Gerhard Wiehler

Mobility, Security und Web Services

Neue Technologien und Service-orientierte Architekturen für zukunftsweisende IT-Lösungen

SIEMENS

Wiehler Mobility, Security und Web Services

Mobility, Security und Web Services

Neue Technologien und
Service-orientierte Architekturen
für zukunftsweisende IT-Lösungen

von Gerhard Wiehler

Publicis Corporate Publishing

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

http://www.publicis-erlangen.de/books

ISBN 3-89578-228-9

Herausgeber: Siemens Aktiengesellschaft, Berlin und München
Verlag: Publicis Corporate Publishing, Erlangen

Printed in Germany

Vorwort

In der Geschäftswelt vollzieht sich derzeit ein gravierender Wandel. Sich rasch ändernde Marktsituationen verlangen Unternehmen immer kürzere Reaktionszeiten ab. Anwendungen und Prozesse müssen durch die Adaption neuer Technologien effizienter gestaltet werden. Nachhaltiger Erfolg lässt sich nur mit einer Geschäftsstrategie erreichen, die diesen Veränderungen Rechnung trägt und Handlungsoptionen offen hält.

Kernprozesse bilden das Rückrat aller geschäftlichen Aktivitäten und spielen deshalb eine ganz besondere Rolle. Unternehmen müssen sich mehr und mehr auf diese Prozesse und auf ihre Schlüsselkompetenzen konzentrieren, wenn sie wettbewerbsfähig bleiben wollen. Dies gelingt nur, indem bestehende Wertschöpfungsketten weiter aufgegliedert und spezialisiert werden. Als Trend zeichnet sich ab, dass konventionelle Wertschöpfungsketten durch ein breit gefächertes Wertschöpfungsnetz abgelöst werden, wobei einerseits Produkte und Dienste eingekauft und auf der anderen Seite Teilprozesse wie z. B. Financial Services oder Human Resource Services ausgegliedert werden.

IT-Services mit den dazugehörigen Architekturen, Infrastrukturen, Plattformen und Anwendungen haben die Aufgabe, diese sich wandelnde Prozesslandschaft bestmöglich zu unterstützen und zu integrieren. Die Erwartungen der Chefetagen sind höher denn je: Prozesskonsolidierung, erhöhte Reaktionsfähigkeit bei veränderten Prioritäten sowie Produktivitätssteigerungen durch Einsatz neuer Technologien bei gleichzeitiger Reduzierung der Betriebskosten. Die Herausforderungen – auch im Hinblick auf einen absehbaren Paradigmenwechsel bei der Entwicklung von IT-Lösungen – sind enorm und bedürfen großer Kraftanstrengungen.

In diesem Kontext sind die Themen des Buches – Mobility, Security und Web Services – von hohem Interesse für IT-Organisationen. Infrastrukturen und Lösungen auf Basis Service-orientierter Architekturen unter Einbeziehung produktiver mobiler Anwendungen und Berücksichtigung zunehmender Sicherheitsrisiken sind heute Topthemen, mit denen sich CIOs auseinandersetzen müssen. Aber auch Line Manager sollten sich der treibenden Kräfte dieser neuen Technologien bewusst werden, um Geschäftsmöglichkeiten frühzeitig zu erkennen und wahrnehmen zu können.

Web Services und mobile Anwendungen sowie die damit verbundenen Security-Implikationen werden IT-Infrastrukturen und -Lösungen deutlich verändern. Eine gemeinsame Betrachtung dieser verschiedenartigen Technologien führt zu neuen Erkenntnissen, die für zukunftsorientierte Architekturen und Anwendungen von wesentlicher Bedeutung sind. Der Autor beschreibt die komplexen Zusammenhänge verständlich und mit übersichtlichen Graphiken illustriert. Das Buch gibt wertvolle Empfehlungen

und weist den Weg in eine neue Ära von IT-Lösungen, die den anstehenden Herausforderungen gerecht werden.

Johann Breidler

Leitung Systemstrategie,
Siemens Business Services
GmbH & Co. OHG

Vorwort

Die traditionellen Kommunikationssysteme, das Internet und die mobilen Netze haben sich in einem langjährigen Evolutions- und Konvergenzprozess zu einer starken Innovationskraft in unserer Gesellschaft entwickelt. Bei der nach wie vor stürmischen Weiterentwicklung sind nicht nur spannende technologische Neuerungen zu beobachten, sondern vor allem die wachsende Bedeutung gesellschaftlicher, insbesondere wirtschaftlicher Aspekte. Die moderne Informations- und Kommunikationstechnik (IT) verändert die Welt nachhaltig. Mobil sein und dabei sicher und in jeder denkbaren Form kommunizieren und Dienste effizient und flexibel nutzen können – so kann man die Herausforderungen aus Sicht der Menschen zusammenfassen.

Der MÜNCHNER KREIS [V.1], als übernationales Forum für Kommunikationsforschung, widmet sich seit über 30 Jahren der Entwicklung der Telekommunikation und den damit verbundenen technologischen, gesellschaftlichen, ökonomischen und politischen Fragestellungen und Trends. Besonderes Augenmerk wird dabei auf die Voraussetzungen gelegt, unter denen Innovationsschritte erfolgreich vollzogen werden können. Besonders wichtig ist die interdisziplinäre Betrachtung der Entwicklungen. Nur so können Trends oder Paradigmenwechsel frühzeitig erkannt und ihre Auswirkungen eingeschätzt werden.

Mit Mobility, Security und Web Services greift das vorliegende Buch Themenfelder auf, die in letzter Zeit auch in den Veranstaltungen des MÜNCHNER KREISES intensiv diskutiert wurden. Als gemeinsame Erkenntnis ist hervorzuheben, dass die IT als Verbindungsglied von immer neuen Kommunikations- und Anwendungsszenarien eine Schlüsselrolle spielen wird. Gewachsene Infrastrukturen und Plattformen werden sich dadurch gravierend verändern. Neue mobile Anwendungen und Service-oientierte Lösungsansätze tangieren unsere Freizeit und Privatsphäre ebenso wie künftige Geschäftslösungen. In der Fachwelt sind noch lückenhafte Sicherheitsvorkehrungen und damit verbundene Risiken zwar erkannt worden, die Brisanz dieser Thematik wird aber häufig auf die leichte Schulter genommen.

Die Gesellschaft muss sich mit diesem Wandel auseinandersetzen. Eine umfassende Aufklärung und Bewusstseinsschärfung ist angesagt. Dieses Buch zeigt in vielen Beispielen auf, wie Kommunikations- und Informationstechnologien zusammenwachsen. Die damit verbundenen komplexen Zusammenhänge werden strukturiert dargestellt und mit anschaulichen Illustrationen verständlich gemacht. Der Autor erläutert wesentliche Evolutionsschritte, stellt Unternehmenslösungen und Anwendungsarchitekturen in den Mittelpunkt und gibt praktikable Empfehlungen für IT-Organisationen.

Dieser faszinierende und zugleich praxisnahe Ausblick auf eine neue IT-Ära eröffnet dem Leser viele neue und interessante Perspektiven. Möge das Buch mithelfen, den Wandel nicht nur zu bewältigen, sondern auch aktiv zu gestalten!

Prof. Dr.-Ing. Jörg Eberspächer,

Lehrstuhl für Kommunikationsnetze
Technische Universität München
und MÜNCHNER KREIS

Inhaltsverzeichnis

1 Einführung

Die Evolution von Informations- und Kommunikationstechnologien verändert die Welt mit atemberaubender Geschwindigkeit. Auch die wirtschaftliche Flaute der vergangenen Jahre hat diese Entwicklung kaum gebremst. Experten gehen davon aus, dass der rasante Fortschritt in der nächsten Dekade andauern wird.

Unsere Gesellschaft wird durch diese technologischen Veränderungen in nahezu allen Lebensbereichen tiefgreifend beeinflusst. Für die Business-Welt ergeben sich gleichzeitig neue, nutzbringende Anwendungen und innovative Geschäftsmöglichkeiten. Zunehmender Wettbewerbsdruck macht es erforderlich, sich den veränderten Marktanforderungen immer wieder schnell und flexibel anzupassen. Auch Verbraucher verändern ihr Verhalten und nutzen zunehmend die attraktiven Angebote der Informations- und Kommunikationsdienste, nicht nur im Berufsleben, sondern auch privat.

Mobility, Security und *Web Services* spielen in zukünftigen Anwendungen eine ganz wesentliche Rolle. Sie werden gravierende Veränderungen mit sich bringen, nicht nur in der IT-Infrastruktur und der Ausprägung und Bedeutung der sog. IT-Middleware, sondern auch in der Art und Weise wie Business Solutions zukunftssicher implementiert werden.

Das Buch erläutert die Zusammenhänge dieser drei Themenkreise und begründet ihre Bedeutung. Es werden insbesondere die Herausforderungen für mittelgroße und große Unternehmen aufgezeigt sowie die unmittelbaren Auswirkungen auf heutige IT-Landschaften dargestellt.

Mobility

Mit der Einführung der Web-Technologie für Business Solutions begann in den Neunzigerjahren ein neues Zeitalter: die Welt des e-Business. Erst durch das Internet als Kommunikations-Backbone wurde es möglich, den Kunden, Partnern und Mitarbeitern Informationen und Prozesse, die zunehmend die Werte eines Unternehmens repräsentieren, z. B. über Web-Portale zugänglich zu machen. Mussten sich Unternehmen in der Vergangenheit nur auf herkömmlich erreichbare Kundenkreise beschränken, so hat das Internet die phantastische Möglichkeit eröffnet, Millionen von neuen Kunden zu erreichen.

Die faszinierende Welt der drahtlosen Zugangsmöglichkeiten gibt den Menschen die Flexibilität, ihren geschäftlichen Aufgaben überall nachzugehen, unabhängig davon, wo sie sich gerade befinden. Mobiltelefone, PDAs und andere über Mobilfunk angebundene Geräte setzen Berufstätige und Verbraucher in die Lage, globalen Zugang zu

Firmenressourcen zu erhalten, wo immer und wann immer sie wollen. Im Gegensatz zum festverdrahteten Desktop können Anwender an jedem Ort und zu jeder beliebigen Zeit erreicht werden oder selbst Kontakte herstellen. Die technologische Vielfalt führt dazu, dass sich berufliche und private Interessen immer mehr vermischen.

Sinkende Kosten und zunehmende Bandbreite der mobilen Netze werden die drahtlose Kommunikation auch für Datenanwendungen immer attraktiver machen. Die Sprach- und Datentechnologien sind konvergierend, so dass mobile Geräte auch als Clients für Geschäftsanwendungen nutzbar sind. Sowohl die gewünschte Verfügbarkeit dieser innovativen mobilen Technologien als auch ökonomische und geschäftliche Anforderungen werden diese Entwicklung weiter forcieren.

Neue Kategorien von Anwendungen werden sich in Abhängigkeit von Akzeptanz und Bezahlbarkeit etablieren können. Absehbar ist etwa, dass Mobiltelefone bald von nahezu allen Berufstätigen genutzt werden.

Internet und mobile Netze sind beide und insbesondere in ihrer Kombination ein Megatrend. Mit ihrer Konvergenz und Evolution beginnt eine neue Ära.

In den nächsten fünf Jahren wird sich ein Übergang vom e-Business zum mobilen Business abzeichnen. Funktionsreiche und integrierte Web-/Mobile-Portale werden dabei eine entscheidende Rolle spielen.

Wesentliche Funktionen sind technisch schon realisiert oder werden in naher Zukunft verfügbar sein. Beispiele sind: End-to-End-gesicherte Transaktionen, ortsabhängige Services, flächendeckende „Always-on"-Technik wie in den GPRS-Netzen und flexible und breitbandige WLAN-Dienste, die in Hotspots wie Flughäfen, Hotels und Messezentren zur Verfügung gestellt werden. Breitbandige, attraktive Multimedia-Anwendungen runden das Spektrum ab.

Mobile-Business-Architekturen werden auf denselben (mehrschichtigen) n-Tier-Architekturen basieren, wie sie heute schon in e-Business Solutions üblich sind. Die Integration von mobilen Anwendungen in die existierende IT-Infrastruktur wird zumindest in der näheren Zukunft die dominierende Vorgehensweise sein. Allerdings sind spezifische Eigenschaften und Einschränkungen der heutigen mobilen Geräte und Netze zu berücksichtigen, die sich von der traditionellen Internet-Technik unterscheiden und die Entwicklung von Internet-basierten Anwendungen erschweren.

Hervorzuheben ist dabei, dass eine sinnvolle Ergänzung von Business Solutions durch mobile Anwendungen nicht nur eine Frage der Integration ist, sondern vielmehr das Verstehen der spezifischen Charakteristika mobiler Ansätze voraussetzt. Unternehmen sollten daher fachliche Beratung in Anspruch nehmen, um sicher zu gehen, dass eine kompetente Evaluierung den richtigen Einsatz und Nutzen für die jeweilige Organisation und die relevanten Geschäftsprozesse gewährleistet.

Web Services und Service-orientierte Architektur

Eine spannende Geschichte ist die sich gerade vollziehende Evolution von den traditionellen IT-Anwendungen hin zum *Web-Services-Paradigma*. Dieser Wandel könnte

sich als der größte Fortschritt in der noch kurzen Historie der e-Business Solutions herausstellen.

Diese bahnbrechende Entwicklung lässt sich mit dem Übergang von der Einzelfertigung zur Fließbandherstellung in der Automobilindustrie vergleichen. Heute läuft die Fertigung weitgehend automatisiert, gesteuert von Leitsystemen, die spezialisierte Roboter für die unterschiedlichen Prozessschritte einsetzen. Analog dazu werden in der IT-Welt Prozesse durch sogenannte „Workflow-Engines“ gesteuert, Web Services oder eingebundene existierende Anwendungen repräsentieren die einzelnen Prozessschritte. Neue Prozessabläufe lassen sich durch die Trennung von Ablaufsteuerung und Funktionsausführung einfacher gestalten und vorhandene Abläufe können flexibler angepasst werden, als dies mit heutigen Anwendungsstrukturen möglich ist.

Web Services sind eine neue Basistechnologie für *Service-orientierte Architekturen* (SOA). SOA steht für eine Architektur in verteilten Systemumgebungen: Anwendungen können entweder lokal oder entfernt über Netze in lose gekoppelter Weise andere Anwendungen aufrufen und deren Funktionen nutzen.

SOA ist durch die Eigenschaft charakterisiert, dass Dienste oder Funktionalitäten verfügbar gemacht werden (Publishing) und diese von anderen genutzt werden können. Dazu gehört die Fähigkeit, gewünschte Dienste im Netz zu finden (Discovering) und automatisiert nutzbar zu machen (Binding).

Die IT-Industrie diskutiert schon seit geraumer Zeit über die Anwendung von Web Services in Service-orientierten Architekturen. Die Vorteile sind besonders in firmenübergreifenden Lösungen offensichtlich: Unabhängigkeit von Anwendungs-Plattformen und Programmiersprachen und lose Kopplung von Anwendungen verschiedener Organisationen und Unternehmen.

Web Services sind autonome, sich selbst beschreibende, modulare Anwendungen, die einerseits innerhalb eines Unternehmens als effiziente Methode zur verteilten Verarbeitung angewendet, andererseits im Internet publiziert, lokalisiert und aufgerufen werden können.

Analysten weisen übereinstimmend auf die Bedeutung von Web Services hin. Eindrucksvoll ist vor allem die Geschlossenheit, mit der diese Technologie von allen wichtigen Software-Herstellern wie IBM, Microsoft, SAP, BEA, HP, Sun und Oracle unterstützt wird. Web Services werden 20 Jahre lang ein kritisches Thema für IT-Infrastrukturen bleiben, behaupten Analysten. Sie betonen gleichzeitig, dass ein so erweitertes Web eine Chance für Unternehmen ist, agiler zu handeln, Trends schneller zu erkennen und besser darauf reagieren zu können.

Revolutionär an der Web-Services-Technologie ist, dass Unternehmen nun verteilte Anwendungen entwickeln und nutzen können, ohne sich um Hardware- und System-Plattformen, Programmiersprachen und Netz-Topologien der verschiedenen involvierten Bereiche und Partner kümmern zu müssen.

In der Vergangenheit galten Sicherheitsbedenken als Haupthindernis für eine breite Akzeptanz und Anwendung von Web Services. IT-Experten haben seit vielen Jahren sichere Lösungen entwickelt, jedoch auf Basis von WAN-Mietleitungen, die vor frem-

den Eingriffen geschützt sind. Unternehmen fordern deshalb, dass die Nutzung von Web Services über das Internet auf mindestens gleichwertigem Security-Niveau möglich sein muss.

Wenn das Thema Security erst einmal gelöst ist, könnte die Vision Wirklichkeit werden, dass sich das Internet auf Basis von SOA und einer weitverbreiteten Nutzung von Web Services zum Business-Web weiterentwickeln wird. Web Services könnten dann dynamisch kombiniert werden, um beliebige Business-Prozesse flexibel und effizient abzuwickeln.

Eine weitere Vision vom *agilen* bzw. *Real-time*-Unternehmen ist die durchgängige Verzahnung und Integration aller Business-Prozesse. Real-time-Unternehmen sind in der Lage, Business-Prozesse flexibel zu handhaben und mit Geschäftspartnern und Kunden konsistent und unternehmensübergreifend zu integrieren, anstatt wie bisher einzelne Prozesse durch IT-Systeme und separate Anwendungen zu suboptimieren. Real-time-Unternehmen können spontan und flexibel auf Marktanforderungen und Kundenwünsche reagieren. Ihnen gelingt die Fokussierung auf Kernkompetenzen in hohem Maße, während Partner, die weitgehend in die Abläufe eingebunden sind, sich auf ausgewählte andere Aktivitäten konzentrieren können.

Verbleibt die Frage: Handelt es sich wieder um eine Blase, die bald platzen wird, wie im Fall des dotcom-Hypes? Oder wird das alles in absehbarer Zukunft schon Realität sein? Eine verlässliche Antwort darauf kann heute niemand geben. Tatsache ist jedoch, dass dieser Paradigmenwechsel bereits sehr konkrete Züge angenommen hat.

Security

Unternehmen haben in jüngster Zeit einen tiefgreifenden Wandel erlebt: die Globalisierung. Sie müssen sich heute dem globalen Wettbewerb stellen. Die Arbeitsplätze sind auf der ganzen Welt verteilt, immer mehr Mitarbeiter befinden sich im Ausland, der Offshoring-Trend ist nicht mehr aufzuhalten. Die zeitnahe Kommunikation wird unerlässlich.

Zweigstellen und Partner, z. B. Zulieferer, müssen unabhängig von Ort und Zeit uneingeschränkt kommunizieren können. Gleichzeitig ist unabdingbar, dass verteilte Transaktionen über alle Geschäftsabläufe hinweg gesichert stattfinden. Dies gilt insbesondere, wenn Geschäftspartnern Zugriff auf Intranet-Anwendungen und Unternehmensressourcen gewährt wird.

Im Geschäftsleben erwartet heute jeder, dass er angeforderte Informationen und Dienste in Echtzeit erhält. Kunden sind nicht bereit zu warten, wenn sie ihrerseits schnell Entscheidungen treffen müssen. Solche Anforderungen setzen Unternehmen stark unter Druck.

Gerade deshalb ist ein zunehmender Konflikt zwischen der tatsächlich implementierten Security in heutigen IT-Infrastrukturen und den zunehmenden Real-Time-Anforderungen zu beobachten. Konfrontiert werden Organisationen heute mit vielfältigen Herausforderungen, wobei die Kunst darin besteht, den richtigen Mittelweg zwischen dem Gewähren von erweiterten Zugangsrechten zu Firmenressourcen und einem entspre-

chenden Sicherheitsniveau zu finden. Die Security muss in der Lage sein, größere Risiken zu vermeiden und sicherheitskritische Geschäftsprozesse zu schützen.

Dies ist eine schwierige Balance, die nur im Kontext mit einer sorgfältigen Untersuchung der relevanten Geschäftsvorgänge und der genauen Einschätzung der damit verbundenen Bedrohungen und Risiken vernünftig austariert werden kann. Diese Balance zum richtigen Zeitpunkt zu finden, stellt Unternehmen und ihre CIOs vor große Probleme. Das mag erklären, warum existierende IT-Infrastrukturen heute eher zögerlich den neuen Anforderungen angepasst werden.

Security ist seit e-Commerce und Internet-basierten Geschäftslösungen ein Thema von höchster Priorität. Mit dem mobilen Internet/Intranet-Zugang und der Integration von mobilen Angestellten, Partnern und Kunden werden die Security-Schwachstellen und Bedrohungen ganz erheblich zunehmen. Darüber hinaus kommt mit Web Services und SOA eine neue Dimension von Herausforderungen und Risiken auf die Unternehmen zu. Insbesondere dann, wenn Partner nun dynamisch in Lösungen eingebunden werden, die vorher noch nie irgendwelche Geschäftsbeziehungen miteinander hatten.

In der Zwischenzeit wurde auch für Web Services ein mehr oder weniger vollständiger Rahmen von Security-Standards definiert. Dieser Prozess ist zwar noch nicht abgeschlossen, doch anwendbare Produkte sind mittlerweile verfügbar. Das Positive an den neuen Security-Standards für Web Services ist, dass sie auf den heute existierenden Basismechanismen aufsetzen, wie z. B. Kerberos, Secure Socket Layer (SSL), digitale Zertifikate und Public-Key-Infrastruktur (PKI).

Eine Analogie mag helfen, das Konzept der Web Services Security verständlich zu machen: Es ist, als begleite eine Eskorte die transportierten Informationen zu ihren Zielorten, um sicherzustellen, dass unterwegs keine Verfälschungen passieren. Sie kümmert sich um Verschlüsselung und Entschlüsselung der Informationen und auch um Identität und Rechte des Senders und Empfängers; diese Kombination macht erst eine vollständig gesicherte Kommunikation innerhalb eines Geschäftsvorgangs aus.

Security ist ein so brisantes Thema, dass sich nun auch die Vorstandsebene damit befassen muss. Die Bewusstseinsschärfung auf höchster Ebene ist die Voraussetzung dafür, dass Geschäftsrisiken angemessen eingeschätzt werden. Damit wird auch der Grundstein für eine adäquate Security-Strategie gelegt. Diese definiert die notwendigen Security-Maßnahmen bei akzeptablen Kosten und beherrschbaren Risiken.

Ein weiterer, ganz wesentlicher Aspekt im Kontext Security ist gegenseitiges Vertrauen (Trust). Eine solide Vertrauensbasis in den Geschäftsbeziehungen gilt heute mehr denn je als Garant für den Erfolg im Wettbewerb. Vertrauen ist immer auch eine wichtige Voraussetzung für neue Geschäftsmöglichkeiten, für verlässliche Kundenbeziehungen und schließlich auch für eine fundierte Kooperation mit Partnern. Vertrauen kann sich jedoch nur entwickeln, wenn alle Beteiligten überzeugt sind, dass sämtliche geschäftlichen Aktivitäten absolut sicher abgewickelt werden. Für ein Unternehmen, das wettbewerbsfähig bleiben und innovative Dienste anbieten will, kann eine zuverlässige und sichere IT-Infrastruktur echten Wertzuwachs bedeuten.

Themen, die nicht Gegenstand dieses Buches sind

Ein weiteres, unmittelbar mit Web Services in Verbindung stehendes IT-Schlüsselthema sind die *Grid Services*. Die Kombination aus Grid Computing – einer Middleware, die für parallelisierbare wissenschaftliche Berechnungen entwickelt wurde – und Web Services, um daraus Grid Services entstehen zu lassen, ist ein spannendes Thema, das derzeit intensiv unter IT-Experten diskutiert wird. Grid Services sind in der Lage, komplexe Funktionen auszuführen, die durch einzelne Services nicht erbracht werden können. Sie stellen ein Kernelement des zukünftigen Computing-Paradigmas dar: *On-Demand Computing*. On-Demand Computing hat das Potenzial, Verarbeitungsleistung wie von einem Wasser- oder Stromversorgungbetrieb quasi aus der Steckdose zu beziehen, weshalb auch die Bezeichnung *Utility Computing* verwendet wird. Auf Grid Services und On-Demand Computing wird in diesem Buch nicht weiter eingegangen.

In den folgenden Kapiteln werden öfters beispielhaft Produkte und Plattformen zitiert. Open-Source-Plattformen werden ohne Zweifel eine zunehmend wichtige Rolle in modernen e-Business-Lösungen spielen. Es würde aber den Rahmen dieses Buches sprengen, auch Open Source Software angemessen zu berücksichtigen. Interessierten Lesern sei das Buch *Open Source Software* [1.1] empfohlen.

Der Autor hat großen Wert auf die Aktualität der in diesem Buch vermittelten Informationen gelegt. Auf innovativen Gebieten werden jedoch neue Produkte und Standards in kurzen Zeitabständen freigegeben. Beispielsweise liegen die Produktzyklen von Mobiltelefonen nur noch bei neun Monaten. Bitte sehen Sie es nach, wenn gelegentlich nicht die allerneueste Version zitiert ist.

2 Evolution von Informations- und Kommunikationstechnologien

Während der vergangenen zwei Dekaden haben sich Geschäftsanwendungen und -lösungen grundlegend verändert. Technologische Fortentwicklungen der *IT (Informationstechnologie)*, neue Architekturen und Paradigmenwechsel, Netz- und Kommunikationstechnologien sowie die faszinierende Innovation von mobilen Geräten haben wesentlich zu diesen Veränderungen beigetragen.

Dieses Kapitel geht im historischen Kontext auf einige dieser Evolutionen ein und zeigt auf, welche Richtung die Zukunft weisen wird. Es ist besonders an Leser adressiert, die an den entwicklungsgeschichtlichen Zusammenhängen von IT- und Kommunikationstechnologien interessiert sind.

2.1 Paradigmenwechsel in der IT

Business-Prozesse in Unternehmen werden durch eine darunterliegende IT-Infrastruktur und entsprechende IT-Anwendungen unterstützt. Letztere steuern und optimieren

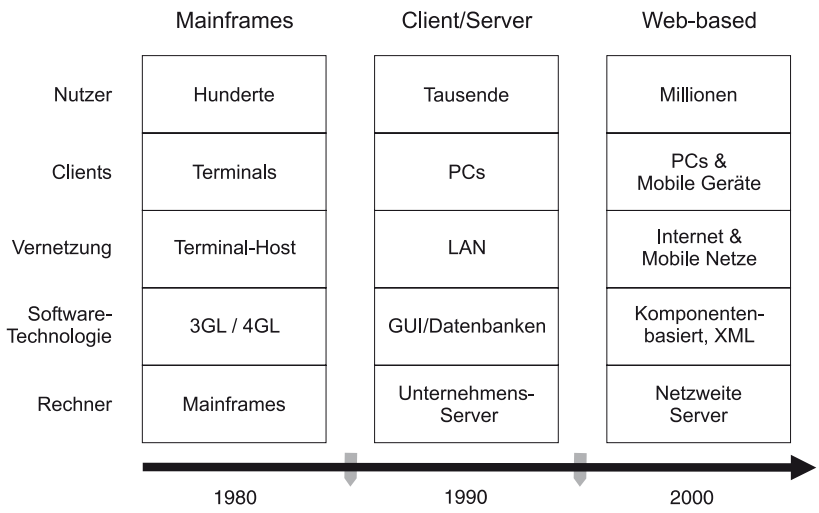


Bild 2.1 IT-Evolution

Unternehmensressourcen und gestalten Einkaufsprozesse, Lieferkettenprozesse (Supply Chain Management), Kundenbeziehungen (Customer Relationship Management) und andere Prozesse. Wie in Bild 2.1 dargestellt, waren es zwei Paradigmenwechsel, die seit den achtziger Jahren jeweils grundlegende Veränderungen sowohl in der IT-Infrastruktur als auch bei einschlägigen Geschäftslösungen (Business Solutions) mit sich gebracht haben.

In den späten achtziger Jahren wurde das *Mainframe-Paradigma* der monolithischen Applikationen, die, basierend auf Programmiersprachen der 3. und 4. Generation, auf sogenannten Mainframes abliefen und einfache textorientierte Terminals unterstützten, durch eine 2-schichtige (2-Tier) *Client/Server-Architektur* abgelöst.

Sehr selten finden Paradigmenwechsel aufgrund der Evolution einzelner Technologien oder als Folge einer hervorragenden Erfindung statt. Vielmehr ist das Zusammenspiel oft komplexer, sich ergänzender Technologien entscheidend, gepaart mit neuen Ideen und Anforderungen aus der Geschäftswelt, wenn daraus gleichzeitig Mehrwert entstehen kann.

Der Wechsel zum Client/Server-Paradigma belegt diese Hypothese eindrucksvoll:

- Die Anforderungen der Geschäftswelt: Wettbewerbsbewusste Unternehmen haben in den achtziger Jahren versucht, viele online-Kunden zu gewinnen, Anwendungen zu dezentralisieren und in ihre Zweigstellen zu verlagern und Datenbanken von den Applikationen zu trennen, damit sie unabhängig benutzt und administriert werden können. Schließlich entstand der Bedarf an komfortableren und Grafik-orientierten Benutzeroberflächen.
- Die technologischen Entwicklungen: Die PC- und LAN-Entwicklungen können als die wesentlichen technologischen Auslöser für diesen Paradigmenwechsel gewertet werden. Allerdings haben eben auch andere, komplementäre Entwicklungen zur Verwirklichung des neuen Paradigmas beigetragen. So z. B. die leistungsfähigen Unix-Server-Plattformen, grafische User Interfaces and funktionsreiche Datenbank-Systeme.
- Die Idee: Ausstattung des Clients mit höherer Prozessorleistung und Intelligenz, um die Verarbeitung (Workload) von Daten auf ökonomischere Plattformen zu verlagern und besser auf die Bedürfnisse der Verbraucher eingehen zu können.

10 Jahre später hat sich ein weiterer Paradigmenwechsel angekündigt. Wiederum war es die Folge aus interessanten technologischen Entwicklungen, verbunden mit neuen Anforderungen, die sich in der Geschäftswelt herausgebildet haben: das Web-basierte e-Business.

Ausschlaggebende Business-relevante Faktoren waren: Trend zur Globalisierung, steigender Wettbewerb mit kürzeren Produktzyklen, flexiblere Unternehmensstrukturen, virtuelle Organisationen und engere Kunden- und Partnerbeziehungen.

Ohne Zweifel war die Entwicklung der Internet-Technologie in erster Linie die treibende Kraft für diesen Wechsel der IT-Lösungswelt hin zu den heute üblichen, mehrschichtigen (Multi-Tier-)Architekturen und dem Web-basierten e-Business-Paradigma.

Internet und e-Business sind heute aus dem täglichen Leben nicht mehr wegzudenken. Daran hat auch das Platzen der dot.com-Blase kaum etwas geändert. Das Internet bietet immer wieder neue Geschäftsmöglichkeiten und täglich profitieren Millionen Privatleute und große Teile der Business-Welt von diesem Paradigma.

Als weitere bedeutende Evolution, die das *Web-basierte Paradigma* signifikant mitgeprägt hat, ist der Standard *XML (eXtensible Markup Language)* zu nennen. XML hat sich aus der Dokumenten-orientierten Sprache *SGML (Structured Generic Markup Language)* und der Präsentations-orientierten Sprache *HTML (HyperText Markup Language*) entwickelt. XML gilt heute als *Lingua Franca* des Internet.

XML, ein offener, in der Industrie weit akzeptierter Standard, stellt die Basis für Datenaustausch und Interoperabilität dar und erlaubt die Beschreibung von Daten, Dokumenten, Informationen, Inhalten jeder Form, ja sogar von Protokollen und Programmen. Mit XML lassen sich Inhalt und Präsentationsform trennen, wobei XML gleichzeitig die einzige Quelle für die Generierung unterschiedlicher Präsentationsformate, z. B. für die Ausgabe auf Arbeitsplätzen und mobilen Geräten repräsentiert. Das erleichtert gleichermaßen den Datenaustausch zwischen Geschäftspartnern der verschiedenen Industriebranchen wie auch zwischen IT-Systemen, unabhängig von der verwendeten Software- und Hardware-Plattform. Schließlich ist XML auch als Basistechnologie für entfernte Funktionsaufrufe (Remote Function Calls) sowie für die XML-Web-Services-Technologie zu sehen.

Als ein zweiter Schritt in der Fortentwicklung des Web-basierten Paradigmas etabliert sich gerade das „Wireless“ Internet. Die Möglichkeiten, mit einer Vielfalt innovativer, mobiler Geräte über Funknetze Zugang zu beliebigen Internet Services zu erhalten, muten geradezu phantastisch an. Dies wird in vielen Belangen den persönlichen Lebensstil aufgeschlossener Menschen beeinflussen, sich aber auch gravierend auf geschäftliche Anwendungsszenarien auswirken. Einige mobile Business Solutions wurden schon erfolgreich erprobt und eingesetzt. Der Nutzen ist offensichtlich. Um nur einige Beispiele zu nennen: Optimierung von Prozessabläufen, Einsparung von Reisekosten, Generierung von Mehrwert für Kunden, Partner, Mitarbeiter und Unternehmen (ausführlich in Kapitel 4).

Technologien und Architekturen, typisch für das Web-basierte e-Business-Paradigma, werden in Kapitel 3 erläutert. Dort werden auch die in naher Zukunft zu erwartenden architekturellen Veränderungen für moderne und zukunftssichere e-Business-Plattformen insbesondere in Bezug auf den Einsatz von Web Services und die zunehmende Integration mobiler Anwendungen behandelt.

2.2 Evolution der Netzwerke

Während der letzten drei Dekaden hat sich das Internet zu einer einzigartigen, globalen Netz-Infrastruktur entwickelt, mit buchstäblich unbegrenztem Zugang zu Informationen und faszinierenden neuen Geschäftsmöglichkeiten.

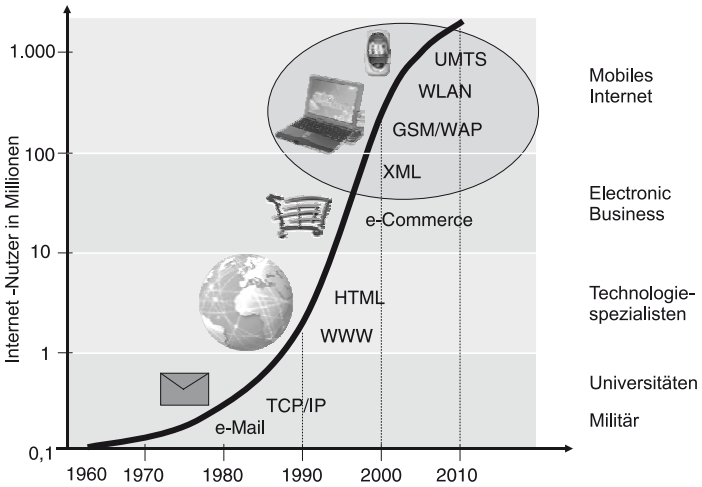


Bild 2.2 Evolution des Internet

In den siebziger Jahren waren die Vorläufer des Internet auf militärische Anwendungen und auf forschungsorientierte Aufgaben in Universitätsnetzen beschränkt. In den Achtzigerjahren wurde das Internet zum „Showcase" für Pioniere der Anwendung neuer Technologien. Schließlich begann in den 90ern mit der Geburt des e-Commerce eine spannende Ära, von der Wirtschaft und Geschäftsleben tiefgreifend tangiert wurden. Diese Entwicklung ist in Bild 2.2 dargestellt.

Das Internet und die Evolution der mobilen Technologien sind als Megatrends einzustufen. Die Konvergenz beider Entwicklungen wird nun zu einer neuen Ära führen – dem *mobilen Internet*. In der laufenden Dekade wird die Anzahl der Internet-Nutzer nochmals beträchtlich steigen und in wenigen Jahren wird die Anzahl der mobilen Teilnehmer deutlich überwiegen. Die Zugangsmöglichkeit über mobile Geräte wird das Internet zu einem „Everywhere Marketplace" machen und einen weiteren Anstoß für innovative Business-Modelle liefern.

Die technologische Evolution des Internet-Backbones in den letzten Jahren war überaus eindrucksvoll. Die Fortentwicklung der optischen Netzkomponenten, Glasfaser, Switches und Router gibt dem Internet-Backbone eine schier unglaubliche, fast unbegrenzte Übertragungsbandbreite. Die Kapazität von Glasfasern hat sich innerhalb eines Jahrzehnts um den Faktor 200 erhöht. Die Entwicklung der *DWDM(Dense Wavelength Division Multiplexing)*-Technologie macht nun Übertragungsraten von theoretisch mehr als 1Terabit/s möglich.

Gleichwohl muss eingeräumt werden, dass eine noch faszinierendere Entwicklung auf dem Gebiet der mobilen Funknetze stattgefunden hat. Im Folgenden werden diese Innovationen kurz erläutert. Es soll gezeigt werden, wie vielfältig und schnell sich diese Entwicklungen vollzogen haben; einige dieser Technologien waren vor fünf Jahren in konkreter Form noch gar nicht bekannt.

GSM

GSM (Global System for Mobile Communications) repräsentiert ein mobiles Kommunikationssystem der 2. Generation. Während die 1. Generation auf analoger Technologie basierte, setzte die 2. Generation auf Digitaltechnik, was signifikante Vorteile in Bezug auf Gesamtkosten, Qualität und Größe der mobilen Geräte mit sich brachte.

GSM [2.2.1], ein Europäischer Standard, wurde 1996 eingeführt und hat sich unter den mobilen Netztechnologien der 2. Generation weltweit zum erfolgreichsten System entwickelt. Mit einem Marktanteil von rund 70% sind GSM-Netze in mehr als 200 Ländern installiert. In naher Zukunft werden bald mehr als 1 Milliarde Teilnehmer durch GSM-Technik versorgt. GSM-Netze werden wegen ihrer Flächendeckung über das Jahr 2010 hinaus bestehen, obwohl GPRS und Netzwerke der 3. Generation dem Markt nach und nach wesentlich höhere Bandbreiten, verbesserte Qualität und eine Reihe von innovativen Anwendungen zur Verfügung stellen können.

GPRS

GPRS (General Packaged Radio System) ist als Weiterentwicklung von GSM zu sehen und umfasst Sprach- und erweiterte Datendienste. GPRS wurde seit 2002 in den meisten GSM-Netzen nachgerüstet und kann mit drei signifikanten Merkmalen bzw. Vorteilen sowohl für Netzbetreiber als auch für Teilnehmer aufwarten:

– Im Vergleich zur verbindungsorientierten (Circuit-switched) Technik bei GSM fallen geringere Verbindungskosten an. GPRS beruht auf einer verbindungslosen, paketorientierten (Packet-switched) Technik, wie sie auch im Internet Verwendung findet. Netzwerkressourcen werden dadurch effizienter genutzt. Anwendungen nehmen Ressourcen nur in Anspruch, wenn gerade Daten transferiert werden.
– Es steht eine größere Bandbreite zur Verfügung – vergleichbar mit ISDN –, wobei im sogenannten Burst Mode etwa die doppelte Übertragungsrate erreicht wird.
– GPRS unterstützt transparent das IP-Protokoll. GPRS kann dadurch einen nahtlosen Übergang zum Internet und zu Intranets bieten. Durch transparentes Tunneln des IP-Protokolls vom mobilen Gerät zum Internet oder Intranet erhält das Gerät denselben Status wie ein IP Server am LAN.

GPRS ist das erste mobile Netz, das die sogenannte „Always-on“-Konnektivität ermöglicht. Diese interessante Kombination von always-on und paketorientierter Übertragung mit einem volumenbasierten statt zeitorientierten Preismodell sowie mit einer zu ISDN vergleichbaren Bandbreite wird entscheidend dazu beitragen, dass mobile Datendienste sich schnell ausbreiten.

SMS/MMS

SMS (Short Message Service) wurde ursprünglich im GSM-Sprachnetz als erster Datenservice angeboten. Er erlaubt die asynchrone Übertragung von bis zu 160 Zeichen in einer Nachricht. Heutzutage unterstützt jedes GSM-Handy SMS. Mit weltweit mehr als 20 Milliarden Nachrichten pro Monat hat sich SMS zur sogenannten *Killer Application* herauskristallisiert.

MMS (Multimedia Message Services) stellen dagegen eine Kombination von SMS, Audio Message Service, Photo Message Service, Video Message Service and Group Message Service dar. Das bedeutet, dass ein mobiles Telefon, das MMS unterstützt, eine Nachricht senden oder empfangen kann, die eine beliebige Kombination der genannten Inhaltsformen enthält: Text, Audio, Foto, Grafik oder Video.

Im Business-Umfeld z. B. können Sprache oder geschriebene Kommentare an ein Sachverständigen-Foto angehängt werden oder auch an einen Video Clip, um anschaulich Wartungsanweisungen für eine komplizierte Maschine zu übermitteln. Der Group Message Service ermöglicht das Versenden einer MMS an eine vom Absender definierte Gruppe von Empfängern in einer einzigen Aktion. Das spart Zeit und Übertragungskosten. MMS wird schon in GPRS-Netzen unterstützt, wird sich aber wegen der benötigten Bandbreite erst in Netzen der 3. Generation voll entfalten können.

WAP

Das *WAP (Wireless Application Protocol)* ist ein Protokoll für die synchrone, bidirektionale Übertragung von Daten via mobile Netze zum Internet. WAP spezifiziert ein Application Framework und Netzwerk-Protokolle für drahtlose Geräte, vornehmlich mobile Telefone, optional auch PDAs. Es berücksichtigt die momentan noch gegebenen Einschränkungen bei Netzen und Geräten: limitierte Bandbreite, CPU-Leistung, Speicherplatz, Ein-Ausgabe.

Das Framework wurde im *WAP Forum* erarbeitet und erstmals 1999 vorgestellt. Später wurde das WAP Forum in die *Open Mobile Alliance* [2.2.2] integriert. Obwohl die Markteinführung von WAP alles andere als positiv verlief, ist WAP heute ein weltweit etablierter Internet-Zugangsstandard für mobile Geräte, der in Europa die größte Rolle spielt. Fast alle heutigen mobilen Telefone unterstützen WAP.

Das WAP-Modell wurde aus dem Web-Modell abgeleitet. Es ermöglicht Netzbetreibern, Software-Herstellern, Diensteanbietern und Firmen, Anwendungen zu entwickeln, die kompatibel und effizient auf einer Vielzahl von Anwendungsplattformen ablauffähig sind. WAP schließt auch eine sogenannte Microbrowser-Umgebung mit folgender Funktionalität ein:

- *Wireless Markup Language* (WML) – eine Präsentationssprache ähnlich HTML, jedoch einfacher
- *WML Script* – eine Script-Sprache ähnlich JavaScript
- *Content Formats* – ein Satz definierter Datenformate einschließlich Images, Telefonbuch und Kalender
- *Wireless Telephony Applications* (WTA) – Telefon-Services mit dazugehörigen Anwendungsschnittstellen.

Das *Wireless Session Protocol* (analog zu HTTP) betrifft die WAP-Anwendungsschicht und bietet konsistente Schnittstellen für verbindungsorientierte wie auch verbindungslose Services. Das *Wireless Datagram Protocol* (teilweise Analogie zu TCP/IP) liefert die allgemeinen Transport Services und entkoppelt die oberen Schichten von den spe-

zifischen Eigenschaften der verschiedenen mobilen Netze. Neben GSM und GPRS können das auch andere Netze sein, die z.B in Amerika oder Asien betrieben werden.

Weitere Details über WAP werden in den Kapiteln 4 (Architektur) und 6 (Security) behandelt.

i-mode

Als proprietäres Protokoll und Modell für den Internet-Zugang mit mobilen Geräten wurde *i-mode* bereits 1999 in Japan von dem dortigen größten Netzbetreiber NTT DoCoMo eingeführt. Im Gegensatz zu WAP war i-mode von Beginn an ein voller Erfolg.

Anstatt WML verwendet i-mode die Präsentationssprache *cHTML (compact HTML)*, die direkt aus HTML abgeleitet wurde. Von Anfang an basierte i-mode auf Paketübertragung, d.h. die Verbrauchskosten leiten sich ausschließlich aus den übertragenen Paketen ab und sind unabhängig von der Zeitdauer. Dieses Preismodell hat entscheidend zum wirtschaftlichen Erfolg von i-mode beigetragen. Ein weiterer wesentlicher Erfolgsfaktor für die schnelle Verbreitung in Asien war das von Nutzern geschätzte, breite Angebot an Services. Durch dieses „Win-Win"-Geschäftsmodell profitieren alle beteiligten Geschäftspartner, insbesondere auch die Anbieter von Inhalten.

Einige Netzbetreiber bieten i-mode nun auch in Europa an. Allerdings wird i-mode in Europa nicht von allen Geräteherstellern unterstützt, da es kein offener Standard ist. Im Wettbewerb mit WAP wird i-mode weder in Europa noch in Nordamerika eine wesentliche Rolle spielen.

WAP und i-mode sind beide als Übergangstechnologien einzustufen. In naher Zukunft wird es technische Lösungen bezüglich der genannten bisherigen Geräteeinschränkungen geben. Dann werden Internet-Protokolle auch in mobilen Geräten und Netzen direkt unterstützt und eine nahtlose Kommunikation in drahtlosen und drahtgebundenen IP-Netzen wird Realität.

Übergang auf Netze der 3. Generation

Die 3. Generation (3G) mobiler Kommunikationssysteme in Europa ist bekannt als *UMTS (Universal Mobile Telecommunication System)* [2.2.3] und wurde durch *ETSI (European Telecommunications Standards Institute)* standardisiert. UMTS schließt synchrone (Real-Time, z. B. für Sprache) und asynchrone Modi (z. B. für e-Mail) ein, wobei bewährte Mechanismen für die zuverlässige Übertragung von Sprache, Nachrichten und Daten Verwendung finden. Darüber hinaus können auch „Stream-Type"-Daten übertragen werden (z. B. Realzeit-Video-Übertragung). UMTS bietet sowohl verbindungsorientierte (Circuit-switched) als auch verbindungslose (Packet-switched, wie GPRS) Kommunikation.

UMTS kann zwar Übertragungsraten bis zu 2 Mbit/s liefern, doch trifft dies nur auf unbewegte Objekte zu. Fußgänger können lediglich mit einer Bandbreite bis zu 384 kbit/s und schneller bewegte Objekte (Kraftfahrzeuge) bis zu 144 kbit/s versorgt werden.

In Europa sind UMTS-Netze und -Services in einigen Ländern seit 2003 eingeführt. Mit einer breiteren Akzeptanz und Nutzung ist aber voraussichtlich erst ab 2005 zu rechnen. Es ist wohlbekannt, dass Netzbetreiber in einigen europäischen Ländern riesige Beträge für den Erwerb von UMTS-Lizenzen vorfinanzieren mussten (allein in Deutschland waren es rund 50 Milliarden €). Für den Aufbau der Netzinfrastruktur müssen Netzbeteiber abermals eine Investition von fast der gleichen Größenordnung vornehmen. Aus diesem Grund werden UMTS-Netze in den nächsten Jahren zwar weite Teile der Bevölkerung erreichen, eine Abdeckung durch UMTS-Netze wird jedoch keinesfalls flächendeckend zur Verfügung stehen, sondern sich eher auf dichtbesiedelte Gebiete beschränken.

UMTS wird dennoch neue Geschäftsszenarien eröffnen und eine Vielfalt innovativer Anwendungen wie Video-Konferenz, Video-Streaming und Video-on-Demand auf den Markt bringen. Bei Systemen der 3. Generation werden Teilnehmer in der Lage sein, Sprachqualität oder Videoqualität selbst zu bestimmen. Die Leistung wird dann je nach in Anspruch genommener Qualität bezahlt. In Kapitel 4 werden weitere Eigenschaften von UMTS unter dem Blickwinkel von Geschäftslösungen erläutert.

Die Migration von GSM (2G) nach UMTS (3G) wird durch sogenannte *2.5 Generation*-Technologien (2.5G) erleichtert. In den meisten europäischen Ländern wurde GPRS als sinnvoller Weg in Richtung 3G gewählt. Wie in Bild 2.3 dargestellt, sind in diesem Zusammenhang zwei weitere mobile Netztechnologien zu nennen – nämlich *HSCSD (High Speed Circuit Switched Data)* und *EDGE (Enhanced Data Rates for GSM Evolution)*. Allerdings spielen diese Netze zumindest in Europa keine mit GPRS vergleichbare Rolle.

HSCSD, eine ausschließlich verbindungsorientierte Technologie mit zu ISDN vergleichbarer Datenrate, ist bereits seit einigen Jahren verfügbar und kommt in der Regel

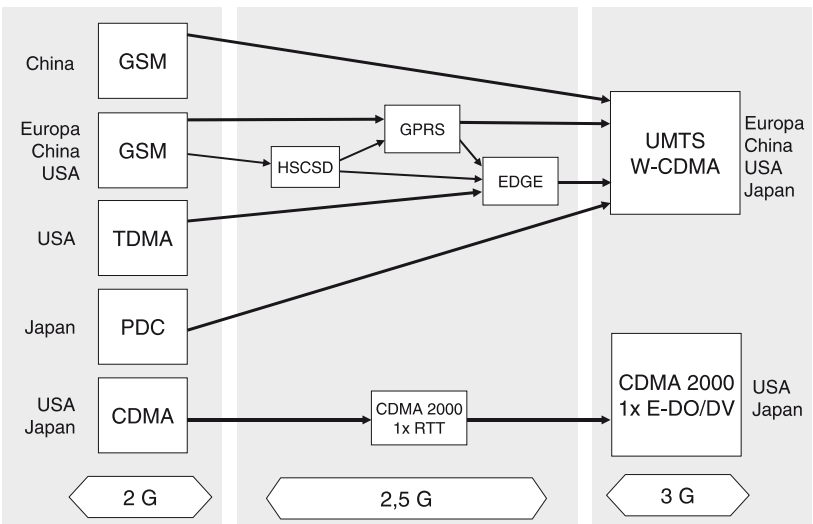


Bild 2.3 Migration der Netztechnologien von der 2. zur 3. Generation

für Nischenanwendungen in Frage, beispielsweise bei Punkt-zu-Punkt-Verbindungen oder erhöhten Security-Anforderungen.

EDGE erlaubt Übertragungsraten bis zu 384 kbit/s (verbindungsorientiert und verbindungslos). Eine größere Ausbreitung ist dennoch nicht zu erwarten, jedenfalls nicht in Europa, da diese Technologie zusätzliches Investment erfordert und kaum eher als UMTS zur Verfügung steht.

In Nordamerika ist die Situation allerdings anders. Hier weisen die anfangs vernachlässigten GSM-Netze nun hohe Zuwachsraten auf. Eine Migration auf EDGE macht Sinn, da EDGE als Weiterentwicklung sowohl von GSM- als auch von TDMA-Netzen geeignet ist. *TDMA(Time Division Multiple Access)*-Netze sind in Nordamerika weit verbreitet. Eine Zusammenführung der Netze wäre damit noch vor der Verfügbarkeit von 3G-Netzen möglich, und zwar mit einer akzeptablen, selbst für anspruchsvollere Anwendungen ausreichenden Bandbreite.

CDMA(Code Division Multiple Access)-Netze werden überwiegend in Nordamerika und Asien (Japan, Korea) eingesetzt und haben keine Auswirkungen auf Europäische Mobilnetze. Eine Weiterentwicklung findet über CDMA2000 1xRTT (2.5G, Bandbreite bis zu 300 kbit/s) zu CDMA 1xE-DO/DV (3G, Bandbreite bis zu 5 Mbit/s) statt.

3G-Netze wurden erstmals in Japan eingeführt. NTT DoCoMo installierte das *FOMA (Freedom of Mobile Multimedia Access)*-Netz bereits 2001. Von Anfang an hatte Asien eine Spitzenstellung inne, mit frühzeitig ausgebauten Netzen in Japan, Korea und Hongkong. Mittlerweile werden dort mehrere Millionen Teilnehmer mit 3G-Netzen versorgt.

Die Standardisierung von 3G-Netzen wird durch die *3GPP (3rd Generation Partnership Projects)* vorangetrieben. 3GPP [2.2.4] wurde 1998 als gemeinsame Projektgruppe gegründet, um die verschiedenen Standardorganisationen für die Telekommunikation zusammenzubringen. 3GPP befasst sich mit *W-CDMA (Wideband Code Division Multiple Access)*, der Basistechnologie von UMTS-Netzen, während 3GPP2 für die CDMA-Technologie zuständig ist.

Aufgrund der notwendigen erheblichen Investitionen für Netzinfrastrukturen und innovative Anwendungen ist die Konsolidierung der Netzbetreiberunternehmen durch Aufkäufe und Gründung von Allianzen derzeit voll im Gange. Jüngste Beispiele sind die Akquisition von AT&T Wireless durch Cingular Wireless LLC in den USA und die Gründung der Starmap Mobile Alliance durch neun kleinere Carrier in Europa.

Mobile Location Technologies (in GSM-, GPRS- und UMTS-Netzen)

Die Fähigkeit, die geographische Position eines mobilen Gerätes zu orten, ist entscheidend für Dienste, die im geographischen Kontext Informationen oder Mehrwert bieten und dadurch das mobile Business stimulieren. Es gibt zahlreiche Technologien, die dazu in der Lage sind.

Am einfachsten und schon seit Jahren im Einsatz ist die *COO(Cell of Origin)*-Methode. Netzbetreiber sind in der Lage, die Teilnehmernummer mit der Zelle zu verknüpfen, in der sich das Mobiltelefon jeweils befindet. Die Genauigkeit dieser Ortsbe-

stimmung variiert allerdings je nach Zellengröße von einigen 100 Metern (bei Zellen in Großstädten) bis zu einigen Kilometern (in ländlichen Gebieten).

Genauere Ergebnisse liefern die LFS *(Location Fixing Schemes)*, wie *GPS (Global Positioning System)*, *TDOA (Time Difference of Arrival)* und *E-OTD (Enhanced Observed Time Difference)*. GPS, heute überwiegend in Navigationssystemen eingesetzt, ist mit einer Toleranz von etwa 20 Metern das genaueste System und wird zunehmend auch in mobilen Geräten (PDAs, Handys) zum Einsatz kommen. Die beiden anderen Methoden erfordern Geräte- und Netzmodifikationen und erreichen je nach Umständen Genauigkeiten im Bereich von 50 bis 200 Metern.

Neben den erwähnten Technologien werden auch Ansätze verfolgt, die auf Software im Gerät basieren und in Standard-GSM/GPRS-Netzen mit einer Genauigkeit von immerhin etwa 100 Metern funktionieren.

Welche Verfahren sich auch immer durchsetzen, die ortsbezogenen (Location-dependent) Informationen werden sehr wahrscheinlich über die nächsten Jahre im Besitz der Netzbetreiber bleiben. Deshalb sind diese in der besten Ausgangsposition, innovative Location-dependent Services anzubieten. So könnte ein Netzbetreiber seinen Kunden, der gerade unterwegs ist, über SMS darüber informieren, dass sich in seiner Nähe z. B. eine Cafeteria, ein Kino oder ein Supermarkt mit Schnäppchenangeboten befindet.

Nun kommt es darauf an, die Anbieter mit den interessanten Inhalten, die mit geocodierten Informationen versehen sind, zusammenzubringen, um letztlich die entsprechenden Technologien in innovativen Anwendungen zu nutzen. Bereits bekannte Anwendungen, die mobile Location Services beinhalten, sind: Flotten-Management, Fahrwegüberwachung aus Sicherheitsgründen, Routenverfolgung bei Diebstahl, Telemetrie, Notfall-Services, Identifikation von Zielen (Points of Interest), Routenführung, ortsabhängige Werbeaktionen.

WLAN

WLAN(Wireless LAN)-Technologien wurden primär entwickelt, um die Verkabelung von Geräten und Systemen bei kürzeren Entfernungen zu vermeiden. WLAN kann auch als Erweiterung von existierenden LANs verstanden werden oder LANs sogar ersetzen. WLANs bieten den Vorteil, dass durch Eliminierung von Kabeln Kosten gespart werden und ein einfacher und flexibler Netzzugang ermöglicht wird.

WLAN ist wegen seiner begrenzten Reichweite (im Bereich von 100 Metern je Access Point) nur bedingt für eine großflächige Abdeckung geeignet. Da WLANs jedoch eine relativ hohe Datenrate erreichen (theoretisch bis 54 Mbit/s), oftmals zu günstigeren Kosten als vergleichbare Lösungen mit Mobilfunknetzen, sind sie eine willkommene Komplementärtechnologie und haben für bestimmte Anwendungsfälle sogar das Potenzial den Mobilfunk zu verdrängen. Dies zeigt das oft zitierte Beispiel des Geschäftsreisenden, der zur Überbrückung seiner Wartezeiten im Airport z. B. seine e-Mails über WLAN bearbeitet.

WLANs sind heute bereits weltweit in Zehntausenden Hotspots (Flughäfen, Ausstellungen, Konferenzzentren) sowie Hotels, Einkaufszentren und Cafes installiert. Einige

Großstädte ziehen sogar schon eine größere Ausdehnung solcher Hotspot-Gebiete in ihren Stadtgebieten in Erwägung. Zunehmend installieren auch Unternehmen WLANs in Konferenzräumen, Bibliotheken und Kundeninformationszentren. Mehr und mehr spielen WLANs auch eine wesentliche Rolle in Business Solutions, da sie gleichermaßen ein flexibles Kommunikationsnetz für Kunden, Partner und eigene Arbeitskräfte darstellen. Allerdings ist bei diesen Geschäftsanwendungen die Security-Thematik noch kritisch zu hinterfragen.

WLAN-Standards basieren auf den *802.11 LAN Standards*. Das *Institute* of *Electrical and Electronics Engineers (IEEE)* hat bereits 1990 die *802.11 WLAN Working Group* ins Leben gerufen. Damals war es Ziel, einen globalen Wireless-LAN-Standard festzulegen. Leider ist das nicht gelungen, und so haben sich bis heute verschiedene und teilweise inkompatible Standards im Markt durchgesetzt.

Der *Standard 802.11b* wurde zuerst eingeführt und ist immer noch weitverbreitet. Er basiert auf dem lizenzfreien 2.4-GHz-Frequenzband und kann theoretisch bis zu 11 Mbit/s übertragen. Eine Weiterentwicklung innerhalb dieses Frequenzspektrums, aufwärtskompatibel zu 802.11b, ist der *Standard 802.11g* mit einer maximalen Übertragungsrate von 54 Mbit/s. Dieser Standard hat sich stark ausgebreitet, und die meisten Anbieter liefern WLAN-Netzkarten, die sowohl 11b als auch 11g unterstützen.

Der neuere *Standard 802.11a* basiert auf dem lizenzfreien 5.2-GHz-Frequenzband. Zwar ist die maximale Übertragungsrate ebenfalls 54 Mbit/s, jedoch ist 11a inkompatibel zu 11b/g. Dieser Standard ist bezüglich seiner Bandbreite von Vorteil, da sich weniger Kanäle gegenseitig überlappen. Dadurch kann eine größere Anzahl gleichzeitiger Nutzer in einer WLAN-Zelle versorgt werden. Allerdings gibt es auch einen Nachteil: In einigen Ländern ist das 5,2-GHz-Frequenzband noch nicht freigegeben. Sicher werden Hersteller auch Netzkarten anbieten, die sowohl Standard 11g als auch 11a unterstützen.

Die als (theoretisches) Maximum angegeben Datenraten können allerdings in der Praxis nicht erreicht werden. Abhängig von der Entfernung des Gerätes zum *WLAN Access Point* und der Anzahl der gleichzeitigen Nutzer in einer Zelle (es sollten nicht mehr als 20 sein), liegt die tatsächlich erreichte Übertragungsrate häufig nur etwa bei 10% der maximalen Rate.

Weitere WLAN-Standards wie WEP, WPA und 802.11i befassen sich mit Security-Themen und werden ausführlicher in Kapitel 6 behandelt.

Die *WECA (Wireless Ethernet Compatibility Alliance)* [2.2.5] testet 802.11-Produkte mit dem Ziel, Interoperabilität zu gewährleisten. Alle Produkte, die diese Spezifikation voll erfüllen, erhalten das *WiFi-Logo*.

Bluetooth

Bluetooth wurde 1994 durch eine Studie von Ericsson initiiert und wird seit 1998 aktiv von der *SIG (Special Interest Group)* promotet. Die SIG wurde gemeinsam von Ericsson, Nokia, Intel, IBM und Toshiba gegründet. Seither sind mehrere Hundert andere Firmen beigetreten.

Bluetooth, seit 2002 in breiterem Einsatz, ist eine „Low-Power"-Funktechnologie, die in erster Linie Kabel und Infrarot-Verbindungen für kürzeste Entfernungen (bis zu 10 Metern) ersetzen soll. Geräte wie Laptops, Drucker, Mobiltelefone und PDAs können über einen speziellen Chip im Gerät miteinander kommunizieren und Daten austauschen.

Eine Bluetooth-Schlüsselanwendung ist die Synchronisation verschiedener Geräte wie PCs, Mobiltelefone und PDAs. Die Eingabe von Daten an nur einem Gerät genügt, alle anderen können dann synchronisiert werden. Weitere interessante Anwendungsgebiete sind z. B. Ticketing, Anwendungen mit POS(Point of Sales)-Terminals und Applikationen, die mit mobilem Handel zu tun haben. Bluetooth-Technologie erlaubt eine nahtlose Kommunikation auch durch nicht-metallische Wände hindurch.

Bluetooth kann z. B. bei Mobiltelefonen mit der Trennung von Hörer, Anzeige und Empfangsteil noch ganz anders genutzt werden. Während das Empfangsteil in der Tasche steckt und der Hörer drahtlos am Ohr sitzt, kann die Anzeige ebenfalls drahtlos in einer Armbanduhr untergebracht sein. Bluetooth bietet hier das Potenzial, Mobiltelefone in persönliche Lifestyle Accessoires zu verwandeln.

Da Bluetooth eine Bandbreite bis zu 1 Mbit/s (real etwa 400 bis 700 kbit/s) bietet und nicht auf Punkt-zu-Punkt-Verbindungen limitiert ist, kann es auch bei Wireless-LAN-Anwendungen zum Einsatz kommen. Schnell und einfach lassen sich *Ad-hoc*-Netze konfigurieren. Z. B. können Teilnehmer einer Besprechung untereinander ad hoc ein sogenanntes Piconet generieren, um Dokumente auszutauschen. Außerdem kann ein Bluetooth-Gerät auch als eine Art „Short-Range Internet Bridge" fungieren, die Zugang zum Internet ermöglicht.

Aufgrund der vielfältigen Anwendungsmöglichkeiten sind für Bluetooth verschiedene Profile definiert worden, die eine Interoperabilität in den jeweiligen Anwendungsbereichen sicherstellen sollen. Profile zeigen an, welche Funktionalitäten von einem Gerät unterstützt werden, damit es mit anderen Geräten der gleichen Profildefinition kommunizieren kann.

Einer breiteren Akzeptanz in Business Solutions stehen leider auch bei Bluetooth noch unzureichend gelöste Security-Themen und Kompatibilitätsschwächen im Weg (Information dazu in Kapitel 6).

Bluetooth-Standards werden durch die Bluetooth Special Interest Group [2.2.6] spezifiziert.

Einordnung der mobilen Netztechnologien

Die oben erläuterten mobilen Netze bilden miteinander ein umfassendes Netzwerk aus komplementären Netztechnologien, die das volle Spektrum von den kleinsten lokalen Funkzellen (Bluetooth, WLAN) bis zu den globalen Netzen (GSM, GPRS) komplett abdecken, wie in Bild 2.4 dargestellt.

Wie erläutert, weisen diese Netztechnologien unterschiedliche Charakteristika in Bezug auf Reichweite, Bandbreite, Standards, Kosten, Quality of Services und Anwendungsschwerpunkte auf. Auch wenn es in einzelnen Bereichen durchaus zu Überlap-

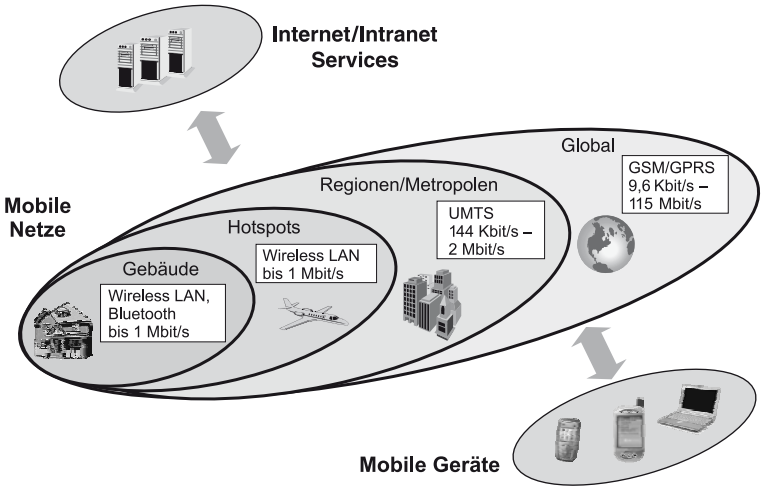


Bild 2.4 Übersicht mobiler Netztechnologien

pungen kommen mag, z. B. zwischen Bluetooth und WLAN in Gebäuden oder zwischen UMTS und WLAN in Metropolen, so heißt das Schlüsselwort doch Komplementarität. Das bedeutet, dass jede dieser Technologien ihren festen Stellenwert hat und sich daran in absehbarer Zukunft nichts ändern wird.

Bei all diesen Netzen gibt es heute eindeutig einen gemeinsamen Trend zur Konvergenz von Sprache und Daten auf Basis von IP-Netzen und Internet-Protokollen. Diese Konvergenz ist von besonderer Bedeutung und die einzig vernünftige Antwort auf die zunehmende Netzkomplexität. Vorangetrieben wird sie vor allem durch wirtschaftliche Überlegungen und offensichtliche Vorteile einer übergangslosen Kommunikation. Die Digitalisierung beliebiger Inhalte wie Text, Daten, Sprache, Grafik, Bild, Video und Multimedia ist eine wesentliche Voraussetzung für ein nach außen einheitlich erscheinendes Netzwerk und wird die Konvergenzbestrebungen zusätzlich stimulieren. Technologien wie VoIP (Voice over IP) und die Adaption der IP-Protokolle in den verschiedenen Zugangsnetzen werden diese Entwicklung ebenfalls rasch voranbringen.

Das hehre Ziel einer nahtlosen Kommunikation mit Services jeder Art, die in heterogenen Netzen angeboten werden und unter Nutzung beliebiger Geräte überall uneingeschränkt in Anspruch genommen werden können, wird wohl in naher Zukunft noch nicht erreichbar sein. In absehbarer Zeit werden sich jedoch Hürden wie unterschiedliche Protokolle, Einschränkungen bei Netzübergängen (Roaming) und Geräte-Restriktionen überwinden lassen.

Lesern, die sich ausführlich über die Vielfalt der mobilen Netze informieren wollen, sei das Buch *GPRS and 3G wireless applications: Professional developer's guide* [2.2.7] empfohlen.

2.3 Evolution der mobilen Geräte

Mobile Geräte für Kommunikation und IT sind seit mehr als 10 Jahren in Gebrauch. Die Vorfahren der heutigen Generation waren ziemlich unhandlich (tragbare PCs, analoge Mobiltelefone) oder funktional eingeschränkt (Pager). Zwei Trends haben die spannende Evolution der letzten Jahre mit einer fast explosionsartigen Vielfalt von eindrucksvollen Geräten forciert beeinflusst: die schnell wachsende Netzinfrastruktur und die Miniaturisierung von elektronischen Bausteinen.

Mobile Geräte wie *Mobiltelefone*, *Smartphones, PDAs* und *Tablet PCs* zählen zu den technologisch am höchsten entwickelten Geräten. Sie beinhalten eine Vielzahl neuester technologischer Errungenschaften: leistungsfähige Signalprozessoren und CPUs, modernste Funkmodule, Speichertechnologien, LCDs und CCDs, Langzeitakkus, Spracherkennung und umfangreiche Software. Insbesondere die Softwareentwicklung ist beeindruckend. Software macht heute etwa 70% der Wertschöpfungskette eines Mobiltelefons aus. In weniger als drei Jahren hat sich die durchschnittliche Anzahl der „Lines of Code“ auf über vier Millionen nahezu vervierfacht.

Die Kombination dieser sich rasch entwickelnden Technologien mit immer anspruchsvolleren Wünschen der privaten und geschäftlichen Anwender hat besonders in den letzten zwei Jahren zu einer breiten Angebotspalette innovativer Geräte geführt. Einige Beispiele sind in Bild 2.5 illustriert.

Ohne vollständig zu sein, erstreckt sich die Liste der Gerätekategorien von Mode-Accessoires über einfache WAP-Telefone, Business-orientierte Smartphones und PDAs, Laptops, Tablet PCs, Webpads bis zu Fahrzeug-Navigationssytemen.

Die interessantesten Weiterentwicklungen sind zukünftig in den Kategorien Fashion Phones, Smartphones und PDAs zu erwarten.

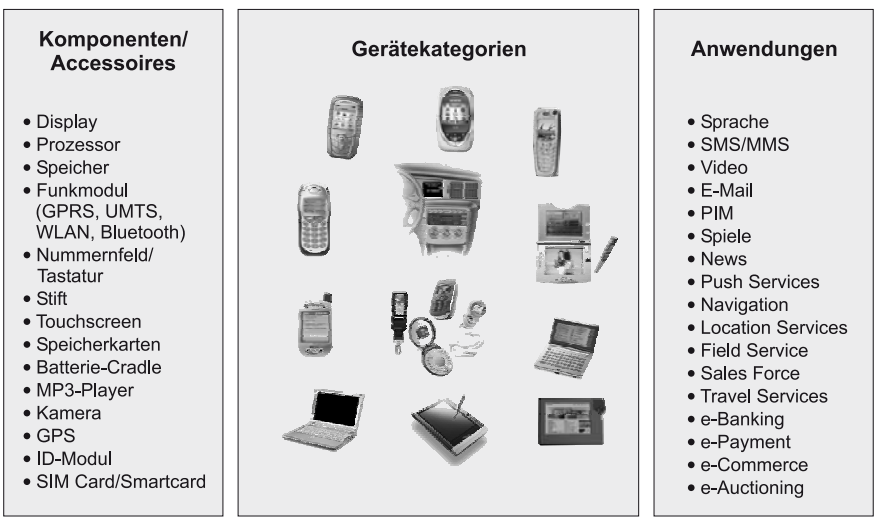


Bild 2.5 Angebotspalette mobiler Geräte

Ein Beispiel für die Fashion-Kategorie ist die Siemens *Xelibri-Familie*. Zielgruppe dieser trendigen Handys sind modebewusste Käufer, die diese Geräte vor allem als attraktives Schmuckstück betrachten. Dem Publikumsgeschmack entsprechend bieten solche Geräte Displays mit 4096 Farben, erweiterte Spracheingabe und polyphone Klingeltöne. Zu Gunsten der Spracheingabe wird gänzlich auf Nummern- und Navigationstasten verzichtet. Die Spracheingabe ermöglicht die vollständige Bedienung des Gerätes, einschließlich des enthaltenen FM-Radios.

Im Gegensatz dazu werden Smartphones und PDAs eine wichtige Rolle in zukünftigen Business Solutions spielen.

Smartphones wie z. B. das Nokia 6600 oder Siemens SX1 basieren auf dem offenen Betriebssystem Series 60, das u.a. einen verbesserten *XHTML Browser* enthält mit Zugang sowohl zu Web- als auch zu WAP-Inhalten, eine erweiterte *PIM(Personal Information Management)*-Funktionalität aufweist und das es erlaubt, Anwendungen über das mobile Netz auf das Gerät zu laden. Solche Geräte sind in der Regel auch mit faszinierenden Multimedia-Funktionen ausgestattet. So können z. B. aus dem Netz Videospiele heruntergeladen und abgespielt werden oder die Geräte verfügen über eine integrierte Videokamera. Darüber hinaus sind Bluetooth- und Multiband-Unterstützung wie GSM, GPRS und HSCSD (später auch UMTS) State-of-the-Art.

Der Wettbewerb in dieser Geräteklasse wird zunehmend härter. Die wichtigsten Hersteller im Rennen um Marktanteile sind in Europa Nokia und Siemens, in USA Motorola und in Asien Samsung und Sony Ericsson. *Series 60* ist das dominierende Betriebssystem in der Smartphone-Geräteklasse mit einem Marktanteil von etwa 75%. Der andere Mitspieler von wachsender Bedeutung in dieser Kategorie wird aller Wahrscheinlichkeit nach Microsoft mit seinem Betriebssystem *Windows Mobile* sein. Weitere Einzelheiten sind in Kapitel 4 nachzulesen.

Die Geräteklasse der PDAs hat sich in den letzten Jahren im Wesentlichen in zwei Richtungen weiterentwickelt: Netzwerkfähigkeit und Funktionserweiterungen durch externe Interfaces. Heutzutage sind PDAs mit integrierten Netzmodulen, meistens Bluetooth und WLAN oder GPRS, ausgestattet bzw. können entsprechende Netzkarten eingesteckt werden. Neuere Modelle verfügen sogar gleichzeitig über Bluetooth-, WLAN- und GPRS-Module. Zunehmend wird auch, wie bei Toshibas e800, die Funktion *Voice over IP* angeboten. Der Anwender erhält damit die Möglichkeit, Sprachverbindungen und insbesondere Fernverbindungen kostensparend über WLANs abzuwickeln.

Aufgrund der Vielfalt der verfügbaren Interface-Karten wie z. B. GPS-Module, steckbare Kameras, Speicherkarten, Smartcards, SIM Cards, Tastaturen und MP3 Player können PDAs nun beliebig konfiguriert werden, und zwar gleichermaßen für private wie für geschäftliche Zwecke.

Auch diese Geräteklasse wird seit Jahren heftig im Wettbewerb umkämpft. Die führenden Hersteller, HP, Palm, Handspring, Sony, Toshiba, Fujitsu Siemens und Dell bringen in kurzen Abständen immer neue Geräte und Funktionen auf den Markt. Die dominierenden Betriebssysteme sind *Palm OS* von Palmsource und Microsofts Windows Mobile (Pocket PC). Jedoch steht auch hier schon *Linux* in den Startlöchern und *RIM*

(Research in Motion), eine kanadische Firma, versucht mit einem interessanten always-on-Konzept und handlichem PDA (BlackBerry) Marktanteile zu gewinnen (weitere Einzelheiten in Kapitel 4).

Die Konvergenz zwischen Smartphones und PDAs wird immer offensichtlicher und es dürfte spannend werden, die rasante Weiterentwicklung dieser Geräteklassen zu beobachten. Zweifellos verfügen Smartphones über die bessere Sprachfunktionalität. Andererseits sind PDAs mit allen möglichen Interfaces ausgestattet. Tatsache ist, dass Smartphones derzeit höhere Wachstumsraten aufweisen. Je weiter die Integration von Komponenten fortschreitet, umso attraktivere Smartphones/PDAs mit unterschiedlichen Formfaktoren werden den Markt bereichern.

Im Kontext mobiler Business Solutions mit Zugang zu sensitiven Unternehmensressourcen werden angemessene Security-Funktionen und -Maßnahmen eine entscheidende Rolle spielen. Diese Security-Überlegungen werden ausführlich in Kapitel 6 behandelt.

3 Architektur zukunftsorientierter e-Business-Lösungen

E-Business-Lösungen sind heute in der Regel auf der Basis heterogener Architekturen, Systemplattformen und Anwendungen realisiert. Aus diesem Grund sind Anwendungen untereinander nur beschränkt interoperabel.

In der Vergangenheit investierten Unternehmen umfangreich in sogenannte „Best-of-Breed"-Produkte, um ihre Business-Prozesse optimal zu unterstützen. In der Zwischenzeit hat sich eine gewisse Desillusionierung breit gemacht, gleichzeitig hat auch der Druck auf die IT-Organisationen enorm zugenommen. Die Unternehmen stehen unter Zugzwang: Sie müssen Kosten reduzieren und ihre Flexibilität steigern, mit dem Ziel, letztendlich Gewinne zu generieren.

Von den IT-Verantwortlichen wird verlangt, mit einer heterogenen Systemlandschaft zurechtzukommen und trotzdem die dringlichsten Business-Anforderungen zu erfüllen. Mehr noch, CIOs sind gezwungen, IT-Infrastrukturen und -Architekturen zukunftssicher zu modernisieren, damit die IT anpassungsfähiger wird und innovative, funktionsübergreifende Prozesse unterstützt werden können.

Die gute Nachricht ist, dass nun auch Software-Hersteller den Ernst der Lage erkannt haben und mehr denn je Spezifikationen für geeignete technische und geschäftsrelevante Standards vorantreiben.

Die folgenden Abschnitte zeigen im Überblick die grundlegenden Bausteine einer zukunftsorientierten Architektur und ihre Funktionen in modernen Business-Lösungen.

3.1 Entwicklung von Anwendungen

Die Anwendungsentwicklung ist seit jeher ein Schlüsselthema bei der Realisierung von Geschäftslösungen. Visuelle Tools für das *GUI (Graphical User Interface)* helfen, das Benutzer-Interface optimal zu gestalten. Sie erlauben es, das Layout, die Steuerung und die Ausgabeelemente mittels „Drag-and-Drop"-Mechanismen zu definieren, ohne dass heute noch explizit codiert werden muss. In diesem Kontext sind Technologien, die eine Vielzahl sehr unterschiedlicher mobiler Geräte unterstützen, zunehmend gefragt. Visuelle Tools für die Implementierung von Datenbankzugriffen oder Web Services sind ebenfalls bereits verfügbar.

Entwicklungsumgebungen sind häufig auf spezifische Betriebssysteme oder Middleware-Plattformen wie Microsofts .NET oder IBMs WebSphere optimiert. IBMs *Eclipse*-Entwicklungswerkzeuge sind seit 2003 als Open Source Framework für jedermann verfügbar. Auf der Basis von Eclipse haben nun andere Software-Hersteller ihre Entwicklungswerkzeuge auf ihre spezifischen Umgebungen angepasst. Ein Beispiel ist SAP, deren Entscheidung, ein Java-Entwicklungstool für die neue *NetWeaver*-Plattform auszuwählen, zu Gunsten von Eclipse gefallen ist. Dadurch könnte sich Eclipse nach und nach zu einer Art Standard-Entwicklungsumgebung für die Java-Welt herausbilden.

Im Gegensatz dazu bietet Microsoft das proprietäre Visual Studio.NET ausschließlich für Microsoft-Plattformen an. Dieses Entwicklungswerkzeug wird von Experten als das beste und effizienteste eingeschätzt, das heute verfügbar ist.

Moderne Entwicklungsumgebungen lassen sich in der Regel einfach in Modellierungs- und Test-Tools integrieren und ergeben damit eine Standardumgebung für den gesamten Entwicklungsprozess.

3.1.1 Komponenten-basierte Software-Entwicklung

In den späten Achtzigerjahren begannen Programmierer und IT-Experten zu realisieren, dass umfangreiche Software-Projekte nicht nur exzessiven Ballast mit sich brachten, sondern darüber hinaus unflexibel zu managen und zu warten waren. Die meisten Anwendungen wurden für eine spezifische Aufgabenstellung programmiert, so dass der entstandene Code nicht mehr für andere Jobs wiederverwendet werden konnte. In Folge musste jede Anwendung wieder von Grund auf neu programmiert werden.

Design-Experten erfanden damals die Objekt-orientierte Programmierung, ein modularer Ansatz, der die Idee des wiederverwendbaren Codes formalisierte. Objekt-orientierte Programmierung ermöglichte erstmals das Zusammenbinden von wiederverwendbaren Objekten zu einer vollständigen Anwendung. Es folgte dann die Einführung des Software-Komponenten-Modells. Es wendete die Prinzipien der Objekt-orientierten Programmierung an, mit dem Ergebnis, dass Entwickler Anwendungen durch das Assemblieren diskreter Komponenten generieren konnten.

Mit diesem Modell konnte ein wichtiges Ziel erreicht werden: die Modularisierung von komplexen Applikationen mit gleichzeitiger Steigerung von Effizienz und Flexibilität.

Komponenten-Technologie war die Voraussetzung dafür, Anwendungen konkret auf bestimmte Business-Prozesse zuschneiden zu können. Dabei sind Funktionalitäten in Komponenten verkapselt und diese werden zu Anwendungen assembliert, vereinfacht dargestellt in Bild 3.1.

Zur Unterstützung eines bestimmten Business-Prozesses führt die entsprechende Anwendung nacheinander Komponenten aus, die hier als *Business-Objekte* bezeichnet sind. Die Art und Weise, wie ein Business-Objekt angewendet wird, ist durch eine *Deployment Description* definiert, die zu jedem Objekt gehört. Sie ist in einem Business-Objekt-Verzeichnis gespeichert und wird zur Runtime (Programmausführung) in

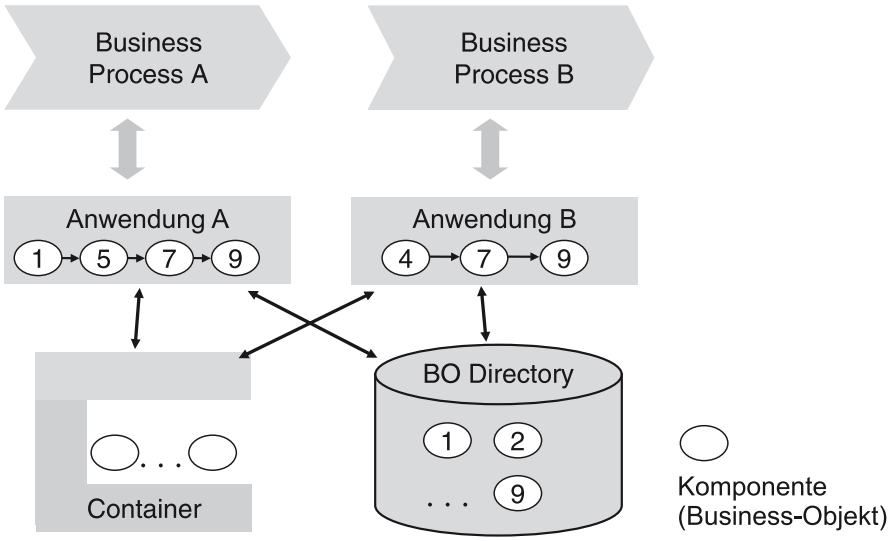


Bild 3.1 Komponenten-basiertes Anwendungsmodell

einem *Component Container* (Teil eines Application Server, siehe später) zum Ablauf gebracht.

Komponenten von existierenden Anwendungen können auch für neue Lösungen verwendet werden. Präsentation und Business-Logik ebenso wie Management von Ressourcen sind strikt voneinander getrennt und deshalb nicht mehr an eine spezifische Anwendung gebunden. Diese Separierung von Komponenten bedeutet, dass Teile von Anwendungen in beliebiger Weise kombiniert werden können. Die Kommunikation zwischen den Komponenten wird auf Basis einiger weniger Standards und Interfaces geregelt, die industrieweit akzeptiert sind.

Die Komponenten-Technologie bringt einige signifikante Vorteile mit sich:

– reduzierter Zeit- und Kostenaufwand aufgrund der Wiederverwendbarkeit von Komponenten
– reduzierte Komplexität durch Aufsplitten komplexer Applikationen in modulare Funktionskomponenten
– reduziertes Entwicklungrisiko dank der Möglichkeit, Teillösungen zu entwickeln und diese sukzessive zu erweitern
– verbesserte Qualität durch Verwendung bewährter Komponenten
– gesteigerte Flexibilität aufgrund von Erweiterungs- und Substitutionsmöglichkeiten von Komponenten in Anwendungen.

Lesern, die sich tiefergehend mit Komponenten-basierter Anwendungsentwicklung auseinandersetzen wollen, sei das Buch *IT-Lösungen im e-Business* [3.1.1] empfohlen.

3.1.2 Die beiden „Camps“

Seit es die Komponententechnologie gibt, bestimmen zwei „Camps“ den Wettbewerb. Diese Wettbewerbssituation hat sich als sehr fruchtbar erwiesen, denn abwechslungsweise haben jeweils beide Seiten die konkurrierenden Konzepte verbessert.

Die Camps werden einerseits von Microsoft mit dem jetzigen .NET Framework (früher COM+) und andererseits durch die Java-Welt mit J2EE (Java 2 Platform, Enterprise Edition) und Enterprise JavaBeans (EJBs) repräsentiert. Das Java Camp wird von Sun angeführt und von fast allen wesentlichen Software-Herstellern – natürlich außer Microsoft – unterstützt, wie z. B. IBM, HP, BEA, Oracle, SAP.

Ziel des Java Camps ist es, offenen Wettbewerb zu schaffen und gleichzeitig Best-of-Breed-Produkte zu fördern. Sun initiierte den Java Community Process (JCP), um neue Ideen schnell einzubinden. Die Java-Technologie besteht aus offenen Spezifikationen, auf deren Basis beliebige Hersteller dann entsprechende Produkte anbieten können. Kunden sind damit auch nicht mehr ganz so abhängig von bestimmten Software-Herstellern. Die J2EE-Architektur basiert ausschließlich auf der Java-Programmiersprache, und Java Code ist deshalb auf allen J2EE-Plattformen ablauffähig, soweit sie den Spezifikationen entsprechen.

Microsoft .NET, auf der anderen Seite, ist eine proprietäre Technologie. Microsoft bietet jedoch den Vorteil, dass es keine Kompromisse mit anderen eingehen muss und viele Funktionen des .NET-Laufzeitsystems eng mit dem Windows-Betriebssystem verknüpfen kann. Diese optimale Nutzung des Betriebssystems ist auch der Grund, dass vielfach behauptet wird, vergleichbare Anwendungen würden auf .NET Plattformen effizienter ablaufen.

Konzeptionell sind die beiden Anwendungsplattformen J2EE und .NET sehr ähnlich, wie Bild 3.2 illustriert.

Beide Plattformen basieren auf einer virtuellen Maschine, einem neutralen Zwischencode und einer gleichartigen Class Library. In Bezug auf ihre Architektur sind beide

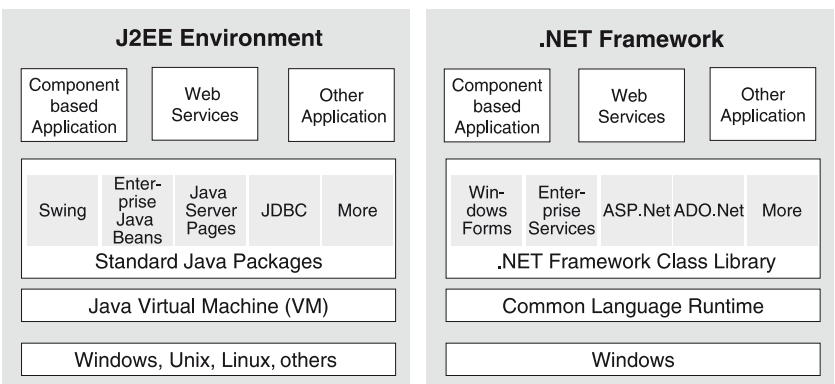


Bild 3.2 Java/J2EE versus .NET

Plattformen auf Server-basierende Verarbeitung mit Unterstützung verschiedener Front-Ends wie Browser, GUI Clients und mobiler Geräte ausgelegt. Es gibt ähnliche Module für GUI (Swing versus Windows Forms), HTML-Präsentation (Java Server Pages versus ASP.NET), Datenbankzugriff (JDBC versus ADO.NET), XML und Web Services. Die jeweiligen Application Server bieten miteinander vergleichbare Parallelverarbeitung, Session and Transaction Management sowie Adapter für Datenbanken und für Systeme von anderen Anbietern.

Als Microsoft die .NET-Technologie entwickelte, konnte die Firma das Beste aus der COM+-Technologie mit den bewährten Java-Konzepten zu einer technologisch moderneren Lösung verbinden. Das kommt z. B. mit der neuen Programmiersprache C# (als Weiterentwicklung von Java) sowie durch die konsistente Integration von XML und Web-Technologie zum Ausdruck. Was den Zugriff auf Daten betrifft, bietet nun Microsofts ADO.NET einiges mehr an Komfort als derzeit mit JDO/JDBC verfügbar ist. Auf der anderen Seite ist das Komponentenmodell Enterprise JavaBeans (EJB) methodisch weiter fortgeschritten als COM+, das als Basis für die Enterprise Services und Managed Components in .NET verwendet wurde. Dies unterstreicht die bereits erwähnte These, dass der Wettbewerb dieser beiden Konzepte dem Anwender zugute kommt, da die besten Funktionen immer abwechslungsweise im .NET und Java-Modell realisiert werden.

Die wirklich wesentlichen Unterschiede zwischen .NET und Java sind mehr auf strategischer Ebene zu finden. Java ist eine offene Technologie-Plattform, die alle nennenswerten Betriebssysteme einschließt und von vielen Software-Herstellern angeboten wird. Ebenfalls von Bedeutung ist, dass mittlerweile attraktive Open-Source-Produkte für alle Komponenten der Java-Technologie verfügbar sind. Diese Produkte, beispielsweise die von der Apache Group, sind nicht nur preiswert, sondern auch leistungsfähig und robust. Im Fall von Microsoft .NET kann positiv vermerkt werden, dass alles homogen aus einer Quelle stammt und damit klare Verantwortungen und rechtliche Rahmenbedingungen gegeben sind. Nachteilig ist allerdings die vollständige Abhängigkeit vom Hersteller.

3.1.3 XML – die „Lingua Franca“ des Internet

Eine der wichtigsten technologischen Entwicklungen ist wohl *XML (eXtensible Markup Language)*, eine Metasprache, die aus HTML und der Dokumenten-orientierten *SGML (Structured Generalized Markup Language)* entwickelt wurde und eine informationsorientierte Verarbeitung im Web erlaubt.

XML ist ein einzigartiger Ansatz zur umfassenden Kommunikation, Präsentation und Verarbeitung von beliebigen Daten. Es ist der Versuch, Information zu standardisieren, zu paketieren, zu strukturieren und zu transformieren, so dass sie auf unterschiedlichen Geräten dargestellt werden kann und sich Speicherung, Abruf und Austausch aller Informationsarten besser an die Bedürfnisse von Menschen und Organisationen anpassen lassen.

Als Metasprache ist XML mehr als nur ein Tool für die semantische Strukturierung von Informationen in Dokumenten. XML erlaubt es auch, Sprachen zu generieren, die eine

Verarbeitung von Informationen aller Art ermöglichen. Dies schließt Präsentation, Transfer, Zugang von Anwendungen auf die Informationsstruktur, Beschreibung der Beziehung zwischen Daten und Datenmodulen (Hyperlinks, Adressen) und Kommunikation zwischen Anwendungen ein. Viele Sprachen, die für die Verarbeitung von XML-Daten kreiert wurden, sind selbst aus XML abgeleitet.

XML ist die Zukunft des Web und wird häufig als *Lingua Franca* bezeichnet. Der entscheidende Faktor ist, dass XML beliebig auf die Bedürfnisse des Anwenders zugeschnitten werden kann, d.h. auf die Charakteristika der zu verarbeitenden Informationen und auch auf die besondere Aufgabenstellung in einer Anwendung.

Neben diesem enormen Potenzial repräsentiert XML auch gewisse Risiken. XML stellt keine Lösung dar, vielmehr ist es ein Werkzeug, um Lösungen zu entwickeln. Diese Lösungen sind ebenso gut oder schlecht wie die Konzepte, auf denen sie basieren.

Die XML-Technologie breitet sich rasant aus. Für viele Industriebranchen haben sich bereits spezifische *XML-Formate (Document Type Definitions, Schemes)* herausgebildet, die homogen und optimal Zugang, Austausch und Verarbeitung von branchenspezifischen Informationen erleichtern. Die wichtigsten Standardisierungsgremien in diesem Umfeld sind *ebXML* [3.1.2], *OASIS* [3.1.3] und *RosettaNet* [3.1.4].

XML, ein weltweit akzeptierter Industrie-Standard, wird von der *W3C Organization* [3.1.5] empfohlen. Ausführlichere Informationen über XML können bei *XML.Org* [3.1.6] recherchiert werden.

Die beiden Szenarien in Bild 3.3 illustrieren die durch XML gewonnene Flexibilität.

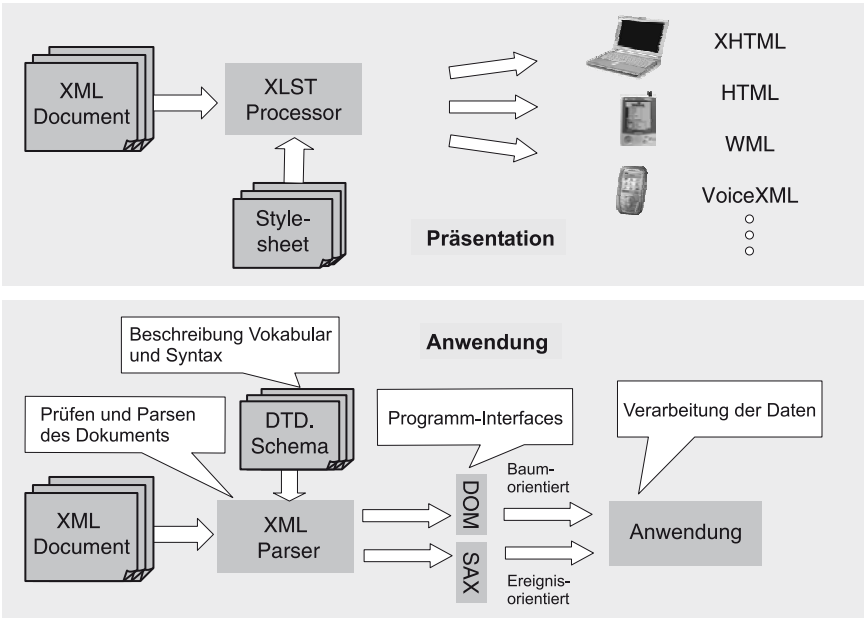


Bild 3.3 XML-Anwendungsszenarien

Das obere Szenario zeigt beispielhaft die verschiedenen Ausgabeformate, die aus einer einzigen XML-Dokumentenquelle erzeugt werden können.

Zu XML gibt es eine komplementäre Technologie namens *XSL (eXtensible Stylesheet Language)*, die eine Methode sowohl zur Formatierung von XML-Information als auch zur Transformation eines XML-Dokuments darstellt. Die Transformation geschieht durch sogenanntes *Pattern-matching* und *Template-based* Transformation.

XML Stylesheets zusammen mit einem *XSL Processor* sind in der Lage, XML-Dokumente in passende Präsentationsformen für beliebige Geräte zu transformieren.

Ein XML Stylesheet enthält einen Satz von Regeln zur Baumkonstruktion einer Dokumentenstruktur, bestehend aus zwei Komponenten. Die erste Regel stellt ein Schema (Pattern) dar, das Elemente (Knoten) des Quellbaums identifiziert, und die zweite eine Vorlage (Template), mit deren Hilfe ein Teilbaum des Zieldokumentes erzeugt wird. Das Stylesheet enthält also eine Schablone der gewünschten Ergebnisstruktur und identifiziert die Daten im Quelldokument, um sie entsprechend in das Zieldokument einzusetzen.

Der XSL-Prozessor arbeitet die einzelnen Knoten des XML-Dokumentenbaums ab. Zunächst stellt er fest, welche Regeln auf ein *Root-Element* (Hauptknoten) anzuwenden sind. Nach Ausführung sucht er nach zugehörigen *Child-Elementen* (Unterknoten) und führt die entsprechenden Regeln aus, bis schließlich der ganze Baum abgearbeitet ist.

Das Szenario in Bild 3.3 unten zeigt, wie ein XML-Dokument von einem Programm verarbeitet werden kann.

Das Vokabular und die Syntax sind in einer *DTD (Document Type Definition)* oder in einem Schema definiert, das in der Regel ein branchenspezifisches Vokabular repräsentiert. Um auf ein öffentlich zugängliches *XML-Schema* zu verweisen, ist oftmals auch eine Referenz-URL in dem XML-Dokument enthalten. Diese URL zeigt auf ein referenziertes Schema und hat eine ähnliche Funktion wie ein Dictionary.

Das XML-Dokument wird durch einen *Software Parser* analysiert, bewertet und weiterverarbeitet. Darüber hinaus wurde die XML-Technologie durch Programmschnittstellen (APIs) erweitert. Diese sind u.a. *DOM (Document Object Model, tree-oriented)* und *SAX (Simple API for XML, event-oriented*) sowie *XLink, XPath* und *XPointer* [3.1.7].

Ein einfaches, aber effektives Beispiel für die Verarbeitung von XML-Dokumenten ist folgender Fall: Mehrere Vertragshändler benötigten bestimmte Produktinformationen aus der Datenbank ihres Autoherstellers, die in den unterschiedlichen Händlersystemen weiterverarbeitet werden sollten. Die Lösung wurde mittels SQL Statement implementiert, mit dessen Hilfe die relevanten Informationen aus der Datenbank extrahiert wurden. Dabei wurden unter Nutzung der Spaltenkennzeichnungen als *Tags* automatisch XML-Dokumente erzeugt. Diese XML-Dokumente wurden dann durch ein Konvertierungsprogramm verarbeitet, das schließlich die passenden Ausgangsformate für die unterschiedlichen Händlersysteme erzeugt hat.

XML Web Services

Von Anfang an war XML ein Plattform-neutraler, Standard-orientierter Ansatz einer Markup-Sprache, die für vielfältige Zwecke und insbesondere für den Austausch von Daten zwischen heterogenen Systemen vorgesehen war. Ausgehend vom XML-Standard kann das modulare Modell der XML Web Services als der nächste logische Entwicklungsschritt gesehen werden.

Um eine Programm-zu-Programm-Kommunikation auf der Basis von Web Services zu ermöglichen, bedurfte es zusätzlicher Spezifikationen, um die Services selbst zu definieren, die Services-Interfaces zu beschreiben und schließlich Mechanismen festzulegen, wie diese Services aufgerufen werden können.

Obwohl mittlerweile Komponentenmodelle wie J2EE/EJB and Microsofts .NET *Object Model* weite Verbreitung und Akzeptanz in Unternehmen gefunden haben, konnten sie nicht erfolgreich in firmenübergreifenden oder technologieübergreifenden (Java-.NET)Projekten eingesetzt werden.

Im Wesentlichen ist dies zwei Gründen zuzuschreiben:

– Die Frameworks der beiden Software Camps sind nicht kompatibel. Die beiden Komponenten-basierten Modelle verwenden verschiedene Plattformen und Kommunikationsmechanismen. Eine J2EE-Applikation kann nicht ohne weiteres mit einer Applikation kommunizieren, die auf der .NET-Architektur basiert.
– Normalerweise werden in Unternehmen aus Sicherheitsgründen Firewalls eingesetzt. Beide Komponentenmodelle können diese Hindernisse nicht überwinden und sind schon deshalb für unternehmensübergreifende Anwendungen nicht geeignet.

Um genau diese Problematik zu lösen, haben eine Reihe von maßgeblichen Softwarefirmen, allen voran IBM und Microsoft, aber auch HP, Sun und Ariba in den späten neunziger Jahren begonnen, die Grundlagen für das Web-Services-Paradigma zu erarbeiten. Sie legten verschiedene Standardvorschläge vor, nämlich XML oberhalb HTTP als Basiskommunikation zwischen Komponenten, sowie eine Reihe von Spezifikationen zur Beschreibung von Services, der dazugehörigen Interfaces und des Mechanismus zum Aufrufen der Services. In Anlehnung an den XML-Standard werden diese Services häufig auch als *XML Web Services* bezeichnet.

Die drei wesentlichen XML Web Services Standards sind *Simple Object Access Protocol* (SOAP), *Web Services Description Language* (WSDL) und das Dictionary *Universal Description, Discovery, and Integration* (UDDI). Microsoft und IBM haben alle drei Entwicklungen maßgeblich vorangetrieben. Ein XML Web Service kann in beliebigen Programmiersprachen implementiert sein und auf unterschiedlichen Plattformen ablaufen, solange er konform zu diesen grundlegenden XML Web Services Standards ausgeführt ist. Eine ausführliche Darstellung des Themas Web Services, mit den Web Services Standards und der Erläuterung der Service-orientierten Architektur (SOA) ist in Kapitel 5 zu finden.

3.2 Multi-tier-Anwendungsarchitektur

Ziel einer unternehmensweiten Anwendungsarchitektur ist die Entwicklung von Anwendungen nach einheitlichen Richtlinien, damit sie untereinander effizient kommunizieren und kooperieren können, auf verschiedenen Plattformen ablauffähig sind und dem Benutzer gleichartig erscheinen. Wie in Bild 3.4 dargestellt, lassen sich moderne Anwendungsarchitekturen in vier Ebenen (Multi-tier) unterteilen: Kommunikations-/Präsentationsebene, Business-Logik-Ebene, Integrationsebene und Services-/Ressourcen-Ebene.

Anwendungen, die auf der Basis dieses Vier-Ebenen-Modells entwickelt werden, sind modular strukturiert, offen, flexibel, anpassungs- und erweiterungsfähig und können verteilt ausgestaltet sein. Dadurch lassen sie sich leichter an die Strukturen moderner Geschäftsprozesse anpassen und auf veränderte Anforderungen kann schneller reagiert werden.

Multi-tier-Architekturen setzen allerdings ein wohl durchdachtes Applikations- und System-Design voraus. An die Stelle monolithischer Programme treten spezialisierte, lose gekoppelte, interaktionsfähige Komponenten, die nach technischen und operationalen Gesichtspunkten jeweils auf verschiedenen Systemen und Plattformen lokalisiert werden können.

Wesentliche Charakteristika einer zukunftsorientierten, unternehmensweiten Anwendungsarchitektur für Design und Implementierung von Business-Lösungen sind:

– Trennung der Anwendung in mehrere Schichten: Präsentation, Business-Logik, Integration und Ressourcen, Services und Daten

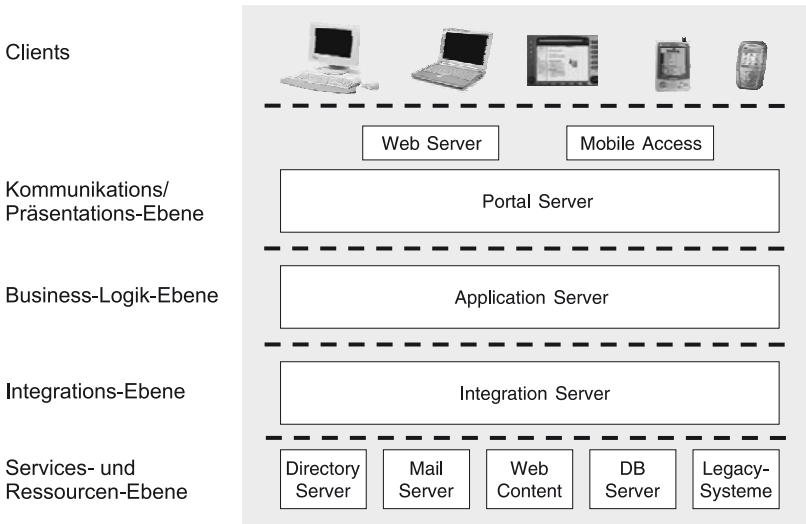


Bild 3.4 Multi-tier-Anwendungsarchitektur

- Verwendung von Web Browsern and Microbrowsern (für mobile Geräte) als das vorzugsweise gewählte Benutzer-Interface mit Unterstützung der relevanten Standards HTTP/HTML und WAP/WML
- Verwendung von Standard-Internet-Protokollen und Datenformaten (z. B. TCP/IP, FTP, SMTP, SSL, LDAP, JMS, XML)
- Verwendung von XML als universelles Datenaustauschformat und als Basis für die Geschäftsprozess-Kommunikation zwischen Unternehmen in Form von XML Web Services
- Nutzung von Komponententechnologien und der dazugehörigen Application Server
- Einsatz von dedizierten, funktionsoptimierten Servern wie Web Server, Portal Server, Application Server, Integration Server, Datenbank- und Directory Server.
- Integration von mobilen Technologien.

Kommunikations- und Präsentationsebene

Diese Ebene schließt die nutzer- und gerätespezifische Kommunikation zwischen Client und Server sowie die Präsentation von Informationen ein. Es geht darum, auf die Eingaben des jeweiligen Nutzers (Clients) zu antworten und die Information adäquat aufzubereiten. Die Kommunikations-/Präsentationsebene besteht aus den Systemkomponeten *Web Server* und *Mobile Access*.

Web Server

Web Server übertragen auf Anforderung eines Clients Web-Seiten via HTTP zu einem Web Browser. Der Web Server verfügt über sytemnahe Software-Module wie z. B. ein Modul zum Monitoring der Kommunikationskanäle und zur Analyse und Interpretation von eingehenden URL-Kommandos. Die wesentlichen Aufgaben eines Web Server sind:

- Analyse der eingehenden HTTP-Anfrage und direkte Rückantwort, falls Web Server über den angefragten Inhalt (Content) verfügt, andernfalls Weiterleitung an eine entsprechende ausführende Komponente (Skript oder Programm)
- Aufbereitung des HTML-Datenstroms und Übertragung der angefragten Web-Seite, so dass sie im Web Browser des Clients entsprechend interpretiert und angezeigt werden kann
- Falls kein eigener Application Server benötigt wird: Implementierung einfacher Business-Logik mit Server-basierten Scripting-Technologien, sowie Zugang zu Datenbanken.

Die meist verwendeten Technologien zur Aufbereitung von Web-Seiten sind:

- Java Server Page (.jsp) und Java Servlets in der J2EE-Entwicklungsumgebung
- Active Server Page.NET (.aspx) in der Microsoft Entwicklungsumgebung
- Web Server sind in der Lage, weit umfangreichere Aufgaben als lediglich die Aufbereitung und Übertragung von HTML-Seiten zu übernehmen. Sie können Business-Logik ausführen, auf Datenbanken zugreifen, Daten Browser-spezifisch aufbereiten oder sog. Applets an den Client übertragen, um Teilaufgaben der Business-Logik auf

dem Client ausführen zu lassen. Web Server mit mächtigem Funktionsumfang können deshalb zusätzlich auch der Ebene der Business-Logik zugeordnet werden.

Mobile Access

Eine Reihe von Protokollen und Formaten ist spezifisch für den Zugang zum Internet mit mobilen Geräten entwickelt worden. Wie in Kapitel 2 erläutert, ist *WAP (Wireless Application Protocol)* ein offener Standard für die Kommunikation von mobilen Geräten mit dem Internet. Das Protokoll ist unabhängig von Mobilnetz und Gerätetyp. Es berücksichtigt die limitierten Geräteeigenschaften von Mobiltelefonen und stellt eine effektive Kommunikation auch bei teilweise eingeschränkter Bandbreite sicher. Es unterstützt u.a. die Mobilfunknetze GSM, GPRS and UMTS. Bestandteil von WAP ist auch die Präsentationssprache *WML (Wireless Markup Language)* für einfache mobile Geräte.

Die *Mobile-Access*-Komponente enthält in der Regel die Funktion eines WAP Gateway, der sich um die Inhalte der mit mobilen Geräten auszutauschenden Informationen kümmert. Er setzt HTML oder andere Datenformate um und speichert oder erzeugt WML-Formate. WML-Inhalte liegen als solche bereits vor oder werden zur Laufzeit gerätespezifisch generiert. Dies kann mit Hilfe von *XSL Stylesheets* oder mittels Transcoding-Verfahren geschehen. Ein WAP Gateway stellt dabei die Verbindungsstelle zwischen Mobilfunknetz und Internet dar und setzt Mobilfunknetz-Protokolle in Internet-Protokolle um und umgekehrt. Immer häufiger sind heute WAP-Gateway-Funktionen in Portal Servern integriert (Details über die WAP-Architektur und Funktionalität sind in Kapitel 4 behandelt).

Neben WAP-Geräten unterstützen intelligentere mobile Geräte wie PDAs und Smartphones zwar optional auch das WAP-Protokoll, verwenden jedoch häufig nur die reinen Internet-Formate und -Protokolle HTML, TCP/IP und HTTP. Wiederum andere Geräte unterstützen das i-mode-Protokoll, das paketorientiert ist und als Präsentationssprache eine Art kompaktes HTML verwendet.

Services- und Ressourcen-Ebene

Diese Ebene enthält die sogenannten Legacy-Systeme, unternehmensweite Services wie z. B. e-Mail und Directory Services, sowie Datenbanken und Web Content Server. Da diese Systeme mehr oder weniger auf etablierten Technologien basieren, wird hier nicht weiter darauf eingegangen.

Business-Logik-Ebene und Integrationsebene

Im Gegensatz zur Services- und Ressourcen-Ebene befinden sich in der Business-Logik-Ebene und der Integrationsebene mit dem *Portal Server*, dem *Application Server* und dem *Integration Server* die Kernstücke einer modernen, zukunftsorientierten Anwendungsarchitektur. Hier haben sich die wesentlichen Innovationen in den letzten Jahren abgespielt. Ihre Architekturen und Funktionen werden deshalb in dem folgenden Abschnitt ausführlicher erläutert.

3.2.1 Portal Server

Portale entwickeln sich in vielen Unternehmen zum zentralen Einstiegspunkt für alle geschäftsrelevanten Vorgänge, einschließlich der Abwicklung von Transaktionen in verschiedensten Geschäftsprozessen. Nutzer solcher Portale sind Kunden, Geschäftspartner, Lieferanten und eigene Mitarbeiter.

Unternehmensportale vereinigen häufig unterschiedliche Unternehmensaufgaben in einem Portal, wie z. B. Kundenportal, Vermittlerportal, Außendienstportal, Innendienstportal, Zuliefererportal oder Redakteursportal. Sie haben sich mittlerweile auch zu einem Kernelement der unternehmensweiten Integration (People Integration) und der Interoperabilität zu Plattformen und Anwendungen anderer Hersteller entwickelt.

Portal Server, die für den Einsatz als Unternehmensportale geeignet sind, müssen laufend an verschiedenste Anforderungen der Unternehmen und ihrer Nutzer angepasst werden können. Für diesen zentralen Baustein moderner Lösungen ist deshalb eine modulare, flexible und zukunftssichere Architektur von besonderer Bedeutung. Voraussetzungen für geeignete Portale sind eine skalierbare Infrastruktur, hohe Verfügbarkeit sowie flexible Präsentations-Services, welche die Unterstützung mobiler Endgeräte ermöglichen. Weitere wesentliche Portal-Funktionen sind die Gewährleistung hoher Sicherheit durch adäquate Authentifikations- und Zugangskontroll-Mechanismen und komfortable Personalisierungsmöglichkeiten, die sowohl aus Sicht der Nutzer als auch aus Sicht des Unternehmens Optimierungsmöglichkeiten bieten. Portal Server sind Bestandteil einer modernen Middleware und somit vielfältig in das existierende IT-Umfeld eingebettet, wie in Bild 3.5 dargestellt.

Bei den konkreten Produktausprägungen verschiedener Hersteller ist der Portal Server in der Regel eine Komponente einer Application-Server-Familie, wobei der Application Server die Laufzeitumgebung und das Rückgrat für die über das Portal laufende

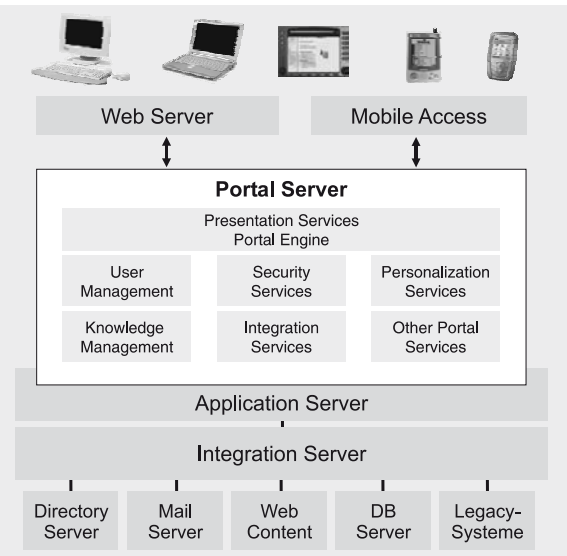


Bild 3.5
Portal Server

Transaktionsverarbeitung darstellt. Die existierenden Implementierungen führender Hersteller basieren alle auf Java-Standards (J2EE, EJB usw.) und sind weitgehend unabhängig von Hardware- und Software-Plattformen (Ausnahme Microsoft).

Führende Portale bieten heute die im Folgenden beschriebenen Technologien und generischen Services.

Portal Engine, Presentation Services

Technologisches Kernstück eines Portal Server ist die Portal Engine. Die *Portal Engine* analysiert eingehende Requests und startet entsprechende Komponenten, deren Aufgabe es ist, Ergebnisse in Form von sog. Portlets zurückzuliefern. Portlets sind die sichtbaren Komponenten, welche die Nutzer auf ihren Portalseiten sehen. Die Portlets werden entsprechend dem Seitenlayout in zugeordneten Frames zusammengestellt und zur Anzeige gebracht. Die Struktur der Seiten ist in der Regel in Template-Dateien (Java Server Pages Markups) definiert und flexibel anpassbar und änderbar. Die Seitenaufbereitung geschieht durch die *Presentation Services*, wobei Berechtigungen und individuelle Parameter des anfragenden Nutzers sowie die Spezifikation des verwendeten Endgerätes berücksichtigt werden.

Aus Sicht der Nutzer ist primär eine einfache, Web-basierte Benutzeroberfläche erwünscht, mit möglichst intuitiven Navigationsmöglichkeiten und Zugang zu allen Anwendungen, die für die Abwicklung ihrer Aufgaben erforderlich sind. Separate oder im Portal integrierte Web Server liefern die entsprechenden Portalinformationen im HTML-Format an Browser-basierte Geräte. Frames, welche die angefragten oder konfigurierten Inhalte (Portlets) wiedergeben, werden typischerweise mit einer Navigationsleiste und Verweisen auf untergeordnete Seiten ergänzt. Portlet-Inhalte können aus beliebigen Quellen stammen, z. B. Kataloge, Dokumente, Umsatzlisten, Adressbücher, Kalender, Worklists und Tickerleisten.

Der Einsatz mobiler Endgeräte (Laptops, PDAs, internetfähige Mobiltelefone) in Geschäftsprozessen (insbesondere B2E und B2C) wird in Zukunft stark zunehmen. Moderne Portal Server berücksichtigen diesen Trend durch integrierte Transcoding- und Rendering-Verfahren (Bestandteil der Presentation Services), die eine gerätespezifische Aufbereitung der Darstellungsinhalte bewerkstelligen. Portale müssen also in der Lage sein, Geräteklassen und ggf. auch Gerätetypen zu identifizieren, um eine geeignete Präsentation und Interaktion zu gewährleisten.

User Management

Das *User Management* hat die Aufgabe, die verschiedenen Nutzergruppen mit Zuweisung von Rollen und Berechtigungen zu verwalten. Die Benutzerverwaltung speichert die Nutzer- und Rollen-spezifischen Informationen, die in Bezug auf die abzuwickelnden Geschäftsprozesse benötigt werden. Nutzer haben die Möglichkeit, sich am Portal anzumelden und Präferenzen und Account-Informationen selbst zu verwalten. Alternativ können bestehende Informationen in den Portal Server integriert werden. In der Regel sind Nutzer und Rollen als Informationen im Portal Server gespeichert und werden mit existierenden Verzeichnissen über LDAP synchronisiert. Häufig enthalten

diese Verzeichnisse auch Berechtigungen und Zertifikate, die von einem CIO überwacht und verwaltet und von den Security-Systemen genutzt werden. Da sich Organisationen, Rollen und Berechtigungen häufig ändern, ist die administrative Einfachheit, Flexibilität und Sicherheit eines entsprechenden Management-Systems von hoher Bedeutung.

Personalization Services

Die *Personalization Services* tragen wesentlich zum Nutzeffekt von Unternehmensportalen bei. Aus der Sicht der Benutzer sind Einstellungen zum Portalinhalt und gerätespezifische Einstellungen, aber auch Präferenzen verschiedener Art, die Auswahl von Informationskanälen, das Ein- und Ausschalten von Notification Services usw. von Bedeutung. Aus Sicht der Unternehmen spielen das Benutzerprofil und die daraus abgeleiteten Regelungen und Berechtigungen in den jeweiligen Situationen eine wichtige Rolle. Aus Sicht von Informationsanbietern können aus dem Navigations- und Kaufverhalten Kundenprofile angelegt werden, die es ermöglichen, dynamisch zur Laufzeit passende Angebote einzublenden.

Die Personalisierung und einfache Menüführung spielt bei mobilen Geräten eine besondere Rolle, da der Anwender wegen der beschränkten Möglichkeiten der Geräte (geringer Informationsausschnitt, eingeschränkte Interaktion) direkt an die für ihn relevanten Informationen herangeführt werden muss.

Security Services

Da das Portal den zentralen Einstiegspunkt für Nutzer mit sehr unterschiedlichen Berechtigungen darstellt, sind *Security Services* unabdingbarer Bestandteil von Unternehmensportalen. Das Security-System kontrolliert die Authentifikation und Autorisierung der Portal-Nutzer und ermöglicht bei Bedarf eine verschlüsselte und/oder authentifizierte Datenübertragung. Darüber hinaus kann es bei Transaktionen Verbindlichkeit gewährleisten.

In den meisten Anwendungen erfolgt heute die Authentifikation mittels Benutzerkennung und Passwort. Führende Portalhersteller bieten aber auch PKI-Unterstützung (Public Key Infrastructure) und die Verwendung von digitalen Zertifikaten für Authentifikation und Verbindlichkeit an. Da Nutzer über den Portal Server Zugriff auf mehrere unabhängige Anwendungen haben, ist eine Single-Sign-on-Funktionalität zweckmäßig. Dazu erhält der Nutzer ein Ticket, das digital vom Portal Server unterzeichnet ist. Anwendungen (auch Third-Party-Anwendungen) können mit Hilfe entsprechender Portal-Bibliotheken dieses Ticket überprüfen und den Zugriff freischalten. Häufig bieten Portal Server auch Schnittstellen zu unabhängigen Authentifikationsprodukten (Details zum Thema Single Sign-on in Kapitel 6).

Die Autorisierung regelt den Zugriff von Nutzern bzw. Nutzergruppen bis auf Portlet-Ebene. Die Zugriffslisten für die jeweiligen Portlets werden von Administratoren abhängig von der Security Policy eines Unternehmens definiert.

Die Komplexität durchgängiger Security-Implementierungen wird häufig unterschätzt. Sichere Transaktionen sind nur durch eine durchgängige End-to-End Security gewährleistet. Diese schließt Endgeräte, Netze, Web Server, WAP Gateways, Portal und Application Server und Back-End-Systeme gleichermaßen mit ein (Details dazu in Kapitel 6).

Knowledge Management

Aufgabe des *Knowledge Management* ist das Auffinden und gezielte Auslesen der von Nutzern gewünschten, strukturierten, wie auch unstrukturierten Informationen. Das Knowledge Management umfasst Aggregation, Kategorisierung, Klassifikation und Verteilung von beliebigen, strukturierten und unstrukturierten Informationen, ebenso wie einfache und komplexe Suchfunktionen. Unternehmensdokumente können entsprechend sortiert abgelegt werden, des Weiteren sind Versionskontrolle sowie Verfahren und Flusskontrolle bei der Veröffentlichung von Bedeutung.

Integration Services

Die Integration existierender Anwendungen und Ressourcen in das Portal spielen eine entscheidende Rolle. Entsprechende *Integration Services* sind im Portal direkt implementiert oder vorhandene EAI-Komponenten eines existierenden Integration Server werden genutzt. Zugriffe auf Daten und Informationen oder Transaktionen müssen häufig unter Einbeziehung von Back-End-Systemen und externen Systemen bzw. Datenquellen abgewickelt werden. Die dazu erforderlichen Aufruf- und Umsetzungsmechanismen liefern die Integration Services. Diese Services stellen standardisierte Adapter in der Form von Portlets oder Remote Portlets zu häufig genutzten Informationsquellen (z. B. Reuters), internen Diensten (z. B. Mail) oder zu Anwendungen (z. B. SAP R/3) bereit.

Spezifische Adaptoren (z. B. zu Legacy-Systemen) lassen sich mit den Entwicklungskomponenten eines Application- oder Integration Server (J2EE, EJB, JSP, JCA) hinzufügen. Web Services beginnen gerade eine zentrale Rolle bei den Integration Services einzunehmen.

Weitere Services

Portal Server verfügen zwar in der Regel über eine Reihe von „Out-of-the-Box“-Funktionen, müssen aber je nach Aufgabenstellung des Unternehmens konfiguriert werden und können sehr unterschiedlich ausgeprägt sein. Oftmals wird eine optimale Ausgestaltung erst nach mehreren Monaten erreicht. Unternehmen erwarten deshalb eine einfache Portal-Entwicklungsumgebung, um eigene Portalkomponenten zu entwickeln und auf Marktänderungen rasch und flexibel reagieren zu können.

Je nach Hersteller der Entwicklungsumgebung können weitere Services Bestandteil des Portals sein; sie werden in Form von Portal-Services bereitgestellt. An erster Stelle sind hier *Collaboration Services* zu nennen. Diese bieten eine verbesserte Zusammenarbeit auch über Unternehmensgrenzen hinweg und ermöglichen verteilt agierenden

Projektteams, synchron und asynchron zu kommunizieren sowie Dokumente gemeinsam zu verwalten und zu bearbeiten.

Weitere optionale Portal-Services sind Publishing Services, Alert/Notification Services und Location-based Services, letztere sind von besonderem Wert für mobile Nutzer des Portals.

Durch das Zusammenwachsen von Informations- und Kommunikationsplattformen wird eine engere Kopplung zwischen Portal Servern und Help Desks erforderlich. Kundenkontakte werden heute sowohl über Internet- als auch über Telefon-Kanäle abgewickelt. Multichannel-Kundenkontakte, Kundenprofile und Zugang zu Back-End-Anwendungen sind für beide Services relevant, deshalb ist eine enge Integration anzustreben.

Portal Server sind in der Regel wegen der Verzahnung zum Knowledge Management und der Verwaltung von Web-Inhalten eng mit Content-Management-Systemen verzahnt. Zunehmend sind Content-Management-Funktionen aber auch Bestandteil von Portal Servern.

3.2.2 Application Server

Ein *Application Server* ist die Kernkomponente von Web-basierten Business-Anwendungen und stellt eine skalierbare Ablaufumgebung für Business-Komponenten und Transaktionsverarbeitung zur Verfügung. Application Server sind heute ausgereifte Produkte, die jedoch ständig weiterentwickelt werden. Die wesentlichen Elemente eines Application Server sind in Bild 3.6 aufgezeigt.

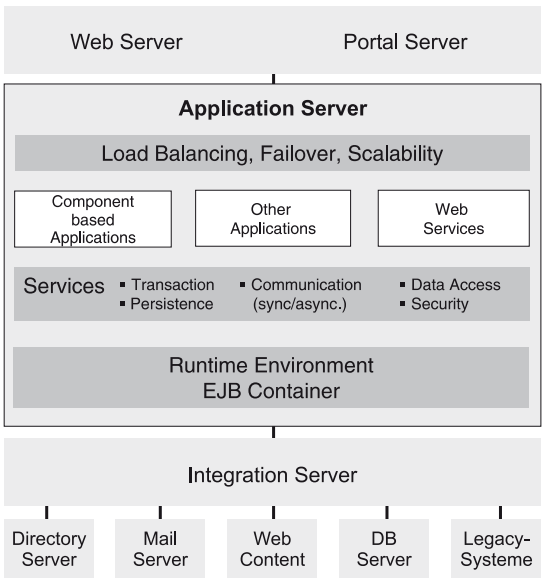


Bild 3.6
Application Server

Die zentrale Komponente des Application Server ist ein sogenannter Container, der die Ablaufumgebung für wiederverwendbare Software-Komponenten darstellt. Komponenten-Technologien wie Enterprise JavaBeans (EJBs) oder Microsoft COM+-Komponenten (in älterer Umgebung), oder .NET-managed Components in originären .NET-Applikationen sind heute überall im Einsatz.

Der Container stellt eine Reihe standardisierter Infrastruktur-Services für Software-Komponenten zur Verfügung. Dieses Konzept befreit Programmierer davon, sich mit komplexen System-relevanten Security-, Transaktions- und Kommunikations-Themen auseinandersetzen und hunderte APIs bedienen zu müssen. Stattdessen können sie sich auf die Implementierung der eigentlichen Business-Logik konzentrieren.

Diese Laufzeit-Services umfassen: Zugriff auf relationale Datenbanken und unstrukturierte Daten einschließlich Cache-Mechanismen zur Performance-Steigerung, Persistenz-Management, Management von Warteschlangen für asynchrone Kommunikation anwendungsspezifischer Nachrichten, Transaktions-Management, Priorisierung von Client-Anfragen und Prüfung von Benutzer-Identifikationen und Zugangsrechten sowie revisionssichere Aufzeichnung aller durchgeführten Aktionen.

Neben diesen Laufzeiteigenschaften muss eine professionelle Anwendungsplattform über eine reiche und produktive Entwicklungsumgebung verfügen und wiederverwendbare Server-seitige Komponenten unterstützen. In der Regel umfasst die Anwendungsentwicklung mehrere Programmiersprachen, visuelle Programmierhilfen, die Möglichkeit des Code-Debugging auch über verteilte Komponenten hinweg, Configuration Management sowie Interfaces, um Tools von anderen Herstellern integrieren zu können.

Application Server bieten auch die Laufzeitumgebung für Standard-Software-Pakete und andere Software, die nicht auf Komponenten-Technologie basiert. Die direkte Unterstützung von Web Services ist in den neueren Versionen der führenden Produkte bereits implementiert, wenngleich wegen des anhaltenden Standardisierungsprozesses laufend mit Weiterentwicklungen zu rechnen ist.

Eine wesentliche Aufgabe von Application Servern ist auch eine weit gespannte Skalierfähigkeit, da in vielen Anwendungsfällen die Anzahl der gleichzeitigen Nutzer nicht vorhersehbar ist. Dazu gehören auch die dynamische Lastverteilung und automatische Failover-Mechanismen in Cluster-Konfigurationen, um einen sicheren Betrieb zu gewährleisten.

Entsprechend der erwähnten Komponenten-Technologien gibt es zwei rivalisierende Application-Server-Plattformen, die sich im Markt etabliert haben. Auf der einen Seite sind dies die Java Application Server wie z. B. IBM WebSphere oder BEA WebLogic, auf der anderen Seite ist die Application-Server-Funktionalität implizit in Microsoft-Windows-Servern enthalten. In älteren Umgebungen (DNA, Distributed Network Architecture) ist die entsprechende Funktionalität im Windows-Betriebssystem integriert. Im .NET Framework werden die Application Services als .NET Enterprise Services bezeichnet, die ebenfalls Bestandteil des Windows-Server-Betriebssystems sind.

Java Application Server entsprechen der Spezifikation der Java 2 Enterprise Edition J2EE, bieten eine Reihe von Middleware Services und unterstützen APIs, die eine Implementierung von geschäftskritischen Web-Anwendungen zulassen. Die wichtigsten dieser Services und APIs sind:

- Java Server Pages (JSPs) für die Erstellung einfacher Web-Anwendungen (HTML-Anweisungen für den Browser werden durch Server-seitige Scripts generiert)
- JavaBeans für die Programmierung Client-seitiger Komponenten, z. B. für Layout- und Navigationselemente zur Gestaltung der Benutzeroberfläche
- Java Servlets für die Kommunikation mit dem integrierten Web Server, sowie zur Programmierung und Steuerung der Business-Logik
- Enterprise JavaBeans (EJBs) als wiederverwendbare Business-Logik-Komponenten und als System-bezogene Laufzeit-Services
- Java Naming and Directory Interface (JNDI) für Adressumsetzung und Ablage von Daten und Attributen in Directories
- Java Mail für das Senden und Empfangen von e-Mails
- Java Messaging Services (JMS) für die asynchrone Kommunikation mittels Warteschlangen-Technik
- Java Transaction Services und APIs (JTS/JTA) für die Transaktionsverarbeitung einschließlich der Synchronisation verteilter Datenbanken
- Java Database Connectivity (JDBC) für den Zugriff auf Datenbanken mittels standardisierter Aufrufe
- Java Connector Architecture (JCA) für eine standardisierte Connector-Technik von kundenspezifischen Anwendungen mit Standard-Paketen wie SAP, Siebel usw.; die JCA ist meist Bestandteil der EAI- (Enterprise Application Integration) Strategie eines Unternehmens
- Java API zum Analysieren von XML-Dokumenten (JAXP)
- Unterstützung von Protokollen für die synchrone Prozess-Kommunikation (RMI via IIOP), CORBA und XML Web Services (auch asynchron).

3.2.3 Integration Server

Integration Server repräsentieren insbesondere in komplexeren Anwendungsszenarien eine wesentliche Komponente der Anwendungsplattform. Sie stellen einen wichtigen Schritt in der Weiterentwicklung prozessorientierter Lösungen dar. Integration Server verbinden funktionale Elemente von Standard-Paketen, von eigenentwickelter Business-Logik und von Legacy-Systemen einschließlich der benötigten Daten so, dass Prozesse optimal unterstützt werden.

Das bisherige Verständnis der *Enterprise Application Integration* (EAI) hat sich in jüngerer Zeit zur umfassenderen *Business Integration* erweitert. Dieser neue Terminus betont in besonderem Maße das Business Process Management (BPM) und die B2B-Interoperabilität.

Bisher voneinander isoliert betriebene Anwendungen werden durch Business Integration so miteinander verflochten, dass Geschäftsprozesse effizienter unterstützt werden.

Solche Anwendungen sind in der Regel *Supply Chain Management* (SCM), *Enterprise Resource Planning* (ERP) und *Customer Relationship Management* (CRM), eigenentwickelte Anwendungen, Zugriff auf Datenbanken sowie ältere Anwendungen, die auf Hosts laufen. Business Integration kann sich über Unternehmensgrenzen hinweg erstrecken und ermöglicht *B2B-Business-Prozesse*, d.h. Geschäftsbeziehungen zu Zulieferern, Partnern und Kunden lassen sich effizient koordinieren. Außerdem werden elektronische Marktplätze zugänglich gemacht.

Integration Server müssen als zuverlässige Laufzeitplattform ausgeprägt sein, unabhängig davon, ob sie unternehmensintern oder für B2B-Anwendungen eingesetzt werden. Ebenso wichtig ist jedoch auch der Umfang der dazugehörigen Services und Tools. Auf jeden Fall sollten vielfältige vorintegrierte Adapter zum Anschluss von Back-End-Systemen, generisch definierte Business-Objekte, Datentransformations-Services und Tools für die Prozess-Modellierung und Simulation vorhanden sein. Ein weiterer Bestandteil sind *Workflow Engines*, die zur Steuerung der Prozessabläufe eingesetzt werden.

Integration Server – wie in Bild 3.7 gezeigt – lassen sich logisch in drei Funktionsschichten unterteilen. In der Netzwerkschicht unterscheidet man *Hub-and-Spoke*-(sternförmige Kopplung der Anwendungen) oder *Bus-orientierte Topologien*. Eine darüber liegende Kommunikationsschicht regelt das Kommunikationsverfahren. Die Alternativen sind hier *Message Broker* (Messaging von Nachrichten, asynchron, z. B. *Publish and Subscribe*), *Integration Broker* (Remote Procedure Calls von Business-Objekten, *Request/Response*, auch als *Business Object Broker* bezeichnet) und Web Services. In Schicht 3 geht es um das Management und die Ausführung von Business-Prozessen.

Die erste und insbesondere die zweite Schicht beeinflussen stark die Eignung eines Integration Server für verschiedene Integrationsanforderungen. Integration Broker sind zwar eher für komplexe Prozess-Integrationen geeignet, andererseits muss aber bei ihrem Einsatz von einem hohen Reengineering-Aufwand ausgegangen werden. Message Broker können mit geringerem Aufwand eingesetzt werden und eignen sich speziell für Nachrichten- und Datenaustausch und für entkoppelte, dezentrale Anwendungen oder Prozesse.

Web Services vereinen gewissermaßen die Vorteile von Message- und Integration-Brokern und deshalb kommt ihnen eine besondere Bedeutung bei der Business-Integration zu. Weitere Vorteile dieser Technologie sind offensichtlich: offene Standards, Unabhängigkeit von Anwendungsplattformen und Programmiersprachen sowie lose Kopplung von Anwendungen verschiedener Organisationen und Unternehmen. Die meisten Integration Server beinhalten heute bereits Web Services Frameworks und tragen damit dieser Entwicklung Rechnung.

Schicht 3 ist zuständig für die Prozess-Integration und das Business Process Management mit den Komponenten Prozessmodellierung und Workflow oder Business Process Engine.

Diese Schicht spielt eine zunehmend wichtige Rolle in zukunftsorientierten Lösungen. Alle wesentlichen Plattform-Anbieter bauen diese Funktionalitäten gerade stark aus.

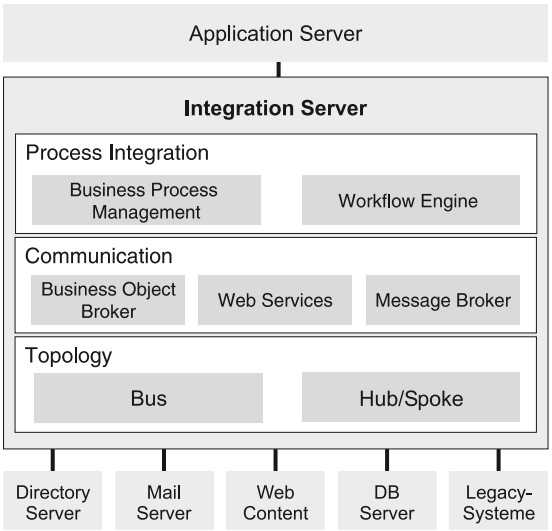


Bild 3.7
Integration Server

Prozess-Modellierungstools mit graphischer Unterstützung erlauben die Definition von Prozessabläufen in einfachen Schritten ohne technisches Hintergrundwissen. Workflow Engines steuern den Prozessablauf von einzelnen Aktivitäten, wobei Web Services oder eingebundene existierende Anwendungen die einzelnen Prozessschritte repräsentieren. Aktivitäten können dabei auch Interaktionen mit Menschen bedeuten. Neue Prozessabläufe lassen sich durch Trennung von Ablaufsteuerung und Ausführung von Funktionen einfacher gestalten. Existierende Abläufe können ebenfalls flexibler angepasst werden, als dies mit den heute üblichen Anwendungsstrukturen möglich ist.

IBM und Microsoft haben die Technologien für die Business Integration auf Basis von Web Services am meisten vorangetrieben. Hervorhebenswert sind hierzu die *Global XML Web Services Architecture* (GXA) und die Definition der *Business Process Execution Language* (BPEL), die mittlerweile von allen wichtigen Software-Herstellern unterstützt wird (Details in Kapitel 5). Standards spielen bei der Business Integration naturgemäß eine besondere Rolle, da effiziente Integration und Interoperabilität nur durch industrieweit akzeptierte Standards zu erreichen sind. Standardisierungsgremien wie W3C, OASIS, BPMI.ORG und Hersteller (IBM, Microsoft, SAP, Sun, BEA usw.) erweitern diese Palette laufend.

Empfehlenswerte Integration Server mit adäquatem Funktionsumfang – wie oben beschrieben – werden heute von führenden Software-Herstellern angeboten (z. B. IBMs WebSphere Business Integration, SAPs Exchange Integration, Microsofts Biztalk Server). Nennenswerte Produkte kommen von einigen Anbietern, die sich auf das Thema Business-Integration spezialisiert haben, wie z. B. die Firmen Tibco und webMethods.

3.3 Architekturen für unternehmensübergreifende Lösungen

Die Integration von existierenden und zukünftigen unternehmensweiten und unternehmensübergreifenden Business-Prozessen ist derzeit wohl die größte Herausforderung für IT-Organisationen. CIOs sollten zuerst eine Zielarchitektur definieren, ehe sie über Software-Investitionen und Veränderungen in der IT-Infrastruktur entscheiden. Bild 3.8 zeigt eine solche Architektur, die übergreifende, flexible und adaptionsfähige Lösungen ermöglicht.

Das Kernstück dieser Architektur ist eine Anwendungsplattform, bestehend aus Portal Server, Application Server und Integration Server einschließlich der Ressourcen und Services-Ebene, wie in den vorangegangenen Abschnitten erläutert. Auf dieser skalierbaren Plattform laufen sowohl Standard-Applikationen wie SCM, ERP, CRM als auch industriespezifische Anwendungen ab.

Die dargestellte Architektur bietet in vielfacher Hinsicht Vorteile und Mehrwert (u.a. Kosteneinsparungen, technologische Unabhängigkeit, Zukunftssicherheit und reduzierte Komplexität). Entscheidend ist jedoch die Fähigkeit, durchgängige und unternehmensübergreifende Prozesse implementieren zu können, um die Produktivität zu verbessern, Flexibilität zu erhöhen und die Wettbewerbsfähigkeit zu steigern. Automatisierte Prozesse und dynamisch eingebundene Services machen es möglich, schnell auf veränderte Marktsituationen zu reagieren. Durch mobile Services lassen sich Abläufe optimieren.

Die Schlüsseltechnologien zukünftiger Business Solutions sind *Mobility, Web Services* und *Security*.

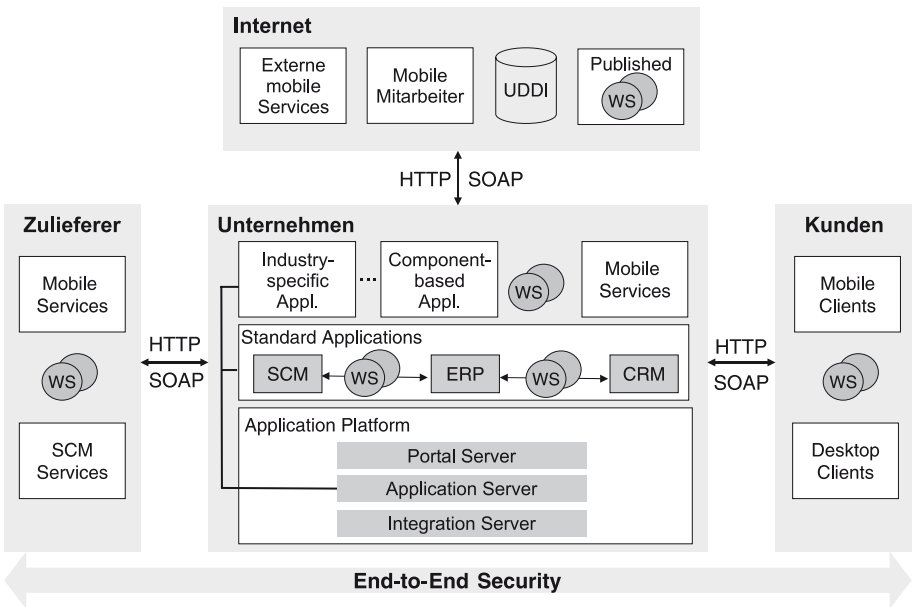


Bild 3.8 Zukunftsorientierte e-Business-Architektur

Mobility

Via mobile Geräte können Kunden, Partner und Mitarbeiter überall erreicht werden und umgekehrt ist der autorisierte Zugang zu Firmen-Ressourcen von jedem Ort aus möglich.

Mobile Services ermöglichen es z. B., Servicetechniker besser zu koordinieren oder Kunden mit ortsabhängigen Informationen und entsprechenden Angeboten zu versorgen. Netzbetreiber wiederum unterstützen Firmen mit mobilen Services, die einerseits Kosten sparen und andererseits innovative Funktionen bieten (z. B. Administration Services, Multimedia Services, Location-based Services,).

Lieferanten und Speditionen können mobile Services aufziehen, z. B. Flotten-Management, um ihre Lieferprozesse zu optimieren, oder Tracking Services, um den Lieferstatus jederzeit zu überprüfen oder verlorengegangene Ware aufzuspüren.

Diese Beispiele mögen als kurze Illustration dienen, wie Unternehmen ihre Wettbewerbsfähigkeit verbessern können, wenn sie die vielfältigen Chancen nutzen, die sich durch Mobility bieten (siehe Kapitel 4).

Web Services

Von Anfang an haben maßgebliche Software-Hersteller die XML Web-Services-Technologie aufgegriffen. In der Regel werden Web Services heute in ihren Frameworks und Produkten wie Application Server, Portal Server, Integration Server, Datenbanken und Client-Systemen einschließlich entsprechender Entwicklungs-Tools unterstützt. Web Services stellen die nächste Stufe der Komponenten-basierten Software-Entwicklung dar und sind insofern schon als integraler Bestandteil moderner Anwendungsarchitektur zu sehen.

Aber darüber hinaus setzen sich Web Services bei der Integration verschiedener Unternehmensanwendungen immer mehr durch; dies ist heute ihr primäres Einsatzfeld. Das wird zu einer erhöhten Integration von Prozessen führen, die heute noch strikt anwendungsspezifisch getrennt sind, wie SCM- oder CRM-Prozesse. Web-Services-Technologie in Kombination mit der Prozesssprache BPEL (Business Process Execution Language for Web Services) ermöglicht eine Zusammensetzung von Prozessschritten aus Elementar-Services (Web Services) und existierenden Applikationen. Damit lassen sich bisher disjunkte Teilprozesse integrieren und bei Bedarf ad-hoc Prozesse aufsetzen, ohne dass eine tiefergehende Kenntnis des technischen Hintergrundes erforderlich wäre.

Auf Basis von SOAP (Simple Object Access Protocol) und HTTP ermöglichen Web Services eine Interoperabilität über Unternehmensgrenzen hinweg und bewirken ein verbessertes Zusammenspiel mit Prozessen von Partnerfirmen. So können auch Client-Anwendungen des Kunden mittels SOAP direkt die Web Services von Firmen aufrufen.

Das Ziel einer modernen Service-orientierten Architektur ist die technologisch bestmögliche Einbindung von Web Services. Dies schließt längerfristig auch das dynamische Aufrufen von im Internet publizierten Web Services über die Discovery- und Bin-

ding-Mechanismen mit ein. SOA und Web Services werden ausführlich in Kapitel 5 behandelt.

Security

Security in e-Business Solutions war immer schon ein äußerst brisantes Thema. Im Rahmen einer zukünftigen Architektur, wie sie hier diskutiert wird, spielt die End-to-End Security eine Schlüsselrolle, ja sie ist sogar eine unabdingbare Voraussetzung für unternehmensübergreifende, verteilte Anwendungen.

Besondere Herausforderungen stellen die mobilen Netze und die erweiterte Integration von Kunden, Partnern und mobilen Mitarbeitern und die damit implizit verbundenen erhöhten Risiken dar. Darüber hinaus bringen die Kommunikation auf Basis von Web Services über Unternehmensgrenzen hinweg sowie das Einbinden von Web Services aus dem Internet in geschäftskritische Anwendungen völlig neue Gefahrenquellen mit sich.

Das Erkennen dieser Brisanz und die Bewusstseinsschärfung für das Thema Security sind die ersten Schritte, um die tatsächlichen Risiken richtig einzuschätzen. Daraus lässt sich dann eine Security-Strategie entwickeln, die eine ausgewogene Balance zwischen Investitionen und Kosten zum Ziel hat und mit den noch verbleibenden Risiken angemessen umgehen kann.

Es ist besonders zu betonen, dass das Vertrauensverhältnis (Trust) zwischen allen involvierten Geschäftspartnern von entscheidender Bedeutung für unternehmensübergreifende Lösungen ist. Vertrauen ist das wichtigste Gut, um erfolgreich im Wettbewerb bestehen zu können. Allerdings wird sich Vertrauen nur einstellen, wenn alle Partner überzeugt sind, dass automatisierte Interaktionen absolut sicher abgewickelt werden.

In Architekturen, die über Unternehmensgrenzen hinausreichen, umfasst die Security Kommunikation, Messaging und Transaktions-Services, wobei Vertrauenswürdigkeit (Confidentiality), Integrität (Integrity), Zuverlässigkeit (Availability) und Verbindlichkeit (Non-Repudiation) sicherzustellen sind (Details in Kapitel 6).

Zusammenfassung

Zukunftsorientierte Business-Lösungen basieren auf offenen, unternehmensübergreifenden Architekturen, die es erlauben sowohl Partner, Kunden und Mitarbeiter als auch über das Internet angebotene Services miteinzubeziehen. Die wesentlichen Charakteristika einer solchen Architektur sind:

- eine Multi-tier-Architektur bestehend aus Kommunikations-/Präsentationsebene, Business-Logik-Ebene, Integrationsebene und Services-/Ressourcen-Ebene
- eine Anwendungsplattform bestehend aus Portal Server, Application Server und Integration Server
- eine Anwendungsplattform, auf der gleichermaßen Standard-Software, branchenspezifische Software, eigenentwickelte, Komponenten-basierte Software, Web Services und mobile Services ablaufen können

– ein Portal Server, der Festnetz- und Mobilnetzzugang einschließt und unterschiedliche Nutzergruppen managen kann
– ein Integration Server, der Message-, Integration-Broker- und Web-Services-Technologien einschließt und in der Lage ist, Business-Prozesse zu managen und auszuführen
– eine Interoperabilität mit Partner-Prozessen und -Services basierend auf SOAP Messages und Web-Services-Technologie
– die Einbindung von Internet Services und mobilen Services in Geschäftsprozesse unter Nutzung von SOAP und Web-Services-Technologie
– umfassende Security-Services, um End-to-End-Sicherheit für alle Business-Prozesse zu gewährleisten.

4 Mobile Anwendungen und Plattformen

Mehr als 1,3 Milliarden Mobiltelefone sind mittlerweile weltweit im Einsatz, und es wird erwartet, dass bis 2008 die Zahl von 2 Milliarden überschritten wird. SMS (Short Message Service) ist nach wie vor eine sogenannte Killer Application, faszinierende neue Anwendungsszenarien wird es jedoch in Zukunft durch innovative Multimedia-Services geben. Diese Anwendungen sind im Unterschied zu den verbindungsorientierten Sprachanwendungen verbindungslose und paketorientierte Datenanwendungen. Daten können dabei beliebige digitalisierte Informationen sein, z. B. strukturierte oder unstrukturierte Daten, Sprache oder Multimedia-Inhalte.

Die wohl bekanntesten Anwendungen wie SMS, MMS (Multi-Media Services), Spiele, News, Ticker, Aktienkurse, Verkehrsinformationen, e-Mail usw. werden heute überwiegend von Netzbetreibern angeboten. Zunehmend entdecken Unternehmen nun auch den Wert mobiler Anwendungen für ihre Business-Lösungen. In diesem Kapitel wird besonderes Augenmerk auf mobile Anwendungen aus Sicht von Unternehmen und ihren Geschäftslösungen gerichtet. Die unterschiedlichen Anwendungskategorien und ihr Mehrwert werden aufgezeigt, geeignete Anwendungsplattformen dargestellt und schließlich eine Reihe von interessanten Anwendungsbeispielen erläutert.

4.1 Kategorien mobiler Anwendungen

Mobile Services erschließen interessante neue Geschäftsmöglichkeiten für B2B (Business-to-Business), B2E (Business-to-Employee) und B2C (Business-to-Consumer). Einige dieser Anwendungen lassen sich ausschließlich geschäftlichen Aktivitäten zuordnen, bei anderen liegt der Fokus auf Freizeit und Unterhaltung. Eine größere Anzahl von Anwendungsklassen schließt jedoch beides mit ein: Business und Freizeit.

Die Anwendungskategorien sind in Bild 4.1 dargestellt.

Die Anwendungen auf der linken Hälfte des Bilds werden überwiegend den Geschäftslösungen zugeordnet, während die rechte Hälfte die von Netzbetreibern angebotenen Services für Endkunden repräsentiert. Allerdings ist dies eine eher oberflächliche Klassifikation, denn tatsächlich gibt es viele Überlappungen. Ein Beispiel der Location Services möge dies verdeutlichen: Netzbetreiber bieten Location Services für interessante Objekte (Points of Interest) an, z. B. dort, wo sich die nächsten Geldausgabeautomaten befinden. Natürlich können auch Banken solche Services anbieten und haben damit die Möglichkeit, für ihre Kunden relevante Informationen hinzuzufügen, z. B. Hinweise

Bild 4.1 Kategorien mobiler Anwendungen

auf Kontoauszugsdrucker oder andere Services. Noch eleganter wäre es, auf Anfrage des Kunden den Kontostand gleich per Handy mitzuteilen.

Mobile Office

ist die meistbenutzte Business-Anwendung und schließt Synchronisation mit Microsoft Outlook sowie Zugang und Interaktion mit den Back-Office-Systemen (Microsoft Exchange, Lotus Notes) über mobile Netze ein. Für diese Anwendungen eignen sich vor allem PDAs mit mobilem Netzanschluss. Aber auch Smartphones mit entsprechenden Displays und Eingabemöglichkeiten werden hier zunehmend eine Rolle spielen. Die wichtigste Office-Anwendung bleibt nach wie vor e-Mail mit der Fähigkeit, Anhänge (Attachments) wie Word-Dateien oder Excel-Tabellen anzuzeigen und zu bearbeiten.

Mobile Intranet-Anwendungen

sind unverzichtbar für die meisten Business Solutions. Sie ermöglichen einen sicheren Zugang zu Unternehmensanwendungen, wie z. B. Travel Management, oder zu spezifischen Anwendungen, die Mitarbeiter zur Erledigung ihrer Aufgaben nutzen, z. B. Unterstützung von Außendiensttätigkeiten und Vertriebsaktivitäten (Field Services, Sales Force Automation). In anderen Geschäftsszenarien wird auch Partnern und Kunden Zugang zu Unternehmensanwendungen, bzw. Diensten und Ressourcen gewährt. Mit der Verbreitung von Intranets und Extranets sind mobile Anwender zunehmend in der Lage, auf Anwendungen und Informationen zuzugreifen und Nachrichten auszutauschen, egal ob sie sich in ihrem Büro aufhalten, im Auto unterwegs sind, sich im Flughafen oder Hotel befinden, von zuhause aus arbeiten oder einen Kundenbesuch absolvieren. Es wird prognostiziert, dass die Zahl mobiler Anwender im Business um 60% pro Jahr zunimmt und dass bis 2005 etwa 200 Millionen Menschen mobile Anwendungen nutzen werden.

Location-based Services

sind eine neue generische Anwendungsklasse, die erstmals in Verbindung mit mobilen Geräten möglich ist. Diese Services erzeugen in den verschiedensten Situationen Mehrwert für die Benutzer mobiler Geräte. Anwendungen erstrecken sich von Freizeitangeboten (z. B. Kino- oder Restaurant-Führer) über Notfallsituationen (Ärzte, Apotheken, Pannendienst), Einkauf, Geldautomat, Routenführung, Überwachung von Objekten bis hin zu reinen Geschäftsanwendungen (Ortsbestimmung von Angestellten, Flotten-Management).

Während alle anderen im Bild gezeigten Services schon von den Festnetzen her bekannt sind, unterscheiden sich Location-based Services dadurch, dass sie nur in Mobilnetzen möglich sind. In Kombination mit Push Services, die proaktiv Nutzer benachrichtigen und mit aktuellen, ortsbezogenen Informationen versorgen, lassen sich interessante neue Geschäftsmöglichkeiten finden.

Einige Beispiele hierzu sind:

- Points of Interest: Mobile Nutzer werden über spezielle Einrichtungen in ihrer unmittelbaren Umgebung informiert oder rufen Informationen ab (z. B. Einkaufsgelegenheiten, Banken, Krankenhäuser, Kinos, Büros, usw.).
- Schnäppchen: Einzelhändler kennen die besonderen Wünsche von registrierten Kunden und senden Rabatt-Coupons auf deren mobile Geräte, wenn sie sich in der Nähe einer entsprechenden Einkaufsgelegenheit befinden.
- Routenführung: Anwender werden abhängig von ihrem Standort zu gewünschten Zielen geleitet.
- Tracking: Mobile Objekte werden aufgespürt und ihre Fortbewegungen nachverfolgt, um Aktivitäten besser zu koordinieren und Prozesse zu optimieren.
- Reise-Services: Mobile Nutzer erhalten aktuelle Informationen und Alternativvorschläge für ihre Reise und ihren jeweiligen Aufenthaltsort (z. B. Flugverspätungen, Verkehrsstaus).

Mobile Steuerung und Überwachung

schließen ein breites Spektrum von unterschiedlichen Anwendungen ein: Notfallhilfe, Alarm bei Diebstahl, Gebäudekontrolle, Steuerung entfernter Geräte, Reparatur- und Telematik-Anwendungen. Solche Anwendungen sind geeignet, Vorgänge zu vereinfachen und Prozesse zu verbessern. Sie tragen auch zur Lebensqualität von Patienten bei, die auf ständige gesundheitliche Kontrolle angewiesen sind oder erhöhen die Sicherheit von Personen und Einrichtungen bei öffentlichen Veranstaltungen. Große Bedeutung und hohes Wachstumspotenzial wird für Maschine-zu-Maschine(M2M)-Anwendungen prognostiziert.

Mobile Kommunikation

ist nach wie vor die bedeutendste Anwendung und bietet nunmehr interessante Optionen wie Text-, Sprach-, Daten- und Multimedia-Kommunikation sowohl in synchronen

als auch asynchronen Modi. Unified Messaging ermöglicht beliebige Kommunikation unabhängig von Gerät, Zeit und Ort.

Mobile Information Services

können von allgemeiner Natur sein, ausschließlich Business-orientiert oder auch ganz persönlich ausgerichtet sein. Bekanntlich ist die Informationsvielfalt im Web unbegrenzt. Es ist offensichtlich, dass Informationen umso interessanter sind, je mehr sie personalisiert und ortsbezogen angeboten werden. Nutzer sind bereit für Dienste zu bezahlen, wenn Informationen für aktuelle Entscheidungen wichtig sind, z. B. freie Parkplätze, Veranstaltungshinweise, Sehenswürdigkeiten, Aktienkurse, Fahrpläne, Directory Services, Umrechnung von Währungen, Gewichten, Größen usw. Personalisierte, ortsbezogene und aktuelle Push Services spielen hier eine ganz besondere Rolle, da sie einen echten Mehrwert in mobilen Netzen darstellen.

Mobile Commerce

schließt alle transaktionsorientierten Anwendungen ein, die etwas mit Bestellung, Einkauf, Verkauf, Auktion, Handel, Ticketing, Zahlungsverkehr, Banküberweisungen usw. zu tun haben. Mobile Commerce hat ein riesiges Potenzial und sollte als Ergänzung zu e-Commerce gesehen werden. Mobile Commerce wird zu einer deutlichen Verhaltensänderung von Konsumenten führen. Darauf müssen sich Netzbetreiber und Diensteanbieter im Wettbewerb einstellen. Da es sich bei Mobile Commerce in der Regel um geldwerte Transaktionen handelt, ist End-to-End Security eine unabdingbare Voraussetzung für diese vielversprechenden Services.

Mobile Entertainment

ist eine Anwendungsklasse, die überwiegend jüngere Menschen fasziniert. Spiele sind ein bewährtes Mittel, um neue Kundensegmente zu gewinnen, attraktive Geräte in den Markt zu bringen und Menschen mit ungewohnten Oberflächen und Interaktionen vertraut zu machen. Nokias „N-Gage“-Spiele und -Geräte sind ein Beispiel dafür, wie die Welt der interaktiven Online-Spiele den Massenmarkt erobert. Die Verfügbarkeit von integrierten Kameras, MP3- und Video-Playern in neueren Mobiltelefonen und PDAs wird das mobile Entertainment richtig in Schwung bringen. Insbesondere das Internetbasierte Musik- und Video-Geschäft steht vor einem Boom, wodurch die Diskussion um Schutzrechte von digitalisierten Inhalten neu entfacht ist.

Es ist so, dass vor allem jüngere Menschen neue interessante Technologien schneller adaptieren. Das beste Beispiel aus der Vergangenheit ist SMS. Deshalb ist davon auszugehen, dass die Nutzung von Bildern und Videoclips in vielfältigen Anwendungen genau so schnell populär wird, wenn dies für die jüngere Generation bezahlbar ist.

Entsprechende Anwendungen in Geschäftslösungen werden dann später nachfolgen. Schon heute steht fest, dass zahlreiche Anwendungsmöglichkeiten für Video Services existieren. Werbung wird eine wichtige Rolle spielen. Beispielsweise könnte Coca Cola durch Werbespots Multimedia Messaging subventionieren. Ein weiteres Beispiel ist ein Service-Techniker, der vor Ort Reparaturanleitungen erhält. Mittels eines Vide-

oclips, das er auf sein mobiles Gerät herunterlädt und abspielt, kann er genaueste Instruktionen über den Reparaturvorgang erhalten.

Was die Nutzung von mobilen Geräten anbetrifft, werden sich Freizeit und Business immer mehr vermischen. *Infotainment*, ein Begriff, der den Mix von Information and Entertainment wiedergibt, ist ein Beispiel dafür, was die Menschen attraktiv finden und wohin der Trend geht. *Mobile Learning* ist ein weiteres Beispiel für neue Anwendungsszenarien. So können sich Reisende an Ort und Stelle über Sehenswürdigkeiten und Highlights einer Stadt informieren, und zwar interaktiv und eingebettet in einen Sprachkurs der Landessprache, den sie mit Hilfe ihres mobilen Gerätes absolvieren.

4.2 Mehrwert mobiler Business-Anwendungen

Hauptgründe, warum Unternehmen über mobile Anwendungsszenarien nachdenken, sind einerseits die nachhaltige Sicherung der Wettbewerbsfähigkeit und andererseits die Suche nach neuen Geschäftsmöglichkeiten und Umsatzquellen.

Aus der Perspektive einer Bank möge das Beispiel der Wettbewerbsfähigkeit betrachtet werden: Vermutlich werden Banken durch das Angebot mobiler Services keine neuen Kunden dazugewinnen können, weil alle anderen Banken nachziehen. Das Risiko, Kunden zu verlieren, ist jedoch hoch, wenn Institute mobile Services nicht in ihr Angebot aufnehmen.

Ein Beispiel, wie neue Geschäftsmöglichkeiten erschlossen werden können, sind Travel Services. Diensteanbieter können vielfältige Services anbieten, z. B. ortsbezogene Services, für die Reisende willens sind zu bezahlen, wenn sie dadurch unterwegs aktuelle und nützliche Infos erhalten.

Mobile Business in der hier verwendeten Definition bedeutet:

- Business von jedem Ort aus: im Büro, zuhause, im Hotel und unterwegs
- Berücksichtigung unterschiedlicher Situationen: Business, Freizeit, Aus- und Weiterbildung
- Nutzung beliebiger Geräte: Mobiltelefone, PDAs, Laptops, PCs
- Nutzung beliebiger Netze: GSM/GPRS, UMTS, WLAN, Festnetze.

Generische Eigenschaften mobiler Anwendungen und deren Nutzen

Mit mobilen Anwendungen sind besondere Eigenschaften und Vorteile verbunden:

Allgegenwart

Anwender praktizieren Echtzeit-Information und Kommunikation unabhängig von ihren jeweiligen Aufenthaltsorten.

Erreichbarkeit

Uneingeschränkte Erreichbarkeit ist von besonderem Nutzen, wenn Unternehmen mit Partnern, Angestellten oder Kunden in engem Kontakt stehen müssen. Mittels mobiler Geräte kann überall und zu jeder Zeit Kontakt aufgenommen werden. Push Services erlauben aktuelle Benachrichtigungen über wichtige Ereignisse, so dass ggf. auch spontane Geschäftsmöglichkeiten wahrgenommen werden können.

Zugang zu Ressourcen

Auf persönliche Daten und Geschäftsressourcen kann geräte- und netzunabhängig zugegriffen werden.

Komfort

Mobile Geräte bieten aus Sicht des Benutzers erhöhten Komfort, da wesentliche persönliche Daten gespeichert und immer verfügbar sind. Die Handhabung der Geräte wird zunehmend einfacher.

Lokalisierbarkeit

Die Lokalisierbarkeit ist für viele Geschäftsanwendungen ein echter Mehrwert. Das Wissen über den jeweiligen Aufenthaltsort von Kunden, Angestellten, Reisenden oder auch Objekten ist eine entscheidende Voraussetzung für innovative Services und neue Geschäftsmöglichkeiten. Business-Aktivitäten lassen sich durch Lokalisierbarkeit von Menschen und Objekten besser koordinieren und Prozesse effizienter gestalten.

Always-on

Die ständige Konnektivität zum Internet und Intranet via mobile Geräte erhöht die Aktionsfähigkeit in Echtzeit und die Kommunikationsfähigkeit. GPRS und UMTS Services beschleunigen diese Entwicklung und mobile Geräte mit Always-on-Eigenschaften werden bald die bevorzugte Variante sein, um auf Informationen im Netz zuzugreifen.

Personalisierung

Personalisierung ist eine Schlüsselfunktion bei mobilen Anwendungen, die heute von Unternehmensportalen geleistet wird. Dank Personalisierung wird das mobile Gerät zu einem komfortablen und täglich benutzten Hilfsmittel, das den einfachen Zugang zu ausgewählten Informationen und Services auf Basis persönlicher Präferenzen und Rechte ermöglicht.

Nutzenszenarien

Es ist zu empfehlen, dass sich Unternehmen intensiv mit Anwendungsszenarien auseinandersetzen, bevor mit der Implementierung mobiler Business-Anwendungen begonnen wird. Das folgende Bild illustriert eine systematische Vorgehensweise.

Eine genaue Analyse mit aufeinanderfolgenden Schritten muss sicherstellen, dass sich das Investment in *Mobile Business* (m-Business) letztendlich in messbarem Mehrwert für die Firma niederschlägt.

Im ersten Schritt ist es wichtig, die beschriebenen generischen Mobility-Eigenschaften zu verstehen und Chancen von mobilen Anwendungen zu erkennen. Als nächstes ist zu evaluieren, welche Geschäftsprozesse infrage kommen und wie diese Prozesse durch Mobility effizienter zu gestalten sind. Schließlich sind die Auswirkungen von modifizierten Prozessen auf die existierende Organisation zu reflektieren.

Auf hohem Abstraktionsniveau sollte nicht nur die Mobility-Erweiterung existierender Applikationen wie *Enterprise Resource Planning (ERP)*, *Customer Relationship Management (CRM)*, *Supply Chain Management (SCM)* und *Sales Force Automation (SFA)* analysiert werden. Es geht auch darum, wie Kommunikation und Informationsfluss mit Kunden, Partnern und Mitarbeitern durch den Einsatz neuer mobiler Anwendungen generell erleichtert und verbessert werden können.

Im Besonderen ist zu beachten, dass bei der Implementierung mobiler Lösungen ganz andere technische Herausforderungen zu bewältigen sind als bei traditionellen Internet-basierten Anwendungen. Im Allgemeinen sind mobile Lösungen sehr viel komplizierter. Unternehmen müssen die Unterschiede in Bezug auf Anwendungsentwicklung, Geräteunterstützung, Security und mobile Trends und Weiterentwicklungen vollständig verstehen. Jedes dieser Themenfelder muss hinsichtlich der damit verbundenen Komplexität bei der Entwicklung mobiler Anwendungen einzeln bewertet werden. Als Ergebnis wird dann deutlich, inwieweit die existierende Infrastruktur für Mobility

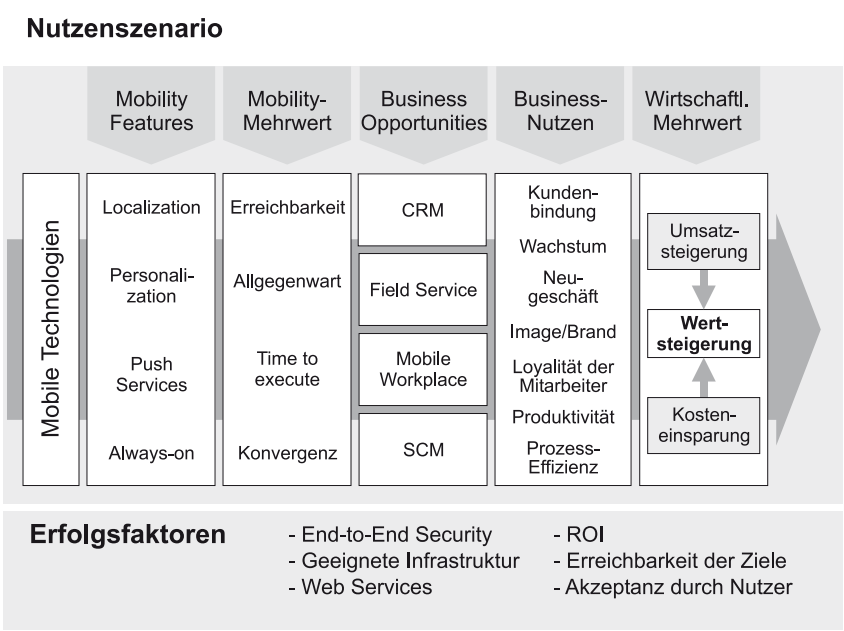


Bild 4.2 Nutzen mobiler Business-Anwendungen

geeignet ist und welche Plattform sich unter Berücksichtigung der Anforderungen und übergeordneten Zielsetzungen als beste herauskristallisiert.

Nach einer solchen systematischen Analyse lässt sich der tatsächliche Mehrwert für das Unternehmen ermitteln und transparent darstellen. Der definitive Nutzen von m-Business kann in Form von verbesserter Kundenbindung, erhöhter Produktivität, neuen Geschäftsmöglichkeiten, gesteigerter Effizienz usw. sichtbar werden.

Wie in Bild 4.2 dargestellt, gibt es eine Reihe von technischen und nicht-technischen Faktoren, die eine erfolgreiche Realisierung eines m-Business-Projektes beeinflussen. Die technischen Aspekte schließen End-to-End Security, Web Services (Wiederverwendbarkeit von Services) und die existierende Infrastruktur mit ein. Der Infrastruktur kommt hier eine besondere Bedeutung zu, da beträchtliche Mehrkosten einzukalkulieren sind, wenn die Erweiterungsfähigkeit für mobile Anwendungen eingeschränkt ist.

Die nicht-technischen Erfolgsfaktoren sind genauso zu beachten. Dazu zählen *Return of Investment (ROI)*, Grad der Akzeptanz bei allen Beteiligten sowie Erreichbarkeit der definierten Projektziele. In der Vergangenheit sind Projekte häufig daran gescheitert, dass überzogene Vorstellungen nicht umgesetzt werden konnten. In der Designphase ist deshalb besonderer Wert auf realistische Zielsetzungen zu legen.

Folgende Checkliste möge helfen, die richtige Entscheidung für den Einsatz mobiler Anwendungen zu treffen:

- Marktentwicklungen identifizieren, bei denen Mobility eine wichtige Rolle spielt
- das Engagement des oberen Managements für m-Business gewinnen
- derzeitige e-Business-Aktivitäten des Unternehmens bewerten
- derzeitige technologische Infrastruktur und erforderliche Erweiterungen bewerten
- die erforderliche m-Business-Expertise im Unternehmen identifizieren
- die wichtigsten mobilen Geschäftsszenarien hinsichtlich Kosteneinsparungen, Qualitätsverbesserungen, Umsatzzuwachs und Ausweitung der Geschäftsmöglichkeiten analysieren
- existierende und neue Prozesse identifizieren, die sich für m-Business eignen
- eine Kosten-Nutzen-Analyse mit den potenziellen quantitativen und qualitativen Einschätzungen aufstellen
- die wesentlichen Erfolgsfaktoren für das m-Business im Umfeld ausgewählter Unternehmensanwendungen identifizieren
- sogenannte „Quick Wins“ identifizieren
- eine m-Business Roadmap als Basis für alle weiteren Aktivitäten einschließlich Migrationsplan aufstellen.

4.3 Plattformen für mobile Anwendungen

Moderne e-Business-Architekturen entwickeln sich weiter zu integrierten e-Business- und m-Business-Architekturen. Damit werden beide, das traditionelle Festnetz und die mobilen Netze, mit den jeweiligen Gerätevarianten unter einen Hut gebracht. Die wesentlichen Komponenten einer geeigneten Anwendungsplattform sind Portal Server, Application Server und Integration Server. Wie in Bild 4.3 gezeigt, repräsentiert das Unternehmensportal den zentralen Zugangspunkt zu allen Unternehmensressourcen. Das Portal enthält integrierte oder separate Zugangskomponenten für Desktops, mobile IP-Geräte (Laptops, PDAs), WAP-Geräte und reine Sprachgeräte.

Das Portal bietet unterschiedlichen Geräteklassen Zugang zu den Services und Ressourcen des Unternehmens. Moderne Portale unterstützen heute bereits eine Vielzahl unterschiedlicher Geräte, sie sind dadurch erheblich komplexer geworden. Der Portal Server muss in der Lage sein, verschiedene Gerätetypen zu identifizieren, Geräte entsprechend ihrer Präsentationseigenschaften (Markup Language) zu bedienen und Netzwerk- und Security-Protokolle über verschiedene Gateways und Proxy Server abzuwickeln.

Ein Unternehmensportal stellt einen einzigen, konsistenten Zugangspunkt für alle Anwendungen, Informationen und Netz-Services dar, die von Kunden, Mitarbeitern oder Geschäftspartnern zur Erfüllung ihrer Aufgaben in Anspruch genommen werden. Portal-Plattformen sind sowohl für das Unternehmen als auch für diejenigen, die die Portal-Services beanspruchen, von großem Nutzen, wenn auch die Ausgestaltung des Portals auf das Unternehmen selbst oder auf eine der Nutzerkategorien optimiert sein kann.

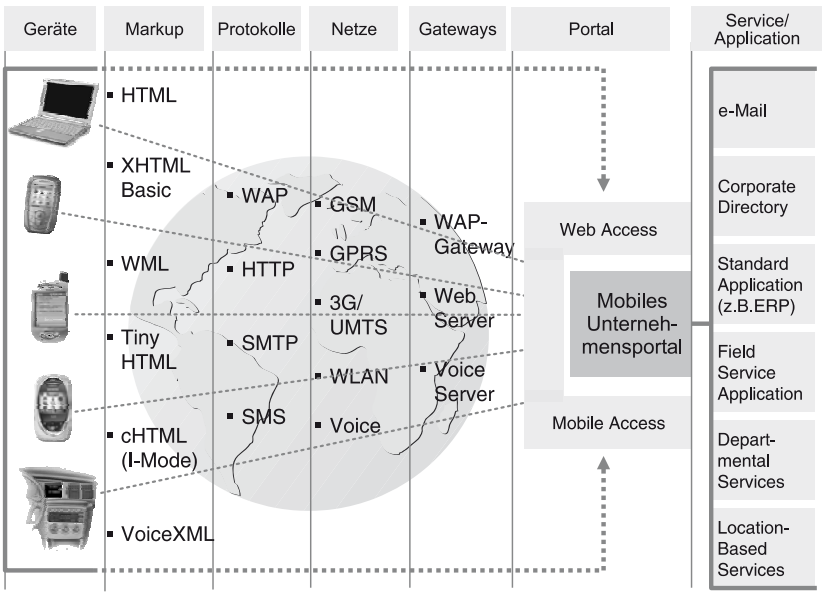


Bild 4.3 Mobiles Unternehmensportal

Das mobile Portal ist als Bestandteil einer zukunftsorientierten erweiterten e-Business-Plattform zu verstehen.

Wesentliche Eigenschaften und Vorteile sind:

- neues einheitliches Front-End-Navigationssystem, das die Integration mobiler Business-Prozesse flexibel und schnell erlaubt
- Rollen-basierter, personalisierter Zugang zu Unternehmensressourcen
- Single Sign-on zu allen Anwendungen und Services
- Push Services, personalisierte Up-to-date-Informationen
- verbesserte Möglichkeiten der Zusammenarbeit (Collaboration)
- Optimierung des Portals durch Nutzungsanalysen und Berücksichtigung von Präferenzen
- zentraler Zugang zu dezentralisierten Ressourcen
- zentrale Administration von Systemen, Geräten und Applikationen
- zentrales Logging, das von *Business-Intelligence*-Anwendungen ausgewertet werden kann.

4.3.1 WAP-Architektur

Obwohl die Markteinführung von *WAP (Wireless Application Protocol)* beinahe ein Flop geworden wäre, unterstützen heute fast alle Mobiltelefone dieses Protokoll. WAP wurde als Protokollschicht konzipiert, die unabhängig von der Netztechnologie funktioniert und gleichermaßen in GSM-, GPRS- und UMTS-Netzen sowie auch in anderen Netztechnologien wie TDMA und CDMA verwendbar ist.

WAP 2.0 [4.3.1], die aktuelle WAP-Version, beinhaltet wie auch schon frühere Versionen Protokollschichten, die mit den Internet-Protokollen TCP/IP, TLS/SSL und HTTP vergleichbar sind. Wenngleich WAP als Interims-Technologie einzustufen ist, repräsentiert es einen weltweiten Standard, der heute von der Mehrzahl der Mobiltelefone für den Zugriff auf Internet/Intranet-Ressourcen und Services unterstützt wird. Andererseits benutzen PDAs die originären Internet-Protokolle, es sei denn, sie sind optional mit einem WAP Browser ausgestattet, der den direkten Zugriff auf WAP-Inhalte erlaubt.

Das *WAP-Architekturmodell*, wie in Bild 4.4 dargestellt, wurde vom WAP Forum definiert und aus dem *WWW(World Wide Web)-Modell* abgeleitet. Es berücksichtigt die derzeitig noch gegebenen technologischen Einschränkungen bei Mobilnetzen und den meisten Mobiltelefonen. Das sind in erster Linie begrenzte Bandbreite, CPU-Leistung, Speicher- und Akkukapazität sowie kleine Displays und stark eingeschränkte Ein-/Ausgabemöglichkeiten.

Wie auch im WWW-Modell wird eine Interaktion durch Anfrage (Request) des Clients an den Server initiiert. Das WAP-Modell bezeichnet diesen Server als *WAP Server* anstatt Web Server. Ein *WAP Gateway* ist zwischen Client und Server positioniert und führt Transformationen aus.

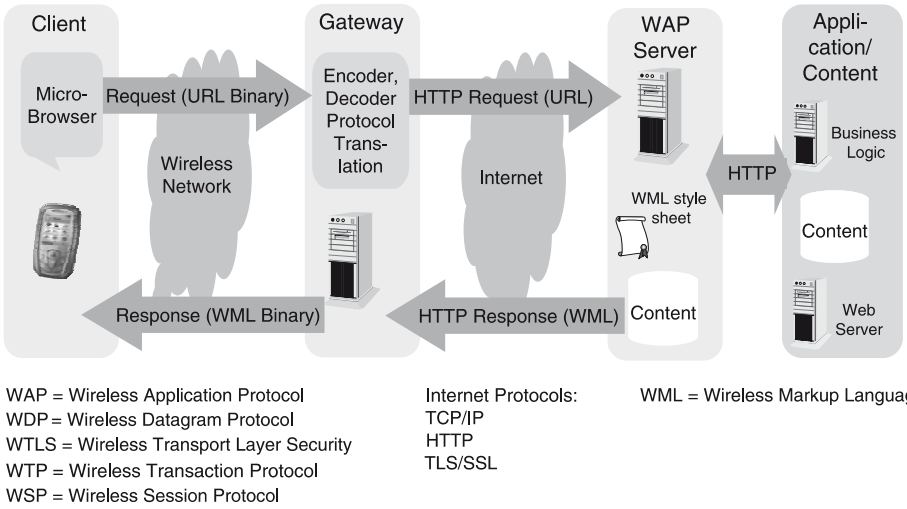


Bild 4.4 WAP-Architektur

Der Client Request ist binär codiert und komprimiert, um somit die geringen Bandbreiten der 2G-Mobilnetze einzuhalten. Inhaltlich enthält er zur Identifikation des WAP-Inhalts die WWW-Standard-*URL (Unified Resource Locator)*.

Der WAP Gateway decodiert den Request und sendet die URL zum WAP Server. Bei diesem Vorgang hat der Gateway die Aufgabe, den WAP-Protokoll-Stack in einen WWW-Protokoll-Stack zu transformieren. Dabei entsprechen in etwa *WDP (Wireless Datagram Protocol)* dem Internet-Protokoll TCP/IP, *WTLS (Wireless Transport Layer Security*) dem TLS/SSL und *WSP (Wireless Session Protocol)* dem HTTP.

Die angefragte URL liegt entweder direkt auf dem WAP Server oder wird von ihm zu einer Applikation oder einer anderen Website weitergeleitet. Von dort wird der Inhalt abgerufen und zum WAP Server zurückgesendet, der das Session Management und die vollständige End-to-End-Interaktion zwischen Client und Inhalts-Server bewerkstelligt. Alternativ können WAP Server oder WAP Gateway die Umsetzung (Transcoding) des Inhalts in das WML-Format übernehmen, wenn der adressierte Inhalt in einer anderen Form vorliegt.

Auf dem Weg zurück zum Client codiert der WAP Gateway den WML-Inhalt in eine komprimierte Binärform, setzt die Internet-Kommunikationsprotokolle in Mobilnetzprotokolle um und sendet den Inhalt so zum Client.

Die Client-Software, das kann z. B. ein *Microbrowser (WAP Browser)* sein, interpretiert WML-Inhalt und WML Script. Der Microbrowser zeigt den Inhalt entsprechend der Benutzeroberfläche analog zu einem Web Browser an. *WML Script* ist eine um einige Funktionen erweiterte Untermenge der JavaScript-Sprache.

Die Client-Software kann zusätzlich ein *Wireless Telephony Applications (WTA)* Interface besitzen, um Sprachanwendungen, die auf einem entsprechenden Sprach-Server

im Mobilnetz residieren, zu nutzen. Der WTA Server bietet damit den WAP-Zugang zu Funktionen der Telekommunikationsinfrastruktur des Netzbetreibers.

Der *Push-Modus* ist ein wesentliches Unterscheidungsmerkmal des WAP-Modells gegenüber dem WWW-Modell. Da der Client im Mobilnetz eine eindeutige Identifikation – die *MSISDN (Mobile Services ISDN)* – besitzt, kann er von Servern direkt adressiert werden. Somit lassen sich, wenn das Gerät eingeschaltet ist, wichtige Informationen z. B. als „Alarm"-Nachricht in Echtzeit an den Client übermitteln.

Die hier erläuterte generische WAP-Architektur muss nicht exakt mit der Implementierung der Funktionen in realen Produkten übereinstimmen. Wie in den nachfolgenden Kapiteln beschrieben, haben die wesentlichen Software-Hersteller die Funktionen eines WAP Gateway mittlerweile in ihren Portal Servern und die eines WAP Server in ihren Application Servern realisiert. Genau diese Plattformen eignen sich bevorzugt für e-Business und integrierte m-Business-Lösungen.

4.3.2 Integration in existierende Anwendungsplattformen

In überschaubarer Zukunft werden wohl die meisten mobilen Anwendungen so konzipiert und implementiert, indem sie in die existierende e-Business-Landschaft integriert werden.

Wie in Bild 4.5 dargestellt, unterstützt eine zukunftsorientierte Anwendungsplattform den Zugang zu Anwendungen, Services und Ressourcen über Festnetz und Mobilnetze.

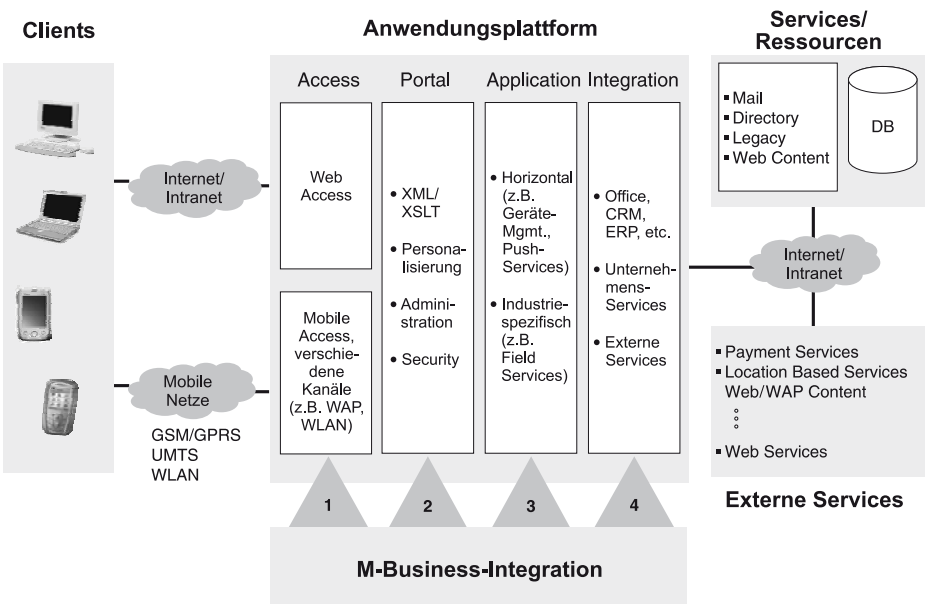


Bild 4.5 Integration mobiler Anwendungen in existierende e-Business Solutions

Der Übergang von e-Business zu m-Business umfasst schwerpunktmäßig vier Integrationsaufgaben, d.h. Erweiterungen der existierenden Plattform:

– Zugang über Mobilnetze (mit 1 im Diagramm markiert)
– Unterstützung mobiler Geräte und Nutzer im Portal (2)
– Implementierung neuer mobiler Anwendungen (3)
– Anwendungs- und Service-Integration (4).

Zugang über Mobilnetze

Die in Bild 4.5 gezeigte duale Plattform kann als einheitliche Web-/WAP-Plattform bezeichnet werden, da sie Geschäftslösungen mit beiden Kommunikationskanälen (Web und WAP) ermöglicht. Auf Basis dieser Plattform werden Anwendungen, Dienste, Ressourcen und Interfaces zu externen Services unabhängig von Gerät und Kommunikationskanal verfügbar gemacht. Beispielsweise ist die Web-/WAP-Plattform in der Lage, den Zugang zu einem Zahlungssystem einer Bank zu autorisieren, unabhängig davon, ob der Nutzer zu Hause am PC sitzt oder unterwegs ein Smartphone benutzt.

Im Einzelnen sollten von einer mobilen Plattform vier Kanäle unterstützt werden:

– Zugang über GSM/GPRS/UMTS-Netze und WAP Gateway, der vom Netzbetreiber betrieben wird
– direkter Zugang über GSM/GPRS/UMTS-Netze, d.h. der WAP Gateway ist in der mobilen Plattform des Unternehmens integriert
– direkter Zugang über GSM/GPRS/UMTS-Netze mittels Internet-Protokoll-Stack (trifft für Laptop und PDA zu)
– Zugang über WLAN.

All diese Kanäle verwenden unterschiedliche Kommunikationsprotokolle und – was explizit betont werden muss – unterschiedliche Quality of Services und Security-Eigenschaften. Insbesondere die Security ist entscheidend für eine geeignete Implementierung ausreichend sicherer m-Business Solutions.

Eine vordergründige Frage ist nun, wie es um die WAP Security steht. Die Inkompatibilität zwischen WTLS und TSL/SSL bedeutet ja, dass bei der Transformation des WTLS-Protokolls in TLS/SSL im WAP Gateway die zu übertragenden Daten, die verschlüsselt sind, bei der Umkodierung für einen Moment unverschlüsselt offen liegen. Damit ist ein ausreichender Schutz gegen Ausspähung oder Manipulation nicht mehr sichergestellt. Es wird deutlich, dass in diesem Fall auch bei höchsten Sicherheitsvorkehrungen im Mobilnetz und im Internet keine ausreichende End-to-End Security gewährleistet ist. Viele Unternehmen haben sich aus diesem Grund entschieden, einen eigenen WAP Gateway in sicherer Umgebung zu betreiben. Weitere Security-Details werden ausführlich in Kapitel 6 erläutert.

Unterstützung mobiler Geräte und Nutzer im Portal

Die Mobility-Integration im Portal ist häufig die größte Herausforderung. Generische Front-End-Funktionen wie Skalierbarkeit, Präsentationsservices, Transformation der

Darstellungsform (Transcoding), Management der Nutzer, Personalisierung, Authentifikation und weitere Portal-Services müssen für beide Nutzergruppen, Web und WAP, zur Verfügung gestellt werden. Hier ist ein hoher Grad von Funktionsüberlappung gegeben, der eine weitgehende Integration erfordert.

Eine *XML/XSLT Engine* führt die Umcodierung beliebiger Qellenformate von Inhalten in XML Code aus. Steht dieser XML Code erst einmal zur Verfügung, kann er mittels *XSLT(eXtensible Stylesheet Language Translation)*-Prozessor (wie beschrieben in Kapitel 3, Bild 3.3) sehr einfach in die verschiedenen Präsentationssprachen transformiert werden. Sie werden dann in den Browsern der mobilen Geräte entsprechend interpretiert: HTML auf einem Web Client, WML auf einem WAP Client, „tiny" HTML auf einem PDA, cHTML auf einem i-mode-Gerät, *VoiceXML (Voice eXtensible Markup Language)* auf einem Sprach-Client und andere, die vielleicht noch standardisiert werden.

Personalisierungsservices ermöglichen oftmals erst, dass mobile Geräte nützlich anwendbar und einfach zu handhaben sind. Simple Menüführung ist hier von besonderer Bedeutung, da die stark eingeschränkten Ein- und Ausgabemöglichkeiten eine direkte Hinführung auf die gewünschten Informationen erforderlich machen.

Aus der Perspektive des Nutzers spielen hierbei personalisierter Portalinhalt, gerätespezifische Einstellungen, konfigurierbare Präferenzen, Auswahl von Informationskanälen und schließlich auch das Ein- und Ausschalten von Benachrichtigungsdiensten (Notification Services) eine wesentliche Rolle.

Aus Sicht der Unternehmen sind Benutzerprofile und Zugangsrechte (Authorizations) von besonderer Bedeutung, da sie den Zugang zu Anwendungen und Services in den verschiedenen Unternehmensprozessen regeln. Da Benutzergruppen Kunden, Partner und eigene Mitarbeiter repräsentieren, ist das User Management einschließlich der Administration ein weiterer wichtiger Aspekt bei der Portalintegration, vor allem wenn Gerätevielfalt und Kommunikationskanäle zu berücksichtigen sind.

Wie geschildert, stellt das Portal den zentralen Zugangspunkt für alle Nutzer dar. Geeignete Security-Funktionen sind aus diesem Grund essentiell für ein Unternehmensportal. Authentifikation und Single Sign-on, Rollen-basierte Autorisierung sowie verschlüsselte und authentische Datenübertragung sind Funktionalitäten, die sowohl für Festnetz- als auch für Mobilnetz-Clients zu implementieren sind.

Einige *horizontale* Portal-Services können sich auch für mobile Anwendungen als sehr nützlich herausstellen. Jedoch hängt das in der Regel von den zu unterstützenden Geschäftsprozessen ab. Solche Services könnten erweiterte Suchmaschinen oder Workflows oder Collaboration Services sein, die Unternehmensgrenzen überschreiten und unternehmensübergreifende Prozesse erleichtern, z. B. collaborative Absatzprognosen, übergreifendes Lager-Management oder Distributor/Reseller Management.

Implementierung neuer mobiler Anwendungen

Mobile Anwendungen setzen sich aus Anwendungsklassen zusammen, wie sie in Kapitel 4.1 dargestellt wurden. Einige davon werden als horizontale Anwendungen bezeich-

net. Oftmals sind darunter auch Grundfunktionen zu verstehen, die in anderen Anwendungen eingebettet sind. Beispiele hierfür sind: *Mobile Office* einschließlich *PIM (Personal Information Management)*, *Location-based Services*, *Push/Notification Services*, *mobile Travel Services*. Andere horizontale Services sind Security Services und administrative Services. Letztere sind unerlässlich für die Verwaltung von Applikationen und Inhalten auf mobilen Geräten. Schließlich gibt es noch branchenspezifische Anwendungen für alle Geschäftsmodelle, B2C (z. B. Location-based Shopping Services, Banking Services), B2B (z. B. Flotten-Management, Tracking Services) und B2E (z. B. mobile Workplace, mobile Workforce, Sales Force Automation).

Aus technischer Sicht ist es empfehlenswert, solche mobilen Anwendungen auf dem existierenden Application Server, d.h. auf der Kernkomponente der Anwendungsplattform des Unternehmens, zu implementieren. Der Grund ist weniger, eine weitere Plattform zu vermeiden, als vielmehr die Portal-Services zu integrieren und zu nutzen, um somit auch eine Optimierung von Geschäftsprozessen zu erleichtern.

Anwendungs- und Service-Integration

Die Integration mit den existierenden Business-Anwendungen und Back-End-Systemen ist nicht weniger wichtig. Unternehmen haben schon große Beträge in die Entwicklung von Anwendungen auf Back-End-Systemen und in die Unterstützung ihrer Geschäftsprozesse durch IT-Lösungen investiert.

Durch die Erweiterung existierender Prozesse mit Mobility lassen sich erhebliche Kosteneinsparungen erreichen, Prozesse optimieren und neue Kunden gewinnen. Die Integration existierender Anwendungen ist dafür immer eine wesentliche Voraussetzung.

Einige Beispiele mögen dies verdeutlichen: Ein Vertriebsmitarbeiter möchte vor Ort aus dem CRM-System einen Kundenvertrag einsehen oder aus dem Sales Force System neueste Produktinformationen abrufen. Ein Wartungsingenieur benötigt Ersatzteildaten aus dem ERP-System, während er gerade eine Maschine beim Kunden repariert. Ein Kunde wiederum möchte über einen mobilen Kommunikationskanal Informationen aus einer zentralen Datenbank abrufen. Diese Beispiele zeigen, dass mobile Anwendungen eine Integration in ERP, CRM, e-Commerce, SCM, Business Information Management (BIM), Legacy-System oder spezifische Intranet-Anwendungen erforderlich machen.

Die Integration externer Services geht noch einen Schritt weiter und eröffnet den Nutzern mobiler Geräte neue Anwendungsfelder. So ist ein Reisender auf dem Weg zum Airport an aktuellen Informationen über die Verkehrssituation oder über eventuelle Flugverspätungen interessiert. Er wäre sogar bereit, für diesen Service zu bezahlen, insbesondere wenn er Alternativvorschläge erhält und eine Umbuchung direkt vom mobilen Gerät aus erfolgen kann. Die Buchungsanwendung könnte ebenfalls auf der Anwendungsplattform laufen und über Interfaces mit den GDS(Global Distribution Services: Amadeus, Sabre usw.)-Systemen kommunizieren. Diesen neuen Geschäftsszenarien wird sicherlich wachsende Bedeutung zukommen.

Weitere Beispiele für die Anbindung externer Services sind Payment Services und Location-based Services, die in der Regel von Banken oder Netzbetreibern angeboten werden und in Unternehmensplattformen eingebunden werden können.

Zukünftig wird die Integration externer Services durch die Web-Services-Technologie und UDDI (Universal Description, Discovery and Integration) stark vereinfacht. Es wird dann möglich sein, dass Business-Logik-Komponenten von Service-Anbietern als Web Services verpackt und diese Funktionen von Unternehmen über standardisierte Aufruf- und Kommunikationsmechanismen genutzt werden können.

4.3.3 Plattformen für mobile Geräte

In e-Business-Lösungen dominieren heute festverdrahtete Desktops und Laptops mit Windows und Browsern, die einen einfachen und standardisierten Zugang zur Business-Logik ermöglichen. Zukünftig wird sich die Client-Welt durch eine Vielfalt mobiler Geräte erheblich erweitern. Das bedeutet, dass sich sowohl Unternehmen als auch Lösungsanbieter mit diesen neuen, heterogenen Client-Systemen auseinandersetzen müssen. Bild 4.6 macht diese Systemvielfalt deutlich.

Es muss davon ausgegangen werden, dass diese vielfältige Systemwelt in den nächsten Jahren keinesfalls übersichtlicher wird. Innovationen und Standardisierungen folgen in kurzen Zeitabständen aufeinander. Produktzyklen von mobilen Geräten sind häufig geringer als ein Jahr.

Die derzeitige Klassifikation mobiler Geräte in *Mobiltelefone* (WAP), *Smartphones*, *PDAs*, *Webpads*, *Laptops*, *Tablet PCs* usw. wird sich voraussichtlich nicht wesentlich

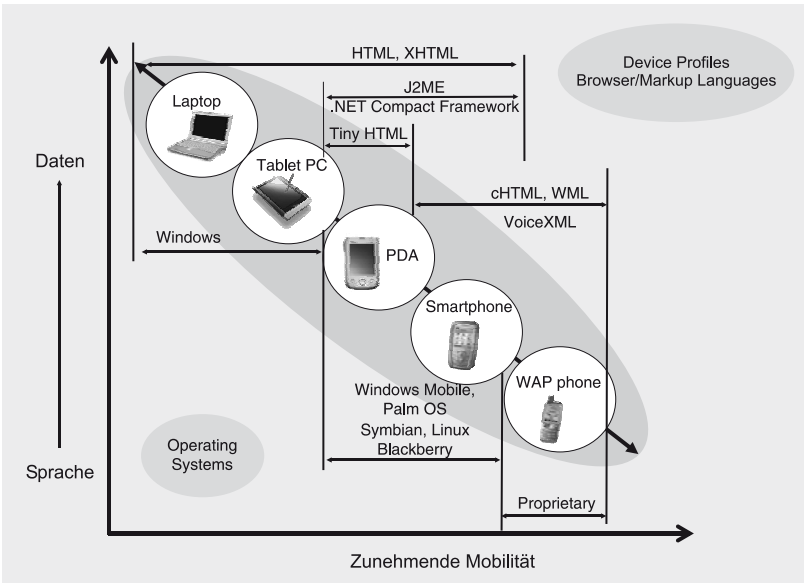


Bild 4.6 Systemvielfalt mobiler Clients

verändern. Allerdings nehmen funktionale Überlappung und Variationen innerhalb der Geräteklassen zu und weitere Klassen könnten für die Geschäftswelt interessant werden (z. B. Fahrzeug-Navigationssysteme).

Mögliche Variationen sind:

- unterschiedliche Display-Charakteristika (Größe, Farben)
- Ein-/Ausgabefunktionen (mit/ohne Tastatur, Stift, Spracheingabe)
- unterschiedliche Funkmodule (GPRS, UMTS, WLAN, Bluetooth)
- kombinierbare Accessoires (MP3 Player, Kamera, Video, GPS usw.)
- unterschiedliche Betriebssysteme (Symbian, Windows Mobile, Palm OS, BlackBerry, Linux).

Ein weiterer Trend hin zu intelligenten mobilen Clients (auch Smart Clients genannt) wird immer deutlicher. Intelligente mobile Geräte besitzen zusätzliche Software (Middleware), die in Form von Browser-Plug-ins oder Device Profiles und Application Services ausgeführt ist.

Intelligente Clients bieten eine Reihe von Vorteilen, z. B.:

- Offline-Applikationen und Datenbanken
- Ladbarkeit von Programmen über das Mobilnetz
- Unterstützung von Peer-to-Peer-Protokollen
- asynchrones Messaging und elektronische Geldbörsen.

Es sollte allerdings bedacht werden, dass die Administration vielfältiger mobiler Geräte einschließlich der Verteilung von Software und Inhalten eine extrem aufwändige Aufgabe werden kann. Deshalb sind reine Browser-basierte Lösungen immer dann zu bevorzugen, wenn die soeben genannten Vorzüge keine explizite Rolle spielen.

Im Folgenden wird das zunehmend komplexe Software-Umfeld für mobile Clients ausführlicher erläutert.

Betriebssysteme

Während Windows souverän seine Position mit über 90% Marktanteil bei Laptops, Tablet PCs and Webpads verteidigen kann, wird der Wettbewerb bei PDAs und Smartphones immer härter. Palm OS (Operating System), Windows Mobile (Pocket PC und Smartphone), Symbian OS, BlackBerry und Linux müssen kämpfen, um sich langfristig in diesem vielversprechenden Markt zu etablieren.

Palm OS

ist weiterhin Marktführer bei PDAs, verliert jedoch Marktanteile an Pocket PC im Sektor Unternehmensanwendungen mit (sicheren) Online-Anwendungen. *Palm OS* [4.3.2] kann auf das breiteste Angebot von 3rd Party Software verweisen und könnte auch die führende Rolle bei Geschäftslösungen behalten. Mit der Ankündigung von Palm OS Cobalt in 2004 erweitert Palmsource, Inc. seine Plattform in den Bereichen Multimedia

und Kommunikation, und mit dem neuen Security Framework versucht man das Wachstum im Business Marktsegment wieder zu forcieren.

Windows Mobile/Pocket PC/Smartphone

sind Derivate des Microsoft OS Windows CE.NET. *Windows Mobile* [4.3.3] ist der neue Name für Microsofts Pocket PC und Smartphone Software. Pocket PC weist derzeit die höchsten Wachstumsraten in der PDA-Klasse auf und wird langfristig auch wegen seiner Affinität zu Windows die bevorzugte Wahl für mobile Online-Anwendungen sein. Im Gegensatz dazu hat Windows Mobile Smartphone erst einen kleinen Marktanteil gewinnen können, so dass hier eine längerfristige Vorhersage schwierig ist.

Symbian OS/Series 60 Plattform

Die Software Firma Symbian gehört anteilig Ericsson, Nokia, Panasonic, Psion, Samsung Electronics, Siemens and Sony Ericsson. Das *Symbian OS* [4.3.4] ist ein offenes, lizenzierbares OS für Smartphones, optimiert auf Sprach- und Datenanwendungen. Nokia hat auf der Basis von Symbian OS die Plattform *Series 60* [4.3.5] entwickelt, die ebenfalls lizenzierbar ist und eine funktionserweiternde Software-Schicht oberhalb Symbian OS darstellt. Series 60 ist derzeit mit Abstand Marktführer in der Klasse der Smartphones.

BlackBerry

ist ein proprietärer PDA, entwickelt von der kanadischen Firma *RIM (Research in Motion)* [4.3.6]. Das Produkt bietet einschließlich Enterprise Server gesicherte End-to-End-e-Mail und Intranet Services. BlackBerry konnte sich erfolgreich in Nordamerika durchsetzen und wird seit 2003 auch im Europäischen Markt angeboten.

Linux

Das Open Source OS *Linux* wird seit 2003 von einigen PDA- und Smartphone-Herstellern auf ihren Geräten eingesetzt. Da der Open-Source-Markt weiterhin wachsen wird, ist anzunehmen, dass Linux auch bei mobilen Geräten eine immer wichtigere Rolle spielen wird.

BREW

ist eine proprietäre Anwendungsplattform, die von der US Firma *Qualcomm* vermarktet wird. *BREW* kommt explizit nur in CDMA-Netzen zum Einsatz, die im Wesentlichen in den USA und Asien verfügbar sind. BREW ist deshalb für Europa nicht von Bedeutung.

Proprietäre OS

werden mehr und mehr verschwinden und nur noch bei Low-Cost-Geräten zu finden sein.

Browser

Browser sind in der Regel Bestandteil des OS. Abhängig vom Gerätetyp werden folgende Präsentationssprachen unterstützt:

- WAP Mobiltelefone: WML
- i-mode-Mobiltelefone: cHTML (proprietäre Sprache, definiert von NTT DoCoMo, Japan, jetzt auch in Europa angewandt)
- PDAs und Smartphones: HTML oder Web Clipping (für eingeschränkte Präsentationsmöglichkeiten). In neueren Geräten wird XHTML unterstützt. XHTML ist eine Weiterentwicklung von HTML und wird sukzessive WML und HTML ersetzen.

Device Profiles

Device Profiles stellen eine einheitliche Anwendungsarchitektur und -plattform für Anwendungen zur Verfügung, die lokal auf intelligenten mobilen Clients laufen. Diese Profile versorgen Anwendungsentwickler mit gerätespezischen Definitionen. Konfigurationen und Profile sind für unterschiedliche Anwendungsszenarien festgelegt. Durch dieses Plattformkonzept lassen sich Anwendungen einfach auf eine Reihe unterschiedlicher Geräte portieren: Mobiltelefone, Smartphones, TV-Set-Top-Boxen, PDAs usw.

Genau wie in der Server-Welt haben sich auch bei den intelligenten Clients zwei führende Plattformtechnologien herausgebildet: die *Java 2 Micro Edition* (J2ME), spezifiziert von Sun und der Java Community, und das *.NET Compact Framework* von Microsoft. Beide Plattformen werden auf lange Sicht den Markt bestimmen. Sie sind in Bild 4.7 dargestellt.

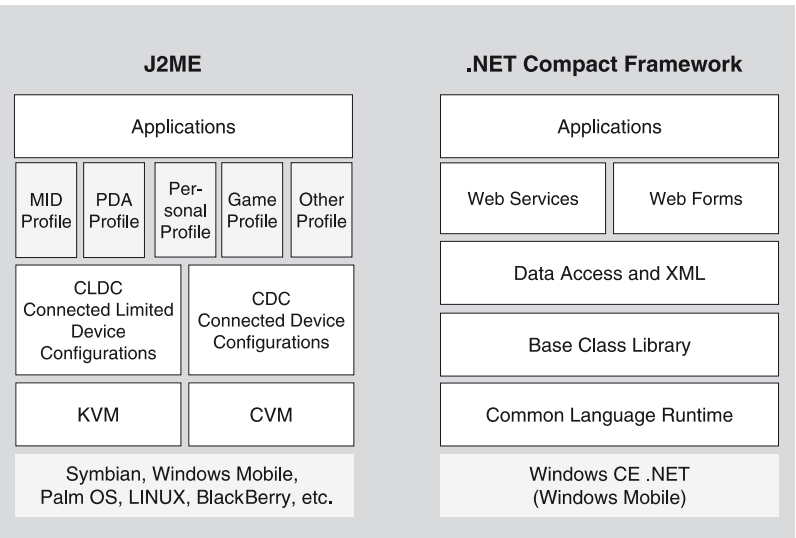


Bild 4.7 Anwendungsplattformen für mobile Clients

Java 2 Micro Edition (J2ME)

J2ME [4.3.7] ist ebenso *wie J2SE (Java 2 Standard Edition*) und *J2EE (Java 2 Enterprise Edition)* Teil der Java-Plattformfamilie und zugeschnitten auf den eingeschränkten Funktionsumfang von einfacheren Geräten (im Vergleich zum PC). J2ME besteht aus einer Reihe von Programm-Interfaces (APIs) und Bibliotheken, die den Java-Entwicklern von der Plattformfamilie her bekannt sind. Die Java-Community spekuliert natürlich darauf, dass sich dadurch auch Java-Client-Anwendungen schnell verbreiten werden. Die der J2ME zugrundeliegende Idee ist die Portabilität von Anwendungen, d.h. einmal entwickelte Anwendungen sind auf allen J2ME-Geräten ablauffähig. J2ME-Implementierungen sind mittlerweile für alle relevanten Client-Betriebssysteme verfügbar, einschließlich Microsoft Mobile Windows.

J2ME gibt es in zwei unterschiedlichen Versionen. Die Variante *Connected Device Configuration (CDC*) basiert auf der klassischen Java Virtual Machine mit vollem Funktionsumfang, wohingegen die Variante *Connected Limited Device Configuration (CLDC)* eine abgespeckte virtuelle Maschine verwendet, die auf die Einschränkungen einfacher Geräte ausgelegt ist.

Das *Mobile Information Device Profile (MIDP)* ist ein J2ME-Profil, das spezifisch für Smartphone-Anwendungen definiert wurde. Es war das erste Profil, das im Java-Community-Programm festgelegt wurde. Verschiedene MIDP-Versionen sind seither freigegeben worden. Sie enthalten Funktionen und APIs für User Interfaces, Datenspeicherung, Internet-Kommunikation, Security und Anwendungs-Lifecycles.

Die auf MIDP-Funktionen und APIs aufsetzenden Anwendungen werden MIDlets genannt. Soweit keine Low-Level-APIs benutzt werden, sind MIDlets portable Applikationen. Andere Profile, wie das *Personal Profile*, Nachfolger des *Personal Java*, sind für eine breite Palette noch intelligenterer Geräte wie TV-Set-Top-Boxen oder Linux-basierte Clients vorgesehen. Der Standardisierungsprozess für PDA-Profile wurde 2003 gestoppt und in eine offenere Entwicklung von sogenannten Profiloptionen umgelenkt.

Von langfristiger Bedeutung ist, dass die J2ME-Plattform auch den direkten Zugriff auf Web Services im Netz erlaubt. Der neue Standard, *JSR 172 (J2ME Web Services Specification)*, definiert entsprechende XML-APIs und RPC-basierten Zugang zu Web Services.

J2ME ist ein bewährtes Java Software Framework, stellt Portabilität über die wesentlichen Betriebssysteme einschließlich Microsoft sicher und erlaubt Offline-Anwendungen ebenso wie einen Mix aus Client- und Server-seitiger Programmierung. Da die J2ME bereits seit einigen Jahren im Einsatz ist, existieren bereits viele Anwendungen, hauptsächlich für Smartphones. Das gibt der J2ME einen deutlichen Vorsprung vor Microsofts .NET Compact Framework.

Microsoft .NET Compact Framework

Das Microsoft *.NET Compact Framework* [4.3.8] gehört zur Microsoft-.NET-Architektur und ist eine eingeschränkte Version des .NET Framework. Das .NET Compact

Framework berücksichtigt die besonderen Charakeristika mobiler Geräte. Es ermöglicht den gesicherten Download von Anwendungen und erschließt die Welt der *XML Web Services* für mobile Geräte. Mit den Erweiterungen der Entwicklungsumgebung für mobile Clients *Visual Studio .NET* sind Entwickler in der Lage, existierenden Code beliebig auf Desktop, Server und mobilen Geräten wiederzuverwenden. Microsoft will mit der Verwendung bekannter APIs und Bibliotheken des .NET Framework auch im Compact Framework das beträchtliche Potenzial an Visual-Basic-Programmierern für die Implementierung von mobilen Client-Anwendungen nutzen.

Das .NET Compact Framework liefert ein Programmiermodell, das für eine Reihe von mobilen Geräten identisch ist, wodurch sich der Entwicklungsprozess für Anwendungen, die auf unterschiedlichen .Net-Geräten laufen sollen, stark vereinfacht. Die Basis dafür ist eine virtuelle Maschine, die durch die *Common Language Runtime* repräsentiert wird. Das Modell kann durch spezifische Klassenbibliotheken für bestimmte Gerätekategorien oder sogar für einzelne Geräte erweitert werden.

Wie in Bild 4.7 dargestellt, bietet das .NET Compact Framework neben den üblichen Basisklassen Unterstützung für die verschiedenen Mobilnetze und XML. Es umfasst außerdem Funktionen für den Datenzugriff (ADO.NET, SQL Server CE) und Security-Funktionen. Das eingebaute Security-Modell stellt sicher, dass bösartiger Code nicht auf System-Ressourcen zugreifen kann, und erlaubt die Abwicklung von Software-Updates über das Mobilnetz.

Das .NET Compact Framework stellt die Plattform für Client-Offline-Anwendungen dar, erlaubt aber auch einen Mix von Client-seitiger und Server-seitiger Programmierung. Von großer zukünftiger Bedeutung ist, dass mit dem .NET Compact Framework Web Services sowohl entwickelt als auch konsumiert werden können. XML Web Services sind gerade in Bezug auf mobile Geräte ein geeignetes Anwendungsmodell, da sie mit einer Vielfalt unterschiedlicher Systeme und Anwendungen unabhängig von Betriebssystem, Plattform und Programmiersprache kommunizieren können.

Microsoft ist für seine exzellenten Entwicklungstools bekannt; das gilt auch für Tools zur Unterstützung des .NET Compact Framework (siehe auch unter 4.3.4).

Im Unterschied zur J2ME ist das .NET Compact Framework nur auf Microsoft-Betriebssystemen (Schwerpunkt Windows Mobile) ablauffähig.

4.3.4 Beispiele zukunftsorientierter mobiler Anwendungsplattformen

Zu Beginn der Ära mobiler Anwendungen haben einige innovative Start-up-Firmen mobile Plattformen auf den Markt gebracht, die dieses Thema überhaupt ins Rollen brachten und durchaus interessante Funktionen aufwiesen. Jedoch passte diese rasch entwickelte Middleware meist nicht in die gewachsene Portal-Server- und Application-Server-Landschaft, sondern basierte auf proprietärer, Nicht-Standard-Software. Die Folge war, dass die meisten dieser Firmen nicht überleben konnten.

Mittlerweile haben alle großen Plattformhersteller Tools und Funktionen für die Integration mobiler Anwendungen bereitgestellt. Microsoft, IBM und SAP sind dabei am besten positioniert. Dies hängt natürlich auch mit der Marktdurchdringung der existie-

renden Plattformen und Anwendungen zusammen. Gleichwohl sind die Technologien noch nicht ausgereift und neue Software-Versionen werden in kurzen Zeitabständen herausgegeben. Vorausgesetzt, dass Web Services eine wesentliche Rolle im m-Business spielen werden, sind die drei erwähnten Hersteller auch zukünftig in führender Position zu erwarten.

Neben den m-Business-Plattformen von Microsoft, IBM und SAP sind zwei spezialisierte mobile Lösungen bzw. Services erwähnenswert: Extended Systems' *Mobile Solutions Platform* und *Managed Mobile Device*, ein Service, der von Siemens Business Services angeboten wird.

Die wichtigsten Merkmale dieser Plattformen werden im Folgenden kurz erläutert.

Microsoft Mobile .NET

Business an jedem Ort, zu jeder Zeit und mit jedem Gerät – Microsofts Vision – führte anfänglich zur Unterstützung mobiler Geräte durch den *Mobile Information Server* und den *Mobile Outlook Manager*, einer Outlook-Komponente. In der Zwischenzeit hat sich Microsofts Engagement eindrucksvoll in einer Reihe von Produktentwicklungen manifestiert wie *Windows Mobile* (Pocket PC und Smartphone), *.NET Compact Framework*, *Outlook Mobile Access* und die Integration mobiler Funktionen in .NET Servern. Microsofts Mobile-.NET-Architektur ist in Bild 4.8 illustriert. Dazu gehören mobile Clients, Unterstützung mobiler Netze, Enterprise Server und -Services, User Experiences, Solutions und Tools. Wie das Bild zeigt, spielen Web Services als Verbindungstechnologie eine zentrale Rolle.

Besonders erwähnenswert sind die Entwicklungstools für mobile Anwendungen des *Visual Studio .NET Development Environment* [4.3.9] mit seinen Erweiterungen *Smart*

Bild 4.8 Microsoft Mobile .NET Architektur

Device Programmability for Visual Studio.NET, die in Verbindung mit dem .Net Compact Framework genutzt werden.

Beim Design von mobilen *ASP.NET*-Web-Applikationen ist darauf zu achten, das User Interface strikt von der Business-Logik und der Datenspeicherung zu trennen. Der Vorteil der Trennung der Präsentationsaufbereitung von der Geschäftslogik liegt darin, dass der Logik-Code, der für den Desktop oder das mobile Gerät geschrieben wurde, wiederverwendbar ist. Es ist zwar erforderlich, einen Satz von *Web Form Pages* für den Desktop und einen Satz *Mobile Web Form Pages* für die mobilen Geräte zu schreiben, der Teil der Geschäftslogik bleibt jedoch unverändert.

Sowohl das .Net Framework als auch das .NET Compact Framework verwenden das Konzept der *Mobile Controls*. ASP.NET teilt große Webseiten automatisch in kleinere Einheiten, die passend sind für die Präsentation auf mobilen Geräten. Zur Laufzeit generieren unterschiedliche Mobile Controls für unterschiedliche Inhaltstypen (z. B. Textview, Textbox, List, Link, Command, Calendar, Image usw.) den entsprechenden Präsentations-Code in Abhängigkeit von der Geräteklasse. Der Entwickler muss sich also nicht um die Präsentationsspezifika der einzelnen Geräte kümmern.

Aufgrund dieses Konzepts der *Mobile Controls* und der Wiederverwendbarkeit der Business-Logik ergibt sich eine weitgehende Gleichheit der Benutzeroberfläche für Desktops und mobile Geräte, während die Entwicklungskosten und -zeiten erheblich reduziert werden können. In Bezug auf Einfachheit und Produktivität nehmen Microsofts Entwicklungswerkzeuge eine führende Rolle ein.

IBM WebSphere Everyplace

Die Produktfamilie *IBM WebSphere Everyplace* [4.3.10] besteht aus verschiedenen Komponenten für Netzwerkverbindungen, Zugangskontrolle zum Unternehmen, Transformation, Management und Entwicklungstools und schließt auch mobile Anwendungen mit ein. Die wichtigsten Komponenten sind:

Everyplace Connection Manager

Der *Everyplace Connection Manager* stellt die Verbindung mobiler Geräte zum Intranet des Unternehmens her. Dies erfolgt unter Nutzung eines VPN über WLAN, GSM/GPRS oder andere Netze. Konfiguriert als WAP Proxy bedient der Connection Manager auch WAP Clients. Der Connection Manager unterstützt zudem verschiedene Authentifikations- und Verschlüsselungsmethoden sowie die Protokolle WTLS und SSL. Hervorzuheben ist die dynamische Roaming-Fähigkeit, die einen nahtlosen Übergang – also ohne Verbindungsunterbrechung – bei Wechsel des Netzes, z. B. von WLAN zu GPRS, gewährleistet.

Everyplace Access

Diese Komponente ermöglicht mobilen Nutzern den Anschluss an existierende Anwendungen im Unternehmen und eröffnet gleichzeitig neue mobile Anwendungen. Wie in Bild 4.9 dargestellt, unterstützt *Everyplace Access* die Synchronisation von PIM und e-Mail mit Lotus Notes und Microsoft Exchange und bietet Services zur Synchro-

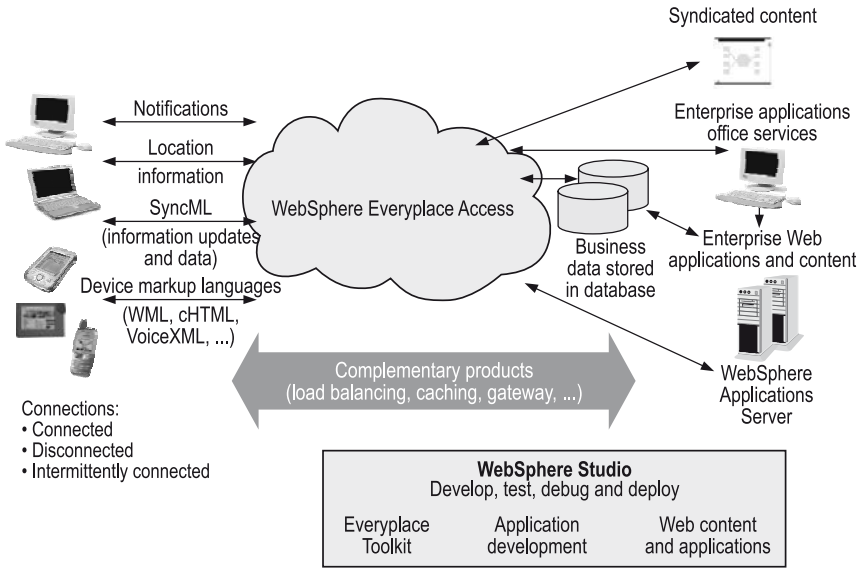


Bild 4.9 WebSphere Everyplace Access (Source: IBM)

nisation von mobilen mit zentralen Datenbanken sowie den Zugang zu Unternehmensanwendungen (CRM, ERP usw.).

Everyplace Access ermöglicht darüber hinaus Notification (Push) Services, durch die Nutzer, ausgelöst durch Nachrichten, e-Mails oder definierte Ereignisse, proaktiv benachrichtigt werden.

Everyplace Access ist Bestandteil der WebSphere-Portal- und Application-Server-Infrastruktur, die eine zuverlässige und skalierbare Anwendungsplattform darstellt.

Everyplace WebSphere Studio

Die Entwicklungsumgebung *Everyplace WebSphere Studio* enthält Portlet-Entwicklungstools sowie Tools zur Inhaltsanpassung, um Anwendungen für den Einsatz Browser-basierter oder Java-basierter (J2SE and J2ME) mobiler Geräte zu erweitern.

IBMs Programmiermodell für mobile Anwendungen sieht Portale als zentralen Mechanismus für das Aggregieren von Informationen und den Zugang zu Unternehmensressourcen vor, unabhängig von den verwendeten Gerätetypen. Aus diesem Grund bietet das Everyplace Toolkit des WebSphere Studios Portal/Portlet-Tools für Entwicklung, Test und Debugging an. Dazu gehört die Entwicklung individueller mobiler Portlets mit entsprechender Inhaltsaufbereitung für mobile Geräte. Schablonen (Templates) helfen dabei, mobile Portlets und Anwendungen schnell und einfach zu erstellen.

Tools zur Inhaltsanpassung und Präsentation wie *Markup and Annotation Editors* erleichtern die Anpassung existierender Inhalte an die unterschiedlichen Markup-Sprachen und unterstützen eine Vielfalt von Geräten. Das Everyplace Toolkit für

WebSphere Studio liefert auch Beispiele und Templates für die häufigsten mobilen Anwendungen.

SAP Mobile Infrastructure

Die *SAP Mobile Infrastructure (SAP MI)* ist Bestandteil sowohl der *mySAP Technologie* als auch der *NetWeaver-Plattform* (Details in Kapitel 5). Sie besteht aus der *Mobile Engine (SAP ME),* der Softwarekomponente auf dem mobilen Gerät und dem *Mobile Engine Server,* der auf dem *SAP Web Application Server* abläuft. SAP MI schließt Synchronisations- und Replikations-Funktionen ein, die es ermöglichen, dass mobile Nutzer sich mit Back-End-Ressourcen synchronisieren können. SAP MI verwendet Authentifikation, Role-Based-Autorisierung und Secure Socket Layer (SSL), um eine sichere End-to-End-Verbindung zwischen dem mobilen Client und dem Back-End-System zu gewährleisten. Die mobile Infrastruktur ist in das *SAP Enterprise Portal* integriert und kann somit zentrale Services wie Installation, User und Application Management nutzen.

SAP ME [4.3.11], wie in Bild 4.10 dargestellt, ist die SAP-Anwendungsplattform für mobile Clients. Als eine betriebssystemunabhängige Laufzeitumgebung für mobile Anwendungen basiert SAP ME auf dem J2ME/J2SE Framework und kann auf Laptops, PDAs oder Smartphones eingesetzt werden. SAP ME unterstützt WLAN, GSM/GPRS und Bluetooth.

SAP ME verfügt über eigene Web Server, Datenbank und Business-Logik, d.h. Nutzer können Unternehmensaufgaben wahrnehmen, unabhängig davon, ob sie online oder offline arbeiten. SAP ME erlaubt Multi-User-Betrieb, so dass z. B. auch Anwendungen für Schicht-Mitarbeiter unterstützt werden können. SAP ME bietet eine Reihe von Tools, welche die Entwicklung mobiler Anwendungen sowie ihre Administration und Nutzung erleichtern.

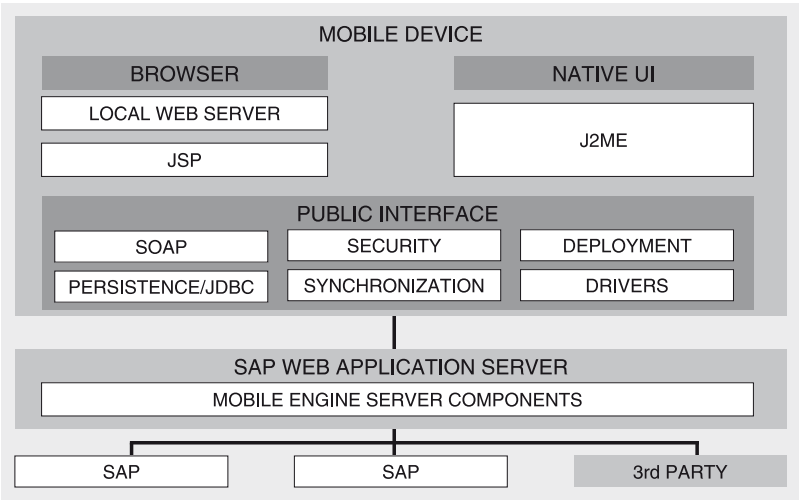


Bild 4.10 SAP Mobile Engine (Source: SAP)

Extended Systems Mobile Solutions Platform

Die *Extended Systems Mobile Solutions Platform* [4.3.12] bietet Business Solutions für Vertrieb und Field Services. Die Plattform soll ermöglichen, dass existierende Anwendungen sowohl für Vertriebsmitarbeiter als auch für Kollegen im Außendienst unterwegs und in Außenstellen entsprechend der Netzarchitektur des Unternehmens verfügbar werden.

Die Mobile Solutions Platform bietet umfangreiche Geräteunterstützung, Netzunterstützung, Entwicklungstools, End-to-End Security, Synchronisation, Management/ Administration sowie Funktionen zur kundenspezifischen Anpassung und Anwendungsintegration.

Die Geräteunterstützung schließt Palm, Pocket PC, Smartphones, Symbian und Browser-basierte Geräte (WAP Phones, Laptops), die Netzunterstützung GSM, GPRS, CDMA, Bluetooth, WLAN, Infrared und Cable/Cradle ein.

Das Konzept der Mobile Solutions Platform ist in Bild 4.11 dargestellt.

Die Plattform kann mehrere Front- und Back-End-Services und -Ressourcen in einheitlicher Form darstellen und ermöglicht Zugang über Single Log-in. Vorgefertigte Konnektoren für Siebel CRM, SAP ERP, Microsoft Exchange und Lotus Notes erleichtern die Integration von Standardanwendungen. Erweiterte Konnektoren erlauben die Integration von kundenspezifischen Anwendungen. Die Plattform läuft auf den gängigen Java Application Servern, sowohl auf Windows als auch auf Unix-Betriebssystemen.

Die Mobile Solutions Platform zeichnet sich durch Systemunabhängigkeit, breite Geräte- und Netzunterstützung und insbesondere durch umfangreiche Management-Funktionen aus.

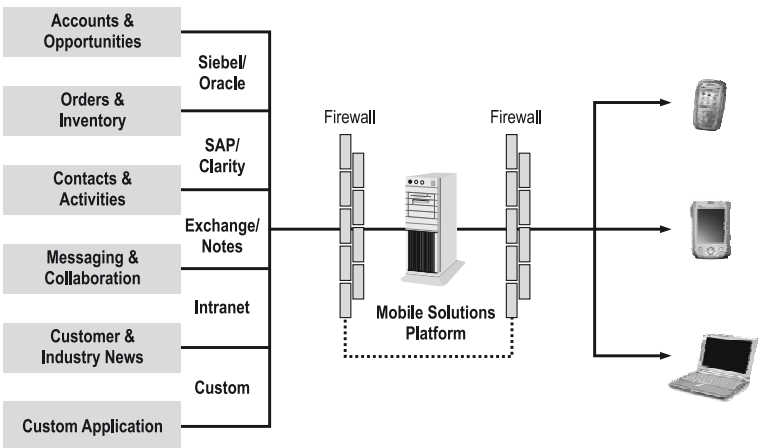


Bild 4.11 Extended Systems Mobile Solution Platform

Managed Mobile Device (MMD) Service von Siemens Business Services

MMD ist ein Service für das Management von PDAs und Smartphones mit dem Betriebssystem Windows Mobile, der von Siemens Business Services angeboten wird. Er umfasst Installation, zentrales Management von Geräten, Anwendungen und Daten sowie den sicheren Zugang zu Unternehmensressourcen. In Bild 4.12 ist eine mögliche Konfiguration und die Einbindung des Service in ein Unternehmensnetz dargestellt.

Die Erstinstallation und Konfiguration des mobilen Gerätes wird mittels einer personalisierten SD/MMC (SD Card/Multimedia Memory Card) durchgeführt, die sämtliche Konfigurationsdaten, persönliche Daten und beliebige kundenspezifische Module enthält. Wenn Nutzer diese Karte auf dem Postweg erhalten haben, wird das Gerät nach Einstecken der Karte und Eingabe der persönlichen ID in wenigen Minuten automatisch konfiguriert, ohne Cradle und ohne dass sich der Nutzer umständlich mit Konfigurationsparametern auseinandersetzen muss.

Ein wesentliches Differenzierungsmerkmal des MMD Service ist, dass unmittelbar nach automatischer Installation der Karte und ohne weitere Einstellungen die kundenspezifisch konfigurierbaren Anwendungen produktiv genutzt werden können. Das zentrale Management der Geräte einschließlich der Software- und Datenverteilung stellt sicher, dass einheitliche Versionen im Einsatz sind, und ermöglicht Updates bei niedrigen Betriebskosten. Updates und Änderungen können online über Mobilnetze (GPRS, WLAN, UMTS) oder LAN durchgeführt werden.

Als weitere Differenzierungen bietet MMD mit Verschlüsselungsfunktionen, VPN und optionalem Virenschutz Sicherheit für höchste Ansprüche sowie hohe Verfügbarkeit durch Backup-Funktionen und automatische Recovery-Funktionen bei Systemausfall.

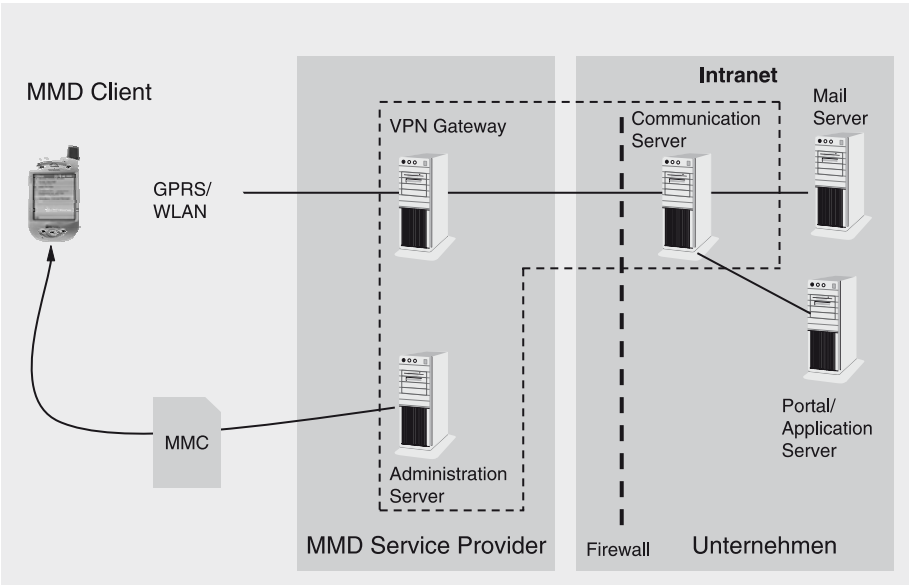


Bild 4.12 Mobile Managed Device (MMD) Service

Mit diesen Eigenschaften ist der MMD Service für beliebige mobile Unternehmensanwendungen mit Zugang zum Intranet geeignet. Das optionale e-Mail/PIM Modul ermöglicht die Nutzung der Mail-/Kontakt-/Kalender-Funktionen von Microsoft Exchange oder Lotus Domino.

Mobility Solutions von Fujitsu Siemens Computers

Fujitsu Siemens Computers bietet zusammen mit Partnern *Mobility und Business Critical Computing Solutions* [4.3.13]. Diese Lösungen sollen den Anspruch erfüllen, zu jeder Zeit, an jedem Ort und mit beliebigen Geräten auf Informationsdienste zugreifen zu können, die sowohl von Organisationen für ihre Geschäftstätigkeiten benötigt als auch von Konsumenten für private Aktivitäten gewünscht werden.

Die Mobility Solutions von Fujitsu Siemens Computers sind auf fünf strategische Felder fokussiert:

- Security: Gewährleisten von End-to-End Security in Infrastrukturen für mobile Lösungen
- Manageability: Sicherstellen, dass Mobility-Infrastrukturen von IT-Abteilungen einfach zu managen sind
- Messaging: Verfügbar machen von Messaging- und Collaboration-Infrastrukturen für mobile Beschäftigte
- Connectivity: Gewährleisten eines zuverlässigen, skalierbaren und sicheren drahtlosen Zugangs zu Infrastrukturen und Anwendungen von Unternehmen
- Business Information Access: Ermöglichen mobilen Zugangs zu geschäftsrelevanten Informationen sowie geschäftskritischen Infrastrukturen und Anwendungen wie Enterprise Resource Planning (ERP), Customer Relationship Management (CRM) und Sales Force Automation (SFA).

Fujitsu Siemens Computers bietet eine umfassende Palette von mobilen Produkten an. Dazu zählen: Pocket LOOX PDA, LIFEBOOK professional Notebooks, STYLISTIC Tablet PCs, CELSIUS Mobile Workstations und FUTRO thin Clients.

4.4 Beispiele mobiler Anwendungen

Die erste Welle mobiler Anwendungen in Unternehmen ist vorüber. Die proprietären Technologieansätze und Plattformen sind wieder verschwunden. M-Business-Projekte verliefen häufig enttäuschend oder haben jedenfalls die Erwartungen hinsichtlich Nutzen und Mehrwert für das Unternehmen nicht erfüllen können.

Studien von Analysten zeigen, dass Qualität und Funktionalität von mobilen Geräten mittlerweile ausreichend sind (mit Ausnahme der Batteriekapazitäten), wohingegen Systemunterstützung, Anwendungsintegration und mobile Services verbesserungsbedürftig sind. Das einzig wirklich kritische Thema heißt Security – und das könnte eine breitere Akzeptanz mobiler Anwendungen weiterhin verhindern.

Interessant ist, welch unterschiedliche Argumente von CEOs, Bereichsverantwortlichen und CIOs als Hindernisgründe genannt werden. Während Vorstände im Wesentlichen auf die hohen Einführungs- und Betriebskosten verweisen, erwähnen die Bereichschefs nur die Einführungskosten, betonen aber, dass noch Funktionalitäten fehlen, um wirklichen Mehrwert schaffen zu können. CIOs dagegen führen als Hauptgrund an, dass die Security noch nicht adäquat gelöst sei.

Gleichwohl haben die vergangenen Jahre auch gezeigt, dass ausgewählte Anwendungen den Unternehmen durchaus Mehrwert bringen können. Dies gilt besonders für folgende Lösungsbereiche:

– Sales Force Automation
– Field Service
– Optimierung von Lieferketten
– Tracking und Logistik
– Prozessüberwachung.

B2E-Anwendungen wie Sales Force Automation und Field Service werden unter 4.4.1 ausführlicher erläutert. Nachfolgend wird ein kurzer Blick auf die anderen Anwendungsfelder geworfen.

Optimierung von Lieferketten

Die Effizienz von Lieferketten hängt mit der optimalen Koordination aufeinanderfolgender Schritte zusammen, die zur Erzeugung eines Produktes notwendig sind. Das gilt sowohl für eine Fließbandfertigung wie auch für einen Lieferservice. Die Koordination kann durch eine Leitzentrale optimiert werden, die über den jeweiligen Ort der involvierten Objekte informiert ist. Nach einem vordefinierten Prozessmodell greift die Leitzentrale aktiv ein und steuert die Bewegung der Objekte entsprechend koordinierter Abläufe. Unternehmensübergreifende Lösungen sind hier die populärsten Ansätze.

Die Ortserfassung der Objekte zu beliebigen Zeitpunkten kann durch Anwendung drahtloser Techniken wie *RFID (Radio Frequency Identification)*, GSM/GPRS oder GPS erreicht werden, entweder automatisch (z. B. durch eingebettete RFID Chips) oder durch Personen, die Ortsveränderungen via GPRS or WLAN an die Leitzentrale melden.

Der offensichtliche Nutzen von Prozesssteuerungen mit mobilen Technologien sind verkürzte Produktionszeiten, Vermeidung von Engpässen, effiziente Nutzung von Lagerbeständen und flexible Handhabung in Ausnahmefällen.

Tracking and Logistik

Von Mitarbeitern verursachte Fehler und unkontrollierte Aktivitäten in der Logistik und bei Auslieferungen sind Probleme, mit denen Logistikfirmen häufig zu kämpfen haben. Das verursacht auch Verärgerung bei betroffenen Kunden. Mit dem Einsatz drahtloser Technologien können Lieferobjekte unabhängig von der jeweiligen Position aufgespürt und verfolgt werden, während gleichzeitig die Auswahl des Transportmit-

tels, die Koordination der Routen und Partner und andere kostenrelevante Maßnahmen effizient organisiert werden können. Wie bei Lieferkettenlösungen lassen sich auch hier verschiedene Mobiltechnologien kombiniert einsetzen.

Die Vorteile sind präzisere Informationen, kürzere Reaktionszeiten, Kosteneinsparungen sowie Kunden- und Partnerzufriedenheit.

Prozessüberwachung

Prozessabläufe in Unternehmen können als eine Serie zusammenhängender Transaktionen gesehen werden, die sich über die gesamte Wertschöpfungskette erstrecken. Anwendungen unterstützen dabei die verschiedenen Prozesse wie HR (Human Resource), CRM, Auftragsbearbeitung, Auslieferung, Rechnungsstellung, Revision, Qualitätssicherung, Reparatur usw. Wesentlich für eine laufende Anpassung und Effizienzsteigerung dieser Prozesse ist ihre Überwachung, um Engpässe und Fehler herauszufinden und Leistungskriterien zu identifizieren. Selbstverständlich sollten diese Überwachungsaufgaben nicht auf Festnetztechnologien beschränkt bleiben.

Die Art und Weise, wie Unternehmensprozesse durch mobile Technologien unterstützt werden können, hängt sehr von den Prozessen selbst ab. Um ein Beispiel zu nennen: In manchen Fällen könnte es sich als effizienter herausstellen, einen Satz von IT-Ersatzteilen in einsatzbereiten Fahrzeugen anstatt in herkömmlichen Ersatzteillagern zu deponieren. Die Standorte und Routen dieser Fahrzeuge können, abhängig von den gemeldeten Störungen, in Echtzeit optimal gesteuert werden. Damit lassen sich Ausfallzeiten verkürzen und Service Level deutlich verbessern.

4.4.1 B2E-Anwendungen

Analysten erwarten, dass sich B2E-Anwendungen erfolgreich als m-Business-Lösungen etablieren werden. Beispiele von *B2E-Anwendungen* sind in Bild 4.13 gezeigt.

Untersuchungen haben gezeigt, dass branchenabhängig 20% bis 80% der Mitarbeiter als mobile Beschäftigte einzustufen sind, wobei angenommen wurde, dass sie 20% ihrer Arbeitszeit außerhalb des Unternehmens verbringen oder zumindest unterwegs auf mobile Services angewiesen sind. Im Durchschnitt sind davon etwa 40% Vertriebsmitarbeiter, während weitere 30% im Außendienst arbeiten. Dann folgt mit etwa 20% die Gruppe der Reisenden, 10% fallen auf Manager und Vorstände.

PIM (e-Mail, Kalender, Kontakte und Notizen) verbunden mit Microsoft Exchange oder Lotus Notes ist für all diese Gruppen unverzichtbar. PIM ist deshalb die horizontale Mobilanwendung mit der höchsten Priorität. Unterstützende Travel Services (Fluginformationen, Reservierungen, Buchungen, Routenführungen, Points of Interest usw.) sind weitere horizontale Anwendungen, die zusammen mit PIM entweder von Unternehmen selbst oder von Netzbetreibern (z. B. Location-based Services) und anderen Diensteanbietern (z. B. Global Distribution Services wie Amadeus, Sabre) angeboten werden.

Die anderen in Bild 4.13 gezeigten Anwendungen sind unternehmensspezifisch in existierende Ressourcen zu integrieren (z. B. Directory Services, Datenbanken, Data Ware-

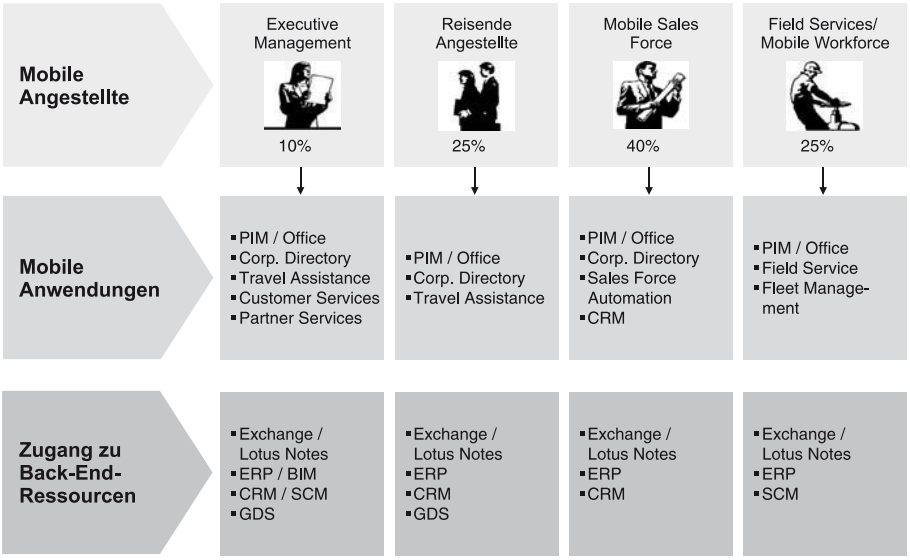


Bild 4.13 B2E-Anwendungen

houses) oder gehören in die Kategorie der vertikalen Anwendungen, die dedizierte Aufgaben meist branchenspezifisch unterstützen. In der Regel sind diese mobilen Anwendungen in die gängigen Unternehmensanwendungen (z. B. CRM, ERP, SCM) zu integrieren. In den meisten Fällen werden vertikale Anwendungen von den Unternehmen selbst implementiert oder von spezialisierten Outsourcing Service-Providern im Auftrag ihrer Kunden betrieben.

Die Szenarien Travel Services, Sales Force Automation und Field Service werden im Folgenden in Beispielen erläutert, um die Bedeutung von mobilen Anwendungen bewusst zu machen sowie Nutzen und Realisierbarkeit zu veranschaulichen.

Mobile Reisedienste

Ein hervorragendes Beispiel für den Nutzen von mobilen Services sind Reisedienste (Seamless Mobile Travel Services), die den Reisenden vor, während und nach einer Reise unterstützen, wie in Bild 4.14 veranschaulicht.

In modernen Unternehmen arrangieren Angestellte ihre Geschäftsreisen selbst von ihrem Arbeitsplatz aus, indem sie Travel Services im Unternehmensportal aufrufen: Erstellen eines Reiseplans, Buchung von Bahn- oder Flug-Tickets, Mietwagen und Hotelresevierungen. Meist müssen firmenspezifische Reiserichtlinien berücksichtigt werden. Gegebenenfalls kann der Reisende nach Überprüfung seines Miles&More-Kontos einen Upgrade für den Flug vornehmen. Das Portal bietet noch weitere Services, so dass schon im Voraus für das Wochenende am Zielort Veranstaltungen gebucht werden können.

Unterwegs zum Airport wird der Reisende automatisch über Verkehrsstaus informiert und alternative Routen werden vorgeschlagen. Vor Eintreffen im Airport erhält er eine weitere (Push-)Nachricht auf seinem Mobiltelefon, um ein vorgezogenes Check-in zu

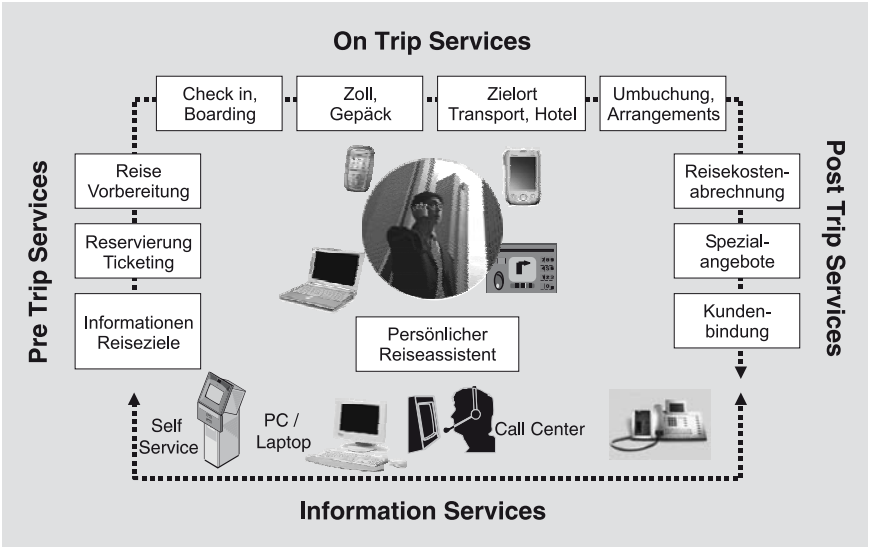


Bild 4.14 Rund-um-die-Uhr-Travel-Services

ermöglichen. Der Reisende bestätigt das Check-in und erhält anschließend Parkplatznummer, Flugbezeichnung und Sitzplatznummer sowie die aktuelle Abflugzeit mitgeteilt. Entspannt parkt der Reisende auf dem reservierten Parkplatz und begibt sich ins Flugzeug. Am Check-in Gate wird dann über Bluetooth die Autorisierung für diesen Flug geprüft.

Vor dem Kundenbesuch am Zielort möchte der Reisende noch die aktuellen Umsatzzahlen und Produktpreise aus dem Firmennetz abrufen und in die Powerpoint-Präsentation übernehmen. Vom Hotel aus wählt er sich in das Firmennetz ein und erhält nach Authentifikation über das Unternehmensportal Zugang zu den entsprechenden Anwendungen.

Ein Travel Service rund um die Uhr zeichnet sich dadurch aus, dass eine Reise jederzeit auch vor Ort geändert werden kann, wenn unvorhergesehene Ereignisse dies erfordern. Die Unterstützung durch eine Sekretärin ist nicht mehr nötig.

Der personalisierte Travel Service, implementiert als Software-Komponente im Portal, hilft dem Reisenden, der sich vielleicht gerade in New York aufhält, Flüge umzubuchen und Hotelreservierungen zu stornieren, während seine Sekretärin in München ruhig in das Wochende hineinschläft. Der Travel Service kennt den Aufenthaltsort des Reisenden, ist über Reiseplan, Terminkalender und persönliche Reisepräferenzen informiert und beachtet die Reiserichtlinien des Unternehmens. Darüber hinaus liefert der Travel Service ortsabhängige Wetter- und Verkehrsinformationen und hält den Reisenden mit aktuellen Infos auf dem Laufenden. Optionale Services wie Stadtführer, Straßenkarten, öffentlicher Nahverkehr, Einkaufsgelegenheiten und Freizeitangebote tragen dazu bei, den Aufenthalt für den Reisenden so angenehm wie möglich zu gestalten.

Da der Travel Service alle Reiseaktivitäten samt Umbuchungen verfolgt, wird am Ende der Reise automatisch eine Reisekostenabrechnung erstellt. Im Portal integrierte Business Intelligence Software analysiert die gesamten Reiseaktivitäten und zeigt Kosteneinsparungspotenziale auf. Verantwortliche Manager können daraus Schlussfolgerun-

gen ziehen und z. B. günstigere Buchungskonditionen aushandeln und Reiseprozesse optimieren.

Mobile Vertriebsunterstützung

Vertriebsleute sind naturgemäß viel unterwegs und mit dem Einsatz mobiler Technologien können erhebliche Produktivitätssteigerungen erreicht werden. Mobile Vertriebsunterstützung (Mobile Sales Force Automation) kann Informationsdefizite vermeiden helfen, indem in Echtzeit-Kommunikation neueste Produktinformationen, Auftrags- und Umsatzzahlen ausgetauscht werden und aktuell auf Wünsche des Kunden eingegangen werden kann. Darüber hinaus bieten mobile Lösungen die Möglichkeit des nahtlosen Informationsaustauschs zwischen Vertriebs- und Service-Mitarbeitern, auch wenn sie an verschiedenen Standorten des Kunden tätig sind. Diese Kompetenz beeindruckt Kunden und erhöht die Kundenzufriedenheit.

Das folgende Szenario aus dem Arbeitsalltag eines Vertriebsbeauftragten zeigt, wie sich Produktivität durch den Einsatz mobiler Technologien signifikant steigern lässt.

Robert, ein Vertriebsprofi, arbeitet in einer Firma, die IT-Services und -Produkte anbietet. Er beginnt seinen Arbeitstag, indem er seinen Laptop von zuhause aus via DSL und VPN mit dem Firmennetz verbindet. Robert wird zunächst am Unternehmensportal authentifiziert. Das geschieht automatisch durch Einschieben seiner Firmen-Smartcard in den Kartenleser seines Laptops. Auf der Smartcard sind sowohl digitale Zertifikate, die in Verbindung mit der Firmen-PKI zur Authentifikation verwendet werden, als auch die erforderlichen Passwörter für den Zugang zu Portalanwendungen gespeichert. Zunächst beantwortet Robert die eingelaufenen Mails, wirft dann einen Blick auf seinen Terminkalender und die anstehenden Kundentermine (Outlook/Exchange), sowie auf die aktuellen Kundenaufträge (CRM) und Liefertermine (ERP).

Auf dem Weg zum ersten Kunden benutzt Robert seinen PDA mit GPRS und GPS und die Tom Tom Navigator Software, um seinen Kunden auf dem schnellsten Weg zu erreichen. Unterwegs fällt ihm ein, dass eine technische Frage des Kunden noch nicht beantwortet wurde. Mit seinem GPRS-Mobiltelefon greift er auf eine firmeninterne WAP-Applikation zu, um die Telefonnummer eines technischen Experten aus dem Corporate Directory herauszufinden. Dann ruft er den Experten an und klärt die offene Frage.

Auf dem Parkgelände des Kunden verbindet Robert seinen PDA via GPRS und VPN mit seinem Firmennetz und greift auf die CRM-Anwendung zu. Dort kann er den aktuellen Stand der Wartungsarbeiten beim Kunden abfragen. Er erfährt, dass am Morgen ein ernsthaftes Problem beim Update einer mySAP Anwendung aufgetreten ist. Mit wenigen Eingaben am PDA – mittels Stift – kann er in der CRM-Anwendung einen Nachrichten-Service aktivieren, durch den er unmittelbar nach Beheben des Update-Problems benachrichtigt werden soll.

Robert präsentiert beim Kunden ein neues Service-Level-Konzept anhand einer Offline-Anwendung auf seinem Laptop und erläutert die technischen Details der Kundenanfrage. Anschließend will der Kunde noch über einige kritische Liefertermine informiert werden. Robert benutzt wieder seinen „Always-on“-PDA und fragt eine ERP-Anwendung ab, um die angeforderten Informationen abzurufen. Erleichtert stellt er fest, dass die fraglichen Produkte am Vortag abgeschickt wurden und somit sogar noch vor dem vereinbarten Termin geliefert werden können. Während der abschließenden Besprechung mit dem Kunden meldet sich Roberts PDA mit der Nachricht, dass das Service-

Team das Update-Problem soeben behoben hat und der Produktivbetrieb wieder aufgenommen wurde. Der Kunde ist sehr zufrieden und unterzeichnet die neue Service-Level-Vereinbarung.

Robert sucht als nächstes ein Cybercafé auf. Nach Vorzeigen eines Vouchers erhält er eine Benutzer-PIN. Damit kann er das dortige WLAN nutzen und seinen Laptop via VPN mit dem Firmennetz verbinden. Er meldet die Abschlussdaten des neuen Service-Level-Vertrags an das CRM-System, um noch Eingang in den Monatsbericht zu finden, der bis zum Abend automatisch erstellt wird. Motiviert durch den erfolgreich verlaufenen Kundenbesuch, veranlasst Robert das CRM-System, Terminvorschläge für fünf weitere Kunden zu versenden, denen er das neue Service-Level-Konzept vorstellen will. Das CRM-System bietet Multichannel Services und hat die Kommunikationsmöglichkeiten und -präferenzen der Kunden gespeichert. Das System stellt fest, ob ein Kunde vorzugsweise per e-Mail, Fax oder Telefon zu benachrichtigen ist. In Echtzeit wird Robert durch das CRM-System informiert, dass einer der ausgewählten Kunden am besten per Telefon kontaktiert werden sollte. Robert schaut sich in der Datenbank noch die vorangegangenen Aktivitäten bei diesem Kunden an und vereinbart dann telefonisch einen Termin.

Während Robert noch im Café sitzt, führt die zentrale Administration einen Update-Lauf für die im Unternehmen eingesetzten PDAs durch. Abhängig von Roberts Aufgabenprofil werden automatisch die neuesten Informationen auf seinen „Always-on"-PDA geladen. Robert wird abschließend informiert, dass neue Produkt-Konfigurationen freigegeben und die entsprechenden Preise in der neu geladenen Preistabelle ergänzt worden sind. Da diese Informationen wichtig für seinen nächsten Kundenbesuch sind, verbindet er Laptop und PDA via Bluetooth und ergänzt Produktinformationen und Preistabelle als Anhang zum Vertrag, den er auf dem Laptop vorbereitet hat und mit dem Kunden besprechen möchte.

Im Büro des Kunden druckt Robert auf dem dort vorhandenen Drucker über Bluetooth den Vertrag samt Anhängen aus. Nun kann er den aktualisierten Vertrag gleich in ausgedruckter Form zur Besprechung vorlegen. Das kommt bei den meisten Kunden gut an.

Bevor Robert den Parkplatz des Kunden verlässt und sich am späten Nachmittag auf den Weg zum Airport begibt, ruft er per Mobiltelefon eine WAP-Anwendung auf und ordert einen Blumenstrauß, der seiner Frau am nächsten Tag als Geburtstagsüberraschung überreicht werden soll. Danach fordert er per SMS mit Ankunftszeit und Aufenthaltsdauer eine Parkplatzreservierung am Flughafen an. Einige Sekunden später erhält er eine SMS, die die Anfrage bestätigt und eine Parkplatznummer mitteilt. Per SMS bestätigt Robert den Buchungsvorgang. Die Abrechnung von Blumen und Parkgebühr erfolgt mit der nächsten Telefonrechnung des Netzbetreibers.

Im Airport muss Robert etwa eine Stunde Wartezeit überbrücken und nutzt wiederum das dort verfügbare WLAN, um seinen Laptop ins Firmennetz einzuloggen. Er bearbeitet die Liste der neu eingegangenen e-Mails und lädt eine Powerpoint-Datei, die von einem Kollegen überarbeitet wurde und die er am nächsten Tag für einen ausländischen Kunden benötigt. Als nächstes startet er das e-Learning-Programm des Unternehmens, um seine Kenntnisse über die Bilanzregeln von US GAAP zu vervollständigen. Die zentrale e-Learning-Web-Applikation hat Roberts Lernstatus laufend überwacht und registriert, welche Lernmodule lokal auf seinem Laptop gespeichert sind. Robert absolviert den Test der letzten Lektion und erhält eine sinnvolle Auswahl der nächsten Module zum Download angeboten, die er dann zu einem beliebigen Zeitpunkt offline bearbeiten kann.

Nach dem Flug kommt Robert am späten Abend im reservierten Hotelzimmer an und nutzt seine Geräte nun für Freizeitaktivitäten. Er versendet MMS (ein Bild des Hotelzimmers an seine Frau), macht ein Restaurant in der Nähe ausfindig und entspannt sich schließlich nach dem Abendessen bei MP3-Musik in seinem Zimmer.

Mobile Field Service

Das folgende Beispiel, *m-Butler*, ist eine mobile Anwendung, die von Siemens Business Services angeboten wird und an unterschiedliche Außendienst-Szenarien angepasst werden kann. Der Überblick in Bild 4.15 zeigt den Anbieter des Field Service (Außendienst), den mobilen Service-Techniker, den Kunden vor Ort sowie die typischen Arbeitsschritte im konkreten Einsatzfall.

Das Service-Unternehmen bietet Wartungs- und Reparatur-Services für komplexe medizinische Systeme wie Computertomographen, Angiographie- und Röngtensysteme usw. an. Es betreibt ein Call Center sowie CRM- und ERP-Systeme auf Basis SAP/R3 zur Kundenbetreuung und Abwicklung von Wartungsdiensten, Reparaturarbeiten und gemeldeten Störungen. Zusätzlich ist ein Kommunikationszentrum mit dem R3-System verbunden, das den Einsatz von einigen Hundert mobilen Arbeitskräften steuert. Dazu gehört auch ein Nachrichtendienst, der je nach Situation verschiedene Kommunikationskanäle wie e-Mail, SMS/MMS und Fax benutzt.

Die mobilen Service-Techniker sind ständig unterwegs und kommunizieren mit der Zentrale über ihre PDAs mit GSM/GPRS-Mobilnetzanschluss.

Störungsmeldungen eines Kunden werden im Call Center entgegengenommen. Wenn durch die Call-Center-Beratung der Fehler nicht ausreichend identifiziert werden kann, wird ein Störungsprozess im R3-System initiiert und gleichzeitig ein Service-Techniker zugewiesen. Die Auswahl des Technikers erfolgt abhängig von Verfügbarkeit, technischer Qualifikation und Entfernung zum Standort des Kunden. Diese Parameter der Service-Techniker werden laufend überwacht und die Zuweisung des Technikers wird vom System automatisch durchgeführt.

Das CRM-System kennt die Historie des Kunden und seine Maschinenkonfiguration. In Verbindung mit dem ERP-System kann das Call Center in manchen Fällen nach Eingabe charakteristischer Fehlersymptome entsprechende Reparaturanweisungen erhalten und an den Kunden oder Service-Techniker weiterleiten. Falls erforderlich, wird im Ersatzteillager die Verfügbarkeit benötigter Teile abgefragt und Ersatzteile werden schon vorab durch einen Lieferservice zum Kunden losgeschickt.

Während der Service-Techniker auf dem Weg zum Kunden ist, steht er online via PDA mit dem Kommunikationszentrum und dem R3-System in Verbindung und besorgt sich Informationen wie Kundenhistorie, Maschinenkonfiguration, Fehlerhinweise, Reparaturanweisungen, Ersatzteillieferungen usw. Er bestätigt den Auftrag und gibt die erwartete Ankunftszeit an. Das PDA-Navigationssystem führt ihn auf dem schnellsten Weg zum Kunden. Der Service-Techniker holt ggf. vorher noch Ersatzteile von einem vereinbarten Ort ab und erfasst die Ersatzteilnummer mit dem Scanner, der an seinem PDA angeschlossen ist.

Schließlich meldet der Service-Techniker der Zentrale, dass er beim Kunden angekommen ist. Nach erfolgreichem Abschluss der Reparatur ruft er über den PDA eine Maske im R3-Sytem auf, um seinen Reparaturbericht einzugeben. Der Bericht erfordert Eingaben über Reparaturdauer, Kundendaten, Materialverbrauch, fehlerspezifische Angaben, Qualitätsaussagen sowie die Auflistung von Ersatzteilen, die zur Reparatur in das

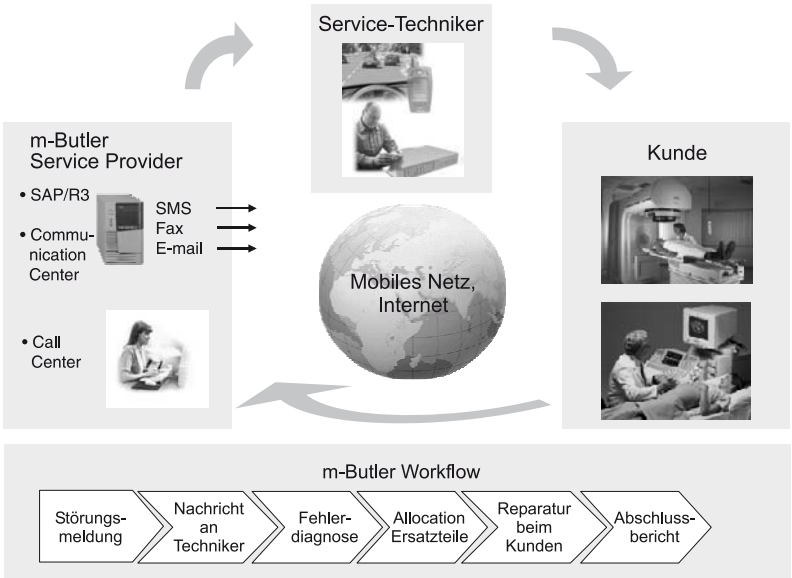


Bild 4.15 Mobile Field Service: m-Butler

Reparaturzentrum eingeschickt werden müssen. Das R3-System verarbeitet den Bericht automatisch und löst die erforderlichen Folgeprozesse wie Rechnungsstellung, Aktualisieren der Kunden- und Fehlerdatenbank sowie Reparatur der eingeschickten Ersatzteile aus.

Dieses Beispiel zeigt wiederum die Optimierung von Service-Prozessen, so dass sowohl Service-Unternehmen als auch Kunden davon profitieren. Die Vorteile für den Kunden, wie unkomplizierte Störungsabwicklung, schnelle und kompetente Reaktion, niedrige Ausfallzeit und geringer Umsatzverlust führen zu Kundenzufriedenheit und verstärkter Kundenbindung. Der Nutzen für das Service-Unternehmen liegt vor allem in seiner Wettbewerbsfähigkeit und der enormen Kosteneinsparung. Weitere Vorteile sind Kostentransparenz, vereinfachte Administration, Motivation der Techniker sowie verbesserte Material- und Qualitätssicherungsprozesse.

4.4.2 Weitere mobile Anwendungen

Mobile Anwendungen werden unsere Gesellschaft und das tägliche Leben von Grund auf verändern. Deshalb werden nicht nur Netzbetreiber, sondern auch viele andere Service-Unternehmen wie Finanzinstitute, Versicherungen, Warenwirtschaft, Agenturen, Versorgungsunternehmen, Kommunen und andere Diensteanbieter die faszinierenden Chancen des m-Business zu nutzen wissen.

Mobile Zahlungsverfahren und mobiles Ticketing sind besonders lukrative Anwendungsfelder, und eine Vielzahl von Lösungen ist heute bereits verfügbar. Hier kommt es nun darauf an, eine Konsolidierung und Vereinheitlichung zu erreichen, um einen weiteren Impuls für weltweit einsetzbare Lösungen zu erzeugen.

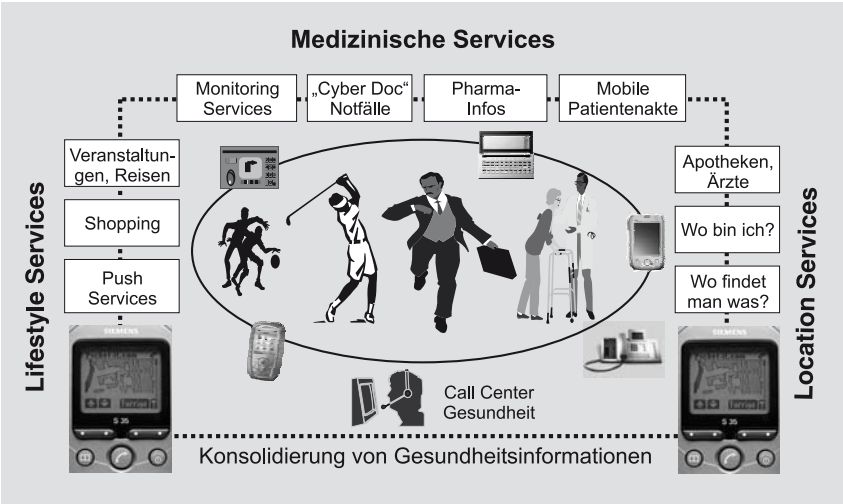


Bild 4.16 Mobile Life Portal

Mobile Werbeaktionen, mobiles Einkaufen, mobile Auktionen und mobile Internet-Portale zeigen die breit gefächerte Welt der mobilen Anwendungen. Auch Kommunen und Regierungen setzen auf mobile Technologien, z. B. beim Einsatz von Streifenwagen der Polizei und bei der Verfolgung von Straftätern.

Es ist nicht Absicht dieses Buchs, die Vielfalt inspirierender neuer Anwendungen im Einzelnen aufzuzeigen. Es sei jedoch auf das Beispiel eines Gesundheits-Portals verwiesen, das verdeutlicht, wie sehr mobile Anwendungen immer mehr auch das persönliche Umfeld und Wohlbefinden der Menschen beeinflussen werden. Bild 4.16 zeigt solch ein Gesundheitsportal.

Das Portal bietet seinen Klienten konsolidierte Gesundheitsinformationen, Lifestyle Services, medizinische Dienste und Location Services, abrufbar über mobile Geräte. Solche Portale werden z. B. von privaten Krankenversicherungen betrieben, die ihren Kunden rund um die Gesundheit zusätzliche Services anbieten. Sie differenzieren sich dadurch im Wettbewerb und binden ihre Kunden langfristig.

Die Palette von personalisierten, konsolidierten Informationen und Services umfasst: Tipps für Patienten, Überwachungsdienste bei chronischen Krankheiten (Diabetes usw.), medizinische Beratung, nicht zu vergessen gesundheitsfördernde Freizeitaktivitäten wie Gymnastik, Wellness, gesunde Ernährung, Einkaufs- und Reiseinformationen usw. sowie Location Services (Wo ist die nächste Apotheke?). Solch nützliche und attraktive Services werden von vielen Portalbesuchern sicherlich gut angenommen.

Das Beispiel eines solchen Portals ist im Internet zu sehen [4.4.1].

4.4.3 Ausblick auf UMTS

Auch wenn *UMTS*-Netze in Europa gerade im Aufbau sind, werden GSM/GPRS-Netze mindestens noch bis 2010 bestehen bleiben. Es soll deshalb nochmals betont werden,

Download times for typical applications
Examples

Application	ISDN	GSM	GPRS	UMTS
e-Mail 10 Kbytes	1 sec	8 sec	0,7 sec	0,04 sec
Web Page 20 Kbytes	2 sec	20 sec	1,6 sec	0,1 sec
PowerPoint 2 Mbytes	4 min	28 min	2 min	7 sec
Video Clip 4 Mbytes	8 min	48 min	4 min	14 sec

Source: UMTS Forum

QoS requirements for application classes
Examples

Application	Data Rate	Delay Time	Reliability FER
Conversational Voice	< 25 Kbit/s	< 150 ms	< 3%
Videophone	< 384 Kbit/s	< 150 ms	< 1%
Voice Messaging	< 13 Kbit/s	< 1 sec	< 3%
Web Browsing	< 50 Kbit/s	< 4 sec/p	< 3%
E-Commerce	< 50 Kbit/s	< 4 sec	0%
Streaming Video	< 384 Kbit/s	< 10 sec	< 1%
Telemetry (Monitoring)	< 25 Kbit/s	< 10 sec	0%

Bild 4.17 UMTS – Quality of Services

dass die vorher beschriebenen m-Business-Lösungen nicht auf UMTS-Netze angewiesen sind. Allerdings werden durch die spezifischen UMTS-Funktionen und -Services existierende Anwendungen teilweise noch attraktiver und neue Marktsegmente werden sich entwickeln.

Verbesserte *Quality of Services (QoS)* werden sicher eine Schlüsselrolle für den Erfolg von UMTS spielen, wobei die erhöhte Bandbreite wohl der entscheidende Faktor für neue Geschäftsmöglichkeiten sein wird.

Wie in Bild 4.17 gezeigt, werden sich Download-Zeiten in UMTS-Netzen erheblich verkürzen. Anwendungsklassen wie Videophonie, Streaming Video oder Multimedia Messaging werden die größere Bandbreite in UMTS-Netzen für eine bessere Qualität nutzen. GSM-Netze erfüllen heute bereits einige QoS-Anforderungen, wie aus der Tabelle hervorgeht. Das Browsen im Web mit einem GSM-Gerät würde allerdings keinen Sinn machen. Mit GPRS könnte das gerade noch als akzeptabel empfunden werden, wohingegen Browsen mit einem UMTS-Gerät eine völlig neue Erfahrung ist. Ähnliche Entwicklungen haben im Feststnetz bereits stattgefunden (vom 9,6-kbit-Modem über ISDN zum DSL-Anschluss).

Das UMTS Forum hat sechs 3G/UMTS-Service-Klassen definiert, die den 3G-Markt inspirieren sollen:

– Mobiler Zugang zu Intranets/Extranets (Business)
– Location-based Services (Konsumenten und Business)
– Rich Voice (Konsumenten und Business)
– Multimedia Messaging Services (Konsumenten)
– Mobiler Zugang zum Internet (Konsumenten)
– Customized Infotainment (Konsumenten).

Aus dem Blickwinkel von Unternehmensanwendungen sind die ersten drei Service-Klassen die wichtigsten. Hierzu einige Erläuterungen:

Mobiler Zugang zu Intranets/Extranets ist heute schon weit verbreitet. Mit UMTS werden sich positive Erfahrungen einstellen und neue Anwendungen werden praktikabel. Browsen mit 144 kbit/s Übertragungsrate macht sicher mehr Spaß, und das Herunterladen einer Powerpoint-Datei oder großer Datenmengen ist dann nicht mehr so frustrierend, dass man darauf von vornherein verzichtet. Die Fähigkeit, Videoclips in brauchbarer Qualität zu übertragen, wird zu innovativen Anwendungen führen. So könnte etwa auf einer Baustelle bei kniffligen Arbeitsgängen Rat von auswärtigen Fachleuten eingeholt werden. Reparaturanweisungen per Video könnten die heutige Anwendungspalette bereichern.

Location-based Services werden heute auch schon in großer Vielfalt von Netzbetreibern angeboten. Mit Ausnahme verbesserter Genauigkeit bei der Ortsbestimmung gibt es aber keine nennenswerten Unterschiede zwischen UMTS- und GPRS-Services. Damit diese Services jedoch weltweit verfügbar werden, ist es notwendig, dass Netzbetreiber erweiterte Roaming-Vereinbarungen vorantreiben. Darüber hinaus hängt der Erfolg von Location-based Services in erster Linie davon ab, dass alle in der Wertschöpfungskette involvierten Partner von diesen Services profitieren. Dabei geht es um komplizierte Business-Modelle, die Netzbetreiber, Anbieter von Inhalten, Aggregatoren von Inhalten, Lösungsanbieter, Serviceanbieter, Unternehmen und Konsumenten einschließen.

Der 3G *Rich Voice* Service ist ein Real-Time-Service, gleichermaßen geeignet für Konsumenten- und Geschäftsanwendungen. Er bietet neben den traditionellen Sprachfunktionen anspruchsvollere Sprachdienste wie gleichzeitige Sprach- und Datenübertragung auf Basis von VoIP (Voice over IP), Netzzugang über Spracheingabe und Web-initiierte Sprachdienste. Sprache wird zu einer wesentlichen Komponente in vielen datenorientierten Services und entwickelt sich zu einem paketorientierten und IP-basierten Service, der neue Anwendungen wie Spracherkennung und durch Sprache aktivierten Zugang zum Intranet ermöglicht.

Mobile Videophonie ist die natürliche Weiterentwicklung heutiger Sprachdienste und attraktive Multimedia-Services werden sich auf lange Sicht mit Sicherheit auch zu nützlichen Anwendungen für Unternehmen entwickeln.

4.5 Zusammenfassung und Empfehlungen

Ausblick

Die Aussichten für m-Business Solutions sind vielversprechend. Laut einer Studie der Boston Consulting Group liegt der bis zum Jahr 2006 zu erwartende Zuwachs an Produktivität in Unternehmen durch mobile Lösungen bei $ 520 Milliarden weltweit. Die jährlichen Produktivitätssteigerungen werden auf 6% geschätzt. Nach dieser Prognose werden Unternehmen $ 340 Milliarden für Entwicklung und Implementierung von m-Business-Lösungen ausgeben. Damit wird ein Mehrwert von $ 180 Milliarden geschaffen. Schlüsselfaktoren für den erfolgreichen Einsatz sind Kosteneinsparungen und -transparenz, verbesserte Prozesse und effektives Management von Unterneh-

menswerten, produktivere Mitarbeiter, verstärkte Kundenbindung und neue Geschäftsmöglichkeiten.

Laut Aussagen von Gartner wird sich die IT weltweit bis 2006 wieder erholt haben. Die meisten Unternehmen werden nicht mehr ausschließlich auf Kosteneinsparung und Gewinnausrichtung Wert legen, sondern ihren strategischen Fokus mehr in Richtung Wachstum und Innovation verlagern.

Das sich ändernde Verhältnis zwischen Arbeit und Freizeit wird enorme Auswirkungen auf das m-Business haben. Mit der Einführung flexibler Arbeitszeiten hat sich das traditionelle Modell der festgelegten Arbeitszeiten in Richtung „Arbeit zu jeder Zeit" geöffnet. Durch die Bildung von Teams, deren Mitglieder an verschiedenen Standorten sitzen, hat sich der herkömmliche, feste Arbeitsplatz gewandelt in Richtung „Arbeit an jedem Ort". In einer Gesellschaft, die rund um die Uhr online vernetzt ist (Connected Society), wird Arbeit immer mehr in virtuellen, temporär zusammenarbeitenden Teams erledigt, die durch entsprechende IT-Systeme vermittelt und unterstützt werden. Gartner geht davon aus, dass sich die „Always-on Society" oder „Connected Society" sehr rasch ausbreiten wird und prognostiziert, dass bis 2007 mehr als 75% der EU- und US-Bürger während 80% ihrer Freizeit die Möglichkeit haben, unmittelbar auf Netz-Services zuzugreifen.

Architektur

Mobile Lösungen sollten auf bewährten, Standard-orientierten Infrastrukturen, einer Multi-Tier-Architektur und einfach integrierbaren Komponenten basieren. Akzeptanz und Anforderungen der Nutzer wie auch die unterschiedlichen Ansprüche der Geschäftsbereiche und IT-Organisationen lassen sich so am besten durch schrittweise Implementierungen erfüllen.

Wiederverwendbare Web Services, integriert in Unternehmensportale, sind ein zielführender Weg, wenn es darum geht, Lösungen unter ökonomischen Gesichtspunkten zu realisieren und gleichzeitig einen hohen Grad an Flexibilität und Agilität zu erreichen. Den neuen Herausforderungen im Wettbewerb kann damit erfolgreich begegnet werden.

Während Portal-Architekturen weiterhin in Unternehmen dominieren, wird sich mittelfristig der direkte Zugriff von intelligenten Clients auf Web Services im Netz (z. B. Travel Services) durchsetzen. Die Fähigkeit der Offline-Verarbeitung von abgerufenen Ergebnissen (z. B. der Eintrag von Flugdaten in Terminkalender und Reiseplan) wird das Spektrum interessanter Client-Anwendungen erheblich erweitern. Allerdings müssen intelligente Clients nicht obligatorisch sein. Zentralisierte Anwendungen mit Browser-Clients sind einfacher zu managen und stellen häufig die bessere Lösung dar.

Strategie

Unternehmen müssen mobile Anwendungen rechtzeitig in ihre IT-Architektur einbauen. Auch wenn eine Experimentierphase zweckmäßig ist, sollten auch die ersten Projekte schon Teil einer längerfristigen strategischen Planung sein und ein kurzfristiges ROI (Return on Investment) erwirtschaften. Deshalb sollte mit unkomplizierten

Szenarien und Anwendungen begonnen werden, die einen schnellen Nutzen erkennen lassen. Die Empfehlung lautet: Keep it simple. Allerdings sind langfristige Auswirkungen auf Infrastruktur, Architektur und strategische Ausrichtung zu beachten.

Insbesondere müssen mobile Anwendungen und Lösungen in eine umfassende Security- und Web-Services-Strategie eingeplant werden. Außerdem sind die Entwicklungen der Service-orientierten Architekturen, des Business-Prozess-Managements und der unternehmensübergreifenden Prozesse zu beobachten und einzubeziehen (Details dazu in Kapitel 5). Unternehmen, die die Auswirkungen von Mobility auf ihre Infrastruktur und Architektur nicht ernst nehmen, vernachlässigen nicht nur einen immer wichtigeren Teil ihres Geschäftes, sondern laufen auch Gefahr, dass ihre Infrastrukturkosten mittelfristig stark ansteigen.

Erfolgsorientierte Unternehmen sollten mobile Lösungen zwar kritisch betrachten, aber bei der Umsetzung auch Phantasie entwickeln und das Nutzenpotenzial dem Aufwand der Implementierung und den zu erwartenden Implikationen bei betroffenen Organisationen und Prozessen gegenüberstellen. In den meisten Fällen wird es sich als richtig erweisen, dass mobile Lösungen in zahlreichen Geschäftsszenarien früher oder später zwingend erforderlich werden.

5 Web Services

Wie schon in Kapitel 3 erläutert, sind IT-Manager in den letzten Jahren verstärkt unter Druck geraten: Um wettbewerbsfähig zu bleiben, müssen Kostenreduzierungen mit notwendigen Innovationen der IT-Infrastruktur und verbesserten Serviceleistungen in Einklang gebracht werden, während gleichzeitig verlangt wird, schnell auf strategische Geschäftsziele zu reagieren.

Zwei wesentliche Ursachen liegen dieser Problemetik zugrunde: die heterogene System- und Anwendungslandschaft sowie die sich rasch ändernden Marktanforderungen.

Die meisten Unternehmen sind nicht in der Lage, ihre IT auf einen einzigen Software-Hersteller zu konzentrieren, da das Angebot weder ausreichend noch flexibel genug ist. Obwohl mehr Kosten verursacht werden, ist ein heterogener Lösungsansatz mit Best-of-Breed-Applikationen häufig die bessere Alternative. Interoperabilität zwischen den Systemen zu schaffen, ist daher der beste Weg, diese Inkonsistenzen zu bewältigen. Dies wird wohl auch neue IT-Investitionen nach sich ziehen.

Die zunehmenden Marktveränderungen sind der zweite Grund. Unternehmen sind gezwungen, sich rasch an den dynamischen Wettbewerb anzupassen und ihre IT muss diesen Veränderungen folgen können.

Wandel ist ein andauernder Prozess in der heutigen IT-Welt:

Weltweit wirkende Ursachen wie Globalisierung und e-Business tragen zur Beschleunigung der Veränderungen bei. Globaler Wettbewerb führt zur Verkürzung von Produkt-Lebenszyklen, da Firmen versuchen, global zu bestehen oder ihre Marktanteile auszuweiten. Schließlich sind es auch die technologischen Weiterentwicklungen, die mit zunehmender Geschwindigkeit neue Kundenbedürfnisse wecken (bestes Beispiel: Handys).

Die IT-Verantwortlichen müssen neue Wege finden, um folgenden Herausforderungen gerecht zu werden:

- Unzureichende Kosteneffizienz, die es schwierig macht, auf die sich laufend ändernden Kundenanforderungen reagieren zu können
- kostenintensive, unflexible Integrationstechnologien, die nicht tolerierbare Risiken mit sich bringen
- monolithische Applikationen, die hohe Kosten bei der Anpassung an Kundenanforderungen und bei der Wartung verursachen
- Abhängigkeit von Software-Herstellern

– nicht ausreichende Sicherheit bei komplexen, automatisierten firmenübergreifenden Geschäftsprozessen
– fehlende Transparenz und unzureichende Steuerungsmöglichkeit der Geschäftsbereiche bei automatisierten Prozessen
– wegen der Komplexität und noch unzureichender Sicherheits-Infrastruktur begrenzte Möglichkeiten, Nutzen aus Mehrwert-Netzen (Value Networks) zu ziehen.

Um auf diese vielfältigen und durchaus ernst zu nehmenden Herausforderungen schlüssige Antworten zu finden, sind die IT-Organisationen mehr denn je gefordert.

In dieser schwierigen Situation ist ein evolutionärer, Standard-basierter Architektur-Ansatz hoch willkommen, wenn er eine geeignete Basis liefert, um die erwähnten Problemfelder in den Griff zu bekommen. Dieser Ansatz basiert auf Web Services und ist als Service-orientierte Architektur (SOA) bekannt.

5.1 Web-Services-Paradigma – SOA

Das Web-Services-Paradigma beruht auf einer Service-orientierten Architektur, die eine Umgebung für verteilte Verarbeitung darstellt. In dieser Architektur rufen Anwendungen in lose gekoppelter Weise Funktionen aus anderen Anwendungen auf, entweder lokal, über ein internes Netzwerk oder über ein externes IP-Netz.

Unter Web Services versteht man sich selbst beschreibende, modulare und autonome Anwendungskomponenten. Diese können innerhalb einer Firma sozusagen als effiziente Methode der verteilten Verarbeitung angewendet oder im Internet publiziert und dort aufrufbar lokalisiert werden. Im Web publizierte Web Services (Software als Services) können von beliebigen Anwendungen jederzeit aufgerufen und genutzt werden.

Mit Web Services wird das Ziel einer Application-to-Application-Kommunikation verfolgt. Dieses Ziel wird durch eine Dokumenten-orientierte Methode der verteilten Verarbeitung erreicht.

Die wesentlichen Elemente von Web Services lassen sich folgendermaßen zusammenfassen:

– Der *Service* ist durch eine Software repräsentiert, die ein XML-Dokument verstehen und verarbeiten kann, das sie von einer aufrufenden Anwendung über ein internes Interface oder ein IP-Netz empfangen hat. Die interne Struktur dieser Software sowie die Realisierung der angeforderten Funktion spielen dabei keine Rolle. Ob es sich also um eine Objekt-orientierte Technik oder um eine eigenständige Anwendung oder um eine als Web Service verpackte Legacy-Anwendung handelt, ist ohne Bedeutung. Diese Software muss lediglich in der Lage sein, spezifizierte XML-Dokumente zu verarbeiten und Funktionen auszuführen, die durch diese Dokumente angefordert werden.

– Das *XML-Dokument* ist das Kernstück eines Web Service. Es enthält alle anwendungsspezifischen Angaben und ist als XML-Schema beschrieben. Die beiden involvierten Anwendungen müssen Kenntnis über dieses Schema haben, um das Dokument korrekt bewerten und interpretieren zu können. Als Beschreibungssprache des Web Service wird die *Web Services Description Language (WSDL)* verwendet.
– Die *Adresse* gibt an, wo der Service aufzufinden ist, d.h. sie besteht aus einem Transport-Protokoll, kombiniert mit einer Netzwerk-Adresse.
– Das *Envelope* umschließt das XML-Dokument und enthält zusätzliche Systeminformationen, welche die beiden kommunizierenden Anwendungen austauschen möchten. Das können z. B. Routing- oder Security-Informationen sein. Solche Informationen können angefügt werden, ohne dass das XML-Dokument selbst verändert werden muss. SOAP (Simple Object Access Protocol) ist das Message-Protokoll, das in den meisten Fällen für Web Services Verwendung findet. Es besteht in der Regel aus zwei Elementen: dem SOAP-Header, der die erwähnten Systeminformationen enthält, und dem SOAP-Body, der das XML-Dokument darstellt.

Service-orientierte Architekturen

SOA beschreibt eine Architektur, die im Prinzip schon seit einigen Jahren Anwendung findet. Ein Beispiel dafür ist *CORBA (Common Object Request Broker Architecture)*, promotet von der Object Management Group und seit vielen Jahren insbesondere in der Telekommunikationsbranche angewendet. Ein weiteres Beispiel ist *DCOM (Distributed Component Object Model)*, das entsprechende Konzept von Microsoft. Beide Konzepte beruhen auf Interface Definition Languages (IDL, MIDL) und eng gekoppelten (*tightly coupled*) Mechanismen.

Als Prinzip ermöglicht SOA das Design von Services, die über publizierte Interfaces als eigenständige Funktionalität anderen Anwendungen zur Verfügung stehen. In diesem Sinne kann SOA als eine Anwendungsarchitektur bezeichnet werden, in der alle Funktionen als unabhängige Services mit wohldefinierten, aufrufbaren Interfaces realisiert sind. In einer Sequenz aufgerufen, können diese Services Prozessabläufe darstellen.

Im Gegensatz zu CORBA und DCOM verkörpert SOA auf Basis von Web Services jedoch ein lose gekoppeltes (*loosely coupled*) Modell, wie in Bild 5.1 dargestellt, wobei es sowohl Unabhängigkeit von der Anwendungsplattform (bezüglich der beiden Lager Java und Microsoft) und von der Programmiersprache als auch von Transport- und Message-Formaten einschließt.

Außerdem lässt es das Web-Services/SOA-Modell zu, unter Nutzung des http-Protokolls Firewalls zu passieren. Der Service kann elektronisch an einem Ort im Netz aufgerufen werden, der zunächst der aufrufenden Anwendung nicht bekannt ist und automatisch ermittelt werden kann.

SOA auf Basis von Web Services ist durch die Fähigkeit charakterisiert, Services im IP-Netz in einer entsprechenden Registry bekannt zu machen (Publishing). Das Netz kann entweder ein Unternehmensnetz oder das Internet sein. Die Registry ist standardi-

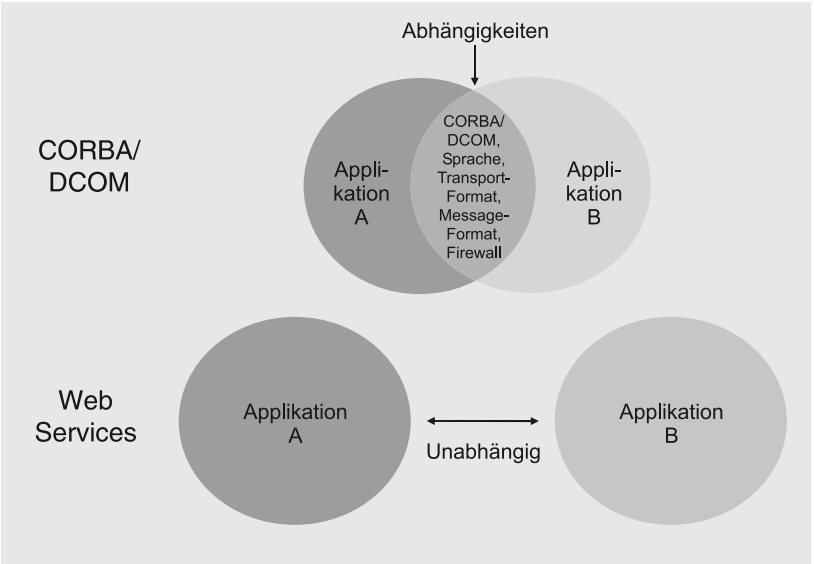


Bild 5.1 Unabhängigkeit von Plattformen

siert, hat die Bezeichnung *UDDI (Universal Description, Discovery and Integration)* und kann ebenfalls unternehmensspezifisch oder im Internet platziert sein.

UDDI besteht aus einem XML-Schema, das vier Datenstrukturen definiert: Geschäftszweig, Service-Kategorie, Definitionen bezüglich der Einbindung des Service sowie Programm-Interfaces als auch operative Interfaces für die genannten Strukturen.

Web Services werden durch die standardisierte Sprache WSDL beschrieben. Das im UDDI vorhandene WSDL Listing besteht aus drei Elementen: Die White Pages enthalten grundsätzliche Informationen über das Unternehmen und seine Dienste, die Yellow Pages, nach Branchen geordnet, beschreiben Service-Typ oder Geographie. Schließlich geben die Green Pages Auskunft über den technischen Inhalt und die Location, wo der Service zu finden ist (z. B. URL) und wie er ausgeführt werden kann.

Neben dem Publishing weist SOA zwei weitere Basis-Funktionalitäten auf, die von Anwendungen zur Ablaufzeit (Runtime) genutzt werden können: die Fähigkeit, eine gesuchte Funktion (Service) im Netz zu finden (*Discovery*), sowie die Fähigkeit, diesen Service automatisiert aufzurufen und in Anspruch zu nehmen (*Binding*).

Wie in Bild 5.2 dargestellt, korrespondieren diese Fähigkeiten mit drei unterschiedlichen Rollen: Web Service Provider (*Publishing*), Web Service Broker (*Discovery*), Web Service Requester.

Ist ein Web Service in die *UDDI Registry* eingetragen worden (P im Diagramm), kann er von beliebigen Anwendungen (Requester) über das Netz aufgerufen werden. In der Regel läuft das in drei Schritten ab: Zunächst sucht der Web Service Requester in der UDDI Registry nach der gewünschten Funktion (1). Hat er sie gefunden, konnektiert er den entsprechenden *Web Service Provide*r mittels SOAP, um den Web Service zu akti-

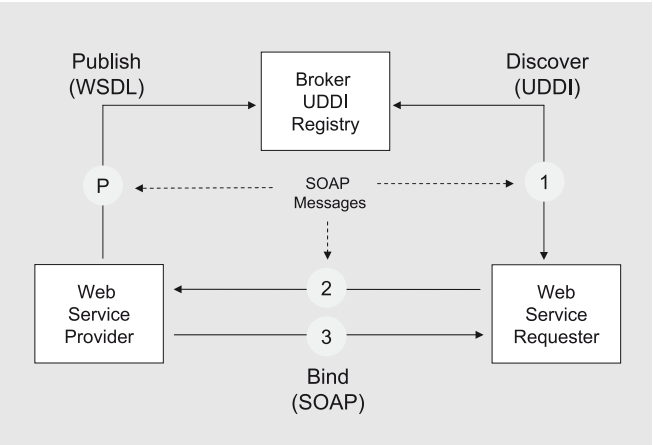


Bild 5.2 Web-Services-basierte Service-orientierte Architektur

vieren (2). Nach der Ausführung liefert der Web Service das Ergebnis – ebenfalls mittels SOAP – an den *Web Service Requester* zurück (3).

Nutzen und Grenzen von SOA

Nutzen

Bemerkenswert ist die Tatsache, dass alle wesentlichen Software-Hersteller die Web-Services-Technologie unterstützen. Nicht zuletzt geschieht dies aufgrund überzeugender Vorteile, z. B.:

- Flexibilität beim Design neuer Software
- Wiederverwendbarkeit von Komponenten im Netz
- Fähigkeit zur Interoperabilität und Integration
- einfache Erstellung neuer Geschäftsprozesse.

Jüngste Entwicklungen in der Software-Industrie haben dazu beigetragen, die SOA zu forcieren. Zunehmend werden Lösungen erforderlich, die auf wiederverwendbaren Anwendungskomponenten basieren. Im Besonderen trifft dies zu bei personalisierten Portal-Anwendungen, die darüber hinaus vielfältige Kanäle zu den Anwendern bedienen.

Unterschiedliche Anwendergruppen wie Kunden, Angestellte oder Manager verwenden mehrere Geräte (Laptops, PDAs, Smartphones) in den verschiedensten Business-Situationen (Büro, Hotel, Zuhause). In all diesen Fällen wird Zugang zu den gängigen Geschäftsanwendungen gefordert. SOA mit seinen lose gekoppelten Mechanismen bereitet die natürliche Basis für eine Vielfachverwendbarkeit solcher Anwendungen. Deshalb wird durch den Übergang zu Multi-Client- und Multi-Channel-Lösungen ein Software-Design auf der Grundlage von Web Services besonders interessant.

Zweifellos werden durch SOA Wettbewerb und Innovation in der Anwendungsentwicklung angekurbelt. *Best-of-breed*-Komponenten können als autonome Web Services ins Netz gestellt und im UDDI registriert werden und sind damit als wiederverwendbare Services weltweit zugänglich. Dabei ergeben sich nicht nur für innovative Software-Startups beste Geschäftsmöglichkeiten; auch die etablierten Software-Firmen werden ihre Anwendungspakete modularisieren und Komponenten als Web Services über das Internet einem größeren Kundenkreis zur Verfügung stellen.

Vermehrt fordern Kunden eine verbesserte Interoperabilität zwischen den Anwendungsplattformen verschiedener Hersteller, z. B. IBM, Microsoft und SAP. Dies betrifft auch die Integration aufsetzender Anwendungen und firmeneigener Entwicklungen. Mit viel Aufwand wurden in der Vergangenheit in zahlreichen Projekten spezifische APIs geschaffen, um Legacy-Systeme und andere existierende Programme in komplexe Transaktionen einbinden zu können. SOA bietet vom Ansatz her die passenden Mechanismen für die Komposition und Integration von existierenden und neuen Echtzeit-Transaktionsmustern.

Evolution von IT-Anwendungsarchitekturen

Die Möglichkeit, Ad-hoc-Prozesse einfach zu erstellen, sowie die Repräsentation einer für die Prozessintegration geeigneten Technologie sind wahrscheinlich die meistgewünschten positiven Eigenschaften von SOA. Wie in Bild 5.3 gezeigt, wird dies zu einer weiteren Aufsplittung der Anwendungsschichten führen.

Das alte monolithische Anwendungsparadigma, gekennzeichnet durch unflexible und unstrukturierte Programme, die mittels Programmiersprachen der 3. und 4. Generation erstellt wurden, auf Mainframe-Systemen abliefen und textorientierte Alpha-Terminals unterstützten, wurde Ende der Achtzigerjahre durch eine Client/Server-Architektur abgelöst.

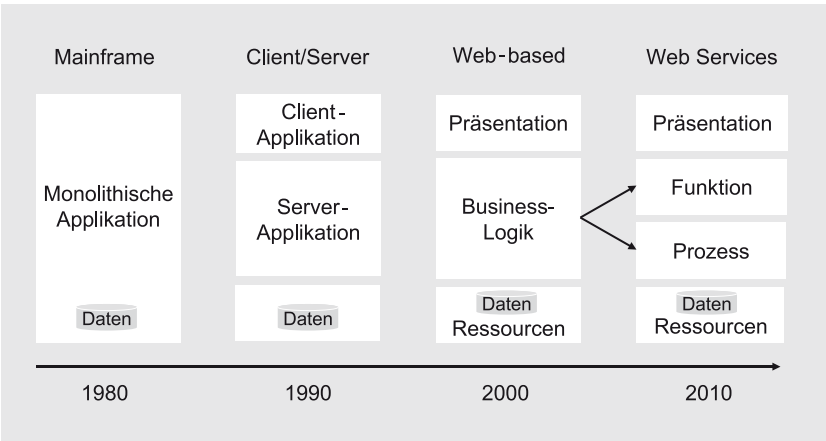


Bild 5.3 Evolution von IT-Anwendungsarchitekturen

Wie schon in Kapitel 2 dargestellt, hat sich 10 Jahre später, aufgrund tiefgreifender technologischer Entwicklungen und geschäftsrelevanter Veränderungen, ein weiterer Paradigmenwechsel vollzogen: der Übergang zu Web-basierten e-Business-Lösungen. Die Evolution des Internet war hier sicherlich das treibende Moment, das schließlich zu der heute typischen Multi-Tier-Architektur führte. Sie besteht aus der Präsentationsschicht, die überwiegend Browser-Clients unterstützt, der Geschäftslogik-Schicht, welche die zentralen, funktionalen und prozeduralen Abläufe repräsentiert, und der Ressourcen-Schicht, die typischerweise Datenbanken, Web-Inhalte, Legacy-Systeme und weitere unternehmensweite Services umfasst.

Nun steht die Entwicklung durch SOA auf der Grundlage von Web Services an der Schwelle zu einer weiteren Veränderung bezüglich Architektur, Design und Zusammenspiel von Geschäftslösungen: einer Aufsplittung der Geschäftslogik in Funktionen und Prozessabläufe.

In diesem Paradigma können Geschäftsabläufe und Aktivitäten sehr effizient durch eine Komposition von koordinierten Web Services dargestellt werden, welche die unterschiedlichen Funktionen repräsentieren. Der lose gekoppelte Mechanismus von SOA in Kombination mit der neuen Business Execution Language (BPEL, Details später) und Workflow Engines, die in der Lage sind, definierte Prozessschritte abzuarbeiten, ermöglichen das schnelle Aufsetzen von Ad-hoc-Prozessen. Dabei können bereits existierende Anwendungen mit neuen Web Services integriert werden.

Dieses Paradigma, das auch als *zweistufiges Programmiermodell* (getrennt in Funktion und Prozess) bezeichnet werden kann, hat allerdings erhebliche Auswirkungen sowohl auf die Design-Phase als auch auf die operative Phase. In der Design-Phase ergeben sich durch die Komposition von Web Services eine Reihe von neuen Herausforderungen: Definition einer geeigneten Gesamtarchitektur der Lösung, Koordination von Web Services untereinander und Handhabung von Transaktionen, die mehrere Web Services einschließen. In der operativen Phase von Web Services sind ebenfalls erhebliche Auswirkungen zu beachten, z. B. Quality of Services, Security, Service Level Agreements und Prozess-Management.

Grenzen und offene Themen

SOA sollte nicht als Allheilmittel für alle existierenden Problemkreise in heutigen heterogenen IT-Architekturen angesehen werden und es wird sicher auch nicht allen zukünftigen Herausforderungen gerecht.

So stellt SOA im Falle von lang andauernden asynchronen Prozessen wohl nicht den besten Ansatz dar. SOAs natürliche Stärken liegen trotz der losen Kopplung eher im automatisierten Real-Time-Nachrichtenaustausch (Request-Response) als in solchen Vorgängen, die häufig durch eintretende Ereignisse gesteuert werden (Event-driven).

SOA erfordert eine entsprechende Ablaufumgebung, d.h. in der Regel einen State-of-the-Art Application Server, wie etwa einen Microsoft .Net Server, SAP Netweaver, IBM WebSphere oder BEA Web Logic. Leider ist derzeit noch keine vollständige Plattform-Unabhängigkeit bezüglich Tools und Ablaufumgebung gegeben.

Business-Komponenten, die ausschließlich in geschlossener Umgebung verwendet werden und deren Wiederverwendung nicht in Betracht kommt, können von SOA nicht profitieren, da zusätzliche Design- und Entwicklungsaufwände anfallen würden.

Das größte Problem von SOA und Web Services stellen heute jedoch die noch nicht ausreichend gelösten Sicherheitsprobleme dar. Es wurde zwar mittlerweile ein mehr oder weniger umfangreiches, aber noch keineswegs vollständiges Rahmenwerk von Security-Spezifikationen erarbeitet. Eine Reihe von anwendbaren Produkten ist schon verfügbar. Jedoch sind die Security-Maßnahmen für geschäftskritische Vorgänge, die externe Web Services über das Internet einschließen, in den meisten Fällen noch nicht ausreichend. Weitere Details werden in Kapitel 6 behandelt.

Ebenfalls kritisch bei Lösungen, die auf Web Services basieren, ist die Handhabung von Transaktionen bei aufeinanderfolgenden Request-Response-Abläufen. In den meisten Fällen können existierende Applikationen, die als Web Services in eine Transaktion eingebunden (Wrapping) werden, nicht den Status einer *ACID (Atomicy, Consistency, Isolation, Durability) Transaction* erfüllen. Sogenannte *Extended Transactions* werden deshalb schon in der Designphase sehr wichtig. Dabei wird definiert, unter welchen Randbedingungen eine nicht ACID-fähige Transaktion akzeptabel gehandhabt werden kann. Beispielsweise könnte eine lang andauernde Transaktion umstrukturiert werden und durch eine Reihe von kurzen, unabhängigen Transaktionen ersetzt werden.

Ein weiterer kritischer Aspekt bei Lösungen mit Web Services ist das koordinierte Zusammenspiel von Web Services untereinander und mit existierenden Anwendungen, insbesondere dann, wenn komplexere Funktionen durch aggregierte Web Services abgebildet werden. Geschäftsprozesse setzen sich üblicherweise aus vielfältigen koordinierten Aktivitäten zusammen, bei denen Kontext, Abhängigkeiten und Vorfälle zu berücksichtigen sind. Dazu wird ein Koordinierungswerkzeug mit entsprechenden Protokollen benötigt, das diese Anforderungen adressieren kann.

Abschließend sind einige Problemfelder zu erwähnen, die bei geschäftskritischen Anwendungen eine besondere Rolle spielen, nämlich die Vertrauenswürdigkeit (Trust) eines Web Service Providers, die garantierte Zuverlässigkeit und Qualität eines angebotenen Dienstes und auch, inwieweit sich vertragliche Bedingungen ausreichend flexibel verhandeln lassen.

Zusammenfassung

Der Nutzen von SOA/Web Services wird längerfristig deutlich werden. SOA/Web Services

- beruhen auf offenen Standards und können uneingeschränkt jede Software-Komponente als aufrufbaren Service darstellen, egal ob Legacy-Anwendung, Standard-Software oder J2EE-Komponente,
- ermöglichen es, individuelle Software als eigenständige Lösungskomponente in vielen Lösungen einzusetzen,

– bieten Entwicklern eine standardisierte Möglichkeit, Software-Komponenten einzubinden und zusammenzustellen ohne sich mit komplizierten und spezifischen APIs auseinandersetzen zu müssen,
– tragen zur Reduzierung von Komplexität, Kosten und Risiken mit einem einfachem Architekturmodell bei, auf dessen Basis sich gleichermaßen Anwendungen erstellen, betreiben und managen lassen.

Zusammenfassend ist festzustellen, dass SOA vielfältig nutzbringend angewendet werden kann und Bestandteil zukunftsweisender Lösungsprojekte sein sollte. Fehlende SOA-Erfahrung kann sich als mangelnde Wettbewerbsfähigkeit auswirken. Unternehmen müssen die Bedeutung von SOA und Web Services verstehen und Stärken und Grenzen richtig einordnen, damit sie diese Technologie in einer modernen Anwendungs- und Lösungsarchitektur richtig positionieren können.

5.2 Web-Services-Standardisierung

Die Web-Services-Standards und Standard-Vorschläge lassen sich strukturieren, wie in Bild 5.4 dargestellt. Standards und Protokolle können in drei Struktur-Blöcke unterteilt werden: *Description/Discovery Standards*, *Infrastructure und Deployment Standards und Protokolle* für die Anwendung von Web Services sowie das *Web Services Implementation Framework*. Zur besseren Übersichtlichkeit sind die Infrastructure und Deployment Standards und Protokolle nochmals in die Schichten *Transport, Messaging, Quality of Services* und *Processes/Composition* unterteilt.

Die Basis-Standards für das Erstellen und Anwenden von Web Services werden bereits seit einigen Jahren genutzt. Dazu gehören SOAP, das erweiterbare XML-basierte Protokoll zum Informationsaustausch in verteilten, heterogenen Umgebungen, WSDL zur Beschreibung des Web Services und UDDI für die Registrierung von Web Services. Die darunterliegenden Transport-Protokolle TCP/IP und HTTP sowie XML selbst können ebenfalls dazu gezählt werden.

Eine Reihe von erweiterten Standards und Services (*Extended Services*) ist jedoch erforderlich, wenn die Vision eines *Business Web* Wirklichkeit werden soll. In diesem Szenario werden Web Services als Anwendungskomponenten genutzt und dynamisch zu neuen Geschäftsprozessen kombiniert. Um das zu verwirklichen, werden Dienste, Protokolle und Sprachen benötigt, welche die höchsten Qualitätsansprüche für Transport, Messaging, Security und Transaktionsverarbeitung sicherstellen können. Des Weiteren sind Standards für Monitoring, Accounting, Collaboration und Orchestration von Bedeutung. All diese Standards sind für einen zuverlässigen, sicheren, nachhaltigen und koordinierten Betrieb von Lösungen auf Basis von Web Services essentiell.

Diese Extended Services wurden überwiegend von den bekannten Software-Herstellern spezifiziert und prototypisch implementiert, allen voran IBM und Microsoft. Standardisierungsorganisationen wie OASIS (Organization for the Advancement of Structured Information Standards) und das W3C (World Wide Web Consortium) haben diese Spezifikationen schon weitergeführt und entsprechende Standards verabschiedet bzw.

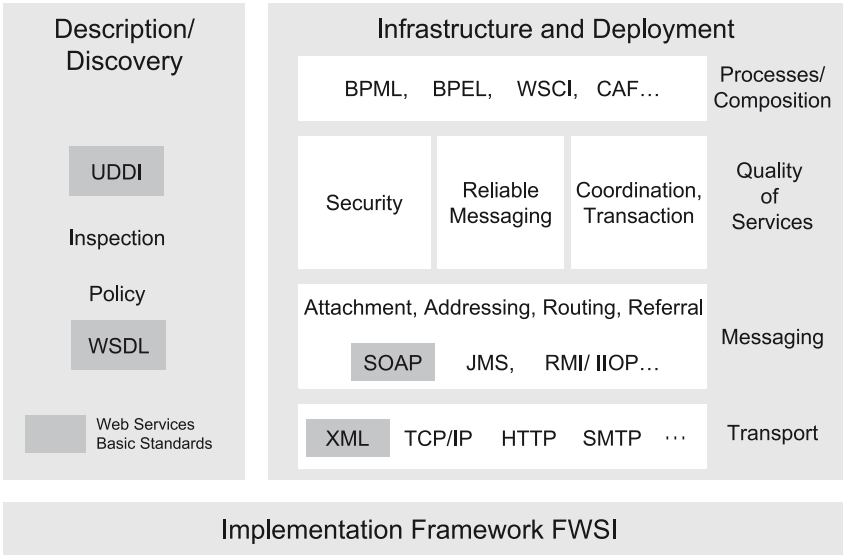


Bild 5.4 Web-Services-Standards

sind gerade dabei, dies zu tun; gleichzeitig greifen sie weitere relevante Standardisierungsthemen auf.

Global XML Web Services Architecture

Ein wesentlicher Beitrag zur Standardisierung war die Spezifikation *Global XML Web Services Architecture (GXA),* die Ende 2001 von Microsoft vorgestellt wurde [5.2.1]. Die Spezifikation wurde in den Folgejahren unter Mitwirkung anderer Hersteller erweitert und mittlerweile sind konkrete Standards und Protokolle verabschiedet worden.

Laut Microsoft basiert GXA auf vier Design-Prinzipien:

- Modular
  GXA nutzt die Erweiterbarkeit der SOAP-Spezifikation mittels zusammensetzbarer Module, die End-to-End-Funktionalitäten ermöglichen. Für den Fall, dass neue Funktionen erforderlich werden, lassen sich weitere Module festlegen.
- General Purpose
  GXA ist für einen breiten Einsatz von XML Web Services konzipiert. Dies schließt B2B, B2C und EAI bis hin zu P2P(Peer-to-Peer)-Lösungen ein.
- Federated
  GXA basiert auf verteilter Verarbeitung und unterstützt organisationsübergreifende Anwendungen ebenso wie grenzüberschreitende Vertrauensbereiche (Trust Boundaries), und zwar ohne dass zentrale Services und Administration erforderlich sind.
- Standards-based
  GXA-Protokolle sollen Standardisierungsgremien übergeben werden und Microsoft will mit Interessenten zusammenarbeiten, um Standards zu vervollständigen.

Web Services Interoperability Organization (WS-I)

Microsoft und IBM haben 2002 die *Web Services Interoperability Organization (WS-I)* [5.2.2] mit dem Ziel gegründet, die Interoperabilität von Web-Services-Implementierungen verschiedener Hersteller sicherzustellen. Aufgabe der WS-I-Organisation ist es, die unterschiedlichen Ansätze zu koordinieren und in Einklang zu bringen. WS-I stellt Leitlinien, Beispiellösungen, Tools und Testumgebungen zur Verfügung, damit Web Services unabhängig von Plattformen und Herstellern fehlerfrei untereinander kommunizieren können. WS-I erstellt Basisprofile, die Leitlinien und Empfehlungen zur Implementierung interoperabler Web Sevices unter Nutzung der Basis-Technologien und -Protokolle (SOAP, WSDL, UDDI, XML und XML Scheme Definition, XSD) enthalten.

Standards und Spezifikationen

Die Standardisierung von Web Services ist ein fortwährender Prozess. Der aktuelle Informationsstand kann im Web recherchiert werden [z. B. 5.2.3]. Einige wichtige Web-Services(WS)-Standards bzw. vorgeschlagene Spezifikationen sollen hier aber erläutert werden:

WS-Inspection

Die *WS-Inspection* spezifiziert ein XML-Format zur Inspektion einer Website über verfügbare Services und regelt, wie inspektionsbezogene Informationen verfügbar gemacht werden sollen. Ein WS-Inspection Document enthält aggregierte Referenzen zu bereits bestehenden Service-Beschreibungen, die in beliebigen Formaten ausgeführt sein können. Inspection Documents sind dort zu finden, wo der Service angeboten wird oder über eine Referenz zugänglich ist.

WS-PolicyFramework

Das *WS-PolicyFramework* definiert ein allgemein gültiges Modell einschließlich entsprechender Syntax zur Beschreibung und Kommunikation von Web Services Policies. Durch Policies werden Angaben/Informationen festgelegt, die erforderlich sind, um den Service nutzen zu können.

WS-Attachments

Die Spezifikation *WS-Attachment* definiert ein abstraktes Modell für SOAP-Anhänge (Attachments) und einen Mechanismus zur Verkapselung von SOAP Message samt Anhang in einer *DIME Message (Direct Internet Message Encapsulation)*. In vielen Anwendungsszenarien macht es keinen Sinn, XML-codierte Daten an einen Web Service zu senden (z. B. Bilder oder Grafiken). DIME spezifiziert, wie Anhänge gepackt, WS-Attachments definiert und DIME-codierte Anhänge im SOAP-Protokoll behandelt werden.

WS-Addressing

WS-Addressing spezifiziert einen Transport-neutralen Mechanismus zur Adressierung von Web Services und Messages. Insbesondere definiert diese Spezifikation XML-Elemente zur Identifikation von Web-Service-Endpunkten sowie eine sichere End-to-End-Identifikation. Es wird festgelegt, wie Messaging-Systeme die Nachrichtenübertragung über Netze, Netzknoten und andere Netzkomponenten wie Firewalls und Gateways in Transport-neutraler Art und Weise unterstützen.

WS-Routing

WS-Routing ist erforderlich, um Messages über einen dynamisch konfigurierten Netzpfad zu leiten. Ein alternativer Rückwärtspfad und beliebige Zwischenstationen können spezifiziert werden. Das Modell schließt eine direkte Identifikation der Zwischenstationen ein und unterstützt, dass bestimmte Services auf ausgewählten Zwischenstationen ausgeführt werden können.

WS-Referral

WS-Referral erweitert das WS-Routing-Konzept. Es wird für die Verwaltung der Routing-Verzeichnisse benötigt, die auf den Zwischenstationen gespeichert sind. Der Grund dafür ist, dass die Web-Services-Kommunikation (Austausch von Requests und Responses) in den seltensten Fällen direkt zwischen zwei benachbarten Rechnerknoten erfolgt. Meistens erstreckt sich der Kommunikationspfad je nach Netztopologie über viele Zwischenstationen.

WS-Security

WS-Security beschreibt SOAP-Erweiterungen, um die Integrität, Vertraulichkeit und Authentifikation von Nachrichten zu gewährleisten. Des Weiteren ist die Handhabung von Security Tokens definiert. Eine ausführliche Behandlung dieses Themas ist in Kapitel 6 enthalten.

WS-ReliableMessaging

Die Spezifikation *WS-ReliableMessaging* beschreibt ein Protokoll, das einen zuverlässigen Nachrichtenaustausch zwischen verteilten Anwendungen erlaubt, auch wenn Fehler in der Software, im System oder im Netz auftreten. Das Protokoll ist unabhängig von unterschiedlichen Netzwerk-Transport-Technologien konzipiert.

WS-Coordination

Die Spezifikation *WS-Coordination* beschreibt ein Framework für Protokolle, die für die Koordinierung von Aktionen in verteilten Anwendungen erforderlich sind. Insbesondere geht es um die Gewährleistung von konsistenten Transaktionen. Das Framework erlaubt es, Kontexte zwischen Services herzustellen, indem Meldungen ausgetauscht werden. Das Framework ermöglicht zudem, existierende Prozessabläufe, Workflows und Systeme trotz proprietärer Protokolle in ein heterogenes Umfeld einzu-

binden. Ferner definiert die Spezifikation eine Kontext-Struktur und beschreibt die Rahmenbedingungen für das Propagieren von Kontext zwischen kooperierenden Services.

WS-Transaction

WS-Transaction und *WS-Coordination* wurden gemeinsam spezifiziert. WS-Transaction garantiert einen konsistenten Zustand über alle beteiligten Prozesse und Daten zu jedem beliebigen Zeitpunkt. WS-Transaction unterscheidet zwei Fälle: *Atomic Transaction* und *Business Activity*. Eine Atomic Transaction ist eine Transaktion mit sehr kurzer Laufzeit innerhalb einer Domäne. Bei Business Activity geht es um unternehmensübergreifende Geschäftsprozesse, die asynchron über einen längeren Zeitraum abgewickelt werden (Long-Living Transactions).

BPML, BPEL, WSCI, WS-CAF

Das große Interesse der Software-Hersteller bei der Durchsetzung ihrer Web-Services-Technologien wird am Beispiel der Spezifikationen für firmenübergreifende Geschäftsprozesse deutlich. Zu diesem Thema konkurrieren mehrere Vorschläge mit teils unterschiedlichem Fokus.

Die *Business Process Modelling Language (BPML)* wurde im Sommer 2002 von der Business Process Management Initiative veröffentlicht. Diese Initiative umfasst mehr als ein Dutzend namhafter Hersteller, darunter auch BEA, CSC, HP, IBM, SAP und Sun. Mit BPML können die Geschäftsprozesse eines Unternehmens über alle Ebenen hinweg modelliert werden. Jede einzelne Aktion kann definiert werden; das gilt auch für komplexe, unternehmensübergreifende Geschäftsprozesse. Diese werden als grafische Objekte dargestellt, die über eine einfache Bedienoberfläche verändert oder mit anderen Prozessen verknüpft werden können.

BEA, SAP und Sun haben eine XML-basierende Spezifikation entwickelt, mit der sich ebenfalls Geschäftsprozesse definieren lassen. Das *Web Services Choreography Interface (WSCI)* beschreibt dabei dynamische Schnittstellen für Web Services, über die sich Daten unter Anwendung von statischen Business-Regeln austauschen lassen.

Microsoft wiederum hat seine eigene Business Process Language *XLANG* entwickelt. Sie findet im BizTalk Integration und Orchestration Server Anwendung. Auch IBM hat eine entsprechende Prozesssprache entwickelt: die *Web Services Flow Language (WSFL)*.

IBM und Microsoft sind einen Schritt weiter gegangen und haben auf der Basis ihrer Entwicklungen (WSFL und XLANG) gemeinsam mit BEA die drei komplementären Spezifikationen *WS-Coordination*, *WS-Transaction* und *Business Process Execution Language für Web Services (BPEL4WS kurz: BPEL)* entwickelt, um den Workflow zwischen Service-basierten Geschäftsprozessen zu regeln. Damit ist die Erstellung von kaskadierbaren Web Services möglich, über die sich beispielsweise Flüge, Mietwagen und Hotelzimmer buchen lassen. Falls der Flug ausgebucht ist, werden automatisch die Hotelreservierung und der Mietwagen mit Hilfe einer Kompensationstransaktion storniert und der Benutzer wird darüber informiert.

In der Zwischenzeit haben fast alle wesentlichen Software-Hersteller angekündigt, BPEL zu unterstützen, auch Microsoft wird eine Migration von XLANG nach BPEL anbieten. Aus diesen Gründen dürfte BPEL die besten Chancen haben, der Standard für firmenübergreifende Prozessdefinitionen zu werden.

WS-CAF

Das Ziel dieses kürzlich von OASIS initiierten Technical Committee *Web Services Composite Application Framework (WS-CAF)* [5.2.4] ist die Spezifikation eines lizenzfreien, generischen und offenen Frameworks, das Anwendungen unterstützen soll, die aus mehreren in Kombination genutzten Web Services bestehen (Composite Applications).

Framework für die Implementierung von Web Services

OASIS-Mitglieder haben ein weiteres Technical Committee *Framework for Web Services Implementation (FWSI)* [5.2.5] ins Leben gerufen. Es erstellt Leitlinien, die es Systemintegratoren und Software-Herstellern erleichtern, Lösungen auf Basis von Web Services einfach zu implementieren.

Das Ziel ist insbesondere die Realisierung von robusten Web Services unter Verwendung einer praktikablen und gründlichen Methodik. Es wird Implementierungsprozesse und gemeinsame Funktionen enthalten, die von Unternehmen adaptiert werden können, um qualitativ hochwertige Web-Service-Lösungen zu konstruieren, ohne diese Funktionalitäten jeweils neu entwickeln zu müssen. Damit soll eine zu langsame Adaption von Web Services vermieden werden, die wegen fehlender Methodik und unzulänglicher Kenntnisse über die Zuverlässigkeit von Komponenten zu erwarten ist.

Standardization Outlook

Alle wichtigen Software-Hersteller und Standardisierungs-Organisationen zeigen schon lange großes Interesse und arbeiten kooperativ bei der Entwicklung von Standards zusammen. Sie sind sich bewusst, dass eine breite Akzeptanz nur erreicht werden kann, wenn die Interoperabilität von Web Services gewährleistet ist.

Allerdings ist die Standardisierung ein laufender und langwieriger Prozess mit ständigen Ergänzungen und neuen Versionen. Zusätzliche Aktionsfelder mit weiteren Standardisierungsbemühungen sind noch zu erwarten. Beispiele hierfür sind: Web Services Security, Policy, Provisioning, Long-running Transactions, Federation, Composition, Orchestration und Management.

Einige der von Herstellern eingebrachten Vorschläge wurden (noch) nicht von Standardisierungsgremien verabschiedet (z. B. Security). Leider haben manche Mitspieler unterschiedliche Geschäftsinteressen, so dass überlappende oder nicht kompatible Spezifikationen Interoperabilität und einheitliche Anwendbarkeit verhindern.

5.3 Auswirkungen durch Web Services

Web Services haben das Potenzial, den nächsten evolutionären Schritt des Internet einzuleiten: das *Business Web*. Der größte Nutzen wird mit der durchgängigen Kommunikation zwischen Unternehmen (B2B) entstehen. Dies ermöglicht die Realisierung komplexer, dynamischer, firmenübergreifender Prozessabläufe. Damit lassen sich Auftrags-, Liefer- und Zahlungsverkehrs-Transaktionen vollständig automatisieren. Dank einfacher Implementierung und breit akzeptierter Standards können mit Web Services auch kleine und mittlere Firmen am e-Business teilhaben. Wenn man von Security absieht, sind keine komplizierten, neuen Infrastrukturen und Vernetzungen vorzusehen. Wie in Bild 5.5 dargestellt, können Web Services problemlos in eine existierende Systemlandschaft eingebettet werden.

Dargestellt sind zwei Partnerfirmen A und B, die auf verschiedene externe Web Services (Zahlungsverkehr, Lieferlogistik) zugreifen. Diese können kostenpflichtige Services sein, die von einem unabhängigen Web-Service-Anbieter im Netz offeriert werden. Außerdem nutzen beide Firmen einen externen Service zur Authentifikation, um sich sowohl bei dem externen Web-Service-Anbieter als auch untereinander authentifizieren zu können. Des Weiteren bietet Firma A einen Web Service an, der es der Einkaufsanwendung von Firma B erlaubt, den aktuellen Lagerbestand von A abzufragen. Beide Unternehmen verwenden State-of-the-Art Application Server, die basierend auf Standards in der Lage sind, Web Services aufzurufen und mit existierenden Anwendungen wie Einkauf, Abrechnung, Lagerhaltung usw. zu verknüpfen.

Auch wenn sich Web Services unkompliziert in die existierende Infrastruktur einfügen lassen, werden mittelfristig die Auswirkungen auf die Gesamtarchitektur und die

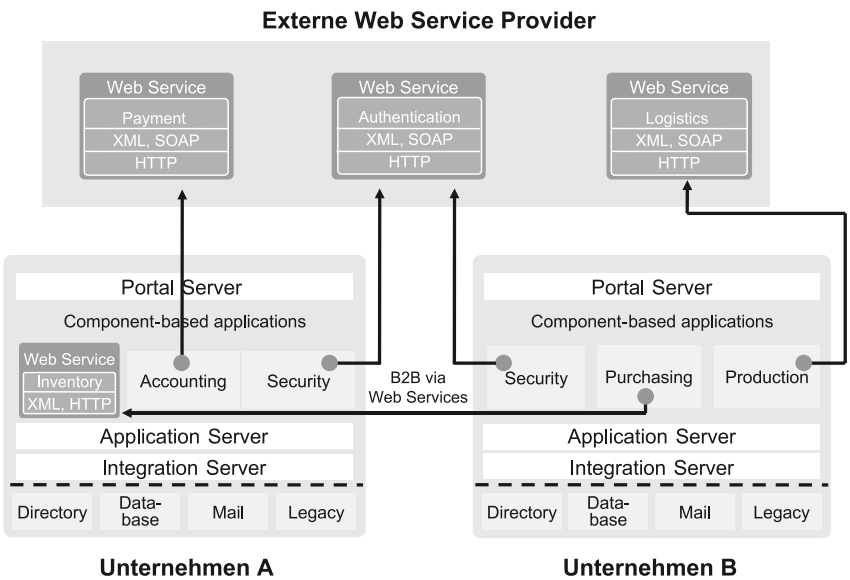


Bild 5.5 Web Services in existierender IT-Infrastruktur

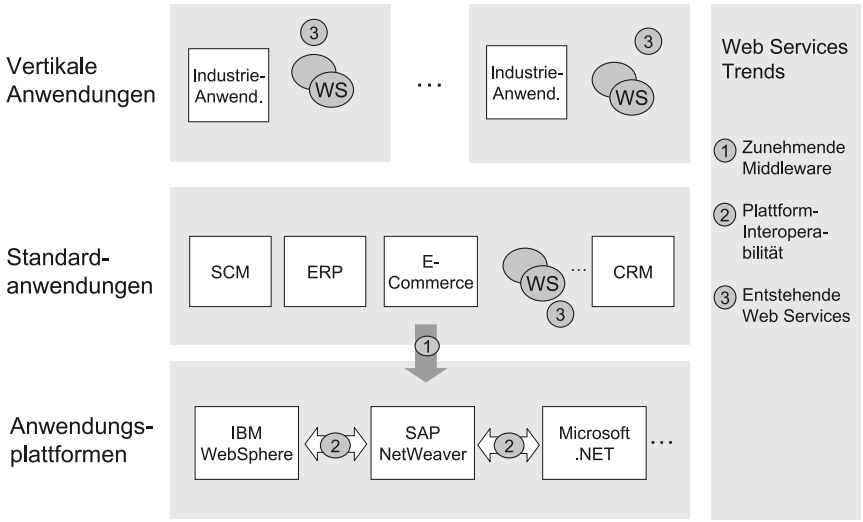


Bild 5.6 Auswirkungen von Web Services (1)

Gestaltung der Middleware erheblich sein. Dies hängt damit zusammen, dass Web Services mehr Wettbewerb mit sich bringen und sich nach und nach standardisierte, autonome Teilprozesse herauskristallisieren. Unternehmen können dadurch flexibler auf Marktanforderungen reagieren.

Internet, SOA und Web Services werden gemeinsam die Grundlage für ein zukunftssicheres B2B-, B2C- und B2E-e-Business werden. In den Bildern 5.6 und 5.7 sind die fünf wesentlichen Trends mit ihren Auswirkungen auf Architektur und Geschäftslösungen dargestellt.

Zunehmende Middleware (Trend 1)

Heutige Application Server unterstützen die Web-Services-Basis-Standards, d.h. sie sind in der Regel mit Containern und Tools ausgestattet, um Web Services entwickeln zu können und ablaufen zu lassen. Darüber hinaus können existierende Anwendungen als Web Services verkapselt werden (Wrapping).

Standard-Anwendungen wie SCM, ERP, CRM laufen heute weitgehend isoliert voneinander, jedoch führt jede für sich einige gleichartige, horizontale Funktionen aus, z. B. Security, Personalisierung, User Management, Identity Management usw. Derartige Funktionen könnten demnächst von Anwendungsplattformen in Form von Web Services zur Verfügung gestellt werden, die dann jeweils bei Bedarf von den Standard-Applikationen aufgerufen werden. Es ist offensichtlich, dass dies die Produktivität von Unternehmen steigern könnte und Hersteller von Standard-Software Spielraum gewinnen würden, um dann ihren Fokus vermehrt auf innovative Funktionserweiterungen zu legen.

Plattform-Interoperabilität (Trend 2)

Wie zu Beginn des Kapitels erläutert, stehen IT-Manager unter Zugzwang, die Interoperabilität verschiedener Anwendungsplattformen und Anwendungen zu verbessern. Dieses Ziel sollte über alle drei Server-Ebenen hinweg erreicht werden: Portal, Application und Integration Server.

Oftmals gewähren Unternehmen mehreren Benutzergruppen über unterschiedliche Portale Zugang zu denselben Anwendungen, Services und Ressourcen. Web Services bieten hierfür eine adäquate Technologie, die inhärent die Interoperabilität in zukünftigen Systemen sicherstellt. Mit dem *WSRP(Web Services for Remote Portals)*-Standard lassen sich Inhalte aus beliebigen Quellen oder auch Anwendungen, die auf anderen Plattformen laufen, als *Remote Portlet* in ein Portal integrieren. Da WSRP mit einschließt, dass der Service-Anbieter auch die Form der Darstellung festlegt, ist die Integration in eine andere Portalumgebung sehr einfach zu vollziehen.

Gemeinsame Portal-Services wie Authentifikation, Location-based Services und Billing Services werden als Web Services implementiert – plattformunabhängig und daher anwendbar über verschiedene Unternehmensportale. Ressourcen, z. B. Web-Inhalte oder Informationen aus Datenbanken, können durch standardisierte Web Sevices beliebigen Benutzergruppen zur Verfügung gestellt werden.

State-of-the-Art Application Server unterstützen die Basis-Standards und Web Services können damit zum Ablauf gebracht werden. Die Interoperabilität zwischen Plattformen verschiedener Hersteller gehört bald zum täglichen Geschäft. Dies wird durch die Nutzung gemeinsamer Web Services und darauf basierender Interaktionen erreicht. Ein weiterer Standard wird die Interoperabilität zwischen J2EE-Plattformen fördern. *Web Services for J2EE Architecture (JSR109)* ist eine Service-Architektur, die auf der J2EE-Komponenten-Architektur beruht und ein entkoppeltes Client/Server-Programm-Modell darstellt, das über J2EE Application Server portabel ist.

Künftig entstehende Web Services (Trend 3)

Das Web-Services-Paradigma wird zweifelsohne Innovation und Wettbewerb steigern und damit das e-Business nachhaltig voran bringen. Best-of-breed-Business-Komponenten können als autonome, wiederverwendbare Web Services in einer UDDI Registry eingetragen werden und stehen damit der ganzen Welt zur Verfügung. Wie in Bild 5.6 gezeigt, werden dadurch viele neue, automatisierte Business-Funktionen entstehen, die sich zu wohldefinierten Geschäftsabläufen zusammensetzen lassen.

Mit der Möglichkeit, Web Services zu publizieren, haben intelligente Software-Startups gute Chancen, Best-of-Breed-Services in den Markt zu bringen. Jedoch weitaus wichtiger ist die Tatsache, dass auch etablierte Anbieter von Standard-Software wie SAP, Peoplesoft oder Siebel ihre Anwendungspakete modularisieren und Einzelkomponenten via Internet anbieten.

Web Services werden häufig in Geschäftsteilprozessen, z. B. für eine Reklamationsbearbeitung eingesetzt. Hier geht es darum, diese Teilprozesse zu optimieren, ohne dass die existierende System- und Anwendungslandschaft aufwändig modifiziert werden

muss. Ein einleuchtendes praktisches Beispiel für eine Teilprozessoptimierung ist in der Zeitschrift *Objektspektrum* [5.3.1] beschrieben.

Auch branchenspezifische Anwendungen werden mehr und mehr durch Web Services ergänzt und auch ersetzt. Sie werden sowohl von spezialisierten Software-Unternehmen als auch von der Branchenindustrie selbst entwickelt, um beispielsweise Geschäftspartner besser in die Prozesse einzubinden.

Business-Prozess-Integration – Das Real-Time-Unternehmen (Trend 4)

Unternehmen müssen sich in sich schnell ändernden Märkten behaupten und streben deshalb Lösungen an, die es erlauben, Prozesse über verschiedene vertikale Applikationen und Anwendungsplattformen hinweg zu integrieren. Effektive Business-Integration bedeutet das Zusammenwirken disjunkter interner und externer Komponenten und Ressourcen mit dem Ziel, Geschäftsprozesse und -strategie optimal zu unterstützen.

Um erfolgreich auf dem Markt bestehen zu können, bedarf es einer Prozessoptimierung durch verstärkte Koordination von Funktionalitäten, die heute in existierenden Anwendungen wie ERP, SCM, e-Commerce und vertikalen Applikationen isoliert ausgeführt werden. Die gewünschten Echtzeit-Ergebnisse lassen sich nur erreichen, wenn diese isolierten Anwendungen integriert, ihre Funktionalitäten genutzt und in anwendungsübergreifenden Prozessen koordiniert werden, wie in Bild 5.7 dargestellt.

Ad-hoc-Business-Prozesse (Trend 5)

Unternehmen sehen eine besondere Herausforderung, wenn es darum geht, schnell auf veränderte Marktgegebenheiten zu reagieren. Es gilt, sich auf neue Geschäftspraktiken, Finanzierungsmodelle und Wettbewerbssituationen einzustellen und kreative Wege zu

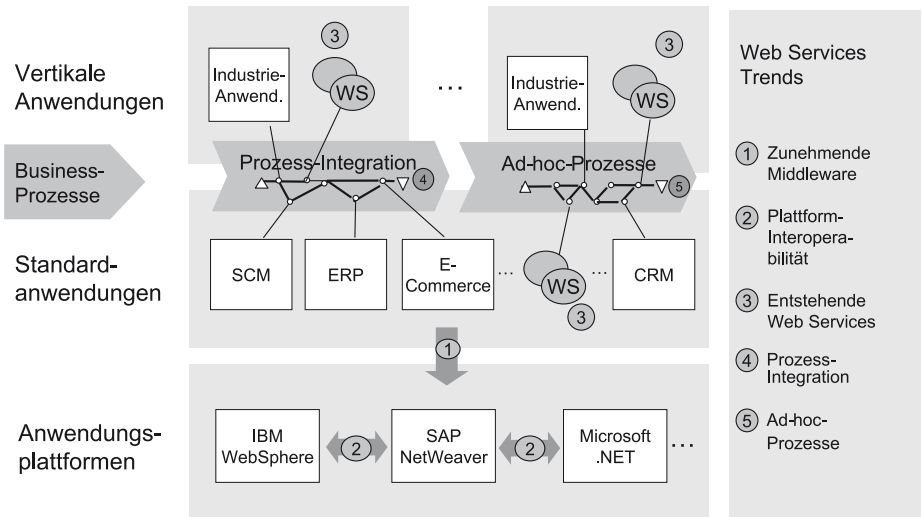


Bild 5.7 Auswirkungen von Web Services (2)

finden, um Kunden zufriedenzustellen und neue hinzuzugewinnen. Häufig kommt es auch darauf an, neue Geschäftsmöglichkeiten aufzubauen, noch unerschlossene Märkte mitzugestalten, neue Vertriebsmodelle zu erproben und effiziente, elektronische Einkaufskanäle mit bereits existierenden zu integrieren.

Die Dynamik des e-Business erfordert *Business Agility*, um schnell genug neue Marktkräfte und Geschäftsmöglichkeiten adaptieren zu können. Unternehmen müssen in der Lage sein, Marktchancen rasch zu realisieren und Dienstleistungen bereitzustellen, die die Kundenerwartungen möglichst sogar noch übertreffen. Sie sind gefordert, ihren Kunden laufend nachgefragten Mehrwert zu bieten, sowohl über entsprechende Preisangebote als auch durch zusätzliche Services.

Unternehmen sollten deshalb in der Lage sein, sogenannte Ad-hoc-Prozesse aufzusetzen, um diesen neuen Anforderungen gerecht zu werden. So könnte mit der Web-Services-Technologie aus der Kombination von CRM-Funktionalität mit einer branchenspezifischen Applikation und einigen zusätzlichen Funktionen kurzfristig ein Workflow arrangiert werden, der die Business Agility ganz wesentlich verbessert.

Business-Integration mit Web Services

Entsprechend den aufgezeigten Trends müssen sich Unternehmen zunehmend und mit hoher Priorität des Themas *Business-Integration* und *Business Process Management* auf Basis der Web-Services-Technologie annehmen.

Wie in Bild 5.8 dargestellt, spielt sich die Business-Integration auf vier Integrationsebenen ab:

– Integration der Anwender (Kunden, Geschäftspartner und eigene Angestellte)
– Integration von internen und externen Applikationen
– Integration von Informationen, einschließlich Content und Knowledge Management
– Prozess-Integration: Integration von internen und externen Prozessen.

Die Anwender-Integration berücksichtigt zunehmend die persönlichen Anforderungen und den Kontext (Situation) des Nutzers sowie erweiterte Wünsche bezüglich Mobility und Security. Gleichzeitig ermöglicht die Integration auf Portalebene eine effizientere Kollaboration mit dem Ziel, zeitkritische Prozesse zu verbessern. Integration wird durch sogenannte Portlets erreicht, die unkompliziert in Portal-Frameworks eingebunden werden können oder aber über den schon erwähnten WSRP-Standard, wenn entfernte Ressourcen zu integrieren sind. Services, z. B. User Management, Rollenverwaltung und Personalisierung werden schrittweise in Form von Web Services realisiert.

Die nächste Ebene betrifft die Integration von Anwendungen. Das aufwändige und überholte Konzept der Punkt-zu-Punkt(Spagetti)-Integration wird zunehmend durch leistungsfähige Integration Server abgelöst. Wie in Kapitel 3 erläutert, bieten sie ein breites Connector-Angebot, sowie Component und Message Broker und Web Services. Letztere werden sich längerfristig zur dominierenden Integrationsmethode entwickeln.

Die Integration von Daten und Informationen kann am besten auf einer Metadaten-Ebene durch eine Reihe von Standards wie *JMI (Java Metadata Interface)* und *XMI*

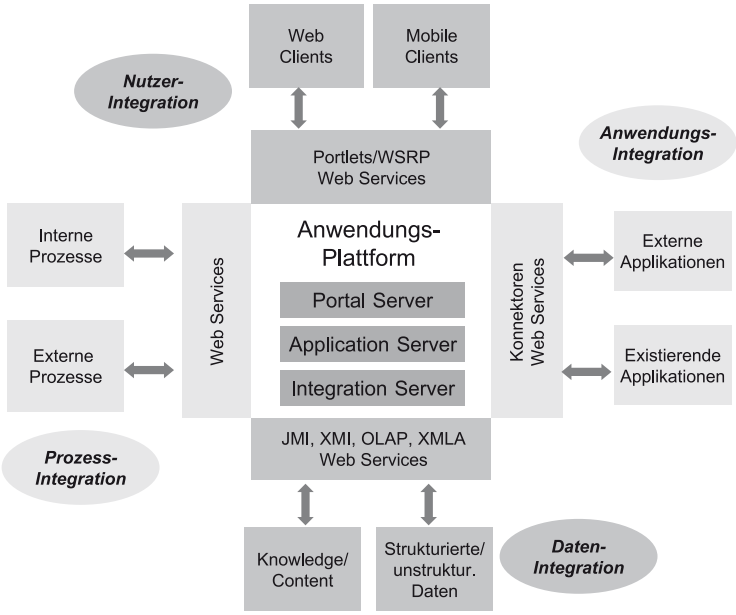


Bild 5.8 Business-Integration mit Web Services

(XML Metadata Interchange) erreicht werden. Ebenso spielen *OLAP (Online Analytical Processing),* das den generischen Zugriff auf eine breite Palette von Anwendungen erlaubt, sowie *XMLA (XML for Analysis),* das ein ähnliches API basierend auf SOAP und XML aufweist, eine wesentliche Rolle. Neben der reinen Messaging-Funktionalität ist auch zentralisiertes, integriertes Knowledge- und Content-Management zweckmäßig.

Die Integration von internen und externen Business-Prozessen sowie die Realisierung von Ad-hoc-Prozessen wird in Zukunft eine zentrale Rolle spielen. Hierfür werden sich Web Services als geeignete Technologie etablieren. Voraussetzung ist allerdings, dass die für eine unternehmensübergreifende Kommunikation benötigten Security-Mechanismen erweiterungsfähig sind und breite Akzeptanz finden. Derzeit ist eine ausreichende Implementierung in den meisten Fällen noch nicht möglich.

In der Vergangenheit wurden individuelle Geschäftsprozesse durch dedizierte Anwendungen unterstützt. Dies hat in der Regel dazu geführt, dass zwar eine Optimierung genau des jeweiligen Prozesses erreicht, jedoch eine gesamtheitliche Lösungssicht vernachlässigt wurde. Übergeordnete Anforderungen konnten deshalb häufig nur unzureichend erfüllt werden. Die nun verfügbaren Integrationstechnologien erlauben einen wesentlich effizienteren und gleichzeitig flexibleren Lösungsansatz, der die existierende und zukünftige Anwendungslandschaft, auch die von Geschäftspartnern, mit einschließen kann.

Business Process Management

Business Process Management (BPM) umfasst die Verfahrensweise mit den dazugehörigen Tools, die dazu dienen, Geschäftsprozesse Schritt für Schritt zu modellieren, grafisch aufzubereiten und zu simulieren. Analyse und Design von BPM-Abläufen machen ein klares Verständnis der einzelnen Prozessschritte erforderlich. Mittels BPM lassen sich ganzheitliche Business-Prozesse ausführen, deren Einzelschritte häufig mit wohlbekannten Geschäftsaktivitäten korrespondieren, wie z. B. Prüfen der Kreditfähigkeit, Ausstellen einer Kundenrechnung und Abfrage des Lagerbestandes. In seiner Ausführung ist der BPM-Prozessablauf oft lediglich eine Folge wohldefinierter und koordinierter Services.

Eine effektive Methode für flexibleres Design von Business-Lösungen basiert auf der Trennung von Prozessablauf und Funktion, wie in Bild 5.9 dargestellt.

Durch die Anwendung von SOA und Web Services in Kombination mit einer Business-Prozess-Sprache, z. B. *BPEL*, wird genau dieses Ziel erreicht. BPEL verwendet ausschließlich Web Service Interfaces zum Exportieren und Importieren von Nachrichten und damit zum Aufrufen von Funktionen und zum Empfangen von Ergebnissen. Durch das Separieren von Prozessabläufen von der eigentlichen Funktion wird die Unabhängigkeit des Prozessablaufs von Funktionsimplementierungen erreicht. Funktionen lassen sich mittels Web Services direkt oder auch in existierenden Anwendungen (SAP, Legacy usw.) ausführen. Entsprechende Interfaces werden über *WSDL* bedient.

Dieses Konzept ermöglicht die Integration von Business-Prozessen durch eine Kombination von Funktionen aus unterschiedlichen Applikationen, die z. B. einen optimierten *Workflow* für die Auftragsbearbeitung repräsentieren können. Gleichzeitig bietet es

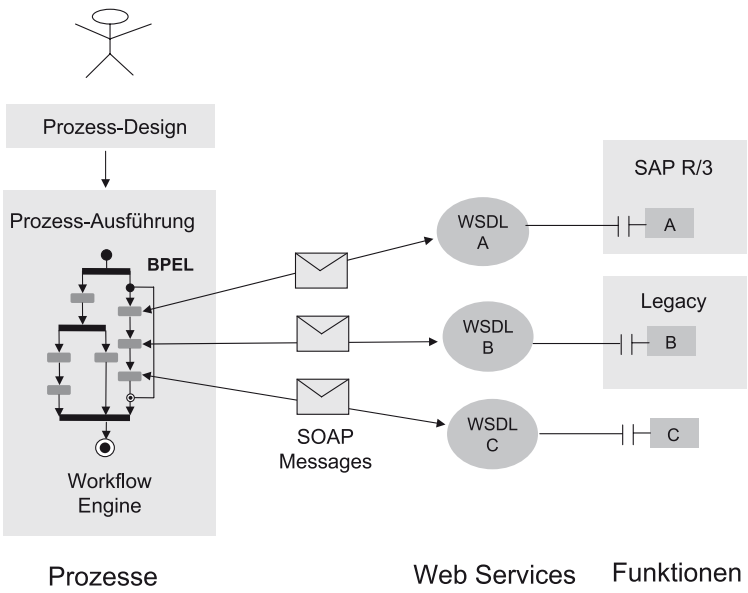


Bild 5.9 Trennung von Prozessablauf und Funktionen

die erforderliche Flexiblität, um Ad-hoc-Prozesse kurzfristig aufsetzen zu können und zwar weitgehend unabhängig von den organisatorischen Gegebenheiten und vorhandenen IT-Ressourcen, die solche Prozesse unterstützen.

Als Analogie mag eine Fertigungsstraße, mit der Teile eines Automobils gefertigt werden, zum Verständnis beitragen. Die einzelnen Fertigungsstationen (z. B. Roboter) entsprechen den o.g. Funktionen (z. B. Web Services) und das Fertigungsprogramm ist mit dem durch BPEL definierten Prozess vergleichbar. Fertigungsprogramme können heute flexibel und kurzfristig geändert werden. Das trifft auch bei BPEL-Prozessabläufen zu. Bei der Umrüstung der Fertigungsstraße werden häufig nur der Einsatz von Teilen (entspricht Daten) und Roboterprogrammen (entspricht Web Services) geändert. Fertigungsstationen und Fertigungsprogramme können unabhängig voneinander modifiziert werden, was eine höhere Flexibilität zur Folge hat.

Der Vorläufer von BPM, der klassische Dokumenten-Workflow, war auf die von Personen ausgeführten Dienste ausgerichtet. Im Gegensatz dazu wird mittels BPEL und Anwendungsintegration mehr Priorität auf eine durchgängige Automatisierung gelegt. Dabei können Menschen – meist als Exception Handling – weiterhin eingreifen.

SOA ist der architekturelle Ansatz, um herkömmliche Anwendungen schrittweise in wohldefinierte Services zu verwandeln. BPM hat einen inhärenten Bezug zu Services. SOA bringt Services hervor und BPM, das einen Prozessablauf festlegt, nimmt diese Services in Anspruch. Als Vision eröffnet SOA ein riesiges Potenzial von Services, die mittels BPM/BPEL zu beliebigen und vollständigen Geschäftsabläufen orchestriert werden können.

Die daraus resultierende *Business Agility* ist offensichtlich, Ablauf und Service existieren unabhängig voneinander und damit wird die Flexibilität erhöht. Neue Services (Funktionen) können generiert und via BPM in neu komponierte (*orchestrierte*) Anwendungen (*Prozesse*) eingebunden werden.

Effektive BPM-Lösungen verlagern die Kontrolle über Business-Prozesse von den IT-Organisationen zurück zu den geschäftsführenden Einheiten. Das heißt, Geschäftsbereiche werden in die Lage versetzt, selbst in Business-Prozesse einzugreifen und diese unmittelbar zu ändern, wenn es die aktuellen Marktgegebenheiten erfordern. BPM erlaubt es auch, z. B. Vorstände mit aktuellsten Informationen zu versorgen, damit sie umgehend geschäftsrelevante Entscheidungen treffen können.

Wie in Kapitel 3 bereits erläutert, sind moderne Integration Server sowohl mit BPM-Modellierungs- und Simulations-Tools als auch mit Workflow Engines ausgestattet, die Business-Prozesse zur Ausführung bringen.

Web Services Management

Im Mittelpunkt des Managements von Web Services stehen insbesondere geschäftskritische Anwendungen. Unternehmen sollen in die Lage versetzt werden, Plattformen, Anwendungen, Services und Prozesse zu managen. Web-Services-Management-Produkte müssen eine geeignete Infrastruktur und Funktionalität zur Verfügung stellen, die es möglich macht, aus einzelnen fein-granulierten Web Services, verbunden mit Daten

aus verschiedenen Quellen, ganzheitliche Business-Prozesse zu koordinieren, zu managen und deren Ablauf zu überwachen.

Die Bedeutung eines umfassenden Managements wird offensichtlich, wenn sich die Web-Services-Technologie erst einmal konsolidiert hat und eine zunehmende Anzahl von Web Services verfügbar ist. Unternehmen werden dann schnell Tools nachfragen, die einen sicheren und automatisierten Betrieb ermöglichen.

Weder der Funktionsumfang noch die Standardisierung auf diesem Gebiet sind bis dato einigermaßen definiert oder gar weit fortgeschritten. Allerdings wird das Interesse mittlerweile durch eine Reihe von kürzlich eingebrachten Standard-Vorschlägen dokumentiert. Bei *OASIS* wurde jetzt ein entsprechendes Technical Committee *Web Services Distributed Management (WSDM)* [5.3.2] gegründet, um das Thema voranzubringen.

Web Services Management ist wichtig für Unternehmen, die Anwendungen und Prozesse in eigener Regie betreiben. Von größtem Stellenwert ist es jedoch für professionelle IT-Service-Provider, die in der Regel auch einen umfangreicheren Funktionsumfang anbieten und beherrschen müssen.

Web-Services-Management-Funktionen sollten folgende Funktionalitäten umfassen:

- Infrastruktur- und Applikations-Management
- Monitoring und Metrics
- Security und Certification Services
- Service Level Agreements, Abrechnungsfunktionen, Finanz-Services, Vertragsmanagement.

Infrastruktur- und Applikations-Management betreffen Erweiterungen von traditionellen Management-Funktionen aufgrund der Tatsache, dass Web Services eine zusätzliche Middleware-Schicht darstellen.

Monitoring Services bedeuten u.a. auch das Monitoring der Interaktionen mit Partnern und Kunden. IT-Organisationen stehen unter besonderem Druck, den Wert ihrer IT-Investitionen aus Sicht der Geschäftsziele und -tätigkeiten ständing nachweisen zu müssen. Deshalb ist eine verbesserte Transparenz des IT-Betriebs unbedingt nötig. Die ganzheitliche Sicht sämtlicher Service-Interaktionen gibt tiefen Einblick in die Effizienz der Abläufe. Entsprechende Kennwerte (Metrics) tragen dazu bei, dass Web-Services-basierte Business-Prozesse laufend optimiert werden.

Mit zunehmender Zahl publizierter Web Services von mehr oder weniger unbekannten Quellen werden Security, Zuverlässigkeit (Availability), Qualität und Vertrauen (Trust) zu Schlüsselthemen für Unternehmen, die diese Services in Anspruch nehmen wollen. Die Zertifizierung solcher Services und die Garantie, dass bestimmte Qualitäts-Level eingehalten werden, ergeben sicherlich noch interessante Geschäftsmöglichkeiten für IT- und Outsourcing-Service-Provider. Des Weiteren stellen passende Service Level Agreements, Billing- und Finanzdienste und Vertragsmanagement im Zusammenhang mit Web Services neue Herausforderungen dar. Mit derartigen Services haben Service-Provider die Chance, sich in Zukunft zu profilieren.

5.4 Zukunftsorientierte SOA-Plattformen

Die wesentlichen Anbieter von Anwendungsplattformen haben die Web-Services-Technologie adaptiert und entwickeln schon ihre Plattformen in Richtung SOA. Im Folgenden werden einige Beispiele erläutert.

5.4.1 SAP NetWeaver

SAPs *NetWeaver Plattform* [5.4.1] ist ein Beispiel für eine zukunftsorienierte Anwendungsplattform. Sie verbindet in beispielhafter Weise die Koexistenz der traditionellen Anwendungswelt (SAP R/3, mySAP) mit dem SOA/Web-Services-Paradigma.

SAP hat in den Neunzigerjahren – im Wesentlichen mit seiner ERP-Software SAP R/3 – die führende Weltmarktposition für betriebswirtschaftliche Software erobert. Ende der Neunzigerjahre wurde diese Position durch einige schnell wachsender Software-Anbieter bedrängt, deren Lösungen Internet-basierend und unternehmensübergreifend ausgelegt waren und zunächst sehr positiv vom Markt aufgenommen wurden (Ariba, Commerce One, I2, Siebel usw.). SAP hat darauf mit der Technologie mySAP.com reagiert und sein Angebot sukzessive um CRM, SCM und weitere Komponenten ergänzt. Heute kann auch auf diesen Anwendungsfeldern eine Marktführerschaft von SAP registriert werden.

Die jüngste Herausforderung besteht nun in der Umsetzung der Service-orientierten Architektur mit Web Services als Basistechnologie in die zukünftige Lösungslandschaft.

SAP hat zunächst auf diese Entwicklung mit einer zunehmenden Unterstützung von Web Services im Umfeld von mySAP und im Herbst 2002 mit der Ankündigung der xApps-Technologie geantwortet.

Mit xApps lassen sich funktionsübergreifende Prozesse generieren, indem sie auf bestehenden Systemen aufsetzen und Informationen bzw. Funktionen verschiedener Anwendungen so miteinander verknüpfen, dass gewünschte Ergebnisse und Abläufe effizient erzielt werden können.

Enterprise Services Architecture (ESA) und die NetWeaver Plattform

Mit der Ankündigung der Technologieplattform NetWeaver Anfang 2003 vollzieht SAP nun eine durchgängige SOA-Unterstützung und gleichzeitig eine wesentliche Änderung der Geschäftsstrategie. Zum einen begibt sich SAP in das Lager der Technologie- und Plattformanbieter und steht hier mindestens teilweise in direktem Wettbewerb zu Microsoft, IBM, BEA und SUN. Zum anderen verlässt SAP den bisherigen Ansatz, ausschließlich auf eine ganzheitliche SAP-Lösungswelt bei seinen Kunden zu setzen. SAP öffnet sich stärker in Richtung Standards (Java, XML, Web Services) und setzt gleichzeitig auf eine strategisch wichtige Interoperabilität und Integration der NetWeaver-Plattform und -Anwendungen mit Microsoft- und IBM-Middlewareprodukten.

NetWeaver bildet gleichzeitig die informationstechnische Basis für eine Service-orientierte Architektur, bei SAP wird sie als *Enterprise Services Architecture (ESA)* bezeichnet. ESA soll die Basis für flexible und erweiterbare Unternehmenslösungen in heterogenen IT-Landschaften bieten, ist aber auch als das Grundkonzept für eine vollständige Unternehmensintegration zu verstehen.

Nach der SAP-Konzeption erweitert ESA das Web-Services-Paradigma zu einer Architektur für Geschäftsanwendungen. Während Web Services zunächst nur ein technisches Konzept darstellen, ist ESA das Konzept für umfassende und Service-basierende Geschäftsanwendungen.

SAP definiert ESA wie folgt:

ESA

- unterstützt alle Personen, die an einem Geschäftsprozess teilnehmen, sowohl innerhalb als auch außerhalb des Unternehmens,
- umfasst alle Informationen, die für den Geschäftsprozess relevant sind,
- integriert alle Systeme, die für den Prozess wichtig sind, und zwar unabhängig davon, ob es sich hierbei um interne oder externe, um SAP- oder um Nicht-SAP-Systeme handelt.

Künftig sollen alle SAP-Lösungen wie *SAP R/3 Enterprise*, alle *mySAP-Lösungen*, sowie *xApps* entsprechend dieses ESA-Entwurfes konzipiert werden.

NetWeaver schafft für SAP die technologische Basis, um die ESA-Vision umzusetzen. Zum ganzheitlichen Verständnis des NetWeaver/ESA-Konzeptes sind zwei Aspekte zu unterscheiden. Diese Aspekte spiegeln sich in den kombinierten Funktionalitäten der NetWeaver-Plattform wider, nämlich in ihren Ausprägungen als

- Ablauf- und Integrationsplattform für existierende und neue SAP-Anwendungen und
- als offene Interoperabilitäts- und Integrationsplattform mit dem besonderen Fokus auf einer Interoperabiltät mit den Technologien IBM WebSphere- und Microsoft .NET.

Ablauf- und Integrationsplattform für SAP-Lösungen

NetWeaver bietet als Plattform für alle aktuellen und zukünftigen SAP-Lösungen eine Reihe von neuen Funktionen und Integrationsfunktionen, die von den verschiedenen SAP-Lösungen ganz oder teilweise genutzt werden. Bild 5.10 zeigt die NetWeaver-Plattform.

Die SAP R/3-Enterprise-Lösung soll über sogenannte Extensions die neuen NetWeaver-Funktionen (z. B. das Portal) nutzen. Die mySAP-Lösungen, die als Einzellösungen (z. B. *mySAP ERP*) oder als gebündelte Lösungen (*mySAP Business Suite, mySAP Smart Business Solutions*) auf NetWeaver verfügbar sind, sollen ebenfalls nach und nach die NetWeaver-Funktionalität nutzen können. SAP wird die sukzessive Migration seiner Lösungen auf die NetWeaver-Plattform in seiner Produkt- und Release-Strategie im Einzelnen festlegen und vollziehen.

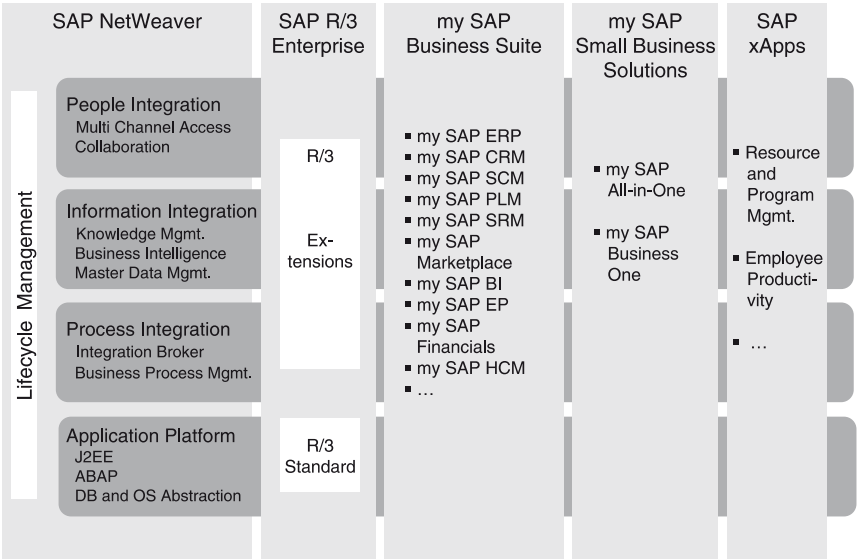


Bild 5.10 SAP NetWeaver

Die NetWeaver-Schlüsselkomponenten werden teilweise auch als Einzelkomponenten angeboten. Zu diesen Schlüsselkomponenten gehören neben dem *Web Application Server (WAS),* dem Enterprise Portal Server und der *Exchange Infrastructure (XI)* weitere Komponenten, die von vielen SAP-Anwendungen genutzt werden, wie Collaboration, Multichannel-Zugriff, Knowledge Management, Business Intelligence, Master Data Management und Life-Cycle Management.

Die wesentlichen Komponenten sind:

– Portal Infrastructure
wird über *mySAP Enterprise Portal* verfügbar gemacht und ermöglicht einen einheitlichen, personalisierten und Rollen-basierten Zugriff von Mitarbeitern, Partnern oder Kunden auf die angebundene heterogene IT-Umgebung.

– Collaboration
ermöglicht die dynamische Echtzeit-Kommunikation innerhalb fester oder flexibel zusammengestellter Teams oder Gemeinschaften. Sie umfasst Funktionalitäten wie den gemeinsamen Zugriff auf E-Mails, Kalender, Diskussionsforen und gemeinschaftlich verfügbare Dokumentenspeicher.

– Multichannel Access
wird über *mySAP Mobile Business* zur Verfügung gestellt und umfasst die Möglichkeit, sich mit dem Unternehmenssystem über Festnetz oder Funktechnologien in Verbindung zu setzen, und schließt Sprach- und Datendienste ein.

– Knowledge Management
bietet nutzerorientierte Services, über die Zugriffe auf das Content-Management-System von SAP oder von Drittanbietern ermöglicht werden. Integrierte Werkzeuge

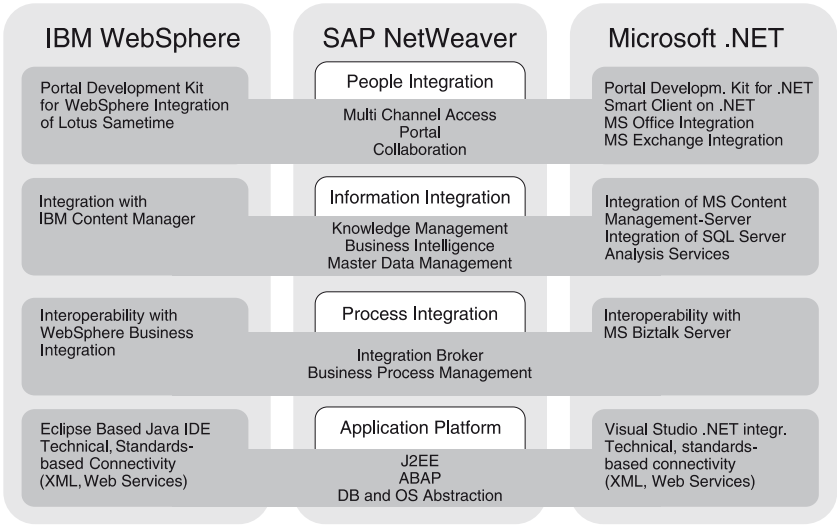
unterstützen Suche, Taxonomie, Klassifizierung, Publishing sowie die damit verbundenen Workflow-Prozesse.

– Business Intelligence
  Mit dieser Komponente können zeitkritische und wichtige Informationen analysiert, integriert und verteilt werden. Sie wird mit *mySAP Business Intelligence* zur Verfügung gestellt und bietet einen Werkzeugkasten, der das Design von interaktiven und individuellen Reports und Anwendungen erleichtert.
– Master Data Management
  ermöglicht die Datenintegrität über die heterogene IT-Infrastruktur eines Unternehmens. Es erlaubt Stammdaten systemweit zusammenzuführen und zu harmonisieren. Damit soll unabhängig von Hersteller und räumlicher Verteilung der beteiligten Systeme eine übergreifende Datenkonsistenz möglich werden.
– Exchange Infrastructure
  besteht aus dem *Integration Server* und dem *Business Process Management*. Die Exchange Infrastructure bietet entsprechende Integrationsmethoden und Tools für die Integration von SAP-Anwendungen und solche von Drittanbietern (wird nachfolgend ausführlicher behandelt).
– Application Platform
  ist die Ablaufbasis für alle SAP-Lösungen und wird als *SAP Web Application Server (WAS)* zur Verfügung gestellt. Sie unterstützt die beiden aus SAP-Sicht wesentlichen Schlüsseltechnologien ABAP und J2EE. Damit werden bestehende Investitionen geschützt und gleichzeitig die Öffnung zu einem weitverbreiteten Standard mit zukünftigen offenen Lösungen geschaffen. Ein integriertes Web Services Framework unterstützt plattformunabhängige Web Services. Ein Security Framework beinhaltet Elemente wie Single Sign-on, rollenbasierte Autorisierung, zentrale Benutzerverwaltung, sicherer und verschlüsselter Datenaustausch, Unterstützung von digitalen Signaturen und Public-Key-Infrastrukturen.
– Life-Cycle Management
  unterstützt alle Phasen des Software-Zyklus, einschließlich Design, Entwicklung, Einsatz, Implementierung, Versionierung und Test. SAP hat sich für eine Standardisierung der Entwicklungswerkzeuge auf der Grundlage des Open-Source-Frameworks Eclipse entschieden. Die integrierte Java-Entwicklungsumgebung basiert daher auf Eclipse.

Offene Interoperabilitäts- und Integrationsplattform

Mittelgroße Firmen und vor allem Großunternehmen entscheiden sich immer häufiger für SAP, IBM und Microsoft als Hauptlieferanten für ihre Geschäftslösungen und technologische Infrastruktur. Die Gesamtkosten hängen entscheidend davon ab, wie gut die Anwendungen der Zulieferer zusammenwirken. Aus diesem Grund wird von den Herstellern zunehmend gefordert, die Interoperabilität zu verbessern.

In dieser Situation hat SAP mit der offenen Interoperabilitäts- und Integrationsplattform NetWeaver eine geeignete Antwort gefunden. NetWeaver unterstützt wesentliche Standards, die von internationalen Organisationen wie dem W3C, der WS-I, dem Java Community Process und OASIS vorangetrieben werden.



Source: SAP

Bild 5.11 NetWeaver – Interoperabilität mit IBM WebSphere und Microsoft .NET

SAP hat des Weiteren mit *IBM* und *Microsoft* enge Kooperationsvereinbarungen über eine verbesserte Interoperabilität zu deren Middleware und Technologien getroffen. Als Ergebnis werden Interoperabilitäts-Komponenten und -Schnittstellen und teilweise auch Integrationsvorhaben zu einer erweiterten Plattform führen, wie in Bild 5.11 dargestellt.

Die gemeinsamen Bestrebungen, eine akzeptable Interoperabilität zwischen den verschiedenen Plattformen herzustellen, umfassen folgende Ebenen:

– Anwendungs- und Entwicklungs-Plattform
  Der SAP Web Application Server (WAS) unterstützt wie auch die entsprechenden Plattformen von IBM und Microsoft eine Reihe von offenen Standards (XML, SOAP, WSDL, UDDI, usw.). Eine bidirektionale Kommunikation wird zu J2EE-Anwendungen über den SAP Java Connector (Jco) und zu .NET über den SAP .NET Connector unterstützt. Kunden, die WebSphere oder .NET einsetzen, können damit auf vorhandene Geschäftsobjekte zugreifen und SAP-Anwendungen integrieren. Bei den Entwicklungsumgebungen für Java setzen SAP und IBM auf das Open Source Framework Eclipse, wodurch eine hohe Interoperabilität mit dem *WebSphere Studio Application Developer (WSAD)* gegeben ist. Der SAP .Net Connector bietet auch Unterstützung der Entwicklungsumgebung von Visual Basic.
– Portal-Ebene
  SAP wird den neu eingeführten *WSRP(Web Services for Remote Portals)*-Standard unterstützen und mit dem *Java Portlet Standard JSR 168* kompatibel sein. Das Portal kann somit transparent Portlets aufnehmen, die aus anderen Entwicklungsumgebungen stammen. SAP stellt Portal Developer Kits für IBM WebSphere und Microsoft .NET zur Verfügung. Damit sollen Entwickler in der Lage sein, Portaldienste in WebSpere- oder .NET-Umgebung zu entwickeln und diese in das SAP-Portal einzu-

betten. Umgekehrt stellt SAP für etwa 200 BAPIs XML-Schemata zur Verfügung, so dass die entsprechenden SAP-Anwendungen mittels Web Services einfach in WebSphere- oder .NET-Umgebungen eingebunden werden können.

– Collaboration
  An einer Integration von LOTUS/Sametime (Instant Messaging, Web-Konferenzen, virtuelle Team-Räume) arbeiten IBM und SAP gemeinsam. Eine Interaktion sowohl mit Daten aus Microsoft Exchange und Office als auch Lotus/Domino ist bereits möglich.
– Daten-, Analyse- und Informationsebene
  SQL Server Analysis Services von Microsoft können als mehrdimensionale Datenspeicher in SAP BW verwendet werden. Entsprechende Management-Tools werden in beiden Systemen integriert. Auf der Metadaten-Ebene stellt SAP auf Basis von *JMI (Java Metadata Interface)* und *XMI (XML Metadata Interchange)* Datenintegration zur Verfügung. Des Weiteren wird *OLE DB* für *OLAP* und *XMLA* für die Analyse unterstützt. SAP KM unterstützt Standards für Zugriff, Interaktion und Bereitstellung von unstrukturierten Informationen und stellt offene APIs bereit, die eine Verbindung mit anderen Repositories erlauben. In Untersuchung befinden sich Integrationsszenarien zwischen dem SAP KM Repository Framework und den Content-Management-Systemen von IBM und Microsoft.

Exchange Infrastructure

Auf der Anwendungs- und Prozesse-Ebene stellt SAP die Exchange Infrastructure (XI) als die Kernkomponente für Integration und Interoperabilität zur Verfügung. Sie enthält insbesondere auch das Business Process Management. XI ist SAPs Integration Server. Sie ist Bestandteil der meisten SAP-Lösungen, kann aber auch als eigenständige Integrationskomponente eingesetzt werden.

SAP XI stellt eine Anzahl technischer Adapter bereit, etwa JMS-Adapter für die Interoperabilität mit WebSphere Business Integration (MQSeries) oder Partneradapter zu Microsoft Message Queuing (MSMQ) und BizTalk. Es wird darüber hinaus ein Adapter Framework auf der Basis der Java Connector Architecture (JCA) zur Verfügung gestellt. In dieses Framework lassen sich die bereits von einigen Unternehmen angebotenen JCA-Adapter von Drittanbietern einfügen, wie von IBM. SAP hat allerdings nicht vor, diese Adapter selbst zu entwickeln.

Wie in Bild 5.12 dargestellt, besteht die Exchange Infrastructure aus dem Integration-Server-Laufzeitsystem und zugeordneten Knowledge-Daten, die im Integration Directory und Integration Repository abgelegt sind. Der Integration Server realisiert eine XML/SOAP-basierte Kommunikation zwischen Anwendungen verschiedener SAP-Lösungen oder auch Anwendungen anderer Anbieter.

Die wesentliche funktionale Erweiterung der letzten XI-Version war das verbesserte Business Process Management. Mit dem neuesten BPM lassen sich Geschäftsprozesse modellieren und in einem dynamischen Umfeld anpassen. Es ermöglicht die Kombination von Anwendungen zu sogenannten adaptiven Prozessen, die vollständige Wertschöpfungsketten umfassen können.

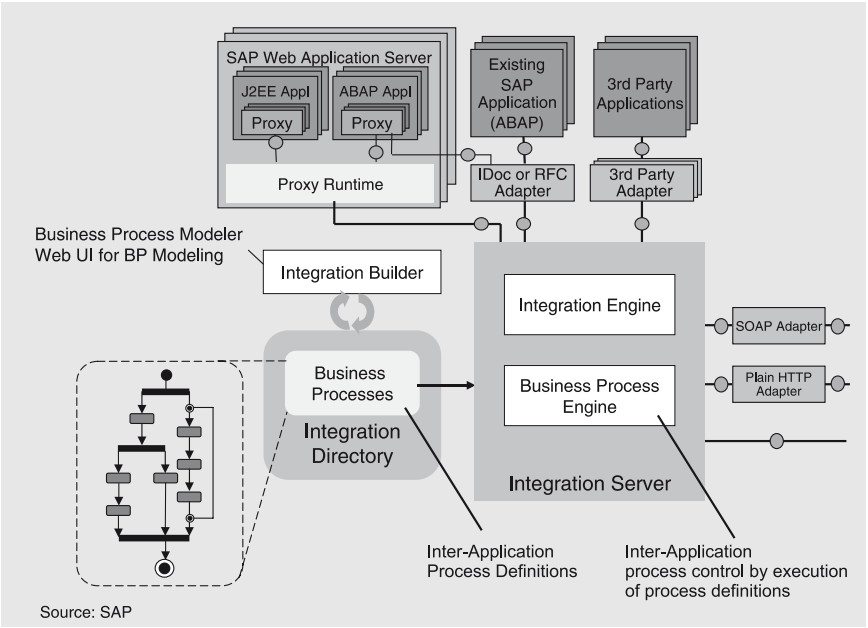


Bild 5.12 SAP Exchange Infrastructure – Business Process Management

BPM besteht aus folgenden Komponenten: *Integration Directory, Integration Repository, Integration Builder* und *Business Process Engine*.

Das Integration Directory enthält Informationen, die zur Laufzeit benötigt werden, z. B. Interfaces wie BAPIs, IDocs, (das sind SAP-spezifische Schnittstellen), RFCs (Remote Function Calls), Mappings, Routing-Einstellungen, Adressen und Workflows. Integrationsszenarien und Business-Prozesse werden schon in der Entwicklungsphase im Integration Repository abgelegt. Das Repository enthält bereits für die Integration von SAP-Anwendungen eine Reihe von Szenarien und Prozessen. Partner und Kunden können bei Bedarf sowohl ihre eigenen als auch die Anwendungen von Drittanbietern ergänzen.

Der Integration Builder ist ein Prozess-Modellierungs-Tool, unterstützt BPEL, erlaubt Import und Export von Prozess-Definitionen und ermöglicht die Integration von Business-Szenarien und Business-Prozessen, die im Integration Repository abgelegt sind.

Die Business Process Engine ist Bestandteil des XI Integration Server und steuert die einzelnen Prozessschritte entsprechend der Abläufe, die im Integration Directory definiert sind.

Die Exchange Infrastructure ist zwar nur auf dem SAP Web Application Server ablauffähig, ist aber als offene Integrationsplattform positioniert. Sie unterstützt u.a. die Industrie-Standards *RosettaNet*, *Chemical Industry Data Exchange (CIDX)* und *Petroleum Industry Data Exchange (PIDX)*. Das dokumentiert sich auch mit dem offenen Adapter Framework JCA, und der Möglichkeit, Partner Profiles in das Integration

Directory aufzunehmen. Die XI bietet auch ein besonderes Integration Tool für SMBs (Small and Medium Business).

Die Frage ist allerdings, mit welchem Sicherheitslevel unternehmensübergreifende Prozesse realisiert werden können.

xApps

xApps stellen eine neue Klasse von Anwendungen dar, die in das Umfeld der NetWeaver Plattform eingebettet sind. Sie wurden mit dem Ziel der Geschäftsoptimierung und Innovation konzipiert. Mit der Fähigkeit, existierende heterogene Systeme in unternehmensübergreifende End-to-End-Prozesse zu kombinieren, können durch xApps Business-Prozesse auf eine verbesserte Agilität (Business Agility) ausgerichtet werden. Das bedeutet größere Agilität in Bezug auf die Adaption von veränderten Geschäftsmodalitäten der agierenden Unternehmensbereiche und ihrer Partner. Es bedeutet aber auch, das Bestmögliche aus dem, was bereits existiert, herauszuholen: Wissen, Produkte, Geschäftsbeziehungen, IT-Lösungen und andere Werte.

xApps, die von SAP und ausgewählten Partnern entwickelt werden, sind auf funktionsübergreifende Prozesse fokussiert. xApps-Familien werden Lösungsfelder wie Enterprise Change Management, Product Portfolio Management, Employee Relationship Management und Employee Services Automation einschließen, um nur einige zu nennen. Es wird erwartet, dass xApps-Familien schnell wachsen und eine vielversprechende Methode sind, um Best-of-Breed-Applikationen zu implementieren.

xApps wurden mit folgenden Design-Zielsetzungen konzipiert:

- Einfache Einbindung in die existierende Infrastruktur mit unterschiedlichen Back-End-Systemen
- Nutzung aller zukünftigen Funktionserweiterungen der NetWeaver-Plattform
- garantierte Konsistenz bezüglich User Interface, Business-Objekten und Services, die inhärent verwendet werden
- Unterstützung von semi-strukturierten Ad-hoc-Prozessen

Der architekturelle Ansatz der xApps umfasst

- einen Modell-orientierten Ansatz. Alle Elemente sind in einem einzigen Repository modelliert und daraus wird der Code generiert, für das UI, für die Integration Proxies und für den Inhalt sämtlicher anderer Repositories, die integriert werden können. Dadurch wird erreicht, dass neue Plattformfunktionen einfach adaptiert werden können.
- eine Service-orientierte Architektur, die es ermöglicht, dass xApps existierende Business-Objekte, Applikationen, Persistence Services, Prozesse, Workflows und User Interfaces verwenden können.
- einen Pattern-basierten Ansatz für das Interface Design. Wohlbekannte Patterns (Muster) erhöhen die Konsistenz und die Akzeptanz durch den Benutzer und erleichtern das Design von Lösungen.

– einen standardisierten Zugriff auf Objekte einschließlich Life-Cycle Services und Services wie Search, Classify usw. Aus Sicht des Programmierens erhöht dies die Produktivität erheblich.

Zusammenfassend werden die Besonderheiten der xApps nochmals hervorgehoben:

Entwickler können sämtliche vorhandene Netweaver Tools verwenden: UI-Modellierung, Prozess- und Workflow-Modellierung, Business-Objekt-Modellierung und Service-Modellierung. Zur Laufzeit können ebenfalls alle NetWeaver-Funktionalitäten in Anspruch genommen werden, wie Knowledge Management oder Business Process Management.

Bewertung

Mit der NetWeaver-Plattform hat sich SAP in Richtung SOA geöffnet und will langfristig die Durchgängigkeit dieser Architektur in allen SAP-Anwendungen sicherstellen.

SAP geht mit NetWeaver den Weg, vollständig unabhängig von der Middleware anderer Hersteller (z. B. IBM WebSphere, BEA Weblogic) zu werden. Diese Unabhängigkeit bindet einerseits Entwicklungsressourcen, da wettbewerbsfähige Middleware-Komponenten von SAP selbst entwickelt werden müssen. Andererseits setzen zukünftig alle SAP-Lösungen, sowohl J2EE als auch ABAP, auf derselben Plattform auf, was Entwicklungs- und Testressourcen einspart und strategisch von Bedeutung ist.

Es bleibt abzuwarten, ob SAP die Technologie-Plattform NetWeaver auch als offene Plattform unabhängig von SAP-Anwendungen vermarkten wird. Unter Nutzung der NetWeaver-Plattform-Services wie Application Server, Portal und Exchange Infrastructure könnten Unternehmen jedenfalls beliebige Web Services integrieren, um ihre Prozesse so flexibel wie möglich zu gestalten.

SOA wird zweifellos den Markt für innovative Lösungen und Services in Bewegung bringen. Neue Chancen eröffnen sich für Nischenanbieter mit sehr spezialisierten oder innovativen Services, die sie netzweit über die standardisierten Interfaces und Protokolle anbieten. Für SAP bedeutet dies zunehmenden Wettbewerb bei Lösungen. Andererseits hat SAP selbst die Chance, eigene Web Services als Standard-Services anzubieten, die plattformunabhängig genutzt werden können. SAP dürfte hier mit seinem existierenden Prozess-Know-how in einer komfortablen Position sein.

5.4.2 Plattformen anderer Hersteller

Technologien und Architekturen wie XML, Web Services, SOA und BPM hatten in den vergangenen Jahren deutliche Auswirkungen auf die Ausprägungen der Anwendungsplattformen aller wesentlichen Software-Hersteller. Neben SAP sind es besonders Microsoft und IBM, die umfangreiche Middleware-Plattformen anbieten. Sie weisen in die Richtung von Eigenschaften und Funktionen, wie sie in diesem Kapitel beschrieben wurden und stellen eine geeignete Basis für zukunftssichere e-Business-Lösungen dar.

Im Folgenden wird auf einige Highlights hingewiesen.

Microsoft

Wie bereits erläutert, ist *Microsoft* [5.4.2] einer der beiden Initiatoren und hervorzuhebenden Promotoren (IBM ist der andere) der Web-Services-Technologie und Standardisierung. Aus diesem Grund ist das .NET Framework sozusagen vom Design her mit den XML- und Web-Services-Technologien verwoben.

Komponenten

Microsoft hat eine *Service-Oriented Application Architecture* für .NET definiert, die folgende Komponenten umfasst:

- UI Components
  UI Components bilden die Endbenutzerschnittstelle (Benutzeroberfläche). Das kann eine Web-Anwendung oder eine Windows-Anwendung sein. User Interfaces werden mit Hilfe von ASP.NET WinForms und/oder WebForms erstellt, mit Funktionen für serverseitige Controls, Plausibilitätsprüfungen, Rendering und Datenformatierung.
- UI Process Components
  In vielen Fällen folgt die Benutzerinteraktion mit dem System einem vordefinierten Prozess. Zum Beispiel gibt der Benutzer erst seine Bestellinformationen (Produktauswahl, Menge) ein, legt dann die Zahlungsmodalitäten fest (Bankverbindung, Kontonummer) und gibt zuletzt Lieferinformationen an (Wunschtermin, Lieferadresse). Um diese logisch aufeinander abgestimmten Zwischenschritte zu synchronisieren und zu orchestrieren, kann man UI Process Components nutzen. Der Prozessfluss und das State Management werden dann in der Benutzerschnittstelle nicht fest verankert.
- Service Interfaces
  Um Geschäftslogik in Form eines Service zur Verfügung zu stellen, muss eine Service-Schnittstelle bereitgestellt werden, die von vielen anderen Service-Nutzern verwendet werden kann. Die Service-Schnittstelle beschreibt Themen wie Format, Protokoll, Security und Ausnahmebehandlung.
- Business Workflows
  Viele Geschäftsprozesse bestehen aus mehreren Schritten, die in der richtigen Reihenfolge ausgeführt werden müssen. Business Workflows definieren und koordinieren langlaufende, mehrschrittige Geschäftsprozesse und können implementiert werden, indem man Business Process Management Tools, z. B. BizTalk Server Orchestration verwendet.
- Business Components
  Mit Business Components können Geschäftsregeln abgebildet oder bestimmte geschäftsrelevante Aufgaben erledigt werden. Business Components implementieren und repräsentieren die Geschäftslogik der Anwendung.
- Business Entities
  In vielen Anwendungen müssen die Daten von einer Schicht zur anderen transportiert werden. Die Daten repräsentieren „Real-World“-Business-Entities wie Produkte oder Bestellungen. Die Business Entities, die intern in der Anwendung genutzt werden, verwenden in der Regel Datenstrukturen wie ADO.NET DataSets, DataReaders oder XML Streams.

– Data Access Components
  In den meisten Anwendungen muss auf Datenbanken zugegriffen werden. Datenzugriffsfunktionen werden aus Gründen der besseren Skalierbarkeit, Konfigurierbarkeit und Konsistenz in einer separaten Schicht implementiert.
– Service Agents
  Business-Komponenten benötigen manchmal Informationen von einem externen Service. Dann wird die Kommunikationsschnittstelle von Service-Agenten korrekt bedient. Sie verbergen die komplizierte Kommunikationsschnittstelle zum externen Service und können Data Format Mapping übernehmen, wenn die eigene Anwendung andere Datenformate als der externe Service benutzt.

.NET Server

Microsoft hat jetzt seine .NET Enterprise Server unter dem Branding *Windows Server System 2003* zusammengefasst. Zur Application Infrastructure gehören SQL Server, Content Management Server, Commerce Server, BizTalk Server und Host Integration Server. Zur Information Worker Infrastructure zählen der Project Server, der Exchange Server und der SharePoint Portal Server. Zur IT Infrastructure gehören Internet Security & Acceleration Server, Systems Management Server, Application Center und Operations Manager.

Beispiel einer Web-Services-Integration

Beispiel einer nahtlosen Integration von Systemen und Services, die bisher vollständig disjunkt waren, ist der direkte Zugang zu Amazon.com aus Microsoft Office. Benutzer können aus Office heraus direkt auf die Funktionen von Amazon zugreifen, ohne einen Web Browser öffnen zu müssen. Die Integration wurde durch Amazons Web Services erreicht. Der Office-Benutzer gelangt von der *Research Task Pane*, verfügbar ab der Office 2003 Edition, direkt zu Amazon. Er erhält Zugriff, ohne dass er das Office-Dokument oder die Mail, an der er gerade arbeitet, vorher schließen muss.

Ohne große manuelle Eingriffe können außerdem Fußnoten, bibliographische Einträge und Designs für Buchumschläge von Amazon nahtlos in Microsoft Dokumente übernommen werden. Die *Research Task Pane* nutzt XML für Abfrage und Navigation von Web-basierter Information aus Office-Anwendungen heraus. Diese Funktion steht Word, Excel, Outlook Messaging und Collaboration, PowerPoint, Access, OneNote, Publisher und Visio zur Verfügung.

IBM

IBM ist mit der *WebSphere*-Produktfamilie Marktführer bei J2EE Application Servern. Mit dem Software-Fokus auf Middleware hat sich IBM besonders auf komplexere und geschäftskritische Lösungen spezialisiert. Zur WebSphere-Produktfamilie [5.4.3] gehören Portal Server, Application Server, Integration Server inclusive BPM und fortgeschrittene, auf Standards basierende Interoperabilität mit anderen Plattformen. Weitere Stärken sind die Realisierung unternehmensübergreifender Business-Transaktionen und -Prozesse, einschließlich der erforderlichen Security. Bei Technologie und

Standardisierung fokussierte sich IBM in den letzten Jahren auf Web Services und Business-Integration.

Der WebSphere Application Server stellt eine J2EE-Technologie-Plattform mit integrierten Tools dar, die eine Reihe von Web-Services-Standards unterstützen wie SOAP, UDDI, WSDL und WS-Security. Die technologische Einbettung von Web Services in WebSphere erlaubt es Applikationen, unter Nutzung dieser Standards dynamisch mit Web Services zu interagieren. Web Services von anderen Herstellern können ebenfalls integriert werden. Außerdem ist der WebSphere Application Server Administrator in der Lage, die Security sowie die Life-Cycle-Attribute solcher Services zu managen. Des Weiteren erlaubt WebSphere die Transformation existierender Applikationen in Web Services.

Die WebSphere-Familie stellt eine Plattform mit außerordentlichem Funktionsreichtum dar, die zunehmend auf SOA und Web-Services-Technologie ausgerichtet wird und BPM einschließt. Der IBM WebSphere Application Server ist eine hochperformante, skalierbare Transaktions-Maschine und von daher bestens geeignet für dynamische e-Business-Lösungen. Aufgrund der offenen Service-Infrastruktur von WebSpere ist diese Plattform besonders als Kernkomponente für einen zuverlässigen und zukunftsorientierten IT-Betrieb geeignet. Gleichzeitig ist sie in der Lage, große Transaktionsvolumina und sichere Transaktionen unter Einschluss von Web Services zu bewältigen.

5.5 Zusammenfassung und Empfehlungen

Erstmals in der IT-Geschichte wird eine neue Architektur (SOA) einvernehmlich von den verschiedenen Technologielagern (Microsoft, IBM, Sun usw.) und Lösungsanbietern (SAP, Siebel usw.) vorangetrieben. Dabei ist bemerkenswert, dass die Marktführer (Microsoft, IBM und SAP) offensichtlich einen besonders engen Schulterschluss anstreben.

Es ist zu erwarten, dass SAP, IBM und Microsoft die angekündigte Interoperabilität sowohl im eigenen Interesse als auch im Sinne ihrer Kundenanforderungen realisieren werden. Dies wird die Position der drei Marktführer weiter stärken und den Mitbewerb in eine schwierige Situation bringen.

Allerdings wird sich das besondere Interesse von Unternehmen allmählich verlagern: von den Anwendungsplattformen und der Middleware hin zu Business-Prozess-Integration und Industrie-spezifischen Anwendungen. Auf diesen Feldern ist in den kommenden Jahren starker Wettbewerb zu erwarten, insbesondere auch zwischen SAP, IBM und Microsoft.

Web Services werden hier als zukünftige Anwendungsentwicklung und geeignete Technologie für die Prozessintegration dominieren. Es ist deshalb wichtig, dass sich Unternehmen frühzeitig mit dieser Thematik auseinandersetzen. Anwendungsintegra-

tion, heute häufig noch durch Punkt-zu-Punkt(Spagetti)-Verbindungen realisiert, wird sukzessive durch moderne Technologien unter Nutzung von Web Services ersetzt.

Unternehmen sollten – wenn nicht schon geschehen – unmittelbar die Planung für eine Service-orientierte Architektur auf Basis von Web Services aufsetzen, und zwar durchgängig für alle Bereiche. So eine strategische Planung wird deutlich machen, gespiegelt an den zukünftigen Anforderungen, für welche Anwendungsklassen sich Web Services am besten eignen. Dabei ist besonders zu beachten, dass Security unbedingt integraler Bestandteil der Strategie und Planung sein sollte. Schulung und Training spielen ebenfalls eine wichtige Rolle, um Technologie und Standards besser zu verstehen und Expertise aufzubauen.

Für erste Implementierungen hat sich immer schon die Strategie *Keep it simple* bewährt. Es wird empfohlen, diese neuen Technologien eher konservativ anzugehen und vor allem geschäftskritische Anwendungen anfangs auszusparen.

Nach einer kürzlich veröffentlichen Analyse der Meta Group werden sich Web Services in Business Solutions in drei Phasen durchsetzen:

– Phase 1 (2003/2004)
  Unternehmen evaluieren Vorteile und Nachteile von Web Services/SOA und bewerten ihre existierende Infrastruktur und EAI-Produktlandschaft. Sie wenden Web Services bereits in internen Integrationsprojekten an und implementieren auf Basis von Web Services einige nicht-kritische Applikationen. Sie fangen an, Roadmaps aufzusetzen und starten erste Projekte, um existierende Architekturen nach SOA zu migrieren .
– Phase 2 (2005/2006)
  IT-Budgets wachsen wieder. Die Mehrheit der Unternehmen wendet dann Web Services an. Web Services werden nun nicht mehr ausschließlich für einfache und statische Services eingesetzt, sondern gestalten zunehmend auch dynamische Abläufe. Externe Partner werden mittels Web-Services-Technologie in unternehmensübergreifende Prozesse eingebunden.
– Phase 3 (2007/2008)
  Das Paradigma „Software als Services“ wird Realität. Anwendungen mit dynamischem Charakter werden unter Einbeziehung von Geschäftspartnern und Kunden aus Web Services orchestriert, und zwar weitgehend automatisiert und ohne Intervention von Personen. SOA und eine integrierte Prozessinfrastruktur werden zur Norm in Großunternehmen. Sogenannte „Late Followers“ werden schließlich auch Web Services adaptieren.

Bedeutung der Professional IT-Service-Provider

Es ist anzunehmen, dass SOA und die Web-Services-Technologie den Trend zum Outsourcing verstärken werden. Die kombinierten Fähigkeiten des professionellen Designs von Geschäftsprozessen mit der Business-Integration und einem breiten Outsourcing-Angebot könnten sich als die Schlüsselfaktoren für erfolgreiche moderne Geschäftslösungen herauskristallisieren. Deshalb wird empfohlen, dass Unternehmen

sich ernsthaft mit der Frage auseinanderzusetzen, inwieweit kompetente IT- und Outsourcing-Service-Provider in Lösungskonzeptionen einzubeziehen sind.

Dabei sollten Service-Provider bevorzugt werden, die technologische Grundlagen von SOA/Web Services beherrschen (Entwicklung und Einsatz), und vor allem Erfahrung in den strategischen Kompetenzfeldern mitbringen: Prozess-Design, Business-Integration und Web-Services-Management (Infrastruktur, Applikationen, Monitoring, Metrics, Security, Certification, Vertragsmanagement, Service Level Agreements usw.). Ebenso von Vorteil dürfte die Plattform-Neutralität von Service-Providern und ihre Expertise in der Interoperabilität von Plattformen sein. Service-Provider sollten auch über ein breites Spektrum von Outsourcing Services verfügen.

6 Security

2005 werden über 80% aller Unternehmen das Internet für ihre Geschäftsprozesse nutzen. Folglich werden immer mehr Firmen mit den Sicherheitsrisiken konfrontiert sein, die mit der Nutzung des Internet verknüpft sind.

Wie in Bild 6.1 dargestellt, waren Hacker im Jahr 2003 aktiver denn je. Nach Angaben des *Computer Emergency Response Team (CERT),* dem Computer Security Clearing-House der Carnegie Mellon University in Pittsburgh [6.1], wurden 68% mehr Störfälle als im Jahr zuvor gemeldet. Insgesamt wurden 137.529 Vorfälle registriert, u.a. Angriffe auf Websites, bösartige Viren und unbefugtes Eindringen in Computernetze. Um die Zahlen in die richtige Perspektive zu rücken: Die 2003 gemeldeten Ereignisse machen immerhin 42% aller Angriffe aus, die seit Beginn der Aufzeichnungen im Jahr 1988 registriert wurden.

Es liegen immer noch nicht genügend Informationen vor, wie gravierend sich Sicherheitszwischenfälle kurz- und langfristig auf das Geschäft auswirken. Unternehmen, insbesondere Kreditkartengesellschaften und Finanzdienstleister, haben natürlich kein Interesse daran, die durch Sicherheitszwischenfälle verursachten Verluste zu veröffentlichen – sie möchten auf keinen Fall ihren guten Ruf aufs Spiel setzen. Experten sind daher der Auffassung, dass Sicherheitsvorfälle oftmals überhaupt nicht gemeldet werden.

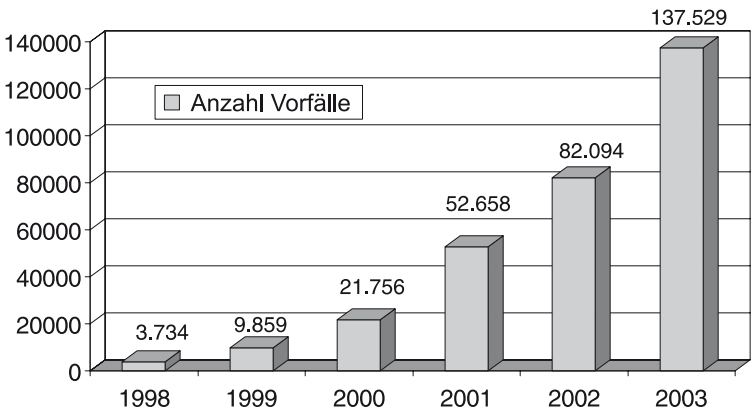


Bild 6.1 Security Incidents Statistics

6.1 Gefahrenquellen und Schwachstellen

Unternehmensübergreifende Prozesse setzen in der Regel voraus, dass Geschäftspartnern und Zulieferern Zugang zu Unternehmensnetzen und -ressourcen gewährt wird. Informationen und Werte des Unternehmens, die bisher streng unter Verschluss gehalten wurden, werden anderen damit zugänglich gemacht.

Wie in Bild 6.2 dargestellt, treten hierbei offensichtliche Sicherheitsrisiken auf, denn ein weltweites und offenes Netz bietet viele potenzielle Angriffspunkte. Die neuen Herausforderungen des drahtlosen Internet-Zugangs und die zunehmende Integration mobiler Mitarbeiter, Geschäftspartner und Kunden haben zudem zur Folge, dass Schwachstellen und Sicherheitslücken vermehrt auftreten. Bedingt durch Service-orientierte Architekturen und Web Services entsteht eine neue Dimension von Risiken für die Geschäftswelt und verstärkte Security-Mechanismen und Maßnahmen werden unverzichtbar.

Je stärker sich die B2C-, B2B- und B2E-Geschäftsprozesse auf offene Netzwerke stützen, desto größer wird auch die Wahrscheinlichkeit, dass sich Personen mit böswilliger Absicht illegal Zugang zu Unternehmenssystemen verschaffen und Schäden anrichten.

Solchen Fälle ist umso schwieriger vorzubeugen, da es den typischen Feind eines Unternehmens nicht gibt. Unzufriedene Arbeitnehmer und Hacker sind zwar die wahrscheinlichsten Angreifer, aber andere Unternehmen und sogar fremde Staaten könnten ebenfalls versuchen, in Systeme einzudringen und wichtige Informationen zu stehlen oder zu manipulieren. Wirtschafts- und Technologiespionage ist eine der am meisten unterschätzten Bedrohungen der Gegenwart.

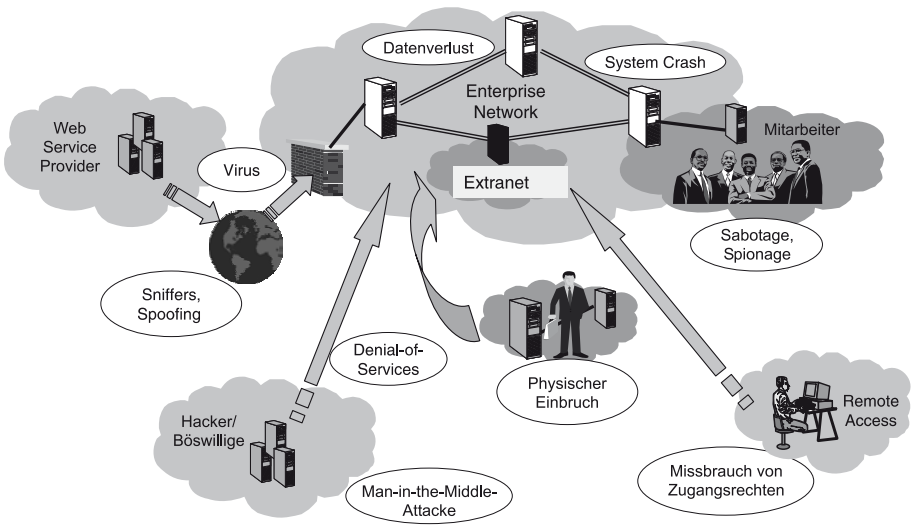


Bild 6.2 Gefahrenquellen in offenen Netzen

Die bekanntesten Angriffsszenarien werden im Folgenden kurz aufgezeigt:

Viren

Viren stellen die häufigste Gefahrenquelle dar. Viren sind ein Programm oder Code, das oder der ohne Kenntnis des Unternehmens auf seine Computer geladen und gegen dessen Willen ausgeführt wird. Viren hängen sich an Programme oder Dateien an. Die meisten können sich selbst replizieren, so dass schnell der gesamte verfügbare Speicherplatz in Beschlag genommen wird. Viele können sich auch selbst über Netze weiterverbreiten.

Packet Sniffer

Packet Sniffer ist eine Software-Anwendung, die unter Zuhilfenahme einer Netzwerkkarte alle Pakete analysiert, die über das Netz gesendet werden. Sniffer werden in Netzen legitim zur Unterstützung bei der Fehlersuche und Verkehrsanalyse eingesetzt. Da jedoch verschiedene Netzanwendungen Daten in Klartext senden (z. B. telnet, FTP, SMTP, POP3), kann ein Packet Sniffer auch sensible Informationen wie Benutzernamen und Passwörter herausfiltern.

IP Spoofing

Bei einem IP-Spoofing-Angriff gibt sich ein Hacker dem angegriffenen IT-System gegenüber als ein vertrauenswürdiger Computer aus. Er kann dies auf zweierlei Weise tun: Entweder verwendet er eine IP-Adresse aus dem Bereich der vertrauenswürdigen IP-Adressen für ein dediziertes Netz, oder er verwendet eine autorisierte externe IP-Adresse, die ebenfalls als vertrauenswürdig eingestuft wird und Zugriff auf genau spezifizierte Ressourcen in einem Netz hat.

IP-Spoofing-Angriffe dienen oft als Ausgangspunkt für andere Angriffe. Das klassische Szenario ist die Einleitung eines Denial-of-Service-Angriffs (DoS) mit gefälschten Absenderadressen, mit dem Ziel, die Identität des Hackers zu verbergen.

Passwortangriffe

Hacker können Passwortangriffe mit verschiedenen Methoden lancieren, zu denen etwa Brute-Force-Attacken, Trojanische Pferde, IP Spoofing und Packet Sniffer zählen. Doch obwohl auch Packet Sniffer und IP Spoofing User Accounts und Passwörter liefern können, bezieht sich der Ausdruck Passwortangriffe meist auf wiederholte Versuche der Identifikation eines User Accounts bzw. Passworts. Diese wiederholten Versuche werden als Brute-Force-Attacken bezeichnet.

Eine Brute-Force-Attacke wird oft mit einem Programm gestartet, das über das Netz ausgeführt wird und versucht, sich bei einem gemeinsam genutzten Betriebsmittel wie etwa einem Server anzumelden. Gelingt es dem Hacker, sich Zugang zu den angegriffenen Ressourcen zu verschaffen, dann hat er dort die gleichen Rechte wie der Benutzer, dessen Account kompromittiert ist. Verfügt der betroffene Account über ausreichende Berechtigungen, kann der Hacker sogenannte Backdoors einrichten, um künf-

tig Zugang zum System zu erhalten, ohne dass ihn Status- oder Passwortänderungen des kompromittierten User Accounts behindern würden.

Denial-of-Service-Angriffe (DoS)

Bei einem DoS-Angriff verschafft sich ein Hacker Zugang zu mehreren Computern, die über das Internet erreichbar sind, und installiert Code auf diesen Systemen. Auf ein Signal des Hackers hin beginnen die Systeme dann, Daten an Websites zu senden, die der Hacker als Angriffsziel gewählt hat. Das plötzliche große Verkehrsaufkommen überlastet die Web Server und betroffene Netze, so dass sich die Performance verschlechtert und die Website letztlich zum Absturz gebracht wird.

Man-in-the-Middle-Angriffe

Ein Man-in-the-Middle-Angriff setzt voraus, dass der Hacker Zugriff auf Pakete hat, die über ein Netz transportiert werden. Eis solcher Hacker könnte beispielsweise ein Mitarbeiter eines ISP (Interner Service-Provider) sein, der Zugriff auf alle Netzpakete hat, die zwischen dem ISP-Netz und beliebigen anderen Netzen übertragen werden. Derartige Attacken werden oft mit Hilfe von Network Packet Sniffern und Routing- und Transportprotokollen ausgeführt. Mögliche Ziele solcher Angriffe sind Diebstahl von Informationen oder Hijacking laufender Sessions, um Zugang zu privaten Netzressourcen zu erhalten. Weitere Ziele können die Verkehrsanalyse zur Ermittlung von Informationen über ein Netz und seine Nutzer, das beschriebene Denial of Service, die Korrumpierung übertragener Daten oder das Einschleusen von gezielten Informationen sein.

Physische Einbrüche

Bei dieser Angriffsform dringen Unbefugte tatsächlich physisch in ein Rechenzentrum ein oder stehlen Geräte. Die Sicherheitsvorkehrungen für Rechenzentren müssen über das einfache Abschließen der Tür hinausgehen. Rechenzentren stellen oft die wichtigsten Vermögenswerte eines Unternehmens dar. Diebstahl von Laptops und PDAs ist ein leidiges Problem, nicht nur wegen der hohen Kosten für Ersatzgeräte, sondern vor allem wegen der gespeicherten, vertraulichen Informationen.

6.2 Security in e-Business Solutions

Security und involvierte Methoden, Maßnahmen, Techniken und Komponenten lassen sich in der Regel nicht von den ansonsten eingesetzten Hardware- und Software-Komponenten abgrenzen, die in e-Business Solutions Verwendung finden. Security-Komponenten sind meist eingebetteter Bestandteil von Hardware oder Software in Mainframes, Servern, Desktops, Laptops, mobilen Geräten, Routern, Switches, Netzzugangskomponenten, Betriebssystemen, Middleware, Standard-Applikationen, vertikalen Applikationen, Web Services und Business-Prozessen. Allerdings schließt dies nicht den zusätzlichen Einsatz diskreter Security-Komponenten wie Crypto-Boxen oder Firewalls aus, die als dedizierte Geräte für besondere Funktionen entwickelt wurden.

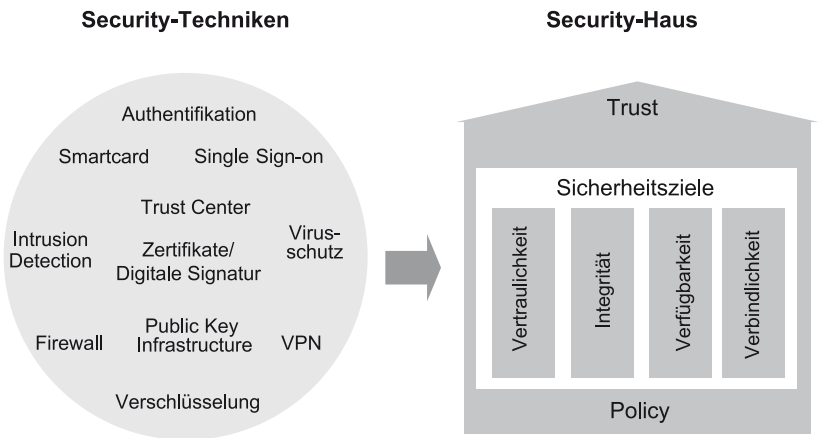


Bild 6.3 Das Security-Haus

Es ist zu betonen, dass jede der oben genannten Lösungskomponenten mit geeigneten Security-Funktionen ausgestattet sein muss, um eine End-to-End Security zu gewährleisten. Letztendlich ist dies eine unverzichtbare Eigenschaft von zuverlässigen e-Business Solutions.

6.2.1 Das Security-Haus

Es ist empfehlenswert, dass sich Unternehmen eine Art Security-Haus zimmern. Bild 6.3 veranschaulicht die Konstruktion dieses Hauses. Die *Policy* als Fundament definiert, wie mit den Werten des Unternehmens umgegangen wird (wer darf was) und *Trust* als das Dach des Hauses stellt das Vertrauen zwischen allen beteiligten Partnern sicher. Die Säulen in der Mitte repräsentieren die *Sicherheitsziele*, die es zu erreichen gilt, um Lösungen sicher zu gestalten. Vielfältige Bausteine, die *Sicherheitstechniken,* helfen dieses Haus zu erstellen. In Bild 6.3 sind die wesentlichen Techniken im Kreis erfasst, dies ist jedoch keine vollständige Aufzählung.

Sicherheitsziele

Informationssicherheit hat viele Facetten: Hauptziele sind Schutz der Vertraulichkeit (Confidentiality) und Geheimhaltung persönlicher Daten (Privacy) sowie Integrität (Integrity) und Verfügbarkeit (Availability) der Informationen, die einem Unternehmen gehören oder die es in Verwahrung hat.

Werden diese Ziele nicht eingehalten, kann dies unter Haftungs- wie auch Imagegesichtspunkten schnell zur Gefährdung eines Unternehmens führen. Die Nachweisbarkeit oder Verbindlichkeit (Non-Repudiation) bei Transaktionen (z. B. Bestellungen) ist ein weiteres unverzichtbares Merkmal im e-Business.

Die genannten Qualitäten der Informationssicherheit können wie folgt definiert werden:

Vertraulichkeit und Geheimhaltung

verhindert die Offenlegung sensibler Informationen gegenüber unbefugten Empfängern und stellt sicher, dass Informationen geheim gehalten werden und nur befugten Personen offen stehen. Vertraulichkeit verringert das Risiko finanzieller Verluste, öffentlicher Bloßstellung oder der rechtlichen Haftbarkeit für unbefugte Offenlegung sensibler, kritischer bzw. persönlicher Informationen oder schließt dieses Risiko völlig aus.

Integrität

gewährleistet die Vollständigkeit und Unversehrtheit von Informationen und schließt aus, dass eine versehentliche oder böswillige Veränderung nicht wahrgenommen wird. Die Integrität von Informationen bietet die Gewähr dafür, dass die betreffenden Informationen authentisch sind und nur auf genau spezifizierte und genehmigte Weise durch befugte Personen geändert werden dürfen. Das Risiko versehentlicher oder absichtlicher Manipulation kritischer Informationen wird dadurch für das Unternehmen verringert oder völlig ausgeschlossen.

Verfügbarkeit

bezieht sich auf die Zugänglichkeit von Systemen und Informationen für befugte Benutzer und ermöglicht, dass Informations- und Kommunikationsdienste zur Nutzung verfügbar sind. Verfügbarkeit stellt sicher, dass Systeme in Betrieb sind und Dienste nicht verweigert werden. Bei nahezu 100-prozentiger Verfügbarkeit von Systemen lässt sich das Risiko von verpassten Geschäftschancen oder Betriebsunterbrechungen wegen Nichtverfügbarkeit von Informationen beträchtlich verringern.

Verbindlichkeit

bedeutet, dass Geschäftsvorgänge nachprüfbar und nachweisbar sind und dass Geschäftspartner einander vertrauen können. Verbindlichkeit ist eine Methode zum Nachweis der Datenübermittlung des Absenders und bestätigt dem Empfänger die Identität des Absenders, so dass keine Seite später die Transaktion abstreiten kann.

Die Bedeutung von Policy und Trust

Security Policy

Die Sicherheitsrichtlinien (Security Policy) bilden die Grundlage für sichere e-Business- und m-Business-Transaktionen. Effektive Sicherheit beginnt mit der Formulierung der Richtlinien für den Zugriff auf Vermögenswerte des Unternehmens. Dadurch wird die ordnungsgemäße Nutzung aller Arten von Werten (Daten, Anwendungen usw.) nach verschiedenen Kategorien betrieblicher Nutzer (Absatzorganisation, Ingenieure, Controller, Marketing-Mitarbeiter usw.) definiert.

Eine Security Policy ist im m-Business angesichts der geschilderten Problemstellungen von allergrößter Bedeutung. Durch die Vielfalt mobiler Endgeräte erhöht sich die Zahl

der Geräte pro Nutzer und damit nehmen auch die Bedrohungen für das Unternehmen zu.

Security Policy und Security Management müssen berücksichtigen, dass Mitarbeiter über mehrere Geräte verfügen und möglicherweise verschiedene Netzbetreiber mit im Spiel sind.

Trust

Vertrauen ist im heutigen Wirtschaftsklima ein wesentlicher Faktor für erfolgreiches Bestehen im Wettbewerb. Vertrauen ist ein Katalysator, der die Nutzung neuer e-Business-Chancen ermöglicht: Erreichen eines größeren Kundenkreises, engere Zusammenarbeit mit Lieferanten, Mitarbeiter-Empowering sowie Erschließen neuer Umsatzquellen. Vertrauen entsteht jedoch nur, wenn alle Partner überzeugt sind, dass jede geschäftsbezogene Interaktion mit höchsten Sicherheitsstandards abgewickelt wird.

Die gebräuchlichsten Sicherheitstechniken

Sicherheitstechniken umfassen ein weites Feld von Technologien. Leser, die sich einen vollständigen Überblick über die Vielfalt der Techniken und Verfahren verschaffen wollen, finden ausführliche Informationen im Buch *IT-Sicherheit. Konzept, Verfahren, Protokolle* [6.2.1].

In den letzten zehn Jahren wurden ausgereifte Sicherheitstechniken entwickelt, mit denen sich die genannten Sicherheitsziele weitgehend erreichen lassen.

Die im Folgenden kurz erläuterten Sicherheitstechniken haben sich bewährt und werden in Geschäftslösungen häufig eingesetzt.

Authentifikation

Die Technik der *Authentifikation* stellt einen Mechanismus für die Identifikation eines Objekts bereit, z. B. das eines Benutzers, eines Systems, einer Anwendung. Nach seiner Authentifikation kann diesem Objekt Zugang zu den gewünschten Diensten gewährt werden, wobei sich seine Aktivitäten überwachen lassen. Authentifikationsmechanismen reichen von der allgemein bekannten Abfrage von User ID und Passwort über digitale Authentifikationszertifikate bis hin zu hochentwickelten biometrischen Systemen, bei denen Benutzer anhand körperlicher Merkmale, etwa ihrer Fingerabdrücke, authentifiziert werden. Authentifikation ist ein fundamentaler Bestandteil jeder Security-Implementierung.

Anti-Virus-Software

Es gibt verschiedene Arten von *Anti-Virus-Software*, von Lösungen für einzelne Geräte bis hin zu solchen, die File- und Messaging Server schützen. Sie alle sind für die Abwehr von Viren erforderlich. Zu einer wirkungsvollen Antivirenstrategie gehören insbesondere regelmäßige Software-Updates zum Schutz vor neuesten Virenmustern (Signaturen) sowie die laufende Aufklärung der Benutzer. Sie müssen sich der Gefahren bewusst werden und Maßnahmen zur Vermeidung der Gefahren ergreifen können.

Von größter Bedeutung ist, dass eine Anti-Viren-Strategie Richtlinien für Konfiguration und Nutzung von Geräten vorgibt. Restriktionen bezüglich der Software, die Mitarbeiter auf ihre Systeme laden dürfen, verhindern das Einschleppen von Viren und ermöglichen eine gezielte Beseitigung im Fall eines Virenbefalls.

Virtual Private Networks

Virtual Private Networks (VPNs) ermöglichen Mitarbeitern den Zugriff auf Unternehmensressourcen, wenn sie sich außerhalb des Unternehmens aufhalten. In der Regel wird dabei das Internet als Zugangs- und Übertragungsmedium genutzt. Verschlüsselungstechnologie und sichere Tunneling-Protokolle sorgen für den privaten Charakter des Netzes, auch wenn die Datenübertragung über öffentliche Telefonnetze oder Mobilnetze erfolgt. Prinzipiell ermöglicht ein VPN den sicheren Austausch von Informationen über ein öffentliches Netz. Dies ist unerlässlich wenn mobile Endgeräte in Mobilnetzen eingesetzt werden.

Firewalls

Eine *Firewall* prüft Daten beim Eintritt in das Unternehmensnetz und blockiert den Verkehr, wenn nicht bestimmte Kriterien erfüllt sind. Es gibt verschiedene Arten von Firewalls, die kombiniert eingesetzt werden können. Ein Proxy Server fängt alle Nachrichten ab, die beim Unternehmensnetz ankommen oder dieses verlassen und verbirgt die Netzadresse des Zielrechners. Ein Paketfilter prüft Daten, die beim Unternehmensnetz ankommen oder dieses verlassen, um sie dann auf Basis bestimmter Kriterien zu akzeptieren oder zurückzuweisen. Ein Application Gateway sichert spezifische Anwendungen. Ein Circuit Level Gateway wendet Sicherheitsmechanismen beim Verbindungsaufbau an. Nach dem Verbindungsaufbau fließt der Netzverkehr ohne weitere Prüfungen.

Intrusion Detection Systems

Anwendungen, die Betriebssysteme und Netzverkehr aktiv auf Angriffe und Sicherheitsverletzungen überwachen, werden *Intrusion Detection Systems (IDS)* genannt. Ein IDS soll nahezu in Echtzeit ein Abbild dessen liefern, was im Unternehmensnetz gerade abläuft. Es gibt zwei Ansätze, um das Eindringen in Firmennetze zu verhindern: netzbasierte und hostbasierte Systeme. Netzbasierte Systeme überwachen (*sniffen*) die Leitung und vergleichen tatsächliche Verkehrsmuster mit einer Liste bekannter Attacken. Hostbasierte Systeme arbeiten mit Software-Agenten, die auf allen Servern installiert sind und Aktivität an eine zentrale Konsole melden. Für eine umfassende Lösung müssen beide Arten von IDS eingesetzt werden. Wie Anti-Virus-Software setzen beide auch die regelmäßige Aktualisierung der Liste bekannter Attacken voraus.

Transportverschlüsselung

Transportverschlüsselung (Transport Encryption) ist in den Standard-Transportprotokollen des Internet, *Transport Layer Security (TLS)* und *Secure Socket Layer (SSL)* implementiert. Für WAP-Anwendungen in Mobilnetzen wurde entsprechend das Wireless Transport Layer Security Protocol (WTLS) entwickelt. Diese Protokolle ermögli-

chen eine sichere Nachrichtenübermittlung und verhindern Mithören (Eavesdropping), Manipulation (Tampering) oder Fälschung von Nachrichten.

Das Transportprotokoll fragmentiert die zu übertragenden Nachrichten in handliche Blöcke, komprimiert die Daten (optional), wendet einen Hashed Message Authentification Code (HMAC) an, verschlüsselt dann das Ergebnis und überträgt es. Die empfangenen Daten werden entschlüsselt, verifiziert, dekomprimiert, reassembliert und dann an höhere Protokollschichten übergeben.

Datenverschlüsselung

Die Datenverschlüsselung dient dem Schutz von Inhalten (Daten, Sprache, Video ect.), die auf beliebigen Geräten, Servern oder Speichermedien verwendet werden oder abgelegt sind. Dabei wird sichergestellt, dass nur befugte Personen, die den geheimen Dechiffrierschlüssel besitzen, auf die Inhalte zugreifen und diese bearbeiten können.

Single Sign-On (SSO)

Hier kann ein Benutzer mit einer einzigen Anmeldung (Single Sign-On) auf jene Ressourcen zugreifen, für die er eine Berechtigung entsprechend den Sicherheitsrichtlinien besitzt. Die Zugangsberechtigung ist unabhängig davon, auf welche Systeme, Anwendungen oder Ressourcen während einer Sitzung oder innerhalb eines bestimmten Zeitrahmens zugegriffen wird.

Zertifikate und digitale Signatur

Eine vertrauenswürdige Institution, d.h. ein *Trust Center (TC)* oder eine *Certification Authority (CA)* weist einer bestimmten Person das Schlüsselpaar zu, generiert die ordnungsgemäßen Zertifikate und verteilt diese (siehe Public Key Infrastruktur). *Digitale Zertifikate* dienen zur Generierung digitaler Signaturen, die verwendet werden, um die Integrität von Daten/Inhalten zu garantieren. *Digitale Signaturen* sind elektronische Unterschriften, die mit den unterzeichneten Daten so verknüpft werden, dass Manipulationen nicht unbemerkt bleiben und der Absender eindeutig identifiziert werden kann.

Digitale Signaturen werden auch zur Benutzer-Authentifikation verwendet. Durch andere Formen elektronischer Signaturen wie z. B. PINs wird die Datenintegrität nicht geschützt. Zur Erstellung einer digitalen Signatur verwendet der Unterzeichner einen privaten Schlüssel (*Private Key*), der nur ihm gehört. Für diesen privaten Schlüssel gibt es einen passenden öffentlichen Schlüssel (*Public Key*), der zur Verifizierung der Signatur verwendet wird.

Public Key Infrastructure

Die *Public Key Infrastructure (PKI)* ist eine Infrastruktur, die sowohl zur Authentifikation als auch zur Verschlüsselung dient. Die Infrastruktur kombiniert Software, Verschlüsselungstechnologien und Dienste, um Datenübertragungen über Netze und e-Business-Transaktionen zu schützen.

PKI umfasst ein System digitaler Zertifikate, die zur Sicherstellung der Datenintegrität und zur Bestätigung der Identität des Absenders dienen sowie ein Trust Center, das solche Zertifikate herausgibt. Verteildienste stellen eine netzweite und aktuelle Verfügbarkeit gültiger Zertifikate sicher.

Folgende Informationswerte werden durch eine PKI umfassend geschützt: Authentifikation (Identitätsprüfung anhand eines digitalen Zertifikats), Verifizierung der Integrität (Sicherstellung, dass Nachrichten nicht verändert oder Daten nicht korrumpiert wurden) und Sicherstellung der Vertraulichkeit (Schutz gegen das Abfangen von Informationen während der Übermittlung).

Smartcards

Geheime Daten wie z. B. private Schlüssel werden am besten in manipulationssicheren Modulen gespeichert. *Smartcards* repräsentieren solche Module. Sie basieren auf einer geschützten *(Tamper-resistant)* Chiptechnologie, die Hardware- und Software-Schutzvorkehrungen umfasst und dadurch ein sehr hohes Sicherheitsniveau erreicht. Smartcards sind *Chipcards (ICC, Integrated Circuit Cards),* die eine CPU beinhalten. Sie sind seit mehr als zehn Jahren standardisiert (ISO 7816).

Im Prinzip ist die Smartcard ein multifunktionales Werkzeug, das sich ideal für die Realisierung von Anwendungen wie Firmen- oder Personalausweis eignet, die wiederum eine Vielzahl von Verwendungsmöglichkeiten umfassen (Zutrittskontrolle für Gebäude und Räume, bargeldlose Bezahlung im Mitarbeiterrestaurant, Benutzer-Authentifikation vor dem Zugriff auf Anwendungen und Netze, digitale Signaturen zum Nachweis des Ursprungs von elektronischen Dokumenten).

6.2.2 Der holistische Lösungsansatz

Die aktuellen Informationssicherheitskonzepte sind vor allem auf eine technische IT-Security ausgerichtet. Technische, meist isolierte Sicherheitslösungen reichen jedoch allein nicht mehr aus. Vielmehr müssen zur Realisierung einer wirklich umfassenden Informationssicherheitspolitik technische, personelle und betriebliche Sicherheitsmaßnahmen kombiniert werden. Das bedeutet, dass in einem Unternehmen die unterschiedlichen Sichtweisen der Informationssicherheit und die entsprechenden Anforderungen zu beachten sind.

Ein *holistischer* Security-Lösungsansatz berücksichtigt alle Perspektiven und kombiniert auf Basis eines Security-Standardportfolios geeignete Maßnahmen zur ganzheitlichen Sicherstellung der gesteckten Sicherheitsziele.

Die verschiedenen Perspektiven des Unternehmens

Sicht der Unternehmensleitung

Hier geht es um die Verantwortung des Vorstands. Diese Perspektive betrifft das Unternehmen als Ganzes und befasst sich mit den Verpflichtungen gegenüber Mitarbeitern, Aktionären und Öffentlichkeit und ist verantwortlich für Gesetzeskonformität. Die

Informationssicherheit muss den übergeordneten Zielen des Unternehmens folgen. Die Gewährleistung der Informationssicherheit durch das Unternehmen im Ganzen liegt in der Verantwortung des Vorstands. Dazu gehört auch die Vorgabe von Rahmenbedingungen für den Katastrophenfall.

Sicht der Prozess-Verantwortlichen

Prozess-Verantwortliche haben die Aufgabe, einen effizienten und reibungslosen Ablauf von Business-Prozessen sicherzustellen. Um dies zu gewährleisten, müssen zunächst alle Risiken, die die Geschäftsprozesse gefährden können, aber auch die finanziellen Risiken richtig eingeschätzt werden. In einem zweiten Schritt geht es darum, geeignete technische, organisatorische und personelle Gegenmaßnahmen zur Reduzierung dieser Risiken zu veranlassen.

IT-Sicht

Die allgemeine Rolle des CIO besteht in der Bereitstellung von IT-Infrastrukturen und der zugehörigen Dienstleistungen zur Unterstützung der Unternehmensziele und Geschäftsprozesse. Die Bereitstellung dieser Infrastrukturen und Dienstleistungen muss Wirtschaftlichkeitsprinzipien folgen. Effizienz lässt sich am besten durch Vermeidung von spezifischen Einzellösungen und unkoordinierten Reaktionen erreichen. Stattdessen ist ein Übergang zu standardisierten Security-Architekturen und -Diensten und die Festlegung auf ein Standard-Security-Portfolio erforderlich. Dieses Portfolio muss mit der Unternehmensstrategie und den Geschäftsprozessen des Unternehmens in Einklang stehen, um heutigen und zukünftigen Informations- und Kommunikationsmodalitäten zu entsprechen.

Information Security Management System

Ein Information Security Management System hat die Gewährleistung der Informationssicherheit und die Transparenz des aktuellen Sicherheitsstatus für die Unternehmensführung zum Ziel.

Ein *Information Security Management System (ISMS)* besteht aus Dokumenten, in denen die verschiedenen Geschäftsprozesse und IT-Security-Verfahren in definierten Kategorien (z. B. Zugangskontrolle, Personensicherheit) beschrieben werden. Das ISMS dient zur Orientierung für das Personal und liefert der Unternehmensführung Informationen über die aktuelle Wirksamkeit aller Sicherheitsmaßnahmen. Voraussetzung für die Effektivität des ISMS ist zum einen die richtige Dimensionierung und zum anderen die klare Definition seiner Grenzen. Größere Unternehmen sollten mehrere separate ISMS etablieren, die vom lokalen Management gesteuert und kontrolliert und dann auf höherer Ebene zusammengefasst werden.

Der Prozess eines Managementsystems mit dem Fokus auf Sicherheit ähnelt im Übrigen stark dem eines Managementsystems für Qualitätssicherung. Viele Organisationen verfügen über ein aktives Qualitäts-Management-System, das regelmäßigen Audits nach Normen wie etwa ISO 9001 unterzogen wird. Mit ISO 17799 wird dieses Prinzip auf den Bereich der Informationssicherheit ausgedehnt. Eine formelle Zertifizierung ist

nicht unbedingt erforderlich, um aus der Anwendung des ISMS Nutzen ziehen zu können. Ein methodischer Ansatz, mit dem eine formelle Zertifizierung auch später noch möglich wäre, ist allerdings empfehlenswert.

Ein ISMS wird umgesetzt, indem zunächst die aktuellen Sicherheitslücken entsprechend den Kategorien von ISO 17799 festgestellt und anschließend geeignete Schritte zur Zielerreichung definiert werden. Darüber hinaus wird eine unternehmensweite Security Policy herausgegeben und mit der Beteiligung des oberen Managements werden Verantwortlichkeiten festgelegt, um die Erreichnug der Ziele des ISMS sicherzustellen.

Das holistische Konzept

Ein *holistisches (ganzheitliches) Security-Konzept* berücksichtigt die vorher erwähnten Unternehmensperspektiven und umfasst ein Portfolio von standardisierten Security-Architekturen, Komponenten, Services und Policies. Ein solches Konzept stellt eine zuverlässige Implementierung sicherer Business-Prozesse entlang der Wertschöpfungskette von der Beratung bis zum Betrieb sicher.

Heutige Geschäftsszenarien sind durch rasche Veränderungen und ständig neue Anforderungen gekennzeichnet, wie zunehmender mobiler Einsatz von Mitarbeitern, Entwicklung neuer Kundenkanäle, Integration von Lieferkettenpartnern, Gründung neuer Niederlassungen und so weiter. Unternehmen müssen sich mit vielfältigen Bedrohungen und Gefahren auseinandersetzen: Sabotage, Spionage, versehentliche Schadensvorfälle, Verlust von Vermögenswerten des Unternehmens, Gefährdung von Mitarbeitern, Störung geschäftskritischer Prozesse.

Bild 6.4 veranschaulicht die Zusammenhänge: verschiedene Unternehmenssichten und die korrespondierenden Security-Maßnahmen, die sich auf die I&C-Infrastruktur, die

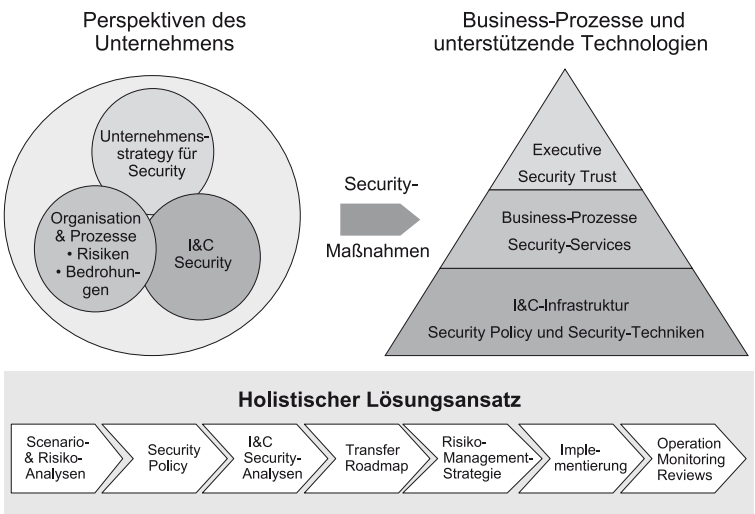


Bild 6.4 Der holistische Security-Lösungsansatz

Prozessebene und die Vorstandsebene auswirken, sowie die erforderlichen Prozessschritte, die im Einzelnen zu vollziehen sind, um eine ganzheitliche Security-Lösung zu verwirklichen.

Um zukunftssichere Security-Lösungen umsetzen zu können, müssen die Szenarien, Geschäftsprozesse und I&C-Infrastruktur eines Kunden erfasst und entsprechende Security-Maßnahmen systematisch, gemäß der in Bild 6.4 dargestellten Prozessschritte, evaluiert werden.

Dabei sind u.a. folgende Schlüsselfragen zu klären:

- Risikoanalyse von Geschäftsprozessen: Was sind die Werte des zu schützenden Geschäftsprozesses? Vor welchen Risiken muss geschützt werden? Wie lauten die Prioritäten? Welchen Grundsätzen ist zu folgen?
- Sicherheitsrichtlinien (Security Policy) für Geschäftsprozesse: Wie sollen die beteiligten Personen Sicherheit praktisch handhaben? Wer ist wofür verantwortlich? Welche Auditing-, Meldungs- und Überwachungsmaßnahmen gibt es?
- Sicherheitsanalyse der bestehenden I&C-Infrastruktur und -Anwendungen: Was ist der aktuelle Sicherheitsstatus? Welches sind die Schwächen und Bedrohungen, für die sinnvolle Maßnahmen erforderlich sind? Welche ergänzenden Maßnahmen sind infolge der vorausgegangenen Beurteilungen notwendig?
- Transferplan und Security Roadmap: Aus welchen Komponenten soll das zukünftige Security-Portfolio bestehen? Wie soll die Security-Architektur aussehen? Welche Techniken sollen eingesetzt werden? Welcher Nutzen und welche Kosten sind voraussichtlich mit den einzelnen Maßnahmen verbunden? Welche Prioritäten gelten für die verschiedenen Szenarien? Wie sollen die Maßnahmen bezahlt werden? Wer kann die Maßnahmen umsetzen und wann? Wie sehen die Auswirkungen auf die Geschäftsprozesse aus?
- Risiko-Management-Strategie: Wie ist bei Schäden vorzugehen, die trotz Schutzmaßnahmen aufgetreten sind? Wie werden unvorhersehbare Ereignisse behandelt? Wie sieht das Eskalationsverfahren aus?
- Implementierung: Wie sieht der Entwicklungsprozess aus und soll dieser in den Prozess der Anwendungsentwicklung integriert werden? Wie wird die Migration und Integration in den laufenden Betrieb gelöst?
- Betrieb, Überwachung, Reviews, Audits, Zertifizierung: Wie kann gewährleistet werden, dass das erreichte Sicherheitsniveau genau dokumentiert und aufrechterhalten wird? Wie kann gewährleistet werden, dass proaktive und geeignete Sicherheitsvorkehrungen für neue Szenarien oder sich wandelnde Geschäftsprozesse berücksichtigt werden?

Security Policy und Security Roadmap sind die Eckpfeiler dieses Prozesses. Genau dort sollte die Unternehmensführung eingebunden werden und Strategie und maßgebliche Bedingungen klar definieren. Dies wird unternehmensweit zu einem einheitlichen Verständnis der Problematik beitragen und die Grundlage für die Ableitung geeigneter Ziele und Scorecards darstellen.

Risiko-Management

Geschäftsprozesse werden immer mehr von der Informationstechnologie abhängig. Das bedeutet, dass ein IT-Ausfall zu hohen Verlusten oder noch dramatischeren Konsequenzen für ein Unternehmen führen kann.

Durch die verheerenden Terroranschläge hat sich in der Versicherungspraxis vieles geändert. Erst- und Rückversicherer haben erkannt, dass die starke Nutzung internationaler Netzwerke unter Umständen Leistungsansprüche in Milliardenhöhe nach sich ziehen kann. Rückversicherungsunternehmen stornierten daher Versicherungsverträge mit Schadensabdeckung bei Ausfällen von IT-Systemen. Die Abdeckung dieses Risikos wurde auf Erstversicherer abgewälzt. Doch auch viele von ihnen stuften das Risiko als zu hoch ein, so dass sie Verträge ebenfalls annullierten. Auf Grund dieser Entwicklung tragen Unternehmen heute mehr denn je die Verantwortung für eigene Vorsorgemaßnahmen und das Thema Sicherheit rückt in ein neues Licht.

Die IT-Infrastruktur ist ein wesentliches Kriterium für die Stabilität und Verfügbarkeit der meisten Geschäftsprozesse. Gesteigerte Verfügbarkeit bringt jedoch auch höhere IT-Investitionen und Betriebskosten mit sich. Wie in Bild 6.5 dargestellt, soll ein effizienter Schutz bei möglichst niedrigen Kosten erreicht werden. Hier geht es um die Kunst, die richtige Balance zwischen mangelhaftem und übertriebenem Schutz zu finden.

Eine konsequente Notfallplanung mit sofortigem Übergang auf eingeschränkte Fortführung des Geschäfts (*Desaster Recovery* und *Business Continuity)* ist eine ganz wichtige Aufgabe für Unternehmen, die das Risiko-Management ernst nehmen.

Eine solche Notfallplanung ist in der Regel ein dreistufiger Prozess:

- Durchführung einer Analyse zur Eingrenzung kritischer Prozesse, Ermittlung und Priorisierung der Risiken für diese Prozesse sowie Festlegung von Richtlinien zur Vermeidung oder Reduzierung der Risiken.
- Entwicklung eines Desaster-Recovery-Plans für geschäftskritische Systeme und Ressourcen. Dies umfasst die Bildung von Recovery-Teams, die Einrichtung von Benachrichtigungsabläufen, die Bestimmung von Besprechungsorten, die Hardware- und Software-Bestandsverfolgung, die schnelle Verfügbarkeit von Kontaktinformationen von Lieferanten sowie klar definierte Backup- und Recovery-Techniken.
- Festlegung von Trainings- und Erprobungsintervallen für das Disaster Recovery Team und den Business-Continuity-Plan, so dass gegebenenfalls Änderungen vorgenommen werden können und ständig die Gewissheit besteht, dass der Plan erprobt ist und auch im Chaos funktioniert.

Die Disaster-Recovery-Planung ist eine komplexe Aufgabe. Gleichwohl ist es von besonderer Bedeutung, dass der Plan einfach und praktikabel für die Ausführenden bleibt. Im Notfall muss schnell und unkompliziert gehandelt werden.

Abhängig von *Security-Strategie* und *Risiko-Management* müssen Unternehmen die optimale Balance zwischen Kosten und Risiko herausfinden, d.h. wie hoch muss ein sinnvolles Investment in Security-Maßnahmen sein und wie wird mit den verbleiben-

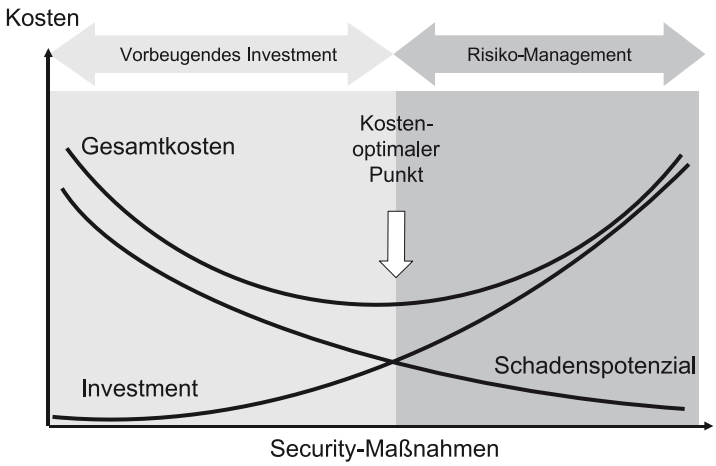


Bild 6.5 Kosten-Risiko-Optimierung

den Risiken umgegangen. Dabei bedeutet Risiko die Abschätzung und Gewichtung von Gefahren und Schwachstellen, denen die Werte eines Unternehmens ausgesetzt sind.

Bild 6.6 zeigt einen systematischen Ansatz, wie Risiken klassifiziert werden und wie mit unterschiedlichen Risikogruppen umzugehen ist.

Die Unterscheidung zwischen eindeutig identifizierbaren Risiken und solchen, die nicht vorhersehbar sind, aber als Risiken angenommen werden müssen, ist sinnvoll. Auch wenn ein Unternehmen Vorsorge für Risiken getroffen hat (z. B. durch Bildung von Rückstellungen), muss es sich darüber im Klaren sein, dass Risiken verbleiben, die nicht voraussehbar sind und akzeptiert werden müssen. Es kann auch durchaus ange-

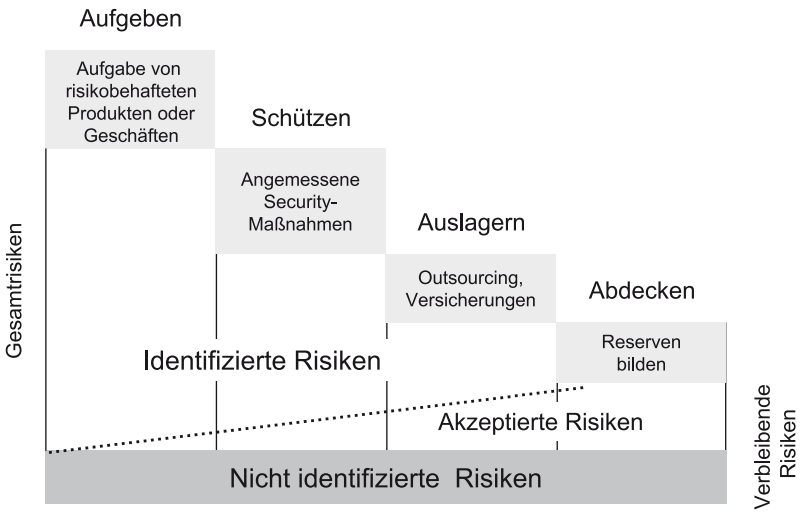


Bild 6.6 Management von Risiken

messen sein, auf sehr risikoreiche Geschäftsaktivitäten ganz zu verzichten, wenn dadurch die Bedrohung des Kerngeschäfts vermieden werden kann.

In der Regel lässt sich der weitaus größte Teil der identifizierbaren Risiken durch adäquate organisatorische, persönliche und technische Security-Maßnahmen eingrenzen. Dazu gehört auch, dass Risiken durch Versicherungen abgedeckt oder von Fremdfirmen übernommen werden. Spezialisierte Security-Service-Provider bieten *Managed Security Services* an oder übernehmen ganze Geschäftsprozesse in ihre Verantwortung.

Managed Security Services

End-to-End Security in e-Business-Prozessen ist ein komplexes, aber unverzichtbares Thema. Immer mehr Firmen entscheiden sich deshalb für die Inanspruchnahme von *Managed Security Services*, die von spezialisierten Service-Providern angeboten werden. Es liegt auf der Hand, dass Security-Aufgaben von Experten viel kompetenter und zuverlässiger erledigt werden können als von Unternehmen, deren Kerngeschäft auf ganz anderem Gebiet liegt.

Erfahrene Security-Diensteanbieter sind oftmals in der Lage, Schaden durch proaktive Maßnahmen abzuwenden, sparen dadurch Geld und fördern die Reputation von Unternehmen.

Das Beispiel des *Slammer Worm* kann dies veranschaulichen.

Die plötzliche Verbreitung des Slammer Worm verursachte in vielen Unternehmen einen riesigen Schaden, der durch präventive Maßnahmen zu vermeiden gewesen wäre, da entsprechende Hinweise bereits sechs Monate vorher veröffentlicht wurden.

In den frühen Morgenstunden (USA) des 25. Januar 2003 entdeckten Netzadministratoren den Slammer Worm. In nur wenigen Minuten hatte sich der Wurm über die ganze Welt verbreitet, alle 8,5 Sekunden verdoppelte sich die Zahl der infizierten Hosts. Zehn Minuten nach seinem Ausbruch hatte Slammer mehr als 90% der nicht geschützten Hosts befallen. Mit Slammer wurde eine Schwachstelle in Microsofts SQL Server ausgenutzt. Das wirkte sich auf Windows NT-, 2000- und XP-Systeme aus, auf denen SQL Server 2000 abliefen, ohne dass die entsprechenden Patches eingefahren waren.

Der Slammer Worm verlangsamte durch das Scannen von IP-Adressen den Internet-Verkehr massiv. Das verursachte einen Schaden in der Größenordnung von $ 1 Milliarde durch erhebliche Störungen insbesondere in den Finanznetzen, einschließlich der angeschlossenen Geldautomaten und Kreditkarten-Validierungssysteme.

Unternehmen können sich derartige Probleme ersparen, wenn sie Managed Security Services in Anspruch nehmen.

Kompetente Service-Provider bieten Managed Security Services an, die beispielweise folgendes Portfolio umfassen:

– Aufbereitung der Information-Security-Richtlinien (Policies), Security-Strategie und Security Roadmap, zugeschnitten auf die spezifischen Anforderungen des Unternehmens

- Management und Monitoring von Firewalls und VPN-Lösungen, um bösartige Angriffe schnell erkennen und abwehren zu können
- Unterstützung durch Experten bei Implementierung und Wartung adäquater Konfigurationen zur Sicherstellung von Verfügbarkeit, Integrität und Vertraulichkeit für Netze und Daten
- Echtzeit-Monitoring und Analysen bei Alarmen
- Security-Management, das durch Fernsteuerung und Wartung unterstützt werden kann und System-Updates sowie Updates von Virensignaturen einschließt
- Evaluierung und Scannen von Systemen, die direkt mit dem Internet verbunden sind wie Firewalls, Webs und Mail Server, um Viren und nicht autorisierte Zugriffe zu erkennen und unerlaubte Manipulationen und Diebstahl zu verhindern
- Bewertung der Security-Maßnahmen in Bezug auf die Einhaltung der Security Policy
- Eliminieren von Schwachstellen, die das Geschäft beeinträchtigen oder beschädigen können.

Handlungsoptionen für Unternehmen

Mit der Perspektive auf eine holistische Security-Lösung sollten Unternehmen Schritt für Schritt entlang der Wertschöpfungskette (Beratung, Design, Implementierung, Betrieb und Wartung) vorgehen.

Dabei sollten die verschiedenen Handlungsoptionen wohl bedacht werden.

- Die erste Option könnte bedeuten, dass eine eigene Organisation innerhalb des Unternehmens sämtliche Security Services selbst anbietet und verantwortet.
- Eine andere Option sieht vor, dass Managed Security Services in Anspruch genommen werden, d.h. die Vergabe von definierten Services (Outtasking) oder das Outsourcing an Service-Provider auf der Basis vereinbarter Leistungen (Service Level Agreements).
- Eine weitere Option ist das Business Process Outsourcing, das bedeutet, dass ein Service-Provider die Abwicklung und Verantwortung für ganze Geschäftsprozesse übernimmt, z. B. für Personalprozesse oder andere Prozesse einschließlich der Sicherstellung einer End-to-End Security.
- Noch eine Option ist das strategische Outsourcing, was eine komplette Ausgliederung der I&C-Aktivitäten samt Unternehmenswerten und Angestellten bedeutet und die Übernahme bestehender Verträge umfasst.

Sicherlich sind auch Kombinationen dieser Optionen überlegenswert.

Entsprechend dieser Optionen haben auch Security-Service-Provider ihre Angebote strukturiert. Die einen fokussieren mehr auf Security-Produkte und dazu passende Services wie z. B. Entrust und Symantec, die anderen leisten primär IT-Unterstützung für Geschäftsprozesse mit eingebetteter Security und korrespondierenden Security Services wie z. B. IBM Global Services und Siemens Business Services.

Beispiel: Security Portfolio eines Security-Service-Providers

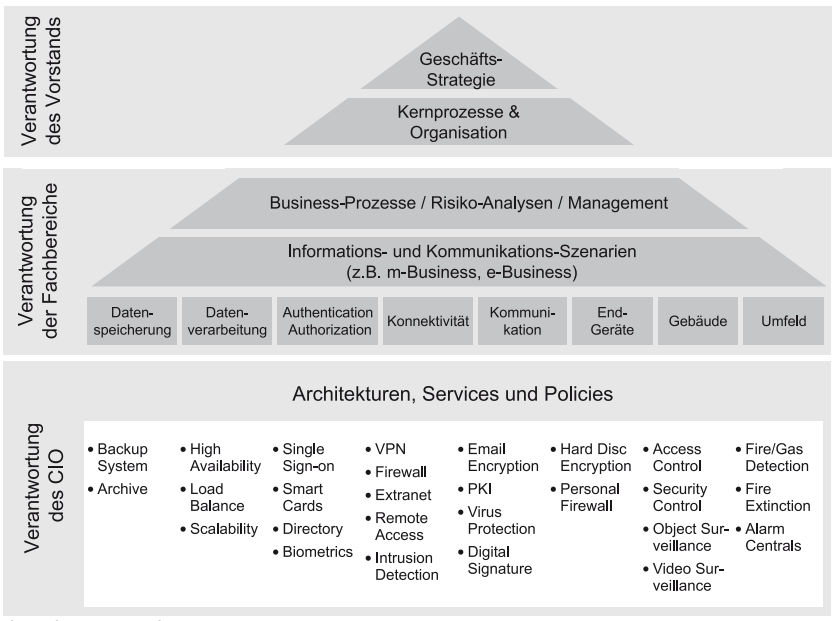
Siemens Business Services verfolgt den Ansatz einer holistischen Security-Lösung und bietet Services entlang der gesamten Wertschöpfungskette. Als Beispiel ist in Bild 6.7 das Security Portfolio von *Siemens Business Services* [6.2.2] dargestellt.

Das Portfolio adressiert drei unterschiedliche Verantwortungsebenen: die IT-Organisation (CIO), die geschäftsführenden Einheiten und die Vorstandsebene.

Das Portfolio der CIO-Ebene enthält I&C-Security-Architektur, Services, Policies und Security-Produkte. Dies umfasst ein weites Feld von Backup-Systemen über Smartcards, VPNs, digitale Signaturen, PKI, Intrusion Detection, Single Sign-on usw. bis zu Überwachungssystemen. Security-Technologien und Produkte von Partnern sind in das Portfolio von Siemens Business Services als Bausteine eingebunden.

Das Portfolio für die Geschäftsbereiche und Fachabteilungen berücksichtigt die unterschiedlichen Branchenspezifika sowie die Anforderungen an Kommunikation, Intranet-Zugang, Geräte, Verarbeitung, Integration und Umfeld. Es umfasst Methoden und Services für Risiko-Analysen und Risiko-Management.

Das Angebot für die Vorstandsebene besteht aus der Ausarbeitung einer Security-Strategie, die sich an der Geschäftsstrategie des Unternehmens ausrichtet und sich mit den Verpflichtungen gegenüber Aktionären, Mitarbeitern und der Gesellschaft sowie mit der Verantwortung für Gesetzeskonformität befasst. Des Weiteren schließt eine Security-Strategie Rahmenvorgaben für Kernprozesse und die Festlegung organisatorischer Verantwortungen ein.



Source: Siemens Business Services

Bild 6.7 Security Portfolio

Beispiel: Interdisziplinäres Portfolio

Ein besonderes Beispiel eines Security-Service-Providers mit interdisziplinärem Portfolio ist das Institut für Sichere Telekooperation (SIT[6.2.3]) der *Fraunhofer Gesellschaft* in Deutschland. SIT kombiniert die eigene Kompetenz in IT- und Telekommunikationstechnologien mit sozialer, ökonomischer, organisatorischer und rechtlicher Expertise von Partnern aus Forschung, Industrie und Verwaltung, um Lösungen zu produzieren, die intuitiv nutzbar, sicher und verlässlich, standardisiert und damit global einsetzbar sowie rechtlich und sozial verträglich und somit breit akzeptierbar sind.

6.2.3 Security-Schwerpunktthemen

Wie auf den vorangegangenen Seiten dargestellt, ist die Security im Kontext e-Business ein Thema mit vielen Facetten und Schwerpunkten. Unternehmen müssen diese Problematik verstehen, um richtige Entscheidungen treffen zu können. Beispiele wie die Einführung einer PKI oder ein unternehmensübergreifendes Identity Management, das Kunden, Partner und Mitarbeiter einschließt, zeigen die Spannweite. Im Folgenden werden drei Schwerpunktthemen näher erläutert, mit denen sich die meisten Unternehmen heute auseinandersetzen müssen (Zusammenfassung in Bild 6.8).

Mobile Security

Wenngleich mobile Internet-Anwendungen nicht ganz so erfolgreich gestartet sind wie ursprüngliche Prognosen erwarten ließen, so ist Mobility mit Zugang zu Unternehmensressourcen über das Internet von jedem Ort aus doch ein offensichtlicher Trend, der sich mit innovativen mobilen Geräten, höheren Bandbreiten und vor allem verbes-

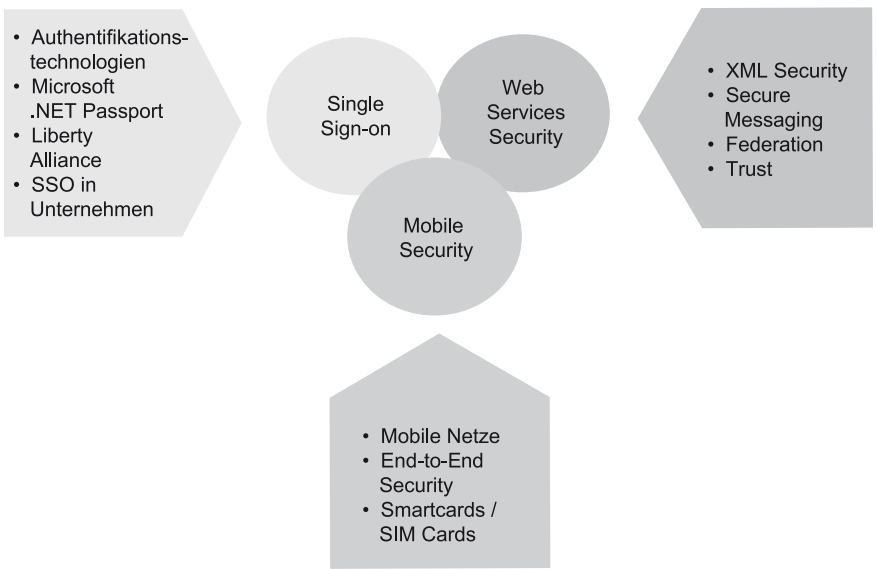


Bild 6.8 Security-Schwerpunktthemen

serter Security noch verstärken wird. Die Security-Herausforderungen sind jedoch deutlich größer als bei vergleichbaren Lösungen im leitungsgebundenen Internet.

Voraussetzung sind Security und Zuverlässigkeit jeder einzelnen Komponente, die in einen Prozess eingebunden ist. Maßgeblich ist eine End-to-End-Sicherheit sämtlicher Transaktionen sowie ein uneingeschränktes Vertrauen, das Kunden und Partner dem Unternehmen entgegenbringen. Die geeigneten End-to-End-Security-Maßnahmen ergeben sich aus einer genauen Risikobewertung der Geschäftsprozesse.

Unternehmen müssen sich den Mobility-Herausforderungen stellen. Die Gewährleistung der Sicherheit von Daten und Transaktionen unter Einschluss der mobilen Geräte, der Mobilnetze, des Internets und der Server umfasst vielfältige Security-Maßnahmen auf verschiedenen Ebenen. Smartcards und SIM Cards können wichtige Komponenten sein, um diese hohen Security-Erwartungen zu erfüllen.

Mobile Security wird in Kapitel 6.3 ausführlich erläutert.

Single Sign-on

Eine zunehmende Diskrepanz zeichnet sich ab zwischen der erforderlichen Offenheit in den Geschäftsbeziehungen und den existierenden IT-Infrastrukturen, die den zukünftigen Security-Anforderungen nicht mehr gerecht werden. Unternehmen können nicht umhin, ihren Geschäftspartnern immer mehr Zugang zu einzelnen Daten und Anwendungen zu gewähren, was aber mit traditionellen Firewall-Strukturen so nicht mehr zu managen ist.

Für die verschiedenen Nutzergruppen mit unterschiedlichen Business-Profilen gilt es, Authentifikations- und Autorisierungsmechanismen zur Verfügung zu stellen, um gezielt Unternehmensressourcen zugänglich zu machen. Diese Mechanismen sollen kosteneffizient und einfach zu handhaben sein. Web-basierte Single-Sign-on-Authentifikationssysteme reduzieren die Managementkosten erheblich und vereinfachen zudem die Anwendung, da der leidige Ärger mit der Vielfalt von Passwörtern vermieden wird.

Die erforderliche Stärke der eingesetzten Authentifikationsmechanismen hängt von den Risiken ab, die mit den jeweiligen Prozessen, Services und Anwendungen verbunden sind. Eine Rolle spielt sicher auch der Aufwand, um diese Risiken möglichst gering zu halten.

Bei Web-basierten Single-Sign-on-Lösungen können zwei Klassen unterschieden werden: Internet Single Sign-on Services wie Microsoft Passport bzw. Lösungen, die den Spezifikationen des Liberty Alliance Projekts entsprechen und Single-Sign-on-Lösungen, die in den Anwendungsplattformen von Unternehmen direkt integriert sind.

Details hierzu werden in Kapitel 6.4 behandelt.

Web Services Security

Web Services erlauben eine Verbindung von Anwendungen über das Internet sowohl innerhalb von Organisationen als auch unternehmensübergreifend. Der Nutzen solch

einer lose gekoppelten, sprachneutralen und plattformunabhängigen Softwaretechnologie wird immer offensichtlicher. Bedenken wegen unzureichender Security haben allerdings die weite Verbreitung von Web Services bislang behindert.

Ein Reihe von Security-Standards für Web Services wurde mittlerweile definiert. Die Standardisierung ist zwar noch im Fluss, jedoch sind nun einige Security-Produkte für Web Services z. B. auf Basis der XML Security auf dem Markt und einsetzbar.

Web Services Security basiert auf einem Mechanismus, der Security Token mit SOAP Messages verbindet, um auf diese Weise zuverlässige und sichere Nachrichten zu garantieren.

Trust spielt bei der Anwendung von Web Services eine ganz besondere Rolle, da die beteiligten Partner sich möglicherweise nicht kennen. Trust-Modelle schließen sowohl direkte Beziehungen zwischen den beteiligten Partnern ein als auch Beziehungen, die über Dritte (Broker) vermittelt werden. Die Umsetzung einer Trust Policy und die Gestaltung von sogenanntern föderierten Trust-Szenarien sind die größten Herausforderungen, die es noch zu lösen gilt.

Kapitel 6.5 befasst sich mit den Security-Themen bei Web Services.

6.3 Mobile End-to-End Security

Moderne e-Business-Architekturen unterstützen zunehmend mobile Geräte und entwickeln sich nach und nach zu integrierten e- und m-Business-Architekturen. In der absehbaren Zukunft werden m-Business-Lösungen auf vorhandenen e-Business-Architekturen aufsetzen. M-Business weist zwar spezifische Merkmale auf, basiert im Übrigen aber auf der bekannten Multi-Tier-Architektur: Trennung der Kommunikations-/Präsentations- und anderer Middleware-Services (Front-End) von der Geschäftsprozess-Implementierung und den Unternehmensressourcen (Back-End).

Zukünftige Front-End-Plattformen (Web/Portal Server, Application Server) unterstützen sowohl drahtgebundene als auch drahtlose Geräte, wie in Bild 6.9 dargestellt. Diese Art von Plattform kann als integrierte Web-/WAP-Plattform beschrieben werden, da gemeinsame Portal-Services und Business-Logik für drahtgebundene und drahtlose Kommunikationskanäle zur Verfügung stehen.

Die Plattform stellt auch Interfaces zu Back-End-Systemen, Datenbanken und anderen Unternehmensressourcen wie z. B. Directory Services bereit. Darüber hinaus können weitere Schnittstellen zu externen Diensten wie z. B. Zahlungssystemen implementiert werden. Eine solche Web-/WAP-Plattform kann Anwender online mit einem Zahlungssystem verbinden, unabhängig davon, ob der Bezahlvorgang über den PC oder unterwegs mit dem Smartphone abgewickelt wird.

Front-End Server befinden sich meist in der so genannten *Demilitarisierten Zone (DMZ)* mit einer Firewall zum Schutz vor unbefugtem Zugriff durch die offenen Netze.

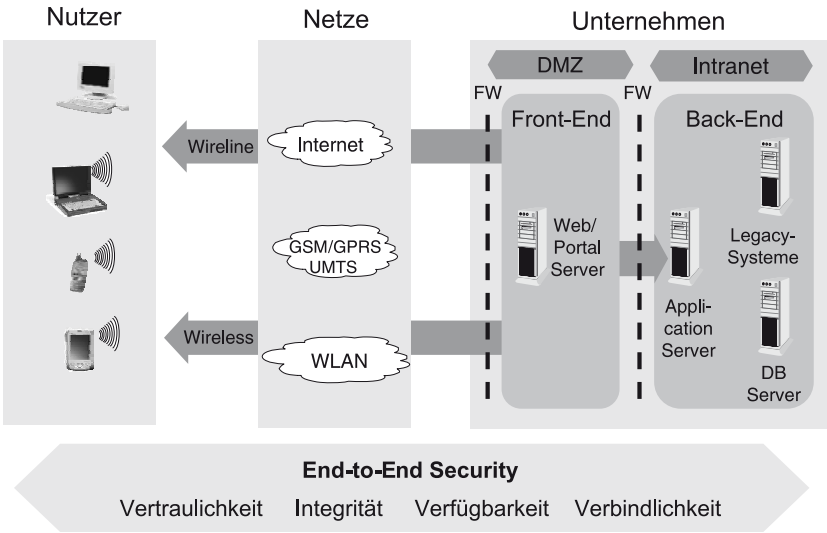


Bild 6.9 E- und m-Business-Security-Architektur

Weitere Firewalls können je nach Sicherheitsanforderungen Back-End-Systeme, das Intranet oder besondere Segmente des Unternehmensnetzes schützen.

6.3.1 Sichere Übertragungskanäle

Mobile Technologien weisen inhärente Sicherheitsschwachstellen auf. Einige sind mit den bekannten Risiken in Festnetzen vergleichbar, andere Gefahren kommen hinzu und erhöhen die Risiken beträchtlich. Die besondere Schwachstelle mobiler Netze ist das für Eindringversuche relativ offene Kommunikationsmedium – die Luft.

Mobilnetze werden auf Basis unterschiedlicher Standards, Protokolle und Service-Qualitäten betrieben und unterscheiden sich in ihren Security-Eigenschaften. GSM-Netze z. B. verfügen zwar über eine integrierte Security-Architektur, verwenden aber für die Sprachverschlüsselung sehr kurze Schlüssel (64 bit) und einen schwachen Verschlüsselungsalgorithmus. Sie unterstützen nicht die Verschlüsselung von SMS-Nachrichten. Integritätsprüfungen sind nicht vorgesehen und bei der Authentifikation von Teilnehmern können „Man-in-the-Middle"-Attacken nicht ausgeschlossen werden.

Die Wahrung von Vertraulichkeit und Integrität und die Bedrohung durch eine Denial-of-Service(DoS)-Attacke sind die Schwachstellen und Risiken, die mit Mobilnetzen verbunden sind. Nicht-autorisierte Nutzer können sich Zugang zu Unternehmenssystemen und -ressourcen verschaffen, Daten zerstören, auf Kosten anderer Bandbreite nutzen, die Netz-Performance schwächen oder berechtigten Nutzern den Zugang zum Netz verwehren.

Zu den typischen Bedrohungen und Schwachstellen in Mobilnetzen zählen:

– Unberechtigter Zugang zu Unternehmensnetzen über Mobilnetze unter Umgehung des Firewall-Schutzes

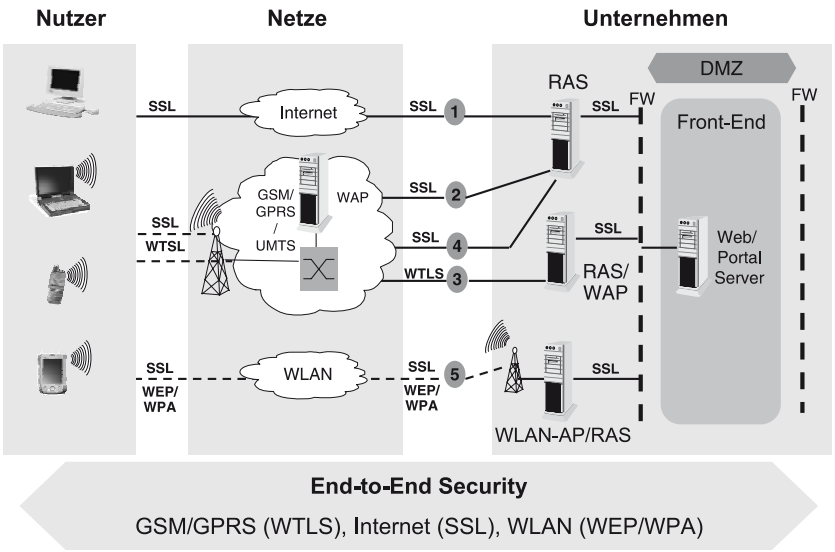


Bild 6.10 Sichere Übertragungskanäle

– vertrauliche Informationen, die nicht oder mit nicht ausreichend sicheren Krypto-Techniken verschlüsselt sind, werden bei der Übertragung abgefangen und offen gelegt
– gezielte DoS-Attacken auf drahtlose Verbindungen oder mobile Geräte
– Stehlen der Identität eines legitimierten Nutzers und Inanspruchnahme von Leistungen an Stelle des Berechtigten
– Beschädigung wichtiger Daten durch unsachgemäße Synchronisation
– Verletzung der Privatsphäre von Nutzern, indem ihre örtlichen Bewegungen verfolgt werden
– missbräuchliche Nutzung nicht vertrauenswürdiger Netzdienste von Dritten, um unberechtigten Zugang zu Unternehmensnetzen zu erschleichen.

Für die Gewährleistung einer sicheren Übertragung sind deshalb zusätzliche Security-Mechanismen erforderlich. Wie in Bild 6.10 veranschaulicht, lassen sich zwischen Endgeräten und Front-End fünf Übertragungskanäle mit verschiedenartigen Netzen, Netzprotokollen und Security-Eigenschaften unterscheiden.

Direkter Festnetzzugang (Kanal 1)

Security Transport Services für drahtgebundene Geräte wie PCs und Laptops werden durch das Standard-Internet-Protokoll *SSL/TLS (Secure Socket Layer/Transport Layer Security)* bereitgestellt. *HTTPS*(*HTTP Secure*)-Verbindungen nutzen dieses Protokoll unabhängig vom vermittelnden Internet-Service-Provider.

Zur Gewährleistung einer hochsicheren Verbindung kann während der Einwahlprozedur ein *VPN* (meist auf Basis des *IPsec-Standards*) zwischen dem mobilen Client und

dem Ziel-Front-End aufgebaut werden. Das VPN sorgt für Client/Server-Authentifikation und Verschlüsselung der übertragenen Nachrichten.

Zugang über WAP-Geräte in GSM-, GPRS- und UMTS-Netzen (Kanal 2)

WAP-Telefone oder Mobilgeräte mit einem *WAP Browser* werden meistens über das *WAP Gateway* eines Netzbetreibers zum Front-End eines Unternehmens vermittelt. Ein mobiler Client wird mit dem Front-End über das WAP Gateway des Netzbetreibers durch Sicherung des Übertragungswegs vom Client zum WAP Gateway über das drahtlose Netz sowie vom WAP Gateway zum Front-End über das Internet verbunden.

WTLS (Wireless Transport Layer Security) ist das Standard-Protokoll für die Abwicklung sicherer WAP-Verbindungen über das drahtlose Netz. WTLS bietet Funktionen wie Datenverschlüsselung, Datenintegrität und Client/Server-Authentifikation.

Mit dem WAP-Standard [6.3.1] wurden drei Sicherheitsklassen für die Kommunikation mobiler Geräte mit einem WAP Gateway definiert:

– Class 1: Data Encryption
– Class 2: Server (Gateway)-Authentifikation
– Class 3: Client (Mobile Device)-Authentifikation

Entsprechende Funktionen und Dienste für das Internet werden durch das Standard-Protokoll SSL/TLS bereitgestellt.

WTLS ist für die Nutzung über Schmalband-Kommunikationskanäle optimiert und daher nicht mit SSL/TLS kompatibel, d.h. dieses Protokoll stellt andere Verschlüsselungsalgorithmen bereit. Diese Inkompatibilität bedeutet, dass die Daten während der Konvertierung des WTLS-Protokolls in TLS/SSL bzw. umgekehrt kurze Zeit ungeschützt offen liegen, so dass die Möglichkeit einer Sicherheitsverletzung besteht. Auch wenn sowohl das drahtlose Netz als auch das Internet über leistungsfähige Sicherheitsmechanismen verfügen, sind zusätzliche Maßnahmen wie z. B. Service Level Agreements mit dem Betreiber des WAP Gateway erforderlich. Nur so kann End-to-End Security gewährleistet werden.

Zugang über den WAP Gateway eines Unternehmens (Kanal 3)

Die oben beschriebenen Sicherheitsrisiken haben viele Unternehmen dazu veranlasst, ein eigenes WAP Gateway in vertrauenswürdiger Umgebung zu betreiben, um die Kontrolle selbst auszuüben. In diesem Fall kann das Mobile Switching Center des Netzbetreibers das Gerät direkt zum WAP Gateway des Unternehmens vermitteln. Sicherheitsdienste werden dann durch die Protokolle WTLS und SSL/TLS im eigenen WAP Gateway bereitgestellt.

Zugang über IP-Geräte in GSM-, GPRS- und UMTS-Netzen (Kanal 4)

Es gibt eine immer größere Palette von GSM/GPRS/UMTS-kompatiblen drahtlosen *IP-Geräten* mit HTML Browsern (d.h. Laptops, PDAs, Smartphones). Das WTLS-Protokoll wird auf diesen Geräten nicht angewendet. End-to-End Security auf der Trans-

port-Ebene wird stattdessen durch das SSL/TLS-Protokoll erreicht, das durchgängig zwischen dem Gerät und dem Front-End über einen dazwischen liegenden Proxy Server zur Anwendung kommt.

Zugang über WLAN (Kanal 5)

Mobile Geräte mit einem *WLAN*-Zugang (entsprechend den Standards 802.11 a, b, g) werden mit dem Ziel-Front-End über den drahtlosen Access Point (WLAN AP) verbunden, der sich in Hotspot-Bereichen z. B.auf einem Flughafen oder auch in einem Unternehmen befinden kann.

Diese Geräte entsprechen dem Security-Standard *WEP (Wired Equivalent Privacy)*, einem Verschlüsselungsmechanismus zwischen dem Gerät und dem Access Point. Dieser Standard weist jedoch einige wesentliche Sicherheitsschwächen auf, die mit den Längen der Schlüssel, dem Management größerer Konfigurationen und dem Wechsel von Zugangspunkten im Falle eines sich fortbewegenden Benutzers (Roaming) zu tun haben. Aus diesem Grund sind VPNs für Netzkonfigurationen dieser Art unerlässlich.

Neuere WLAN-Geräte und Komponenten unterstützen den *WPA(Wi-Fi Protected Access*)-Standard [6.3.2], der von einem Industrie-Konsortium definiert wurde und die bekannten Schwächen von WEP eliminieren soll. WPA kann allerdings nur als ein Übergangsstandard gesehen werden, der zwar die Security deutlich verbessert und auch bereits einige Security-Funktionen, wie sie von der *IEEE 802.11i* Task Group erarbeitet wurden, beinhaltet. Diese Task Group definiert gerade die Security Features eines sogenannten *RSN (Robust Security Network)*, dessen Ziel die Ermöglichung vollständig sicherer WLAN-Verbindungen ist. Komponenten, die dem Standard 802.11i vollständig entsprechen, sind Ende 2004 oder 2005 zu erwarten.

Im Vergleich zu WEP enthält die WPA-Version 1 einige Erweiterungen wie dynamische Schlüssel, verbesserte Integritätsprüfungen von Nachrichten, automatisierte Key Management Services, Negotiation Services für Verschlüsselung und Authentifikation. WPA-Version 2, verfügbar seit 2004, ersetzt den RC4-Verschlüsselungsalgorithmus durch den *AES (Advanced Encryption Standard)* und unterstützt das Roaming.

Der Einsatz von WPA in WLANs kann in einigen Business-Szenarien VPNs erübrigen, allerdings gilt dies nicht, wenn öffentliche Netze benutzt werden.

An dieser Stelle soll auch auf den neuen Standard 802.1x für Authentifikation hingewiesen werden. 802.1x ermöglicht ein einheitliches und netzunabhängiges Authentifikationsverfahren. Lösungen sind seit 2004 verfügbar.

Wie bei drahtgebundenen Konfigurationen werden WLAN HTTPS-Verbindungen auf der Transportschicht durch Anwendung des SSL/TSL-Protokolls sowohl auf Server- als auch auf Client-Seite gesichert.

Andere Übertragungskanäle

Andere Mobilnetze wie DECT und Home RF werden in diesem Buch nicht behandelt, da sie in Geschäftslösungen kaum eine Rolle spielen.

Bluetooth dagegen hat das Potenzial, zum Standard für *Ad-hoc-Netze* zu werden, die in Geschäftsszenarien künftig eine wichtige Rolle spielen werden. Bluetooth Security ist allerdings kein einfaches Thema, da allein fünf verschiedene Security-Profile existieren: Device Discovery Application Profile, Headset Profile, Dial-up Networking Profile, LAN Access Profile und Synchronization Profile. Auf Details wird hier nicht eingegangen. Ausführliches dazu ist im Bluetooth Security White Paper [6.3.3] nachzulesen.

Der Bluetooth-Standard definiert bereits Security Features für Authentifikation und Verschlüsselung. Bluetooth-Netze sind aufgrund etlicher Sicherheitsschwächen heute noch nicht für Implementierungen zu empfehlen, die hohe Sicherheit erfordern, wie für den Zugriff auf Intranet-Ressourcen von Unternehmen. Während robuste Verschlüsselungsmechanismen bereits angewendet werden, liegt das Problem bei der Authentifikation des Gerätes, bei der ein unsicherer Austausch von geheimen Schlüsseln stattfindet.

Es ist zu erwarten, dass sich diese Schwächen in den nächsten Jahren beseitigen lassen, da Bluetooth nun den Rang eines offiziellen IEEE-Standards erhalten hat: 802.15.1-2002. Die Arbeitsgruppe 802.15.1 prüft derzeit, wie die Sicherheit von Bluetooth z. B. durch Unterstützung von digitalen Zertifikaten und PKI verbessert werden kann.

6.3.2 Anwendungsplattform mit End-to-End Security

Wie bereits erläutert und in Bild 6.11 dargestellt, ist besonderes Augenmerk auf die *End-to-End Security* und ihre vollständige Integration in zukunftsorientierte Anwendungsplattformen zu legen. Dazu zählen drahtgebundene und mobile Geräte, Internet/Intranet und mobile Netze, Gateways, Web-, Portal- und Application Server, sowie Legacy-Systeme, Datenbank-Server und weitere Ressourcen des Unternehmens.

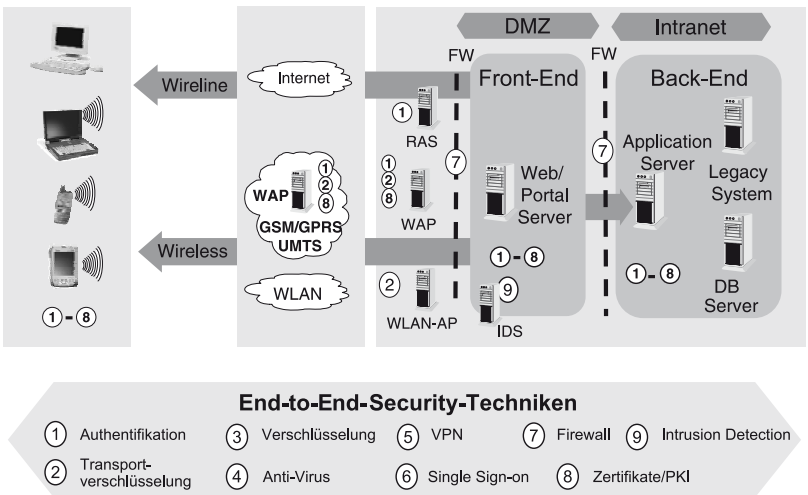


Bild 6.11 Anwendungsplattform mit End-to-End Security

Die Gewährleistung von End-to-End Security erfordert die Implementierung von Security-Funktionen in jeder Plattformkomponente. Die Funktionsbreite reicht von Authentifikationsmechanismen bis zu einer Public-Key-Infrastruktur, wie in Bild 6.11 veranschaulicht.

VPN ist für die meisten Business-Anwendungen zwingend erforderlich und SSO wird vermehrt gewünscht.

PKI und digitale Signaturen werden sich als sichere, durchgängige und zukunftsorientierte Technik für Integritätssicherung und Authentifikation langfristig bei vielen Lösungen der Administration und in Unternehmen durchsetzen. Die zunehmende Nutzung von Zertifikaten in Verbindung mit mobilen Endgeräten setzt schließlich geeignete PKI-Unterstützung voraus.

Front-End-, Back-End- und Firewall-Konfigurationen können sich von Unternehmen zu Unternehmen je nach deren konkreten Sicherheitsprioritäten, Netztopologien und Standorten unterscheiden.

In den meisten modernen Konfigurationen ist das Front-End der Dreh- und Angelpunkt für die End-to-End Security. Das Front-End fungiert als Single-Point-of-Access für drahtgebundene und drahtlose Geräte und verbindet Geräte mit Portal-Services und angeschlossenen Unternehmensressourcen. Adäquate Sicherheitsmechanismen müssen auf Geräteseite implementiert und im Front-End angepasst werden. Dabei muss eine dynamische Anpassung beim Einsatz von neuen Geräten möglich sein. Vorhandene, oft proprietäre Protokolle und Sicherheitstechniken auf der Back-End-Seite müssen adaptiert werden, um tatsächliche End-to-End Security zu erreichen.

Intrusion-Detection-Systeme für die Überwachung von Betriebssystemen, Netzverkehr und Zugangsberechtigungen vervollständigen das Security-Portfolio.

Im Folgenden werden die Security-Anforderungen an die verschiedenen Komponenten näher beleuchtet.

Mobile Geräte

Gerätehersteller werden ihre Produkte in den nächsten Jahren weiterhin differenzieren, um ihre Marktanteile in diesem schnell wachsenden Segment auszubauen. Unternehmen und Kunden werden eine Vielzahl von Geräten nachfragen, die sich durch Preis, Funktionalität und spezifische für Daten- und Sprachanwendungen optimierte Features unterscheiden.

Über einen gewissen Zeitraum werden miteinander konkurrierende Plattformtechnologien wie Palm OS, Windows Mobile, Symbian und auch Linux den Markt bestimmen. Neue Technologien wie J2ME (Java 2 Micro Edition) und .NET Compact Framework haben vermutlich das Potenzial zur grundlegenden Änderung bestehender Anwendungsparadigmen. Insbesondere die Möglichkeit des Downloads von Objekten und Applets sowie Schnittstellen für den direkten Aufruf von XML Web Services werden neue Anwendungsszenarien eröffnen, gleichzeitig aber zusätzliche Sicherheitsfragen aufwerfen.

Im Allgemeinen sind spezifische Sicherheitsrisiken bei mobilen Geräten zu berücksichtigen:

- Das kleine Format der Geräte und ihre mobile Nutzung erhöhen das Risiko, dass sie gestohlen werden oder verloren gehen. Oftmals sind dann auch vertrauliche Informationen betroffen.
- Angestellte kaufen Geräte oft selbst und nutzen sie geschäftlich, ohne die CIO-Organisation darüber zu informieren.
- Mobile Geräte werden häufig sowohl privat als auch geschäftlich genutzt. Dabei werden die damit verbundenen Security-Implikationen für die geschäftlichen Anwendungen in der Regel nicht gesehen.
- Viele Nutzer haben kein ausgeprägtes Sicherheitsbewusstsein und die potenziellen Sicherheitsrisiken speziell mit diesen Geräten sind ihnen nicht bekannt.
- Mit mobilen Geräten lassen sich vielfältige Programme, Spiele usw. einschließlich der Freeware- und Shareware-Programme aus dem Netz von überwiegend unbekannten Quellen herunterladen. Dabei kann bösartiger Code das mobile Gerät selbst, durch die Synchronisation auch den PC des Nutzers und sogar die Netzressourcen des Unternehmens erheblich beschädigen.

Zur Realisierung von zukunftssicheren Lösungen müssen Kunden sorgfältig und umfassend beraten werden, damit sie unter Berücksichtigung der Komplexität von Implementierung und Betrieb geeignete Geräte-Plattformen auswählen können.

Im Kontext Sicherheit und mobile Geräte kann zwischen WAP-Geräten (Mobiltelefone, PDAs) und TCP/IP-Geräten (PDAs, Laptops) unterschieden werden. Im Folgenden wird erläutert, wie sich die Sicherheitstechniken und Features bei diesen beiden Kategorien unterscheiden.

WAP-Geräte

Das WAP Forum hat eine Reihe von Standards definiert, die unter Berücksichtigung der eingeschränkten technologischen Möglichkeiten von WAP-Geräten entstanden sind. Veröffentlichte Spezifikationen schließen *WAP 1.1* (1999), *WAP 1.2.1* (2000) und *WAP 2.0* (2002) ein. Im WAP-Standard sind Sicherheitsspezifikationen für WTLS, WMLScript Crypto Library und WIM/WPKI enthalten. Sie decken Funktionalitäten wie Authentifikation, Transportverschlüsselung, Zertifikate, digitale Signatur und PKI-Unterstützung ab.

WTLS Class 1 definiert Mechanismen für Schlüsselaustausch, Datenverschlüsselung und Datenintegrität.

WTLS Class 2 definiert zusätzlich zu den Mechanismen gemäß Class 1 auch Mechanismen für die Zertifikat-basierte Server (WAP Gateway)-Authentifikation.

WTLS Class 3 definiert zusätzlich zu den Mechanismen gemäß Class 2 auch Mechanismen für die Zertifikat-basierte Authentifikation von Clients (WAP-Geräten).

WML Script Crypto Library spezifiziert das Library Interface zur ständigen Authentifikation bei Transaktionen, die während einer WTLS-Verbindung erfolgen können. Dies ist bei vielen Anwendungen erforderlich (z. B. e-Commerce), bei denen ein ständiger

Beleg dafür notwendig ist, dass jemand eine Transaktion autorisiert hat. Zur Bereitstellung eines derartigen Belegs, im Standard als *signText* bezeichnet, wird eine digitale Signatur mit den Daten verknüpft, die infolge der Transaktion (z. B. einer Bestellung) generiert werden.

Der Server muss Zugriff auf das Zertifikat des Anwenders haben, um die digitale Signatur zu verifizieren. Hierfür hat der Server mehrere Möglichkeiten:

– Das Zertifikat wird an die Signatur angehängt.
– Der Hash-Wert des öffentlichen Schlüssels wird der Signatur angehängt. Der Server kann das entsprechende Zertifikat von einem Zertifikat-Service abrufen.
– Eine URL des Zertifikats wird an die Signatur angehängt. Der Server kann das Zertifikat über das Internet abrufen.
– Der Server kennt das Zertifikat des Benutzers von einem früheren Datenaustausch her.

Das *WIM (Wireless Identity Module)* dient zur Abwicklung von Sicherheitsfunktionen auf Transport(WTLS)- und Anwendungsebene und insbesondere zur Speicherung und Verarbeitung von Informationen, die für die Identifikation und Authentifikation von Benutzern benötigt werden. Mit dieser Funktionalität werden sensible Daten (vor allem Schlüssel) im WIM gespeichert und alle Operationen, an denen diese Schlüssel beteiligt sind, können im WIM ausgeführt werden.

Eine wichtige Anforderung an das WIM ist seine manipulationssichere Ausprägung (*Tamper-resistant*). Dies bedeutet, dass bestimmte physische Hardware- und Software-Schutzvorkehrungen gegeben sind, die es unmöglich machen, geschützte Informationen aus dem Modul zu extrahieren oder im Modul zu verändern.

Beispiele für die Realisierung derartiger Schutzvorkehrungen sind *Smartcards* und *SIM Cards*. Normale Mobiltelefone und PDAs können nicht als Tamper-resistant eingestuft werden. Bei diesen Geräten ist die Extraktion von Informationen zwar schwierig, mit der geeigneten Technik aber möglich. Das WIM ist als unabhängige Smartcard-Anwendung definiert, so dass die Implementierung als reine WIM Card (WIM-only Card) oder als Teil einer Multifunktionskarte mit anderen Kartenanwendungen auf einer SIM Card möglich ist.

WIM wird bei WTLS für folgende Zwecke verwendet:

– Ausführung von kryptographischen Operationen während des Handshake, vor allem derjenigen Operationen, die zur Client-Authentifikation dienen
– Sicherung lang andauernder WTLS-Sitzungen
– Das WIM dient zum Schutz permanenter (meist zertifizierter) privater Schlüssel. Es speichert diese Schlüssel und führt Operationen unter Verwendung dieser Schlüssel aus. Im Einzelnen handelt es sich dabei um die folgenden Operationen:
– Signing Operation für die Client-Authentifikation, falls für das ausgewählte Handshake-Konzept erforderlich
– Key Exchange Operation mit einem festen Client-Schlüssel
– die privaten Schlüssel verlassen nie das WIM.

Security-Operationen auf Anwendungsebene, die das WIM nutzen, sind u.a. die Unterzeichnung (Signing) und Entschlüsselung (Unwrapping) eines Schlüssels. Beide Operationen nutzen einen privaten Schlüssel, der ebenfalls nie das WIM verlässt. Diese Operationen sollen generischen Charakter haben, um beliebigen Anwendungen zu dienen, die im WAP (z. B. mit WMLScript) oder außerhalb des WAP definiert sind. Ein Schlüssel muss entschlüsselt (unwrapped) werden, wenn eine Anwendung einen Nachrichtenschlüssel empfängt, der mit einem öffentlichen Schlüssel chiffriert wurde, der wiederum einem privaten Schlüssel im WIM zugeordnet ist.

Digitale Signaturen können für Authentifikationen oder Nachweise verwendet werden (z. B. zur Unterzeichnung eines Dokuments oder zur Bestätigung einer Transaktion = signText-Operation). Für Zwecke der *Nachweisbarkeit (Non-Repudiation)* wird meist ein gesonderter Schlüssel verwendet, der Benutzer wird zur Eingabe von Authentifikationsinformationen (PIN) für jede geleistete Signatur aufgefordert.

Neben den Sicherheitsfunktionen auf der WTLS- und WAP-Anwendungsschicht kann das WIM auch zur Sicherung von Nicht-WAP-Anwendungen eingesetzt werden, die ein manipulationssicheres Gerät für die Abwicklung folgender Funktionalitäten erfordern:

- Signatur für Authentifikationszwecke
- Signatur für Zwecke der Nachweisbarkeit
- Entschlüsselung privater Schlüssel
- Speicherung von Benutzerzertifikaten
- Speicherung von Zertifikaten vertrauenswürdiger CAs (Certification Authority).

Der Einsatz von WIM und Zertifikaten setzt eine Public-Key-Infrastruktur voraus, wie sie im WPKI-Standard spezifiziert ist.

Neben diesen durch Standards definierten Sicherheitsfunktionen können je nach *SDK (Software Development Kit)*, der von den Geräteanbietern bereit gestellt wird, noch weitere Features implementiert werden. So ist beispielsweise die Implementierung von Datenverschlüsselung, VPN oder Single Sign-on möglich, wenn das Gerät derartige Funktionen unterstützt.

TCP/IP-Geräte

Diese Gerätekategorie wird überwiegend durch *Laptops* und *PDAs* repräsentiert. Künftig werden auch immer mehr Mobiltelefone mit Implementierung des Standards WAP 2.0 zu dieser Kategorie zählen.

Die wichtigsten Betriebssysteme sind hier Windows 2000/Windows XP (Laptops), *Palm OS* (PDAs, Smartphones), *Windows Mobile* (PDAs, Smartphones) sowie stark zunehmend *Symbian/Nokias Series 60* (Smartphones). Die integrierten Sicherheits-Features dieser Betriebssysteme reichen im Allgemeinen nicht aus, um den Geräten auf dieser Basis den Zugriff auf sensible Intranet-Ressourcen eines Unternehmens zu erlauben.

Tabelle 6.1 Erforderliche Sicherheitsfunktionen in Business-Anwendungen

Security-Niveau Security-Funktionen	Secure Access	Confidential Access	Remarks
Lokale Authentifikation			
Pin, Password	√	√	7 oder mehr Zeichen
Biometrie	Nice to have	Nice to have	Fingerprint, Signatur
Remote Authentifikation			Zugang zum Intranet
Website	√	√	SSL Authentifikation
Remote Access Server	√	√	z. B. CHAP, RADIUS, 802.1x
PKI-basiert	Nice to have	√	z. B. Digitale Signatur
Datenverschlüsselung	Nice to have	√	128-bit-Schlüssel
VPN Client	√	√	IPsec, damit nicht nur für Web-Anwendungen einsetzbar
Anti-Virus	√	√	Automatischer Update
Personal Firewall	√	√	Erforderlich, wenn Internet-Zugang erlaubt wird
PKI Support	Nice to have	√	End-to-End Support
Digitale Signatur	Nice to have	√	X.509 Standard
Smartcard Support	Nice to have	√	Privater Schlüssel und Zertifikat sind auf der Smartcard gespeichert

Wie bereits erläutert, kommunizieren diese mobilen TCP/IP-Geräte über die TCP/IP- und Internet-Protokoll-Stacks, ohne ein WAP Gateway zu nutzen, sofern das Betriebssystem oder ein installierter WAP Browser eines Drittanbieters nicht auch die WAP-Protokolle unterstützt.

Wegen der Vielfalt der Betriebssysteme mit unterschiedlichen Versionen und der üblichen kurzen Lebenszyklen dieser Versionen macht es keinen Sinn, detailliert auf die jeweiligen Security-Funktionen einzugehen. Details können den aktuellen Produktinformationen der Hersteller entnommen werden. Sehr informativ sind auch Security White Papers, wie *Security on the Pocket PC* [6.3.4] und *Handheld security for the mobile enterprise, Palm OS* [6.3.5], deren Aktualisierung jedoch nicht sichergestellt ist.

In Tabelle 6.1 sind die üblicherweise erforderlichen Security-Funktionen für Business-Anwendungen zusammengestellt. Es werden zwei unterschiedliche Sicherheitsniveaus berücksichtigt und die Betriebssysteme Windows Mobile und Palm OS betrachtet. Die Darstellung und Auswahl von Funktionen mag als Anhaltspunkt für IT-Organisationen dienen. In einem realen Security-Projekt kann es abhängig von der jeweiligen Risikoeinschätzung jedoch zu anderen Ergebnissen kommen.

Das Niveau *Secure Access* ist definiert als Zugang zu Intranet-Anwendungen, die nicht unter die Kategorie firmenvertraulich und geschäftskritisch (Mission-critical) fallen. Das Niveau *Confidential Access* schließt dagegen diese kritischen Geschäftsanwendungen durchaus mit ein.

Heutige Betriebssysteme können nicht alle diese Anforderungen erfüllen. Ergänzend kann aber 3rd Party Software eingesetzt werden. Hier sind einige Beispiele von bewährten Security-Komponenten für PDAs:

- *Certicom movianCrypt* (Authentifikation, Datenverschlüsselung für Windows Mobile und Palm OS)
- *Glück & Kanja Technology AG, CryptoEx Volume* (Mail-Verschlüsselung)
- *Certicom movianVPN* (VPN für Windows Mobile und Palm OS)
- *Certicom Trustpoint Client* (PKI für Palm OS)
- *Entrust VPN client* (VPN-Portal-Lösung für Windows Mobile)
- *Checkpoint VPN-1Secure Client* (VPN und Personal Firewall für Windows Mobile)
- *F-Secure* (Anti-Virus für Windows Mobile und Palm OS)
- *Trend Micro PC-cillin* (Anti-Virus für Palm OS)
- *Trend Micro Office Scan* (Anti-Virus für Windows Mobile)

Front-End und Back-End Security

Remote Access Server, Authentication Server

Mobile Nutzer müssen sich, wann immer sie Zugang zum Firmennetz wünschen, zunächst an einem *Remote Access Server (RAS)* einwählen, um sich an einem *Authentication Server* zu authentifizieren. Diese Server können getrennt oder als Produkteinheit ausgeführt sein. Authentication Server können unterschiedliche Authentifikationsmethoden unterstützen wie Passwort, SecurID Card oder Zertifikat-basierte Methoden, z. B. mit Smartcards, und bauen meistens auch eine VPN-Verbindung auf. Eine einfache Authentifikation mittels Passwort ist für einen Zugang zum Intranet nicht ausreichend. Stattdessen ist eine *starke Authentifikation* mit zwei Faktoren erforderlich, d.h. etwas, das man weiß (z. B. ein Passwort) und etwas, das man hat (z. B. SecurID Card oder ein geheimer Schlüssel) sind in Kombination anzuwenden. PKI-basierte Authentifikationsmethoden mit digitalen Signaturen sind zukunftsorientiert. Methoden mit noch höherem Security-Niveau, wie die Auswertung der Retina oder des Fingerabdrucks (der dritte Faktor, nämlich etwas, das man selber repräsentiert) sind in der Regel für traditionelle Business-Anwendungen nicht praktikabel, sondern eher Speziallösungen vorbehalten.

In der Vergangenheit haben sich verschiedene RAS-Authentifikationsprotokolle entwickelt, wie z. B. *RADIUS* (Näheres in Kapitel 6.4). Als zukunftsorientiert ist hier der neue *Standard 802.1x* zu nennen, der sich ab 2004 vermutlich rasch im Markt durchsetzen wird.

Neben der Authentifikation bei der Einwahl sind in Geschäftslösungen Authentifikationen auch auf anderen Ebenen erforderlich: WAP Gateway, SSL/TLS, Portal-Ebene, Anwendungsebene.

Bewährte RAS werden von Firmen wie Cisco, 3Com, Nokia und anderen angeboten, entsprechende Funktionen werden aber zunehmend auch in Betriebssystemen, Web Servern, Portal Servern und Application Servern zur Verfügung gestellt. Authentication Server sollten in sicherer Umgebung betrieben werden, um Manipulationen bei Authentifikationen auszuschließen.

WAP Gateways

Wie bereits erläutert, wird ein WAP Gateway entweder von Netzbetreibern oder von Unternehmen selbst betrieben.

Heute verfügbare Anwendungsplattformen wie IBM WebSphere, BEA WebLogic, SUN ONE, Oracle Application Server, SAP NetWeaver und Microsoft Exchange Server haben bereits eine WAP-Gateway-Funktionalität einschließlich Authentifikation, Integrität, Verschlüsselung und PKI-Unterstützung entsprechend der WAP-Standards integriert. Unternehmen, die eine solche Plattform betreiben, müssen also keinen separaten WAP Gateway installieren. Allerdings sollte eine sichere Betriebsumgebung auch für diese Plattform gewährleistet sein, da bei der Konvertierung der Protokolle von WTLS in SSL/TLS und umgekehrt die Daten kurzzeitig offenliegen.

Web Server, Portal Server und Application Server

E-Business- und m-Business-Lösungen basieren auf Anwendungsplattformen. *Web Server, Portal Server, Firewalls* und *Application Server* sind üblicherweise entsprechend Bild 6.11 aufgestellt. Davon abweichend und orientiert an der Sicherheitsarchitektur des Unternehmens können Portal Server aber auch hinter der zweiten Firewall konfiguriert sein. Im Prinzip müssen alle diese Server die folgenden Security-Features aufweisen:

- Authentifikation
- Rollen-basierte Autorisierung
- Transportverschlüsselung (SSL/TLS)
- Datenverschlüsselung
- VPN-Unterstützung
- Single Sign-on (mindestens für Web-Anwendungen)
- digitale Zertifikate, digitale Signaturen
- PKI-Unterstützung.

Die vorher erwähnten Plattformen (Microsoft, IBM, SAP, BEA, SUN, Oracle) bieten diese Features mehr oder weniger ausgeprägt und weitgehend auf der Basis moderner Security-Technologien (z. B. XML Security).

Um End-to-End Security sicherzustellen, sind diese Security-Features aber auch in Integration Servern und Back-End-Systemen erforderlich. Insbesondere Legacy-Systeme verwenden vielfach proprietäre Protokolle und Funktionen, so dass in einigen Fällen ernsthafte Interoperabilitätsprobleme auftreten können.

Die Erfahrung lehrt allerdings, dass selbst eine vollständige und hochqualitative Implementierung von Security-Funktionen auf allen Ebenen eine Kompromittierung nicht absolut sicher verhindern kann. Insbesondere Betriebssysteme und Web Server (und hier hauptsächlich Microsoft-Produkte) sind Zielscheibe unentwegter Angriffe von Hackern, die täglich ihr Unwesen treiben und Software-Hersteller wie auch Unternehmen schädigen wollen. Immer wieder gelingt es ihnen, Schwachstellen aufzuspüren

(z. B. Buffer Overflow). IT-Organisationen sind gut beraten, die Instruktionen von CERT und den entsprechenden Software-Firmen sorgfältig zu befolgen.

Virtual Private Networks

VPN ist eine Technologie, die den sicheren Informationsaustausch über öffentliche Netze ermöglicht, unabhängig vom geographischen Standort des Benutzers, in einem entfernten Firmenstandort, in einem Hotel, in einem Büro des Kunden oder unterwegs. Verschlüsselungstechnologie und Secure-Tunneling-Protokolle machen das Netz dabei zu einem *privaten* Netz, wenn auch die Kommunikation über öffentliche Telefonleitungen oder Mobilnetze erfolgt.

Der Einsatz von VPN-Technologie ist unverzichtbar, wenn Kunden, Partnern oder Firmenangestellten Zugang zum Intranet von außerhalb gewährt werden soll.

Eine geeignete VPN-Lösung für Unternehmen sollte beliebige mobile Geräte unterstützen und einheitlich für LAN, WLAN und Mobilnetze einsetzbar sein. Als besonders elegante Funktion ist ein automatisches Roaming beim Wechsel zwischen den Zellen verschiedener Netztypen (z. B. WLAN – GPRS) zu erwähnen.

Als Beispiel einer durchgängigen VPN-Technologie wird im Folgenden die CORINA-Lösung von Siemens Business Services kurz erläutert. Sie unterstützt verschiedene Kanäle, wie in Bild 6.12 gezeigt.

CORINA ist eine Client/Server-Applikation, deren Client-Komponente auf Laptops, Tablet PCs oder PDAs und deren Server-Komponente auf Windows- oder Unix-basierten Remote Access Servern läuft. CORINA enthält ein elektronisches Telefonbuch, verwendet zur Authentifizierung SecureID Cards oder digitale Zertifikate, setzt eine hochwertige Verschlüsselungstechnologie (128-bit-Schlüssel) ein und bietet weltweite Einwahlmöglichkeiten.

Die CORINA-Familie unterstützt vier unterschiedliche Zugangskanäle:

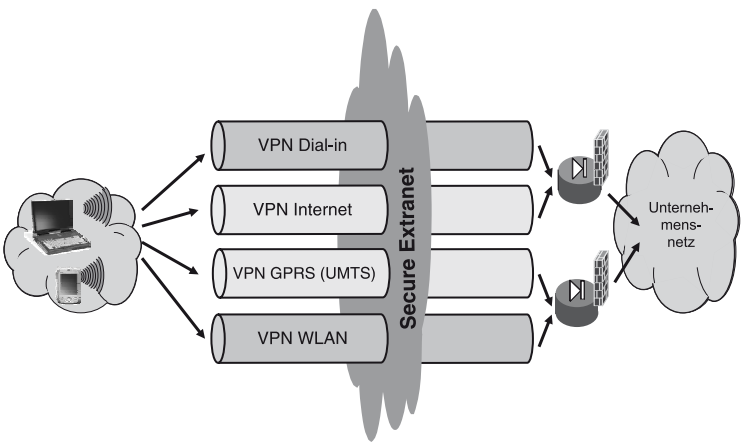


Bild 6.12 VPN Solution

VPN Dial-in

Ermöglicht weltweit den Wählzugang zum Intranet des Unternehmens über PoP(Public access Points)-Listen. Neben dem herkömmlichen Zugang über analoge und digitale Telefonverbindungen können auch Mobilfunknetze auf Basis von GSM/HSCSD genutzt werden. Im letzteren Fall wird ein Mobiltelefon meist über Infrarot mit dem Laptop verbunden. Es stellt den Zugang zum Remote Access Server über das Mobilfunknetz her.

VPN Internet

CORINA PIN (Zugang über das Internet) unterstützt die Mobilität des Anwenders durch die Möglichkeit der Nutzung öffentlicher Internet-Verbindungen, z. B. von Cafés, Hotels oder Flughäfen aus. Bei Nutzung öffentlicher Ressourcen für die Datenkommunikation wird die Sicherheit vom Netz auf die Anwendungen verlagert. Verbindungen zum Internet sind möglich über Modem, High Speed x-DSL oder direkten LAN-Zugang.

VPN GPRS

CORINA GPRS ermöglicht den Zugang zu Unternehmensressourcen über das GPRS-Netz, wobei dieses auf zweierlei Weise genutzt werden kann: Zum einen kann ein Laptop-Nutzer über ein GPRS-Mobiltelefon, das mit dem Laptop verbunden ist, sicheren Zugang zu Unternehmensressourcen erhalten. Zum anderen kann der Benutzer einfach nur das Handy für den WAP-Zugriff auf Unternehmensdaten über ein WAP Gateway verwenden.

VPN WLAN

Als Teil der *CORINA WLAN*-Lösung werden die von Siemens Business Services betriebenen Wireless Access Points (AP) in einem *Secure Wireless Extranet* konfiguriert und über sichere Gateways in die Intranets von Unternehmen eingebunden. Das WLAN-inhärente Sicherheitsprotokoll WEP wird im konzeptuellen CORINA-Entwurf aufgrund seiner Untauglichkeit für groß dimensionierte Anwendungsszenarien nicht verwendet. An seiner Stelle kommt die bewährte VPN-Variante zum Einsatz. Der Wireless Access Point wird als Dial-in PoP (ohne tatsächliche Einwahl) betrachtet und dient zum Aufbau eines sicheren Wireless Extranet. Ein dynamisches *DHCP (Dynamic Host Configuration Protocol)* sichert den Transport zum Ziel-RAS des Unternehmensnetzes.

6.3.3 Zusammenfassung und Empfehlungen

Mobile Anwendungen werden überwiegend in existierende e-Business-Architekturen integriert. End-to-End Security bedeutet, dass Security-Funktionen in alle Plattform-Komponenten eingebettet sind. Daher ist es von entscheidender Bedeutung, dass mobile Anwendungen auf modernen, Standard-basierten, zuverlässigen und sicheren Plattformen implementiert werden.

Technische, personelle und operationale Security-Maßnahmen müssen kombiniert werden, um eine wirklich umfassende Security Policy zu garantieren. Das heißt auch, dass die unterschiedlichen Perspektiven eines Unternehmens (CEO, Geschäftsbereiche und IT-Organisation) einschließlich der Mobility-Aspekte einzubeziehen und sorgfältig abzuwägen sind. Security Policy, Security Roadmap und Risiko-Management sind die Eckpfeiler eines kontinuierlichen Security-Prozesses.

Die Geschäftsbereiche müssen sich Klarheit verschaffen über die infrage kommenden mobilen Business-Szenarien, aber auch über die besonderen Kommunikations-, Netzzugangs-, Geräte-, Verarbeitungs- und Umgebungsanforderungen. Daraus abgeleitet erstellen IT-Organisationen die entsprechenden Richtlinien und implementieren die erforderlichen Security-Maßnahmen.

Der Vorstand eines Unternehmens muss sich mit den Geschäftsmöglichkeiten und Risiken von mobilen Anwendungen auseinandersetzen und trägt auch die Verantwortung für eine Ausrichtung der Security-Strategie an der übergeordneten Geschäftsstrategie des gesamten Unternehmens.

Unternehmen sollten offen sein für eine Unterstützung durch erfahrene Security-Service-Provider. Kompetente Security Services können gravierende Schäden vermeiden helfen und durch proaktives Handeln eskalierende Security-Vorfälle frühzeitig eindämmen. Dadurch sparen Unternehmen Geld und können ihre Reputation bewahren.

6.4 Authentifikation, Single Sign-on

Die Herausforderung

Immerhin zehn Prozent der Weltbevölkerung loggen sich mindestens einmal im Monat in das Internet ein. Sie benutzen unterschiedliche Geräte vom PC bis zum Mobiltelefon und gehen von zuhause, von der Arbeitstätte, von der Schule, von Bibliotheken, Cafés oder Airports online.

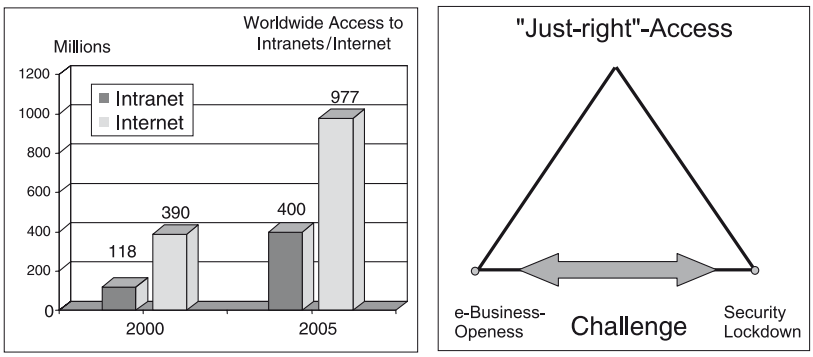


Bild 6.13 Steigende Zugangszahlen zu Internet und Intranets

International Data Corp. [6.4.1] schätzt, dass sich die Zahl der Internet-Nutzer zwischen 2001 und 2006 von 500 Millionen auf etwa 1 Milliarde verdoppeln wird. Der drahtlose Internet/Intranet-Zugang und die zunehmende Integration von mobilen Angestellten, Partnern und Kunden mit einer durchschnittlichen jährlichen Wachstumsrate von 28% auf etwa 400 Millionen Nutzer im Jahr 2005 (Bild 6.13) stellen weitere Herausforderungen dar, die zu bewältigen sind.

Unternehmen müssen die richtige Balance finden zwischen einer erweiterten Öffnung der Unternehmensressourcen für Geschäftspartner und der Wahrung eines ausreichenden Security-Niveaus, das eine Gefährdung des Geschäfts verhindert. Dies ist eine schwierige Gratwanderung und erfordert eine genaue Analyse der wesentlichen Geschäftsprozesse und eine realistische Einschätzung der damit verbundenen Risiken.

6.4.1 Definitionen

Identity

Identity (Identität) ist das digitale Synonym für einen Nutzer oder ein beliebiges Objekt. Die Identität sollte eindeutig sein und kann durch einen Namen, eine Mail-Adresse, einen Ausweis usw. definiert sein. Ein Zertifikat ist eine sichere *elektronische Identität (Electronic Identity, Digital Passport)*. Zertifikate enthalten üblicherweise den Namen des Nutzers und seinen öffentlichen Schlüssel (Public Key).

Network Identity bezieht sich auf einen globalen Satz von Attributen, die in den Accounts unterschiedlicher Service-Provider enthalten sein können. Diese Attribute können Namen, Adressen, Telefonnummern, Versicherungsnummern, Kreditkartennummern, persönliche Präferenzen usw. umfassen. Auf Privatpersonen bezogen ist die Network Identity die Summe aller finanziellen, medizinischen und persönlichen Daten, die überwiegend schützenswert sind. Für Geschäftsanwendungen repräsentiert die Network Identity das Wissen über Geschäftspartner, um dadurch für Partner und Unternehmen Werte zu schaffen.

Identity Management

umfasst das Management von Prozessen, die auf den Inhalten digitaler Identitäten basieren, und steuert, wem Zugang zu welchen Objekten zu gewähren ist. Identity Management bietet Unternehmen mit komplexen Organisations- und Kundenstrukturen eine zentrale Administration zur Verwaltung vielfältiger Accounts einschließlich der zugehörigen digitalen Identitäten über den gesamten Lebenszyklus.

Authentifikation

ist der Vorgang der Verifizierung einer Identity. Um beispielsweise auf eine Website oder Ressource zugreifen zu können, muss sich der Nutzer durch ein Passwort oder mittels anderer Methoden wie Smartcards oder biometrische Kennzeichen ausweisen (authentifizieren).

Authentifikation basiert auf drei Faktoren: etwas, das man weiß (z. B. Passwort, PIN), etwas, das man hat (z. B. Smartcard, privater Schlüssel) und etwas, das man selbst verkörpert (z. B. Fingerabdruck, Retina). Die *1-Faktor-Authentifikation* wird auch *schwache Authentifikation* genannt, während man bei der *2- oder 3-Faktor- Authentifikation* von *starker Authentifikation* spricht.

Single Sign-on (SSO)

ermöglicht den Zugang zu vielen Systemen und Ressourcen, dabei genügt eine einmalige Authentifikation.

Bei SSO muss sich der Nutzer nur einmal einloggen und hat dann transparenten Zugang zu allen Services und Anwendungen, zu deren Nutzung er berechtigt ist. Dies gilt solange, bis vereinbarte Zeitlimits überschritten werden oder der Nutzer die Session selbst beendet (Log-out). SSO hat den Vorteil, benutzerfreundlich zu sein und ermöglicht es Firmen, Authentifikationen konsistent zu managen. Der Nachteil ist, dass alle Systeme auf die Sicherheit eines Authentifikations-Services angewiesen sind. In Web-basierten SSO-Systemen kann per Browser auf Web-Applikationen zugegriffen werden. Der Zugang zu anderen Ressourcen des Unternehmens, auch zu Legacy-Systemen, kann jedoch durch Anpassung an spezielle Interfaces realisiert werden.

Federated SSO ermöglicht Nutzern das Sign-on bei einem Mitglied einer miteinander verbundenen Interessentengruppe (Affiliate Group), mit anschließender Nutzung von Sites anderer Mitglieder dieser Interessengruppe, ohne dass sich der Nutzer dabei ein weiteres Mal authentifizieren muss.

Autorisierung

ist der Vorgang, berechtigten Zugang zu gewähren. Bei der Autorisierung wird der Zugang zu Datenbanken oder Anwendungen mittels Access-Control-Listen oder Zertifikaten oder anderer Zugangskontrollmethoden überprüft und bei Berechtigung Zugang gewährt.

Access Control

umfasst alle Mechanismen und Maßnahmen, die erforderlich sind, um berechtigten Nutzern Zugang zu Unternehmensnetzen und entsprechenden Ressourcen zu gewähren, einschließlich Zugangs-Policy, Authentifikation, Identity Management, Autorisierung, Auditing, Monitoring und Supervising.

6.4.2 Authentifikationstechniken

Sowohl Internet- als auch Unternehmensanwendungen müssen gegen unberechtigten Zugang durch Authentifikationstechniken geschützt werden. Die dazu erforderlichen Komponenten und Schnittstellen sind in Bild 6.14 dargestellt.

Das Diagramm zeigt einen Gesamtüberblick. Obwohl nicht vollständig, wird die Vielfalt der Komponenten auf den verschiedenen Ebenen sichtbar und die Komplexität deutlich. Zur Gewährleistung einer End-to-End-Authentifikation oder sogar SSO-

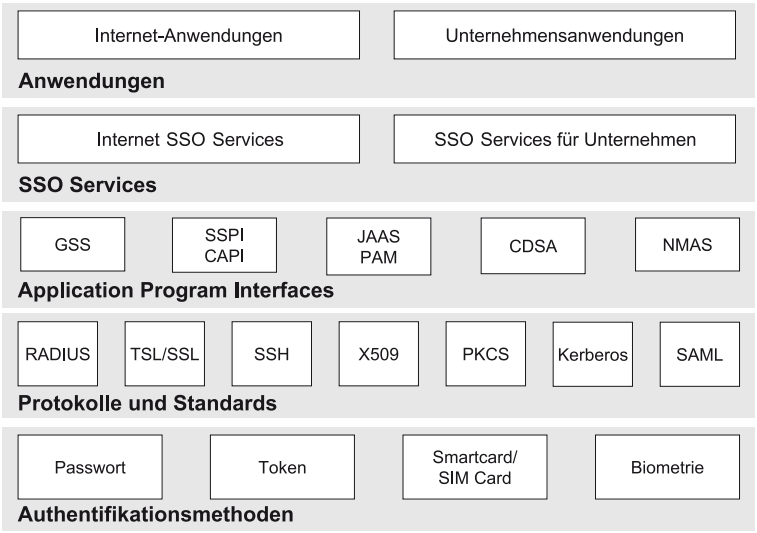


Bild 6.14 Building Blocks für Authentifikation und SSO

Funktionalität sind Methoden, Komponenten und Schnittstellen genau aufeinander abzustimmen.

Die verschiedenen Ebenen werden auf den folgenden Seiten beschrieben.

Authentifikationsmethoden

Wie in Bild 6.15 dargestellt, können Unternehmen je nach Sicherheitsanforderungen unterschiedliche *Authentifikationsmethoden* einsetzen. Häufig wird eine geeignete Lösung auch durch Kombination dieser Methoden erreicht.

Die Alternativen sind durch die variable Anwendung der drei Faktoren der Authentifikation gegeben: etwas, das man weiß (Faktor eins), etwas, das man hat (Faktor zwei)

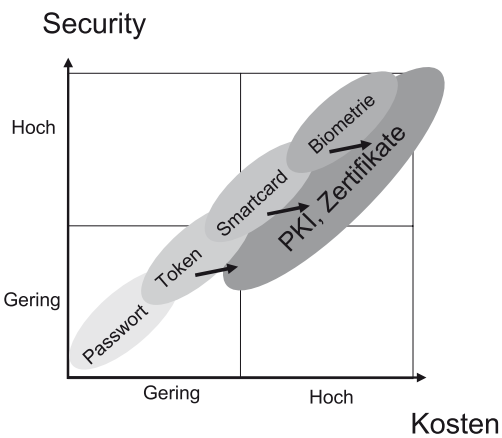


Bild 6.15
Authentifikationsmethoden

und etwas, das man selber repräsentiert (Faktor drei). Die drei Faktoren korrespondieren mit den dargestellten Methoden: Passwort (eins), Token/Smartcard (zwei) und biometrische Methoden (drei). Jede dieser Methoden hat ihre besonderen Eigenschaften und ist entsprechend vorgegebener Sicherheitsrichtlinien einzusetzen.

Passwort

Passwörter und/oder PINs in Kombination mit einer Benutzeridentifikation (User ID) sind und bleiben für viele Anwendungen im Internet die dominierende Authentifikationsmethode. Die Anwendung verlangt die Eingabe einer Zeichenfolge und/oder einer PIN, die über das Netz an ein Authentisierungsprogramm zur Überprüfung übermittelt wird. Es handelt sich dabei um eine schwache Authentifikation, da sie sich relativ einfach manipulieren lässt. Einige Angriffsmöglichkeiten können durch Verschlüsselung der zu übermittelnden Zeichenfolge ausgeschlossen werden.

Die größte Schwachstelle ist der Anwender selbst. Häufig werden kurze Passwörter benutzt, die meisten können mit sogenannten Dictionary-Attacken geknackt werden. PINs oder kurze Ziffernfolgen sind grundsätzlich unsicher. Ausschließlich starke Passwörter, die aus einem Mix von Zeichen, Ziffern und Sonderzeichen bestehen, wie z. B. 225.xA6$zo, können Dictionary-Attacken widerstehen.

Unternehmen sind gut beraten, nur starke Passwörter zuzulassen und strenge Richtlinien aufzustellen und konsequent anzuwenden. Nutzer müssen angehalten werden, Passwörter unzugänglich zu machen. Accounts sollten nach wenigen Fehlversuchen gesperrt werden. Die regelmäßige Erneuerung von Passwörtern (z. B. nach jeweils 90 Tagen) gehört ebenfalls zu einer adäquaten Passwort-Policy. Im Allgemeinen führen aber solche stringenten Richtlinien zu erhöhten Trainings- und Support-Kosten und verringerter Akzeptanz bei den Nutzern. Deshalb ist ein Trend zur Selbstverwaltung zu erkennen. Dabei pflegt der Nutzer das eigene Profil in einem Directory selbst. Von dort wird es per Synchronisation in andere Systeme übernommen oder das Log-in wird über dieses Directory gesteuert.

Token

Access Token (Zugangsschlüssel) repräsentieren den Authentifikationsfaktor *etwas, das man hat*. Solche Schlüssel können aus Software oder Hardware bestehen. Wichtig ist, dass verantwortliche Organisationen nicht nur den Schutz des geheimen Algorithmus gewährleisten, auf dessen Basis die Authentifikation stattfindet, sondern auch einen gesicherten Verifikationsvorgang zwischen Nutzer, Gerät und Authentication Server.

Üblicherweise wird die Sicherheit bei Authentifikationsverfahren dadurch garantiert, dass private Schlüssel in Hardware geschützt sind und/oder geheime Schlüssel verschlüsselt über das Netz transportiert werden. Organisationen müssen aber auch genaue Richtlinien festlegen, wie Nutzer identifiziert und wie Access Token generiert und an Nutzer übergeben werden.

Ein typisches Beipiel für ein Hardware Token ist die *SecurID Card* der Firma RSA Security. Sie zeigt über das Diplay eine Ziffernfolge an, die pro Minute nach einem bestimmten Algorithmus geändert wird und damit ein kurzlebiges Passwort darstellt,

das in Verbindung mit einer PIN als Authentifikationsparameter benutzt wird. Da der Authentication Server die PIN und den Passwort-Algorithmus kennt, ist eine eindeutige Validierung gewährleistet.

Ein anderes Beispiel, die *ActivCard,* ist ein Challenge/Response-Gerät mit Display und Zifferneingabe. In diesem *Challenge/Response-Verfahren* startet der Nutzer das Log-on mit der Eingabe seiner User ID am PC. Nach Validierung der User ID wird eine Zahl, welche die *Challenge* repräsentiert, an den PC zurückgesendet und angezeigt. Der Nutzer tippt diese Ziffernfolge in die ActivCard ein und erhält als Antwort eine weitere Zahl auf dem Display – die *Response*. Er überträgt diese Response-Ziffernfolge in die Log-on-Session-Maske. Bei fehlerfreier Eingabe und Validierung erfolgt das Einloggen durch das System, das wiederum den Challenge/Response-Algorithmus kennt.

Software Token funktionieren ähnlich wie Hardware Token, erreichen allerdings nicht das hohe Sicherheitsniveau, da der jeweilige Algorithmus per Software abgebildet und damit in der Regel nicht so gut schützbar ist.

Smartcards/SIM Cards

Smartcards stellen eine besondere Form von Hardware Token dar. Sie finden als multifunktionales Tool Verwendung und können vielseitig für Security-Anwendungen eingesetzt werden.

Smartcards werden auch als *Prozessor-Chipkarten* bezeichnet und gehören zu den *Integrated Circuit Cards (ICCs),* deren Basis-Standards (*ISO 7816*) schon vor mehr als zehn Jahren definiert wurden. Smartcards werden heute erfolgreich in vielen Anwendungsfeldern eingesetzt. Immer mehr Unternehmen nutzen Smartcards als Mitarbeiterausweis oder Identity Card. Die Anwendungen können vielfältig sein: Zutrittskontrollen zu Gebäuden und Räumen, Authentifikation für Syteme und Anwendungen, Erzeugung digitaler Signaturen auf elektronischen Dokumenten, Speicherung privater und geheimer Schlüssel oder bargeldlose Bezahlung in Firmenkantinen. Ein Beispiel ist die Siemens Corporate Card, die mittlerweile weltweit als Mitarbeiterausweis eingesetzt wird und neben der Zutrittskontrolle zu Standorten für eine Reihe von Security-Diensten verwendet wird, die alle auf einer unternehmensweit ausgerollten PKI basieren.

Private und geheime Schlüssel werden am sichersten in speziell geschützten (Tamper-resistant) Modulen gespeichert. Smartcards basieren auf einer *Tamper-resistant*-Chiptechnologie, die sowohl Hardware- als auch Software-Schutzmaßnahmen auf einem sehr hohen Sicherheitsniveau aufweist. So eignen sich Smartcards, die mittlerweile als State-of-the-Art-Medium in vielen Geräten einsetzbar und wie Kreditkarten portabel sind, besonders als Speichermedium für *Private Keys* und andere schützenswerte Objekte.

SIM Cards, verwendet in Mobiltelefonen, basieren auf der gleichen ICC-Technologie und dem ISO Standard 7816 wie Smartcards, werden jedoch überwiegend nur zur Authentifikation der Teilnehmer bei ihrem Netzbetreiber verwendet. Dies kann sich allerdings schnell ändern, da mittlerweile Geräte in großer Anzahl auf dem Markt sind, die dem WAP-Standard 1.2 oder 2.0 entsprechen. Bestandteil dieser Standards ist das

Wireless Identification Module. Wie bereits in Kapitel 6.3 erläutert, ist *WIM* ein dediziertes Modul für private Schlüssel und Zertifikate des Nutzers, das außerdem über kryptographische Funktionen verfügt.

Biometrische Verfahren

Bei der biometrischen Authentifikation werden physische Charakteristika (etwas, das man selber ist) mit repräsentativen, vorher erzeugten und aufgezeichneten Mustern verglichen. Bekannte *biometrische Verfahren* sind die Analyse von *Fingerabdruck* und *Iris* sowie die *Sprecherverifizierung*. Nach vielen Jahren aufwändiger Entwicklungen haben diese Verfahren nun einen gewissen Reifegrad erreicht, sind zuverlässig, weisen mittlerweile akzeptable Fehlerraten auf und können zu vertretbaren Kosten realisiert werden. Allerdings ist der Bedarf für einen breiten Einsatz bei Geschäftsanwendungen nach wie vor nicht gegeben.

Die *biometrische Authentifikation* ist sicherlich die stärkste Form der Authentifikation, da es kaum Möglichkeiten der Nachahmung persönlicher Merkmale gibt. Aber auch hier gilt es, vollständig sichere und durchgängige Identifikations- und Authentifikationsvorgänge zu gewährleisten, die Nutzeridentifikation, Merkmalerfassung und -speicherung, Eingabegeräte und Authentication Server einschließen.

Ein vielversprechender Hybrid-Ansatz könnte die Kombination von Smartcards und Biometrie sein: Private Schlüssel, Zertifikate, Passwörter und biometrische Merkmale werden lokal verschlüsselt auf der Smartcard gespeichert und können kombiniert in vielfältigen Security-Verfahren verwendet werden.

Digitale Zertifikate/PKI

Die Public Key Infrastructure (PKI) wird zur Authentifikation sowie für die Integrität und Verschlüsselung von Informationen genutzt. Sie umfasst Software, Krypto-Technologien und Services, um die Kommunikation über beliebige Netze und Business-Transaktionen vollständig sicher abwickeln zu können. Die PKI schließt ein System von digitalen Zertifikaten sowie ein Trust Center ein, das diese Zertifikate erzeugt. Die PKI unterstützt Authentifikationsvorgänge und die Integrität von Daten, indem mittels digitaler Zertifikate die Identität des Nutzers und die Authentizität und Unverfälschtheit einer Nachricht verifiziert werden können. Durch Unterstützung der Verschlüsselung von Daten und Nachrichten wird die Geheimhaltung von Informationen gewährleistet.

Protokolle und Standards für die Authentifikation

Wie in Bild 6.14 dargestellt, gibt es mehrere Authentifikationsprotokolle für unterschiedliche Einsatzfälle. Gängige Authentifikationsprotokolle umfassen *Transport Layer Security (TLS)/Secure Socket Layer (SSL)*, *Remote Access Dial-in User Services (RADIUS)*, *Kerberos V5 und Security Assertion Markup Language (SAML)*. Public Key sowie kryptographische Standards und Funktionen ergänzen diese Protokolle mit Security-Mechanismen und Datenformaten. Dazu zählen Formate für *X.509 Zertifikate*, *Public Key Cryptography Standards (PKCS)* und weitere Mechanismen, z. B. für das

Hashing, wie *Digest-MD5*, *Secure Hash Algorithm (SHA-1)* sowie der Krypto-Standard *Advanced Encryption System (AES)*.

Remote Access Dial-in User Services (RADIUS)

RADIUS [6.4.2] ist ein heute häufig angewendetes Authentifikationsprotokoll für die Einwahl über Telefonnetz oder Internet auf einen zentralen Authentication Server. RADIUS verschlüsselt User ID und Passwort bzw. Challenge/Response-Daten bei der Übertragung über das Netz.

RADIUS hat sich mittlerweile auch zum Standard-Mechanismus für Internet-Service-Provider (ISPs) entwickelt, die Authentifikationen von Clients zu Unternehmensnetzen durchleiten. Besonders im Zusammenhang mit *Virtual Private Networks (VPN)* benutzen Produkte von Check Point, Cisco, RSA SecurID und viele andere RADIUS als den gängigen Authentifikationsmechanismus.

Transport Layer Security/Secure Socket Layer (TLS/SSL)

TLS/SSL [6.4.3] ist der Security-Mechanismus für sichere Web-Anwendungen. In einem Handshaking-Verfahren werden gegenseitige Authentifikation von Server und Client mittels X.509 Zertifikaten durchgeführt, Krypto-Algorithmen ausgehandelt, die während der Session verwendet werden. und Session Keys für Verschlüsselung und Integrität ausgetauscht. Die optionale Client-Authentifikation setzt voraus, dass der Client den Public Key des Servers kennt. Als Client ist das Gerät und nicht der Anwender gemeint.

Secure Shell (SSH)

SSH [6.4.4] ist ein Protokoll und ein Satz von Tools für entfernte Authentifikation und Zugang zu einem Server. SSH kann zur Absicherung des Netzverkehrs beliebiger Punkt-zu-Punkt-Verbindungen eingesetzt werden. SSH ist auf den meisten UNIX-Systemen, Windows- und Client-Plattformen ablauffähig und es existiert eine Open Source Software dafür. Das SSH-Protokoll besteht aus drei Komponenten: TLS gewährleistet Server-Authentifikation, Vertraulichkeit und Integrität, das User-Authentifikationsprotokoll authentifiziert den Client und das Connection-Protokoll ermöglicht das Multiplexen des verschlüsselten Tunnels in einzelne logische Kanäle.

X.509

X.509 [6.4.5] gehört als Untergruppe dem X.500 Directory-Standard an. X.509 definiert sowohl die Syntax für Zertifikate als auch das Protokoll, wie Zertifikate für die Authentifikation zu benutzen sind.

Public Key Cryptography Standards (PKCS)

PKCS definiert ein zu X.509 kompatibles System, das auf Public-Key-Technologie aufsetzt und Details wie Verschlüsselungsalgorithmen und Key-Formate spezifiziert. Der PKCS-Standard [6.4.6] besteht aus einer Reihe von Dokumenten, die von RSA

veröffentlicht werden und die Definition von Algorithmen, Nachrichteninhalten, Zertifikaten, Attributen und anderen kryptographischen Details umfassen. PKCS #7 und PKCS #10 z. B. werden heute in der Regel für Zertifikatsanfragen angewendet.

Kerberos

Kerberos [6.4.7] wurde vor vielen Jahren vom Massachusetts Institute of Technology entwickelt und ist ein sehr breit eingesetztes Authentifikationssystem für die verteilte Verarbeitung. Es basiert auf einer Passwort-Authentifikation und einem zentralen Authentifikations-Server, der als *Key Distribution Center (KDC)* bezeichnet wird. Der KDC gibt sogenannte Tickets an Nutzer aus und gewährt damit Zugang zu Anwendungen. Das KDC-Konzept ermöglicht optional die Delegation der Zugangserlaubnis von einer Anwendung zu einer anderen und ebenfalls optional den vertraulichen (trusted) Informationsaustausch zwischen Gruppen von KDCs in unterschiedlichen Domänen. Damit ist Kerberos das einzige weitverbreitete Protokoll, das eine End-to-End-Nutzer-Identifikation und -Authentifikation über vielfache Applikationen in einem verteilten, interaktiven Anwendungsszenario gewährleistet. Kerberos ist heute standardmäßig in Windows und fast allen UNIX- und Linux-Systemen implementiert. Microsoft Kerberos ist interoperabel mit UNIX Kerberos, allerdings gibt es Einschränkungen bei der Autorisierung.

Security Assertion Markup Language (SAML)

SAML [6.4.8] ist ein XML-basierter Security-Standard. Diese XML-Security-Standards werden in Zukunft dominieren, weil sie plattformunabhängig, herstellerunabhängig und erweiterbar sind. In Kombination mit entfernten Funktionsaufrufen (RPCs) mittels Simple Object Access Protocol (SOAP) verkörpert SAML ein Authentifikationsprotokoll für heterogene Security Services. SAML ermöglicht eine Vereinigung (Federation) von Authentifikation in lose gekoppelten Domänen mit heterogenen Systemen und unterschiedlichen Authentifikationsmethoden. Obwohl noch relativ neu, ist das SAML-Protokoll bereits in vielen Authentifikationssystemen adaptiert worden.

APIs für Authentifikation

In der Schicht oberhalb der Standards und Protokolle befinden sich die Authentifikations-APIs wie in Bild 6.14 dargestellt. Häufig verwendete APIs sind das *Generic Security Service (GSS) API,* der *Java Authentication and Authorization Service (JAAS)*, das Microsoft *Security Support Provider Interface (SSPI)* und *CryptoAPI*, Intels *Common Data Security Architecture (CDSA)* API und Novells *Modular Authentication Service (NMAS)*.

Generic Security Service (GSS) API

GSS API ist ein Satz generischer Programm-Interfaces, die für Authentifikation, Datenintegrität und Datenvertraulichkeit entwickelt wurden. GSS wurde zusammen mit Kerberos im Wesentlichen auf UNIX-Systemen implementiert. Windows unterstützt GSS nicht. GSS hat aus diesem Grund nur eingeschränkte Bedeutung.

Security Support Provider Interface (SSPI) und CryptoAPI

Microsofts SSPI stellt ähnlich wie GSS einen generalisierten Security-Rahmen dar. Die Schnittstellen verbergen für den Anwedungsprogrammierer die Details von Authentifikation und Kryptographie. Das CryptoAPI ermöglicht die Nutzung spezifischer kryptographischer Funktionen ohne Kenntnis der verwendeten Algorithmen. Das CryptoAPI ruft zur Ausführung der Funktionen einsteckbare (pluggable) Module auf, sogenannte Cryptographic Service Provider (CSP). Das SSPI ist das High-Level Interface für Authentifikationsprozesse und für Kerberos, während das CryptoAPI Low-Level-Krypto-Funktionen ausführt.

Java Authentication and Authorization Service (JAAS) and Pluggable Authentication Module (PAM)

Der *Java Authentication and Authorization Service (JAAS)* bietet Interfaces für verschiedene Methoden zur Authentifikation: Passwörter, Kerberos Tickets und Zertifikate. JAAS ist die Java-Version des Pluggable Authentication Module (PAM) Frameworks, das ursprünglich von SUN entwickelt wurde und von Unix-Herstellern und Open Group Mitgliedern favorisiert wird. JAAS und PAM sind ein offenes und flexibles Framework für UNIX- und Linux-Plattformen und Java-basierte Anwendungen.

Common Data Security Architecture (CDSA)

Die CDSA wurde von Intel initiiert und die Security Working Group der Open Group hat die CDSA-Spezifikationen später übernommen, gepflegt und erweitert. Im Unterschied zum CryptoAPI ist CDSA betriebssystemneutral. Ein *Common Security Service Manager (CSSM)* stellt den Kern des Frameworks mit steckbaren und erweiterbaren Security-Services dar. Die Services umfassen Authentifikations-Services, kryptographische Funktionen und die Verwaltung von Zertifikaten.

Novell Modular Authentication Service (NMAS)

NMAS ist mit PAM, CDSA und SSPI vergleichbar und bietet ein erweiterbares Interface für Authentifikation. NMAS wird im Umfeld des Novell Directory eingesetzt und ist in Novells Produkten und einigen 3rd-Party-Anwendungen implementiert.

SSO-Services

Als oberste Ebene in Bild 6.14 vervollständigen die SSO-Services die Building Blocks für Authentifikation und SSO, wobei zwischen Internet SSO-Services und SSO-Services, die primär in Unternehmen eingesetzt werden, unterschieden wird.

SSO-Services ermöglichen nach einmaliger Authentifizierung den transparenten Zugang zu beliebigen Anwendungen für Nutzungsberechtigte, ohne dass bis zum Logout noch weitere Log-ins erforderlich sind. SSO-Services umfassen in der Regel Identifikation, Authentifikation und Autorisierung.

In den folgenden Kapiteln werden einige Web-basierte SSO-Ansätze und Technologien erläutert. Sie lassen sich folgendermaßen klassifizieren:

Microsoft .NET Passport ist ein Service, der ausschließlich von Microsoft angeboten wird, jedoch von beliebigen Internet-Anwendungen wie z. B. e-bay genutzt werden kann. Das *Projekt Liberty Alliance* ist als technologische Initiative zu verstehen, mit dem Ziel, Spezifikationen zu erstellen und offen zu legen, nach deren Definitionen Produkte von beliebigen Herstellern implementiert werden können. *Entrust GetAccess*, *RSA ClearTrust* und *Netegrity SiteMinder* sind verfügbare SSO-Services, die unabhängig von Anwendungsplattformen in unterschiedliche Infrastrukturen von Unternehmen integrierbar sind. *SAP Enterprise Portal SSO* und *IBM WebSphere/Tivoli SSO* sind plattformabhängige Services, die in die jeweilige Middleware dieser Anbieter voll integriert sind.

6.4.3 Microsoft .NET Passport

Ziele und Grenzen

Microsoft .NET Passport [6.4.9] besteht aus einer Reihe von Services zur Authentifikation von Nutzern beliebiger Websites im Internet. Der .NET Passport SSO-Service (Microsoft bezeichnet ihn als *Single Sign in Service*) ermöglicht die Authentifikation, indem er die Eingabe von nutzerspezifischer Angaben (Set of Credentials) erlaubt, die der Nutzer selbst bestimmt. Mittels dieser Credentials erhält der Nutzer Zugang zu jeder Website, die den .NET Passport Service unterstützt. Ein Beispiel ist die Website von e-bay. Auf den jeweiligen Log-in-Seiten befinden sich kleine *Sign-in*-Felder bzw. auf deutschen Webseiten Felder *Passport anmelden*. Mit dem Anklicken dieser Felder kann sich der Nutzer bei e-bay authentifizieren. Für diesen Authentifikationsvorgang wird im Hintergrund der Microsoft .NET Passport-Mechanismus genutzt.

Kunden, die bei .NET Passport registriert sind, können sämtliche Anwendungen der Websites, die Passport unterstützen, uneingeschränkt nutzen, indem sie sich einmal mit Mail-Adresse und Passwort identifizieren. Anbieter von Websites brauchen sich nicht um eine sichere Infrastruktur für die Authentifikation zu kümmern und können sich mehr auf ihre Kundenbeziehungen konzentrieren. Kundendaten bleiben beim Anbieter unabhängig von Passport erhalten und können beliebig erweitert werden. Sie korrespondieren mit Passport lediglich, um Kunden durch Name und Passwort eindeutig identifizieren zu können.

Kunden haben selbst die Kontrolle darüber, welche Daten an die von Passport unterstützten Websites weitergeleitet werden. Einige mögen an besonderen Services interessiert sein und erlauben deshalb die Weitergabe ausführlicher Profilinformationen, andere möchten, dass lediglich Name und Passwort an Websites übermittelt werden.

Das Ziel ist eine ausgewogene Lösung, die sowohl der Sicherheit und Vertraulichkeit als auch der Benutzerfreundlichkeit, je nach Priorität des Kunden, Rechnung trägt. Die Grenzen sind allerdings offensichtlich: Beides gemeinsam ist ohne Einschränkungen nicht zu erreichen. Passport bietet eine gewisse Flexibilität, um privaten und geschäftlichen Nutzern Spielraum zu geben.

Authentifikationsprozess und Single Sign-in

Passport basiert auf dem Kerberos-Security-Mechanismus, der um einige Funktionen erweitert wurde. Passport Messages werden in Form von elektronischen Tickets übermittelt. Nach Auswertung des Tickets kann die ausgewählte Site feststellen, ob der Kunde bereits ein erfolgreiches Sign-in getätigt hat. Das Ticket enthält neben Informationen, die im Authentifikationsprozess eine Rolle spielen, auch den Zeitpunkt, wann er sich das letzte Mal eingeloggt hat. Bei Passport ist das Ticket in Form eines verschlüsselten Cookies realisiert. Bild 6.16 zeigt die aufeinanderfolgenden Schritte der Authentifikation und des Single-Sign-in-Prozesses.

Schritt 1: Ein Nutzer, der bereits bei Passport.com registriert ist und einen Passport-Account besitzt, möchte auf eine geschützte Website zugreifen. Er klickt auf das Standard Passport *Sign in Logo* auf dieser Website, um den Authentifikationsprozess anzustoßen.

Schritt 2: Der Nutzer wird zu Passport umgeleitet.

Schritt 3: Passport überprüft das Cookie des Nutzers, um festzustellen, ob er bereits ein aktives Ticket hat. Da es sich aber um den ersten Authentifikationsversuch handelt, ist dies noch nicht der Fall. Passport behält die Information, die Site A bei der Umleitung mitgeliefert hat, und leitet den Nutzer zu einer Seite weiter, die ihn zur Eingabe von Name und Passwort auffordert. Nach korrekter Eingabe folgt Schritt 4.

Schritt 4: Der Nutzer wird von Passport zur Site A zurückverwiesen. In Form von Cookies bringt er dabei zwei verschlüsselte Informationen mit. Das erste Cookie enthält das Ticket für die Authentifikation, das zweite die Profilinformationen, die der Nutzer zur Weitergabe an Websites definiert hat, sowie einige operationale Informatio-

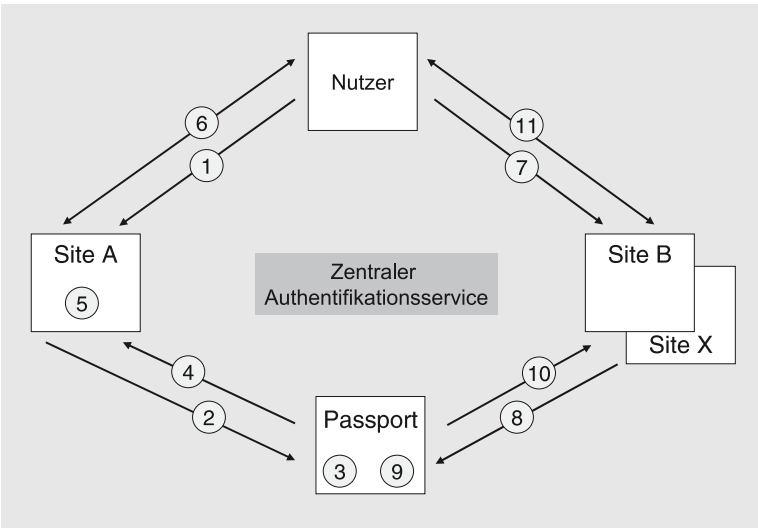


Bild 6.16 Passport-Single-Sign-in-Prozess

nen und Identifier. Diese beiden Cookies werden entschlüsselt unter Verwendung eines geheimen Schlüssels, der nur zwischen Site A und Passport vereinbart wurde.

Schritt 5: Site A entschlüsselt das Authentifikations-Ticket sowie die Profilinformationen und erlaubt dem Nutzer nun Zugang zur Site (Sign in). Außerdem erzeugt Site A nun ein eigenes Cookie, das fortan für den Zugang zu allen Applikationen von Site A benutzt wird, indem mittels der Passport User ID in einer entsprechenden Datenbank Zugang und Autorisierungen überprüft werden. Die Profilinformationen können dabei für Personalisierungszwecke genutzt werden.

Schritt 6: Der Nutzer ist jetzt in der Lage, beliebige Seiten der Site A aufzurufen und deren Services in Anspruch zu nehmen.

Schritt 7: Der gleiche Nutzer möchte nun Zugang zu Site B. Dazu klickt er auf das Standard Passport Sign in Logo der Site B.

Schritt 8: Wie in Schritt 2 wird der Nutzer zu Passport umgeleitet.

Schritt 9: Passport liest das Cookie des Nutzers, um zu überprüfen, ob er bereits ein aktives Ticket besitzt. Da dies der Fall ist, kann der Nutzer direkt zur Site B zurückgeleitet werden und Schritt 10 folgt. Die Schritte 8, 9 und 10 werden dabei vom Nutzer nicht wahrgenommen.

Site B kann für die Authentifikation verschiedene Alternativen wählen. Da das Ticket auch einen Zeitstempel enthält, kann Site B entscheiden, ob das Ticket ggf. aktualisiert werden muss, weil es bereits ein definiertes Zeitlimit überschritten hat. Liegt das Ticket noch im Zeitlimit, verweist Passport den Nutzer wieder zu Site B mit den verschlüsselten Ticket- und Profil-Cookies zurück. Ist das Ticket jedoch bereits abgelaufen, fordert Passport den Nutzer auf, seine Credentials nochmals einzugeben, um das Ticket zu erneuern.

Alle teilhabenden Websites können individuell die Gültigkeitsdauer von Tickets bestimmen. Außerdem haben sie die Möglichkeit, unabhängig von der Gültigkeit des Tickets, eine nochmalige Eingabe des Passwortes zu verlangen, was eine zusätzliche Sicherheit bedeutet und für Websites mit sensitiven Informationen zu empfehlen ist.

Schritt 10: Dieser Schritt ist identisch mit Schritt 4/5 in Bezug auf Site B.

Schritt 11: Dem Nutzer wird der Zugriff auf die angeforderten Seiten, Ressourcen und Services gewährt.

Jede weitere Authentifikation auf andere Sites X geschieht dann in derselben Weise wie in den Schritten 7 bis 11 beschrieben. Aus Sicht des Nutzers entspricht diese Prozedur einem Single Sign-in, egal auf wie viele Websites er schließlich zugreift.

Das Log-out wird einfach per Klick auf das entsprechende Passport Sign out Logo ausgelöst, das sich auf allen teilhabenden Sites befindet. Dadurch werden die Cookies von sämtlichen beteiligten Rechnern wieder eliminiert.

Nutzer können wählen, ob das Passport Sign in künftig automatisch geschehen soll. Wenn der Nutzer die automatische Sign in Funktion wählt, ist die Passport-Sign-in-Seite nicht zu sehen und der gesamte Authentifikationsprozess, einschließlich der

Ticket-Ausstellung sowie der Ticket- und Profilübergabe an die Website, spielt sich im Hintergrund ab. Um diese automatische Funktion wieder aufzuheben, genügt es einfach den Passport *Sign out* Link zu wählen.

Zusätzliche Passport Services

Security Key

Passport bietet eine optionale zweite Security-Ebene, die von den teilhabenden Sites selbst gesteuert wird. Sites können zusätzlich zum Passwort eine 4-stellige PIN verlangen, bevor der Nutzer sensitive Transaktionen tätigen oder auf vertrauliche Informationen zugreifen kann. Anders als beim Passwort kann diese PIN nicht auf einem Computer gespeichert werden; sie muss jedesmal, wenn sie angefordert wird, erneut eingegeben werden.

Passport Express Purchase (.NET Passport Wallet)

Eine weitere Option zum Single Sign-in Service von Passport ist der *Express Purchase Service*. Dieser Service ermöglicht den Online-Einkauf durch Nutzung eines *.NET Passport Wallet* (eine Art Brieftasche), in dem Rechnungs- und Lieferdaten gespeichert werden. Mit diesem Service können Konsumenten Online-Einkäufe bei jeder Website tätigen, die diesen .NET Passport Express Purchase Service unterstützt. Mit wenigen Klicks werden die Kaufinformationen im Wallet gepeichert und ohne wiederholte Eingabe dem Händler über mit SSL verschlüsselte Leitungen zur Verfügung gestellt.

Kids Passport Services

Kids Passport Services bestehen aus einem Tool Set, der es Websites in den USA ermöglicht, den *Privacy Protection Act (COPPA)*, der im April 2000 eingeführt wurde, zum Schutz von Kindern zu implementieren. Eltern können diesen Service dazu verwenden, das Profil ihrer Kinder so zu modifizieren, dass die Kids auf definierte Websites, die Passport unterstützen, gar nicht oder nur eingeschränkt zugreifen können.

Unterstützung mobiler Geräte

Passport unterstützt auch *Windows Mobile*. Allerdings werden nicht alle .NET Passport-Funktionen angeboten wegen noch eingeschränkter Gerätefunktionen und der verschiedenen Browser, die auf diesen Geräten laufen. Schlüsselfunktionen wie Registration, Sign in und Sign out sind aber verfügbar.

Folgende Browser werden unterstützt: Microsoft Mobile Explorer (MME), HTML, i-mode Phones, WAP Phones, HDML (Handheld Device Markup Language) Phones.

Einsatz von .NET Passport

Unternehmen, die .NET Passport auf ihren Websites einsetzen wollen, müssen ein .NET Service Agreement unterschreiben. Das Standard .NET Service Agreement schließt auch ein Service Level Agreement (SLA) mit ein. Sites mit sehr hohem Ver-

kehrsvolumen können spezielle SLAs abschließen, um ihre besonderen Anforderungen abzudecken.

Mit der Unterschrift des .NET Service Agreements verpflichtet sich die teilnehmende Site, die persönlichen Daten ihrer Passport-Nutzer zu schützen und die Integrität ihres Systems sicherzustellen.

Beispielsweise beinhaltet der Vertrag, dass alle Websites eine Verpflichtung über den vertraulichen Umgang mit persönlichen Daten veröffentlichen müssen. Diese Veröffentlichung muss online und für Nutzer einfach zugänglich sein. Microsoft empfiehlt außerdem, dass Sites sich bei einer industrieweit anerkannten Organisation wie *TRUSTe* registrieren lassen, die ein Gütesiegel für Vertraulichkeit ausstellt.

.NET Passport wird heute als Authentifikations-Service für Microsofts MSN und Hotmail sowie für einige Hundert andere Websites genutzt.

Kommentar zu .NET Passport

Die Stärke von .Net Passport ist eine ausgewogene Balance zwischen Security, Vertraulichkeit und Benutzerfreundlichkeit und ist für die meisten Internet-Anwendungen geeignet, mit Ausnahme solcher, die ein besonders hohes Sicherheitsniveau erfordern.

Viele Kunden besuchen Websites nur gelegentlich und können sich deshalb oft nicht mehr an ihre Log-on-Daten erinnern. Bei dreimaliger Falscheingabe wird manchmal sogar der Zugang gesperrt. Analysen zeigen, dass Kunden dann oftmals aufgeben und für diejenigen, die sich ein neues Passwort zuweisen lassen, ist der Aufwand groß. Websites, die .NET Passport nutzen, brauchen sich um all diese Dinge nicht zu kümmern, und es kann weitgehend vermieden werden, dass frustrierte Kunden dann auf Online-Einkäufe verzichten.

Allerdings ist auf einige Punkte hinzuweisen, die die Einsatzmöglichkeiten von .NET Passport doch noch erheblich einschränken:

- Passport bietet zurzeit keine Form der starken Authentifikation an, wobei der Nutzer außer seinem Passwort auch noch etwas präsentieren muss, das er hat, wie ein digitales Zertifikat oder eine Smartcard.
- Wünschenswert wäre mehr Transparenz für Nutzer und Unternehmen, die Passport, einen zentralen und ausschließlich von Microsoft durchgeführten Service, einsetzen. Kontrolle und Überwachung durch eine unabhängige Organisation könnte dazu beitragen, das Vertrauen in Microsofts Passport Service zu stärken.
- Nutzer können nicht individuell bestimmen, welche persönlichen Daten an welche Website weitergegeben werden dürfen.
- Unternehmen, die Passport für interne Anwendungen einsetzen wollen, sind nicht in der Lage, Passport-Registrierungsformate und Authentifikationsprozeduren zu ändern. Existierende Authentifikationsmethoden können nicht integriert oder adaptiert werden. Passport ist außerdem nur für Web-Anwendungen geeignet.
- Passport ist derzeit nicht interoperabel mit anderen existierenden Authentifikationsmethoden.

Kunden und Unternehmen haben immer noch große Bedenken, dass sich Unberechtigte Zugang zu vertraulichen Daten und Firmenwerten verschaffen und diese manipulieren oder missbrauchen könnten. Aus diesem Grund wären Transparenz und unabhängige Überwachung von Passport sehr wichtig für eine verbesserte Akzeptanz.

Microsoft hat angekündigt, dass Passport zukünftig *WS-Security* unterstützen soll, so dass es mit anderen, ebenfalls den WS-Security-Standard unterstützenden Systemen interoperabel wäre. Durch die Integration dieser Standards in seine Produkte und Services würde Microsoft eine wesentlich offenere Lösung schaffen, die sich auch für föderierte Security-Szenarien eignen würde. In solchen Szenarien würde Passport einen Knoten in einem breit angelegten Föderationsnetz darstellen.

Des Weiteren spricht Microsoft von einer neuen Technologie für firmenübergreifende Authentifikation mit dem Codenamen *TrustBridge*. Unternehmen können TrustBridge kaufen und selbst betreiben. Die TrustBridge-Technologie soll es Unternehmen ermöglichen, ihren Authentifikationsknoten in ein Föderationssystem zu integrieren. Es soll dabei mit der Außenwelt über WS-Security kommunizieren. TrustBridge kann mit dem Active Directory oder mit Kerberos-basierten Systemen verbunden werden. Da sowohl Passport als auch TrustBridge den WS-Security-Standard unterstützen sollen, können Unternehmen, die TrustBridge einsetzen, gemeinsam mit dem Passport Service an einem föderierten Netz teilhaben.

Da .NET Passport in der heutigen Form nicht sehr erfolgreich außerhalb Microsofts eigener Services eingesetzt wird, ist die Wahrscheinlichkeit einer grundlegenden Weiterentwicklung in Richtung föderierter Identitäts-Services hoch. Diese Services orientieren sich mehr an dem neueren Liberty-Alliance-Ansatz.

6.4.4 Das Projekt Liberty Alliance

Das *Projekt Liberty Alliance* [6.4.10] wird durch ein breites Spektrum von Software-Herstellern und Industrievertretern repräsentiert, das sich zusammengetan hat, um für das Internet ein neues Niveau für Vertraulichkeit und sichere Kommunikation zu schaffen. Heute sind Identitäten im Internet fragmentiert über vielfältige Identity-Provider wie Unternehmen, Internet-Portale, Communities und andere Diensteanbieter. Dies hat bis heute zu einer schwerfälligen und unnötig aufwändigen Handhabung bei übergreifenden Authentifikationen geführt.

Eine föderierte Netz-Identität (*Federated Network Idenitity*) und *Single Sign-on* sind die Schlüsseltechnologien, um dieses Problem zu lösen. Der Ansatz einer föderierten Netz-Identität basiert auf einer offenen Architektur und im Gegensatz zu Microsoft Passport nicht auf den Services einer einzigen Firma. So war es wohl auch die Absicht des Projektes, die Liberty Alliance Standards gegen Microsoft Passport zu positionieren.

Ziele der Liberty Alliance

Die wesentliche Ziele von Liberty sind:

– beliebigen Netzteilnehmern Vertraulichkeit und Sicherheit ihrer Netz-Identitäten zu ermöglichen

– der Geschäftswelt die Möglichkeit zu geben, ihre Kundenbeziehungen ohne Dritte zu managen und zu pflegen
– einen Single-Sign-on-Standard zu kreieren, der eine dezentralisierte Authentifikation und Autorisierung mit mehreren Providern erlaubt
– eine Network-Identity-Infrastruktur zu schaffen, die sämtliche verfügbaren und zukünftigen Netzzugangsgeräte berücksichtigt.

Diese Eigenschaften können erreicht werden, wenn Organisationen sich zu sogenanten *Circles of Trust* zusammenschließen, in denen die geschäftlichen Vertrauensbeziehungen vereinbart werden. In einem Circle of Trust föderieren Nutzer die isolierten Accounts, die sie mit ihren jeweiligen Geschäftspartnern eingerichtet haben, so dass ihre Identitäten innnerhalb dieses Circle of Trust Gültigkeit haben.

Federated Network Identity

Heute sind unzählige Identity-Inseln über das Internet verteilt. Jede Firma, die mit dem Internet verbunden ist, hat ihr eigenes Identity-Schema für ihre Angestellten. Telekommunikationsunternehmen, Internet Service Provider und beliebige Service-Anbieter im Internet betreiben für die Pflege ihrer Kundenbeziehungen unterschiedliche Identity-Systeme.

Federated Network Identity ist die Lösung zur Überwindung dieser Inkonsistenzen und eröffnet gleichzeitig neue Geschäftsmöglichkeiten. In einer Welt des föderierten e-Commerce werden die Online-Identitäten des Nutzers – wie persönliche Profile und Kommunikationskonfigurationen, Kaufgewohnheiten sowie Reise- und Einkaufspräferenzen – vom Nutzer selbst administriert und in gesicherter Weise den von ihm ausgewählten Organisationen zur Verfügung gestellt.

Federated Network Identity bedeutet aber auch, dass Konsumenten wie Unternehmen die Möglichkeit haben, unterschiedliche Sätze von Identity-Informationen von separaten Anbietern managen zu lassen. Die Föderation von Accounts ermöglicht die Assoziierung und Einbindung der verschiedenen Internet Accounts eines Nutzers in eine vereinigte Gruppe von Partnern (Affiliated Group), die sich aus kommerziellen und nichtkommerziellen Organisationen zusammensetzen kann und durch gemeinsame vertragliche Vereinbarungen verbunden ist.

Föderierte Security ist die Möglichkeit und Fähigkeit für Websites, Services und Applikationen, Identities und Authentifikationsbestätigungen (Assertions), die von einem der vertrauensvollen Partner des Circles of Trust stammen, zu akzeptieren und sicher zu erkennen.

Nach Architektur und operationalen Vereinbarungen, wie von Liberty Alliance definiert, ermöglichen sogenannte *Circles of Trust*, dass Nutzer innerhalb eines Circles in sicherer und übergangsloser Art und Weise Transaktionen durchführen können, wie in Bild 6.17 illustriert.

Nach der Definition von Liberty partizipieren in einem Circle of Trust User, Service-Provider und Identity-Provider. Die Kategorie der Service-Provider schließt beliebige Anbieter im Web wie Internet-Portale, Händler, Reiseanbieter, Banken und Versiche-

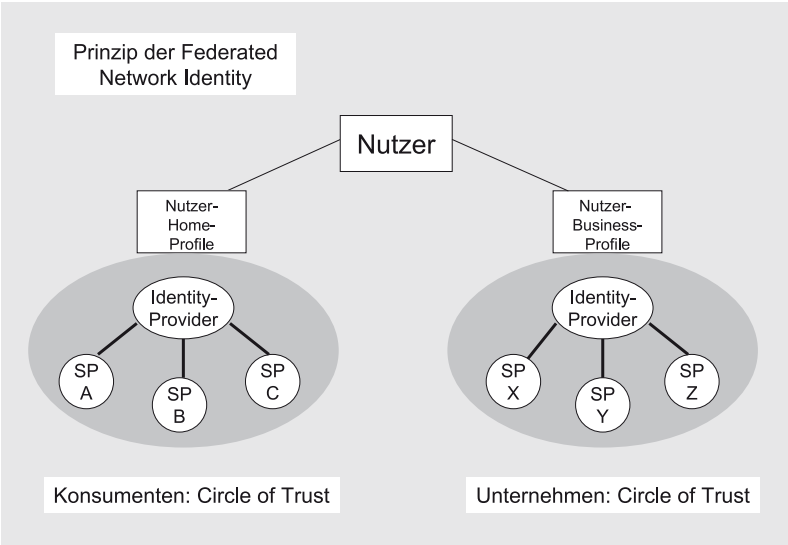


Bild 6.17 Prinzip der Federated Network Identity

rungen, Unterhaltungsanbieter, Vereine und Verbände, Ministerien und Kommunen usw. ein. Identity-Provider sind Service-Provider, die für andere Provider geschäftliche Anreize bieten, so dass sich die Partner entsprechender vertraglicher Vereinbarungen zusammenschließen (affiliate). Beispielsweise könnte im *Circle of Trust* ein Identity-Provider die Identitäten der Angestellten aller partizipierenden Unternehmen betreuen. Ein anderes Beispiel ist der *Circle of Trust* von Konsumenten. Hier könnte eine Bank geschäftliche Beziehungen zu anderen Service-Providern aufbauen, um es sowohl ihren Kunden als auch diesen partizipierenden Service-Providern zu ermöglichen, Kunden-Identitäten untereinander zu nutzen. Ein- und dieselbe Organisation kann beides repräsentieren, den Identity-Provider und den Service-Provider, entweder generell oder auch nur für einzelne Interaktionen.

Um derartige Szenarien zu verwirklichen, müssen Service-Provider und Identity-Provider ihre Infrastrukturen entsprechend der Liberty-Spezifikationen aufrüsten, während Nutzer nichts anderes benötigen als die üblichen Web Browser.

Angewandte Techniken

Web Redirects

Liberty benutzt den *HTTP Command 302 Temporary Redirect*. Web Redirects funktionieren, indem der URI (Unified Resource Identifier) einer anderen Location in das Location-Feld der HTTP-Antwort eingesetzt wird. Der Browser, der die Antwort empfängt, führt dann automatisch eine Anweisung HTTP GET aus, die auf den mitgelieferten URI verweist. Dies ermöglicht den Aufbau eines direkten Kommunikationskanals zwischen Identity-Provider und Service-Provider. Während des Web Redirect können

auch private Informationen in der HTTP Message übertragen werden. Diese Informationen werden durch Verwendung des HTTPS-Protokolls geschützt.

SSL

SSL verschlüsselt alle HTTP-Kommunikationen zwischen Client und Server, so dass vertrauliche Informationen auch im Fall einer angezapften Leitung geschützt wären.

SOAP und SAML

Liberty verwendet für den Austausch von Identity-Informationen existierende Protokolle und Sprachen wie SOAP, SAML und Web Redirects. Die SOAP Message enthält neben der eigentlichen Nachricht die Aussage, wer sie bearbeiten soll und ob sie obligatorisch oder optional ist. Die SOAP Messages übermitteln außerdem die Liberty-Verarbeitungsregeln für die auszutauschenden Datentypen. Auch Remote Procedure Calls mittels SOAP (Web Services) werden in Liberty verwendet.

SAML definiert drei Assertion-Typen: Authentifikation, Attribute und Autorisierung. Liberty verwendet Authentifikationbestätigungen (Assertions), die aussagen, zu welchem Zeitpunkt ein Subjekt durch welches Mittel authentifiziert wird.

SAML-Authentifikationen werden entweder durch SOAP oder Web Redirects zum Austausch von Identity- und Authentifikationsinformationen befördert.

Single-Sign-on-Prozess

In Bild 6.18 ist ein Beispielszenario des Single-Sign-on-Prozesses nach Liberty-Spezifikation dargestellt, im Folgenden wird es erläutert.

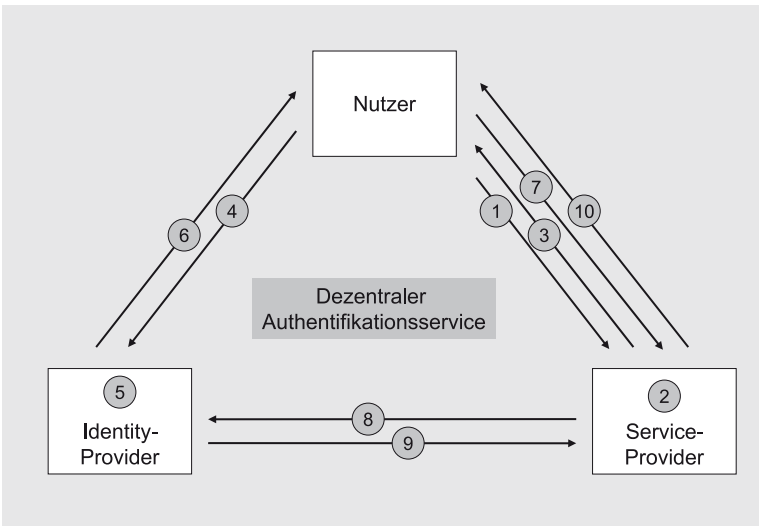


Bild 6.18 Liberty-Single-Sign-on-Prozess

Schritt 1: Auf der Website des Service-Providers wählt der Nutzer einen Identity-Provider für die Authentifikation aus (je nach vordefiniertem Ablauf kann diese Auswahl auch direkt der Service-Provider vornehmen). Die Auswahl des Identity-Providers geschieht auf der Website des Service-Providers z. B. durch Klicken auf das entsprechende Logo oder durch Eintrag in ein Dialogfeld oder indirekt durch Anforderung einer bestimmten Webseite, so dass der Service-Provider den Identity-Provider aus dem Kontext entnehmen kann.

Schritt 2: Der Service-Provider bestimmt die Adresse des Identity-Providers und generiert einen alternativen URI, der auf die Adresse des Identity-Providers zeigt.

Schritt 3: Der Service-Provider gibt auf die Anfrage des Nutzers eine HTTP-Antwort, die im Location-Feld den alternativen URI des Identity-Providers enthält. In dieses alternative URI-Feld ist ein zweiter URI eingebettet, der zurück auf den Service-Provider verweist.

An dieser Stelle variiert das Liberty-Protokoll, je nachdem ob es auf HTTP GET, POST oder auf WML Browsern basiert. Im Folgenden wird das am häufigsten vorkommende Szenario, d.h. Nutzung von HTTP GET, beschrieben.

Schritt 4: Der Browser des Nutzers stellt eine HTTP-GET-Anfrage an den Identity-Provider mittels des URI, der in Schritt 3 vom Service-Provider übermittelt wurde.

Schritt 5: Der Identity-Provider verarbeitet diese HTTP-GET-Anfrage. Falls der Nutzer nicht schon authentifiziert war, geschieht die Authentifikation jetzt.

Schritt 6: Der Identity-Provider antwortet mit einer Authentifikationsbestätigung (in Form eines sogenannten SAML Artefact) oder mit einer Fehlmeldung. Diese Antwort wird durch einen HTTP Redirect transportiert, der im Lokationsfeld den URI des Service-Providers enthält.

Schritt 7: Der Browser des Nutzers erhält die Authentifikationsbestätigung. Der Nutzer sendet daraufhin eine HTTP-GET-Anfrage an den Service-Provider mit der kompletten URI aus dem Location-Feld der in Schritt 6 erhaltenen Antwort.

Schritt 8: Die Schritte 8 und 9 erfolgen nur, wenn in Schritt 6 als Antwort ein SAML-Artefact gesendet wurde (Das SAML-Artefact ist eine kleine Zufallszahl, die auf Authentifikationsbestätigungen verweist.). Der Service-Provider versucht nun die Authentifikationsbestätigung zu bekommen, die zum erhaltenen SAML-Artefact korrespondiert. Dazu sendet er eine SOAP Message an den Identity-Provider und fordert diese Bestätigung an.

Schritt 9: Der Identity-Provider antwortet auf die Anfrage mit der korrespondierenden Authentifikationsbestätigung.

Schritt 10: Der Service-Provider sendet eine HTTP-Antwort an den Nutzer und schließt damit die Anfrage des Nutzers in Schritt 1 positiv ab. Der Nutzer hat nun Zugang zu allen Ressourcen des Service-Providers, für die er autorisiert ist (Single Sign-on).

Kommentar zu Liberty

Liberty Alliance verfolgt einen offenen und Standard-basierten Ansatz, der sich als SSO-Lösung gleichermaßen für B2C-, B2E- und B2B-Geschäftsmodelle eignet.

Da die Ergebnisse aus dem Projekt Liberty Alliance jedoch keine Produkte, sondern lediglich Spezifikationen sind, werden zuverlässige Produkte, die auf dem Stand der neuesten Versionen sind, erst nach und nach verfügbar sein.

Liberty und Web Services Security setzen beide auf den XML-basierenden Security-Standards wie SAML, XML Signature, XML Encryption, XACML (Access Control) und XKMS (Key Management) auf und können deshalb als zukunftsorientierte und zukunftssichere Technologien eingestuft werden. Allerdings werden wohl einige Jahre ins Land ziehen, bis der Beweis geführt ist, dass keine Security-Schwachstellen existieren und die komplexen Föderationsmechanismen in beliebigen Szenarien und auch in einem Massenmarkt praktikabel funktionieren.

Wenngleich auch .NET Passport und Liberty derzeit noch ganz unterschiedliche Identity-Ansätze verfolgen, ist doch zu hoffen, dass Weiterentwicklungen eine Interoperabilität ermöglichen werden.

6.4.5 Entrust GetAccess

Im Unterschied zu .NET Passport ist das Zielsegment des SSO-Service *GetAccess* von der kanadischen Firma Entrust die Integration dieses Service in das existierende Anwendungsumfeld von Unternehmen. Der Service ist so konzipiert, dass verschiedene, bereits eingesetzte Security-Mechanismen weiterverwendet werden. Im Unterschied zu Liberty handelt es sich um reale Lösungskomponenten und nicht um einen Satz von Spezifikationen, wobei Entrust allerdings die Umsetzung des Liberty-Ansatzes verfolgt.

Portfolio

Als Grundlage der *Entrust Secure Web Portal Solution* [6.4.11] bietet das *Entrust GetAccess* Portfolio einen einzigen Zugangspunkt für die Identifikation und die Berechtigung zur Nutzung von Web-Portal-Applikationen.

Die Software Entrust GetAccess umfasst ein zentralisiertes Security-Management sowie folgende Services und Funktionen:

Identifikation, Authentifikation und Single Sign-on

GetAccess ermöglicht S*ingle Sign-On (SSO)* für Web-Ressourcen und Applikationen von Websites. Hat sich ein Nutzer erst einmal beim GetAccess Server identifiziert, ist keine weitere Authentifikation auf Anwendungsebene erforderlich. GetAccess verifiziert dann die Credentials (Authentifikationsparameter) des Nutzers und informiert die Anwendung über die Identität des Nutzers.

GetAccess unterstützt die folgenden Authentifikationsmethoden und -mechanismen:

– User ID/Password

– externes LDAP Directory
– digitale Zertifikate nach X.509v3
– verschiedene Token (einschließlich Smartcards und RSA SecurID)
– Windows-Domain-Authentifikation.

Autorisierung und Rollen-basierte Zugangskontrolle

GetAccess realisiert Autorisierungen (*Entitlements)* durch ein Modell der Rollen-basierten Zugangskontrolle (*Roles-Based Access Control, RBAC)*. Dieses Modell verwendet die Zuweisung von Rollen in einem Unternehmen als Abstraktionsebene zwischen Nutzern und jenen Ressourcen, auf die Zugriff erfolgen soll. Zunächst wird durch einen Administrator festgelegt, welche Ressourcen zu schützen sind und für welche Rollen der Zugang freigegeben wird. Als nächstes werden den zu verwaltenden Nutzern die ihren Aufgaben in der Organisation entsprechenden Rollen zugeordnet. GetAccess ist auf Basis dieser Eintragungen in der Lage, den Zugang zu Ressourcen dynamisch freizugeben. Die Abstraktion reduziert den Aufwand, der erforderlich ist, um eine große Anzahl von Nutzern und Privilegien individuell zu verwalten.

Dynamic Resource Menu

Nach der Authentifikation generiert GetAccess ein personalisiertes HTML-Menü, das sämtliche Ressourcen und Applikationen aufzeigt, zu denen ein Nutzer Zugang hat. Dies ermöglicht schnelles Navigieren, ohne dass man nach irgendwelchen Bookmarks suchen muss. Außerdem zeigt es dem Nutzer den jeweils aktuellen Stand seiner Berechtigungen. Die angezeigten Ressourcen werden bei jedem Zugriff dynamisch neu berechnet, so dass für den Nutzer immer der letztgültige Stand seiner Zugangsberechtigungen sichtbar ist.

Multi-Domain-Zugang

Wenn Unternehmen sich mit anderen zusammenschließen oder Partnerschaften eingehen oder aber sich in verschiedene Markenbereiche aufsplitten, wird eine Ausweitung von Identifikationen und Berechtigungen auf mehrere Internet Domains unumgänglich. Allerdings können Cookies, die primär für die Speicherung von Credentials in Browsern benutzt werden, wegen ihrer eingeschränkten Implementierung nicht über mehrere Domains hinweg verwendet werden. Deshalb geht GetAccess einen anderen technischen Weg für die Unterstützung von Multi-Domain-Authentifikation, Autorisierung, Session Management, Rücknahme von Zertifikaten (Revocation) in Echtzeit sowie für das Log-out.

Kundenspezifische Oberflächen

Die HTML-Seiten, die von GetAccess generiert werden, basieren auf einem Schablonen-Modell (Templates), so dass eine Anpassung an ein bestimmtes Look-and-Feel einfach ist und der Inhalt der Seiten nicht berührt wird.

Web-basierte Administration und Delegation

Der GetAccess Server ist mit einem Browser-basierten Administrations-Tool ausgestattet. Mit diesem Tool lassen sich alle Nutzer, Rollen, Ressourcen und weitere Objekte managen. Da es lediglich einen Browser erfordert, ist auf den Administrationsplätzen keine Installation notwendig. Administratoren können auch aus der Ferne (remote) die Security-Infrastruktur einer Organisation betreuen.

GetAccess ermöglicht die Delegation von administrativen Aufgaben. Das Delegationsmodell eröffnet die Möglichkeit, unterschiedliche Niveaus von Administrationsprivilegien an Administratoren zu delegieren.

Self-Service und automatisches Provisioning

Self-Service erlaubt es Nutzern sich selbst ohne administrative Eingriffe am GetAccess Server registrieren zu lassen. Dabei werden automatisch die ihrer Funktion entsprechenden Berechtigungen zugewiesen (Provisioning).

GetAccess kann an bereits existierende User-Management-Systeme, wie ein LDAP-Directory oder eine Windows-Domain-Infrastruktur, angeschlossen werden. Ein Nutzer, der bereits in einem externen Directory registriert ist, kann sich selbst am GetAccess Server anmelden, indem er die gültigen Authentifikationsparameter für das externe Directory präsentiert. GetAccess validiert die Credentials bei diesem Directory und erzeugt automatisch einen GetAccess Account für den Nutzer, wenn die Validierung positiv verlaufen ist.

GetAccess bietet auch einen Self-Service für die Pflege der Nutzer-Accounts. Authentifizierte Nutzer können für ihre eigenen Accounts Passwörter ändern und Präferenzen auswählen.

Integration von Nicht-Web-Anwendungen

Das GetAccess-Portfolio enthält auch ein Toolkit, das die Integration von Client/Server- und anderen Nicht-Web-Anwendungen in das GetAccess-System erlaubt. Das dafür verfügbare API, genannt CAAS (Client Authentication and Authorization Service), ist in den Sprachen Java und C++ implementiert.

CAAS stellt ein programmatisches Interface für die GetAccess-Funktionalität zur Verfügung und kann verwendet werden für die Authentifikation von Nutzern zum Erhalt ihrer Credentials, zur Zugangskontrolle und zur Überprüfung der Gültigkeit einer User Session.

APIs und Erweiterungen

Um die Integration von GetAccess in die IT-Landschaft von Unternehmen zu erleichtern, bietet das Produkt Schnittstellen, die den programmtechnischen Zugriff auf User-Management-Funktionen ermöglichen. Implementiert in Java, können diese APIs verwendet werden, um andere User-Management-Systeme anzubinden, einschließlich existierender ERP-/HR-Systeme und 3rd-Party-Administrations-Tools. APIs können

auch dazu benutzt werden, Meta-Tools zu entwickeln, die es erlauben, über ein einziges Interface, zusammen mit dem GetAccess Server, mehrere Infrastruktur-Komponenten zu managen. Die APIs können darüber hinaus zur Abfrage von Echtzeit- oder Batch-Updates dienen.

Es wird immer Situationen geben, in denen durch neue Geschäftsanforderungen Modifikationen im Ablauf oder im Verhalten des Systems notwendig werden. Das GetAccess-System hat verschiedene Interfaces, die sogenannten Events (Ereignisse), die zu definierten Ablaufpunkten stattfinden. Beispiele solcher Ereignisse sind erfolgreiches Log-in, fehlgeschlagenes Log-in, Passwort-Rücksetzung usw. Entwickler oder System-Integratoren können kundenspezifische Änderungen/Anpassungen durch Erweiterungen der entsprechenden Events vornehmen. Erweiterungen bestehen aus compiliertem Java Code, der die Kernfunktionalität von GetAccess ergänzt und die spezifischen Kundenanforderungen erfüllt.

Unterstützung mobiler Geräte

GetAccess bietet die Unterstützung mobiler Geräte mit dem *GetAccess Mobile Server*. Der Mobile Server kann in das GetAccess-Umfeld integriert werden und erlaubt den Zugang von PDAs und Mobiltelefonen zu entsprechenden Anwendungen. Voraussetzung ist allerdings die Integration solcher Anwendungen in die existierende IT-Infrastruktur, wie in Kapitel 4.3 erläutert.

Architektur

Die GetAccess-Architektur ist entsprechend der traditionellen Multi-Tier-Anwendungsarchitektur konzipiert. Die entsprechenden Services können auf üblichen Hardware- und Software-Plattformen im DMZ-Bereich oder im Intranet lokalisiert sein, wie in Bild 6.19 dargestellt.

Access Service

Der Access Service fungiert als User Interface für das Log-in, Log-out, Account Management und Ressourcen-Menü sowie für die Selbst-Registrierung. Die verschiedenen Servlets interagieren mit den entsprechenden Back-End-Komponenten, um die gewünschten Funktionen auszuführen. Der Access Service ist ein Client des Authentication and Authorization Routing Service (AARS), des Session Management Service (SMS) und des Registry Service. Auf den Access Service greift der Nutzer (User) mittels Browser über HTTP or HTTPS zu.

Identification and Authorization Service and Pluggable Authentication and Authorization Modules (PAAMs)

Die GetAccess-Architektur erlaubt das Einbinden von modularen Authentifikations- und Autorisierungs-Services, die zu entsprechenden Authentifikationsmethoden gehören. Diese Module, genannt PAAMs, repräsentieren die Funktionalität der jeweiligen Authentifikationsmethode. Diese Art der Abstraktion ermöglicht es, die restliche GetAccess-Infrastruktur ohne spezifische Kenntnisse der verschiedenen PAAM-Funk-

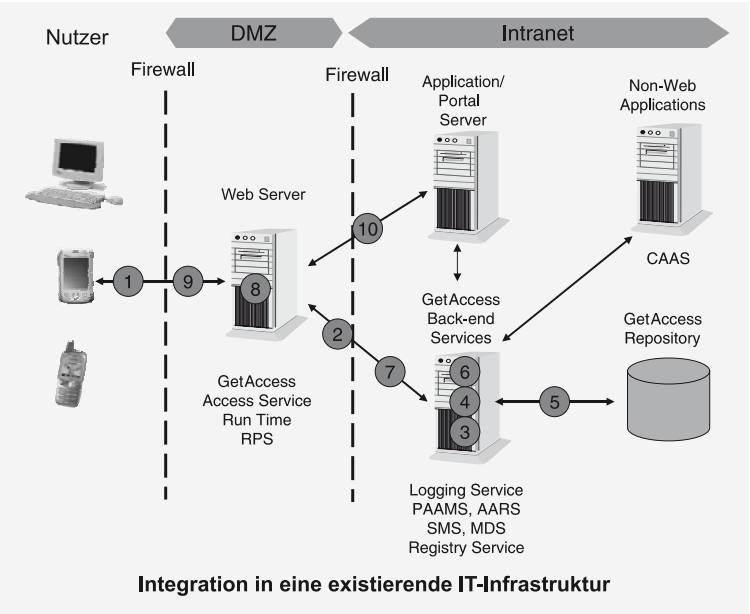


Bild 6.19 Entrust GetAccess

tionalitäten aufzubauen. PAAMs können aus ganz unterschiedlichen Quellen stammen: entwickelt vom Unternehmen, von Spezialanbietern solcher Security-Komponenten oder von Herstellern schon installierter Plattformen.

PAAMs werden vom GetAccess Authentication and Authorization Routing Service, abhängig von der verwendeten Authentifikationsmethode, aufgerufen.

Authentication and Authorization Routing Service (AARS)

Der AARS nimmt verschiedene Funktionen innerhalb des GetAccess-Systems wahr und ist zuständig für die Annahme der Authentifikationsanfrage beim Log-in. Außerdem leitet der AARS die erforderlichen Parameter zur Durchführung der Authentifikation zum entsprechenden PAAM weiter. Ist die Authentifikation erfolgreich, kommuniziert der AARS mit dem SMS (Session Management Service), um eine neue Session für diesen User zu starten. Der AARS ist darüber hinaus für die Verschlüsselung der User Credentials während der Log-in-Zeit verantwortlich.

Der AARS abstrahiert die Authentifikations- und Autorisierungslogik von der restlichen GetAccess-Architektur. Der AARS wird vom Access Service aufgerufen und dient als Client für die verschiedenen PAAMs, den Registry Service und den SMS.

Logging and Audit Service

Der zentralisierte Logging Service bietet Logging-Funktionen, die es dem Administrator erlauben, auf Komponenten-Ebene den Detailgrad der Logfiles festzulegen. Auf

diese Weise lassen sich Umfang und Art der Informationen auswählen, um Risiken und Ressourcen angemessen zu managen.

Session Management Service (SMS)

Der SMS führt eine Session-Tabelle, die alle aktiven User umfasst. Der Service hat die Aufgabe Sessions zu starten, wenn User authentifiziert sind, und Sessions zu verfolgen, während User auf verschiedene geschützte Ressourcen zugreifen.

Resource Protection Service (RPS)

Der RPS, auch als GetAccess-Runtime-System bezeichnet, ist als Plug-in für Web Server implementiert und führt sämtliche Zugangskontrollfunktionen zu den geschützten Ressourcen durch. Der RPS prüft jede einlaufende Web-Anfrage, um festzustellen, ob sie eine geschützte Ressource betrifft. Bei gültiger Berechtigung gibt RPS den Zugang frei.

Data Repository and Registry Service

Während GetAccess externe Directories und Datenbanken als Informationsquellen für Authentifikation und Autorisierung benutzt, betreibt es ein eigenes Repository, um Daten über geschützte Ressourcen und weitere Systeminformationen zu speichern. Dieses Repository enthält auch GetAccess-spezifische Daten über User, wie gültige Zeitlimits, fehlerhaftes und erfolgreiches Log-in usw.

Multi-Domain Service (MDS)

GetAccess verwendet ein Modell der gespeicherten und abrufbaren Credentials während einer Session, um damit den Transfer von Credentials über mehrere Internet Domains zu erleichtern. Wenn sich ein User einmal in einer *Primary* Domain authentifiziert hat, kann er auf geschützte Ressourcen in allen *Primary* und *Secondary* Domains zugreifen, ohne sich nochmals authentifizieren zu müssen. Der Status eines Users während seiner Session wird laufend verfolgt, unabhängig davon, in welcher Domain er sich bewegt. So führt eine ausgedehnte Zeitdauer, die der User für Anwendungen in Domain B spendiert, nicht dazu, dass er ein gesetztes Zeitlimit in Domain A überschreitet. Auch das Zurückziehen eines Users durch den Administrator wird über alle Domains wirksam. Wenn der User schließlich das Log-out getätigt hat, wird die Session vom zentralen SMS beendet, was bedeutet, dass alle Zugriffe auf Anwendungen sämtlicher Domains verweigert werden.

Single-Sign-on-Prozess

Wenn ein Nutzer sich in das GetAccess-System einloggt, werden seine Authentifikationsinformationen eingeholt und verifiziert und dem Nutzer wird Zugang gewährt. Eine neu gestartete Session erzeugt verschlüsselte Cookies, die während der Session als Credentials dienen.

Der Single-Sign-on-Prozess läuft im Einzelnen ab, wie in Bild 6.19 dargestellt:

Schritt 1: Der Nutzer fordert ein Log-in an. Der *GetAccess Access Service* stellt die entsprechende Log-in-Seite zusammen, indem er sich Firmenlogo und weitere Informationen aus einem entsprechenden HTML Template holt. Der Nutzer gibt dort seine User ID/Passwort-Kombination ein.

Schritt 2: Der *Access Service* transferiert die Information zur Validierung zum AARS.

Schritt 3: Der AARS stellt fest, dass diese Authentifikationsanfrage beim Corporate Directory (z. B. gespeichert im Active Directory) zu überprüfen ist und sendet sie zum PAAM.

Schritt 4: Der *Identification and Authorization Service* übernimmt die Anfrage und überprüft die Angaben mit dem Active Directory. Das Directory liefert die Rechte des Nutzers einschließlich der organisatorischen Zugehörigkeiten und anderer Attribute. Der *Identification and Authorization Service* meldet die erfolgreiche Authentifikation an den AARS und leitet die Nutzer-Rechte entsprechend der Angaben im Active Directory weiter.

Schritt 5: Der AARS holt sich das Profil des Nutzers aus dem GetAccess Repository. Das Profil gibt Auskunft darüber, ob er weitere Berechtigungen besitzt und welche Zeitlimits für den Nutzer Gültigkeit haben.

Schritt 6: Der AARS fordert beim SMS den Start einer neuen Session an. Der SMS erzeugt eine Session auf Basis des vom AARS gelieferten Timeout-Wertes. Außerdem generiert er einen temporären Schlüssel für diese Session, den er an den AARS zurückliefert.

Schritt 7: Der AARS verwendet den temporären Schlüssel zur Verschlüsselung der Credentials für diese Session. Er schickt diese Credentials zum *Access Service* zurück.

Schritt 8: Der Access Service packt die verschlüsselten Credentials in Session Cookies und sendet sie zum Browser des Nutzers. Diese Art von Cookies wird niemals auf Platte gespeichert und wieder gelöscht, wenn der Nutzer den Browser schließt oder mit Log-out das System verlässt.

Schritt 9: Dem Nutzer wird durch den RPS das *Dynamic Resource Menu* angezeigt, das alle Anwendungen auflistet, zu denen der Nutzer nun Zugang hat.

Schritt 10: An dieser Stelle ist der Log-in-Prozess abgeschlossen. Der Nutzer ist erfolgreich authentifiziert und autorisiert. Die Credentials, die seine Rechte widerspiegeln, sind in seinem Browser abgelegt und er hat eine personalisierte Sicht auf die für ihn zugänglichen Ressourcen. Auf die entsprechenden Anwendungen und Services kann er nun über Portal und Application Server nahtlos zugreifen.

Kommentar zu GetAccess

Entrust GetAccess ist als Plattform für SSO-Lösungen in Unternehmen geeignet.

Als integrale Komponente der *Entrust Secure Portal Solution* bietet GetAccess die Funktionalitäten Authentifikation, Autorisierung und SSO für Portale mit sensitiven Informationen und geschäftskritischen Transaktionen.

GetAccess beeindruckt durch hohe Flexibilität bei der Integration von SSO-Services in existierende Security-Infrastrukuren und durch vielfältige Authentifikations- und Autorisierungsfunktionen. Die GetAccess-SSO-Lösung ist besonders geeignet, wenn mittlere und starke Authentifikation gefragt sind. Die Performance könnte bei Implementierungen mit einer großen Anzahl von gleichzeitigen Nutzern ein Thema sein, da die Abstraktionsebenen für Authentifikation, Autorisierung und Management-Prozesse zu einem gewissen Overhead führen.

6.4.6 Andere SSO-Services

GetAccess ist ein SSO-Service für Unternehmen, angeboten von einer Firma, die sich ausschließlich auf Security-Themen spezialisiert hat. Dieser Service ist plattformneutral und kann deshalb in die meisten modernen Anwendungsplattformen integriert werden. Allerdings gibt es weitere plattformneutrale SSO-Services auf dem Markt. Besonders erwähnenswert sind *RSA ClearTrust* [6.4.12] und *Netegrity Siteminder* [6.4.13]. In Bezug auf Funktionalität, Flexibilität, Preise und Reputation im Markt sind die genannten Systeme annähernd vergleichbar.

Eine andere Kategorie sind die plattformabhängigen SSO-Services, die für eine spezifische Anwendungsplattform konzipiert und ausschließlich auf diese Umgebung optimiert wurden. Als geeignete Beispiele hierzu werden im Folgenden kurz die SSO-Services des *SAP Enterprise Portal* und der Produktfamilie *IBM WebSphere* erläutert.

SAP Enterprise Portal SSO

Das *SAP Enterprise Portal* bietet Authentifikation/SSO-Services für SAP-Anwendungen, die auf User ID und Passwort oder Zertifikaten basieren. Der Portal Server leitet die Log-on-Informationen an einen externen Authentifikationsmechanismus weiter. Der externe Mechanismus prüft die Daten und schickt die authentifizierte User ID zum Portal Server, welcher der externen User ID einen Portal *User ID* zuweist und ein Log-on-Ticket generiert. Mit diesem Ticket wird dem Nutzer Single-Sign-on-Zugang zu allen Anwendungen gewährt, die vom Portal aus erreichbar sind. Nicht-SAP-Anwendungen können das Ticket, das vom Portal Server digital signiert ist, ebenso nutzen. Sie sind in der Lage, das Ticket durch Verwendung einer speziellen Bibliothek, die Teil der Portal-Infrastruktur ist, zu verifizieren. *Entrust GetAccess* oder *RSA ClearTrust* oder auch andere Authentifikationen können in die SAP-Portal-Server-Infrastruktur integriert werden und als externer Authentifikationsmechanismus verwendet werden.

Der SAP Portal Server bietet eine Rollen-basierte Zugangskontrolle, wobei die Rolleninformationen im Content Directory enthalten sind. Dieses Verzeichnis agiert als genereller Speicher für Objekte aller Art, wie Rollendefinitionen, Administrationsobjekte und Datenobjekte für die Visualisierung von Webseiten. Das Portal Management System weist den Usern die Rollen zu, den Rollen die Worksets und den Worksets die iViews zu.

IBM WebSphere SSO

Der *WebSphere Portal Server* bietet Authentifikation und SSO-Services basierend auf User ID und Passwort oder Zertifikaten. Der Portal Server leitet die Log-on-Informationen an die Authentifikationskomponente wie den *WebSphere Application Security Server* oder den *Web SEAL-Lite* (eine Komponente des IBM Policy Director) oder den *Netegrity SiteMinder* oder an andere *Authentication Proxy Server* weiter. Der Authentication Proxy Server kann in den WebSphere Application Server mittels der *Trust Association Interceptor APIs* integriert werden. Diese APIs stellen ein sicheres und einheitliches Interface für den WebSphere Portal Server dar. Der WebSphere Security Server und der Authentication Proxy Server sind so konfiguriert, dass sie für die Authentifikation den LDAP Directory des Portals verwenden. Der WebSphere Portal Server speichert verschiedene Informationen eines Users: User ID, Passwörter sowie Credentials einschließlich der Tokens und CORBA Credentials. Diese Credentials sind für Portlets über das Standard JAAS API verfügbar, so dass sie auch an Back-End-Anwendungen weitergeleitet werden können und dadurch Single Sign-on erreicht wird.

Der WebSphere Portal Server basiert auf Rollen-basierter Zugangskontrolle. Administratoren können Access Control Lists definieren, die den Zugang für einzelne Portlets regeln. Die Implementierung des Zugangskontrollsystems im Portal Server kann komplett durch ein anderes System wie den IBM Policy Director oder Netegrity Siteminder ersetzt werden.

6.4.7 Zusammenfassung und Empfehlungen

Während einige Authentifikationsmethoden und -technologien wie Passwörter, Token, Kerberos und .NET Passport weitverbreitet sind, müssen sich andere wie digitale Zertifikate/PKI, SAML und Liberty noch im Markt durchsetzen. Den richtigen Zeitpunkt zu erkennen und rechtzeitig bei einer neuen Technologie „aufzuspringen“, ist eine schwierige, aber essenzielle Entscheidung für erfolgreiche Unternehmen. Wenn Investitionen zu früh getätigt werden und mit noch nicht ausgereiften Technologien experimentiert wird, bleibt den Firmen häufig eine schmerzliche und teure Lektion nicht erspart. Erfolgt der Einstieg zu spät, ist das Risiko hoch, dass Mitbewerber die neuen Technologien bereits zu ihrem Vorteil genutzt haben.

Die folgenden Empfehlungen lassen sich unterscheiden in:

– generelle Aussagen, die sich auf allgemeine Anforderungen in der Geschäftswelt und auf Technologietrends beziehen
– Überlegungen zur Evaluierung von SSO-Services mit einer groben Bewertung, welche Plattform am besten für welches Business-Szenario geeignet ist.

Generelle Aussagen

Unternehmen sollten sich zuerst mit den Anforderungen und Security-Klassifikationen (öffentlich, privat, sensitiv, streng vertraulich) auseinandersetzen und sich die globale und lokale Nutzung von Unternehmensressourcen und -anwendungen sowie die damit verbundenen Risiken klar machen. Erst dann lässt sich fundiert festlegen, welche Stärke der Authentifikation gerechtfertigt ist.

Empfehlungen sind:

- Für Routine-Anwendungen wird User ID/Passwort für die nächsten Jahre voraussichtlich die adäquate Identifikations-/Authentifikationsmethode bleiben.
- Große, komplexe Unternehmen werden mehrere Technologien für unterschiedlich geforderte Authentifikationsstärken und vielfältige Anwendungsarten und Security Domains einsetzen müssen. Geeignete Authentifikationssysteme sollten deshalb gängige Methoden unterstützen wie User ID/verschlüsselte Passwörter, X.509 Zertifikate und Kerberos.
- Für eine mittlere Authentifikationsstärke sollte auf eine strikte Passwort-Policy geachtet werden und die Einführung einer PKI mit Software-basierten Zugangs-Token ins Auge gefasst werden. Langfristig sind solche Lösungen am flexibelsten.
- Für geschäftskritische Anwendungen mit hoher Authentifikationsstärke sollten Smartcards plus PINs oder andere durch Hardware oder Biometrie unterstützte PKI/Zertifikats-basierte Authentifikationsmethoden eingesetzt werden. Die Grenze zwischen mittlerer und hoher Authentifikationsstärke hängt von den Kosten- und Risikofaktoren einer Anwendung in ihrer spezifischen Prozessumgebung ab.
- Unternehmen sollten frühzeitig mobile Anwendungen und alle Kategorien mobiler Geräte (Laptops, PDAs, Smartphones, WAP-Phones) in ihr Authentifikationskonzept miteinbeziehen. Die hier möglichen Varianten sind vielfältig und reichen von SMS-basierter 2-Faktor-Authentifikation bis zu PKI/Zertifikats-basierter Authentifikation.
- Als Voraussetzung für einen effizienten SSO-Service sollten Unternehmen ein zentralisiertes, Policy-basiertes Management aller IT-Ressourcen und -Nutzer organisieren.

Bewertung von SSO-Services

Organisationen können Microsoft .Net Passport für B2C-Anwendungen einsetzen, wenn starke Authentifikationsmethoden nicht zwingend gefordert sind und eine Integration dieser Anwendungen in die existierende Security-Infrastruktur des Unternehmens keine Rolle spielt.

Liberty-Alliance-konforme SSO-Plattformen sind für B2C-, B2E- und B2B-Geschäftsmodelle gleichermaßen geeignet. Allerdings ist die Standardisierung nicht abgeschlossen, und bis jeweils die neuesten Funktionen in Produkten realisiert sind, werden Monate vergehen. Für Unternehmen bedeutet dies eine längere Migrationsstrecke bis zu einer zukunftsorientierten SSO-Lösung, vor allem bis zu komplexen SSO-Systemen in föderierten Netzen.

Es ist anzunehmen, dass die SSO-Spezialisten wie Entrust, RSA Security und Netegrity diesen Liberty-Weg gehen werden. Deshalb und auch wegen ihrer Flexibilität und Integrationsfähigkeit sind diese SSO-Plattformen für mittlere und größere Unternehmen zu empfehlen. Insbesondere, wenn ein unternehmensweiter Identifikations- und Authentifikationsservice mit unterschiedlichen Anforderungen an die Stärke der Authentifikationen gefordert wird und gleichzeitig die Integration in die existierende Infrastruktur mit heterogenen Security-Komponenten und Applikationen erreicht werden soll. Welche der drei genannten SSO-Plattformen, GetAccess oder ClearTrust oder

SiteMinder schließlich vorzuziehen ist, hängt von den kundenspezifischen Anforderungen und Ausgangssituationen ab.

Plattform-integrierte SSO-Lösungen wie SAP Enterprise Portal SSO oder IBM WebSphere SSO sind immer dann die erste Wahl, wenn eine (relativ) homogene Software-Umgebung auf Basis einer dieser Plattformen vorhanden und in Zukunft zu erwarten ist. Allerdings haben integrierte SSO-Lösungen meist nicht die Flexibilität und die breite Funktionalität wie die vorher zitierten Spezialsysteme. Deshalb sind aus heutiger Sicht unabhängige SSO-Plattformen langfristig oft die bessere Lösung, auch wenn integrierte SSO-Lösungen durchaus noch andere, also nicht plattform-homogene Anwendungen, einbeziehen können.

Die Auswirkungen der Web-Services-Technologie können allerdings diese Einschätzungen und die heutige Wettbewerbslandschaft wesentlich verändern, sofern die anstehenden Security-Herausforderungen gelöst werden.

6.5 Web Services und Security

Die faszinierende Technologie der Web Services auch in geschäftskritischen Anwendungen und Prozessen zum Einsatz zu bringen, ist seit langem das Ziel von Software-Herstellern und Unternehmen. Web Services können ohne signifikantes Zusatzinvestment in Hardware und Software entwickelt werden. In einigen Projekten wird sich deshalb nach kurzer Zeit bereits ein positiver ROI einstellen. Der wesentliche Gewinn von Web Services wird sich aber erst zeigen, wenn es gelingt, die Integration von Nutzern, Anwendungen, Daten und Prozessen nicht nur innerhalb der Unternehmen, sondern vor allem unternehmensübergreifend signifikant zu verbessern. Voraussetzung hierfür ist allerdings, dass Web Services in vertrauenswürdiger Umgebung absolut sicher abgewickelt werden können.

Web Services Security: Herausforderungen und Ziele

In vieler Hinsicht sind die Security-Herausforderungen, die sich mit dem Einsatz von Web Services stellen, ähnlich wie sie schon bei der ersten Generation der Web-Technologie aufgetreten sind. Die Zielsetzung ist die gleiche: eine benutzerfreundliche und vertrauenswürdige Umgebung zu schaffen, die es Unternehmen erlaubt, unternehmensübergreifende Kommunikation, Transaktionen und Geschäftsprozesse sicher abzuwickeln.

Auch die zugrundeliegenden Fragestellungen sind ähnlich:

- Mit welchen Security-Maßnahmen kann die wachsende Anzahl von sensitiven Ressourcen gegen zunehmende Gefahren und Schwachstellen geschützt werden?
- Wie lassen sich Identitäten managen und wie kann verifiziert werden, wer oder welcher Service sich am anderen Ende der Netzverbindung befindet?

– Wie kann ein fein-granulierter Zugang zu sensitiven Ressourcen erreicht werden?
– Wie können Vertraulichkeit und Integrität bei Transaktionen und Kommunikationen sichergestellt werden?

Ein zukünftiges Security-Konzept macht es notwendig, existierende Anwendungen, Prozesse und Security-Technologien schrittweise in eine Anwendungswelt zu transformieren, die zunehmend auf Web Services basiert. Gefordert ist ein einheitliches Security-Konzept und Framework, das den besonderen Eigenschaften dieser Anwendungsarchitektur Rechnung trägt und technologische wie geschäftsrelevante Aspekte (Policy, Trust, Risiken) berücksichtigt. Ein solches übergreifendes Security-Konzept kann nur durch eine koordinierte Anstrengung von Plattformherstellern, Herstellern von Anwendungs-Software, Security-Spezialisten, Netz- und Infrastruktur-Betreibern, Standardisierungsgremien und Industrievertretern erreicht werden.

Das übergeordnete Ziel muss sein, Unternehmen in die Lage zu versetzen, trotz heterogener Systemlandschaften interoperable Lösungen zu entwickeln. Integration durch Abstraktion von Security-Funktionen ist eine geeignete Methode. Beispielsweise unterstützt das Secure-Messaging-Modell sowohl eine Public-Key-Infrastruktur (PKI) als auch den Kerberos-Authentifikationsmechanismus als weitverbreitetes Verfahren und ist fähig auch andere Security-Mechanismen zu unterstützen.

Jeder Prozess, jeder Web Service hat seine spezifischen Security-Anforderungen entsprechend seiner geschäftlichen Verwendung und seines operationalen Umfeldes. Ein erfolgreicher Ansatz für Web Services Security erfordert das flexible Zusammenspiel interoperabler Security-Technologien, die durch Konfigurationen und Policies ein weites Feld von unterschiedlichen Szenarien abdecken sollen.

Ausführliche Informationen zum Thema Web Services Security sind auch im Buch mit dem gleichnamigen Titel zu finden [6.5.1].

6.5.1 Web Services Security, Standards und Spezifikationen

Terminologie

Zum besseren Verständnis des Web-Services-Security-Modells und der dazu zitierten Spezifikationen werden im Folgenden einige Begriffe erläutert.

Security Token

ist die Repräsentation einer Security-Information für die sichere Abwicklung von Web Services Messages und enthält eine Reihe dazugehöriger Claims, z. B. X.509 Zertifikate, Kerberos Tickets, User IDs/Passwörter oder Security Token von SIM Cards oder Smartcards.

Signed Security Token

ist ein Security Token, der vom Herausgeber kryptographisch signiert wurde.

Subject

eines Security Token kann eine Person, eine Anwendung oder ein beliebiges anderes Business-Objekt sein, auf die oder das die Claims, die im Security Token enthalten sind, anzuwenden sind. Als Besitzer (Owner) des Security Token besitzt das Subject die erforderliche Information, um die Besitzverhältnisse nachweisen zu können.

Claim

ist eine Aussage über ein *Subject*, die entweder vom Subject selbst gegeben oder von einem Bezugspartner erzeugt wird. Claims können Aussagen sein über Schlüssel, die zum Signieren oder Verschlüsseln von Nachrichten verwendet werden oder den Security Token bei einer Nachricht begleiten. Claims beanspruchen ein Nutzungsrecht und enthalten die Identität oder eine autorisierte Rolle des Senders.

Web Service Endpoint Policy

Bei der Festlegung von Claims, die erforderlich sind, um Web Services nutzen zu können, gibt es vollständige Flexibilität hinsichtlich der inhaltlichen Definitionen. Claims (Ansprüche auf Nutzungsrechte) und dazugehörige Informationen beziehen sich auf die Web Service Endpoint Policy (Gewährung von Nutzungsrechten), d.h. auf die angewandten Richtlinien an den Endpunkten der zu kommunizierenden Nachricht. Entsprechen Claims nicht den Anforderungen der Policies, kann eine Nutzung nicht zustande kommen. Endpoint Policies können in XML ausgedrückt sein und für Authentifikation, Autorisierung oder für andere Anforderungen angewendet werden.

Claim Requirements

sind Anforderungen, die mit der ganzen Nachricht verknüpft sein können oder mit einzelnen Elementen der Nachricht oder mit sämtlichen Aktionen eines bestimmten Typs oder mit Aktionen unter bestimmten Randbedingungen. Ein Service könnte z. B. vom Anfragenden (Requester) verlangen, dass er die Einkaufsberechtigung für Beträge nachweist, die größer als das angegebene Limit sind.

Intermediaries

Wenn SOAP Messages von einem Anfragenden (Requester) zum Service-Provider geschickt werden, können sie unterwegs Vermittlungsstationen (Intermediaries) passieren, die Aktionen wie Routing oder sogar Modifikationen der Nachricht durchführen. Beispielsweise könnte ein Intermediary die Nachricht mit Headern ergänzen oder einen Teil der Nachricht verschlüsseln oder zusätzliche Security Token anhängen. In diesen Fällen ist sicherzustellen, dass derartige Veränderungen die Integrität der Nachricht nicht beschädigen sowie das Trust-Modell und die Verantwortlichkeiten nicht verletzen.

Actor

kann ein Intermediary oder ein Endpoint sein, der durch einen URI identifiziert ist und eine Nachricht abwickelt. Weder User noch Client Software werden als Actors bezeichnet.

Das Web-Services-Security-Modell

Web Services können vom Requester durch Senden einer SOAP Message zum Service-Endpunkt, der durch einen URI gekennzeichnet ist, in Anspruch genommen werden. Die angeforderten Ergebnisse werden dann mit einer weiteren SOAP Message zurückgeliefert. In diesem Kontext unterteilt sich das Ziel, Web Services sicher zu gestalten, in zwei Teilziele: zum einen die Gewährleistung der Integrität und Vertraulichkeit der Nachricht, zum anderen die Sicherstellung, dass der Service nur ausgeführt wird, wenn die der Policy entsprechenden Nutzungsanforderungen erfüllt werden (Authentifikation und Autorisierung).

Das *SSL/TLS*-Protokoll wird zur Absicherung der Transportebene verwendet. SSL/TLS bietet Security-Funktionen für Authentifikation, Datenintegrität und Vertraulichkeit und ermöglicht sichere Punkt-zu-Punkt-Verbindungen.

IPsec stellt einen weiteren Standard auf Netzebene 3 dar, der auch für Web Services von Bedeutung ist. Wie SSL/TLS bietet auch IPsec sichere Netzverbindungen mit Authentifikation, Datenintegrität und Vertraulichkeit.

Anwendungstopologien schließen heute Kombinationen von mobilen Geräten, Gateways, Proxies, Load Balancer, DMZs (Demilitarized Zones), Outsourcing-Datenzentralen und global verteilten, dynamisch konfigurierbaren Systemen ein. Alle diese Systeme sollten die Fähigkeit besitzen, Nachrichten als Vermittlungsstation sicher zu befördern. Das *SOAP-Message*-Modell funktioniert auf Basis logischer Endpunkte und abstrahiert dabei das physische Netz und die Anwendungsinfrastruktur, so dass häufig auch mehrere Vermittlungsstationen als Intermediate Actors involviert sind.

Wenn Daten von einer Vermittlungsstation empfangen und weitergeleitet werden, können oberhalb der Transportschicht sowohl die Integrität der Nachricht verloren gehen als auch beliebige Security-Informationen, die mit versendet wurden. Dies bedeutet, dass sich jeder Vermittler in der Reihenfolge auf die Security-Evaluierungen der jeweils vorhergehenden Station verlassen muss und den dort erfolgten Manipulationen am Inhalt der Nachricht vollständig vertrauen muss. Was in einer umfassenden Web-Services-Security-Architektur benötigt wird, ist ein Mechanismus, der End-to-End-Security gewährleistet. Erfolgversprechende Web Services Security Solutions müssen deshalb sowohl auf der Transport- als auch auf der Anwendungsebene entsprechende Security-Mechanismen vorsehen.

Das folgende Web-Services-Security-Modell und Bild 6.20 zeigen, wie die geforderten Ziele erreicht werden können:

– Ein Web Service kann verlangen, dass eine einlaufende Nachricht die angeforderten Bedingungen und Nachweise (Claims) erbringt (z. B. Name, Key, Zulassung, Fähigkeit usw.). Falls die Nachricht diese Claims nicht vorweisen kann, wird sie ignoriert

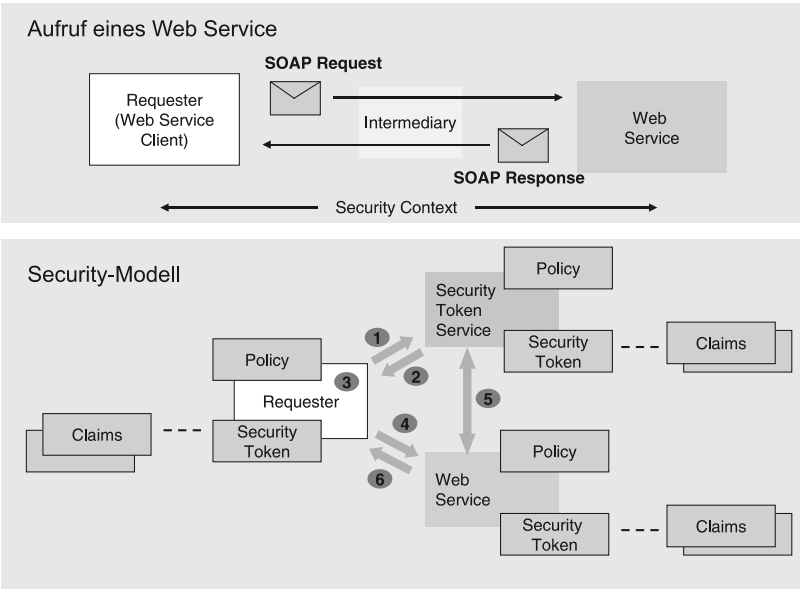


Bild 6.20 Web-Services-Security-Modell

oder zurückgewiesen. Die geforderten Claims und die dazugehörigen Informationen stehen in Bezug zur Policy.

– Beim Anfragenden (Requester) kann es sich ebenfalls um einen Web Service handeln, der Nachrichten mit den erforderlichen Claims mittels beigefügtem Security Token versendet. Eine Nachricht muss sowohl die spezifische Aktion beschreiben als auch den Nachweis enthalten, dass der Sender die Berechtigung besitzt (Claim) diese Aktion anzufordern.
– Wenn ein Anfragender die geforderten Claims nicht hat (weil der Service-Provider ihn nicht kennt und ihm deshalb nicht vertraut), kann er oder in seinem Auftrag ein Dritter versuchen, die erforderlichen Claims durch Kontaktieren anderer Web Services zu erhalten. Diese anderen Web Services (Trust Broker), hier als Security Token Services bezeichnet, können wiederum einen eigenen Satz von Claims anfordern. Security Token Services vermitteln Vertrauen (Trust) zwischen verschiedenen Domains durch die Herausgabe von Security Token.
– Das Modell schließt ein, dass der Requester ebenfalls durch einen Web Service repräsentiert ist und dass auch der Security Token Service ein Web Service mit definierter Policy ist und für die Inanspruchnahme seiner Services einen Security Token verlangt.

Ein Nachrichtenfluss läuft in der Regel folgendermaßen ab:

Schritt 1: Der Requester (Web Service Client) sendet eine Anfrage für einen Security Token an den Security Token Service.

Schritt 2: Der Security Token Service sendet den angeforderten Token zurück.

Schritt 3: Der Web Service Client fügt den Token der SOAP Message an.

Schritt 4: Der Web Service Client signiert die Nachricht und sendet sie zum Web Service.

Schritt 5: Beim Web Service wird die Gültigkeit des Client Token durch Kontaktieren des Security Token Service überprüft.

Schritt 6: Der Web Service führt den Service aus und sendet das Ergebnis an den Web Service Client.

Der Security Token Service kennt drei Typen von Token, die durch ihn generiert und validiert werden: den Typ *User ID/Password,* den Typ *X.509 Zertifikat* und den Typ *Kerberos*. Beispielsweise könnte ein *Kerberos Ticket Granting Service*, der in diesem Modell als Security Token Service zu verstehen ist, durch das Kerberos-Protokoll von der Security-Schicht des Client-Betriebssystems aufgerufen werden. Hat der Web Service Client den Token erhalten, kann er ihn in eine SOAP Message einfügen und die Message signieren.

Der Web Service ist in der Lage, die Signatur je nach Typ des Tokens auf verschiedenen Wegen zu verifizieren. Wenn der Client den Typ *User ID/Password Token* für die Authentifikation verwendet, sendet er den Hash-Wert des Passworts in der Nachricht mit und signiert die Nachricht unter Nutzung dieses Passworts (Hash-Wert ist vereinfacht ausgedrückt das Ergebnis einer durch einen Algorithmus reduzierten Zeichenfolge). Der Server kann dann verifizieren, ob der Client tatsächlich die Nachricht gesendet hat, wenn die Signatur, die er für die Nachricht erzeugt hat, mit der Signatur übereinstimmt, die in der Nachricht enthalten ist. Bei Verwendung von *X.509 Zertifikaten* kann die Nachricht mit dem Private Key des Client signiert werden. Die Nachricht enthält das Zertifikat im Security Token. Der Web Service kann dann mit dem korrespondierenden Public Key des Client die Signatur verifizieren. Schließlich, wenn ein Kerberos Ticket verwendet wird, kann die Nachricht mit einem Session Key signiert oder verschlüsselt werden, der im Kerberos Ticket enthalten ist. Da das Kerberos Ticket mit dem Schlüssel des Empfängers verschlüsselt wird, ist nur der Empfänger in der Lage, das Ticket zu entschlüsseln, daraus den Session Key zu entnehmen und die Signatur zu verifizieren.

Dieses allgemeine Nachrichten-basierte Security-Modell subsumiert und unterstützt verschiedene mehr spezifische Modelle wie Identity-basierte Security, Access Control Lists und Security, die auf definierten Eigenschaften und Fähigkeiten (z. B. geschäftsrelevante Zertifikate) basiert. Es ermöglicht die Verwendung von existierenden Technologien wie vorher erläutert (Passwort, Kerberos, X.509 Zertifikate). Es erlaubt außerdem die Abstrahierung von Security-Mechanismen und bietet damit die Möglichkeit, unterschiedliche Techniken zu überbrücken. Dieses generische Modell ist die Grundlage für den Austausch von Schlüsseln, für Authentifikation und Autorisierung, für das Auditing sowie für Trust-Mechanismen.

XML Security Standards

Die Standardisierung von Web Services wird von Software-Herstellern (vor allem von IBM und Microsoft) und Standardisierungsgremien wie *W3C, WS-I, OASIS, UDDI.org* [6.5.2] vorangetrieben.

Genauso wie XML die Basis für Web Services darstellt, ist *XML Security* als Grundlage für die Web Services Security Standards zu sehen. Im Wesentlichen wurden die XML Security Standards von W3C und Industriekonsortien entwickelt.

Die wichtigsten Standards werden kurz erläutert:

XML Signature

ist die Definition eines XML-Schemas für die kryptographische Authentifikation von Daten. Die authentifizierten Daten können aus einem vollständigen Dokument, einzelnen Elementen eines XML-Dokuments oder einem externen Datenobjekt bestehen, auf das durch ein XML-Dokument verwiesen wird.

XML Encryption

ist die Definition eines XML-Schemas für die Verschlüsselung von Daten. Die verschlüsselten Daten können aus einem vollständigen Dokument, einzelnen Elementen eines XML-Dokuments oder einem externen Datenobjekt bestehen, auf das durch ein XML-Dokument verwiesen wird.

XML Key Management Specification (XKMS)

ist die Definition vertrauenswürdiger Web Services für das Management kryptographischer Schlüssel einschließlich öffentlicher Schlüssel. Die Spezifikation umfasst Services für die Partei, die den Verweis auf den kryptographischen Schlüssel benötigt (Location und Validierung) sowie Services, die durch den Inhaber eines kryptographischen Schlüssels genutzt werden (Registrierung, Sperrung, Neuausgabe, Key Recovery). Ein wesentliches Ziel von XKMS ist, die Anwendung von der komplexen darunterliegenden PKI abzuschirmen. Dies wird durch Delegation der Details der Verarbeitung von digitalen Zertifikaten an separate Web Services erreicht.

Security Assertion Markup Language (SAML)

ist das Framework für die Definition und den Austausch von *Trust Assertions* in XML. Trust Assertions sind vertrauenswürdige Behauptungen über Eigenschaften eines Subjektes, das Nutzungsrechte wahrnehmen will. Als Trust Assertions können beliebige Daten dienen, die zur Feststellung einer Berechtigung herangezogen werden, z. B. Beglaubigungen, Bonitätseinstufungen, genehmigte Rollen usw. SAML ist wichtig für die Interoperabilität und daher auf die Unterstützung interoperabler Authentifikations- und Autorisierungsdienste ausgelegt.

XML Access Control Language (XACML)

ist die Sprache zur Definition, wie Richtlinien als Zugriffsrechte beschrieben und umgesetzt werden. Durch Regeln kann der Policy-Autor flexibel und selektiv definieren, welche Web Services welche Zugriffsrechte auf welche XML-Dokumente ausüben dürfen.

Security Framework und Spezifikationen

Da Web Services Teile eines unternehmensübergreifenden Prozesses sein können, sind eine Reihe von *Web Services Security Specifications* [6.5.3] auf der Grundlage von Message-basierter Collaboration ausgearbeitet worden. Diese Spezifikationen umfassen die Themenfelder Vertraulichkeit (Privacy), Policy, Vertrauen zwischen Partnern (Trust) und Föderation (Federation). Die Arbeiten wurden von Microsoft und IBM vorangetrieben und von den Security-Spezialisten Verisign und RSA Security unterstützt. Bis dato sind erst die Basis-Spezifikationen (WS-Security) von OASIS als Standard abgesegnet worden. Die darauf aufsetzenden Vorschläge können noch nicht als Standard eingestuft werden.

In Bild 6.21 ist dieses Web Services Security Framework illustriert.

Das Message-Security-Modell, genannt WS-Security, stellt die Basis für die anderen Spezifikationen dar. In einer Ebene darüber sind die Modelle für Policy (WS-Policy), Trust (WS-Trust) und Vertraulichkeit (WS-Privacy) definiert. Diese Spezifikationen stellen die Grundlage dar, auf der sichere und interoperable Web Services über verschiedene Trust Domains hinweg funktionieren können.

In der obersten Ebene wird das Framework durch Modelle für sichere Konversation (WS-Secure Conversation), föderiertes Vertrauen (WS-Federation) und Autorisierung

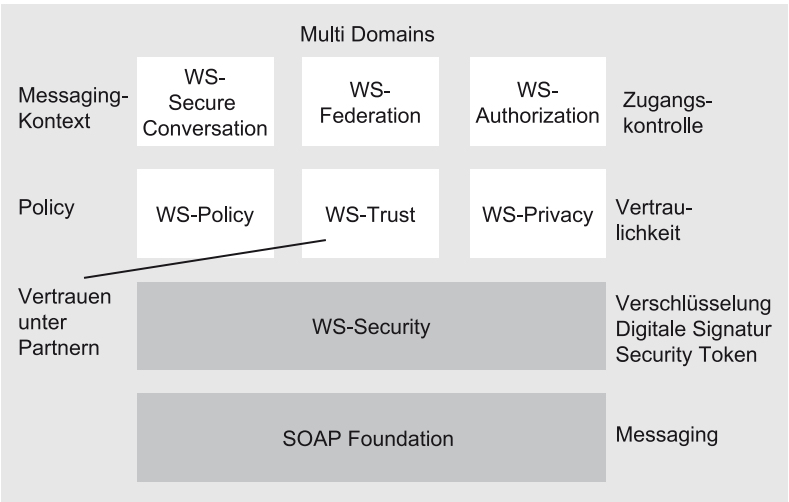


Bild 6.21 Web Services Security Framework

(WS-Authorization) ergänzt, womit eine Vielfalt von Anwendungsszenarien erschlossen wird. Die Kombination der in diesen Spezifikationen definierten Funktionalitäten soll letztendlich eine Interoperabilität von sicheren Web Services über heterogene Systemwelten hinweg ermöglichen.

Die folgenden Beschreibungen geben einen kurzen Überblick über Intention und Funktion der Security-Modelle.

WS-Security

WS-Security verkörpert einen allgemein nutzbaren Mechanismus zur Verbindung von Messages mit Security Token. Wie schon erläutert, wird kein spezifischer Token-Typ vorausgesetzt. Im Gegenteil, das Design ist auf Erweiterbarkeit (Unterstützung vielfältiger Token-Formate) ausgelegt. Beispielsweise könnte ein Requester seine Identität durch den Besitz einer für das Geschäft relevanten Zertifizierung nachweisen.

WS-Security beschreibt Erweiterungen zum SOAP Messaging, mit dem Ziel, eine Qualität der Sicherheit durch Integrität und Vertraulichkeit der Message sicherzustellen, und es definiert, in welcher Weise ein Security Token in eine SOAP Message eingefügt und verknüpft wird. Die Spezifikation enthält Mechanismen zur Spezifizierung binär verschlüsselter Security Token (z. B. X.509 Zertifikate). Diese Mechanismen können unabhängig oder in Kombination verwendet werden, womit ein breites Spektrum von Security- und Verschlüsselungs-Technologien zum Einsatz kommen kann.

Darüber hinaus beschreibt WS-Security einen Mechanismus zur Verschlüsselung binärer Security Token. Die Spezifikation beschreibt, in welcher Weise X.509 Zertifikate und Kerberos Tickets zu verschlüsseln sind und wie verschlüsselte Keys zu behandeln sind. Außerdem enthält WS-Security Erweiterungen, welche die Beschreibung zusätzlicher Charakteristika von Security Token erlaubt.

WS-Policy

WS-Policy beschreibt, wie Sender und Empfänger zur Nutzung von Web Services ihre Voraussetzungen/Anforderungen (Requirements) und Möglichkeiten/Fähigkeiten (Capabilities) definieren.

WS-Policy ist flexibel erweiterbar und schränkt die zu beschreibenden Typen von Anforderungen und Möglichkeiten nicht ein. Die Spezifikation enthält jedoch als Basis einige Service-Attribute wie Privacy-Attribute, Verschlüsselungsformate, Anforderungen an Security Token sowie unterstützte Algorithmen.

Diese Spezifikation definiert eine Art generisches SOAP-Policy-Format, das mehr als nur Security Policies unterstützen kann. Die Spezifikation beschreibt auch, in welcher Weise Service Policies an SOAP Messages angefügt werden können.

WS-Trust

Bei WS-Trust geht es um das Modell der direkten Vertrauensbeziehung zwischen Partnern sowie um die Vermittlung solcher Trust-Beziehungen durch Dritte.

Die Spezifikation beschreibt, wie die Vermittlung von Trust durch das Schaffen eines unabhängigen Security Service realisiert werden kann, der Security Token auf Anforderung erzeugt und herausgibt. Dieser Security Token Service setzt auf WS-Security auf und transferiert den angeforderten Security Token so, dass Integrität und Vertraulichkeit gewährleistet sind.

Außerdem beschreibt die Spezifikation, wie verschiedene existierende Trust-Mechanismen im spezifizierten Trust-Modell genutzt werden können.

Das Trust-Modell erlaubt explizit Delegation und Impersonation.

WS-Privacy

Unternehmen, die Web Services entwickeln oder anwenden, haben in der Regel Richtlinien bezüglich der Vertraulichkeit aufgestellt und verlangen von eingehenden Anfragen, dass der Sender entsprechende Nachweise (Claims) erbringt, um diesen Richtlinien (Policies) gerecht zu werden.

Mit einer Kombination aus WS-Policy, WS-Security und WS-Trust sind Unternehmen prinzipiell in der Lage, Konformität zu postulierten Privacy Policies darzulegen. WS-Privacy beschreibt ein Modell, wie eine Privacy-Sprache in die WS-Policy-Beschreibung eingebettet werden kann und wie unter Verwendung von WS-Security die Privacy Claims mit einer Message assoziiert werden können. Schließlich beschreibt die Spezifikation, wie Privacy Claims unter Nutzung der Mechanismen von WS-Trust für Nutzer und Unternehmen praktikabel anwendbar sind.

WS-Secure Conversation

Die Spezifikation WS-Secure Conversation beschreibt, wie einerseits der Web Service eingehende Messages und andererseits der Requester angeforderte Web Services authentifiziert und wie ein beidseitig authentifizierter Security-Kontext hergestellt wird.

Außerdem beschreibt die Spezifikation, wie Session Keys und abgeleitete Keys gebildet werden.

Sie beschreibt auch, wie ein Service den Security-Kontext sicher austauschen kann (Sammlung von Claims über Security-Attribute und dazugehörige Daten). Um dies zu erreichen, basiert die Spezifikation auf dem Konzept der Security-Token-Mechanismen (Herausgabe und Austausch), die in WS-Security und WS-Trust definiert sind. Bei Verwendung dieser Mechanismen könnte ein Service beispielsweise einen Security Token mit einer weichen symmetrischen Schlüsseltechnologie, aber auch einen Security Token mit starken asymmetrischen Schlüsseln verwenden.

WS-Secure Conversation ist für die SOAP-Message-Ebene konzipiert und stellt sicher, dass die Message unter Wahrung der End-to-End Security mehrere Vermittlungsstationen passieren kann. Dies schließt die Verwendung in anderen Messaging Frameworks aber nicht aus. Um die Security aller involvierten Systeme zu verbessern, kann die Transport Level Security in Kombination sowohl mit WS-Security als auch mit WS-Secure Conversation verwendet werden.

WS-Federation

Diese Spezifikation definiert, wie föderierte Trust-Szenarien unter Verwendung von WS-Security, WS-Policy, WS-Trust und WS-Secure Conversation gebildet werden. Beispielsweise wird beschrieben, wie Kerberos und PKI in föderierten Netzen verwendet werden.

Außerdem wird eine Trust Policy eingeführt, um die Art und Weise des zu vermittelnden Vertrauens zu bezeichnen und zu identifizieren.

Die Spezifikation definiert auch einen Mechanismus für das Managen von Vertrauensbeziehungen.

WS-Authorization

Diese Spezifikation beschreibt, wie Zugangs-Policies für einen Web Service spezifiziert und gehandhabt werden, insbesondere wie Claims in Security Token spezifiziert und wie diese Claims am Endpunkt interpretiert werden.

Auch hier wurde auf Flexibilität und Erweiterbarkeit sowohl in Bezug auf das Autorisierungsformat als auch auf die Autorisierungssprache Wert gelegt. Dies ermöglicht eine breite Einsetzbarkeit und lange Lebensfähigkeit des Security Frameworks.

Standardisierung – Ausblick

Die globalen Player auf dem Gebiet der Web Services haben ein echtes und starkes Interesse, bei der Entwicklung von Security-Standards eng zusammenzuarbeiten. Sie haben alle erkannt, dass eine breite Akzeptanz und Einsetzbarkeit nur mit adäquaten Mechanismen zu erreichen ist, die den Schutz privater Werte sowie Vertraulichkeit und Integrität bei Transaktionen gewährleisten.

Die Bemühungen, gemeinsame Standards zu erreichen, werden vermutlich schwieriger, wenn es um die komplexeren Sachverhalte wie föderierte Identitäten und Vertrauensverhältnisse und eine Vereinheitlichung mit den Spezifikationen der Liberty Alliance geht.

Die Liberty Alliance veröffentlichte Ende 2003 die Phase 2 der *Federated Identity Specifications*, in denen Identity-Funktionen für Web Services definiert sind und die die Grundlage für das *Liberty Identity Web Services Framework* darstellen.

Während Phase 1 die föderierten Identitäten für Single Sign-on betraf, wie in Kapitel 6.4 erläutert, geht es bei Phase 2 in einer höheren Ebene um gemeinsam nutzbare (Permissions-based) Attribute. Das Web Services Framework geht den Weg von Identity-basierten Web Services, um diese sicherer zu gestalten und den Schutz privater Werte zu gewährleisten.

Liberty Alliance hat des Weiteren eine *Services Expert Group* ins Leben gerufen, um interoperable Service-Spezifikationen zu entwickeln, die das Liberty Identity Web Services Framework nutzen und auf die spezifischen Bedürfnisse von Industriebranchen,

Anwendungen und Geschäftsmodellen eingehen sollen. Diese Spezifikationen heißen *Identity Service Interface Specifications (ID-SIS)*.

Leider stehen die Spezifikationen WS-Federation und WS-Trust nicht im Einklang mit den Liberty-Alliance-Spezifikationen, da weder Microsoft noch IBM, die beiden Promotoren der WS-Spezifikationen, Mitglieder der Liberty Alliance sind. Als Konsequenz wird die Industrie mindestens in den nächsten Jahren mit zwei unterschiedlichen Standardisierungsansätzen leben müssen.

Ein weiteres Problemfeld hat mit der Semantik von Lösungsansätzen zu tun. Die Standardisierung muss einerseits einen hohen Abstraktionsgrad verfolgen, um unterschiedliche Techniken unterstützen sowie Attribute und Policies flexibel definieren zu können. Andererseits bedeutet dies aber, dass der semantische Kontext in konkreten Umgebungen zwischen Partnern oft noch zu vereinbaren ist.

Beziehung zu existierenden Security-Techniken

Wie bereits erwähnt, ist das Web-Services-Security-Modell kompatibel mit existierenden Techniken für Authentifikation, Integrität und Vertraulichkeit, wie sie heute allgemein verwendet werden. Es ist deshalb möglich, Lösungen, die auf Web Services basieren, mit existierenden Security-Modellen zu integrieren. Im Folgenden dazu einige Beispiele:

Transport-Security

Existierende Technologien wie SSL/TLS gewährleisten für eine Nachricht Punkt-zu-Punkt-Integrität und Vertraulichkeit. Das Web-Services-Security-Modell unterstützt diesen Transport-Mechanismus in Verbindung mit WS-Security (und anderen WS-Spezifikationen) und stellt damit End-to-End-Integrität und Vertraulichkeit insbesondere über vielfältige Transportwege, Transportprotokolle und Vermittlungsstationen sicher.

PKI

Das PKI-Modell schließt Trust Center, die Schlüssel-Zertifikate generieren und herausgeben, und Authorities ein, die auch andere Eigenschaften und Attribute validieren. Besitzer dieser Zertifikate und Eigenschaften benutzen diese, um Claims und Identitäten auszudrücken. Das Web-Services-Security-Modell unterstützt Security Token Services, die Security Token in Public-Key-Technologie herausgeben. Eine PKI ist hierbei im weitesten Sinn zu verstehen und erfordert nicht irgendein hierarchisches Modell.

Kerberos

Das Kerberos-Modell basiert auf einem Key Distribution Center (KDC), das Trust zwischen den Parteien mittels Austausch verschlüsselter symmetrischer Schlüssel gewährleistet. Das Web-Services-Modell basiert mit dem Security Token Service auf einem vergleichbaren Ansatz. Trust wird wie bei Kerberos durch die Erzeugung von Security Token mit verschlüsselten symmetrischen Keys und verschlüsselten Dokumenten gewährleistet.

Allerdings bietet das Web-Services-Modell mehr Freiheitsgrade. Um Interoperabilität zu erreichen, müssen Adaptoren und/oder Algorithmen für Signaturen und Verschlüsselung untereinander vereinbart werden.

Existierende Modelle für Föderation, Autorisierung (einschließlich Delegation), Privacy und Trust sind weniger verbreitet. Dies sind Themen gerade entstehender oder zukünftiger Spezifikationen.

Trust-Modelle funktionieren heute in der Regel auf der Basis entsprechender vertraglicher Regelungen zwischen Geschäftspartnern. Eine offene Frage ist, ob derartige Regelungen für komplexere Web Services jemals automatisiert und standardisiert für beide Seiten (Provider und Requester) akzeptabel vereinbart werden können, wenn sich die Partner über UDDI ausfindig gemacht haben.

6.5.2 Web-Services-Security-Szenarien

Web Services werden sich sukzessive durchsetzen, zunächst innerhalb von Unternehmen und zunehmend auch unternehmensübergreifend, wenn Standards und verfügbare Technologien dies mit überschaubarem Risiko möglich machen.

Es ist zu erwarten, dass diese schrittweise Entwicklung folgendermaßen abläuft:

Phase 1: Unternehmensintern

Unternehmen werden beginnen, Web Services intern einzusetzen, hauptsächlich für EAI (Enterprise Application Integration), um damit ausgewählte Geschäftsprozesse transparenter und produktiver zu gestalten. Beispielsweise könnten Web-basierte Liefersysteme und Legacy-Systeme, welche die Rechnungsvorgänge für Kundenkonten bearbeiten, miteinander integriert werden, um die Rechnungsstellung unmittelbar an den Lieferzeitpunkt zu koppeln, womit sich Zinsverluste vermeiden und die Voraussage des Cash Flow verbessern ließen. Es ist vorteilhaft mit internen Anwendungen zu beginnen, da hierfür Standards und Technologien verfügbar, kompatibel und ausreichend sicher sind.

Phase 2: Unternehmensübergreifend mit ausgewählten Partnern

Sobald Web Services durch internen Einsatz ausreichend erprobt sind, werden Unternehmen versuchen, Partner mit einzubeziehen, mit denen bereits vertragliche Beziehungen bestehen. Anwendungen werden Schritt für Schritt auf eine Web-Service-Plattform transformiert, um z. B. das Supply Chain Management zu optimieren. So könnten dabei Web Services für die Weiterleitung und Ausführung von Aufträgen, zur Abfrage und Konsolidierung von Lieferkapazitäten und zur Aufbereitung des aggregierten und terminierten Produktionsbedarfs bei den in der Wertschöpfungskette beteiligten Zulieferern eingesetzt werden. In dieser zweiten Phase werden geeignete Transaktionsprotokolle und Security-Standards für den Erfolg von Web Services bereits eine entscheidende Rolle spielen.

Phase 3: Partner Communities

Je mehr sich der Einsatz von Web Services ausbreitet, desto mehr wächst das Potenzial für anspruchsvollere Interaktionen. Während dieser Phase werden Unternehmen wahrscheinlich versuchen, geschäftliche Vereinbarungen innerhalb einer Gruppe von Partnern, Zulieferern und Kunden auf eine automatisierte Basis zu stellen. Ein Unternehmen könnte z. B. eine Anfrage nach Lieferfähigkeit und Preisen an seine Zulieferer-Community versenden und die eingehenden Angebote dynamisch und automatisch nach vereinbarten Regeln und Abläufen verhandeln. Diese Phase ist bereits weitaus dynamischer als die vorangegangenen und setzt neue Geschäftspraktiken voraus, die sich erst noch entwickeln müssen. Mit einem solchen System lassen sich Interventionen durch Personen ganz vermeiden, es sei denn, es handelt sich um Ausnahmefälle.

Phase 4: Dynamische Collaboration

Diese in der Evolution der Web Services faszinierendste Phase geht über die Möglichkeiten der Phase 3 hinaus, indem neue Partner, mit denen bislang keine Geschäftsbeziehungen bestanden, dynamisch gesucht, identifiziert und automatisch in Prozesse involviert werden. Ist ein potenzieller Partner einmal identifiziert, ermöglichen Web Services die automatisierte Verhandlung der Partnerbeziehungen und der Bedingungen, unter denen Dienste oder Produkte in Anspruch genommen werden können, einschließlich der Verrechnungs- und Bezahlungsmodalitäten. Eine solche dynamische Collaboration setzt allerdings weitreichende Vereinbarungen, Verfahren und Standards über eine Automatisierung von Geschäftsbeziehungen voraus. Darüber hinaus müssen globale Directories die Möglichkeit bieten, dass anonyme, seriöse und legitimierte Interessenten an dieser Art der Collaboration einfach und zuverlässig teilhaben können.

Entsprechend der dargelegten Phasen sind in Bild 6.22 die unterschiedlichen Einsatzphasen von Web Services illustriert.

Das Diagramm zeigt einen Business-Prozess, unterstützt durch einen Workflow mit orchestrierten Web Services. Die in diesem Workflow gezeigten Web Services repräsentieren entweder autonome Business-Prozess-Objekte oder stellen Verbindungen zu existierenden Anwendungen und Ressourcen des Unternehmens bzw. zu Partnern und Kunden her. Die durch Web Services aufgerufenen internen und externen Anwendungen/Ressourcen werden entsprechend des Prozessablaufs eingebunden und liefern die angeforderten Ergebnisse.

Als Beispiel der vorher erläuterten Phase 1 sind solche Web Services zu nennen, die innerhalb eines Unternehmens auf einer einheitlichen Anwendungsplattform laufen (mit 1 gekennzeichnete Pfeile in Bild 6.22). Diese Web Services rufen andere Web Services auf oder verbinden mittels WSDL eine existierende Standard- oder Legacy-Anwendung oder greifen auf eine Datenbank zu.

Als Beispiel für Phase 2 und 3 können ausgewählte Partner (Pfeile 2) oder eine definierte Community (Pfeile 3) in den Workflow über Web Services integriert sein. Wenngleich ein Unternehmen geschäftliche Beziehungen mit all seinen Partnern vertraglich vereinbart haben mag, sind hier die Security-Auswirkungen hinsichtlich Authentifikation, Vertraulichkeit, Integrität und Verbindlichkeit erheblich, da Web Services über das

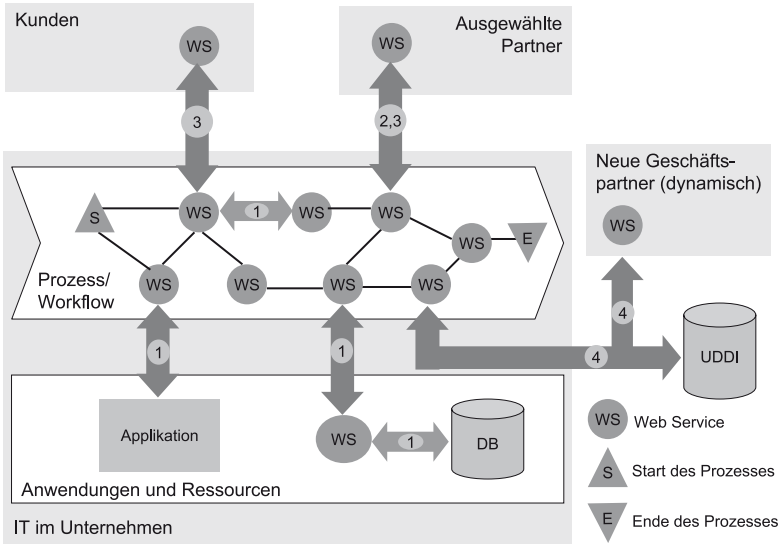


Bild 6.22 Einsatzphasen von Web Services

Internet kommunizieren und die Anbindungen auf Basis des http-Protokolls die Firewalls ohne Kontrolle passieren.

Wie in Phase 4 erwähnt, kann in Geschäftsprozessen ein dynamisches Suchen und Einbinden von Service-Anbietern, mit denen niemals vorher Geschäftsbeziehungen bestanden haben, erforderlich sein (Pfeil 4). In der Tat ermöglicht diese Lösungsarchitektur völlig neue Wertschöpfungsmodelle und -netze, gleichzeitig stellt sie jedoch aus Sicht der Security-Implikationen das anspruchsvollste Szenario dar. Vertrauen zwischen all diesen Partnern muss dynamisch und automatisch durch standardisierte Verfahren und Verhandlungen sichergestellt werden.

6.5.3 Einsatzbeispiel von Web Services

Das Einsatzbeispiel in diesem Kapitel soll demonstrieren, in welcher Weise Security-Technologien in Business-Prozessen, die auf Web Services basieren, zum Einsatz kommen. Bild 6.23 zeigt einen Prozess, in dem ein Darlehen für ein Immobilienobjekt beantragt wird. Dieser Prozess ist dem White Paper der Firma RSA Security mit dem Titel *Web Services Security* [6.5.4] entnommen, ist jedoch hier in anderer Form in Bild 6.23 dargestellt.

Der *Hypotheken-Service* besteht aus folgenden Teilprozessen, die als Web Services implementiert sind: Einholen eines digitalen Zertifikats (WS 1), Prüfen der Kreditfähigkeit des Antragstellers (WS 2), Gewähren des Zugangsrechts auf eine Grundbuch-Datenbank und Verifizierung der Details des Immobilienobjekts (WS 3) sowie Ausstellen und Signieren des Darlehensantrags (WS 4).

Schritt 1: Der Antragsteller wendet sich an eine Bank, füllt online ein Formular zur Beantragung einer Hypothek auf ein Immobilienobjekt aus und sendet es an die Bank

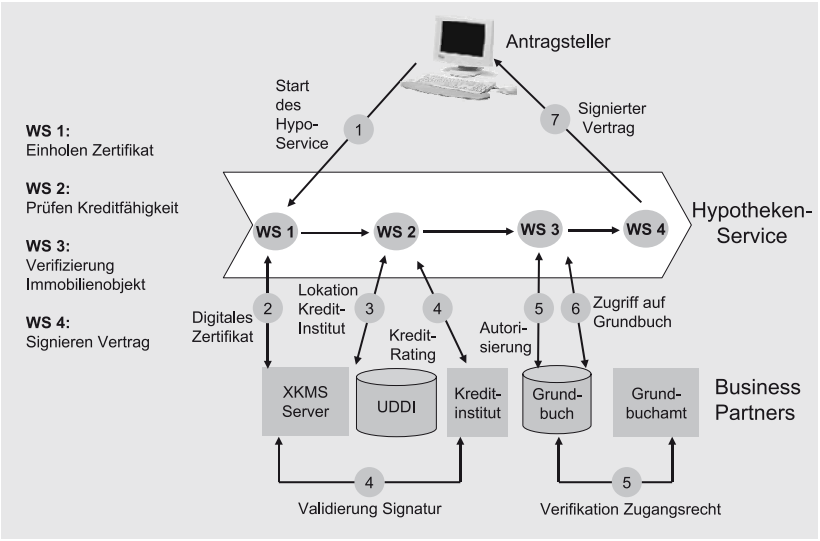


Bild 6.23 Einsatzbeispiel – Beantragung eines Immobiliendarlehens

zurück. Der Prozess zur Gewährung eines Hypothekendarlehens wird angestoßen, die Anwendung *Hypotheken-Service* wird gestartet.

Schritt 2: Bevor die Web Services der Anwendung *Hypotheken-Service* mit anderen Web Services kommunizieren können, müssen sie in der Lage sein, sich selbst zu diesen Services authentifizieren zu können. Dies kann durch Vorweisen eines digitalen Zertifikats geschehen, das von einem unabhängigen Trust Center ausgestellt wird. Auf Anforderung generiert das Trust Center, repräsentiert durch den *XKMS* Server, ein digitales Zertifikat für den *Hypotheken-Service* und stellt es verschlüsselt zur Verfügung.

Schritt 3: Der *Hypotheken-Service* sucht nun über ein *UDDI* Directory nach einem nationalen Institut, das Auskunft über die Kreditfähigkeit geben kann. Das UDDI gibt die Daten eines der Kreditprüfungsinstitute an den *Hypotheken-Service* zurück und zeigt an, dass Anfragen bei diesem Institut nur bearbeitet werden, wenn sie signiert sind.

Schritt 4: Nachdem der *Hypotheken-Service* die signierte Anfrage unterbreitet hat, kontaktiert das Kreditprüfungsinstitut den XKMS Server, um das Zertifikat des *Hypotheken-Service* validieren zu lassen. Der XKMS Server bestätigt die Gültigkeit. Das Kreditprüfungsinstitut antwortet mit der Bestätigung der Kreditfähigkeit des Antragstellers.

Schritt 5: Nach der Bestätigung der Kreditfähigkeit überprüft der *Hypotheken-Service* die Angaben über das Immobilienobjekt, indem er sich Einsicht in das Grundbuch verschafft. Bevor der Zugang gewährt wird, ist allerdings ein Nachweis erforderlich, dass die Zugangsberechtigung auf das gewünschte Objekt vertraglich geregelt ist. Dieser Nachweis wird durch eine *SAML*-Autorisierungsbestätigung erbracht.

Schritt 6: Der *Hypotheken-Service* sendet nun die konkrete Anfrage an die Grundbuch-DB mit einem WS-Security Header, der die SAML-Autorisierungsbestätigung aus Schritt 5 enthält. Als Antwort wird dem *Hypotheken-Service* mitgeteilt, dass alle Angaben über das Objekt richtig sind und keine Hypothekenbelastungen und hinderliche Dienstbarkeiten eingetragen sind.

Schritt 7: Nach den erfolgreich abgeschlossenen Überprüfungen generiert der *Hypotheken-Service* nun einen entsprechenden Darlehensvertrag, signiert ihn und sendet ihn an den Antragsteller zurück. Integrität und Vertraulichkeit dieses Dokuments werden durch *XML Signature* und *XML Encryption* sichergestellt.

6.5.4 Hersteller und Produkte

Die Implementierung von Web Services Security in gängigen Produkten ist voll im Gang, jedoch noch keineswegs abgeschlossen.

Basiskomponenten sind in den Plattformen der wesentlichen Hersteller integriert. Für komplexere Security-Szenarien wie Föderation besteht noch Diskussionsbedarf über Problemfelder bzw. noch nicht standardisierte Verfahren. Hier gibt es allenfalls herstellerspezifische Lösungsansätze.

Die folgenden Security-Komponenten sind im Großen und Ganzen heute in den Produkten der nachfolgend erwähnten Hersteller verfügbar:

- Secure Socket Layer (*SSL/TSL*) als sichere Basis auf der Transport-Ebene
- Web Services Description Language (*WSDL*) für Integrität
- *SAML* für Authentifikation und Autorisierung
- *XML-Encryption* für granulare Vertraulichkeit von Dokumenten
- *XML-Signature* für granulare Integrität und Verbindlichkeit
- *Web Services Security* für Authentifikation, Vertraulichkeit und Integrität
- *XKMS* für Key Management
- *XACML* für Zugangskontrolle

Hersteller kündigen über ihre Security Roadmaps für Web Services laufend weitere Details an. Wesentliche Funktionalitäten der wichtigsten Hersteller werden im Folgenden kurz angesprochen.

Microsoft .NET

Microsoft hat SSL und XML Security als Grundlage in das .NET Framework eingebaut.

Wie schon erwähnt, hat Microsoft eine Technologie mit dem Codenamen *TrustBridge* [6.5.5] angekündigt, die WS-Security und andere WS-Standards verwendet und einschließt, mit dem Ziel, Credentials über eine Vielzahl von Systemen wie Active Directory, .NET Passport und Plattformen von anderen Herstellern, die WS-Security unterstützen (z. B. IBM WebSphere), kompatibel verwenden zu können.

TrustBridge soll auf Basis von WS-Security die Föderation von unterschiedlichen Authentifikationssystemen ermöglichen. Im Gegensatz zum heutigen Stand soll es dann möglich sein, dass Unternehmen ihren Nutzern die Verwendung ihrer eigenen Credentials für das Sign-in in Websites, die an .NET Passport partizipieren, erlauben können.

Sowohl die Entwicklungstools von Microsoft als auch das .NET Framework unterstützen WS-Security. Eine weitergehende Unterstützung von neuen Standards für die Interoperabilität entsprechend der WS-Security Roadmap ist zu erwarten.

IBM WebSphere und Tivoli

Die aktuelle Version des *WebSphere Application Server* [6.5.6] umfasst Web-Services-Funktionen, die einen UDDI Service, einen Web Services Gateway (der die Kommunikationsfunktionen bei Web Services bezüglich Service Mapping, Import und Export Mapping, Transformationen, UDDI-Publikationen und Lookup wahrnimmt) und eine Implementierung der WS-Security-Spezifikation einschließen. Außerdem werden digitale Signaturen und die Fähigkeit, Identitäten fortzupflanzen unterstützt.

Der *Tivoli Access Manager* (TAM, [6.5.7]) verfügt über Interfaces für das föderierte Identity Management für Web Services, die es Anwendern erlauben, Identity-Standards einschließlich der XML-Key-Management-Spezifikation (XKMS) zu unterstützen.

Neben der Implementierung der WS-Security-Spezifikation ist das *Federated Identity Management Interface* des TAM für einige anspruchsvollere Funktionen erweitert worden. *Web Services Trust Proxy*, *Trust Broker* und *Security Token Service* sind neue Komponenten des TAM, die ein Trust Brokering mit externen Trust Providern z. B. auf Basis der TrustBridge-Technologie ermöglichen. Unternehmen sollen damit in die Lage versetzt werden, den Prozess vertrauensvoller Geschäftsbeziehungen zu automatisieren. IBM hat vor, eine breite Palette von Brokering-Methoden zu unterstützen wie Microsoft TrustBridge, Kerberos Token, Public Key Infrastructure Credentials, SAML und andere Verfahren, die in Zukunft eine Rolle spielen werden.

Der Tivoli Access Manager soll auch das unternehmensübergreifende föderierte Identity Management einschließlich der Validierung und der Bestätigung (Assertion) von Credentials unterstützen, unter Verwendung von systemübergreifenden, föderierten Identity Token, wobei externe Identitäten in interne Identitäten und umgekehrt umgesetzt werden können. Dies soll durch einen *Identity and Credential Mapping Service* für die Transformation der Identitäten zwischen Unternehmen, sowie durch einen *Identity Profile Service* für das Management von Nutzer-Attributen innerhalb föderierter Netze unterstützt werden. Tivoli soll außerdem um eine fein-granulierte Autorisierung für SOAP-Transaktionen in Verbindung mit Web Services erweitert werden. Damit wird die Zugangskontrolle von Web-Services-Anwendungen auf Basis von Nutzer-Identitäten mit zugehörigen Rollen und Berechtigungen ermöglicht.

SAP NetWeaver

Wie in SAPs White Paper *Security: Secure Business in Open Environments* [6.5.8] ausgeführt, bietet die Security-Infrastruktur der *mySAP-Technologie* Funktionalitäten, die

eine heterogene Lösungslandschaft berücksichtigen. Das bedeutet, dass Transaktionen und Informationen von Anwendungen gegen unberechtigten Zugriff durch Authentifikation, Autorisierung, Vertraulichkeit, Verbindlichkeit und Integrität geschützt sind:

- Die Administration von Nutzern mit einem einheitlichen User Store ermöglicht das Managen von Rollen und Zugangsberechtigungen.
- Ein sicheres System-Management schließt Authentifikation und Verschlüsselung ein.
- Digitale Signaturen bieten Sicherheit und Verbindlichkeit auf Anwendungsebene.
- Das Trust Relationship Management umfasst Authentifikation, Single Sign-on und Mechanismen zur Impersonation sowie die Möglichkeit der Integration in Public-Key-Infrastrukturen.
- Ein Audit-Framework kann detailliert Überprüfungen auf existierende Security-Mechanismen vornehmen, um die Integrität von geschäftlichen Transaktionen sicherzustellen.

Die Unterstützung des WS-Security Framework als Teil des Web Application Server (WAS) der NetWeaver-Plattform gehört zu SAPs angekündigter Security Roadmap.

Entrust Secure Transaction Platform

Die *Entrust Secure Transaction Platform* [6.5.9] ist eine Security-Plattform, die definiert, auf welche Weise Basis-Security-Services in Web-Services-Anwendungen zu integrieren sind. Die Plattform erlaubt die Verwendung und Integration von Security-Services mit dem Ziel, Web-Services-Transaktionen durch *Identification, Privacy, Entitlements* (Berechtigungen) und *Verification* sicher und vertrauenswürdig zu machen.

Der *Identification Service* ermöglicht es Unternehmen, Identitäten zentral zu managen, so dass nicht jede einzelne Web-Services-Anwendung diese Aufgabe erledigen muss.

Der *Entitlement Service* versorgt die zentrale Administration mit Zugangsberechtigungen sowie mit Interfaces, die es Anwendungen ermöglicht, diese Berechtigungen zu überprüfen.

Der *Verification Service* bestätigt die Integrität und Verantwortlichkeit von Transaktionen durch zentrale Services für digitale Signaturen und Zeitstempel.

Der *Privacy Service* verschlüsselt Informationen, so dass sie nur den bestimmten Adressaten zugänglich werden.

Entrust bietet vier Methoden zur Integration von Security-Funktionen in Web-Services-Anwendungen:

- Die Integration mit dem Security Toolkit ist die traditionelle Methode; Entwickler betten die Security-Funktionen direkt in ihre Anwendungen ein.
- Die *Direct Integration* erlaubt Web-Services-Anwendungen, eine Reihe von Basis-Security-Services, die Bestandteil der *Entrust Secure Transaction Platform* sind, direkt aufzurufen. Die Plattform bietet Anwendungsentwicklern entsprechende Interfaces.

– Die *SOAP Firewall Integration* stellt eine Methode der transparenten Security dar. Solche SOAP Firewalls kontrollieren den Informationsfluss eines Netzwerks. Sie haben die Aufgabe, nach spezifischen Nachrichten auf Anwendungsebene Ausschau zu halten und diese zu transformieren, wenn sie den Firewall passieren. Der SOAP Firewall kann damit eine Vielfalt von Security-Aktionen im Auftrag einer Anwendung ausführen.
– Die *Application Server Plug-in Integration* beruht auf einem Konzept ähnlich wie dem SOAP Firewall. Security-Funktionen werden im Auftrag von Web Services ausgeführt, jedoch direkt auf dem Application Server, auf dem auch die Business-Logik der Web-Services-Anwendung abläuft.

6.5.5 Zusammenfassung und Empfehlungen

Unternehmen, die den Einsatz von Web Services erwägen, müssen die Security in den Mittelpunkt ihrer IT-Strategie und längerfristigen Planungen stellen. Um Risiko und Komplexität überschaubar zu halten, sollte mit einer Anwendung begonnen werden, deren Security-Anforderungen sich einfach und mit existierenden Mitteln erfüllen lassen. In den meisten Fällen sind dies unternehmensinterne Anwendungen, d.h. Web-Services-Anwendungen, die auf einer einheitlichen Plattform innerhalb der Sicherheitszone laufen (Phase 1 in Kapitel 6.5.2). Auch mit ausgewählten und verlässlichen Partnern können konventionelle Security-Mechanismen zum Einsatz kommen, z. B. können für Punkt-zu-Punkt-Interaktionen zwischen zwei Unternehmen VPN- oder SSL-Verbindungen für sichere Authentifikation und ausreichenden Schutz der auszutauschenden Informationen sorgen (Phase 2).

Web Services werden sich zum De-facto-Standard für Geschäftslösungen entwickeln, wobei die Anwendungsintegration einen Schwerpunkt darstellt. Deshalb müssen sich Unternehmen eher heute als morgen mit dieser Technologie vertraut machen. Anwendungsintegration, traditionell oft durch sogenannte *Spagetti-Verbindungen* realisiert, wird sukzessive durch Hub- und Spoke-Technologien und insbesondere durch den Einsatz von Web Services an Bedeutung gewinnen.

Ad-hoc-Implementierungen von Business-Prozessen lassen sich in Wettbewerbsvorteile umsetzen und helfen Unternehmen, rasch auf veränderte Marktgegebenheiten zu reagieren. Komplexere Web-Services-Lösungen mit vielfältigen oder dynamischen Partnerschaften (Phase 3 und 4) sollten vorerst vermieden oder zumindest sehr vorsichtig angegangen werden. Hierfür sind weitgehende Leistungen für den Einsatz aufwändiger Ressourcen und Security-Techniken bis hin zur Einrichtung einer PKI zu bedenken. Auf der anderen Seite sollten Unternehmen, die bereits eine PKI implementiert haben, durchaus den Mut haben, komplexere Web-Services-Lösungen in die Planungen aufzunehmen.

Unternehmen, die sich strategisch für den Einsatz von Web Services entschieden haben, werden früher oder später auch die Einführung einer PKI erwägen müssen, während Firmen mit bereits eingeführter PKI in einer guten Startposition für den breiten Einsatz von Web Services sind.

7 Ausblick

Die Entwicklung von Gesellschaft und Geschäftswelt wird durch ethische und soziale Themen, individuelle Belange, ökonomische und geschäftliche Einflüsse, politische, legale und regulatorische Vorgaben und schließlich auch durch technologische Weiterentwicklungen bestimmt. Analysten beobachten diese Entwicklungen und entwerfen laufend mannigfaltige Zukunftsszenarien.

Auf diese Zukunftsbilder soll hier nicht weiter eingegangen werden. Gleichwohl werden einige Haupttrends der Informations- und Kommunikationstechnologien und ihre Auswirkungen auf die Themenfelder *Mobility, Web Services* und *Security* erläutert.

7.1 Trends in den Informations- und Kommunikationstechnologien

Wie sich Business Solutions zukünftig entwickeln werden, hängt in großem Maße von wirtschaftlichem Nutzen und breiter Akzeptanz ab. Dabei sind vier Trends von besonderer Bedeutung:

- Konvergenz der Netze
- Virtualisierung von Services
- „Always-on"-Gesellschaft
- intuitive Benutzeroberflächen.

Konvergenz der Netze

Die Tatsache, dass sämtliche Inhalte wie Text, Daten, Sprache, Grafiken, Bilder, Videos oder Multimedia digitalisiert werden können, ist eine entscheidende Voraussetzung für die Konvergenz unterschiedlicher Netze in ein weltweites IP-Netz. Technologien wie VoIP (Voice over IP) und die Implementierung der IP-Protokolle in den verschiedenen Netzzugangstechnologien lassen die Vereinheitlichung von Sprach- und Datennetzen schrittweise Wirklichkeit werden. Bild 7.1 veranschaulicht dieses Szenario.

Der Übergang auf einheitliche IP-Netze ist sowohl für Backbone- und Zugangsnetze (Fest- und Mobilnetze) der Netzbetreiber als auch für Unternehmensnetze von größter Bedeutung. In Unternehmen wird die nächste Generation von Nebenstellenanlagen (PBX) ebenfalls auf IP-Netzstrukturen basieren.

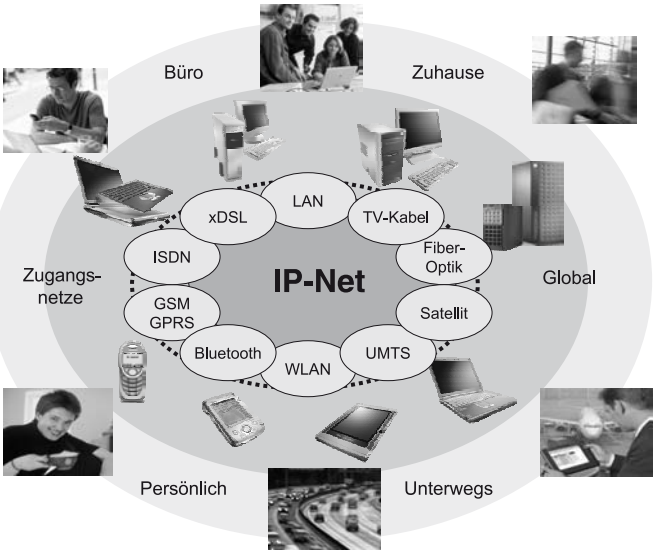


Bild 7.1 Konvergenz der Netze

Konvergenz ist die einzig vernünftige Antwort auf die zunehmende Komplexität der verschiedenen Netzwerke. Langfristige Kosteneinsparungen und nahtlose Kommunikation sind die wesentlichen Aspekte, die diese Entwicklung vorantreiben.

Die einheitliche Transportschicht wird durch das Internet repräsentiert. Die Integration von Echtzeit-Kommunikation mit IT-Anwendungen wird die Ablösung von verbindungsorientierten (Circuit-switched) Techniken durch IP-basierte Vermittlungsanlagen und Router vorantreiben. Das Real-Time-Protokoll *SIP (Session Initiative Protocol)* spielt dabei eine Schlüsselrolle und gewährleistet eine nahtlose Sprachkommunikation sowohl in Festnetzen als auch in Mobilnetzen. In einer Übergangsphase werden Gateways den Übergang zu den traditionellen Protokollen herstellen. Probleme bezüglich der Zuverlässigkeit und Qualität (QoS) sind zwar zu erwarten, sollten aber bis 2007 gelöst sein.

VPN Services werden in durchgängigen IP-Netzen noch an Bedeutung zunehmen. Sie erlauben flexiblen Zugang zu Unternehmensnetzen und ermöglichen virtuelle und sichere Kommunikationskanäle in einem weltweit offenen Netz.

Mobile Geräte werden ebenfalls IP-Protokolle unterstützen. IP Proxies werden WAP Gateways ergänzen und ablösen. Mobile Technologien auf IP-Basis fördern die Entwicklung von neuartigen Geräten. Nutzer werden von phantasievollen Anwendungen begeistert sein und interessante Lösungen schaffen Mehrwert für Unternehmen.

Schließlich stellen konvergente Netze die Voraussetzung für eine starke Verbreitung von Peer-to-Peer-Kommunikation dar. Sie wird zunehmend auch in Business-Anwendungen effizient zum Einsatz kommen, z. B. durch verteilte Verarbeitung, Speicher-Services und dezentralisierte Collaboration.

Virtualisierung von Services

Mobility und Globalisierung bei zunehmendem Kostendruck und weltweitem Wettbewerb sowie vielfältige technologische Weiterentwicklungen führen dazu, dass Unternehmen ihre Organisationen und Dienste verstärkt virtualisieren. Wer schnell und flexibel auf Marktveränderungen reagieren will, muss sich auf seine Kernkompetenzen konzentrieren. Deshalb zeichnet sich der Trend ab, Prozesse, die das Geschäft nicht essenziell tangieren, auszugliedern bzw. in einem virtualisierten Umfeld zu organisieren.

Modelle wie Outsourcing und Offshoring werden bereits erfolgreich praktiziert. Langfristig werden allerdings Technologien wie Web Services, Grid Services, Service-orientierte Architekturen, Software-Agenten und das On-Demand-Paradigma die Virtualisierung von Services weiter vorantreiben. Dadurch kommt es zu gravierenden Veränderungen der heutigen Business Solutions.

Die heute üblichen Standard-Software-Pakete werden modularisiert und spezialisiert und neue Wettbewerber werden mit Best-of-Breed-Services auftauchen. Das Konzept einer überschaubaren, fest definierten Wertschöpfungskette wird durch ein komplexes Netz von ineinander verwobenen Services abgelöst.

Zukünftige Business Solutions sind durch dynamische und ständige Interaktionen mit Partnern und Kunden charakterisiert. Semantische Web Services werden „Plug & Play"-Service-Module und eine automatische Komposition von Services ermöglichen. Outsourcing sowie Virtualisierung von Services und Prozessen werden für jedes Unternehmen bald zur Selbstverständlichkeit. Dank dieser Möglichkeiten werden Firmen Flexibilität gewinnen und in der Lage sein, in Echtzeit zu reagieren, Lieferketten und Lager zu optimieren, Kunden besser zu bedienen und tunlichst unangenehme Überraschungen durch unvorhersehbare Ereignisse zu vermeiden.

Always-on-Society

Laut Gartner wird sich die *Always-on-Society* als Konsequenz der Evolution mobiler Technologien entwickeln. Online-Verbindung zum Netz rund um die Uhr wird eine breite Akzeptanz finden, wenn ausreichend Bandbreiten in mobilen Netzen verfügbar sind, die mit attraktiven Geräten zu bezahlbaren Konditionen genutzt werden können.

Mobility wird zur Selbstverständlichkeit in unserer Gesellschaft und bestimmt immer mehr Aktivitäten und Verhaltensweisen der Menschen. Anwendungen wie Instant Messaging, Location-based und Kontext-abhängige (Context-aware) Services wie auch elektronisches Bezahlen oder Ticketing mit Abrechnung über den Netzbetreiber treiben diese Entwicklung voran.

Mehr noch, in einer Always-on-Welt wird ein mobiles Gerät zum unverzichtbaren Begleiter in der Freizeit: für Kommunikation, Unterhaltung, Information, Shopping, Reisen und Weiterbildung.

Solche persönliche Kompagnons werden mit leistungsfähigen Prozessoren ausgestattet sein und vielfältige Vernetzungsmöglichkeiten sowie ausreichende Batteriekapazität aufweisen. So entwickeln sich mobile Geräte zu persönlichen Anwendungsplattfor-

men. Die Kombination von leistungsfähiger Verarbeitung und Vernetzung fördert die Entwicklung von autonomen Peer-to-Peer-Anwendungen. Solche Anwendungen werden sich in zahlreichen Bereichen etablieren, wie Kommunikation, Messaging, Spiele, Communities, Rendezvous und Medien-Piraterie.

Für zukünftige Geschäftslösungen bedeutet die Always-on-Society eine Neudefinition von Arbeit und Freizeit. Der Trend wird dahin gehen, feste Arbeitszeiten durch Arbeit „zu-jeder-Zeit" und feste Arbeitsplätze durch Arbeit „an-jedem-Ort" abzulösen. Allgegenwärtige Vernetzungs- und Computing-Fähigkeiten werden dazu führen, dass sich Arbeit und Freizeit nicht mehr strikt trennen lassen. Diese Entwicklung stellt die Unternehmen allerdings vor neue Herausforderungen: Die Sicherheitsprobleme nehmen weiter zu, die Arbeitsweise ist mehr Ereignis-getrieben zu organisieren, Aufgaben und Teams müssen dynamisch und flexibel gestaltet und angepasst werden.

Intuitive Benutzeroberflächen

In den vergangenen Jahren sind Geräte, Netze und Anwendungen viel komplexer geworden. Deshalb stehen Nutzer den Neuentwicklungen eher kritisch und zurückhaltend gegenüber. Innovationen werden nur dann akzeptiert, wenn die Bedienung der Geräte dadurch einfacher wird. Deshalb besteht allgemeiner Konsens, dass Benutzeroberflächen signifikant verbessert werden müssen, sei es durch intelligentere Geräte und Anwendungen oder durch den Einsatz neuartiger Mensch-Maschine-Interfaces. Personalisierte, intuitive, selbstlernende Oberflächen müssen in der Lage sein, das Verhalten von Nutzern zu adaptieren und unterschiedliche Situationen zu erkennen. Die Individualisierung von Inhalten und Services muss sich vor allem an den Präferenzen des Nutzers orientieren.

Aus dieser Erkenntnis werden intelligente Anwendungen entstehen, die den Benutzer Kontext-bewusst einbinden, d.h. sie sollen persönliches Profil, Präferenzen, Arbeitsabläufe und Freizeitsituationen, momentanen Aufenthaltsort sowie Geräte- und Kommunikationseigenschaften kennen und berücksichtigen. Solche Anwendungen könnten in ferner Zukunft in der Lage sein, sich auf Verhaltensweisen und Emotionen von Menschen einzustellen.

Multimodale Interfaces, die aus den traditionellen Elementen bestehen und mit Sprach- und Handschrifterkennung kombiniert sind, werden standardmäßig zum Einsatz kommen. Neue visionäre Interaktionskonzepte werden entstehen und die Multimodalität wird es erlauben, die vielfältigen Ein- und Ausgabe-Modi in intuitiver Weise zu kombinieren. So wird es möglich sein, in einer einzelnen Interaktion Sprachbefehle, vordefinierte Textelemente sowie Eingabe über Keypads und Grafiken zu kombinieren. In einigen Szenarien lassen Sensoren Kontext-sensitive Interaktionen mit der Umgebung zu, so dass Lichtverhältnisse, Lautstärke, Bewegungssituationen usw. berücksichtigt werden.

Die Benutzeroberfläche ist zweifellos ein Schlüsselthema für zukunftsorientierte Business-Lösungen und spielt eine entscheidende Rolle für die Akzeptanz neuer Anwendungen und Technologien.

7.2 Auswirkungen auf Mobility, Web Services und Security

Bemerkenswert und einmalig in der IT-Geschichte ist, dass die namhaften Software-Hersteller (Middleware und Anwendungen) gemeinsam eine neue Architektur (SOA) und Technologie (Web Services) unterstützen. Darüber hinaus setzen sich alle wichtigen Hersteller verstärkt für den Ausbau von Mobility- und Security-Funktionen in ihren Plattformen ein.

Web Services

Beachtenswert ist auch, dass die drei Marktführer (Microsoft, IBM und SAP) offensichtlich bei Web Services eng zusammenarbeiten und die Interoperabilität ihrer Plattformen verbessern wollen. Es ist zu erwarten, dass sie sowohl im eigenen Interesse wie auch im Sinne ihrer Kunden bestrebt sind, dieses Ziel zu erreichen. Dadurch wird die Position der Marktführer weiter gestärkt und Mitbewerber dürften in eine schwierige Situation geraten.

Gleichzeitig wird SOA den Markt für innovative Lösungen und Services in Bewegung bringen. Für einige Nischenanbieter mit sehr spezialisierten oder innovativen Services werden sich dadurch neue Chancen eröffnen. SAP, Peoplesoft und andere Software-Hersteller müssen sich dagegen auf zunehmenden Wettbewerb einstellen. Andererseits haben die etablierten Anbieter von Standard-Software selbst die Chance, eigene Web Services als Standard-Services anzubieten, die weltweit und plattformunabhängig genutzt werden können.

Für Unternehmen ist ein Web Service ein virtueller Service. Seine Funktionen sind durch die WSDL-Beschreibung eindeutig definiert. Der Aufrufer eines Web Service muss die Plattform und das Programmiermodell nicht kennen, um diesen Service nutzen zu können.

Mehrere Service-Provider können mittels ihrer Web Services identische Funktionalitäten anbieten, die sich allerdings in den betrieblichen Parametern (Policies) erheblich unterscheiden können. Policies sind definierte Geschäftsvorgaben, wie etwa die Bedingung, dass Daten nur verschlüsselt übertragen werden dürfen. Als Folge benötigt die Service-orientierte Architektur eine Infrastruktur, die genau jene Web Services herausfiltert, die die betrieblichen Aspekte des Anfragers optimal erfüllen. Diese Infrastruktur wird als *Service Bus* bezeichnet und derzeit intensiv unter Experten diskutiert. Der Service Bus ist ein entscheidender Baustein für die Virtualisierung von Services.

Auch andere noch offene Themen wie Security, verteilte Transaktionen, Business Process Languages usw. dürften bis spätestens 2006 gelöst sein. Allerdings haben Software-Hersteller, Standardisierungs-Organisationen und Industriekonsortien oftmals unterschiedliche Sichtweisen und verfolgen divergierende Interessen. Als Beispiel seien die verschiedenen Ansätze zu *Federation* und *Trust* von WS-I und Liberty Alliance genannt. So ist schwer vorhersehbar, inwieweit sich diese Imponderabilien hinderlich auf einen breiten Einsatz von Web Services in Business Solutions auswirken.

Fest steht jedenfalls, dass der Einsatz von Web Services die Unternehmen vor enorme Herausforderungen stellt. Firmen sind deshalb gut beraten, ihre eigene Situation sehr

rasch und kritisch zu durchleuchten, denn für entsprechende architekturelle und technologische Entscheidungen bleibt nur ein begrenztes Zeitfenster offen. Ist der Zug verpasst, steht es schlecht um eine dauerhafte Wettbewerbsfähigkeit.

IT-Service-Provider sollten sich ebenfalls auf diese Veränderungen einstellen und ihr Angebotsportfolio neu ausrichten. Unternehmen brauchen kompetente Beratung, um falsche Ansätze bei der Umstellung auf Web Services zu vermeiden, insbesondere beim Einsatz externer Web Services. Sie brauchen Unterstützung bei der Aufbereitung einer langfristigen und zukunftssicheren Web-Services-Strategie. IT-Service-Provider müssen auch kompetente Lösungs-Architekten zur Verfügung stellen, die in der Lage sind, Unternehmen in eine zukunftsorientierte Lösungswelt hineinzuführen. Außerdem sind IT-Service-Provider in einer hervorragenden Position: Mit dem Angebot vertrauenswürdiger (trusted) Web Services eröffnen sich für sie neue Geschäftsmöglichkeiten. In dieser Rolle treten sie als vertrauenswürdige Vermittler auf, die Services oder ganze Business-Prozesse auf Basis von Web Services anbieten.

Mobility

Mobility ist ein Megatrend, mit dem sich Unternehmen früher oder später auseinandersetzen müssen. Wenn mobile und sichere Lösungen geplant und implementiert werden, sollten vor allem zwei Aspekte Berücksichtigung finden:

Zum Ersten sollten mobile Lösungen auf bewährten, Standard-orientierten Infrastrukturen und einfach integrierbaren Komponenten basieren. Dadurch wird eine kompatible und schrittweise Implementierung ermöglicht. Wiederverwendbare Web Services, integriert in Unternehmensportale, sind der richtige Weg, wenn Lösungen nach ökonomischen Gesichtspunkten realisiert werden müssen und gleichzeitig ein hoher Grad an Flexibilität und Agilität erreicht werden soll. Zentralisierte Anwendungen mit Browser-Clients sind einfach zu managen, sie sind häufig auch die beste Lösung. Allerdings bieten intelligente mobile Clients mehr Flexibilität und werden deshalb langfristig immer interessanter.

Der zweite Aspekt betrifft die Always-on-Society und ihre Auswirkungen auf Beruf und Freizeit. Die Trennung von Arbeit und Freizeit wird sich mehr und mehr verwischen und dies hat sowohl Auswirkungen auf Geräteausprägungen als auch auf Anwendungen und Plattformen.

Immer mehr Menschen wollen uneingeschränkten Zugang zu Services aus dem Netz. Eine Konfiguration, die solche Wünsche erfüllen kann, ist in Bild 7.2 gezeigt.

Das Bild stellt die Vielfalt der Anwendungen dar, die ein Nutzer zukünftig für seine Freizeitaktivitäten und beruflichen Aufgaben zur Auswahl haben möchte. Das dargestellte Smartphone ist insbesondere für Beschäftigte geeignet, die hochqualifizierte Tätigkeiten ausüben (Knowledge Worker). Dieses intelligente Gerät bietet die funktionale Integration einer Vielfalt von Anwendungen. Einige Anwendungsfelder sind dediziert, andere können sowohl für Freizeit als auch Arbeit relevant sein, wie mobiles Bezahlen, Location-based Services, MMS, e-Learning usw.

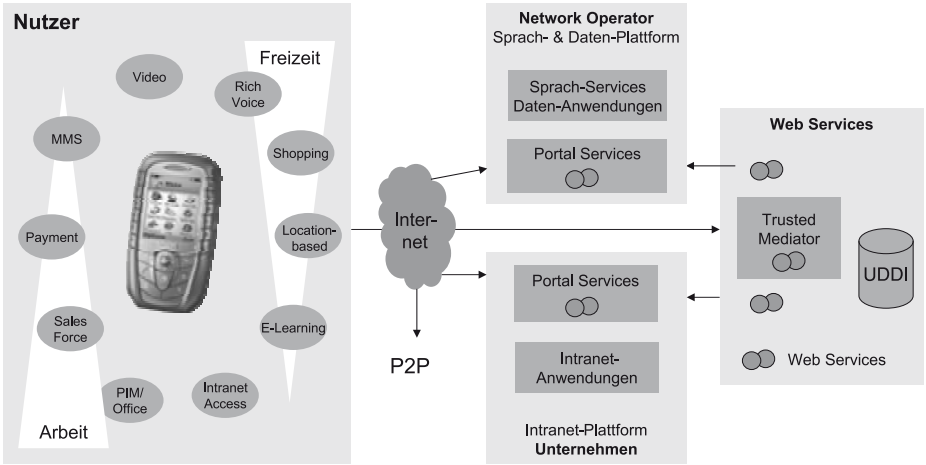


Bild 7.2 Always-on-Plattformen

Für berufliche Tätigkeiten und Freizeitaktivitäten sind vier unterschiedliche Zugangswege aufgezeigt, wie Services aus dem Netz vorteilhaft genutzt werden können: Zugang zum Unternehmensportal, Zugang zum Portal des Netzbetreibers, direkter Aufruf von Web Services aus dem Netz oder über vertrauenswürdige Vermittler und schließlich *Peer-to-Peer(P2P)*-Kommunikation und Services.

Je weiter sich Daten-Services mit digitalisierten Inhalten verbreiten, umso ähnlicher werden sowohl Architekturen von Unternehmens- und Netzbetreiberplattformen als auch angebotene Services. Service-orientierte Architekturen werden sich bei beiden Plattformen durchsetzen. Das Angebot von Web Services wird zunehmen, gleichermaßen durch eigenentwickelte Services der Plattformanbieter wie auch durch innovative und attraktive Services von Drittanbietern.

Folglich wird ein verstärkter Wettbewerb unter Service-orientierten Anwendungsplattformen stattfinden. Beispielsweise könnten Netzbetreiber horizontale Services wie Location-based, Push-, MMS-, PIM- und PKI/Authentifikations-Services für Unternehmen anbieten. Dies könnte insbesondere für kleinere Firmen lukrativ sein. Andererseits haben unabhängige IT-Service-Provider die Chance, die Rolle von vertrauenswürdigen Vermittlern zu übernehmen und Best-of-Breed Web Services anzubieten. Damit treten sie in direkten Wettbewerb zu Netzbetreibern, die sich ihrerseits mit innovativen Services ähnlich positionieren können.

Die Beispiele zeigen, dass dieser Wettbewerb die Verbreitung von Web Services und Service-orientierten Architekturen beschleunigen wird, vorausgesetzt, dass es keine regulatorischen Einschränkungen gibt und die Standardisierung die noch bestehenden Differenzen überwinden kann.

Intelligente mobile Geräte schaffen die Voraussetzung für P2P-Computing. Aufgrund der Entlastung zentraler Ressourcen könnte P2P auch für Geschäftslösungen ein interessantes Modell werden. Allerdings fehlen hierzu noch ausreichende Erfahrungen.

Instant Messaging sowie Datenaustausch und -verteilung wären als Pilotanwendungen geeignet.

Security

In einer Always-on-Welt mit mobilem Zugang zu Unternehmensressourcen, Services von Netzbetreibern und Web Services von Drittanbietern nimmt die sogenannte „*Triple-A*"-Herausforderung (Authentication, Authorization and Accounting) eine neue Dimension an.

Auf der einen Seite stellen VPNs einen geeigneten Mechanismus für sichere Kommunikationskanäle in offenen Netzen dar. Andererseits sind Authentifikationsmethoden mit Passwörtern weder sicher genug, noch einfach zu handhaben, vor allem wenn der Zugang zu mehr als einem Dutzend Ressourcen zu managen ist. Ein zuverlässiges PKI-Umfeld mit Single-Sign-on-Funktionalität scheint in diesem Fall die einzig vernünftige Lösung, insbesondere bei Zugang zum Intranet und zu unternehmenskritischen Anwendungen.

Vertrauliche Informationen wie private Schlüssel werden am besten in besonders geschützten (Tamper-resistant) Modulen gespeichert. Smartcards und SIM-Cards basieren beide auf einer *Tamper-resistant* Chip-Technology, bei der Schutzmaßnahmen in Hardware und Software integriert sind. Dadurch ist ein sehr hohes Sicherheitsniveau gewährleistet. Chipkarten haben sich seit vielen Jahren bewährt, sind standardisiert, portabel und in vielen Geräten einsetzbar. Das bedeutet, dass Nutzer ihren privaten elektronischen Schlüssel wie Kreditkarten mit sich herumtragen und in unterschiedlichen Geräten verwenden können.

Wie in Kapitel 6 beschrieben, ist eine Smartcard ein multifunktionales Security Tool, geeignet für ein ganzes Bündel von Anwendungen mit hohen Sicherheitsanforderungen, z. B. für den Zutritt zu Gebäuden und Räumen, zur Authentifikation und Autorisierung beim Zugang zu Applikationen und für die digitale Signatur zum Signieren von e-Mails und zur Beglaubigung der Authentizität elektronischer Dokumente. Diese kombinierten Funktionen machen die Smartcard zu einem idealen elektronischen Identitäts-Tool, z. B. in Form eines Mitarbeiterausweises oder einer Bürgerkarte mit vielfältigen sicherheitsrelevanten Anwendungsmöglichkeiten.

SIM Cards basieren auf derselben Prozessor-Technologie und den gleichen Standards (ISO 7816) wie Smartcards und werden zurzeit im Wesentlichen als Schlüssel (Token) zur Authentifikation des Mobiltelefons beim Netzbetreiber verwendet. Mit den WAP-Standards 1.2/2.0 wurde das Wireless Identification Module (WIM) eingeführt. WIM ist eine dedizierte Spezifikation für Security Token. Der Token besteht aus personenbezogenen privaten Schlüsseln und Zertifikaten.

Das WIM-Modul ist als eigenständige Smartcard-Anwendung definiert. Es kann entweder als Software-Modul auf der SIM Card des Netzbetreibers residieren oder als separate Karte (*WIM Card)* ausgeführt sein. WIM und SIM Card haben den gleichen Formfaktor. WIM-Module oder WIM Cards können von Netzbetreibern oder von anderen Service-Providern (z. B. Banken) oder auch von Unternehmen herausgegeben werden. Separate WIM Cards können neben der SIM Card in einem zusätzlichen Steck-

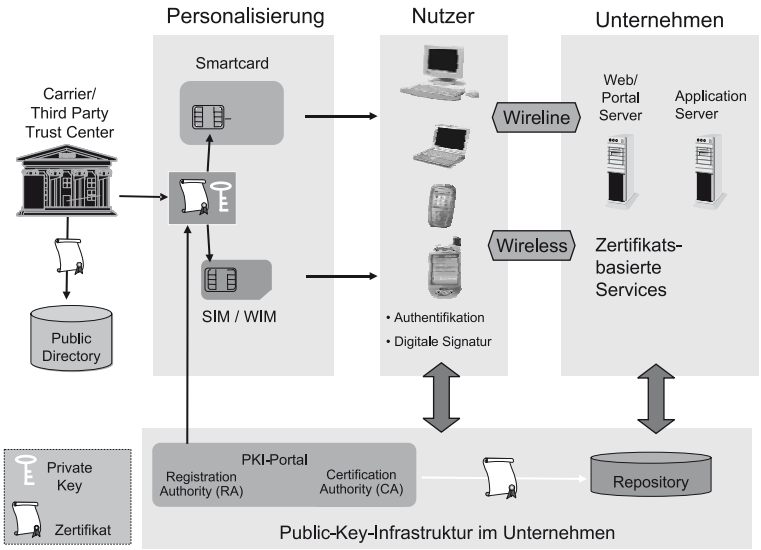


Bild 7.3 Smartcard- und SIM-Card-basierende Security-Lösung

platz, den einige Mobiltelefone aufweisen, eingesetzt werden. In UMTS-Netzen wird statt der SIM Card die *Universal SIM Card (USIM)* verwendet. Sie bietet auf der Basis modernster Chip-Technologie zusätzliche Security-Funktionen durch einen On-chip Crypto-Controller, der in der Lage ist, private Schlüssel auf dem Chip selbst zu generieren.

Mit Rückblick auf die Always-on-Plattformen in Bild 7.2 sind diese kombinierten Smartcard- und USIM/SIM/WIM-Technologien hervorragend für den Einsatz in zukunftsorientierten Lösungen mit höchsten Security-Anforderungen geeignet und stellen die passende Antwort auf die „Triple A"-Herausforderung dar.

Die Elemente einer solchen Lösung sind in Bild 7.3 gezeigt.

Diese Lösung setzt eine PKI-Infrastruktur voraus. Unternehmen mit Multi-Channel-(Mobil- und Festnetz-)Anwendungsstrukturen stehen vor der Aufgabe, die Security-Architekturen für den mobilen Zugang und das Festnetz zu harmonisieren und in ein zukunftssicheres Design zu investieren. Disjunkte Security-Infrastrukturen für Web und WAP sind aus Kostengründen zu vermeiden.

Eine harmonisierte Security-Architektur ist in Bild 7.3 veranschaulicht. Die Lösung schließt Authentifikation, Integrität und Verbindlichkeit basierend auf Zertifikaten und digitalen Signaturen ein. Die verwendeten Technologien umfassen Smartcards, WAP, SIM-Cards und WIM, später erweiterbar durch USIM Cards.

In einem Personalisierungsprozess werden in Anlehnung an den PKI-Standard private Schlüssel und Zertifikate von Nutzern auf ihren Smartcards und gleichzeitig auch in den WIM-Modulen ihrer mobilen Geräte gespeichert. Entweder das Unternehmen selbst oder ein Netzbetreiber oder ein anderer vertrauenswürdiger Service-Provider

erzeugt die Schlüssel und Zertifikate in einem Trust Center, speichert private Schlüssel und Zertifikate auf der Smartcard und im WIM und verteilt die korrespondierenden öffentlichen Schlüssel (Public Keys) auf entsprechende Directories. Die Personalisierung muss in hochsicherer Umgebung erfolgen und liegt je nach Business-Modell in der Verantwortung des Netzbetreibers (in der Regel, wenn das WIM als SIM-Card-Applikation realisiert ist) oder in der Verantwortung des Unternehmens selbst, bzw. im Fall des Outsourcing an einen Trusted Service Provider in dessen Verantwortung.

In den meisten Fällen ist es zweckmäßig, Nutzern jeweils für Authentifikation und Datenverschlüsselung unterschiedliche Schlüssel zuzuweisen. In fortschrittlichen Lösungen können Nutzer die Generierung des Authentifikationsschlüssels selbst durchführen und sich von einer lokalen Autorisierungsstelle (Local Registration Authority) registrieren lassen. Über den PC initiiert wird das Schlüsselpaar (privater und korrespondierender öffentlicher Schlüssel) in der am PC angeschlossenen Smartcard/USIM Card mittels Cryptocontroller auf dem Chip selbst erzeugt. Der private Schlüssel verlässt diesen Chip niemals, der öffentliche Schlüssel wird in die entsprechenden Directories verteilt. Das Schlüsselpaar für die Datenverschlüsselung wird nach wie vor in einem Trust Center generiert und verwaltet. Unter Verwendung des Authentifikationsschlüssels kann es nun sicher auf die Smartcard/USIM Card geladen werden. Mit einer derartigen Lösung kann der Administrationsaufwand deutlich reduziert werden und trotzdem wird ein hohes Maß an Sicherheit erreicht.

Aus Sicht des Nutzers ist diese Chipkarten-basierte Lösung ein Riesenfortschritt, da sie die Verwendung von Dutzenden immer wieder zu modifizierenden Passwörtern überflüssig macht und unterschiedliche Prozeduren für die Authentifikation und Erzeugung von digitalen Signaturen vermeidet. Aus der Perspektive des Unternehmens spart diese Lösung letztendlich Kosten, obwohl zunächst hohe Investitionen für PKI- Infrastruktur und Personalisierung vorzunehmen sind. Ein weiterer Vorteil ist das hohe Sicherheitsniveau für sämtliche mobilen Geräte. Solche Lösungen eignen sich insbesondere, wenn künftig die Lebensbereiche Beruf und Freizeit nicht mehr zu trennen sind.

Das persönliche Kommunikationsmodul

Die logische Weiterentwicklung der oben skizzierten Lösung basiert auf einer Komponente, die hier in einer Zukunftsvision als *Universal Personal Communication Module (UPCM)* vorgestellt werden soll.

Wie in Kapitel 4 erläutert, wird die Divergenz mobiler Geräte weiter zunehmen. Innovative, intelligente Smartphones, PDAs, Laptops, Tablet PCs, portable TVs usw. werden den Markt erobern. GPRS/UMTS, WLAN und Bluetooth sind komplementäre Technologien, die voraussichtlich über viele Jahre koexistieren werden. Neue Szenarien für Geschäfts- und Freizeitanwendungen werden sich entwickeln. Personalisierung wird bei einer akzeptablen und einfachen Nutzung dieser Anwendungen eine Schlüsselrolle spielen. Identifikation, Authentifikation, digitale Signatur und Verschlüsselung werden obligatorisch für die Nutzung beliebiger Services sein. Damit wird der Wunsch nach einem Medium immer offensichtlicher, das persönliche Daten, Schlüssel und Zertifikate des Nutzers enthält und wie eine Kreditkarte herumgetragen und in beliebigen Geräten netzunabhängig verwendet werden kann.

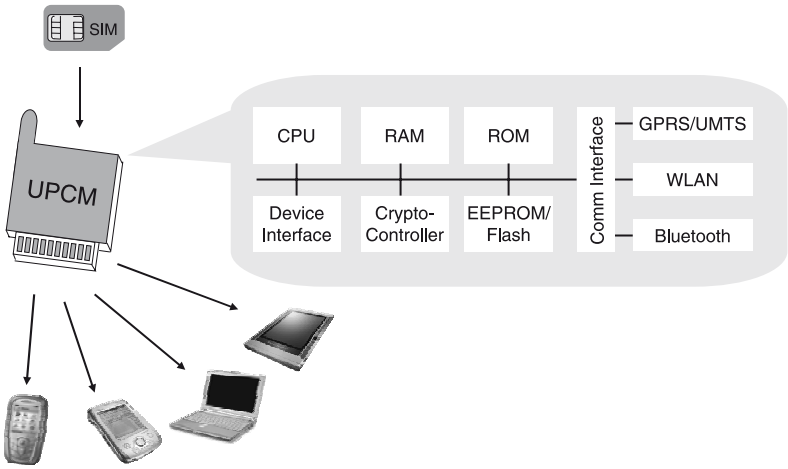


Bild 7.4 Universal Personal Communication Module

Zieht man all diese Aspekte in Betracht (Geräte- und Netzunabhängigkeit, Security und Personalisierung) und geht man wie bisher von einer weiteren Miniaturisierung von Speicher-, Prozessor- und Kommunikationschips aus, dann wird die Idee eines persönlichen Kommunikationsmoduls, des UPCM, plausibel.

Das UPCM könnte Security- und Netztechnologien sowie PIM, persönliche Attribute und Daten in einem einzigen Modul vereinen. Wie in Bild 7.4 veranschaulicht, wäre es machbar, das Modul über ein standardisiertes Interface (z. B. CF Card) in beliebige Geräte einzustecken. Nach Einführen des Moduls erkennt das Betriebssystem automatisch das UPCM, führt die notwendigen Konfigurationen durch und aktiviert es. Optional könnte das UPCM mit einem Fingerprint Sensor ausgestattet sein, so dass es nur durch Fingerdruck des Besitzers aktiviert werden kann.

Bevor diese Idee verwirklicht werden kann, müssen sich freilich Hersteller und Netzbetreiber auf einen geeigneten UPCM-Standard einigen. Als Ausgangsbasis könnte der USIM-Standard dienen. Vereinbarungen über Geräte-Interface und Netzanschlüsse (GPRS, UMTS, Bluetooth, WLAN 802.11 a, b, g, i, usw.) müssten ergänzt werden.

Das UPCM könnte von Geräteherstellern oder Netzbetreibern angeboten werden. Die SIM/USIM-Funktionalität sollte entweder integriert sein oder das UPCM müsste mit einem Slot für die gängigen Karten ausgestattet sein.

Wie in Bild 7.4 dargestellt, ähnelt die vorgeschlagene UPCM-Architektur sehr der von modernen Smartcards, die aus CPU, RAM, ROM, EEPROM/Flash und Cryptocontroller bestehen. Das UPCM sollte sicherheitsgeschützt (Tamper-resistant) ausgeführt sein, um eine sichere Speicherung von Schlüsseln und Zertifikaten zu gewährleisten. Es ist mit einem standardisierten Geräte-Interface und verschiedenen Kommunikationsmodulen auszustatten. Entsprechende Software soll die Synchronisation von PIM und persönlichen Daten via PC ermöglichen.

Im Vergleich zu heute verfügbaren Kommunikations- und Security-Komponenten weist das UPCM eine Reihe von offensichtlichen Vorteilen auf:

- Eine einzige Komponente umfasst Security, Netzanschlüsse und persönliche Daten und ist in beliebigen Gerätetypen (Laptops, Tablet PCs, PDAs, Smartphones) einsetzbar. Sie ersetzt eine Vielzahl heute verwendeter, unterschiedlicher, geräteabhängiger und separater Security- und Kommunikationskomponenten.
- Unabhängig von Gerätetyp und Netzumgebung wird dem Nutzer dank der integrierten Zertifikats-basierten Authentifikationsmethode ein unkomplizierter Zugang zu persönlichen und geschäftlichen Netzressourcen ermöglicht.
- Unabhängig vom verwendeten Gerät sind die PIM-Daten des Nutzers wie auch persönliche Dateien und Attribute sowie Präferenzen, die für Offline- oder Online-Anwendungen eine Rolle spielen, lokal auf dem UPCM gespeichert und immer verfügbar.
- Besitzer des UPCM (CF-Card-Größe) führen es immer mit sich und können es in jedem beliebigen Gerät nutzen, das über ein UPCM-Interface verfügt.
- Das UPCM ist sicherheitsgeschützt (Tamper-resistant), d.h. die Speicherung von Schlüsseln und vertraulichen Informationen sowie das Laden über das Mobilnetz ist mit hohem Sicherheitsniveau gewährleistet.
- Unternehmen können beträchtlich Kosten sparen, da sie anstatt einer Vielzahl von Security- und Kommunikationskomponenten nur noch einen einzigen Typ einkaufen, personalisieren und administrieren müssen.
- Gerätehersteller können Geräte ohne integrierte Security- und Netzkomponenten kostengünstiger designen, während die Entwicklung eines UPCM entkoppelt und in weltweitem Wettbewerb erfolgt und somit zu einer beschleunigten Innovation führen könnte.

Es dürfte spannend werden, wie die Industrie diese technologischen Herausforderungen und die zunehmende Verschmelzung von Beruf und Freizeit bewältigen wird und ob sich in diesem Kontext ein standardisiertes Modul wie das UPCM realisieren lässt.

7.3 Zusammenfassung und Schlussfolgerungen

Laut einer aktuellen Studie von Gartner halten CIOs *Security* für das wichtigste IT-Thema, vor EAI/Middleware und gefolgt von Messaging und Portalen. Bis 2006 wird es auch das dringlichste Thema bleiben. Gleichzeitig werden Web Services, 2003 noch die Nummer 5 bei den Technologiethemen, bis 2006 auf Position zwei vorrücken.

Unbestritten ist, dass Informationen und Wissen mittlerweile das wichtigste Gut eines Unternehmens sind. Der Schutz von Informationen, die gespeichert, verarbeitet oder übertragen werden, ist von essenzieller Bedeutung für das kontinuierliche Geschäft. Es muss sichergestellt sein, dass potenzielle Bedrohungen so gering wie möglich gehalten werden. Security als horizontale Technologie ist Bestandteil jeder Komponente einer e-Business-Lösung. End-to-End Security wird bestimmt durch das schwächste Glied die-

ser Kette. Sowohl die mobilen Anwendungen als auch der Einsatz von Web Services leiten eine Ära neuer und ernstzunehmender Security-Herausforderungen ein.

Web Services und *Service-orientierte Architekturen* bilden ein neues Paradigma für IT-basierte Business-Lösungen. Gravierende Änderungen, verschärfter Wettbewerb und beschleunigte Entwicklung von Anwendungen werden den Markt bestimmen. IT-Manager sind gefordert und machen sich Gedanken, wie sie dies alles unter einen Hut bringen können. Die Anwendung von Web Services stellt das Modell einer zweistufigen Programmierung dar, wodurch größere Flexibilität erreicht wird und sich Geschäftsprozesse einfach ändern lassen. Unternehmen und IT-Service-Provider werden deshalb Geschäftsbeziehungen und Verantwortungen überdenken und neu definieren müssen.

Der Megatrend *Mobility* wird unsere Gesellschaft und Geschäftswelt stark beinflussen und ständig verändern. Laut Analysen der Meta Group wird sich die „Mobilisierung" von Anwendungen zu einem Schlüsselthema für Unternehmen entwickeln und größte Anstrengungen sowie umfangreiche Ressourcen erfordern. Leider passiert es immer wieder, dass Organisationen einen falschen Ansatz wählen und gleich beim ersten Versuch scheitern. Ein Beispiel aus der Vergangenheit ist die Einführung des PC und der Client/Server-Architektur, die einige Unternehmen fast 20 Jahre gekostet haben, bis die letzten Umstellungsprobleme endlich gelöst waren.

Ein erster Schritt wäre die Erstellung und Umsetzung einer Mobility Policy im Unternehmen. Diese Policy kann Kriterien für mobile Anwendungen, Einkaufsrichtlinien, Prozess- und Budgetverantwortung, Hersteller- und Geräteauswahl, einzuhaltende Standards, Sanktionen usw. umfassen. Tatsächlich lässt sich in den meisten Unternehmen eine selektive Mobilisierung heute schon rechtfertigen.

Wenngleich es sich bei *Mobility, Security* und *Web Services* zweifelsfrei um völlig verschiedene Technologien mit in der Regel unabhängigen Implikationen und Historien handelt, müssen sie doch im Kontext anstehender Paradigmenwechsel, evolutionärer Architekturänderungen und neuer Business-Anforderungen ganzheitlich in ihren Auswirkungen gesehen werden. In diesem Buch wurden an vielen Stellen Abhängigkeiten und operative wie auch strategische Zusammenhänge aufgezeigt.

Als Schlussfolgerung aus den vielfältigen und faszinierenden Entwicklungen mögen CIOs, IT-Experten und Entscheidungsträger folgende Empfehlung mit auf den Weg nehmen:

Konzentrieren Sie das im Unternehmen vorhandene Wissen über die drei dargestellten Technologiefelder, legen Sie Policies über Security, Mobility und Anwendungen passend zueinander aus und berücksichtigen Sie das Zusammenspiel dieser Technologien bei der Definition einer zukünftigen IT-Strategie. Entwickeln Sie neue Business-Lösungen nur auf der Basis bewährter, Standard-orientierter Infrastrukturen und modularer, einfach integrierbarer und Plattform-unabhängiger Software-Komponenten. Stellen Sie einen Migrationsplan auf, der den Weg zu einer Service-orientierten Architektur weist, Geschäftsrisiken, Mobility-Anforderungen sowie ein zukunftsorientiertes Prozess- Management berücksichtigt und sich realistisch umsetzen lässt.

Noch nie zuvor wurden Unternehmen mit derartig gravierenden Veränderungen, Herausforderungen und Risiken konfrontiert. Die richtigen Entscheidungen jetzt zu treffen und in zukunftssichere Geschäftslösungen umzusetzen, eröffnet jedoch auch eine einmalige Chance.

Referenzen

Vorwort

[V.1] MÜNCHNER KREIS, Tal 16, 80331 München
http://www.muenchner-kreis.de/index_e.htm

Kapitel 1

[1.1] Open Source Software, von Lothar Gläßer, Publicis Corporate Publishing 2004, ISBN 3-89578-240-8

Kapitel 2

[2.2.1] GSMWorld. http://www.gsmworld.com/index.shtml

[2.2.2] WAP Forum. http://www.wapforum.org/what/technical.htm

[2.2.3] UMTS Forum. http://www.umts-forum.org/servlet/dycon/ztumts/umts/Live/en/umts/Home

[2.2.4] 3GPP. http://www.3gpp.org

[2.2.5] Wireless Ethernet Compatibility Alliance. http://www.wirelessethernet.org/

[2.2.6] Bluetooth. www.bluetooth.org

[2.2.7] GPRS and 3G wireless applications. Professional developer's guide, by Cristoffer Andersson, Publisher John Wiley & S Inc, 2001, ISBN 0-471-41405-0

Kapitel 3

[3.1.1] IT-Lösungen im e-Business, von Lothar Gläßer, Publicis Corporate Publishing, 2003, ISBN 3-89578-203-3

[3.1.2] ebXML. http://www.ebxml.org

[3.1.3] OASIS. http://www.oasis.org

[3.1.4] RosettaNet. http://www.rosettanet.org/RosettaNet/Rooms/DisplayPages/LayoutInitial

[3.1.5] W3C. http://www.w3c.org

[3.1.6] XML. http://www.xml.org

[3.1.7] XML inclusions. http://www.w3.org/TR/2002/CR-xinclude-20020917/

Kapitel 4

[4.3.1] WAP 2.0. http://www.wapforum.org/what/technical.htm

[4.3.2] Palm OS. http://www.palmsource.com/palmos/

[4.3.3] Windows Mobile. http://www.microsoft.com/windowsmobile/default.mspx

[4.3.4] Symbian OS. http://www.symbian.com

[4.3.5] Nokia, Series 60. http://www.forum.nokia.com/main/0,6566,010_40,00.html

[4.3.6] Research in Motion, BlackBerry. http://www.rim.com

[4.3.7] J2ME. http://java.sun.com/j2me/

[4.3.8] .NET Compact Framework. http://msdn.microsoft.com/mobilty/ prodtechinfo/ devtools/netcf/

[4.3.9] Windows Mobile development tools. http://msdn.microsoft.com/library/ default.asp?url=/library/en-us/dnppcgen/html/devtoolsmobileapps.asp

[4.3.10] IBM Enterprise mobile applications. http://www-3.ibm.com/software/ pervasive/enterprise/

[4.3.11] SAP Mobile Infrastructure. http://www.sap.com/solutions/mobilebusiness/

[4.3.12] Extended Systems Mobile Enterprise Applications. http://www.extended systems.com/ESI/Products/Mobile+Data+Management+Products/ Mobile+ Application+Development/MAP+Features.htm

[4.3.13] Mobility Solutions Fujitsu Siemens. http://www.fujitsu-siemens.com/ mobility/

[4.4.1] Mobilelife Portal. https://www.siemens-mobilelife.de

Kapitel 5

[5.2.1] Global XML Web Services Architecture (GXA). http://msdn.microsoft.com/ library/default.asp?url=/library/en-us/dngxa/html/understandgxa.asp

[5.2.2] WS-I Organization. http://www.ws-i.org/

[5.2.3] W3C, Web services standards. http://www.w3c.org/2002/ws/

[5.2.4] WS-CAF. http://www.oasisopen.org/committees/tc_home.php? wg_abbrev=ws-caf

[5.2.5] OASIS FWSI. http://www.oasis-open.org/committees/tc_home.php? wg_abbrev=fwsi

[5.3.1] Objektspektrum, Ausgabe 6/2003. http://www.sigs-datacom.de/sd/ publications/os/index.htm

[5.3.2] OASIS WSDM. http://www.oasisopen.org/committees/tc_home.php? wg_abbrev=wsdm

[5.4.1] SAP NetWeaver. http://www.sap.com/solutions/netweaver/

[5.4.2] Microsoft Web services. http://msdn.microsoft.com/webservices/

[5.4.3] WebSphere & Web services. http://www-106.ibm.com/developerworks/ ibm/library/i-services.html

Kapitel 6

[6.1.1] Computer emergency response team. http://www.cert.org

[6.2.1] IT-Sicherheit. Konzept, Verfahren, ProtokolleClaudia Eckert, Oldenburg 2003, 2. überarbeitete Auflage, ISBN 3-486-27205-5

[6.2.2] Siemens Business Services Security. http://www.siemens.com/index.jsp?sdc_p=po1050773fcl0s2mu2&sdc_sid=6108248724&sdc_bcpath=1050135.s_2%2C1045390.s_2%2C1045390.s_2%2C&

[6.2.3] SIT Fraunhofer Gesellschaft. http://www.sit.fraunhofer.de/german/hps1/

[6.3.1] WAP standards. http://www.wapforum.org/what/technical.htm#Approved

[6.3.2] WLAN Protected Access. WI-FI Protected Access Finally Arrives, Business Communication Review, May 2003

[6.3.3] Bluetooth Security White Paper. http://www.bluetooth.com/upload/24Security_Paper.PDF

[6.3.4] Security on Pocket PC. http://www.microsoft.com/windowsmobile/resources/whitepapers/security.mspx

[6.3.5] Security on Palm. White Paper: Handheld Security for the Mobile Enterprise, 2002 Palm, Inc.

[6.4.1] IDC Report. E-World Survey and Internet Commerce Market Model, 2002

[6.4.2] RADIUS. http://www.ietf.org/rfc/rfc2138.txt?number=2138

[6.4.3] TSL/SSL. http://www.ietf.org/rfc/rfc2246.txt?number=2246

[6.4.4] SSH. http://www.ssh.com/solutions/secureshell.html

[6.4.5] X.509. http://ietf.org/html.charters/pkix-charter.html

[6.4.6] PKCS. http://www.pkcs.org/

[6.4.7] Kerberos. http://www.ietf.org/rfc/rfc1510.txt?number=1510

[6.4.8] XML Security, SAML. http://www.nue.et-inf.uni-siegen.de/~geuer-pollmann/xml_security.html

[6.4.9] Microsoft .NET Passport. http://www.microsoft.com/net/services/passport/

[6.4.10] Liberty Alliance Project. http://www.projectliberty.org/index.html?faqs/index.html~content

[6.4.11] Entrust GetAccess. http://entrust.com/getaccess/index.htm

[6.4.12] RSA ClearTrust. http://www.rsasecurity.com/products/cleartrust/index.html

[6.4.13] Netegrity SiteMinder. http://www.netegrity.com/products/index.cfm?leveltwo=SiteMinder

[6.5.1] Web Services Security by Mark O'Neill et al., Publisher McGraw- Hill/Osborne 2003, ISBN 0-07-222471-1

[6.5.2] UDDI, OASIS. http://www.uddi.org, http://www.oasis-open.org/ home/index.php

[6.5.3] Web services security specifications. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnglobspec/html/wssecurspecindex.asp

[6.5.4] RSA Security, White Paper Web services security. http://www.rsasecurity.com/solutions/web-services/whitepapers/WSS_WP_0802.pdf

[6.5.5] Microsoft Trustbridge. http://www.microsoft.com/presspass/press/2002/Jun02/06-06TrustbridgePR.asp

[6.5.6] IBM WebSphere, WS-Security. http://www-106.ibm.com/developerworks/webservices/wsdk/

[6.5.7] IBM Tivoli Access Manager. http://www-306.ibm.com/software/tivoli/products/ access-mgr-e-bus/

[6.5.8] SAP, Secure Business in open Environments, http://www.sap.com/solutions/netweaver/brochures/

[6.5.9] Entrust Secure Transaction Platform. http://www.entrust.com/stp/index.htm

Stichwortverzeichnis

D

E

F

G

H

I

J

Q

R

S

T

U

V

W

X

Z