, Schadcode in Systeme zu schleusen. Abhilfe schafft hier nur die permanente Überwachung aller Dateien und Applikationen, die auf einem System laufen.

4.3.3 IE – ein Leckerbissen für Malware-Autoren

Auch bei dem Microsoft-Browser Internet Explorer (IE) handelt es sich um eine in Windows integrierte Anwendung, die von Malware-Programmierern gern missbraucht wird, um Windows-Systeme zu infiltrieren. Ein Beispiel hierfür ist der Wurm „Packer.Malware.NSAnti.1", der sowohl über infizierte Web-Seiten als auch über autorun.inf-Files via Wechselmedien verbreitet wurde. NSAnti korrumpiert Verhaltensweisen des IE und stiehlt so Nutzernamen und Passwörter für Online-Spiele wie Silkroad Online oder Lineage. Ein weiterer Schädling, der den Microsoft-Browser für seine Zwecke einspannt, ist der „Trojan.Exploit.ANOP". Der Javascript-Trojaner schleust über iFrame- oder ActiveX-Schwachstellen weitere Schadsoftware in Windows-Umgebungen ein.

4.3.4 Background-Services – die Leiche im Keller

In der Standardeinstellung aktiviert Windows beim Start einige Services, die selten gebraucht werden, jedoch potenzielle Sicherheitslücken darstellen und zudem unnötig Ressourcen verschwenden. Ein Beispiel: Die Windows XP Media Center Edition aktiviert standardmäßig den Remote Desktop – eine Schwachstelle, die es Angreifern ermöglicht, einen kompletten Systemcrash zu verursachen

4.3.5 File Permissions – der Teufel im Detail

Sicherheitsrisiken birgt auch Microsofts Windows-Datei-Management-System – vor allem in Firmennetzen: Die meisten Dateien und Ordner erben die Berechtigungsmerkmale ihrer Stammordner. Wird beispielsweise ein Ordner verschoben, übernimmt dieser automatisch auch dessen neue Eigenschaften. Einerseits kann dieser Mechanismus helfen, via Dateiverschiebung von einem Ordner in den anderen auf einfache Weise mehrere Zugriffsberechtigungen zu ändern. Doch kann eine solche Aktion auch zur Feuerprobe avancieren, wenn viele Dateien und Ordner von einem System auf das andere übertragen werden. Der Berechtigungsstatus sensibler Dateien sollte daher vor dem Verschieben sorgfältig geprüft werden.

4.3.6 Angriffsziel Windows-Client

Im Vergleich zu Windows-Servern, die hinsichtlich Sicherheit und Abwehrstrategien unter der Aufsicht von Netzadministratoren stehen, sind Windows-Clients schwerer zu verwalten und zu schützen. Verantwortlich dafür ist neben der ungleich höheren Anzahl ihre Flexibilität.

Die vielen Windows-basierenden Notebooks, Netbooks und anderen mobilen Geräte mit all ihren Konfigurationsmöglichkeiten und bestehenden Accounts, die zudem von verschiedenen Nutzern in unterschiedlichen Bereichen genutzt werden, bergen eine Fülle potenzieller Sicherheitslücken. Darüber hinaus lassen sich Windows-Clients leicht als Zugangstor zu sensiblem Datengut missbrauchen, das in der Regel verhältnismäßig sicher auf dem Server liegt. So ist es fast unmöglich, eine mobile Festplatte zwecks Datendiebstahl an einen Server anzuschließen. Einfacher ist es, sich über einen Client Zugang zum Server zu verschaffen, um sensible Daten auf einen USB-Stick zu kopieren und dabei eine ganze Reihe von Sicherheitsmaßnahmen zu umgehen. Aus diesem Grund greifen Hacker mit Vorliebe Windows-Clients an.

Client-Security-Lösungen können hier helfen, über zentral gemanagte Features wie Antivirus, Firewall und Antispam vor Bedrohungen wie Viren, Spyware, Rootkits oder Spam sowohl auf Client- als auch auf Server-Ebene zu schützen.

4.3.7 Vorsicht mit Admin-Rechten

Eine Hauptursache für den Erfolg von Zero-Day-Angriffen ist die in vielen Unternehmen sorglose Vergabe von Rechten. So besitzen unnötig viele Windows-Clients administrative Rechte. Die Gefahr: Einerseits kann der Anwender versehentlich oder aus Nachlässigkeit Dateien und Verzeichnisse ändern oder löschen, die die Funktion des Gesamtsystems beeinträchtigen. Andererseits erleichtert es ein mit administrativen Rechten ausgestatteter Windows-Client Hackern, ihn mit Schadsoftware zu infizieren.

Auf den Punkt gebracht: Nicht nur dem Anwender werden umfassende Rechte eingeräumt, sondern auch dem Angreifer. Nach einer aktuellen Untersuchung der auf Priviledge-Management spezialisierten Beyond Trust Corporation können sich Unternehmen, deren Nutzer lediglich über Standardrechte verfügen, besser gegen Malware und Zero-Day-Threats schützen.

Laut Studie enthalten 92 Prozent der von Microsoft als kritisch eingestuften Security Bulletins genau diese Empfehlung. Ein weiteres Ergebnis: Das von 94 Prozent der Office-, 89 Prozent der Internet-Explorer- und 53 Prozent der Windows-Schwachstellen ausgehende Risiko ist für Firmen, die bei Windows-Clients auf administrative Rechte verzichten, geringer.

4.3.9 Die Gefahr lauert in fremden Netzen

Die Bedeutung sorgfältiger Rechtevergabe oder Datei- und Druckerfreigaben wird vor allem deutlich, wenn Windows-Clients in ungesicherten WLAN-Umgebungen wie Flughäfen, Bahnhöfen oder Hotels genutzt werden: Sind Datei- und Druckerfreigaben nicht deaktiviert, können Dritte die auf dem Client enthaltenen Dokumente offen einsehen. Daher ist es ratsam, darüber hinaus Verschlüsselungsmethoden zu verwenden, die sowohl den Zugang zu Daten als auch den Diebstahl der Informationen verhindern. Ein SSL/TLS-Protokoll (Secure Sockets Layer/Transport Layer Security) kann hier Sicherheit bieten und auch die Integrität von Daten für die Web-basierende Kommunikation (Corporate E-Mail) gewährleisten.

4.3.10 Kombinierte Gegenwehr

Ein Fünftel der Erdbevölkerung (rund 1,35 Milliarden Menschen) ist heutzutage mit dem Internet verbunden – und im Schnitt mit täglich 2000 neuen Viren, monatlich 50.000 Phishing-Attacken und jährlich mit mehr als einer Million entwendeten PCs konfrontiert. Gut 80 Prozent dieser E-Threats richten sich explizit gegen Windows-Systeme. Doch lassen sich die Risiken eindämmen – mit einer Kombination aus regelmäßigen System-Updates, dem richtigen Umgang mit sensiblen Daten sowie zuverlässigen Schutzlösungen.

Harald Philipp

Harald Philipp ist Geschäftsführer der BitDefender GmbH in Tettnanag.

TecChannel-Links zum Thema	Webcode	Compact
Windows – wo die Gefahren lauern	2019861	S.138
Tipps und Tools für Sicherheit unter Windows	2019859	S.126
Gebündelte Sicherheit mittels Forefront	2019860	S.133
Zehn IE-Einstellungen für sicheres Surfen	2019862	S.178
Die besten Check- und Sicherheits-Tools	481351	S.183

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

4.4 Apple-Viren – Gefahr für Mac und Windows

Mac-Malware gefährdet nicht nur Apple-Systeme. Kriminelle greifen gerne auf den Mac zurück, um Windows-Systeme unerkannt zu infizieren. TecChannel zeigt Ihnen die größten Gefahren und wie Sie infizierte Macs erkennen, bereinigen und künftig schützen.

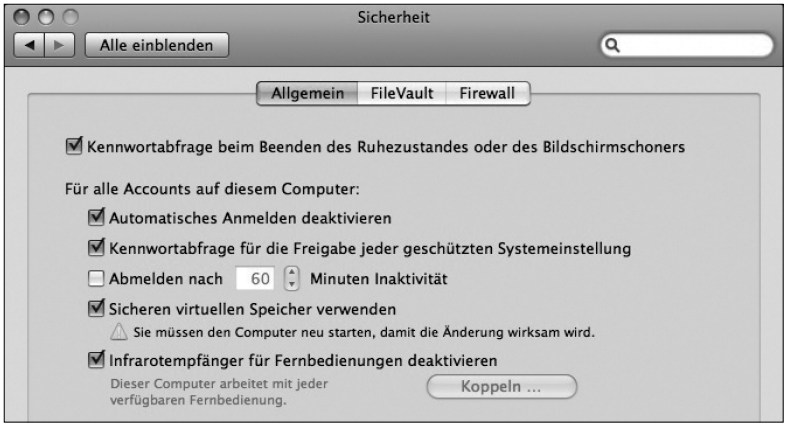
Im April 2009 wurde erstmals ein Botnet gefunden (Webcode **2018297**), das nur aus Apple-basierten Rechnern besteht. Damit ist klar: Auch für Mac-Nutzer gibt es keine Insel der Seligen, sie sind wie jeder PC-Anwender im Visier der Cyberkriminellen. Zwar ist die Bedrohungslage noch lange nicht so massiv, dennoch sollten sich auch Mac-Nutzer mit der Anschaffung einer Anti-Viren-Software auseinandersetzen. Denn eine weitere Gefahr lauert im Einsatz von heterogenen Umgebungen: Einige Malware-Autoren nutzen Mac OS als Inkubator, um von dort aus Windows-Systeme zu infizieren. Vor allem mobile Geräte wie Notebooks sind geeignet, solche Attacken auszuführen. Administratoren sollten also auch bei Macs auf einen geeigneten Malware-Schutz bestehen, wenn die Systeme in ihrem Netzwerk angeschlossen werden sollen.

In diesem Artikel setzen wir uns mit den Gefahren eines Apple-Botnetz auseinander. Dabei beleuchten wir den Mac-Virus OSX.RSPlug.A genauer und zeigen, warum Conficker Macs zwar nicht betrifft, Apple-Nutzer aber dennoch Sicherheitsvorkehrungen treffen sollten. Wir zeigen Ihnen, wie Sie Ihren Mac auf den Virus überprüfen und wie Sie die größten Schwachstellen im Mac OS X schließen.

4.4.1 Was den Mac unsicher macht

Der Mac-Virus OSX.RSPlug.A hat gezeigt, wo die Gefahr für Mac-Besitzer am größten ist: Wenn man die manipulierte Software selbst installiert. Bei OSX.RSPlug.A ist es eine angeblich fehlende Software für die Wiedergabe eines Videos; unter Windows ist einer der Tricks, sich als Antivirensoftware auszugeben (zum Beispiel „Spyware Protect 2009“).

Relativ gering ist dagegen mit Mac OS X die Gefahr, allein beim Besuch einer Internet-Seite (ohne Zutun des Benutzers) oder bei einer bestehenden Internet-Verbindung „gehackt“ zu werden. Denn für Hacker bietet Mac OS X weniger Angriffspunkte – zumindest solange man die diversen Komfortfunktionen nicht nutzt, die Apple in den Systemeinstellungen unter „Sharing“ anbietet. Wer einige davon privat nutzen will oder muss, findet im Kapitel „Sicher trotz Sharing“ die wichtigsten Sicherheitstipps zu diesem Thema. Wer die Dienste unter „Sharing“ in einer Firma nutzt, sollte sich darauf verlassen können, dass die Firma passende Sicherheitsvorkehrungen getroffen hat – wer ein Mac-Notebook aus der Firma mitnimmt, sollte prüfen, ob die Dienste zu Hause nicht abgeschaltet sein können.



Sicherheit: Ein abgeschotteter Mac ist auch ein sicherer Mac.

Allen diesen „Diensten" (oder „Services") ist eines gemeinsam: Sie starten ein Hintergrundprogramm, das Mac OS X online (oder im lokalen Netz) ansprechbar macht. Findet ein Hacker eine Sicherheitslücke in einem dieser Hintergrundprogramme, kann er versuchen, ob sich diese Lücke nutzen lässt, um den Mac fernzusteuern oder um Dateien vom Mac zu lesen. Sind die Dienste dagegen deaktiviert, kann ein Hacker auch eventuell vorhandene Sicherheitslücken nicht ausnutzen.

4.4.2 Hintergrund: Ein spezialisierter Virus für den Mac

Ende Oktober/Anfang November 2007 tauchen die ersten Berichte über einen Trojaner auf, der sich auf Macs einnistet. Der Softwarehersteller Intego nennt den Schädling „OSX.RSPlug.A": Er gibt sich als Videocodec aus, der notwendig ist, um gewisse Pornofilme abzuspielen. Der angebliche Codec wird von Porno-Internet-Seiten zum Download angeboten; wer auf das Standbild des Videos klickt, erhält eine DMG-Datei (eine virtuelle Festplatte), die nach dem Öffnen ein harmlos aussehendes Installationsprogramm zeigt. Startet man die Installation, wird man nach dem Kennwort eines Administrators gefragt und danach läuft unter Mac OS X 10.4 und 10.5 (scheinbar) alles wie gewohnt. Nur die versprochenen Videos fehlen. Allerdings erhält man in Wirklichkeit keinen neuen Videocodec, sondern ein Internet-Plug-in, das die eigentlich schädliche Software installiert. Das Internet-Plug-in wird automatisch mit allen Browsern geladen, deshalb ist der Schaden in der Regel schon geschehen, wenn man einen Browser nach der Installation des angeblichen Codecs startet.

Der Schaden, der durch OSX.RSPlug.A angerichtet wird, ist schnell beschrieben: Die Software ändert die Liste der DNS-Server und leitet den Nutzer so auf gefälschte Webseiten, um Passwörter und Nutzerdaten zu stehlen.

Wie man OSX.RSPlug.A erkennt und bereinigt

Insgesamt gibt es drei Merkmale für den Trojaner OSX.RSPlug.A. Ein Anzeichen für die Infektion mit dem Trojaner ist die Datei „plugins.settings“ im Ordner „/Library/Internet Plug- Ins“. Da allerdings Hacker dazu neigen, solche Dateinamen von Zeit zu Zeit zu ändern, versteckt sich der Trojaner möglicherweise hinter einem anderen Dateinamen.

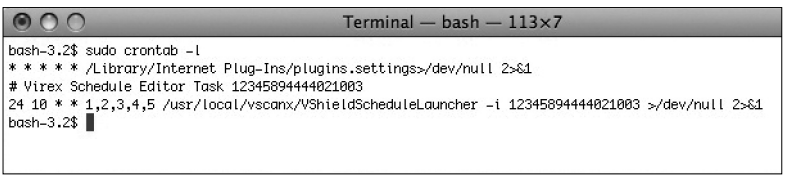
Ein anderes Indiz ist ein Eintrag in der Auftragstabelle für den Benutzer „root“, die der Hintergrundprozess Cron auswertet. Diese Cron-Tabelle ist normalerweise für den Benutzer „root“ leer; allerdings hinterlassen manche Spezialprogramme dort Spuren, so dass auch dieses Indiz nicht eindeutig ist. Wer die Tabelle zur Sicherheit prüfen will, muss sich als Benutzer mit Verwaltungsrechten (siehe „Systemeinstellungen > Benutzer“) anmelden, das Dienstprogramm Terminal starten und dort den folgenden Befehl eintippen:

```
sudo crontab -l
```

Wenn man diesen Befehl eingibt und die Eingabetaste betätigt, muss man noch das Kennwort für den gerade aktiven Benutzer eintippen, damit das Unix-System den Befehl ausführt. Erhält man die folgende Antwort, kann man sich sicher sein, dass der Trojaner auf diesem Mac nicht aktiv ist:

```
crontab: no crontab for root
```

Umgekehrt gilt das aber nicht: Nicht jeder Eintrag in der Cron-Tabelle ist ein Hinweis auf OSX.RSPlug.A.



Verdächtig: Die zweite Zeile deutet auf einen aktiven Trojaner hin.

Die einzig eindeutige Methode, den Trojaner zu erkennen, ist ein Vergleich zwischen den Systemeinstellungen und der Information, die ein Unix-Befehl liefert – das ist aber nur unter Mac OS X 10.5 möglich:

```
scutil
show State:/Network/Global/DNS
...
exit
```

Der Befehl `scutil` liefert Informationen darüber, welche DNS-Server das Betriebssystem verwendet, um Internet-Namen wie www.tecchannel.de in die num-

merische Form zu übersetzen. Der Trojaner ersetzt die normal zugeteilten DNS-Server in der Liste durch eigene Adressen, hinter denen manipulierte Systeme des Hackers stehen. Damit kann der Hacker den Browser zu völlig anderen Servern schicken. Wer beispielsweise auf der Suche nach www.ebay.com war, wurde vom Trojaner zu einer gefälschten Internet-Seite geleitet, die ähnlich aussieht wie Ebay USA, die aber nur dazu dient, Benutzername und Kennwort von Ebay-Teilnehmern in Erfahrung zu bringen. Ist der Trojaner aktiv, stehen vor oder nach den normalen DNS-Einträgen weitere. Zum Vergleich kann man (nur unter Mac-OS X 10.5) die Liste der DNS-Einträge in den Systemeinstellungen prüfen (unter dem Punkt „Netzwerk", wenn links die Schnittstelle gewählt ist, über die die Internet-Verbindung hergestellt wird).

```
<dictionary> {
ServerAddresses : <array> {
0 : 192.168.13.13
1 : 192.168.13.14
}
DomainName : officemuc.idg
}
```

Bei einem manipulierten System sieht in den Systemeinstellungen eine Liste von DNS-Servern, wobei die Einträge teilweise in grauen Buchstaben und teilweise in schwarzen dargestellt werden.

Ist ein System befallen, entfernt man den Trojaner am einfachsten mit einer Anti-Viren-Software, etwa dem kostenlosen ClamXav (www.clamxav.com). Doch auch eine manuelle Reinigung ist möglich. Dazu müssen sie die Internet Plug-Ins sowie den entsprechenden cron-Job entfernen. Die Seite MacApper hat dazu eine Anleitung verfasst (http://macapper.com/2007/11/10/remove-osxrspluga-trogan/).

4.4.3 Sicherheit trotz Sharing

Als Betriebssystem ist Mac OS X ist ab Werk relativ sicher. Das liegt vor allem daran, dass Netzdienste (in den Systemeinstellungen unter „Sharing") deaktiviert sind. Wir prüfen, welche Dienste einigermaßen sicher und welche möglicherweise gefährlich sind. In den Systemeinstellungen unter „Sharing" legt man fest, ob (und wenn ja, wie) Mac OS X auf Anfragen aus dem Netz antwortet (das kann das lokale Netz in einer Firma sein oder das globale Internet). Jeder dort aktive „Dienst" braucht mindestens ein Hintergrundprogramm, das auf entsprechende Anfrage aus dem Netz aktiv wird. Oder anders formuliert: Wer „Printer Sharing" aktiviert, stellt damit einen Drucker, der über USB am Mac angeschlossen ist, anderen Benutzern im Netz zur Verfügung. Solange dieser Dienst aktiv ist, wartet im Hintergrund die Unix-Software cups auf Anfragen anderer Benutzer. Beim Druck ist dann keine Autorisierung notwendig: Ein anderer Mac kann auf einem „freigegebenen" Drucker ohne Angabe von Benutzername und Kennwort drucken.

Komfort oder Sicherheit?: Abschalten der Dienste macht den Mac zwar sicherer, allerdings fehlen dann viele Funktionen.

Relativ ungefährlich sind folgende Dienste

Printer-Sharing: Das dazugehörige Hintergrundprogramm cups wird regelmäßig aktualisiert; Sicherheitslücken regelmäßig geschlossen.

Web-Sharing: Dahinter steckt der Webserver Apache, von dem Apple in Mac-OS X eine nicht ganz aktuelle Version verwendet. Da Sicherheitslücken aber regelmäßig geschlossen werden, ist die damit verbundene Gefahr relativ gering.

Entfernte Anmeldung: Gemeint ist der Unix-Dienst ssh (= „secure shell"), dessen Hintergrundprogramm als gut geschützt gilt. Wenn aber zum Beispiel ein Benutzer namens „admin" eingerichtet ist und das Kennwort leer ist oder „admin" lautet, dann wird die „Entfernte Anmeldung" zum offenen Tor: Mit dieser leicht zu erratenden Kombination aus Benutzername und Kennwort kann jeder die komplette Kontrolle über den Mac übernehmen. Sicher ist dieser Dienst nur, wenn das Kennwort schwer zu erraten ist.

Screen-Sharing, Entfernte Verwaltung: Beide Dienste greifen auf Apples Remote Desktop zurück; in den Optionen lässt sich außerdem das Hintergrundprogramm VNC aktivieren. Wie bei der entfernten Anmeldung ist die Sicherheit dieses Dienstes von der Qualität des Kennwortes abhängig. Manche Experten halten VNC für weniger sicher als Apple Remote Desktop; wir raten dazu, diese Option nur zu aktivieren, wenn die Arbeit mit Apple Remote Desktop nicht möglich ist.

Kritisch sehen wir die Dienste

Filesharing: Filesharing ist ein Sammelbegriff für Dienste, die den Zugriff auf die Festplatte des Mac erlauben (oder auf einzelne „freigegebene" Ordner). Seit Mac-OS X 10.5 wird das Kennwort für Filesharing nicht mehr im Klartext übertragen; ist also für andere Personen im gleichen Netz nicht mehr ohne weiteres lesbar. Doch das gilt nur, wenn man weder FTP- noch SMB-Sharing aktiviert. Bei diesen

beiden Diensten wird das Kennwort weiter im Klartext übertragen – deshalb sollte man diese Zugriffsart nur in einem gut geschützten Firmennetz aktivieren und speziell bei einem Notebook auf Reisen abschalten. Ganz generell empfehlen wir bei Filesharing den Gastzugriff abzuschalten.

Internet-Sharing: Damit wird ein Mac zum Router; sprich: der Mac nutzt beispielsweise Airport, um ein weiteres Gerät in das drahtgebundene Ethernet zu bringen. Damit muss der Mac aber alle Daten von einem Anschluss zum anderen transportieren, wobei immer die Gefahr der Überlastung besteht. Bislang konnte man diese Funktion immer wieder dazu nutzen, bei extremer Überlastung oder bei einem Fehler in der Transportsoftware (= „routed") beide Internet-Verbindungen lahm zu legen.

Bluetooth-Sharing: Für den Betrieb einer drahtlosen Maus oder Tastatur muss Bluetooth-Sharing nicht aktiv sein. Notwendig ist die Funktion nur, wenn man beispielsweise Dateien zwischen einem Handy und dem Mac übertragen will. Wir empfehlen Bluetooth-Sharing nur zu aktivieren, wenn wirklich Daten übertragen werden und danach wieder auszuschalten. Außerdem sollte man generell festlegen, dass der „Verbindungsaufbau nötig" ist – denn dann muss man das Bluetooth-Gerät mindestens einmal bei Mac-OS X anmelden und registrieren, damit die Kommunikation funktioniert.

Entfernte Apple-Events: Dieser Dienst erlaubt die Fernsteuerung eines Mac von einem anderen aus; benutzt werden dabei Applescript-Befehle. Nach der Eingabe von Benutzername und Kennwort erhält man bei der Fernsteuerung keine weiteren Informationen, dass der Mac gerade im Hintergrund Befehle eines anderen Rechners ausführt. Deshalb empfehlen wir dringend diesen Dienst nur einzuschalten, solange man diese Funktion benötigt.

4.4.4 Conficker: Mac kein Hauptziel, aber Verbreitungsweg

Intego und andere Anbieter von Antivirensoftware für den Mac haben Entwarnung gegeben: Der Computerwurm Conficker (alias „Downadup" oder „Kido" Webcode **1986704**) ist eine Gefahr für Windows, speziell für Windows XP, Mac-Nutzer bleiben aber einstweilen verschont. Möglicherweise könnte der Wurm sich aber in einer virtuellen Windows-Umgebung wie Apple Bootcamp, Parallels Desktop oder Vmware Fusion festsetzen. In diesem Fall sollte man unter Windows beispielsweise die kostenlose „Software zum Entfernen bösartiger Software" von Microsoft installieren (oder ein anderes kommerzielles Antivirenprodukt von Herstellern wie Symantec, Kaspersky oder F-Secure). Die Hacker hinter Conficker hatten anfangs eine Sicherheitslücke in Windows genutzt, um den Wurm zu installieren. Neuere Varianten des Wurms versuchen aber verstärkt, in Firmennetzen die Sharing-Dienste von Windows-PCs als Eingangstor zu nutzen.

Wieder andere Varianten werden über USB-Stick oder CDs verbreitet, wo sie sich als automatisch startendes Programm tarnen. Allen Verbreitungswegen ist ge-

mein, dass Mac OS X dagegen immun ist. Wer viele Daten (per E-Mail oder auf CDs und ähnlichem) erhält, sollte dennoch auf dem Mac Software installieren, die Conficker erkennt und entfernen kann. Daher macht es durchaus Sinn, seinen Mac mit Anti-Viren-Software zu schützen. Denn so verhindert der Mac-Benutzer, dass er im Netzwerk oder im Bekanntenkreis als Virenschleuder Dateien Viren an Windows-Nutzer schickt.

4.4.5 Update-Muffel sind gefährdet

Für Windows und Mac OS X veröffentlicht der jeweilige Hersteller in mehr oder minder regelmäßigen Abständen Aktualisierungen oder „Updates". Microsoft hat dafür den zweiten Dienstag im Monat etabliert; Apple liefert unregelmäßig: Das Update auf Mac OS X 10.5.6 am 15. Dezember 2008 und ein Sicherheits-Update 2009-001 am 12. Februar 2009. Wer auf diese Aktualisierungen verzichtet, ist leichte Beute für Hacker: In der Regel veröffentlichen Microsoft und Apple nach einem solchen Update detaillierte Informationen über geschlossene Sicherheitslücken. Was im Gegenzug bedeutet, dass Hacker Informationen bekommen, wo sich ein Angriff lohnt: Wer etwa Apples „Security Update 2009-001" nicht installiert, hat eine offene Sicherheitslücke in Safari, mit der sich Javascript-Befehle in RSS-Nachrichten verstecken lassen. Deshalb kann es für Hacker lohnend sein, entsprechend präparierte RSS-Nachrichten im Internet anzubieten und auf Internet-Surfer mit veraltetem Mac-Betriebssystem zu warten.

Aktualisierung: Auch Apple-Systeme können sich automatisch updaten.

Wir empfehlen für Updates von Apple folgendes Verfahren: In den Systemeinstellungen wechselt man in den Bereich „Softwareaktualisierung" und aktiviert dort die tägliche Suche nach Updates: „Nach Updates suchen: Täglich". Danach deaktiviert man allerdings die Automatik „Wichtige Updates automatisch laden"; damit man jederzeit vollständige Kontrolle über den Ablauf hat. Dann wird man täglich über Updates informiert; steht in der Liste ein Update für das Betriebssystem „Mac OS X ..." oder ein „Security Update" macht man sich eine Notiz auf

Papier oder im elektronischen Kalender. Spätestens nach einer Woche sollte man dieses Update dann installieren, aber nicht ohne vorher auf den einschlägigen Informationsbörsen im Internet (discussions.apple.com oder macwelt.de) nach möglicherweise darin enthaltenen Fehlern zu suchen.

4.4.6 Installierte Software muss aktuell sein

Ein Hacker hat auf der Konferenz Consec West im März 2009 (Webcode **1830597**) gezeigt, wo heute eine der Gefahren für Mac-Besitzer liegt (selbst wenn man Anfängerfehler vermeidet): Das Preisgeld für einen schnellen Einbruch in einen Mac verdiente er sich mit einem Einbruch in Safari – in unter einer Stunde. Obwohl die Details noch nicht klar sind, zeigt das, wo die Gefahr liegt: Bei Zusatzsoftware wie Adobe Reader, Adobe Flash oder dem Plug-in Flip4mac, mit dem man im Browser Windows-Filme abspielen kann. Diese Software kann Fehler enthalten, die ein Hacker für den Einstieg in das Betriebssystem nutzen kann. Der Umkehrschluss heißt deshalb, dass man Zusatzprogramme auch regelmäßig aktualisieren muss.

Hacker nutzen gerne weit verbreitete Software. Auf dem Mac zählen dazu die Browser Firefox und Safari, Adobe Reader und das dazugehörige Reader-Plug-in, Adobe Flash Player-Plug-in sowie das Plug-in Flip4mac. Verwendet man eines dieser Programme oder Plug-ins, sollte man regelmäßig (mindestens einmal im Monat) deren Versionsnummern prüfen. Die Browser sollten im Ordner „Programme“ zu finden sein, die Plug-ins im Ordner „Library/Internet Plug-ins“. Zur Gegenkontrolle nutzt man Update-Dienste wie MacUpdate (www.macupdate.com) oder Versiontracker (www.versiontracker.com) – dort werden täglich aktuell die neuesten Versionen der Software veröffentlicht.

4.4.7 Fazit

Macs haben den guten Ruf, „angriffssichere“ Computer zu sein. Was uns aber seit Jahren beschäftigt, ist Apples unguter Ruf, wenn schnelle Reaktion auf eine Bedrohung gefragt ist. Stefan Frei von der Universität Zürich hat dazu eine Zählmethode entwickelt und sechs Jahre gezählt: Wie viel Zeit vergeht, bis ein Hersteller eines Betriebssystems auf eine schwere Bedrohung reagiert und ein Update bereitstellt, das den Fehler behebt? Hier liegt Apple klar hinter Microsoft.

Für die Zukunft schadet es auch den Mac-Nutzern nicht, wenn sie deutlich mehr Vorsicht walten lassen. Denn schon lange sind auch die Apple-Rechner im Visier von Kriminellen. Die Windows-Fraktion hat hier einen Vorteil: Seit Jahren wird sie mit Malware bombadiert, Sicherheits-Software gehört mittlerweile auf jede Windows-Maschine. Bleibt zu hoffen, dass sich auch auf dem Mac ein Bewusstsein für Sicherheitsproblematiken entwickelt.

Walter Mehl

5 Praxis und Know-how

Das letzte Kapitel in diesem Compact beschäftigt sich mit der Sicherheitsprophylaxe. Das Spektrum der Themen reicht von richtigen Verhaltensweise nach Angriffen über biometrische Erkennungsverfahren bis hin zu Security-Tools.

5.1 Verhaltensweise nach IT-Angriffen

Wenn es zu einem IT-Zwischenfall in Ihrer Firma kommt, gilt zunächst: Keine Panik. Anschließend sollten Sie nicht selbst Detektiv spielen, sondern einen IT-Forensiker beauftragen. TecChannel sagt Ihnen, was zu tun ist, wenn der Hacker zuschlägt. Wenn es um Computersicherheit geht, denken die meisten Menschen zuerst an Begriffe wie „Firewall“ oder „Virenscanner“ – „IT-Forensik“ hingegen, auch bekannt als Computer- oder Digital-Forensik, ist noch immer eine recht unbekannte Disziplin im Security-Sektor. Ein Grund dafür ist häufig das tiefe Vertrauen in bereits vorhandene Sicherheitsvorkehrungen: Vertrauliche Dokumente werden durch ein durchdachtes User Rights Management, Passwörter, Türschlösser und wachsames Personal geschützt. Zusätzlich wachen Virenscanner darüber, dass sich keine Malware an den Systemen gütlich tun. In vielen Fällen reichen diese Sicherheitsvorkehrungen aber nicht, in noch mehr Fällen sind die genannten Maßnahmen nicht konsequent umgesetzt – wenn also alle Stricke reißen und ein Angriff bereits erfolgt ist, liegt in der IT-Forensik die letzte Hoffnung, entstandenen Schaden zu begrenzen. Dabei geht es auch darum, den Angriff nachzuvollziehen, um Sicherheitslücken zu schließen oder die Schuldigen zu finden.

5.1.1 Hinter den Kulissen

In der öffentlichen Diskussion sind Viren ein beliebtes Thema – über gezielte Angriffe auf Unternehmen liest man jedoch recht wenig. Dabei sind gezielte Angriffe auf Firmen keine Ausnahmeerscheinung. Das Problem ist hier, dass viele Unternehmen gar nicht wissen, dass sie bereits ein Sicherheitsleck haben – ein gestohlenes Notebook ist ein offensichtliches Problem, die heimliche, verschlüsselte Übertragung kritischer Betriebsgeheimnisse hingegen wird vielleicht nie entdeckt.

Zudem haben betroffene Firmen in den meisten Fällen kein großes Interesse daran, solche Vorfälle an die große Glocke zu hängen und dadurch einen erheblichen Imageschaden zu riskieren. Letztlich sind die Medien vornehmlich an großen Meldungen interessiert, wo es um Millionenbeträge geht – was für ein mittelständisches Unternehmen eine Katastrophe sein kann, ist der Presse oft nur eine Meldung im Lokalteil wert. Dennoch werden immer wieder Fälle bekannt,

die aufhorchen lassen: Im Jahr 2002 rächte sich ein unzufriedener Administrator der renommierten Schweizer Bank UBS an seinem Arbeitgeber, indem er eine ganze Reihe von Servern lahm legte. Schaden: rund drei Millionen Dollar. Letztes Jahr sorgte die Geschichte eines deutschen Programmierers für Schlagzeilen, der mit vermeintlichen Werbe-CDs Trojaner in zahlreiche israelische Unternehmen einschleuste. Die im Hintergrund gesammelten Daten (inklusive Screenshots) wurden für monatlich 1.500 britische Pfund an Mitbewerber verkauft.

Woher weiß man aber, ob eine forensische Untersuchung überhaupt Sinn macht? Bei direkter Erpressung oder dem plötzlichen, gleichzeitigen Ausfall wichtiger Systeme ist die Situation klar. Oft sind es aber nur Indizien, die auf Schlimmeres hindeuten. Ist ein Mitbewerber bei Ausschreibungen plötzlich viel erfolgreicher? Wurde nach dem Wechsel auf einen anderen Virenscanner Malware gefunden, es ist aber unklar, wie lange sich das Programm schon im Netzwerk befindet? Oder wurde kürzlich ein Mitarbeiter entlassen, der Zugriff auf wichtige Systeme oder Daten hatte, und dem eine Racheaktion zuzutrauen wäre? In sicherheitskritischen Bereichen kann auch eine routinemäßige forensische Untersuchung Sinn machen, ohne dass ein konkreter Verdacht besteht.

5.1.2 Verhalten im Verdachtsfall

Nehmen wir an, Sie haben einen Verdacht und ziehen eine entsprechende Untersuchung in Betracht. In jedem Fall sollten Sie einige Grundregeln beachten. Der Grund, warum IT-Forensik immer von einem externen Dienstleister durchgeführt werden sollte, ist simpel: In vielen Fällen kommt ein Angriff aus den eigenen Reihen. Wird nun also ein Administrator mit der Lösung des Falls beauftragt, für den er vielleicht selbst verantwortlich ist, wird der Schuldige nie gefunden.

Selbst wenn man seinem Mitarbeiter hundertprozentig vertraut, besteht doch die Gefahr, dass er mangels Erfahrung relevante Spuren übersieht oder sogar unbeabsichtigt verwischt und damit eine spätere professionelle Untersuchung erschwert. Sind Sie der Entdecker des Zwischenfalls, dann sind folgende Punkte zu beachten:

- Wenden Sie sich direkt an den Geschäftsführer
- Erzählen Sie niemandem sonst von Ihrem Verdacht
- Kontaktieren Sie einen professionellen IT-Forensik-Dienstleister
- Versuchen Sie keinesfalls, selbst Spurensuche zu betreiben
- Erstellen Sie eine Liste der möglicherweise betroffenen Systeme

Nun nehmen die Dinge ihren Lauf. Im ersten Schritt wird sich ein professioneller Dienstleister ein genaues Bild über die Situation machen und prüfen, welche Systeme eventuell betroffen sind, bevor er diese überhaupt untersucht. In manchen Fällen ist es sinnvoll, mit weiteren Schritten bis zum Wochenende zu warten, damit Mitarbeiter nicht in die laufenden Untersuchungen involviert werden und aus Angst oder Unbehagen hastig potentielle Spuren verwischen.

5.1.3 Rechnen Sie mit unglaublichen Datenmengen

Die Wichtigkeit einer Situationsanalyse wird deutlich, wenn man sich vor Augen hält, wie viele Datenträger – und damit potentielle Beweismittel – sich durchschnittlich in einem Unternehmen befinden: Festplatten, USB-Sticks, CD-ROMs, PDAs, Mobiltelefone etc. Bei 500 Rechnern mit jeweils 80 GByte kämen alleine hier schon 40 TByte zusammen – das vollständige Kopieren dieser Datenmassen würde Tage dauern, weshalb es so wichtig ist, Prioritäten zu setzen.

Ein Profi wird zudem berücksichtigen, dass Spuren nicht nur in digitaler Form vorliegen können, und – wenn es die Situation erfordert – seinem Kunden empfehlen, die Polizei zur Sicherung und Auswertung physischer Spuren .

Achten Sie außerdem darauf, dass der Dienstleister all seine Schritte sorgfältig protokolliert – und zwar von Anfang an. Am Ende der Untersuchung wird dann ein Abschlussbericht stehen, der idealerweise in zwei Fassungen angeboten wird: einmal für technisch versierte Personen, zum anderen in einer auch für Laien verständlichen Form. Denn sollte es nach der Untersuchung zu einem Gerichtsverfahren kommen, werden Richter und Anwälte Einsicht in die Ergebnisse nehmen und natürlich auch verstehen wollen. Schließlich wird ein Notfallplan erstellt: Welche Systeme sollten umgehend mittels eines Backups wiederhergestellt werden? Welche Computer müssen vorerst komplett abgestellt werden? Ist es notwendig, einzelnen Mitarbeitern den Zugang zu bestimmten Bereichen vorerst nicht mehr zu gestatten? Der Sinn des Notfallplans ist es, weitere Risiken zu minimieren, dabei aber den Betrieb des Unternehmens sicherzustellen.

5.1.4 Die Analyse

Sind diese Punkte abgeschlossen, geht es an die Sicherung der Beweismittel zur anschließenden Analyse. Hierbei wird zwischen Live- und Dead-Analyse unterschieden. Live-Analyse bedeutet, dass im laufenden System analysiert wird. Bei der Dead-Analyse hingegen wird ausschließlich mit den Daten gearbeitet, die auf einem Datenträger gespeichert sind, nachdem der eigentliche Computer abgeschaltet wurde. Sind die wichtigsten Beweismittel gesichert, erhält der Kunde eine Kopie der gesammelten Daten. Die weitere Untersuchung findet in aller Regel allerdings beim Dienstleister statt.

Bei allen Spuren gilt es nun, folgende Fragen zu klären:

- Wer hat es getan?
- Warum wurde es getan?
- Wann wurde es getan?
- Was genau wurde getan?
- Von welchem Ort aus wurde es getan?
- Welche Programme und Hilfsmittel wurden dabei verwendet?

Der Analyst versucht also, den genauen Tathergang möglichst lückenlos nachzustellen beziehungsweise Auffälligkeiten in der Datenflut aufzuspüren. Als Datenquelle dienen ihm dabei komplette Kopien von Datenträgern, Logdateien oder Memory dumps. Vormals gelöschte Dateien werden wieder hergestellt, es wird nach Schlüsselwörtern und Verletzungen von Zugriffserlaubnissen gesucht. Wichtig ist dabei, dass grundsätzlich nie mit den Originaldatenträgern gearbeitet wird. Alle Untersuchungen werden immer an Kopien durchgeführt, nicht zuletzt, weil die Originaldatenträger im Unternehmen meist benötigt werden, während die Untersuchung läuft. Am Ende der Analyse steht schließlich der Abschlussbericht. Im Idealfall konnte festgestellt werden, wer der Angreifer war, was seine Motive waren, was genau passiert ist, in welchem Zeitraum der Angriff stattfand und auch, wie hoch das Restrisiko einzuschätzen ist. Natürlich sollte ein Hinweis nicht fehlen, wie das Unternehmen ähnliche Vorfälle in Zukunft vermeiden kann.

5.1.5 IT-Forensik fordert Vertrauen

Nicht immer können alle Fragen abschließend geklärt werden. Darüber hinaus gibt es aber noch weitere Probleme, über die sich ein Unternehmen im Klaren sein sollte, bevor man eine Untersuchung in Auftrag gibt: IT-Forensik kann nur dann funktionieren, wenn der Analyst auf wirklich alle Daten Zugriff erhält.

Dies erfordert ein hohes Vertrauen in den Dienstleister, bedeutet es doch, dass er unter Umständen brisante Geschäftsgeheimnisse erfährt oder auf Daten stößt, die dem Auftraggeber vielleicht unangenehm sein könnten. Gleiches gilt für die Mitarbeiter selbst – dem IT-Forensiker ist es egal, ob ein Angestellter zum Beispiel Privatbilder seiner Freundin auf dem Arbeitsrechner hat, da diese mit dem eigentlichen Fall nicht viel zu tun haben dürften.

Versuchen Mitarbeiter aber nun voller Panik, solche „Spuren" zu löschen, machen Sie sich unnötig verdächtig, und dem Forensiker entsteht zusätzliche Arbeit. Auch sollte sich der Auftraggeber vor Augen halten, dass ein Analyst zwar feststellen kann, von welchem PC aus ein Angriff erfolgte – dies aber keinesfalls automatisch bedeutet, dass der entsprechende Mitarbeiter auch wirklich der Schuldige ist. Ein weiterer Grund, einen erfahrenen Dienstleister zu wählen, damit durch Übereifer aus einer Untersuchung keine Hexenjagd wird.

5.1.6 Fazit

IT-Forensik ist ein unverzichtbarer Bestandteil der IT-Sicherheit, erfordert aber von allen Beteiligten ein hohes Maß an Vertrauen, Verantwortungsbewusstsein und Fingerspitzengefühl. Wenn diese Voraussetzungen gegeben sind, können Schäden zumindest begrenzt und weitere Risiken für das betroffene Unternehmen minimiert werden. Bereits vor einem Zwischenfall sollte daher jedes Unternehmen gültige IT-Policies definieren (und diese auch durchsetzen!) sowie einen Ab-

laufplan für den Notfall bereit halten. Wer sich hier weiterinformieren will: Auf den Seiten des SANS Institute findet sich zu diesem Thema zahlreiche Anregungen, besonders das Paper Security Incident Handling in Small Organisations ist einen Blick wert. Außerdem stellt die das Institut eine Reihe von Templates für Security Policies zur Verfügung.

Magnus Kalkuhl

Magnus Kalkuhl arbeitet als Viren-Analyst bei Kaspersky Labs Deutschland. Neben der Beobachtung der Malwaresituation in Deutschland, Österreich und der Schweiz widmet er sich vor allem dem Thema Forensik. Weitere Schwerpunkte seiner Tätigkeit sind das Verfassen von Analysen, Feldforschung und eine enge Zusammenarbeit mit Forschungsinstituten.

TecChannel-Links zum Thema	Webcode	Compact
Grundschutz für Web-Applikationen	1785530	S.151
Computer-Forensik: Analyse von Angriffen	402313	–
Sicherheitslücke Roadwarrior	402189	–
Datenrettung: Professionelle Hilfe statt Datenverlust	401608	–
Schutz von Webshops und E-Commerce-Lösungen	1817630	S.37

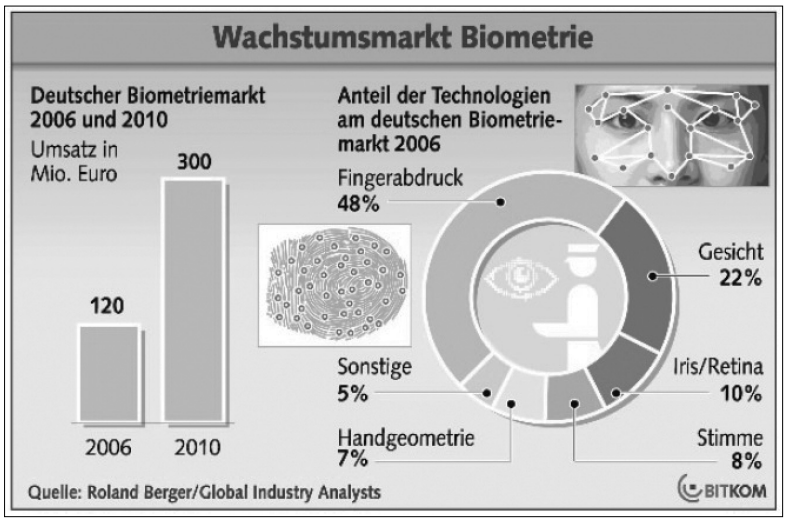
Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

5.2 Von Fingerprint bis Gesichtserkennung

Die biometrische Identifikation per Fingerprint, Gesichtserkennung oder Iris-Scan bietet einen wirksamen Zugangsschutz für PC und Server. Wir erläutern die Vor- und Nachteile sowie Funktionsweisen der einzelnen Biometrie-Verfahren.

Will man der Industrie Glauben schenken, ist der klassische Login an PC-Systemen per Tastatur mit einer Abfolge von Ziffern und Buchstaben bald passé. Denn zukünftig sollen unveränderbare körpereigene Merkmale wie Fingerabdruck, Gesicht, Augeniris, Stimmanalyse oder Schreibverhalten die Zugangsberechtigung ermöglichen. Mehr Schutz vor Missbrauch beziehungsweise unbefugter Benutzung von PC-Systemen ist das Ziel.

Aber nicht nur Computersysteme bieten sich für biometrische Identifikationsverfahren an, sondern auch sicherheitssensitive Dokumente, Institutionen oder Orte. Dazu zählen beispielsweise die EC- oder Kreditkarte, der Reisepass und Personalausweis, Server-Räume, Labore und Banken sowie Flughäfen und Grenzübergänge. Die herkömmliche Methode, die Identifikation von Personen per Ausweis vorzunehmen, ist nicht mehr zeitgemäß und zudem sehr unsicher. Zusätzlich erfordert die traditionelle Zugangsberechtigung beziehungsweise Personenüberprüfung einen hohen personellen und zeitlichen Aufwand.

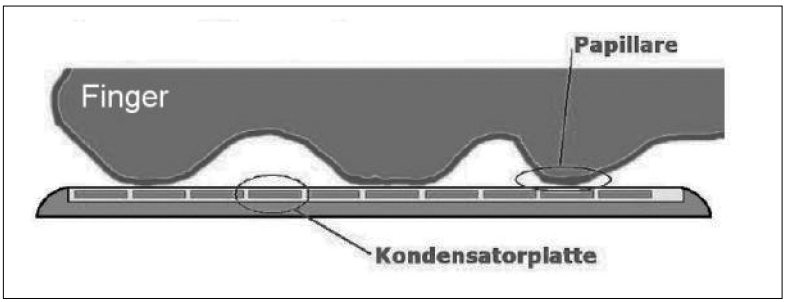


Auf dem Vormarsch: Die biometrische Zugangskontrolle per Fingerabdruck-Identifikation und die Gesichtserkennung beherrschen den Markt. Aber auch andere Verfahren gewinnen Marktanteile. Laut Bitkom soll der Markt für biometrische Verfahren rasant wachsen. (Quelle: Bitkom)

Diese entscheidenden Nachteile können durch den Einsatz von biometrischen Erkennungsverfahren behoben werden. Denn diese überprüfen nicht nur die Gültigkeit der Daten, sondern ermitteln auch, ob die Person berechtigter Besitzer dieser Informationen ist. Somit können biometrische Systeme wie Fingerprint oder Gesichts-Scan in puncto Kosten und Leistungsfähigkeit eine Alternative zu traditionellen Sicherheitssystemen sein oder diese sinnvoll ergänzen. Dieser Artikel informiert Sie ausführlich darüber, welche biometrischen Verfahren derzeit aktuell sind und wie sie im Detail funktionieren.

5.2.1 Optische und kapazitive Fingerprint-Systeme

Die Zugangskontrolle per Fingerabdruck zählt zu der einfachsten und am häufigsten eingesetzten Identifikationstechnik. Um den Fingerabdruck einzulesen, bietet der Markt eine Vielzahl von technologisch unterschiedlichen Systemen an.



Kapazitiver Sensor: Bei dieser Methode dient die Oberflächenbeschaffenheit des Fingerabdrucks als Kontakt und entlädt die Kondensatorplatten unterschiedlich. (Quelle: IFI Zürich)

Am meisten verbreitet ist das Erfassen der spezifischen Fingermerkmale per optischem Sensor. Bei diesem Verfahren wird Licht von einer speziellen Leuchtquelle durch ein Prisma auf die Fingeroberfläche gestreut. Die reflektierten Lichtstrahlen nimmt eine im Gerät integrierte CCD-Kamera auf und verarbeitet die Daten zu einem Schwarzweißbild, das die Besonderheiten des aufgenommenen Profils eines Fingerabdrucks zeigt. Die Auflösung dieser Systeme bestimmen der Sicherheitsgrad und der Verwendungszweck. Bei den kleinen fein strukturierten Fingerkuppen von Kindern wird beispielsweise eine Scantiefe von etwa 1000 dpi empfohlen, bei Erwachsenen genügt bereits eine Auflösung von bis zu 500 dpi.

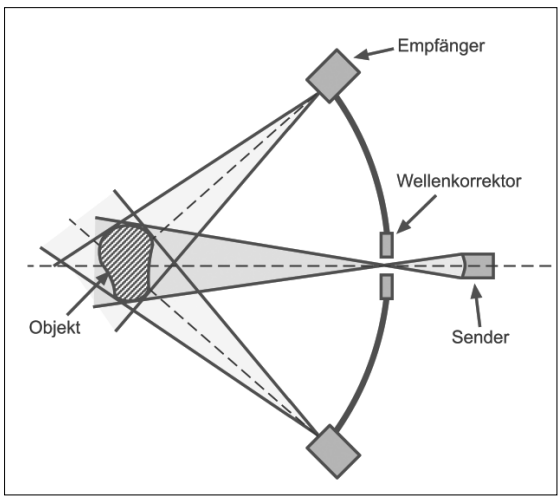
Neben den optischen Erfassungssystemen gewinnen aus Kostengründen immer mehr die kapazitiven Sensoren an Bedeutung. Diese erfassen mittels einer so genannten Scanplatte, in der sich je nach Ausführung über 100.000 kapazitive Sensorelemente befinden, die Fingeroberfläche. Bei dieser Methode dient die Oberflächenbeschaffenheit des individuellen Fingerabdrucks als Kontakt und entlädt die

kleinen Kondensatorelemente unterschiedlich. Die daraus resultierenden Kapazitätsdifferenzen erfasst eine spezielle Elektronik und erzeugt ein Graustufenbild der Fingerrillen. Ähnlich wie das optische System erreicht die kapazitive Methode eine Auflösung von zirka 500 dpi.

5.2.2 Thermo- und Ultraschall-Fingerprint-Systeme

Eine zunehmende Marktrelevanz bei der Fingerabdruckerkennung spielen die komplizierter aufgebauten Ultraschall- und die thermischen Sensoren. Sie haben etwa die gleiche Auflösung wie die kapazitiven und optischen Pendants.

Bei der thermischen Methode erfasst eine spezielle Matrix von Einzelsensoren das Wärmeabbild des Fingers. Bedingt durch die Oberflächenstruktur des Fingers erzeugt der Wärmesensor aus den unterschiedlichen Temperaturgradienten ein dreidimensionales Bild des Fingerabdrucks.



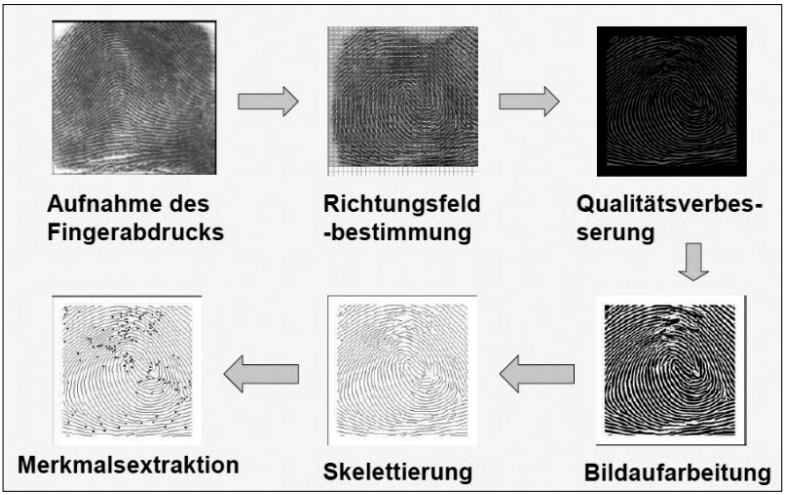
Ultraschall Fingerprint: Schematischer Aufbau eines Gerätes zur Erfassung eines Fingerprints per Ultraschall. (Quelle: Optel)

Die Ultraschallsensoren zählen derzeit zu den sichersten, aber auch teuersten Methoden, um Fingerabdrücke zu erfassen. Der Grund: Die erzeugten Schallwellen lassen sich weder durch Schmutz oder Verletzungen noch durch Schweiß beeinträchtigen. Mehrere unterschiedlich positionierte Sensoren schicken Schallwellen in Richtung der abzutastenden Fingeroberfläche ab.

Die gleichen Ultraschallsensoren empfangen die reflektierten Schallwellen und erzeugen durch die unterschiedlichen Laufzeiten der Signale ein dreidimensionales Bild der Fingeroberfläche.

5.2.3 Analyseverfahren von Fingerabdrücken

Um die Datenmenge eines Fingerabdrucks für eine spätere Nutzung in einer Datenbank möglichst gering zu halten, speichert das System kein 1:1-Abbild des Fingerscans. Es analysiert zwar die gesamte Aufnahme, erfasst aber nur signifikante Merkmale und speichert diese in einem Template ab. Dies ist besonders bei den eingesetzten Identifikationssystemen von Bedeutung, bei denen in kurzer Zeit sehr viele Datensätze miteinander verglichen werden.

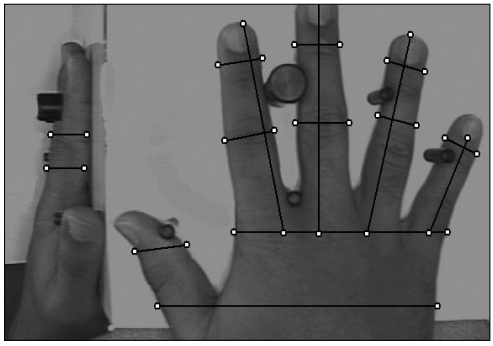


Fingerprint-Analyse: Aus dem eingescannten Fingerprint extrahiert das entsprechende Verfahren besondere Fingerabdruckmerkmale. (Quelle: BioFinger)

Insgesamt verfügt der Fingerabdruck über zirka 35 unterschiedliche spezielle Ausprägungen (Minutien) wie Kreuzungen, Endungen, Verzweigungen oder Punkte. Zu einer eindeutigen Identifikation genügt es in der Regel, 8 bis 22 Merkmale zu überprüfen. Das Template eines Fingerabdrucks ist entweder direkt im Gerät gespeichert, liegt auf einer SmartCard oder zentral auf einem Server. Stimmen bei einem Vergleich die erfassten Identifikationspunkte mit den gespeicherten innerhalb einer festgelegten Toleranz überein, wird der Zugang gewährt. In der Biometrie heißt das Analyseverfahren Minutiae-Based Fingerprint Matching (MBFM). Es erfordert durch die Extrahierung der einzelnen Minutien einen erhöhten Aufwand der Bildbearbeitung und Auswertung. Einen anderen Ansatz bietet das Correlation Based Fingerprint Matching (CBFM). Statt einzelne Merkmale mit der Referenz zu vergleichen, benutzt es charakteristische Bildausschnitte als Referenz und vergleicht diese Bildfragmente mit dem aufgenommenen Fingerprint. Stimmt der Mustervergleich, erfolgt die Zugangsberechtigung.

5.2.4 Handgeometrie

Wie bei der Gesichtserkennung verwendet auch das Handgeometrie-Verfahren ein optisches System in Form einer CCD-Kamera, um die spezifischen Merkmale einer Hand abzubilden. Dabei werden der Handrücken und über Spiegel die Seitenansicht der Hand optisch aufgenommen und ausgewertet.



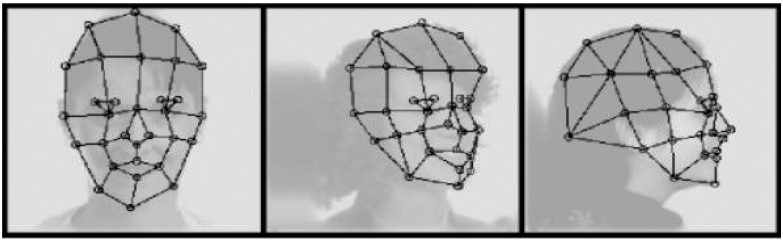
Alles aus einer Hand: Auf das eingescannte oder fotografierte Abbild der Handgeometrie werden zu Analysezwecken Linien und Knotenpunkte gesetzt. (Quelle: Biometrics)

Auf das Abbild der Hand werden nach einem bestimmten Analyseverfahren Knotenpunkte und Linien gesetzt. Sie dienen zur Messung der Länge, der Breite und der Dicke der einzelnen Finger. Diese Daten der Handcharakteristik speichert das Erfassungssystem in einer Datenbank ab. Bei der Verifikation eines Benutzers vergleicht das System unter Berücksichtigung einer gewissen „Unschärfe" die aktuellen Informationen mit denen in der Datenbank.

5.2.5 2D-Gesichtserkennung

Zu den einzigartigen Merkmalen eines Gesichts gehören Kinn, Mund, Nase, Augen und Stirn. Hinderlich bei der Gesichtserkennung wirken sich veränderliche Merkmale wie Bartwuchs, eine Brille oder wechselnde Lichtverhältnisse aus. Deshalb muss das Identifikationssystem aus dem aufgenommenen Kamerabild diese veränderbaren Informationen extrahieren und sich bei der Analyse auf die eindeutigen Parameter des Gesichts beschränken. Zusätzlich ist die unterschiedliche Mimik bei der Gesichtserkennung zu berücksichtigen. Für zuverlässige Ergebnisse bedient sich die Gesichtserkennung zweier Verfahren: Elastic Graph Matching und Eigen-Faces. Das Elastic Graph Matching erfasst besondere Merkmale des Gesichts mit Hilfe von Graphen. Dabei wird ein Gitter über das Gesicht gelegt. Das Verfahren platziert die Knotenpunkte des Gitters auf die markanten Gesichtselemente wie Augen, Mundwinkel oder Nasenspitze. Die ausgewählten Gesichtspunkte bilden ein „verbogenes" elastisches Gitter mit festen Relationen. Diese feste Beziehung bleibt auch bei Verzerrungen durch wechselnde Mimik oder

veränderte Kamerapositionen erhalten. Innerhalb des aufgenommenen Vergleichsbildes gilt es, die festgelegten Knotenpunkte zu finden und aufzutragen. Anschließend vergleicht das Verfahren die gefundenen Merkmale mit einer abgespeicherten Referenz und ermittelt den Grad der Gitterverbiegung bei einer optimalen Übereinstimmung der beiden Bilder. Die daraus resultierenden Ergebnisse bewerten die Übereinstimmung der Gesichtsgeometrien.

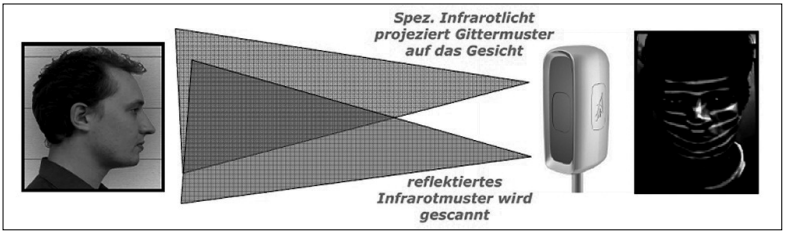


Gesichtserkennung: Das Verfahren platziert Knotenpunkte auf markante Stellen des Gesichts, um die Gesichtsgeometrien metrisch zu erfassen. (Quelle: INI Bochum)

Die Eigen-Faces-Methode versucht, das gescannte Gesicht durch die Kombination von einem bestimmten Datensatz an gespeicherten Basisgesichtern (zirka 100 fremde Referenzgesichter) sowie deren Projektionen und Verzerrungen möglichst originalgetreu nachzubilden. Der daraus resultierende Merkmalsvektor des Gesichts ist ein Maß für die Übereinstimmung.

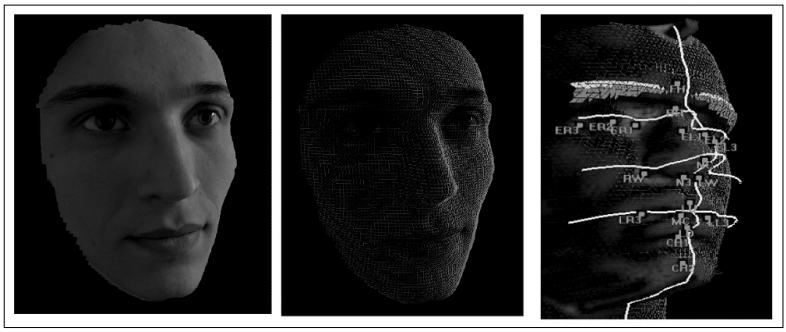
5.2.6 3D-Gesichtserkennung

Anders als die 2D-Gesichtserkennung erfordert das 3D-Verfahren einen wesentlich komplizierten gerätetechnischen Aufwand. Dafür bietet diese Methode mehr Toleranz bei der Aufnahme des Objektes und eine höhere Erkennungssicherheit. Das 3D-Gesichtserfassungssystem besteht aus einem Infrarotlicht-Sender und einem entsprechenden Scanner als Empfänger.



3D-Verfahren: Ein System aus Infrarotlichtsender und einem entsprechenden Scanner bildet das Herzstück der 3D-Gesichtserfassung. (Quelle: Unisys)

Der Sender projeziert ein für das menschliche Auge unsichtbares Infrarotlicht-Gittermuster auf das Gesicht einer Person. Das von der Oberfläche des Gesichts reflektierte Infrarotmuster wird von einem speziellen Scanner erfasst und in Bildinformationen umgerechnet. Die Erfassungsgeschwindigkeit entspricht dabei einem Real-Time-Video mit 25 Bildern pro Sekunde. Daraus resultieren die Vorteile dieses 3D-Verfahrens wie schnelle Erkennungszeit und die relative Unabhängigkeit von Gesichtsbewegungen. So reichen 2-3 Sekunden aus, um eine Person zu erfassen. Die Identifikation durch das System dauert nicht länger als 1/10 Sekunde. Das Kamerasystem ist relativ handlich und unauffällig montierbar. Der Betrachtungswinkel des optischen Systems ist unkritisch. Auch Spiegelungen oder schlechte Beleuchtung sind bei diesem Verfahren nicht von Bedeutung. Zusätzlich arbeitet das System berührungslos und bietet so eine hohe Benutzerakzeptanz.



3D-Analyse: Aus einem 3D-Gesichts-Scan erzeugt das System Vektorpunkte, die zur Identifikation der erfassten Person benutzt werden. (Quelle: Unisys)

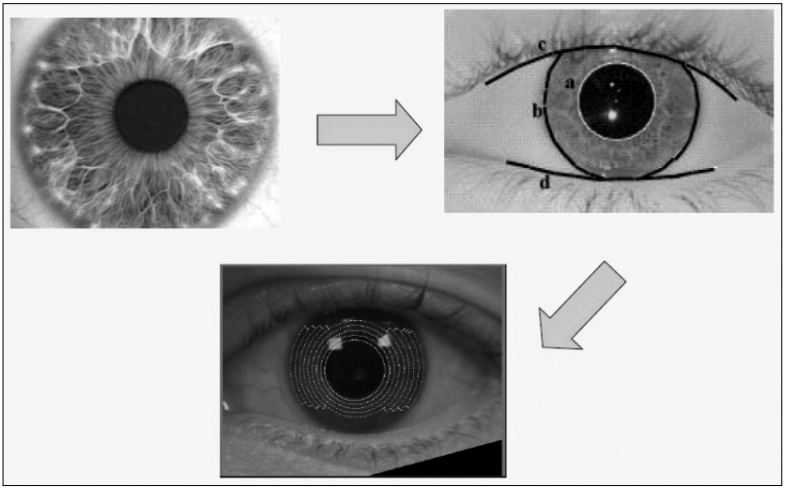
Um eine sichere Identifizierung oder Verifizierung einer Person durchzuführen, speichert das System eine benutzerdefinierte Anzahl von Referenzbildern mit den entsprechenden 3D-Vektoren ab. Das System vergleicht bei einer Identifizierung das erfasste Bild mit mehreren oder allen Referenzbildern und errechnet daraus eine Erkennungswahrscheinlichkeit.

5.2.7 Iriserkennung

Die Iris beziehungsweise Regenbogenhaut ist ein ringförmiger Augenmuskel zwischen Hornhaut und Linse. Sie besteht aus zirka 266 individuellen komplexen Mustern wie Furchen, Bändern, Gruften und Stegen und bietet somit ideale Voraussetzungen, sie als einzigartiges Identifikationsmerkmal zu nutzen.

Da die Irisgröße vom Lichteinfall abhängt, ist bei der Iriserkennung die Umgebungshelligkeit wichtig. Darüber hinaus benötigt der Sensor eine gewisse Grundhelligkeit, um beim Scannen die einzelnen Merkmale eindeutig zu erfassen. Das

Erfassungssystem (Sensor) besteht aus einer herkömmlichen CCD-Kamera, die berührungslos aus einer Entfernung von 10 bis 50 cm das Auge als Schwarzweißbild aufnimmt. Als Lichtquelle dient eine blendungsfreie Infrarot-Lampe, um eine gewisse Unabhängigkeit vom Umgebungslicht zu erreichen.



Augen auf: Das Iriserkennungsverfahren legt die Abmaße der Iris fest und generiert aus den Merkmalen einen digitalen Code (Bild links oben). (Quelle: TAB Arbeitsbericht 76)

Zur Analyse des Bildes legt das Erfassungssystem ein Gitter über die Aufnahme. Es bestimmt den Mittelpunkt der Iris und legt die Radien der Irisränder fest. Ein Algorithmus kodiert die dunklen und hellen Muster des Irisrings in ein digitales Format. Beim Identifikationsvorgang wird der erfasste Iriscode mit dem in einer Datenbank abgelegten Datenstamm verglichen.

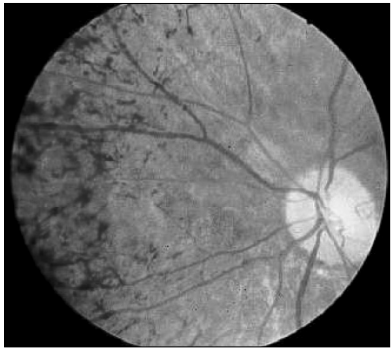
Ob eine Übereinstimmung der beiden Datensätze vorliegt, muss der Anwender vorher festlegen, indem er einen Schwellwert für die Hamming-Distanz vorgibt. Die Hamming-Distanz gibt an, in wie vielen Bits sich zwei gleich lange Binärwörter unterscheiden. Je geringer die Hamming-Distanz, desto mehr Übereinstimmungen sind vorhanden. Für die Iriserkennung bedeutet das: Liegt die ermittelte Hamming-Distanz der beiden digitalen Datensätze unterhalb des festgelegten Grenzwerts, so gilt die Person als identifiziert.

5.2.8 Retina-Scan

Mit der Retina-Erfassung wird ein Muster der Blutgefäße im Augenhintergrund für biometrische Zugangsysteme verwendet. Das Verfahren arbeitet berührungslos und benutzt ein optisches System zur Erfassung der biometrischen Merkmale.

Das retinale Blutadermuster im menschlichen Auge bleibt auch bei Alterung oder bei Krankheit unverändert und ist in der Natur einzigartig. Damit bietet es die besten Voraussetzungen, um es für biometrische Zugangssysteme zu verwenden.

Bei der Retina-Erkennung nutzen die optischen Systeme Infrarotlicht, das den Augenhintergrund ausleuchtet. Das reflektierte Licht erfasst ein Scanner und verarbeitet die Bildinformationen in einen Datensatz. Dieser Datensatz kann dann mit einem entsprechenden Referenzdatensatz einer zu identifizierenden Person verglichen werden.



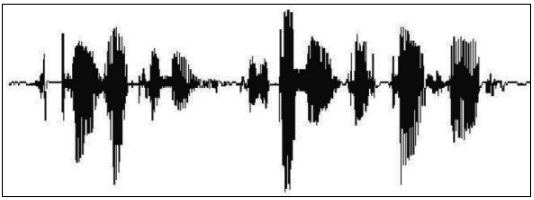
Augen auf: Beim Retina-Scan werden die Blutgefäße des Augenhintergrunds zur biometrischen Analyse herangezogen. (Quelle: TBS)

Das Verfahren der Retina-Erkennung ist relativ Fälschungssicher und besitzt eine geringe Fehlerrate. Darüber hinaus belastet der erzeugte Datensatz durch seine geringe Größe nicht die Speicherressourcen des Systems. Allerdings besitzt die Retina-Erfassung eine geringe Benutzerakzeptanz, da während des Erfassungsvorganges der Kopf einen bestimmten Abstand zum Erfassungsgerät haben muss und während des Scan-Vorgangs nicht bewegt werden darf. Auch eine Brille akzeptiert das System nicht. Weitere Nachteile sind die aufwendige Erfassungsapparatur und die damit verbundenen hohen Kosten.

5.2.9 Stimmidentifikation

Bei der Stimmerkennung benutzt man die Stimmverifikation, den Vergleich mit einer textabhängigen Referenzprobe. Zusätzlich kommt die Stimmidentifikation zum Zuge. Hierbei erfolgt der Stimmvergleich textunabhängig. Beide Verfahren nutzen die personenbezogene und eindeutige Charakteristik der Sprache aus.

Um Störungen zu vermeiden, dient als Aufnahmegerät ein qualitativ hochwertiges Mikrofon. Die gesprochenen Wörter speichert das Verfahren zeit- und Amplituden-abhängig in ein Frequenz-Spektrogramm. Nach einer Zeitnormierung der aufgezeichneten Stimmprobe vergleicht das System die entsprechenden Frequenzen und Amplituden mit dem abgespeicherten Referenzsignal.

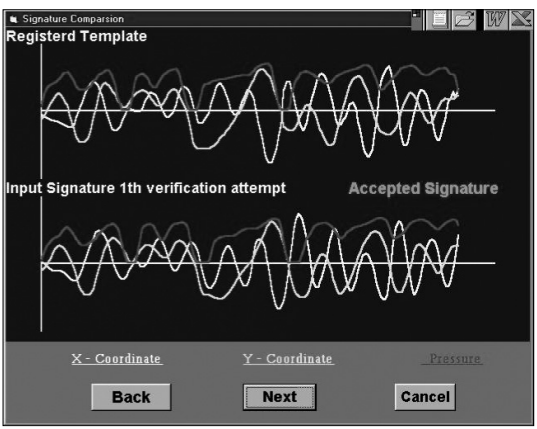


Stimmenanalyse: Das Frequenz-Spektrogramm der Sprache lässt sich gut zur Stimmerkennung für biometrische Zugangskontrollen nutzen. (Quelle: Universität Hamburg)

Da die Sprache ein dynamischer Vorgang ist, wirkt sich zum Beispiel eine Erkältung oder Heiserkeit besonders negativ auf die Lautstärke oder die Deutlichkeit des artikulierten Worts aus. Allerdings bleiben die typischen Charakteristika wie Akzent, Betonung oder Sprechgeschwindigkeit nahezu unverändert und ermöglichen somit eine gute Stimmerkennung. Beim Vergleichen zweier Sprachmuster muss ein Toleranzwert vorgegeben werden. Dieser Wert legt fest, bei welcher Ungenauigkeit das System die Sprachaufnahme als identifiziert erkennt.

5.2.10 Unterschriftenerkennung

Das biometrische Verfahren zur Unterschriftenerkennung nutzt das dynamische Schreibverhalten eines Benutzers. Es analysiert dabei die Bewegung des Stifts in x- und y-Richtung und den Druck des Schreibgeräts auf die Unterlage in Abhängigkeit von der Zeit. Beim Erfassen und Digitalisieren der Stiftbewegung kommen spezielle Druck- beziehungsweise Bewegungssensoren zum Einsatz. Diese befinden sich entweder in der Schreibunterlage oder in einem speziellen Stift. Sie liefern die zeitkorrelierten Parameter Druck, Bewegungsrichtung und Geschwindigkeit. Eine spezielle Analyselogik extrahiert die typischen Merkmale der getätigten Unterschrift und erstellt einen spezifischen Merkmalsvektor.



Schriftanalyse: Bei der Unterschriftenerkennung entscheidet der Grad der ermittelten Übereinstimmungen von dynamischen Parametern wie Bewegungsrichtungen, Schreibgeschwindigkeit oder Schreibdruck, ob die Unterschrift echt ist. (Quelle: Cyber SIGN)

Das bedeutet aus der Sicht des Anwenders, dass die Informationen seiner Schreibdynamik in Echtzeit erfasst werden, um daraus die notwendigen Parameter für eine Identifikation zu errechnen. Die so gewonnenen Werte beziehungsweise den Merkmalsvektor seiner individuellen Unterschrift vergleicht das System mit den bereits abgespeicherten Referenzdaten und wertet diese aus.

Je höher dabei die Anzahl der übereinstimmenden dynamischen Schreibmerkmale ist, desto wahrscheinlicher stimmen die Unterschriften überein. Die Toleranzgrenze für den Grad der Übereinstimmung oder auch Echtheit legt nicht das System fest, sondern der Anwender.

5.2.11 Venen- oder Aderscan

Die Venen beziehungsweise Adern unter der Haut sind bei jedem Menschen – ähnlich einem Fingerabdruck – unterschiedlich. Adermuster sind sogar unter eineiigen Zwillingen einzigartig. Das Einzige, was sich im Laufe der Entwicklung eines Menschen an ihnen verändert, ist ihre Größe. Diese Eigenschaft macht sich die Venenscan-Technologie zunutze, die die Forscher von den Fujitsu Laboratories (www.fujitsulabs.com) entwickelt haben.

Beim Venenscan-Verfahren werden die Handflächen mit infrarotem Licht kontaktlos bestrahlt. Dabei treten die direkt unter der Hautoberfläche verlaufenden Adern als Muster hervor. Diese Strukturen erfasst ein Bildsensor und vergleicht sie mit der zuvor gespeicherten „Venen-Karte“ des Benutzers. Beim Auftreffen des Lichts sind die Venen als dunkle Reflexion sichtbar.

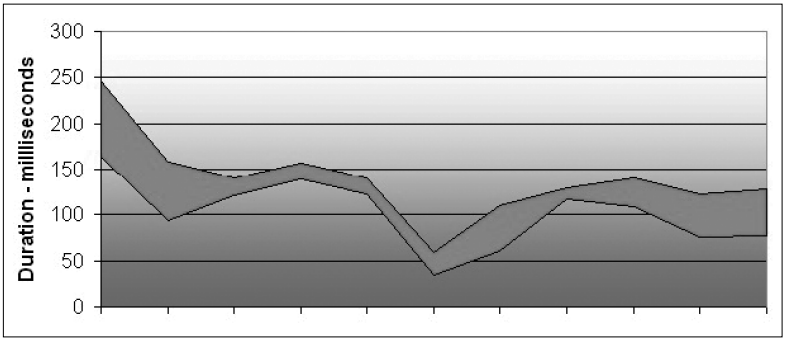
Venenscan: Das Verfahren erkennt mittels Infrarotlicht und Bildsensor den Verlauf der Blutgefäße unter der Haut und kann es zur Authentifizierung von Personen mit einem entsprechenden Referenzmuster vergleichen. (Quelle: Fujitsu)

Im Detail funktioniert die Venenerkennung wie folgt: Das desoxydierte Hämoglobin in den Blutadern und besonders in den Verzweigungen der Gefäße absorbiert das Licht in einem definierten Spektrum. Dieses liegt innerhalb des Nahinfrarotbereichs bei einer Wellenlänge von ungefähr 7,6 x 10^-4 Millimeter. Der Bildsensor erkennt die Blutgefäße als dunkle Linienmuster und speichert die Bildinformationen als Referenzmuster ab.

Ein Vorteil des Adererkennungssystems ist, dass es ohne physikalischen Kontakt funktioniert und daher auch den positiven Hygieneaspekt erfüllt. Zusätzlich besitzt die Technologie eine hohe „Trefferquote". So liegen die falsche Ablehnungsrate des Verfahrens bei weniger als 0,01 Prozent und die falsche Annahmerate bei 0,00008 Prozent. Laut Fujitsu ist die kontaktlose Venenerkennung besonders für den kommerziellen Bereich interessant. Als eine Alternative zu bisherigen biometrischen Systemen wie Fingerabdruckerkennung soll sie sicherer und weniger anfällig für Fälschungen sein. So arbeiten bereits einige Banken in Japan mit dem Aderscanverfahren, um Angestellte und Kunden eindeutig zu authentifizieren.

5.2.12 Tastentippdynamik-Verfahren

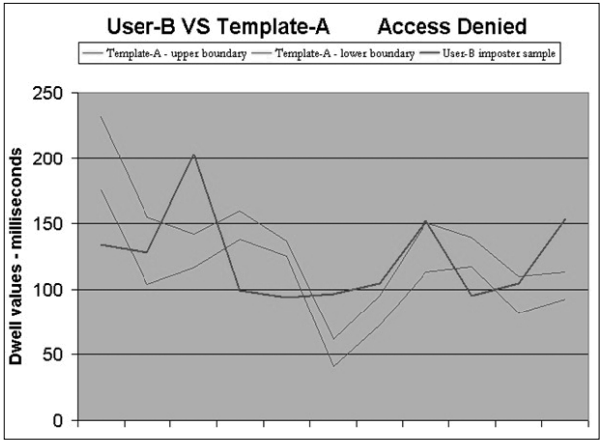
Die Tastentippdynamik-Analysemethode gehört zu den jüngsten biometrischen Systemen im Computersicherheitsbereich. Wie der Name suggeriert, analysiert dieses Verfahren die Eigenheiten des Benutzers, wie er Buchstaben und Zahlen auf der Tastatur tippt. Das System kann in Form einer separaten oder integrierten Tastatur sowie einer speziellen Geräte-Firmware oder speziellen Software auf den Markt kommen. Die Methode der Tastentippanalyse überwacht bei der Eingabe per Tastatur zirka 1000 Mal pro Sekunde die dynamischen Parameter wie die „Flugzeit" der Finger und die Andruckdauer der betätigten Tasten. Dabei wird ein bestimmtes Passwort oder eine vereinbarte Zeichenfolge über eine Tastatur eingegeben und vom System analysiert. Alle so gewonnenen Daten speichert das System als ein sogenanntes Template ab, dieses dient später als Referenzmuster zur Authentifizierung des Benutzers.



Referenzmuster: Das Tippverhalten einer bestimmten Zeichenfolge wird beim Tastentippdynamik-Verfahren als sogenanntes Template gespeichert. Es dient als Referenzmuster zur Authentifizierung des Anwenders. (Quelle: BioPassword)

Um eine Referenzschablone (Template) zu erstellen, benötigt das System eine Mindestanzahl an eingegebenen Zeichen. Das sind typischerweise acht Zeichen,

empfohlen sind zwölf und mehr. Diese können aus einer oder aus bis zu sechs unterschiedlichen Eingabefeldern wie User-Passwort-, Login- oder E-Mail-Eingabefeld stammen. Um die Genauigkeit und die Trefferquote weiter zu steigern, koppelt man das Verfahren mit einer adaptiven Lerntechnologie. Das heißt, je häufiger ein Benutzer seine Authentifizierungsprozedur durchführt, desto exakter und zuverlässiger arbeitet das System. Das biometrische Verfahren der Tastentippdynamik arbeitet mit einer durchschnittlichen Fehlerrate von drei Prozent.



Tippvergleich: Das Tippverhalten des Anwenders bei der Tastentippdynamik-Technologie wird mit einem Referenzmuster verglichen. Je nach Übereinstimmungsrate gewährt oder verweigert das System die Zugangsberechtigung. (Quelle: BioPassword)

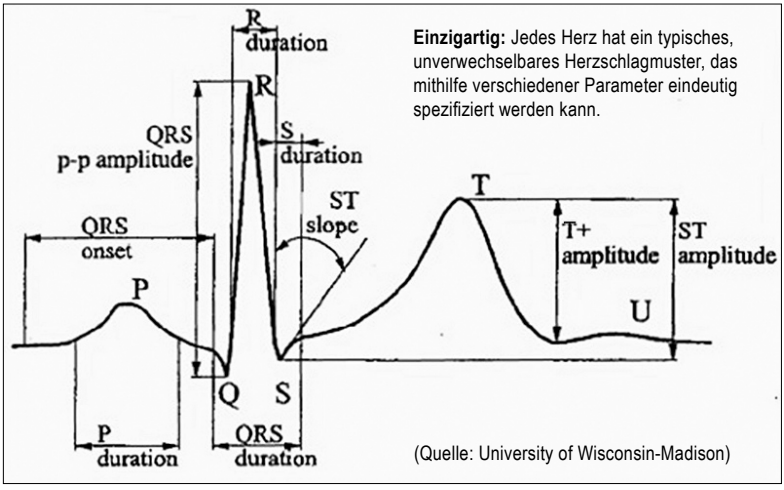
Die Zugangssicherheit durch das Tastentippverhalten kann durch eine Kombination mit benutzerspezifischen Fragen erhöht werden. Da die Antworten nur der Anwender kennt und diese als Tastentipp-Referenz hinterlegt sind, erschwert das System somit zusätzlich einen möglichen Missbrauch.

5.2.13 Personenerkennung durch Herzschlaganalyse

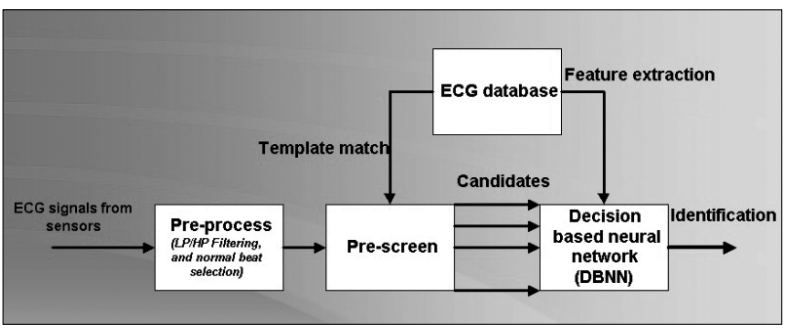
Die Universität von Wisconsin-Madison (www.wisc.edu) geht in puncto biometrische Erkennungsverfahren neue Wege. Die Forscher nehmen sich das menschliche Herz vor. Sie haben erwiesen, dass jedes Herz ein typisches, unverwechselbares Herzschlagmuster aufweist. Diese Erkenntnis machen sie sich zunutze, um ein preiswertes Messverfahren zu entwickeln, das für eine biometrische Authentifizierung anwendbar ist.

Wie bei nahezu allen biometrischen Verfahren erstellt das System zuerst ein Referenzmuster des Herzschlages. Hierbei werden spezifische Parameter des Herzschlages mithilfe eines handelsüblichen Sensors – ähnlich wie bei einem Elektrokardiogramm (EKG) – unter verschiedenen physischen Bedingungen gesammelt. Das aufgenommene Kardiogramm beziehungsweise die entsprechenden Parame-

ter werden wie bei allen biometrischen Verfahren als Template in einer Datenbank hinterlegt. Es dient als Referenzmuster für eine Vergleichsanalyse.



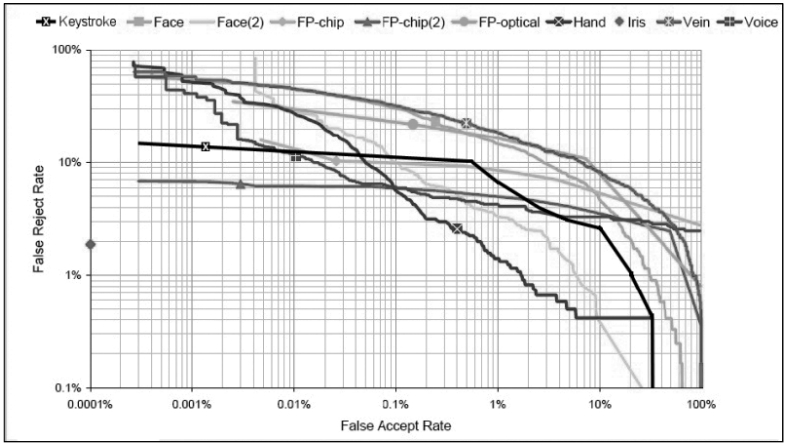
Um eine möglichst hohe Trefferquote beziehungsweise Erkennungsrate zu erzielen, sind das Pre-Prozessing und das Pre-Screening besonders wichtig. In diesen Stufen wird das Herzschlagsignal durch Filter und spezielle Selektion so aufbereitet, dass es in einer nachgeschalteten Erkennungsstufe mit den in einer Datenbank abgelegten Mustern verglichen werden kann. Allerdings ist dieses Verfahren noch relativ unsicher und steht am Anfang der Entwicklung. Doch die Forscher sind sich einig, dass die Authentifizierung mittels Herzschlag in der Praxis möglich ist.



Systemdiagramm: Ein komplexes Analyseverfahren wertet das EKG eines Herzens aus und kann diese gewonnenen Informationen zur Authentifizierung von Personen nutzen. (Quelle: University of Wisconsin-Madison)

5.2.14 Biometrische Systeme im Vergleich

Das nachfolgende Diagramm zeigt die Relation der unterschiedlichen biometrischen Verfahren in Bezug auf falsche Ablehnungsrate und falsche Annahmerate. Diese Faktoren sollten möglichst optimal miteinander korrelieren. Das heißt: Je höher zum Beispiel die False Reject Rate (100 Prozent) desto niedriger sollte die False Accept Rate (0 Prozent) sein.



Vergleich: Im Diagramm sind einige biometrische Verfahren in Bezug auf die Wechselwirkung zwischen falscher Ablehnungsrate und falscher Annahmerate gegenübergestellt. (Quelle: BioPassword)

Die Tabelle gibt einen Überblick über alle wichtigen biometrischen Verfahren. Wir erläutern kurz die Funktionsweise der einzelnen biometrischen Systeme und stellen in Stichpunkten deren Vor- und Nachteile vor.

Wichtige biometrische Verfahren im Überblick

Verfahren	Erläuterung	Vor-/Nachteile
Fingerabdruck	Fingerabdrücke sind von Mensch zu Mensch unterschiedlich und eignen sich zur physiologischen Erkennung	Vorteil: niedrige Falscherkennungsraten von bis zu 1:1.000.000; Nachteil: große Hemmnisse bei den Benutzern hinsichtlich der Persönlichkeitsrechte
2D-Gesicht / 3D-Gesicht	Erkennung erfolgt anhand der persönlichen Gesichtsmerkmale	Vorteil: völlig berührungsfrei, fehlertolerante 3D-Gesichtserkennung; Nachteil: umfangreiche Datensätze erfordern schnelle und teure Systeme. Datenschutzrechtliche Probleme

Hand	Geräte erfassen die Abmessungen der Finger und die Dicke der Hand	Vorteil: schon seit mehr als zehn Jahren im Einsatz; Nachteil: Die geometrischen Abmessungen von menschlichen Händen unterscheiden sich nicht genügend
Herzschlag	Ein Gerät, ähnlich einem EKG-System, erfasst die Herzsignale	Noch in der Entwicklungsphase
Iris (Netzhaut)	Die Augennetzhaut wird mittels eines Laserstrahls oder per Infrarot-Licht abgetastet	Vorteil: sehr fälschungssicher, niedrige Falscherkennungsraten von bis zu 1:1.000.000; Nachteil: Ängste der Benutzer, die Augen mittels Laser abtasten zu lassen
Retina (Augenhintergrund)	Die Augenhintergrund wird mittels Infrarotlicht und eines Scanners erfasst	Vorteil: sehr fälschungssicher, niedrige Falscherkennungsraten; Nachteil: Ängste der Benutzer, die Augen mittels Infrarotlicht abtasten zu lassen
Stimme	Spektralanalyse eines (meist vorbestimmten) gesprochenen Worts	Vorteil: wird vom Benutzer akzeptiert; Nachteil: Problem der Trennung variabler und invarianter Sprachmerkmale bei der Erkennung sowie hoher Zeitbedarf
Tippverhalten	Das Verfahren analysiert die dynamischen Parameter wie die „Flugzeit" der Finger und die Andruckdauer der betätigten Tasten.	Vorteil: preiswert, wird vom Benutzer akzeptiert; Nachteil: lange Anlernzeit, ungenau durch verändertes Tippverhalten
Unterschrift	Erkennung der charakteristischen Unterschriftenmerkmale wie Dynamik des Schreibstiftes	Vorteil: wird vom Benutzer akzeptiert; Nachteil: Problem der Trennung variabler und invarianter dynamischer Schriftmerkmale bei der Erkennung, hoher Zeitbedarf
Venenscan	Der Handrücken wird mittels einer Infrarotlampe und eines Sensors abgetastet	Vorteil, berührungslos, hohe Akzeptanz; Nachteil: aufwendige und teure Geräte

5.2.15 Fazit und Ausblick

Es gibt es eine Vielzahl funktionsfähiger biometrischer Erfassungssysteme. Alle haben eines gemeinsam: Sie verwenden unveränderbare individuelle Körper- und Verhaltensmerkmale. Zu den am weitesten entwickelten biometrischen Technologien zählen zurzeit Systeme, die Daten von Fingerabdrücken, Gesichtsscans, Netzhaut- und Irismuster sowie von Stimmaufnahmen und Unterschriften aufnehmen, analysieren und mit einer Datenbank vergleichen. Stimmen die Merkmale zu einer gewissen Prozentzahl überein, erfolgt eine Zugangsberechtigung. Mit der Einführung von biometrischen Zugangssystemen soll künftig das lästige

Eingeben von Logins und Passwörtern wegfallen. Ein Fingerabdruck auf einem Scanner oder ein freundliches Lächeln in eine Kamera genügt, um eine Zugangsberechtigung zum PC zu bekommen oder auf Flughäfen die Eingangskontrollen zu passieren. Zusätzlich sollen die biometrischen Systeme mehr Sicherheit vor Missbrauch bieten als die herkömmlichen Verfahren.

Aber auch die Biometrie ist nicht zu hundert Prozent sicher – ein Restrisiko durch Missbrauch bleibt auch bei dieser Technologie bestehen. Erst die Kombination mehrerer Biometrie-Verfahren, wie zum Beispiel Gesichtserkennung und Fingerprint, maximieren die Sicherheit. In vielen Bereichen wie Banken, Flughäfen und Zugangskontrollen in Unternehmen werden heute bereits biometrische Verfahren wie die Fingerabdrucküberprüfung oder die Gesichtserkennung zur Personenauthentifizierung eingesetzt. In anderen Anwendungsgebieten wird die Biometrie nur langsam akzeptiert. Hier gilt der Grundsatz: Ist die biometrische Zugangskontrolle wie zum Beispiel Single Sign On in Verbindung mit Fingerprint-Verfahren leichter und bequemer als herkömmliche Zugangstechnologien wie Passwort und Chipkarte, so ist die Akzeptanz beim Anwender höher.

Bernhard Haluschak ist als Hardware-Redakteur bei TecChannel tätig. Der Dipl. Ing. (FH) der Elektrotechnik / Informationsverarbeitung blickt auf langjährige Erfahrungen im Server-Umfeld und im Bereich neuer Technologien zurück. Vor seiner Fachredakteurslaufbahn arbeitete er in Entwicklungslabors, in der Qualitätssicherung sowie als Laboringenieur in namhaften Unternehmen.

TecChannel-Links zum Thema	Webcode	Compact
Von Fingerprint bis zur Gesichtserkennung	402320	S.156
Sicher durch Biometrie	401777	–
RFID – Die technischen Gundlagen	431196	–
Elektronisch unterschreiben	401388	–
Kryptographie-Grundlagen	401402	–

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

5.3 Certgate Protector: Smartphones sicher betreiben

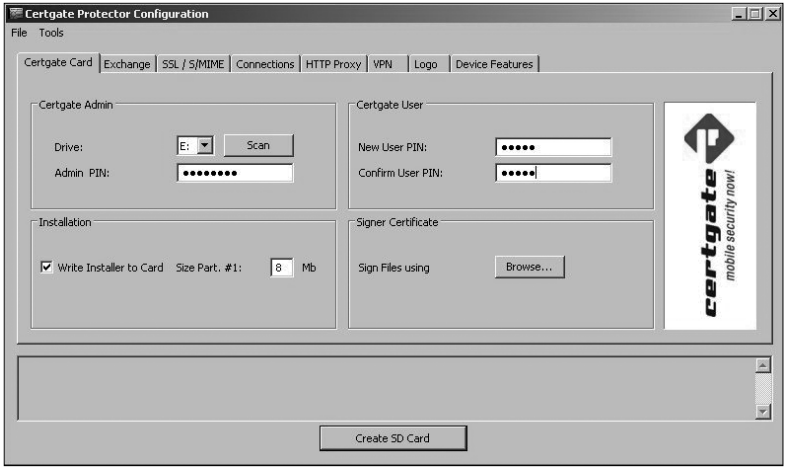
Eigentlich ist in vielen Unternehmen in Sachen Sicherheit ein schlüssiges Konzept vorhanden. Selbstredend ist das Netzwerk gegen Angriffe von außen mit einer Firewall ausgestattet, Verbindungen ins LAN werden nur per VPN oder SSH realisiert. Die internen Server und PCs sind mit ausreichender Sicherheitssoftware ausgestattet und der Webzugriff aus dem LAN ins Internet läuft über einen Proxy. Die Mitarbeiter mit Notebooks verwenden üblicherweise eine Verschlüsselungslösung. Inzwischen nutzen jedoch mobile Mitarbeiter in der Regel Smartphones, die ebenso unternehmenskritische Daten beherbergen können. Diese sind häufig nicht schlüssig in ein Sicherheitskonzept eingebunden. Der Verlust, der auf diesen Geräten gespeicherten Daten, kann aber ebenso dramatische Folgen haben. Nicht umsonst, ist bei hochrangigen Mitarbeitern der Einsatz entsprechender Geräte umstritten. Das Nürnberger Unternehmen Certgate hat mit dem Certgate Protector eine Sicherheitslösung für Smartphones entwickelt. Damit lassen sich Daten sowie E-Mails auf dem Smartphone verschlüsseln. Zudem kann man einzelne Funktionen wie Bluetooth, ActiveSync-USB oder automatische Updates deaktivieren. Die Sicherheitslösung funktioniert folgendermaßen: Windows Mobile besteht aus dem Windows-CE-Kernel, um das herum das mobile Betriebssystem angelegt ist. Von diesem Gebilde wiederum gehen Programmierschnittstellen ab, etwa zu Bluetooth, zum User Interface oder zum GSM-Stack. Hier greift der von Certgate entwickelte und in der Lösung integrierte Kernel-Protector ein: Nach der sicheren Aktivierung durch den Nutzer legt er sich wie ein Schutzmantel um den Windows-CE-Kernel und verhindert Manipulationen in der Gerätekonfiguration. Das Sicherheitsniveau ist dabei individuell festlegbar.

Basis des Certgate Protector ist eine MicroSD-Card. Diese beinhaltet einen integrierten Kryptoprozessor mit der Zertifizierung EAL 4+ (Evaluation Assurance Level). Dieser Prozessor generiert digitale Schlüsselpaare (RSA 2048 Bit) und speichert diese. Die auf der Smartcard abgelegten Zertifikate und Schlüssel werden zur Verschlüsselung der gesamten Benutzerdaten genutzt. Damit sind die Daten selbst bei Verlust des Gerätes zuverlässig gegen unautorisiertes Auslesen geschützt sind. Darüber hinaus werden sie zur Verschlüsselung und Signatur von E-Mails und für den Zugriff auf ein gesichertes Netz (VPN) oder geschützte Internet-Seiten (SSL) eingesetzt. Bislang unterstützt die Certgate-Lösung Geräte ab Windows Mobile 6.1, ein Update auf die geplante Version 6.5 ist für September vorgesehen.

5.3.1 Setup mit vielen Einstellungsmöglichkeiten

Um ein Windows-Mobile-Gerät entsprechend zu präparieren, benötigt man eine Certgate-MicroSD-Karte sowie die Anwendung Certgate Protector Setup-Tool – das Exe-File läuft auf Windows XP oder Vista. Die Applikation ist sehr übersicht-

lich in acht Folder unterteilt, in denen der Administrator verschiedene Einstellungen vornehmen kann. Nachdem die Karte in einem Lesegerät über mit dem PC verbunden wurde, empfiehlt es sich als ersten Schritt, im Folder SD Card den Speicher in einen Sektor für verschlüsselte Dateien sowie einen für unverschlüsselte Installationsdateien unterteilen – zum Schutz vor Manipulationen wird auch diese Partition mit Hilfe des CertProcessor und eines Zertifikats später verschlüsselt. Bereits bei diesem Prozess achtet Certgate auf den Schutz der gespeicherten Daten: Wird eine bereits genutzte Karte verwendet, kann der Administrator trotz PIN-Autorisierung nur die User-Daten löschen, nicht aber auf sie zugreifen. Der Zugriff ist nur mit der individuellen User-PIN möglich, die man an dieser Stelle auch gleich anlegt.



Konfiguration: Das Certgate Protector Setup-Tool ist übersichtlich in acht Folder unterteilt.

Für die Erstinbetriebnahme ist ein Zertifikat erforderlich. Hat man keines parat, kann man unter dem Menüpunkt „Tools“ auch ein selbstunterzeichnetes Zertifikat generieren, mit dem die zu installierenden Programme signiert werden müssen. Die Schlüssel, mit denen das Gerät und der Flashspeicher der SD-Card später verschlüsselt werden, erzeugt das System während der Erstinbetriebnahme direkt auf der Smartcard (Erstauthentifizierung).

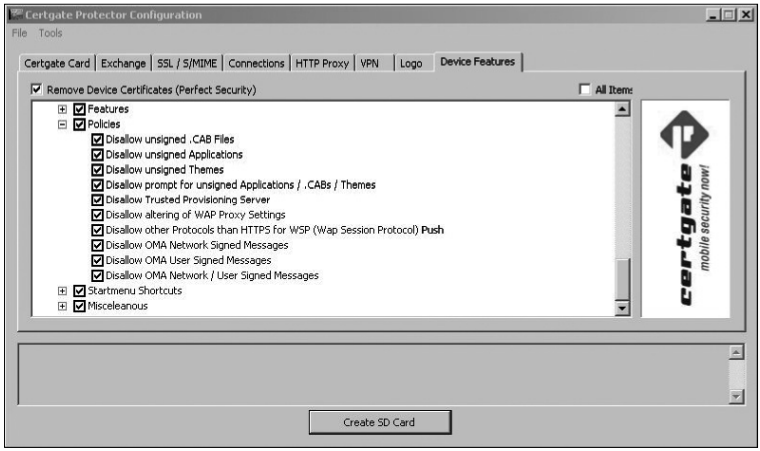
Die übrigen Reiter bieten eine Reihe an Einstellungsmöglichkeiten und sind nahezu selbsterklärend: Im Folder „Exchange“ kann der Administrator die Voreinstellungen des Mail-Account tätigen und verschiedene Optionen zur Synchronisierung festlegen. Dazu zählt etwa Größe und Alter der zu übertragenden Mitteilungen. Außerdem lässt sich einstellen, ob auch Kalender, Aufgaben und Kontakte aus Outlook synchronisiert werden sollen und an welchen Tagen das geschehen soll – nur werktags oder die ganze Woche über. Im Reiter „SSL /SMIME“

lassen sich entsprechend Schlüssel für den Zugriff auf geschützte Web-Seiten (SSL mit zertifikatsbasierender Client-Authentisierung) generieren, während der Bereich „Connections“ die Möglichkeit bietet, den Zugangspunkt (APN) zu konfigurieren. Dieser Schritt erleichtert nicht nur den Roll-out, er ist mitunter auch die einzige Option zur Eingabe der Daten, falls dieser Bereich in den Einstellungen auf dem Endgerät später gesperrt sein soll. Unter „HTTP Proxy“ können Einstellungen für einen entsprechenden Web-Filter vorgenommen werden, während „VPN“ die Konfiguration eines Virtual Private Network erlaubt. Neben der Lösung von Microsoft kann auch ein VPN vom Certgate-Kooperationspartner NCP und anderen Anbietern genutzt werden – sofern der Lizenzschlüssel vorhanden ist. Mit der Funktion VPN Tunnel Timeout kann festgelegt werden, nach welcher Zeit eine VPN-Verbindung unterbrochen wird, um das generell mögliche – aber zeitaufwändige – Knacken der Verschlüsselung zu erschweren. Die Funktion „Logo“ erlaubt es Firmen, die Certgate-Lösung durch die Einbindung eines Logos in die Anmeldemaske des Smartphones an die Corporate-Identity anzupassen.

5.3.2 Sperren von Funktionen

Wichtigster Punkt sind die Device-Features – hier geht es um das Ein- und Ausschalten von Funktionen. Um den Anwender (auch vor sich selbst) zu schützen, lassen sich unter anderem Bluetooth, WLAN oder ActiveSync abschalten, die Kamera oder bestimmte Anwendungen wie den Media-Player deaktivieren oder generell Ports blockieren. Außerdem besteht die Möglichkeit, Hersteller- oder Provider-Zertifikate abzuschalten – dies verhindert die Gefahr durch Trojaner, die sich solcher Hersteller-Zertifikate bedienen. In diesen Bereich hat Certgate einen großen Teil an eigenem Know-how eingebracht. So lassen sich nur mit tiefer Kenntnis über das Zusammenspiel einzelner Komponenten in den Windows-Mobile-Geräten Fehlermeldungen beim Deaktivieren von Funktionen wie der HTC-Touchflo-Oberfläche vermeiden.

Zur besseren Übersichtlichkeit hat Certgate die meisten Funktionen im Menüpunkt Advanced versteckt. Nach dessen Anklicken überfällt den Nutzer eine fast endlos – aber immerhin vollständig – scheinende Liste an Unterpunkten. Diese gilt es abzuarbeiten, wenn es erforderlich ist, eine Unternehmens-Policy abzubilden. Als Alternative bietet Certgate den Button „All items“ an – hier werden alle relevanten Gerätefunktionen deaktiviert und der Administrator kann im Nachgang auf der Liste durch Entfernen von Häkchen benötigte Features wieder hinzuschalten. Etwas gnädiger mit dem Endanwender ist die Voreinstellung „Remove Device Certificates (Perfect Security)“: Um potenzielle Sicherheitsrisiken zu stoppen, werden hier verdächtige Programme wie Adobe Reader, Opera-Browser und Google Maps deaktiviert. Spiele sind ebenso wenig zugelassen wie die Nutzung von integriertem Radio oder der Kamerafunktion. Außerdem setzt Perfect Security eine Reihe von Policies um. Unter anderem werden unsignierte .cab-Dateien, Anwendungen oder Themes nicht zugelassen.



Funktionen auswählen: Im Bereich Device-Features lassen sich User-Policies für das mobile Endgerät detailliert nach den individuellen Anforderungen umsetzen.

Trotz der umfänglichen Auswahl dauert die gesamte Konfiguration in der Praxis keine fünf Minuten – vorausgesetzt, man hat die benötigten Daten parat und eine klare Vorstellung über die Details der gewünschten User-Policy. Um die Einstellungen nicht bei jedem Gerät neu vornehmen zu müssen, kann man die Konfigurationsprofile – außer Exchange-Passwort und User-Pin – speichern. Dank offener Schnittstellen lassen sich außerdem für größere Roll-outs Libraries einbinden.

5.3.3 Beschreiben der MicroSD-Card

Der Befehl „Create SD-Card“ schließt den Prozess ab: Auf Knopfdruck formatiert das Programm die Certgate MicroSD-Karte, überschreibt – falls vorhanden – die vorherige PIN, erstellt eine Partition, schreibt Zertifikate in Filesystem der Smartcard und legt die Installationsdateien an. Der Ablauf wird dokumentiert, wurden Eingaben wie die User-PIN oder die Exchange-Einstellungen vergessen, tauchen Fehlermeldungen auf. Ein erfolgreicher Ablauf wird wie folgt protokolliert:

```
*** Creating card ***
Formatting card (8Mb)... success
Overwriting PIN... success
Writing dummy certificate to slot 1... success
Encrypting Exchange Config File using slot 1... success
Writing installer and signing files... success
Writing cgCustom... success
Writing Bootstrap... success
Generating Cleanup and Blacklist File... success
*** Card successfully created ***
```

Nach diesem Prozess ist die Certgate-Karte einsatzbereit und wird dem Endanwender – möglichst getrennt von der User-PIN und dem Gerät – bereitgestellt. Steckt der Nutzer die MicroSD-card in den dafür vorgesehenen Slot des Smartphones, beginnt die automatische Installation. Nach einmaligem Neustart ist das Gerät einsatzbereit und die Anmeldemaske erscheint. Nach der anschließenden Eingabe des PIN kann das Smartphone verwendet werden. Allzu oft vertippen darf man sich dabei jedoch nicht: Nach drei Fehlversuchen wird die Karte deaktiviert, in diesem Fall ist nicht nur das Telefon gesperrt, sondern die Zertifikate auf der Smartcard sind unwiederbringlich verloren. Damit können die Daten auf dem Gerät ebenso wie auf der Karte nicht mehr ausgelesen werden. Wie Certgate erklärte, handelt es sich dabei um ein wichtiges Sicherheits-Feature. Einziger Weg, das Gerät wieder zu nutzen, ist, es durch einen Hard-Reset in seinen Ausgangszustand zurückzuversetzen. Die Karte muss durch den Administrator neu konfiguriert werden. In beiden Fällen beginnt das mit einer Neuformatierung.

Nutzwert: Abhängig von den blockierten Features funktioniert das Smartphone wie ein herkömmliches Gerät (hier ein HTC Touch Pro) – oder sogar besser.

Wie ein Vergleich mit einem herkömmlichen Gerät zeigte – im Test handelte es sich um zwei HTC Touch Pro – , ist das Certgate-Device durch den Eingriff nicht langsamer geworden. Je nachdem, wie rechen- oder speicherintensiv die abgeschalteten Funktionen wären, reagiert es vielmehr schneller, auch die Akkulaufzeit nimmt zu.

Manfred Bremmer

5.4 Zehn IE-Einstellungen für sicheres Surfen

Wer Sicherheitsverantwortliche nach Einstellungen fragt, die die Nutzung des Internet Explorer (IE) sicher machen, erntet meist entweder Gelächter oder erhält die Empfehlung, einen anderen Browser wie Firefox, Opera, Safari oder Google Chrome zu verwenden. Wie emsig Microsoft vor allem bei den IE-Versionen 7 und 8 auch daran gearbeitet hat, die Sicherheit seines Browsers zu verbessern – Security-Profis trauen dem Produkt nach wie vor nicht so recht über den Weg.

Doch gerade im Unternehmensumfeld lässt sich der Microsoft-Browser aufgrund seiner engen Integration mit dem Windows-Betriebssystem kaum umgehen. „So bald werden wir vom IE nicht wegkommen", prophezeit Christopher Mendlik, Threat-Analyst bei der US-Bank Wachovia. Zudem funktionieren manche Geschäftsapplikationen ausschließlich im Zusammenspiel mit dem IE, und auch Programme, mit denen sich Inhalte online stellen lassen, reagieren häufig schlicht allergisch auf andere Browser.

Unternehmen, denen nichts anderes übrig bleibt, als den IE einzusetzen, behelfen sich mit einer Reihe von Sicherheitsmaßnahmen: Wachovia-Experte Mendlik beispielsweise sperrt den IE über Group-Policies, spielt die jeweils neuesten Patches ein und nutzt Content-Filtering auf einer Proxy-Firewall mit Echtzeit-Blacklists. Darüber hinaus überwacht er interne und ausgehende Verbindungen auf ungewöhnliche Aktivitäten.

Thomas Evans, Netzsicherheitsadministrator in Cleveland, wiederum setzt auf „Sandbox for IE", das es ermöglicht, jedes Programm in einer virtuellen Umgebung (Sandbox) laufen zu lassen und damit potenzielle Schäden auf die Sandbox und die virtuelle Registry zu beschränken. „Sobald die Browsing-Session beendet ist, lässt sich alles, was damit zusammenhängt, sicher löschen", erläutert Evans das Prinzip. Selbst wenn man sich dabei etwas Schädliches via Drive-by eingefangen habe, könne es keinen Schaden anrichten. Abgesehen davon gibt es aber eine Reihe grundlegender IE-Einstellungen, die das Surfen mit dem Microsoft-Browser um einiges sicherer machen sollen. Im Folgenden erläutern wir die laut Jeff Forristal, Senior Security Engineer bei dem Sicherheitsanbieter Zscaler (www.zscaler.com), wichtigsten Security-Settings des Microsoft-Browsers.

5.4.1 Deaktivieren Sie XPS-Dokumente

Die XML Paper Specification (XPS) ist ein Dateiformat für Dokumente, das Microsoft mit Windows Vista eingeführt hat. Angreifer haben in vielen Fällen einen Heidenspaß, Bild- beziehungsweise Dokumentenformate und Parser für ihre Zwecke zu missbrauchen. Daher gilt laut Forristal: Je weniger Formate der Browser unterstützt, desto besser.

So geht's: XPS-Dokumente deaktivieren	
Einstellungen	Extras > Internetoptionen > Sicherheit > Internetzone > Benutzerdefiniert: Stufe anpassen > XPS-Dokumente: deaktivieren.
Nachteile	Diese Einstellung kann das Betrachten von XPS-Dokumenten beeinträchtigen. Laut Forristal bietet Microsoft jedoch einen Stand-alone-XPS-Viewer an, der nicht auf den IE angewiesen ist.

5.4.2 Deaktivieren Sie den Schriftart-Download

Viele Web-Seiten bieten an, sich über den Browser ein Font-File installieren zu lassen, um internationale Schriftzeichen auf der Site korrekt darstellen zu können. Allerdings handelt es sich dabei um ein weiteres Dateiformat – und einen weiteren Angriffsvektor, da Ersteres noch unentdeckte Schwachstellen beherbergen könnte. Wer in der Regel keine fremdsprachigen Websites besuche, benötige das nicht wirklich, so Forristal.

So geht's: Schriftart-Download abschalten	
Einstellungen	Extras > Internetoptionen > Sicherheit > Internetzone > Benutzerdefiniert: Stufe anpassen > Schriftartdownload: deaktivieren.
Nachteile	Manche Web-Seiten sind daraufhin möglicherweise weniger hübsch – laut Forristal jedoch nach wie vor durchaus brauchbar.

5.4.3 Schließen Sie beim Datei-Upload den lokalen Verzeichnispfad aus

Wann immer Sie eine Datei auf einen Web-Server hochladen (etwa ein Bild in Ihren Blog oder Flickr-Account), kann der Browser entweder nur den Dateinamen oder den vollständigen Dateipfad senden – selbst wenn die Web-Seite nur den Dateinamen benötigt. Da der Dateipfad identifizierende Informationen wie den Login-Namen eines PC enthalten kann, ist das riskant. „Sendet der Browser etwa *c:\benutzer\jforristal\bilder\blog.gif*, gibt er meinen Nutzernamen (jforristal) preis", gibt Zscaler-Experte Forristal zu bedenken.

So geht's: Verzeichnispfad ausschließen	
Einstellungen	Extras > Internetoptionen > Sicherheit > Internetzone > Benutzerdefiniert: Stufe anpassen > Lokalen Verzeichnispfad beim Hochladen von Dateien mit einbeziehen: deaktivieren.
Nachteile	keine

5.4.4 Deaktivieren Sie die automatische Eingabeaufforderung

Bei vielen Optionen in der Zone „Sicherheit“ ist die automatische Eingabeaufforderung, die fragt, was Sie jeweils tun wollen, voreingestellt. Tendieren Sie grundsätzlich dazu, „ja“ anzuklicken, wenn Ihnen ein Popup präsentiert wird (übrigens keine gute Angewohnheit!), sollten Sie die Option durchweg deaktivieren.

So geht‘s: Automatische Eingabeaufforderung ausknipsen	
Einstellungen	Extras > Internetoptionen > Sicherheit > Internetzone > Benutzerdefiniert: Stufe anpassen > Automatische Eingabeaufforderung für ... Anpassen.
Nachteile	keine

5.4.5 Geben Sie stets Nutzernamen und Passwort ein

Für Heimanwender oder PC-Nutzer außerhalb eines Unternehmens, das Active Directory verwendet, ist es kein Vorteil, die Auto-Logon-Funktion aktiviert zu haben. Forristal empfiehlt, sich nirgendwo im Internet automatisiert einzuloggen. Zwar begrenzt der IE die automatische Anmeldung üblicherweise auf Sites innerhalb der Intranet-Zone – was aber, wenn ein Angreifer den Browser glauben macht, eine Site befinde sich in einer anderen Zone? Für eine Funktion, die man nicht brauche, sei es nicht sinnvoll, dieses Risiko einzugehen, so der Experte.

So geht‘s: Benutzername und Kennwort erzwingen	
Einstellungen	Extras > Internetoptionen > Sicherheit > Internetzone > Anmeldung > Nach Benutzername und Passwort fragen
Nachteile	keine

5.4.6 Deaktivieren Sie SSL-2.0-Unterstützung

Das Verschlüsselungsprotokoll SSL2 (Secure Sockets Layer) gilt als unsicher, so Forristal. Ihm zufolge führt jede Website, die lediglich SSL2 und nichts Neueres (etwa SSL3 oder TLS) unterstützt, entweder Schlechtes im Schilde oder ist so alt, dass sie vor Schwachstellen strotzt und damit für Hacker interessant ist.

So geht‘s: SSL 2.0 deaktivieren	
Einstellungen	Extras -> Internetoptionen -> Erweitert -> SSL 2.0 verwenden: nicht anklicken.
Nachteile	keine

5.4.7 Aktivieren Sie TLS-Unterstützung

TLS (Transport Layer Security) ist eine Weiterentwicklung des Netzwerkprotokolls SSL (Secure Sockets Layer), die mehr Sicherheitserweiterungen bietet als SSL3. Die Funktion sollte daher aktiviert sein.

So geht's: TLS-Unterstützung abschalten	
Einstellungen	Extras > Internetoptionen > Erweitert > TSL 1.0 verwenden: anklicken.
Nachteile	keine

5.4.8 Deaktivieren Sie die Suche in der Adressleiste

Forristal rät davon ab, Informationen in die Adressleiste des Browsers einzugeben und auf diese Weise als Suchbegriffe direkt eine Suchmaschinen zu schicken. Dabei könne es passieren, dass persönliche Daten unerwünscht preisgegeben werden, warnt der Sicherheitsspezialist.

So geht's: Adressleistensuche entfernen	
Einstellungen	Extras > Internetoptionen > Erweitert > Suchen in Adressleiste: Nicht in Adressleiste suchen.
Nachteile	keine

5.4.9 Deaktivieren Sie unnötige Add-ons

Es gibt jede Menge kleinerer und größerer Tools von Drittanbietern, die sich direkt in Ihren Browser einklinken. Im Prinzip bietet jedes dieser Add-ons eine Möglichkeit für Hacker, Sie anzugreifen. Daher empfiehlt Forristal, möglichst viele der Erweiterungsmodule abzuschalten.

So geht's: Überflüssige Add-ons ausschalten	
Einstellungen	Extras > Internetoptionen > Programme > Add-Ons verwalten.
Nachteile	Leider erschließt sich nicht immer unmittelbar, was man besser in Ruhe lässt und was deaktiviert werden sollte. Laut Forristal tun Anwender dennoch gut daran, die Add-on-Liste nach nicht länger benötigten Tools zu durchforsten. Wer beispielsweise Skype nach einer Versuchsperiode von mehreren Monaten nicht mehr nutze, könne das Skype-Browser-Add-on getrost abschalten.

5.4.10 Deinstallieren Sie alte Java-Installationen

Aus unerfindlichen Gründen installieren sich neue Java-Versionen manchmal als komplett neue Versionen statt als Upgrades älterer Releases. Das kann problematisch sein, weil ein Angreifer die älteren Versionen nach wie vor für seine Zwecke missbrauchen könnte – und diese möglicherweise Sicherheitslücken aufweisen, die in der Nachfolgeversion bereits behoben sind.

Forristal empfiehlt daher, die Liste der installierten Anwendungen zu überprüfen, zu „Java" zu scrollen und – bis auf die an oberster Stelle aufgeführte – alle Versionsnummern zu entfernen. „Bei dieser Gelegenheit lässt sich auch gleich alles andere deinstallieren, was nicht mehr gebraucht wird – und so die Gesamtangriffsfläche verringern", so der Experte.

Nachteile: keine.

Bis auf die Deinstallation alter Java-Versionen lassen sich die aufgeführten Einstellungen schnell wieder rückgängig machen. „Man kann also durchaus damit experimentieren und die Settings ausprobieren – sollten Probleme auftreten, einfach zurückgehen, und alles ist wieder wie vorher", beruhigt Forristal.

Katharina Friedmann

Katharina Friedmann ist Redakteurin mit Schwerpunkt IT-Sicherheit bei unserer Schwesterpublikation Computerwoche, von der wir diesen Beitrag übernommen haben.

TecChannel-Links zum Thema	Webcode	Compact
Zehn IE-Einstellungen für sicheres Surfen	2019862	S.178
Die besten Windows-Tools zur Client-Absicherung	448445	–
Die besten Tools zum sicheren Surfen	1764118	–
Internet Explorer 8 im Test	1841449	–

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

5.5 Die besten Check- und Sicherheits-Tools

Ihre Finanzdaten, private Post, geschäftliche Projekte – auf dem PC findet sich so allerhand, das nicht in falsche Hände geraten sollte. Es gilt daher, Neugierige und Kriminelle auszusperren.

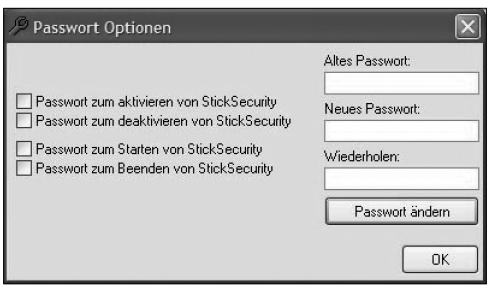
Eigentlich gehört das alles in einen Tresor: Kreditkartennummer, Kontoauszüge, Lizenzschlüssel für Ihre Software, Entwürfe für Mails an die Freundin oder den Steuerberater..., Schnüffler, Datendiebe und Datensammler suchen nach wertvollen Informationen – und allzu oft haben sie leichtes Spiel: Viele PCs sind gar nicht oder nur unzureichend geschützt. Nicht nur Privatanwender sind häufig zu sorglos – auch in Firmen wird die Spionagegefahr nicht selten unterschätzt.

Wir geben Ihnen Tipps, wie Sie sich vor Spionage im Internet, im WLAN, am heimischen PC und am Arbeitsplatz schützen. Dabei gehen wir davon aus, dass die Basis bereits gelegt ist: Das unentbehrliche Trio aus Antiviren- Programm, Firewall und Antispyware- Tool sollte also bereits installiert sein – etwa die drei Gratis-Utilities Antivir PE (www.free-av.de), ZoneAlarm Free (www.zonealarm.com) und Ad-Aware (www.lavasoft.de).

5.5.1 Stick Security: USB-Stick-Zugriffsschutz für den PC

Sie teilen sich Ihren Rechner mit weiteren Benutzern, oder Sie haben den Verdacht, dass Kollegen in der Firma gerne mal einen Blick auf Ihre persönlichen Daten werfen würden? Machen Sie dem Ausspionieren ein Ende. Wer seinen Arbeitsplatzrechner auch dann laufen lässt, wenn er nicht im Zimmer ist, für den ist das Tool Stick Security (Webcode **42237**) interessant.

Wächter: Wenn sich in Ihrer Abwesenheit niemand an Ihrem Rechner zu schaffen machen soll, empfiehlt sich das Tool Stick Security.

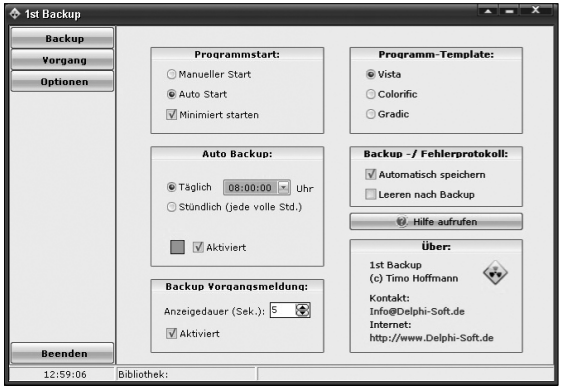


Die Software sorgt dafür, dass nur der auf den PC zugreifen kann, der einen bestimmten Wechseldatenträger besitzt. Hier empfiehlt sich ein USB-Stick. Sobald Sie ihn abziehen, wird der Computer gesperrt. Achtung: Ein Profi, der ein paar Minuten Zeit hat, kann den Schutz umgehen. Trotzdem wird Stick Security das System für die meisten Leute unzugänglich machen.

5.5.2 1st Backup: Tool für die einfache Datensicherung

Programme für die Datensicherung müssen nicht kompliziert sein. Ein Beispiel: 1st Backup (Webcode **124957**). Mit der einfachen Backup-Software sichern Sie Ihre Dateien in ein anderes Verzeichnis oder auf ein anderes Laufwerk.

Sie können wählen, ob das Tool bereits vorhandene Sicherungen überschreiben soll oder als Zusatzsicherung behält. Der Vorgang lässt sich auch automatisieren – allerdings hat man nur die Wahl zwischen täglich oder stündlich. Die Bedienung gelingt nach einer kurzen Eingewöhnung schnell. Das Tool ist nach dem Auspacken sofort lauffähig, es muss nicht installiert werden.



Datensicherung: Für einen automatisierten Backup, kann ein Backup stündlich oder täglich eingerichtet werden.

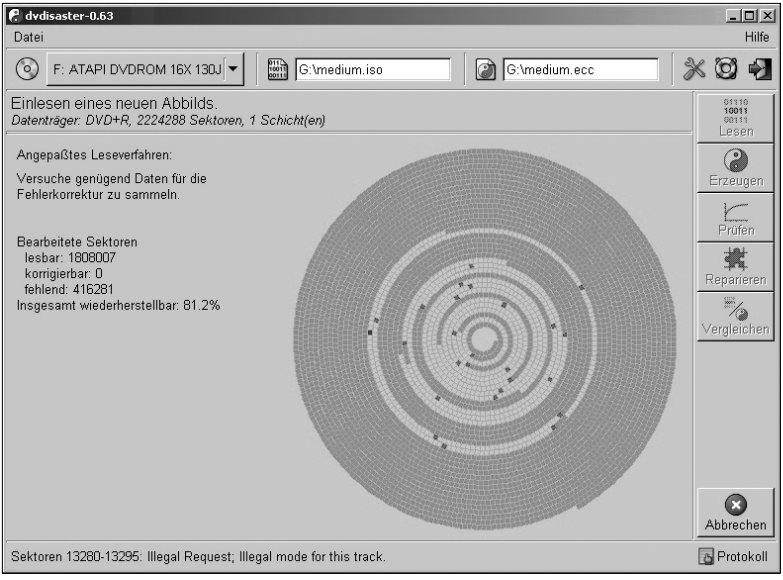
HD Clone (Webcode **74641**) kopiert den kompletten Inhalt einer Festplatte auf eine zweite Platte. Das Programm steht in einer aktualisierten Version zum Download bereit. Das Tool passt auf eine Diskette und kommt mit einem eigenen Betriebssystem, lässt sich daher so gut wie auf jedem Rechner einsetzen. Das Programm unterstützt IDE/ATA/SATA-Festplatten und kopiert bis zu 300 MByte pro Minute. Die kostenlose Variante des Programms kann nur ganze Festplatteninhalte auf größere Platten kopieren.

5.5.3 Autoruns: Zeigt alle Programme im Autostart

Automatisch mit Windows starten nicht nur nützliche Tools, sondern unter Umständen auch nervige oder gar gefährliche Programme. Mit der englischsprachigen Freeware Autoruns (Webcode **43616**) behalten Sie die Kontrolle. Sie informiert über alle Dienste und Programme, die mit Windows geladen werden. Wenn Sie eine unerwünschte Software aufgespürt haben, können Sie den Start gleich über das Tool deaktivieren. Zudem zeigt Autoruns auch Code, der über den Internet Explorer gestartet wird.

5.5.4 Dvdisaster

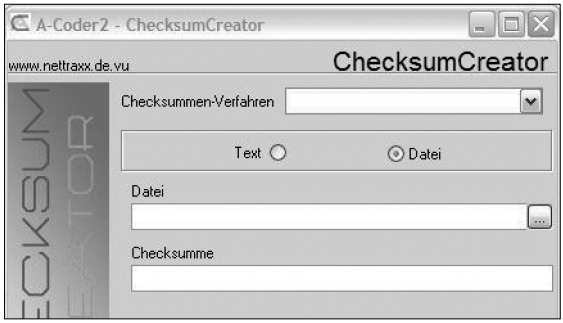
Selbstgebrannte CDs oder DVDs halten nicht ewig. Manche Scheiben lassen sich schon nach ein paar Monaten kaum noch lesen. Vorsichtshalber sollten Sie deshalb wichtige Daten auf CD/DVD mit der Freeware Dvdisaster (Webcode **110023**) behandeln. Das Programm legt Fehlerkorrektur- Dateien auf der Festplatte an. Standardmäßig hat eine solche Datei 15 Prozent der Größe einer CD oder DVD. Ist ein Datenträger später nicht mehr fehlerfrei lesbar, kommen Sie mit dem Tool trotzdem an die Daten.



Schleichender Datenverlust: Die Freeware archiviert Daten so auf CD/DVD, dass sie auch dann wiederherstellbar sind, wenn der Datenträger bereits Lesefehler aufweist.

5.5.5 A-Coder 2 Checksum: Erstellt Prüfsummen

Mit einer Prüfsumme stellen Sie fest, ob Sie die richtige und nicht eine manipulierte Datei haben. Darum finden sich auf vielen Download-Sites zu einer Datei eine MD-5- Prüfsumme (Message Digest 5). Nachdem Sie eine Datei heruntergeladen haben, erstellen Sie mit A-Coder 2 Checksum Creator (Webcode **53493**) die Prüfsumme. Stimmen die Zahlen überein, ist die Datei unverändert. Zudem generiert das Tool Prüfsummen auch nach anderen Algorithmen, etwa SHA (Secure Hash Algorith) und Ripe Message Digest.

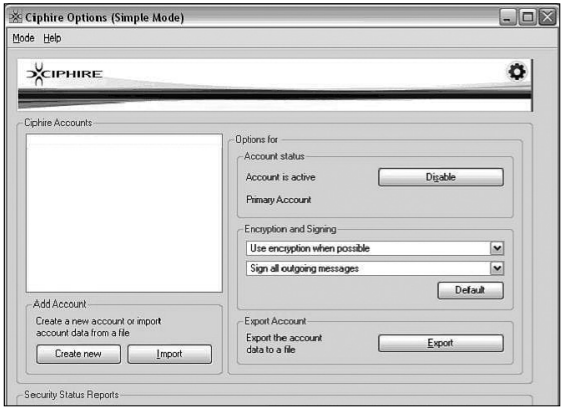


Integritätsverifizierung: A-Coder 2 Checksum versieht eine Datei mit einer eindeutigen Prüfsumme.

Analysieren Sie Ihre CDs und DVDs mit CD-Check (Webcode **9107**). Wenn das Tool dabei fehlerhafte Bereiche findet, gelingt es ihm oft, die Daten zu retten. Der Einsatz empfiehlt sich zum Beispiel dann, wenn Ihr CD- oder DVD-Laufwerk beim Lesevorgang einer Scheibe länger braucht als gewöhnlich und öfter die Geschwindigkeit reduziert. Das sind Hinweise auf ein beschädigtes Medium. Privatanwender müssen sich nach 30 Tagen gratis online registrieren.

5.5.6 Ciphire: Verschlüsselt Mails

Ciphire (Webcode **106599**) verschlüsselt Mails automatisch. Voraussetzung: Sender und Empfänger der Nachrichten müssen das englischsprachige Tool installiert haben. Die Installation und Konfiguration gelingt dank eines Assistenten leicht. Das Verschlüsselungsprogramm arbeitet mit allen POP3- und IMAP- 4-basierenden Mail-Clients zusammen. Vor dem Versand einer Nachricht prüft Ciphire über eine Online-Datenbank, ob der Empfänger ebenfalls das Tool installiert hat.



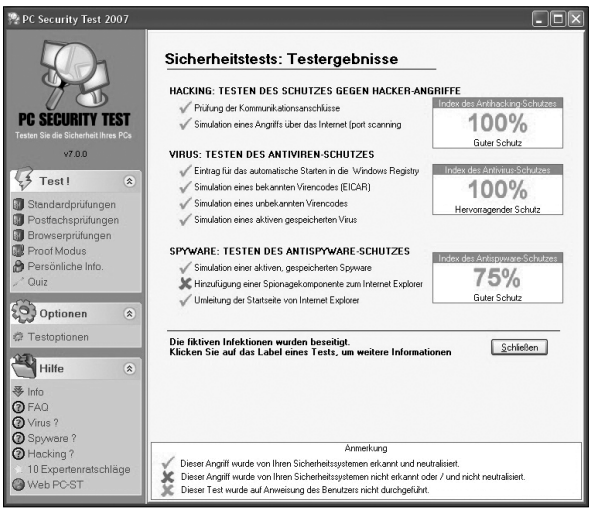
Kryptograf: Ciphire ist ein effektives und leicht zu bedienendes Mailverschlüsselungsprogramm. Die kostenlose Software verfügt es über erstaunlich viele Einstellungsmöglichkeiten.

Wer eine Alternative zur beliebten Firewall ZoneAlarm sucht und versiert ist, sollte sich mal Sunbelt Kerio Personal Firewall (Webcode **104569**) ansehen. Mit dem Tool lassen sich sehr genaue Regeln für den Netzwerkverkehr erstellen. Andere Möglichkeit: Sie konfigurieren die Firewall wie gewohnt im Lernmodus. Schlecht: Einige Meldungen und Menüs sind englischsprachig. Installieren Sie das Tool nicht parallel zu einer anderen Firewall.

5.5.7 PC Security Test: Demonstriert Schwachstellen

PC Security Test (www.pc-st.com/de/) zeigt unter dem Menüpunkt Proof-Modus, wie tückisch Viren sein können. Das macht das Tool interessant. Darüber hinaus aber handelt es sich bei der Software in erster Linie um ein verkapptes Werbemittel für das Tool Viruskeeper, das von der gleichen Firma stammt. Denn PC Security Test führt tatsächliche und angebliche Schwachstellen in der Konfiguration des PCs vor und empfiehlt anschließend die Anschaffung von Viruskeeper, das uns im Test aber nicht überzeugen konnte.

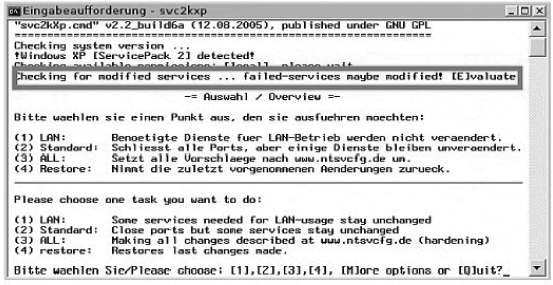
Eigenkontrolle:
PC Security Test den Schutz vor Viren, Spyware und Hackerangriffe.



Die Freeware File Recovery (Webcode **53377**) spürt auf Ihrer Festplatte gelöschte Dateien auf und stellt sie wieder her. Voraussetzung ist allerdings, dass die Sektoren, in denen die Dateien gespeichert sind, nicht bereits mit anderen Daten überschrieben wurden. Darum gilt die Regel: Verursachen Sie im Fall eines Datenverlusts so wenige Schreibzugriffe wie möglich. Deshalb empfiehlt es sich auch, File Recovery bereits vorsorglich zu installieren und nicht erst dann, wenn Sie Daten vermissen.

5.5.8 Sandboxie: Schützt PCs vor Schadcode

Die englischsprachige Software Sandboxie (Webcode **53517**) stellt beliebigen Programmen, etwa dem Internet Explorer, einen Raum bereit, in dem sie tun und lassen können, was sie wollen: Auswirkungen auf den PC hat das nicht. Sollte sich etwa über den IE eine Spyware auf den PC einschleichen wollen, speichert Sandboxie diese in einem temporären Verzeichnis und löscht sie anschließend. Das Tool ist Shareware und erinnert nach 30 Tagen an die Registriergebühr.



Ein Dienst wurde zwischendurch geändert: Svc2kxp erkennt dies und bietet an zu untersuchen, um welchen es sich dabei handelt

Mächtig: Die Batchdatei Svc2kxp nutzt letztlich nur die Windows-Bordmittel, dies aber auf über 1000 Zeilen Code, die alle unerwünschten Ports schließen und überflüssige Dienste abschalten.

Mit der Batchdatei Svc2kxp.cmd (www.ntsvcfg.de) deaktivieren erfahrene Anwender überflüssige Dienste. Bei jeder Änderung speichert Svc2kxp die alte Dienstekonfiguration als REG-Export im Verzeichnis „ntsvcfg". Wenn Sie den Menüpunkt 4 (Restore) wählen, stellen Sie die alte Konfiguration wieder her. Wir empfehlen, zusätzlich das Verzeichnis „ntsvcfg" zu sichern, das die Batch nach dem ersten Einsatz anlegt. Es enthält die Ausgangskonfiguration vor der ersten Manipulation der Dienste überhaupt.

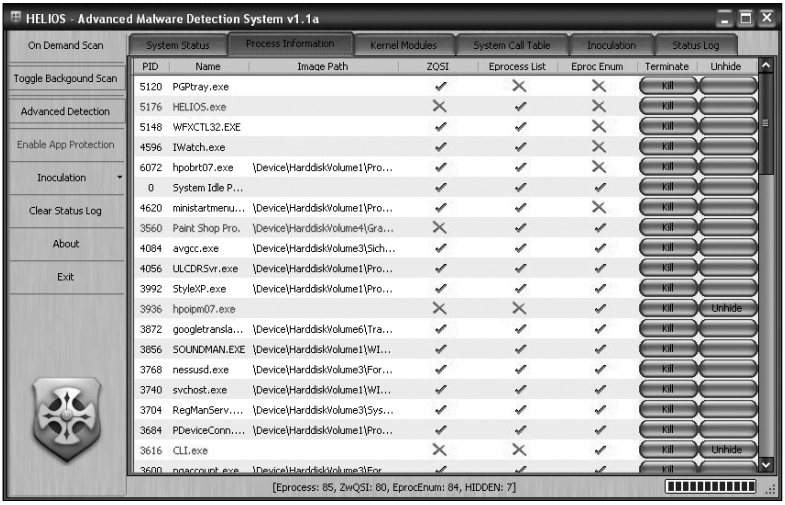
5.5.9 Hitman Pro: Kombiniert Spyware-Suchprogramme

Keine Anti-Spyware-Software kennt alle Schädlinge, die sich auf einem Rechner einnisten können, aber Hitman Pro von Mark Loman und Michel Wester (Webcode **112361**) kommt dem Ideal schon recht nahe. Nach der Installation richtet die Freeware auf Ihrem PC automatisch die bekanntesten online verfügbaren Anti-Spyware-Suchprogramme ein, darunter beispielsweise Ad-Aware, Spybot Search & Destroy, Spy Sweeper und Spyware Doctor.

Hitman Pro scannt Windows danach automatisch mit den verschiedenen Malware-Detektoren und liefert abschließend ein Protokoll der Ergebnisse. Mit der Surfrights-Funktion schränkt die Software außerdem die Benutzerrechte von Internet Explorer, Firefox, Outlook und Outlook Express sowie MSN Messenger ein.

5.5.10 Helios: Unsichtbare Attacken enttarnen

Per Rootkit verstecken Angreifer Prozesse und Dateien vor Virenscannern und führen unbemerkt etwa Spionage-Programme und Hacker-Werkzeuge aus. Erst mit speziellen Tools wie Helios (Webcode **74639**) lassen sich Rootkits aufspüren und löschen. Helios ist nach eigenem Verständnis ein *Adcanced Malware Detection System*, das aus zahlreichen Modulen unter einer zentralen Oberfläche besteht.



Attacken enttarnen: Helios erkennt Manipulationen durch Rootkits.

Zur Erkennung überwacht das Tool fortlaufend zahlreiche Systemparameter und vergleicht etwa Dateien. Entdeckte Prozesse können beendet und die korrespondierenden Dateien entfernt werden. Sicherheit, auch vor bis dato unbekannter Malware, soll eine Impfung gewährleisten.

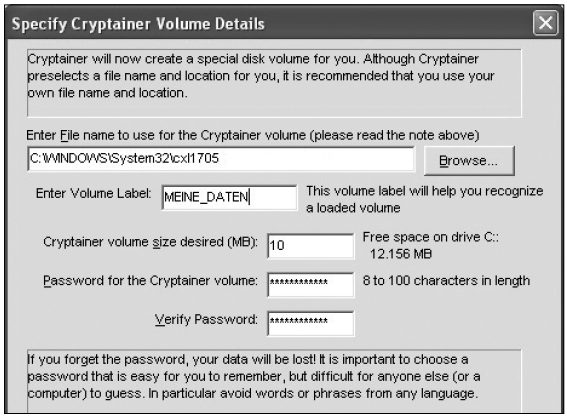
5.5.11 Xpy: Windows XP Gegenspionage

Dass Windows XP immer mal wieder Daten an Microsoft versenden möchte, ist ein offenes Geheimnis. Wer dem Datenaustausch einen Riegel vorschieben möchte, kann die entsprechenden Funktionen mit der Open-Source-Software Xpy (Webcode **106941**) abschalten. Nach dem Start beantworten Sie die Frage des Programms, ob es die XP-Einstellungen selbst ermitteln soll mit *Ja*. Im Dialog *Choose Components* geben Sie an, welche Windows-Funktionen das Tool dauerhaft deaktivieren soll. Zur Auswahl stehen unter anderem das Ausschalten des Windows-Updates *(Disable Automatic Windows Updates)*, das Deaktivieren von Java Script

(Disable Java Script) und die Deinstallation des Windows-Messengers *(Uninstall Windows Messenger)*. Möchten Sie sich nicht durch alle Optionen klicken, stehen Ihnen zwei Möglichkeiten zur Schnellkonfiguration zur Auswahl. Um maximale Sicherheit zu erzielen, wählen Sie *All settings* und bestätigen mit *Apply*.

5.5.12 Cryptainer LE: Verschlüsseln im virtuellen Laufwerk

Das englischsprachige Cryptainer LE (Webcode **74021**) erstellt virtuelle, kennwortgeschützte Laufwerke. Alle Dateien, die Sie im Windows-Explorer oder einer Anwendung auf einem solchen Laufwerk abspeichern, schreibt das Tool in chiffrierter Form auf die Festplatte.



Virtuelles Laufwerk: Cryptainer LE arbeitet mit einer Containerdatei.

Die Daten sind nur mit Cryptainer selbst zu entschlüsseln. Über das Tools-Menü richten Sie neue Laufwerke (Volumes) ein. Dabei bestimmen Sie unter anderem den Laufwerksbuchstaben, den Pfad zur verschlüsselten Datei und das Kennwort. Als Einschränkung der LE-Version sind maximal vier Laufwerke mit je bis zu 20 MByte Größe möglich.

Ramon Schwenk

TecChannel-Links zum Thema	Webcode	Compact
Die besten Check- und Sicherheits-Tools	481351	S.183
Die besten Erste-Hilfe-Tools für Windows	481351	–

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

Index

S

T

U

V

W

X

Z