Dr. Suppan International Institute

Der Netzwerk Insider

Februar 2001

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

"Wozu brauche ich ein Zertifikat?" Verschlüsselung und Signaturen im E-Business/E-Commerce

von Dr. Christian Mrugalla

Im Zusammenhang mit der wachsenden Verbreitung der Informationstechnik in nahezu allen Lebensbereichen und der steigenden Vernetzung der Systeme wird immer wieder auf die erheblichen Effektivitätsreserven hingewiesen, die sich durch konsequente IT-Nutzung in kompletten Geschäftsprozessen realisieren ließen. Durch den Einsatz von digitalen Signaturen und Verschlüsselungsverfahren können auch "anspruchsvolle" Geschäftsprozesse zukünftig ohne Medienbrüche vollständig elektronisch abgewickelt werden.

Erst hierdurch wird ein umfassender elektronischer Geschäftsbetrieb ("E-Business") möglich. Das Internet verliert zunehmend den Charakter einer "Spielwiese" und wird zu einer universellen Aktionsplattform für Geschäftsprozesse aller Art - auch für solche mit erheblichen finanziellen und rechtlichen Auswirkungen.

Der Schlüssel zu E-Business, E-Commerce und E-Gouvernment: Verschlüsselung und Signaturen

Der elektronische Handel im Internet ("E-Commerce") ist nur ein – wenn auch gerade in seiner Außenwirkung wesentlicher – Bestandteil. Ob die weitere Entwicklung diese hochgesteckten Erwartungen erfüllen wird, hängt entscheidend davon ab, ob es gelingt, die Akteure der "elektronischen Geschäftswelt" und insbesondere die Verbraucher von der Zuverlässigkeit und Sicherheit der neuen Dienstleistungen und Angebote zu überzeugen.

Neben E-Commerce und E-Business gerät derzeit auch die elektronische Erbringung von Verwaltungsdienstleistungen ("E-Government") ins Blickfeld der öffentlichen Diskussion. Da E-Government letztlich nichts anderes als E-Business der öffentlichen Verwaltung ist, gelten alle in diesem Artikel angestellten Überlegungen auch für den öffentlichen Bereich.

weiter Seite 11

Sicherheit

Content-Security – noch immer weit unterschätzt

von Dipl.-Inform. Detlef Weidenhammer

Der alleinige Schutz von Netzgrenzen durch Firewallsysteme oder Secure RAS-Lösungen ist schon lange kein ausreichendes Mittel mehr gegen die Gefahren aus dem Internet. Bei sachgerechter Konfiguration bieten sie zwar ein nahezu unüberwindliches Hindernis für direkte Angreifer, viel gravierender sind jedoch die Risiken, die mit der Freigabe von allgemein genutzten Diensten wie Electronic Mail und World-Wide-Web einher gehen. Diese Dienste importieren Daten in das interne Netz, zu deren Kontrolle Firewalls gänzlich ungeeignet sind. Aktueller Stand von Bedrohungen und Gegenmaßnahmen sollen nachfolgend aufgezeigt werden.

Die momentan wohl größte Sicherheitsbedrohung für Unternehmen geht von Netzdiensten aus, die in der Lage sind ungeprüft eigenen Programmcode in ein Netzwerk einzuschleusen. Da aber genau diese Möglichkeit die heute wichtigsten Anwendungen wie Mail, Web und Filetransfer betrifft, kann das einfache Unterbinden dieser Dienste keine Lösung sein. Zumeist wird in diesem Zusammenhang nur von Viren gesprochen, diese stellen aber mittlerweile nicht mehr die alleinige Gefahrenquelle dar. Alle Arten von sog. Malicious Code (Programmcode mit bösartigen Nebenwirkungen) müssen in die Sicherheitsbetrachtungen einbezogen werden.

Noch weitaus gefährlicher als Viren, insbesondere für den aufkommenden E-Business Bereich, sind Schäden, die sich durch das automatische Laden von Programmen oder Programmteilen im Rahmen der Webnutzung ergeben. Zu dieser Art von Mobile Code gehören Java, JavaScript, ActiveX aber auch beliebige Anwendungsprogrammen aus unsicherer Quelle.

Die Manipulationen lassen sich durch herkömmliche Virenscanner selten entdecken und sind in ihren Möglichkeiten nahezu unbegrenzt.

weiter Seite 3

Zum Geleit

Switch-Produkte im Umbruch: was hat noch Bestand?

Der Markt für Switch-Systeme steht vor spannenden Umbrüchen. Mit der Entwicklung ergeben sich auch zunehmend Forderungen an eine starke Verbesserung der bisherigen Produkteigenschaften.

Die sich abzeichnenden Änderungen haben jeweils je nach Produktbereich völlig verschiedene Facetten und Ursachen:

1. Umbruchbereich: Workgroup-Switches
2. Umbruchbereich: Enterprise-Switches
3. Umbruchbereich: Management und Konfiguration

Im Bereich der Workgroup-Switches hat HP eine neue Runde im Kampf um den Kunden eingeleitet. Der neue ProCurve 2524 setzt die traditionellen Marktführer 3Com 3300, CISCO 29xx, 35xx, Intel 510 und Nortel 350/450 schwer unter Druck. Der HP-Switch hat im Layer-2-Bereich alles, was man braucht: 24 Festports, 2 freie Einschübe für Gigabit bzw. LWL-Ports, Spanning Tree, 802.1p, Link Aggregation, RMON, SNMP, VLAN inkl. GVRP, IGMP und natürlich den Monitoring Port für VLANs und Einzelports. Angekündigt für den kostenlosen Uprade sind TACACS und Radius. Und das alles für 2000 DM zzgl. MwSt. Da sehen die bisherigen Produkte doch im Vergleich reichlich angestaubt aus. Und nicht nur das: der Switch ist mit einer ver-

nünftigen Web-Applikation ausgestattet, die tatsächlich nahezu intuitiv nutzbar ist (liebe CISCOs und Extremes: habt ihr das Wort intuitiv zur Kenntnis genommen?), er hat CLI und Menu-Interface für die Konfiguration. Zusätzlich wird er mit der kostenlosen HP TopTools Software für Überwachungs-Management ausgeliefert. Keine Frage, damit ist die nächste Runde im Bereich der Etagen-Switches eingeläutet. Das Motto heißt: funktional komplette Ausstattung zum Kampfpreis. Intel hat auch sofort reagiert und die Preise für den 510T, einen funktional sehr ähnlich und bisher durchaus interessant positionierten Switch, reduziert.

Im Bereich der Enterprise-Switches zeichnen sich ebenfalls größere Umbrüche ab. Der Markt der kleineren Provider und der größeren Campus Netze bei den Unternehmen verschmilzt zunehmend. Optische Technologien bringen völlig neue Leistungen in die Netzwerke. Gefragt sind die Highend-Layer-3-Verfahren bei hohen Weiterleitungs-Leistungen. Dabei zählt weniger die reine theoretische Leistung der Schaltmatrix als vielmehr der tatsächlich erreichbare IP-Durchsatz. Blockadefreie Architekturen, Vermeidung von CPU-Überlasten, ausreichend große Puffer auch für Gigabit-Datenströme im QoS-Betrieb (Hinweis: dabei wird der Puffer häufig für die Verkehrsklassen aufgeteilt und dementsprechend kleiner), ausreichend große Tabellen für die Routenspeicherung kennzeichnen die Technologie der Stunde. Speziell hier zeigt sich, dass die bisherige, doch zu stark simplifizierte Werbung mit den theoretisch erreichbaren Gigabits vorbei ist und die wirklich in einem gegebenen Szenario erreichbare Leistung zählt.

Offensichtlich wird man zunehmend betriebsblind. Erst als ich per Zufall innerhalb von 3 Tagen nacheinander mit den Konfigurations-Mechanismen von CISCO, Extreme und HP konfrontiert wurde, wurde mir wieder einmal deutlich, was uns die Hersteller hier zumuten. Offensichtlich gilt: je weniger intuitiv desto wertvoller muss der Bediener und desto toller das Produkt sein. Bei mindestens einem Anbieter stellt sich das Gefühl ein, dass er nur deshalb eine eigene Ausbildung mit Zertifizierung anbietet, weil seine Produkte grundsätzlich kaum durchschaubar sind in ihrer Konfiguration. Es bedurfte eines 2000-DM-Produkts von HP um mir wieder einmal die Augen zu öffnen. Liebe CISCOS, Extremes und wie ihr auch alle heißt: wie lange wollt ihr uns noch mit kryptischen Command-Line-Oberflächen quälen? Was ist eigentlich so schwer daran, ein intuitiv verständliches Konfigurations-Frontend zu schaffen? Was ihr macht, ist eine absolute Zumutung für den Betreiber. Klar, irgendwann, wenn sich dieser durch diesen völlig unnötigen Ballast gequält hat, wird er sich besonders als Experte fühlen, weil es ja für keinen Normalmenschen verständlich ist, was er da so eintippt.

Gleiches gilt im Management-Bereich. Die Probleme im Bereich der Fehlersuche nehmen in Switch-basierten Netzwerken mit der Einführung von Gigabit stark zu. Normale Analysatoren sind immer weniger eine Hilfe, um die durch die Switch-Systeme selbst ausgelösten Probleme zu lösen. Dabei gibt es einen sehr guten und ernstzunehmenden Lösungsansatz: SMON. Warum, so stellt sich mir die Frage, hat diesen bisher nur Avaya implementiert. Immerhin, bei Extreme ist die SMON-Implementierung angekündigt. Wann werden die anderen Hersteller folgen? Meine Empfehlung ist, dass SMON im Bereich der großen Ausschreibungen auf die Prioritätenliste kommt. Die Anbieter müssen gezwungen werden, dieses Thema ernst zu nehmen. Wer daran zweifelt, sehe sich die SMON-Lösung an und beantworte die simple Frage, wie er die dadurch gewonnene Information ohne SMON im Fall eines Fehlers zu beschaffen gedenkt. Spätestens dann wird klar, dass SMON ganz nach oben auf die Prioritätenlisten gehört.

Wie Sie sehen, der Markt der Switch-Systeme ist noch nicht am Ende. Es herrscht viel Bewegung und in einigen Bereichen muss noch weitere Bewegung hinzu kommen. Dies wird den Markt verändern. Es wird Gewinner und Verlierer geben. Im Moment scheint es so, als wenn der Anwender eher zu den Gewinnern zählen wird.

Ihr Dr. Jürgen Suppan

Impressum

Verlag:
Dr. Suppan International Institute b.v.
Ahornenlaan 12, NL-4493 DG Kamperland

Telefon (0049) 02408/955-400
Fax (0049) 02408/955-399

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung: Zweipfennig

Erscheinungsweise: Monatlich

Bezug:Kostenlos als PDF-Datei über den eMail-VIP-Service der ComConsult Akademie

Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen

Content Security – noch immer weit unterschätzt

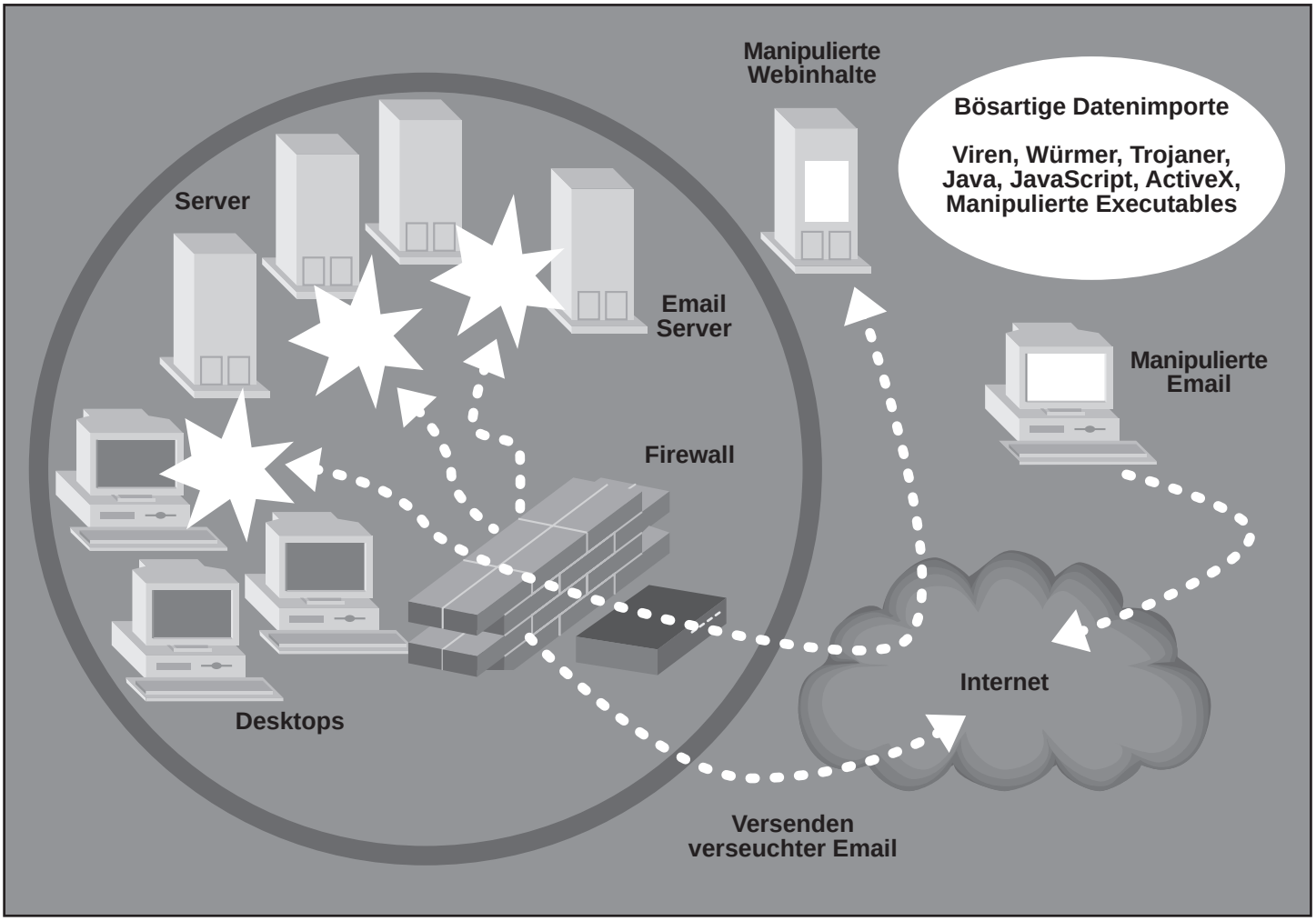
Fortsetzung von Seite 1

Je nach Intention des Erzeugers können sie alle möglichen Manipulationen auf einem Zielsystem starten: Homebanking-Transaktionen auslösen, PGP-Keys stehlen, lokale Passwörter knacken oder gezielt nach bestimmten Inhalten in Dateien suchen. Alle diese Fälle sind bereits real vorgekommen und zeigen die Grundproblematik der heutigen Sicherheitstechnologien auf. Durchaus sehr sichere Basistechniken können überwunden werden, wenn sie auf schlecht administrierten unsicheren Grundsystemen aufsetzen. Hierzu muss leider die gesamte Windows-Familie und damit 90% aller weltweit eingesetzten Endsysteme gezählt werden.

Dipl.-Inform. Detlef Weidenhammer ist als Geschäftsführer der GAI NetConsult GmbH vorwiegend auf den Gebieten Internet/Intranet-Anwendungen und Netzwerk-Sicherheit tätig. Basierend auf langjähriger praktischer Tätigkeit bringt er seine Erfahrungen als Fachberater und auch als Referent bei Seminaren und Kongressen ein.

Die unterschiedlichen Ausprägungen von Malicious Code sollen nachstehend kurz dargestellt werden. Eine erste grobe Unterscheidung ergibt sich aus dem Ladevorgang des Malicious Code. Zum Aktivieren von Viren, Würmern oder auch Trojanern müssen diese lokal gespeichert vorliegen, also zumeist durch Unachtsamkeit über Email oder Filetransfer in das interne Netz gelangt sein. Mobile Code wird bewusst im Rahmen einer erlaubten Anwendung zur Laufzeit geladen und lokal ausgeführt. Mit schädlichen Nebenwirkungen kann zumindest der unerfahrene Benutzer hier nicht rechnen.

Bild 1 Manipulierte Dateninhalte durchtunneln den Firewall-Schutz



Content Security – noch immer weit unterschätzt

Viren, Würmer und Trojaner

Viren zeichnen sich dadurch aus, dass sie andere Programme infizieren (den Code erweitern) und sich dann weiter verbreiten. Sie haben die unterschiedlichsten Auswirkungen, nicht immer bösartige, und sind wegen typischer Codemuster durch gute Virenscanner zumeist zu erkennen. Mindestens 40.000 Virenarten sind heute bekannt, die größten Probleme bereiten nach wie vor Macro-Viren, die sich z.B. in Office-Dokumenten verbergen. Durch die geschätzte Praxis des Dokumentenaustauschs auch über das Internet (per Mail oder ftp) ist damit der Verbreitung solcher Viren Tür und Tor geöffnet. Nur durch eine gute Nutzerschulung und ein mehrstufiges Virenschutzkonzept (Gateway, Server, Endsystem) lässt sich das Problem in den Griff bekommen. Wie gefährlich diese Viren sind, zeigten die Beispiele der berüchtigten Melissa- und LoveLetterVirus, die weltweit einen Schaden von geschätzt mehreren Milliarden Dollar anrichteten.

Würmer sind Viren sehr ähnlich, mit dem Unterschied, dass sie kein "Wirtsprogramm" benötigen, um sich zu verbreiten.

Trojaner sind ausführbare Programme, die als gutartig getarnt auf ein Zielsystem gelangen. Dafür gibt es vielfältige Möglichkeiten: das Laden von Programmen aus unsicherer Quelle, das Einschleusen über manipulierte zip-Dateien oder auch das Ausführen von exe-Attachments, die vorgeblich aus bekannter Quelle stammen. Zum Aktivieren muss dabei nicht mal mehr der berühmte "Doppelklick" durchgeführt werden, bei einigen Programmen (MS Outlook) reicht bereits die aktivierte Preview-Funktion.

Gelingt es dem Angreifer, auf einem der freigegebenen Wege neben den eigentlich zu übertragenden Informationen, zusätzliche Daten in das interne Netz zu transportieren, hat er die Möglichkeit, im Firmennetz vorhandene Sicherheitslücken der gängigen Betriebssysteme und Applikationen für sich auszunutzen. Dabei gehen die Gefahren weit über das bisher bei Viren gewohnte Maß hinaus. Problematisch sind nicht so sehr die Viren mit zerstörerischer Wirkung (Löschen von Systemdateien, Manipulieren von Benutzerdateien), da man deren Auftreten schnell erkennt und Gegenmaßnahmen treffen kann. Neuere Viren und vor allem Trojaner zeichnen sich häufig dadurch aus, dass sie sich maskieren und lange Zeit im Verborgenen ihr Unwesen treiben. Sie können insbesondere dazu verwendet werden, um sensible Informationen aus einem Unternehmen zu stehlen oder auch um den Endpunkt einer an sich "sicheren" VPN-Verbindung abzuhören. Bekanntlich wurde auch Microsoft unlängst Opfer eines solchen Angriffes (mittels QAZ, siehe Kasten).

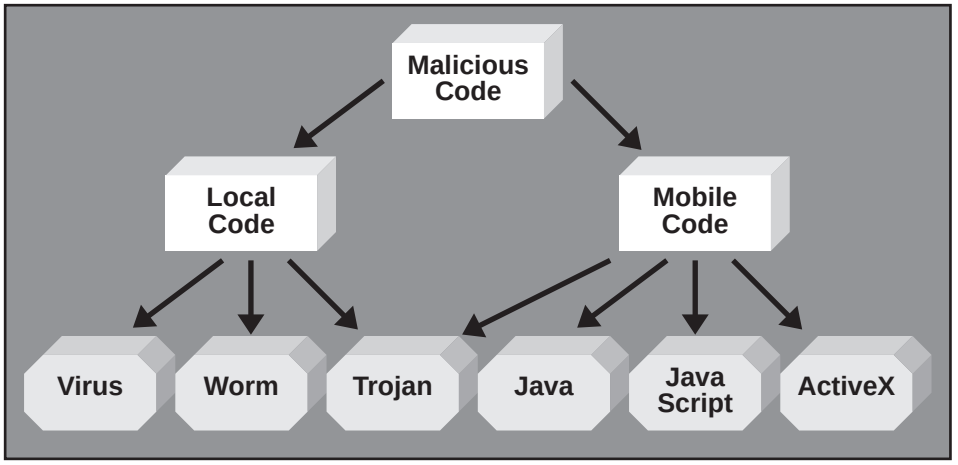


Bild 2 Ausprägungen von Malicious Code

Stehlen von PGP-Keys

Name: Caligula
Typ: Word Macro Virus
Infects: Win

Caligula ist einer der ersten Spionage-Viren, die die Aufgabe haben, Informationen zu stehlen.

Caligula stiehlt den PGP-Keyring von einem infizierten System und schickt ihn per ftp an die Zieladresse codebreakers.org.

Remote Access

Name: QAZ
Typ: Worm
Infects: Win32

QAZ ist ein Wurm mit den Eigenschaften eines Trojaners.

QAZ kopiert sich als NOTEPAD.EXE auf ein Zielsystem. Er bietet einem Angreifer dann die Möglichkeit sich von außen zu verbinden und die Kontrolle über das System zu übernehmen.

Empfehlungen zu Viren, Würmern und Trojanern

Zur Vermeidung dieser Gefahren müssen die mittels Internetzugang über die Dienste Email, Web und Dateitransfer übertragenen Daten auf bekannt schädliche Inhalte hin untersucht werden. Content-Scanner sollen anhand vorgegebener Direktiven entscheiden, wie der untersuchte Inhalt behandelt wird (Passieren, Löschen, Quarantäne). Zumindest die Kontrolle von interaktiven Diensten wie Web ist problematisch, da die Performance hierbei nicht unbeträchtlich eingeschränkt wird. Hierfür werden keine herkömmlichen Virenscanner eingesetzt. Erwähnenswerte Hersteller sind u.a.: Trend-Micro, Content Techn. und eSafe.

Zur Positionierung der Content-Scanner kommen der Netzeingang (Gateway-Version) oder das jeweilige Endsystem in Frage (Desktop-Version). Zusammen mit den (hoffentlich) immer eingesetzten Virenscannern auf Servern und Desktops entsteht eine mehrstufige Abwehrmauer, die weitgehend immun ist zumindest gegen Unachtsamkeiten der Benutzer. Bei Verwendung unterschiedlicher Scan-Engines (mindestens 2) wird durch die verbesserte Überdeckung bei der Virenerkennung eine weitere Erhöhung des Sicherheitsniveaus erreicht.

Da Content-Scanner ihre Kenntnis über Malicious Code aus ihren Scan-Engines beziehen, kommt der Aktualität dieser Informationen eine große Bedeutung zu. Tägliche Anpassungen sind unumgänglich und nur durch gesicherte, automatisierte Web-Updates zu erreichen. Glücklicherweise bieten dies die meisten Hersteller mittlerweile an.

Hilflos sind solche Content-Scanner bei noch unbekannten oder sich ständig verändernden Angriffsmustern. Handelt es sich dann noch um gezielte Attacken, z.B. um bestimmte Informationen aus einem Unternehmen zu stehlen (spying agents), zeigt sich die Anfälligkeit der heutigen Systemlandschaft. Hier helfen nur gute Schutzvorkehrungen auf den lokalen Systemen (Personal Firewalls, Integritätschecker) und der Appell an die Benutzer, keine Programme aus unsicherer Quelle zu laden.

Java

Auch wenn die Entwicklung und Verbreitung der Sprache langsamer vonstatten geht, als sich der Hersteller Sun Microsystems das vorgestellt hat, die Verwendung von Java auf den Websites von Unternehmen, sowie vor allem innerhalb ihrer lokalen Netzwerke dürfte mittlerweile insoweit die kritische Masse erreicht haben, dass die Verantwortlichen an einer Lösung der mit dem Einsatz von Java verbundenen Sicherheitsprobleme nicht mehr vorbeikommen.

Java ist eine plattformunabhängige, objektorientierte Programmiersprache. Zu unterscheiden sind Java Applets, die hauptsächlich innerhalb eines Web-Browsers ausgeführt werden, und Java Applikationen, die wie herkömmliche Programme auf einem Rechner installiert werden und im Kontext einer Java Virtual Machine (JVM) ablaufen.

- Bei der Entwicklung der Sprache wurden Sicherungskonzepte von Anfang an berücksichtigt. Byte-Code Verifier, Class Loader und Security Manager bilden die sogenannte Sandbox. Diese sorgt dafür, dass beliebige Applets ausgeführt werden können, aber mit eingeschränkten Zugriffsrechten, d.h. vor allem ohne Zugriff auf lokale Ressourcen. Erst wenn einem Java Applet explizit erlaubt wird, die Sandbox zu verlassen, erhält es weitere Zugriffsrechte.

- Ab der Java Version 2 ist es auch möglich, Zugriffskontrollisten zu definieren und somit eine noch feinere Steuerung der Rechte zu realisieren. Darüber hinaus verfügt Java über die Möglichkeit, Java Applets zu signieren. Java 2 bietet damit eine Vielfalt neuer Möglichkeiten, präzise zu steuern, welches Applet aus welcher Quelle welche Aktionen ausführen und welche Ressourcen zugreifen darf - mit dem Preis, dass mehr Möglichkeiten auch zu mehr Fehlerquellen in der Implementierung und bei der Umsetzung der Security Policy führen können.

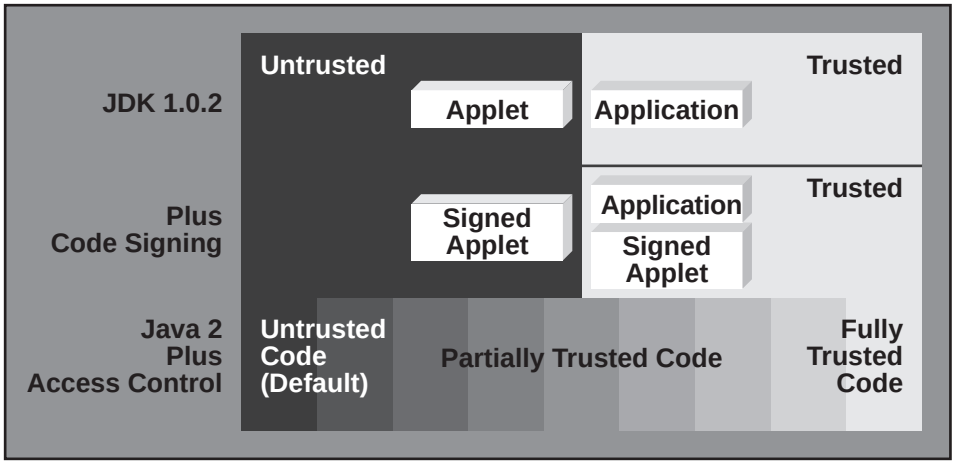


Bild 3 Wachsende Komplexität der Java Sicherheitskonfiguration

Trotz des ausgeklügelten Sicherheitsdesigns wurden in der Vergangenheit einige sicherheitsrelevante Schwachstellen von Java bekannt. Diese bezogen sich allerdings ausschließlich auf die (schlechten) Implementierungen von Browsern und Java Virtual Machines, nicht aber auf die Konzepte an sich. Einige Beispiele sollen dies aufzeigen:

- Anfang August 2000 wurde unter dem Namen Brown Orifice ein Java Applet bekannt, das sehr wohl auf lokale Ressourcen zugreifen konnte, dies auch ohne die erforderliche Erlaubnis. Brown Orifice richtet auf dem Rechner des Anwenders einen Web-Server ein, der lokale Ressourcen einsehen lässt, und ermöglicht es somit, dass andere Anwender auf lokale Ressourcen zugreifen können. Möglich wurde dies durch zwei Schwachstellen im Netscape Browser 4.74.

- Im Netscape 4.05 wurde ein Package eingeführt, das einem Applet praktisch uneingeschränkten Zugriff auf ein speziell gesichertes Verzeichnis gewährte. Dies war zwar zunächst von Netscape auch so beabsichtigt, jedoch nutzte ein Applet namens DiskHog dies aus, um die Platte des Benutzers mit nutzlosen Daten zu füllen, bis es zum System-Stillstand kam.

- Ein anderes Applet (filehole) ist in der Lage, zwar nicht auf Dateien außerhalb der Sandbox lesend zuzugreifen, aber immerhin deren Existenz zu überprüfen. Eine Möglichkeit des Missbrauchs wäre es, damit festzustellen, ob eine bestimmte Software auf dem Rechner des Benutzers installiert ist und die Ergebnisse dieser "Marktforschung" dem Anbieter der Website, von der das Applet (unwissentlich) geladen wurde, zur Verfügung zu stellen.

Diese Probleme wurden zwar meist umgehend durch Updates der Browser beseitigt, stellten aber zumindest solange eine Gefahr dar, wie nicht alle Anwender die neueste Browser-Version installiert hatten.

Empfehlungen zu Java

Mit Java ausführbaren Code aus externer Quelle zu laden stellt eine potentiell sehr große Gefahr dar. Wer also auf der ganz sicheren Seite sein will, der muß die Ausführung von Java unterbinden: entweder am Netzeingang oder auf den Desktops der Benutzer. Ersteres ist deutlich einfacher zu bewerkstelligen, da dazu genügend Produkte existieren und nur ein geringer Aufwand nötig ist.

Will man Java wegen seiner zunehmenden Bedeutung bei der Internet-Nutzung zumindest für bestimmte Benutzer freigeben, dann sollten Applets nur aus sicherer Quelle geladen werden. Dazu müssten sie über eine Digitale Signatur verfügen, wobei für den verwendeten Schlüssel ein nachprüfbares Zertifikat existieren muss. Diese Situation wird jedoch in den seltensten Fällen vorliegen, weshalb man zumeist vor der Frage steht, wie sind Applets zu kontrollieren. Hierzu wurden verschiedene Wege eingeschlagen, von denen sich allerdings nur wenige auch kommerziell halbwegs durchsetzen konnten.

Prinzipiell ist zwischen der Reaktion auf bekannt bösartiges Verhalten und dem vorbeugenden Schutz kritischer Ressourcen zu unterscheiden:

Im ersten Fall wird ein Applet, dessen Verhalten als schädlich identifiziert wurde, zum Beispiel durch seine MD5-Signatur eindeutig identifiziert. Diese Signatur wird in einer

Datenbank abgelegt und die Signatur jedes weiteren Applets, das kontrolliert werden soll, wird mit dieser Signatur verglichen. Damit ergibt sich eine Kontrolle, die der von Viren-Scannern vergleichbar ist und bei diesen deshalb auch immer häufiger anzutreffen ist.

Im zweiten Fall sind Quelle oder Wirkungsweise und somit die Bösartigkeit des Applets nicht im vorhinein bekannt. Sämtliche Zugriffe auf Ressourcen, die das Applet ausführen möchte, werden kontrolliert und ggf. unterbunden. Dadurch ist es möglich, auch die Ausführung von Applets zu verhindern, die neu auftreten und in einer Datenbank noch nicht aufgenommen werden konnten.

Auch eine noch so sorgfältige Überprüfung von Java Applets kann unterlaufen werden, wenn in den Browsern Implementierungsfehler auftreten. Als komplementäre Schutzmaßnahme ist deshalb der Einsatz von Security-Scannern unbedingt zu empfehlen. Ständig aktualisierte Security-Scanner kennen die Schwächen der Browser und weisen den Administrator darauf hin, wenn ältere Versionen von Browsern im Einsatz sind oder auch wenn neuere Versionen nicht mit den neuesten Patches installiert wurden.

JavaScript

Die Skript-Sprache JavaScript von Netscape hat mit der Programmiersprache Java von Sun Microsystems nur die ersten vier Buchstaben gemein. Im Gegensatz zu Java, das sowohl im Browser als auch auf dem Server Verwendung findet, wird JavaScript ausschließlich im Browser ausgeführt. JavaScript wird für Prüfungen von Benutzereingaben verwendet, um neue Fenster zu öffnen, weitere URLs anzusteuern oder allgemein, um Berechnungen auf Client-Seite durchzuführen. JavaScript kann - eigentlich - nicht auf das Dateisystem oder sonstige lokale Ressourcen zugreifen und keine Netzwerk-Verbindungen zu anderen Systemen aufbauen.

Genau wie bei Java ist bei JavaScript zwischen Risiken durch die Möglichkeiten der Sprache und den Fehlern bei der Implementierung zu unterscheiden.

Aufgrund der eingeschränkten Möglichkeiten sind erstere relativ begrenzt. Die Gefahr besteht vor allem in den Fähigkeiten, das vom Benutzer erwartete Browser-Verhalten zu verändern und damit die Reaktionen des Benutzers zu manipulieren. Mit JavaScript lassen sich beispielsweise Hyperlinks verschleiern oder ein gefälschtes Fenster kann zur Eingabe eines Passwortes auffordern. Damit lassen sich also am ehesten Angriffe auf die Authentizität der dargestellten Daten führen. Häufig wird allerdings auch durch den übermäßigen Verbrauch von Ressourcen die Verfügbarkeit beeinträchtigt.

Nicht minder gravierend als die Fähigkeiten, den Benutzer zu täuschen, sind aber auch die zahlreichen Implementierungsfehler im Browser. Allein der Bulgare Guninski (http://www.guninski.com) demonstriert auf seiner Website Dutzende von Sicherheitslücken. Diese umgehen dabei in vielen Fällen die Beschränkungen, die der Sprache eigentlich auferlegt sind. In diversen Varianten ist es möglich, auf beliebige lokale Dateien zuzugreifen, nicht nur auf die Konfigurationsdaten des Browsers. Durch Zugriff auf den Browser-Cache lässt sich außerdem das Surf-Verhalten des Benutzers auslesen. Zwar wurden bereits viele Probleme beseitigt, es werden aber immer wieder neue bekannt.

Empfehlungen zu JavaScript

Flexible Schutzmaßnahmen sind bei JavaScript weitaus schwieriger zu realisieren als bei Java. Gängige Schutzprodukte analysieren lediglich Java-Code, nicht aber JavaScript. So bleibt nur die Möglichkeit, JavaScript am Gateway oder am Browser pauschal zu blockieren oder zu deaktivieren. Dies wird aber in der Praxis kaum gemacht, da JavaScript noch weitaus häufiger als Java Verwendung findet und viele Webseiten ohne JavaScript kaum nutzbar wären.

ActiveX

ActiveX ist die Erweiterung der bekannten OLE-Technik und damit kein eigenständiges System, sondern integraler Teil der Microsoft Windows Plattform. Ein ActiveX-Control ist ein kleines Windows-Programm, das sich z.B. mittels eines Web-Browsers ausführen lässt. Dabei können die Controls bereits vorhanden sein, oder aber beim Aufruf einer Webseite heruntergeladen werden. ActiveX-Controls müssen nur dem COM-Standard entsprechen, können aber praktisch in beliebiger Programmiersprache geschrieben sein.

Auf Grund der engen Verflechtung mit dem Betriebssystem hat ein Control Zugriff auf alle Systemressourcen incl. der lokalen Daten und Programme. Mit der Nutzung von ActiveX ist deshalb immer ein starkes Vertrauensverhältnis verbunden, das in geeigneter Form sicherzustellen ist:

- Die digitale Signatur des Autors ist die maßgebliche Sicherheitsfunktion von ActiveX. Dabei kann der Autor unterscheiden, ob er das ActiveX Control für die Verwendung in Skripten oder zur Parameterübergabe freigibt. Darüber hinaus gibt es keine Abstufung der Zugriffsmöglichkeiten.

- ActiveX verlässt sich ausschließlich auf das menschliche Urteilsvermögen. Der Anwender vertraut dem Code, wenn er dem Hersteller des Codes vertraut. Das Programm hat dann volle Zugriffsmöglichkeiten auf den Rechner des Anwenders. Dabei ist nicht allen Herstellern von ActiveX Controls diese Verantwortung bewusst. Manche interpretieren ihre Unterschrift lediglich als "Autor von" und nicht als "verantwortlich für".

Die Quellenüberprüfung durch Digitale Signatur wird "Authenticode" genannt. Wegen des mit der Zertifizierung verbunden Aufwandes an Zeit und Kosten hat sich dieser Weg nicht durchgesetzt.

Empfehlungen zu ActiveX

Zwar ist mit der digitalen Signatur die Authentizität und Integrität der Software gewährleistet. Die Konsequenzen der Verwendung sind aber nicht absehbar. Das Laden eines ActiveX Controls ist mit der Installation von Software gleichzusetzen. Es kann daher nur dringend davon abgeraten werden, den Zugriff auf ActiveX Controls aus dem Internet oder aus anderer unsicherer Quelle zu erlauben. Viele Firewalls und natürlich auch Content-Scanner bieten hierzu die Möglichkeit bereits am Netzübergang ActiveX-Controls abzublocken.

Fazit

Die wirklichen Bedrohungen, die aus dem Einschleusen von Malicious Code in ein Unternehmen entstehen, sind bisher erst in Ansätzen erkennbar. Waren bisher schon die weltweit Schaden anrichtenden Viren und Würmer mehr als ärgerlich, so ist die Gefahr durch gezielt erzeugte "Malicious Agents" viel bedeutender. Durch ihre nahezu wahlfreie Programmierbarkeit sind sie in der Lage ihre Anwesenheit zu verschleiern, weltweite Ressourcennetze aufzubauen und praktisch jeden "Auftrag" zu erfüllen. Nur eine konsequente Security-Policy mit gut abgestimmten Schutzmaßnahmen kann das Risiko in erträglichen Grenzen halten.

Netzwerk Sicherheits-Forum 2001

Security-Event des Jahres: Netzwerk Sicherheits-Forum 2001

Vom 7. bis zum 9. Mai veranstaltet die ComConsult Akademie zusammen mit der GAI NetConsult im Maritim Königswinter das "Netzwerk Sicherheits-Forum 2001".

Geleitet und moderiert wird das Forum wie in den letzten Jahren von Dipl.-Inform. Detlef Weidenhammer, dem Geschäftsführer der GAI NetConsult.

Das diesjährige Netzwerk Sicherheits-Forum wird sich verstärkt den für die tägliche Praxis notwendigen Erfahrungsberichten und Empfehlungen zum sicheren Betrieb von IT-Umgebungen zuwenden. Wie gewohnt sollen aber auch aktuelle Themen wie z.B. PKI oder "Secure Web-Applications" den Teilnehmern technisch erläutert und in ihrer Bedeutung näher gebracht werden.

Das Forum geht auf die bestehenden Sicherheitsrisiken in modernen, heterogenen, offenen Netzwerken ein und konzentriert sich auf:

- Benennung praxisrelevanter Sicherheitsrisiken

- Methoden zur Vermeidung von Sicherheitsrisiken
- Praxiserprobte Ansätze zur Umsetzung von Sicherheitskonzepten
- Produkte und bestehende Einsatzerfahrungen.

In mehreren parallel angebotenen Workshops werden Betriebsthemen vertieft, aber auch Produktvergleiche nach festgelegtem Präsentationsmuster zusammen mit unterschiedlichen Herstellern durchgeführt.

Die überaus große Beteiligung und die positive Resonanz auf die Kongresse zum Thema Netzwerk-Sicherheit in den vergangenen Jahren zeigt, dass die Auswahl der Themenschwerpunkte das Interesse der Teilnehmer getroffen hat.

Damit ist das Netzwerk Sicherheits-Forum für jeden Sicherheitsverantwortlichen und Admininstrator von Netzwerken zu einer unverzichtbaren Plattform für aktuelle Informtionen, Produktvergleiche und Fachdiskussion geworden.

Namhafte Experten geben einen Überblick über den aktuellen Stand in wesentlichen Bereichen der Netzwerk-Sicherheit, wobei großen Wert auf Praxisnähe gelegt wird. Die Teilnehmer lernen nicht nur Bedrohungen richtig einzuschätzen, sondern erhalten auch Lösungsvorschläge und konkrete Produktempfehlungen.

Themenschwerpunkte

Content-Security
- Wie realistisch sind die Gefahren durch datenimportierende Dienste
- Von BrownOrifice bis QAZ - welche Attacken erregten Aufsehen
- Wie Email und Websurfen ihre Sicherheitsmaßnahmen durchlöchern
- Was leisten konventionelle Virenscanner und was nicht
- Wie gut sind Produkte zur Kontrolle von Java, JavaScript, ActiveX

Secure Web-Applications
- Wie kann die Kommunikation mit unsicheren Kunden-PCs gesichert werden
- SSL - Stärken und Schwächen
- Anforderungen an Clients und Server bei Nutzung von SSL
- Einsatz unterschiedlicher Verschlüsselungs- und Authentisierungstechniken
- Sichere Einbindung interner Backends

Einsatz von PKI-Lösungen
- Aufbau von Sicherheitstrukturen mit PKI
- Komponenten einer PKI
- Schlüssel- und Zertifikatsmanagement bei PKI
- Ist der Aufbau einer eigenen CA sinnvoll

Perimetersicherung
- Firewalls und andere Security-Gateways
- Load-Balancing und hohe Verfügbarkeit
- Pro-aktive Überprüfung durch Security-Scanner
- Aktive Überwachung durch IDS-Systeme
- Sicherung von Administrator-Zugängen

Secure Remote Access
- Von Telearbeitsplätzen bis zu Service-Partnern
- Vom RAS zum Secure RAS
- Vergleich von AAA-Systemen (Radius, Cisco ACS, ...)
- Schwachstelle "Remote Site"
- Auswahl und Einsatz von VPN-Lösungen

Windows 2000
- Funktion des Active Directory
- Authentisierung und Zugriffssteuerung
- Kerberos und Active Directory
- Verwendung von PKI in Windows 2000
- Erfahrungen in Test und Einsatz

Security Management Lösungen
- Lässt sich heute ein umfassendes Security-Management realisieren
- Welche tragfähigen Standards gibt es im Security-Bereich
- Was bieten Enterprise-Management Systeme im Security-Bereich

Betriebsaspekte
- Aufbau von Security-Policy und Sicherheitskonzept
- Betriebskonzepte und -unterstützung
- Erfahrungen mit Outsourcing (Security Provider)
- Datenschutz und Datensicherheit

Anzeige

10 % Vorbuchungs-Rabatt bis zum 28.02.01

Netzwerk Sicherheits-Forum 2001

07.05. - 09.05.01 in Königswinter

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am eMail-VIP-Verteiler bieten wir in diesem Jahr exklusiv eine Vorbuchungsphase für das Netzwerk Sicherheits-Forum 2001 bis zum 28.02.2001 zum Sonderpreis an.

Sie zahlen statt EUR 1.590,-- (regulärer Preis) nur EUR 1.430,-- zzgl. MwSt. und sichern sich damit frühzeitig Ihren Teilnahmeplatz. Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden.

GAI NetConsult

ComConsult Akademie

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk Sicherheits-Forum 2001

☐ Ja, ich möchte den Vorbuchungs-Rabatt nutzen und melde mich verbindlich an zum **Netzwerk Sicherheits-Forum 2001** vom 07.05.-09.05.01 in Königswinter zum Preis von EUR 1.430,-- zzgl. MwSt. (statt regulär EUR 1.590,--)

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Hotel, Königswinter (Übernachtung/Frühstück DM 211,--)

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Sonder-Seminar

Optische Netze

Vom 19. bis zum 21. März veranstaltet die ComConsult Akademie im Hotel Mondial am Dom in Köln ein Sonder-Seminar zum Thema "Optische Netze". Der Referent ist Dr. Franz-Joachim Kauffels, seit mehr als 15 Jahren einer der führenden deutschen Netzwerk-Experten.

Optische Netze sind der nächste, wesentliche Evolutionsschritt der Netzwerktechnik. Das Potential der Optischen Netze kann man nicht einschätzen, wenn man ihre Wirkungsweise nicht versteht und den technischen Fortschritt durch die Integration Optischer Komponenten nicht einordnen kann. Optische Sender und Empfänger, Switches und Speicher, die früher als Einzelteil einen 19 Zoll Schrank gefüllt haben, passen heute auf einen Quadratzentimeter. Das ist die eigentliche Revolution, die uns die Anwendung dieser faszinierenden Technik ab heute zu unvorstellbar geringen vergleichbaren Kosten ermöglicht.

Vielfach stellt man sich jedoch vor, dass diese Systeme an der technologischen Spitze ausschließlich im Wide Area Bereich benutzt werden. Das ist unrichtig.

Wegen der enormen Anforderungen, die in den nächsten Jahren an Netze gestellt werden und dem gleichzeitigen Kostenverfall der entsprechenden Komponenten rücken die optischen Netze bis in die Unternehmensnetze vor.

Anwendungsorientierte Grunddienste wie UMTS, Multimedia und Internet ermöglichen ganz neue Geschäftsmodelle im E-Business. UMTS bedeutet aber bei z.B. 10.000 Teilnehmern eine Datenrate von 20 Gbps zzgl. Erheblichem Overhead. Diese Datenrate will und muß Serverfarmen erreichen, diese werden aber nur ausfallsicher und zuverlässig arbeiten können, wenn sie mit SAN-Konzepten im Bereich mehrerer Dutzend Gigabit/s versorgt werden.

Die Basis aller optischen Netze ist die Übertragung auf Glasfasern. Neue verbesserte Glasfasertypen verschiedener Hersteller ermöglichen eine wesentlich größere Reichweite oder die Verwendung günstiger Sende/Empfangskomponenten bei kürzeren Reichweiten. Strahlungssender werden immer kleiner und billiger, allen voran steht die Entwicklung der integrierten VCSELs. Ein Kanal von 10 Gbps ist Standard und entsprechende Übertragungssysteme werden von vielen Herstellen angeboten. Noch in diesem Jahr werden aber sehr viele auch 40 Gbps Kanäle anbieten. Diese Kanäle können einzeln gebündelt werden oder mittels der DWDM-Technik gemultiplext. Ein DWDM-System hat dann 20, 40 oder noch mehr Kanäle, jeder mit 2,5, 10 oder 40 Gbps. So kommen letztlich aggregate Gesamtübertragungsraten im Terabit-Bereich zusammen. Neue Entwicklungen versprechen 160 oder 1000 Kanäle auf einer einzigen Glasfaser.

Um diese nun nutzen zu können, bedarf es optischer Switches und entsprechender Add/Drop-Multiplexer, die das ein- und ausrangieren von Wellenlängen ermöglichen.

Viele Hersteller arbeiten heute noch vorwiegend auf dem WAN-Bereich, aber mit 10 Gigabit Ethernet etabliert sich ein mächtiger Standard für die Integration bisheriger Systeme in die neue Welt der optischen Netze. 10 GbE ist technologisch mittlerweile eher schon ein "alter Hut", aber die Standardisierung konvergiert. Noch im November wurden keine technischen Vorschläge mehr angenommen, der Standard wird Mitte 2001 fertig. Dann gibt es keine Entschuldigung für Sonderlocken oder lahme Netze mehr.

Verschiedene Hersteller, unter ihnen besonders Extreme Networks oder Nortel Networks arbeiten an der vordersten Front der Integration. Es gibt jetzt schon Hochleistungsswitches mit integrierbaren WDM-Modulen, die letztlich genauso einfach zu benutzen sind, wie andere Einschubmodule zuvor.

Was momentan bleibt, ist das Problem der Kontrolle der gemischten optisch/elektrischen Netze. Allerdings ist die Tendenz zu sehen, auf jeden Firlefanz wie Priorisierung oder Multiprotokollstacks zu verzichten und statt dessen zu klaren Strukturen extrem hoher Leistung zu finden. Themen wie Delay oder Varianzen kann man in diesem Zusammenhang zunächst getrost abhaken.

Angesichts der zunehmenden Bedrohungen traditioneller aber auch moderner LANs stellt sich nun die Frage, wann und wie die optische Technik in die Unternehmensnetze vordringt. Ein größeres Unternehmen wird über kurz oder lang in Access-Bereich seine "eigenen Wellenlängen" für die Hochleistungskommunikation bekommen, einfach, um die gewaltigen Datenmengen, die E-Business der nächsten Generation oder UMTS mit sich bringen, verarbeiten zu können. Wie geht es aber dann weiter? Direkt mit einem lokalen optischen Switch in einen lokalen optischen Backbone oder doch noch mit metallischen Leitern. Man muss sich immer überlegen, dass bei 1 Gbps mit den Drähten endgültig Schluss ist.

Sicherlich werden die meisten Kunden in 2001 hier noch keine allzu großen Schritte machen, aber angesichts der dramatischen Geschwindigkeit dieser Entwicklungen sollte man sich schon recht frühzeitig über die Möglichkeiten und Funktionsweise der Optischen Netze informieren.

Sonder-Seminar

Optische Netze – Inhaltlicher Aufbau

Optische Netze – Motivation und Leidensdruck
- Allgemeine Trends
- Internet Economy Indicators
- Anforderungen aus dem E-Business
- VoIP-Integration
- UMTS-Bedrohung

Optische Netze – Grundüberlegungen
- Struktur heutiger Carrier Backbones
- Struktur bereinigter Carrier-Backbones
- Layer-Konvergenz
- Zauberwort: Spektralpartitionierung
- WDM, CWDM, DWDM
- Schichtenmodell Optischer Netze
- Anwendungsbereiche WAN, Access, MAN, LAN, SAN

Optische Netze – Basiskomponenten
- Optische Datenübertragung
- Glasfasertypen
- Beeinträchtigungen der optischen Übertragung
- PMD, DGD, Raman-Streuung, nichtlineare Effekte
- Neue Fasern
- Höchstleistung auf Multimode-Fasern
- Strahlungsquellen, VCSELs
- Strahlungsempfänger
- Systemeigenschaften moderner Kombinationen
- Optische Verstärker
- Modulatoren

Optische Netze – Bausteine
- Grundaufbau eines ON
- WDM- Multiplexer und Demultiplexer
- Add-Drop-Multiplexer
- Fiber-Bragg Gitter
- Integation optischer Komponenten
- Universalwaffe PHASAR
- Multiwellenlängen-Sender
- Multiwellenlängen-Empfänger
- Integrierte Optische Speicher
- Optische Switches mit Microspiegeln
- Optische Speicher mit Bubble-Technologie

Optische Wide Area und Carrier-Netze
- Leistungsbeispiele Optischer Netze und Rekorde
- Signalspektrum für größere Entfernungen
- Stand der optischen WAN-Technik
- SONET/SDH
- Alternative IP über WDM oder OP-XC

Access/MAN/LAN/SAN-Standard: 10 Gigabit Ethernet
- Einsatzbereiche
- Ziele und Rahmenbedingungen der Standardisierung
- PHY-Alternativen
- Übertragungssysteme
- Struktur des Standards
- 10 GBASE LX 1550
- 10 GBASE LX -4 1310
- 10 GBASE SX-4 850 CWDM
- Koexistenz von 10 GbE und SONET 192C
- Generelle Schnittstellen und Module
- Entwicklungsstand/Prototypen
- Stand der Standardisierung November Meeting

Gemischte Themen
- Optische Kernnetze
- Kreation intelligenter Optischer Netze
- Herausforderungen an Netzwerk-Infrastrukturen
- Praktische Einsatzbereiche intelligenter ON
- Problembereiche und Vergleich
- Optische IP-Terabit Router

Integration von Legacy-Systemen und Optischen Netzen
- Optische Netze vom SAN zum Access Bereich
- Neue Anwendungen
- Schnittstellenprobleme mit Legacy Networks
- Multiprotocol Lambda Switching
- Praktisches Lösungsbeispiel in der Großanwendung

Ethernet Everywhere
- Die Ethernet Everywhere-Strategie, z.B. von Extreme Networks
- Die "Two-Pack"-Strategie
- Entwicklungen auf 1 und 10 Gbps
- Ethernet vom SAN zum Access-Bereich
- Integration von Legacy Systemen
- Gigabit Ethernet MAN

Entwicklungen im Access Bereich
- Serviceanforderungen besonders für Leased Lines
- Technologieentwicklung
- Entwicklung der Angebote der Deutschen Telekom
- Neue Entwicklungen im Netzwerk-Management
- Die Control Plane für dynamisch konfigurierbare Optische Netze

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Optische Netze

☐ Ich melde mich an für das Sonder-Seminar **Optische Netze** vom 19.03.-21.03.01 in Köln zum Preis von EUR 1.590,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **akademie@comconsult.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name _____ Vorname _____

Firma, Abteilung _____ Position, Funktion _____

Straße _____ PLZ, Ort _____

Telefon _____ Fax _____

eMail _____ Unterschrift _____

"Wozu brauche ich ein Zertifikat?" – Verschlüsselung und Signaturen im E-Business/E-Commerce

Fortsetzung von Seite 1

1 Einleitung

Die Ausweitung des E-Business auf immer breitere Geschäftsfelder birgt nicht nur Chancen, sondern auch Risiken, die durch Begriffe wie "Systemabstürze", "Hacker", "Computer-Viren" oder "elektronische Wirtschaftsspionage" beispielhaft umrissen werden können. Ohne angemessene IT-Sicherheitsmaßnahmen drohen sämtlichen Akteuren im Internet nicht kalkulierbare Risiken. E-Business ist daher nur in einem "vernünftig" abgesicherten IT-Umfeld sinnvoll und verantwortbar.

Die Sicherheit des E-Business/E-Commerce kann immer nur im Zusammenspiel aller Beteiligten entstehen. Einen "universellen Sicherheits-Server" mit "Sorglos-Garantie" wird es auf absehbare Zeit nicht geben. Alle Akteure des E-Business - also Unternehmen und insbesondere auch Privatkunden – müssen sich ihrer Verantwortung für ihre eigene Sicherheit stellen und im Rahmen ihrer Möglichkeiten und ihres individuellen Schutzbedarfs eine "Sicherheitsstrategie" entwickeln. Es wird in Zukunft immer mehr zum Alltag gehören, Fragen wie die eingangs gestellte beantworten zu müssen.

In diesem Artikel soll versucht werden, Hinweise für die Schaffung eines angemessenen Sicherheitsniveaus im E-Business zu geben. Der Schwerpunkt liegt dabei auf den Schlüsseltechnologien Verschlüsselung und digitale/elektronische Signatur.

2 Sicherer IT-Einsatz durch IT-Grundschutz

Bevor sich Unternehmen und Kunden mit E-Business- bzw. E-Commerce-Anwendungen ins Internet begeben, sollte das erste Augenmerk auf der Schaffung eines angemessenen Sicherheitsniveaus für die eigenen Systeme liegen. Beide Seiten brauchen dazu eine jeweils auf ihre Bedürfnisse abgestimmte Sicherheitsstrategie. Für ein Unternehmen bedeutet dies die Etablierung eines IT-Sicherheitsprozesses inklusive der Erstellung eines detaillierten und umfassenden IT-Sicherheitskonzepts. Die Strategie des Kunden hingegen muss es sein, durch punktuelle Sicherungsmaßnahmen an seinen vorhandenen Systemen zu versuchen, seinem Sicherheitsbedarf gerecht zu werden. In beiden Fällen sollten die Maßnahmen flexibel, effizient und wirtschaftlich sein.

Dr. Christian Mrugalla ist seit 1998 Referent im Bundesamt für Sicherheit in der Informationstechnik (BSI) im Referat Sicherheitsanalyse und Beratungsdienst. Er hat u.a. mitgewirkt bei der Erweiterung und Überarbeitung des IT-Grundschutzhandbuchs.

Dieser Artikel gibt ausschließlich die persönliche Meinung des Autors wieder. Die Aussagen sind nicht notwendig mit Stellungnahmen oder Empfehlungen des BSI identisch.

Angesichts der Vielzahl der komplexen Bedrohungen, die sich insbesondere beim Agieren im Internet ergeben, ist die Schaffung eines sicheren IT-Umfelds ein komplexer Prozess, der umfassende Fachkenntnisse in vielen Bereichen erfordert. Die Konzepte und Maßnahmen müssen zudem laufend auf neue technische Gegebenheiten sowie neue Risiken und Abwehrmöglichkeiten hin angepasst werden. Das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI) erleichtert sowohl Unternehmen als auch Kunden diese Aufgabe durch konkrete Empfehlungen von Standard-Sicherheitsmaßnahmen. Diese Maßnahmen sind in der Praxis erprobt und können pauschal als wirtschaftlich angemessen gelten. In Bereichen mit erhöhten Sicherheitsanforderungen oder individuellen Besonderheiten kann auf dem erreichten Niveau mit zusätzlichen Maßnahmen aufgebaut werden. Investitionsschutz ist damit gewährleistet. Das Grundschutzhandbuch bietet detaillierte Vorschläge für die Umsetzung von Sicherheitsmaßnahmen zu zahlreichen IT-Systemen nebst Informationen zu den jeweils relevanten Gefährdungen.

Die Erstellung des Sicherheitskonzepts nach IT-Grundschutz erfolgt nach einem Phasenplan, in dem zunächst die grundlegenden Gegebenheiten (vorhandene Systeme mitsamt deren Schutzbedarf) erfasst und anschließend die notwendigen Maßnahmen identifiziert und systematisch umgesetzt werden. Die eigentliche Grundschutzanalyse besteht aus einem Soll-Ist-Vergleich der vorgeschlagenen Maßnahmen mit der tatsächlichen Situation. Auf diese Weise werden Schwachstellen und notwendige Gegenmaßnahmen identifiziert.

Erfahrungen aus der Praxis zeigen, dass die Maßnahmen des IT-Grundschutzhandbuchs bei etwa 90% der untersuchten Systeme ausreichen und eine aufwändige, individuelle Sicherheitsanalyse somit entbehrlich ist. Das IT-Grundschutzhandbuch trägt auf diese Weise auch zur Wirtschaftlichkeit von IT-Sicherheit bei.

Das IT-Grundschutzhandbuch wird zweimal jährlich aktualisiert und erweitert. Es kann als dreibändige Loseblattsammlung über den Bundesanzeiger-Verlag bezogen werden.

Beim BSI kann außerdem gegen Rückporto eine kostenlose CD-ROM mit dem kompletten Inhalt des Handbuchs auf deutsch und englisch sowie ergänzenden Hilfsmitteln bestellt werden.

Eine Volltextversion des Handbuchs findet sich auf den Web-Seiten des BSI unter http://www.bsi.bund.de/gshb/_start.htm

Dort sind auch weitere Informationen zum Handbuch und seiner Fortentwicklung zu finden.

Durch den modularen Aufbau des Handbuchs können sowohl Unternehmen als auch Privatanwender gezielt die sie betreffenden Informationen und Sicherheitsmaßnahmen bestimmen. Mit Hilfe des IT-Grundschutzhandbuchs ist sowohl die Erstellung komplexer Sicherheitskonzepte als auch die Absicherung einfacher IT-Systeme möglich.

In letzter Zeit haben sich im Umfeld des E-Commerce/E-Business zahlreiche Initiativen zur Einführung von Gütesiegeln auch und gerade mit Bezug zur IT-Sicherheit etabliert. Aus Sicht des Verbrauchers ist es im Sinne der Vergleichbarkeit der Angebote sicherlich erfreulich, wenn Anbieter ihre Verantwortung zur Information über das bei ihnen vorhandene Sicherheitsniveau ernst nehmen.

Allerdings führt gerade die Vielfalt der angebotenen Gütesiegel, die manchmal nicht sonderlich transparente Informationspolitik über die Inhalte des Gütesiegels und die in Einzelfällen fragwürdige Sinnhaftigkeit der Zusicherungen zu neuer Verunsicherung. Das BSI hat sich vor diesem Hintergrund dazu entschlossen, ein IT-Grundschutzzertifikat einzuführen. Hierbei soll - über verschiedene zeitlich begrenzte Zwischenstufen - durch unabhängige Prüfungen festgestellt werden, ob ein vorab genau definierter Satz von Sicherheitsmaßnahmen des IT-Grundschutzhandbuchs umgesetzt worden ist. Mit der Ausgabe der ersten Gütesiegel ist im Laufe des Jahres 2001 zu rechnen.

3
Kryptographische Verfahren

3.1
Vertraulichkeit durch Verschlüsselungsverfahren

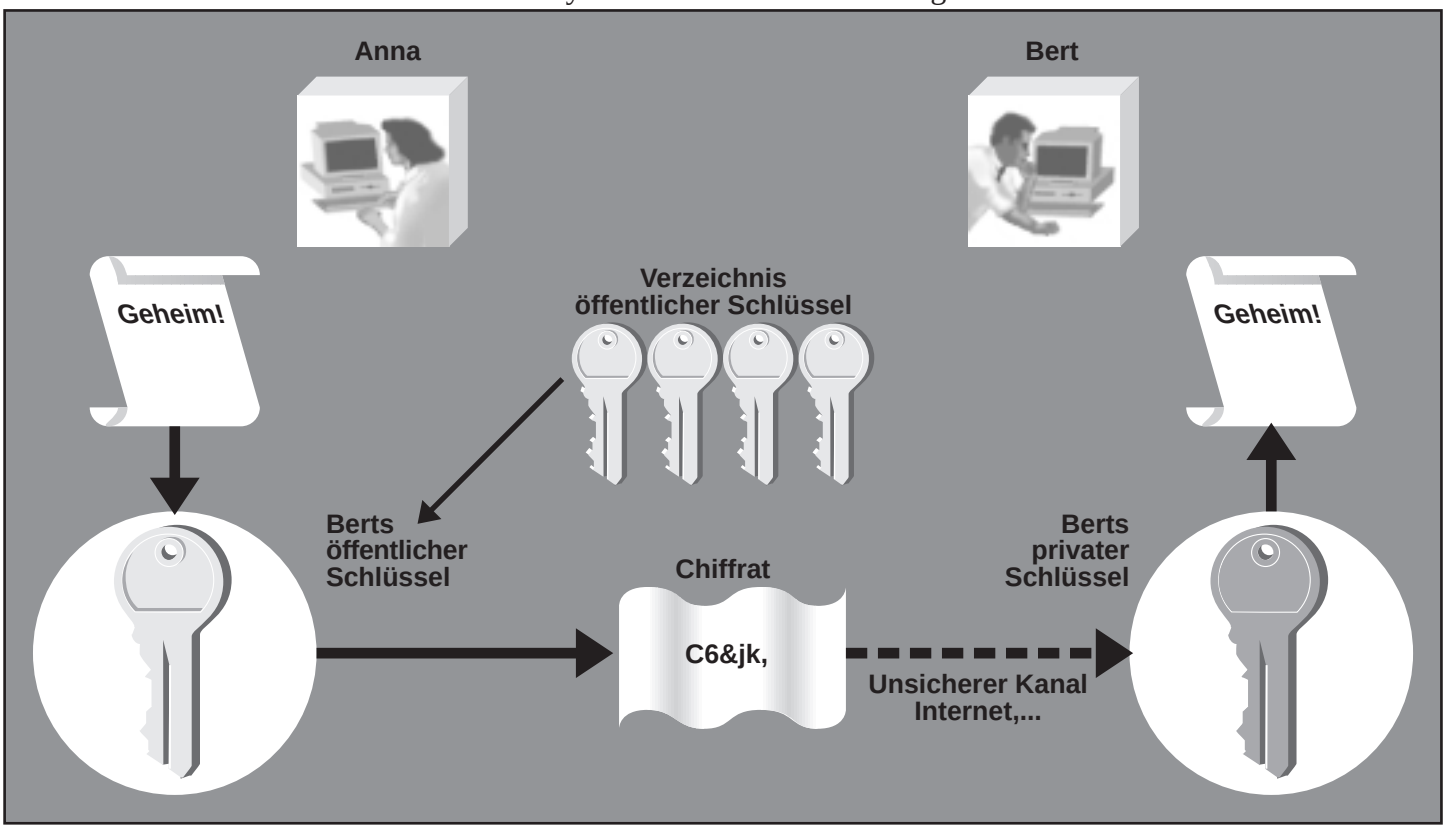
Eine wesentliche Voraussetzung für die Akzeptanz des elektronischen Geschäftsverkehrs ist die Vertraulichkeit der verarbeiten Daten. Hieran haben sowohl Anbieter (Wirtschaftsspionage) als auch Kunden (Bedrohung der Privatsphäre) ein berechtigtes Interesse. Offene Systeme wie das Internet bieten von sich aus keinerlei Absicherung für die Vertraulichkeit sensitiver Daten. Eine E-Mail etwa ist vergleichbar mit einer für jedermann lesbaren Postkarte. Da der genaue Weg einer elektronischen Nachricht vom Absender zum Empfänger vorab völlig unbestimmt ist, ist nicht vorhersehbar, welche unbefugten Personen sich Einblick in sensitive Informationen verschaffen können. Der Einsatz von Verschlüsselungsverfahren ist daher eine notwendige Voraussetzung für ein verlässliches E-Business.

Allgemein betrachtet bestehen Verschlüsselungsverfahren aus zwei Komponenten. Der Kryptoalgorithmus verwandelt den (vertraulichen) Klartext in ein unlesbares "Chiffrat" und wandelt dieses beim Empfänger wieder in den Klartext zurück. Die Entschlüsselungsoperation darf nur vom berechtigten Empfänger durchgeführt werden. Da es sehr schwer ist, einen geeigneten Kryptoalgorithmus zu entwickeln und geheim zu halten, verwendet man in der Praxis Verschlüsselungsprogramme, bei denen man zusätzlich zum Klartext (bzw. zum Chiffrat) einen weiteren Parameter, den sog. Schlüssel, eingibt. Durch Geheimhaltung dieses Schlüssels wird verhindert, dass ein Angreifer ein Chiffrat entschlüsselt, selbst wenn er den Kryptoalgorithmus kennt.

Die klassische Methode der Kryptographie ist die symmetrische. Hierbei verwenden Absender und Empfänger den gleichen - von beiden geheimzuhaltenden - Schlüssel. Moderne symmetrische Verschlüsselungsverfahren ermöglichen eine beliebig hohe Sicherheit und erlauben es, auch längere Texte in sehr kurzer Zeit zu ver- und entschlüsseln.

Problematisch bei symmetrischen Verfahren ist die Tatsache, dass zunächst ein geheimer Schlüssel zwischen Absender und Empfänger - und nur zwischen diesen (!) - ausgetauscht werden muss. Voraussetzung für die vertrauliche Kommunikation ist also eine vertrauliche Kommunikation! Aus diesem Dilemma kann man sich mit Hilfe der asymmetrischen Kryptografie befreien. Hier erzeugt der Empfänger ein Schlüsselpaar. Einen dieser Schlüssel ("privater Schlüssel") behält er für sich, den anderen ("öffentlicher Schlüssel") gibt er öffentlich bekannt. Es gibt hier also kein gemeinsames Geheimnis zwischen Absender und Empfänger. Der prinzipielle Ablauf der Übersendung einer vertraulichen Nachricht von "Anna" zu "Bert" ist in Bild 1 wiedergegeben.

Bild 1 Asymmetrische Verschlüsselung



"Wozu brauche ich ein Zertifikat?" – Verschlüsselung und Signaturen im E-Business/E-Commerce

Voraussetzung für eine sichere Anwendung der asymmetrischen Kryptographie ist, dass die Entschlüsselung nur mit dem privaten Schlüssel möglich ist und dass dieser absolut geheimgehalten wird. Die (eindeutige) Zuordnung von öffentlichem zu privatem Schlüssel bedingt, dass diese nicht unabhängig voneinander gewählt werden können. Vielmehr besteht zwischen diesen Schlüsseln – die letztlich Zahlen sind – ein mathematischer Zusammenhang. Bei der Erzeugung eines Schlüsselpaars geht man in aller Regel so vor, dass zunächst der private Schlüssel als "Zufallszahl" erzeugt wird und daraus dann der öffentliche Schlüssel berechnet wird. Diese Operation sollte also ohne allzu großen Aufwand ausführbar sein. Die umgekehrte Operation - die Berechnung des privaten Schlüssels aus dem öffentlichen - sollte hingegen praktisch unmöglich, d.h. in "überschaubaren" Zeiträumen mit "realistischem Rechenaufwand" nicht durchführbar sein. Gelänge einem Angreifer eine solche Berechnung könnte er jede asymmetrisch verschlüsselte Nachricht mitlesen. Es ist diese "Einwegeigenschaft" der asymmetrischen Kryptographie, die dazu geführt hat, dass erst seit der Einführung "leistungsfähiger" elektronischer Rechner – also etwa seit Mitte der 70er Jahre – brauchbare Verfahren existieren.

Ein Beispiel für ein solches Einwegverfahren ist die Primfaktorzerlegung großer Zahlen. So ist es relativ einfach, nachzurechnen, dass etwa

4353 x 3217 = 13.681.901

gilt. Die umgekehrte Zerlegung ist jedoch wesentlich schwieriger. (Sollte der Leser Zweifel an dieser Aussage haben, so möge er "schnell einmal" die Primfaktorzerlegung von 42.854.447 bestimmen...). Beim Verfahren RSA-1024, das derzeit als von den meisten Experten als hinreichend sicher angesehen wird, verwendet man ca. 150-stellige(!) Primzahlen. Auf modernen Rechnern dauert das Berechnen des Produkts dieser Zahlen einige Sekunden (immerhin schon eine spürbare Zeitdauer); während das Auffinden der Primfaktoren aus dem Ergebnis mehrere Jahrhunderte (auf dem gleichen Rechner) in Anspruch nehmen würde. Die Länge der bei asymmetrischen Verfahren benötigten Schlüssel führt allerdings auch dazu, dass diese Verfahren nur einen geringen Datendurchsatz aufweisen. Eine rein asymmetrische Verschlüsselung längerer Texte ist daher nicht praxistauglich.

Eine grundsätzliche Angriffsmöglichkeit bei asymmetrischen Verfahren besteht darin, dass sich ein Fälscher ("Fritz") ein eigenes Schlüsselpaar erzeugen und versuchen kann, gegenüber "Anna" seinen öffentlichen Schlüssel als denjenigen von "Bert" auszugeben. Gelingt dieser Angriff, kann anstelle von "Bert" nur noch "Fritz" die für "Bert" bestimmte vertrauliche Information lesen. Die Bindung eines (öffentlichen) Schlüssels an eine Person muss also von einer vertauenswürdigen Stelle (Trustcenter, Zertifizierungsstelle) in einem sog. Zertifikat so dokumentiert werden, dass sie nachprüfbar und authentisch, d.h. nicht unbemerkt fälschbar, ist. Dieser Punkt wird im Abschnitt über digitale Signaturen wieder aufgegriffen.

Die Vorteile beider Kryptoverfahren werden in sogenannten hybriden Verfahren kombiniert. Durch ein asymmetrisches Verfahren abgesichert wird zunächst ein Sitzungsschlüssel (= relativ kleine Datenmenge) ausgetauscht, der dann zur symmetrischen (=schnellen) Verschlüsselung der eigentlichen Kommunikation verwendet wird. Auf diese Weise erhält nur der Empfänger die Möglichkeit, die Information wieder zu entschlüsseln. Dieses Prinzip wird heutzutage in praktisch allen gängigen Systemen zur Absicherung von E-Mail- oder Web-Verbindungen eingesetzt.

3.2 Verbindlichkeit durch digitale Signaturen

Elektronische Dokumente unterscheiden sich von Papierdokumenten unter anderem dadurch, dass es möglich ist, sie zu verändern, ohne dabei Spuren zu hinterlassen (fehlende Integrität). In offenen Netzen wie dem Internet ist es zudem unmöglich, den Erzeuger und/oder Absender eines Dokuments zweifelsfrei zu ermitteln; die Absenderangabe in den gängigen E-Mail-Programmen etwa ist leicht zu manipulieren (fehlende Authentizität).

Digitale Signaturen ermöglichen es, durch die Anwendung von asymmetrischen kryptografischen Techniken elektronische Dokumente einer Person zuzuordnen und unbemerkte Fälschungen zu verhindern. Die (beweissichere) Abgabe von verbindlichen elektronischen Erklärungen jeglicher Art - eine unabdingbare Voraussetzung für verlässliches E-Business - wird erst durch diese Technologie überhaupt möglich.

Grundidee der digitalen Signatur ist eine Umkehrung der asymmetrischen Verschlüsselung. Der Absender "verschlüsselt" das elektronische Dokument mit seinem privaten Schlüssel; der Empfänger "entschlüsselt" mit dem öffentlichen Schlüssel des Absenders. Nur der Besitzer des privaten Schlüssels kann somit gezielte (unbemerkte) Änderungen des Dokuments vornehmen; Integrität und Authentizität (sofern dieser Besitzer zweifelsfrei identifiziert werden kann) sind damit gewährleistet. Wegen des geringen Datendurchsatzes (sicherer) asymmetrischer Algorithmen ist diese einfache Vorgehensweise aber nicht praktikabel.

Die existierenden Signaturprodukte umgehen diese Schwierigkeit, indem der zu signierende Text zunächst durch einen sog. Hash-Algorithmus extrem komprimiert wird. Der Algorithmus RIPEMD 160 beispielsweise komprimiert beliebige Datensätze auf eine Datei der Länge 160 Bit. In aller Regel lässt sich aus diesem "Hashwert" der ursprüngliche Datensatz nicht mehr rekonstruieren (Einwegeigenschaft). Eine – speziell für Signaturanwendungen – wesentliche Eigenschaft von Hash-Algorithmen ist die sog. Kollisionsfreiheit, die besagt, dass es nicht möglich sein darf, zwei unterschiedliche "sinnvolle" Texte mit dem gleichen Hashwert zu finden. Ein kollisionsfreier Hash-Algorithmus erzeugt eine "kleine" Datei, die den "großen" Ausgangstext in der gleichen Weise repräsentiert, wie ein "kleiner" Fingerabdruck einen "großen" Menschen erkennbar macht. Hashwerte von elektronischen Texten werden daher auch als digitaler Fingerabdruck bezeichnet. Bei der Signaturerstellung wird zunächst der Hashwert des zu signierenden Textes gebildet und dieser "Fingerabdruck" dann mit dem privaten Schlüssel des Absenders "verschlüsselt". Es entsteht die für jeden Text und jeden privaten Signaturschlüssel einzigartige Signatur. Anschließend werden sowohl der Ausgangstext als auch die Signatur an den Empfänger übersendet. Dieser unterzieht nun den Ausgangstext ebenfalls dem – allgemein bekannten – Hash-Algorithmus und "entschlüsselt" anschließend die Signatur mit dem öffentlichen Schlüssel des Absenders. Die Signaturprüfung besteht nun im Vergleich der beiden so erhaltenen Hashwerte. Stimmen diese überein, so sind Integrität und Authentizität – wie eingangs erläutert – gewährleistet.[1] Der schematische Ablauf der Signaturerstellung/-prüfung ist in Bild 2 dargestellt.

[1] An dieser Stelle ist die Kollisionsfreiheit des Hash-Algorithmus entscheidend, da ansonsten die Möglichkeit bestünde, bei der Signaturprüfung unbemerkt einen "kollidierenden." Text unterzuschieben und so die Willenserklärung des Absenders zu verfälschen.

"Wozu brauche ich ein Zertifikat?" – Verschlüsselung und Signaturen im E-Business/E-Commerce

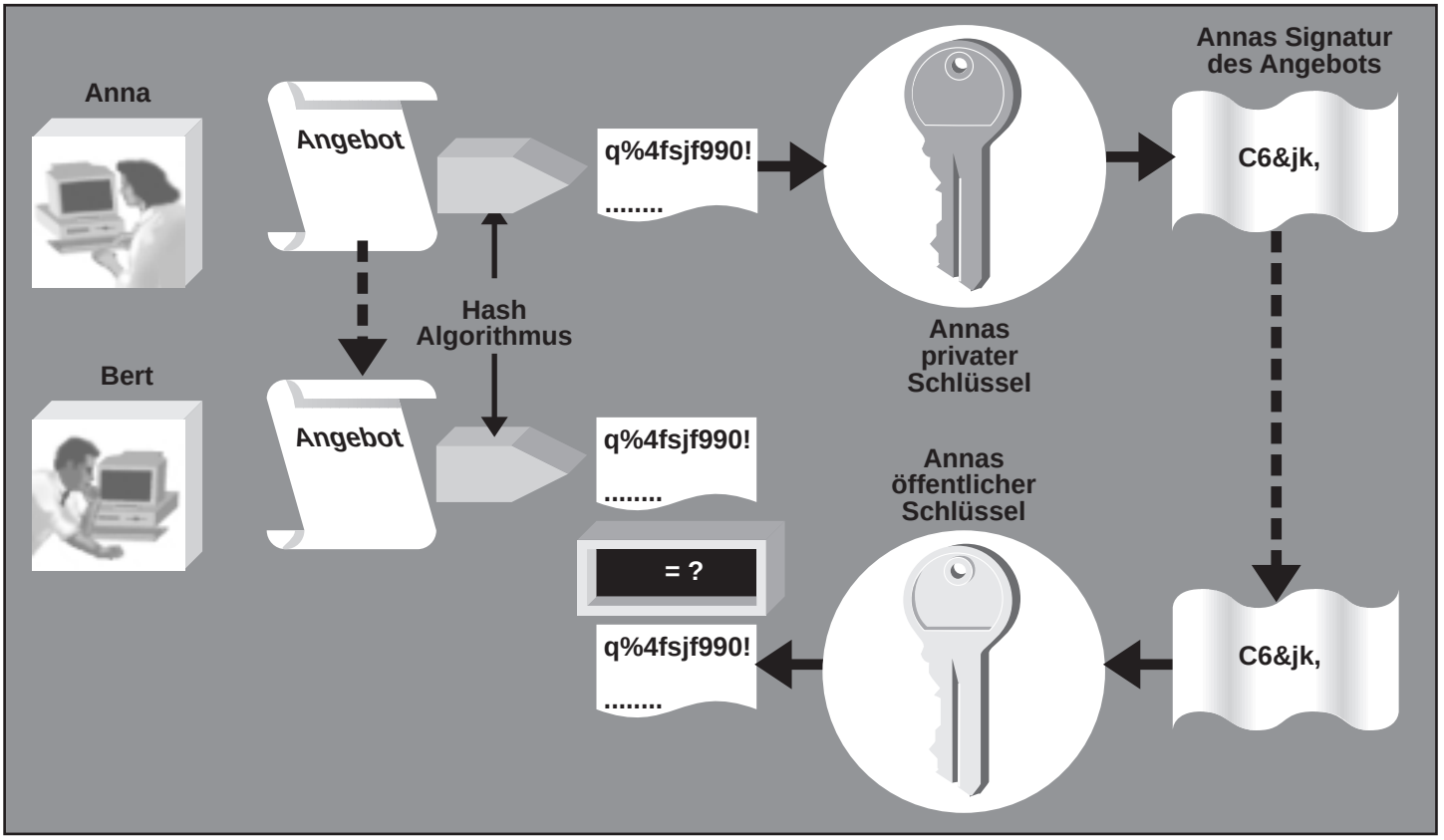


Bild 2 Signaturbildung/-prüfung

Während es bei Verschlüsselungsverfahren durchaus notwendig sein kann, den privaten Schlüssel an einer geeigneten Stelle zu hinterlegen (etwa um eine Vertretungsregelung zu ermöglichen), muss der private Signaturschlüssel absolut geheimgehalten werden und das Anfertigen einer Kopie (auch durch den rechtmäßigen Besitzer) möglichst verhindert werden. Nur unter diesen Voraussetzungen kann der Schlüsselinhaber eine einmal geleistete Signatur nicht nachträglich abstreiten.

Neben der Sicherheit der Algorithmen hängt der "Wert" einer digitalen Signatur wesentlich von der korrekten und verlässlichen Zuordnung des öffentlichen Signaturprüfschlüssels zum Besitzer des zugehörigen privaten Schlüssels ab. Schließlich möchte man das signierte Dokument ja als Willenserklärung einer Person und nicht eines Schlüssels identifizieren. Die Bedeutung von Zertifikaten ist bei Signaturanwendungen daher mindestens ebenso groß wie bei der asymmetrischen Verschlüsselung.

4 Public-Key-Infrastrukturen (PKI)

Im vorangehenden Abschnitt wurde die Bedeutung von Zertifikaten für die Verlässlichkeit asymmetrischer Kryptoverfahren hervorgehoben. Den Erfindern der asymmetrischen Kryptographie schwebte als Lösung des Zuordnungsproblems eine Art "Schlüsselbuch" als Analogie zum Telefonbuch vor. Schon alleine wegen der Länge der Schlüssel (z.B. 150-stellig bei RSA-1024) und dem damit verbundenen Umfang eines solchen Buches sowie der voraussichtlich hohen Fehlerquote beim Abtippen der Zahlen ist dies jedoch nicht praktikabel. Nötig sind vielmehr elektronische Bescheinigungen, die maschinell vom Krypto-Programm ausgewertet werden.

Wegen der großen Bedeutung der Zertifikate sollten diese möglichst von einer vertrauenswürdigen Stelle, idealerweise nach persönlicher Registrierung des Nutzers, ausgestellt und verwaltet werden. Eine solche Stelle wird als Trustcenter, Zertifizierungsstelle oder auch "certification authority (CA)" bezeichnet. Entscheidend für den Wert eines Zertifikat ist es weiterhin, dass dieses integer und authentisch ist. Wie wir gesehen hatten, können diese Eigenschaften bei elektronischen Dokumenten durch die Anbringung von digitalen Signaturen gewährleistet werden. Zur Erlangung eines Zertifikats begibt sich ein (zukünftiger) Nutzer in die Registrierungsstelle eines Trustcenters. Dort wird er – entsprechend dem verwendeten Sicherheitsmodell – identifiziert. Je nach Ausstattung von Kunde und Trustcenter wird für den Kunden dann entweder ein Schlüsselpaar erzeugt (zentrale Schlüsselgenerierung) oder er legt einen selbst erzeugten öffentlichen Schlüssel zur Zertifizierung vor (dezentrale Schlüsselgenerierung). Es sei an dieser Stelle hervorgehoben, dass die CA hierbei den privaten Schlüssel des Kunden nicht explizit kennen muss. Vielmehr existieren Protokolle (z.B. PKCS#10)[2], bei denen dem Kunden lediglich ein unbekannter "Text" zum entschlüsseln bzw. signieren vorgelegt wird.

[2] Bei den "Public Key Cryptography Standards" handelt es sich um von der Firma RSA Securtiy Inc. gepflegte "Quasi-Standards" zur asymmetrischen Kryptographie; sie sind abrufbar unter www.rsa.com

Durch einen derartigen "Proof-of-possesion" kann die CA lediglich anhand der Kenntnis des öffentlichen Schlüssels feststellen, ob sich der Kunde tatsächlich im Besitz des zugehörigen privaten Schlüssels befindet. Zur Zertifikatserstellung müssen somit keinerlei vertrauliche Informationen ausgetauscht werden. Nach Abschluss des Registrierungsvorgangs wird ein elektronisches Zertifikat erstellt, das die Zuordnung zwischen öffentlichem Schlüssel und Schlüsselinhaber bestätigt. Dieses Zertifikat wird dem Kunden auf einem geeigneten Datenträger übergeben und ggf. in einem sog. Verzeichnisdienst öffentlich abrufbar oder überprüfbar gehalten. Neben dem Namen (oder Pseudonym) des Besitzers und dem öffentlichen Schlüssel sollte das Zertifikat auch einen genau festgelegten maximalen Gültigkeitszeitraum sowie Angaben über den Verwendungszweck des Schlüssels (Verschlüsselung, Signatur,...), den Namen der ausstellenden CA und die unterstützen Algorithmen enthalten. Weitere Zertifikatsinhalte können z.B. eine Organisationszugehörigkeit des Besitzers, Nutzungsbeschränkungen oder sonstige anwendungs-bezogene Angaben sein.

Eine wichtige Aufgabe des Verzeichnisdienstes ist es, dem Nutzer die Sperrung seines Zertifikats zu ermöglichen, wenn dieser das entsprechende Schlüsselpaar nicht mehr nutzen will oder kann, etwa beim Verlust der zugehörigen Diskette oder Chipkarte, beim Wegfall von im Zertifikat mitbescheinigten Eigenschaften (etwa Wechsel der Arbeitsstelle) oder wenn der Verdacht auf eine Kompromittierung des Schlüssels besteht. Eine solcher Sperrdienst kann entweder "offline" über die Veröffentlichung von Sperrlisten ("certificate revocation list (CRL)") oder "online" über eine direkte Abfrage des Zertifikatsstatus beim Verzeichnisdienst (etwa über das OCSP-Protokoll) erfolgen.

Um Integrität und Authentizität der erzeugten Zertifikate zu gewährleisten, wird das Zertifikat von der CA mit einem speziell für diesen Zweck bestimmten Signaturschlüssel digital signiert. Bei der Zertifikatsprüfung ergibt sich nun die Notwendigkeit, den zugehörigen öffentlichen Schlüssel der CA authentisch und integer zu erhalten. Mit anderen Worten: Die CA benötigt ebenfalls ein Zertifikat! Dieses kann sie zum Beispiel nach dem oben beschriebenen Schema von einer übergeordneten CA erhalten, die wiederum ein Zertifikat benötigt. Ein Verfahren, das sich prinzipiell über beliebig viele Stufen erstrecken kann. Die so entstandene Zertifikatshierarchie muss an irgend einer Stelle beendet werden. Die an dieser Stelle angesiedelte CA, die Root-CA, die die "Wurzel" des Vertrauens in alle darunter erzeugten Zertifikate repräsentiert und von allen Teilnehmern als vertrauenswürdig anerkannt wird, signiert ihr Zertifikat selbst. Die durch diese Hierarchie von Zertifikaten entstehende Struktur wird als "Public Key Infrastructure (PKI)" bezeichnet.

Eine potentielle Angriffsmöglichkeit, der zunächst jede PKI ausgesetzt ist, ist die Totalfälschung von Zertifikatsketten. Eine solche liegt vor, wenn sich ein Angreifer ein Schlüsselpaar erzeugt und sich für den zugehörigen öffentlichen Schlüssel ein Zertifikat auf den Namen einer existierenden oder vermeintlichen Root ausstellt. Mit Hilfe dieses Zertifikats kann er sich dann Zertifikate für (falsche) CAs und damit dann Zertifikate für "echte" oder "erfundene" Benutzer ausstellen. Innerhalb der PKI-Struktur kann eine solcher Angriff prinzipiell nicht erkannt werden. Als Ausweg müssen externe Sicherheitsanker geschaffen werden. In Frage kommt beispielsweise eine persönliche Übergabe des authentischen öffentlichen Root-Schlüssels etwa auf einer Chipkarte oder einer Diskette oder die Veröffentlichung des Root-Zertifikats (oder eines geeigneten Hash-Wertes; "fingerprint") einem externen Medium (Brief, Zeitung, ...).

Allgemein lässt sich festhalten, dass PKIs, die eine Online-Zertifikatsabfrage anbieten, stabiler gegen Zertifikatsfälschungen und Schlüsselkompromittierungen sind, als solche, die nur das Herunterladen von Sperrlisten unterstützen. Im ersten Fall kann ein Angreifer auch dann, wenn es ihm gelänge an den privaten CA- oder Root-Schlüssel zu kommen, solange keine falschen Zertifikate einstellen wie es ihm nicht gelingt, auch den Verzeichnisdienst zu manipulieren. Bei der alleinigen Verwendung von Sperrlisten hingegen, wird ein solchermaßen gefälschtes Zertifikat, das selbstverständlich niemals gesperrt wurde, auf keiner Sperrliste geführt und daher fälschlicherweise zunächst als gültig erkannt. Die Kompromittierung eines CA oder Root-Schlüssels erfordert - wenn sie denn erkannt wird - im zweiten Fall also eine sofortige Sperrung aller damit erzeugten Zertifikate. Im ersten Fall ist dies solange unnötig, wie der Verzeichnisdienst integer bleibt.

5
Rechtliche Rahmenbedingungen für elektronische Signaturen

Signaturgesetz

EU-Richtlinie

Formvorschriften

Es existieren sowohl national als auch EU-weit gesetzliche Regelungen für den Einsatz der elektronischen Signatur. Diese sollen im Folgenden kurz umrissen werden.

5.1
Das deutsche Signaturgesetz (SigG) vom 22.07.1997

Das "Gesetz zur digitalen Signatur" (Signaturgesetz, SigG) vom 22.07.1997 als Artikel 3 des Informations- und Kommunikationsdienstegesetzes (IuKDG) schafft in Deutschland Rahmenbedingungen für sichere digitale Signaturen[3]. Es definiert also nicht "erlaubte" und "verbotene" Signaturen, sondern beschreibt einen Rahmen, innerhalb dessen digitale Signaturen als "sicher gelten und Fälschungen digitaler Signaturen und Verfälschungen von signierten Daten zuverlässig festgestellt werden können" (§ 1 (1) SigG). In der zugehörigen Signaturverordnung SigV werden verschiedene Regelungen des Gesetzes näher spezifiziert.

Die "Sicherheitsvermutung" des Signaturgesetzes gründet sich auf die Einhaltung verschiedener technischer und organisatorischer Rahmenbedingungen durch die Zertifizierungsstellen. Die Durchführung des Gesetzes steht unter der Überwachung der Regulierungsbehörde für Telekommunikation und Post (RegTP) als "zuständiger Behörde" (§ 3 SigG).

Kernpunkte sind u.a.

- Genehmigung und Überwachung der Zertifizierungsstellen (ZS) durch die RegTP
- Vorlage von geprüften und bestätigten Sicherheitskonzepten für den Betrieb der ZS als Genehmigungsvoraussetzung
- Festlegung von technischen Anforderungen und Prüfstufen für bestimmte technische Produkte

[3] Das Signaturgesetz, die Signaturverordnung und weitere Gesetze sind unter www.iukdg.de abrufbar.

(dies bedingt u.a., dass nach derzeitigem Stand der Technik nur (nach ITSEC E4-hoch oder nach Common Criteria Stufe EAL 5 bestätigte) Chipkarten als "Signaturerstellungskomponenten" in Frage kommen)

- Veröffentlichung einer mindestens einmal jährlich zu aktualisierenden Liste von geeigneten Kryptoalgorithmen durch die RegTP ("Die Eignung wird nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik unter Berücksichtigung internationaler Standards festgestellt. Experten aus Wirtschaft und Wissenschaft sind zu beteiligen."; §17 (2) SigV)
- Vorgaben für die Erzeugung, Veröffentlichung und Sperrung von Zertifikaten
- Dokumentation der Tätigkeit der ZS mit 35-jähriger Aufbewahrungsfrist.

(Diese Dokumentation umfasst u.a. die Antragsunterlagen mit eigenhändig unterschriebener Ausweiskopie des Zertifikatsinhabers. Hierdurch wird die unbemerkte Ausstellung von Zertifikaten für "falsche" Teilnehmer gerichtsfest ausgeschlossen.)

Im Signaturgesetz wird weiterhin die in Bild 3 dargestellte Zertifikatshierarchie mit der RegTP als Rot-CA definiert. Externer Sicherheitsanker dieser PKI ist die Veröffentlichung des öffentlichen Root-Schlüssels der RegTP im Bundesanzeiger.

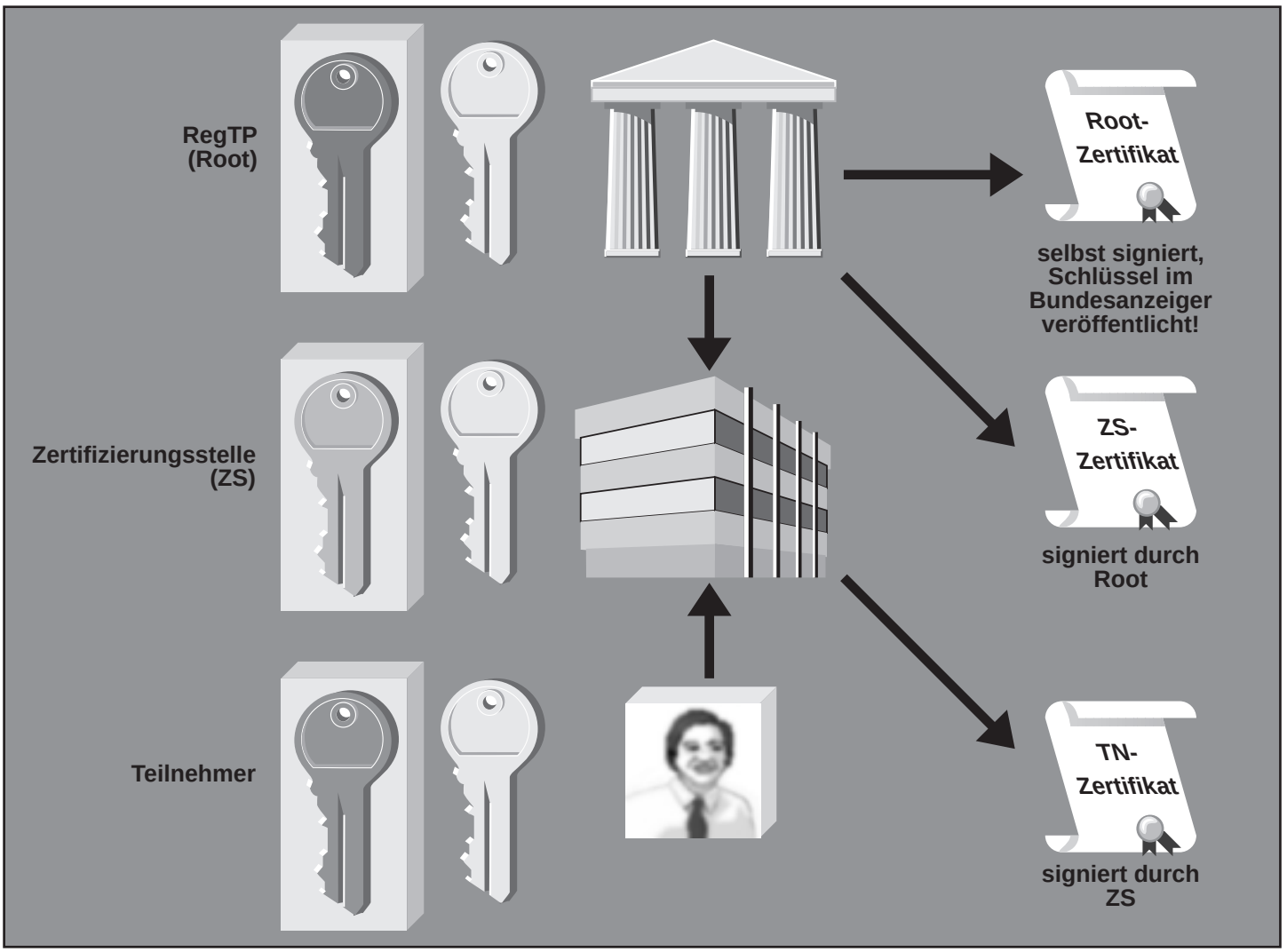
Zum Zeitpunkt der Fertigstellung dieses Artikels bieten zwei genehmigte Zertifizierungsstellen ihre Dienste an. Die Trustcenter Telesec der Deutschen Telekom AG und Signtrust von der Deutschen Post AG. Dem Vernehmen nach steht die Zulassung weiterer Stellen unmittelbar bevor.

5.2 Die EU-Richtline über elektronische Signaturen

Durch die Nutzung des Internet werden globale Handelsbeziehungen und Geschäftsprozesse wesentlich erleichtert. Eine rein nationale Regelung von Sicherheitsstandards und Rechtsfolgen von Signaturen kann daher immer nur eine Zwischenlösung sein. Dieses Problem haben auch die Mitgliedsstaaten der Europäischen Union erkannt und versucht, einen EU-weit einheitlichen Rahmen für Signaturen zu finden.

Ergebnis dieser Bemühungen ist die "EU-Richtline 1999/93/EG vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen", die am 19.01.2000 im Amtsblatt der EU veröffentlicht wurde. Sie hat zum Ziel,

Bild 3 Die SigG-Zertifikatshierarchie



"Wozu brauche ich ein Zertifikat?" – Verschlüsselung und Signaturen im E-Business/E-Commerce

"die Verwendung elektronischer Signaturen [zu] erleichtern und zu ihrer rechtlichen Anerkennung bei[zu]tragen", indem sie "rechtliche Rahmenbedingungen für elektronische Signaturen und für bestimmte Zertifizierungsdienstleistungen fest[legt]" (Art 1 EU-RiLi).

Die EU-Richtlinie definiert elektronische Signaturen dabei weitaus allgemeiner als das geltende Signaturgesetz, das mit dem Begriff der digitalen Signatur ausschließlich auf asymmetrische Kryptographie abzielt. Dieser Unterschied ist jedoch in der Praxis ohne Bedeutung, da andere Verfahren derzeit nicht auf breiterer Basis angewendet werden. Die Richtlinie definiert dann anhand von generischen, also technisch nicht näher spezifizierten Anforderungen[4] "fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen und die von einer sicheren Signaturerstellungseinheit erstellt werden". Für diese Signaturen, für die sich inzwischen der Terminus "qualifizierte Signaturen" eingebürgert hat, wird in Art. 5 der Richtlinie gefordert, dass sie der handschriftlichen Unterschrift im wesentlichen gleichgestellt werden sollen, ohne dass dabei aber ein unmittelbarer Eingriff in einzelstaatliche Formvorschriften vorgenommen werden soll (Art. 1, Absatz 2).

Gemäß dem Grundsatz des ungehinderten Marktzugangs bedürfen Zertifizierungsdiensteanbieter keiner Vorabgenehmigung für die Aufnahme ihrer Tätigkeit (Art. 3 (1) EU-RiLi). Um dennoch die Einhaltung der Sicherheitsanforderungen zu gewährleisten, unterliegen diese Anbieter einem von den Mitgliedsstaaten zu schaffenden "geeigneten Überwachungssystem" (Art. 3 (3)) sowie einer weitgehenden Haftungsregelung (Art. 5). Die Mitgliedsstaaten haben weiter die Möglichkeit, "freiwillige Akkreditierungssysteme" einzuführen oder beizubehalten (letzteres zielt eindeutig auf die existierenden Strukturen des deutschen Signaturgesetzes), um eine Steigerung des Niveaus der Dienstleistungen zu ermöglichen (Art. 3 (2)).

Die Mitgliedsstaaten stehen in der Pflicht, die Regelungen der EU-Richtlinie über elektronische Signaturen bis zum 19.07.2001 in nationales Recht umzusetzen.

5.3 Das neue Signaturgesetz, Anpassung von Formvorschriften

Durch die Umsetzung der EU-Richtlinie über elektronische Signaturen in deutsches Recht werden die Regelungen des SigG dahingehend modifiziert (voraussichtlich zum ersten Quartal 2001), dass Anbieter von "qualifizierten Signaturen" ihre Tätigkeit ohne Vorab-Genehmigung aufnehmen können. Sie unterliegen einer Meldepflicht und einer Überwachung im laufenden Betrieb durch die RegTP. Neu eingeführt werden weitgehende Haftungsregelungen. Das bisherige System mit umfassenden Vorabprüfungen und der Verpflichtung zum weitestgehenden Einsatz geprüfter technischer Komponenten bleibt als freiwilliges Akkreditierungssystem erhalten. Als "Lohn" für den zusätzlichen Aufwand dürfen die akkreditierten Anbieter ein entsprechendes Gütesiegel führen. Sie werden in die eingeführte PKI mit der RegTP als Root aufgenommen. Die RegTP verpflichtet sich, die Dokumentation der Tätigkeit einer akkreditierten Zertifizierungsstelle zu übernehmen, falls diese ihre Tätigkeit einstellt und keinen Nachfolger findet. Durch diese Regelung bleibt die langfristige Überprüfbarkeit von Signaturen unabhängig von wirtschaftlichen Unwägbarkeiten gewährleistet. Zum Zeitpunkt der Fertigstellung dieses Artikels lag ein vom Bundeskabinett verabschiedeter Entwurf zur Novellierung des Signaturgesetzes vor.[5]

Als weiterer Schritt zur Umsetzung der EU-Richtlinie werden die (Schrift-) Formerfordernisse zuächst im Privatrecht, später auch im öffentlichen Recht dahingehend modifiziert, dass - bis auf wenige Ausnahmen wie etwa Testamente - elektronische Dokumente mit qualifizierter Signatur grundsätzlich schriftlichen Dokumenten mit eigenhändiger Unterschrift gleichgestellt werden. Hierdurch sind die Voraussetzungen für einen umfassenden elektronischen Geschäftsverkehr auch in formaler Hinsicht gegeben.

6 Sicherheitsstrategien

Aus den Ausführungen dieses Artikels ergeben sich die im folgenden dargestellten Elemente einer Sicherheitsstrategie für Anbieter und Verbraucher im E-Commerce/E-Business (oder Verwaltungen und Bürger im E-Government).

6.1 Sicherheitsstrategie für Anbieter

- Etablierung eines IT-Sicherheitsprozesses auf Basis des IT-Grundschutz

  Mit Hilfe des IT-Grundschutzhandbuchs können Sie in effizienter Weise ein umfassendes IT-Sicherheitskonzept erstellen, umsetzen und aktualisieren. Dieses Sicherheitsniveau stellt eine Basis für einen stabilen und verantwortlichen IT-Einsatz in Geschäftsprozessen dar.

- Einsatz von kryptographischen Technologien

  Durch Verschlüsselungsverfahren, Authentisierungsmechanismen und Signaturen ermöglichen Sie eine für beide Seiten verlässliche Interaktion. Durch Nutzung dieser Verfahren können Sie auch anspruchsvolle Geschäftsprozesse mit weitreichenden Wirkungen verlässlich über elektronische Medien abwickeln.

- Verwendung transparenter Gütesiegel

  Durch den Erwerb von Gütesiegeln mit transparenten, sinnvollen Inhalten stellen Sie sich Ihrem Kunden gegenüber als sicherer Partner vor. Verbunden mit einer umfassenden Informationspolitik über Sicherheitsfragen und einer effizienten Geschäftsabwicklung präsentieren Sie sich als vertrauenswürdiger Geschäftspartner. Eine unabhängige Prüfung Ihrer Systeme erhöht zudem auch Ihre eigene Sicherheit. In Zukunft dürfte insbesondere das IT-Grundschutz-Zertifikat eine große Bedeutung erlangen.

6.2 Sicherheitsstrategie für Verbraucher

- Umsetzung der relevanten IT-Grundschutzmaßnahmen

  Mit Hilfe des IT-Grundschutzhandbuchs können Sie gezielt die für Ihr IT-System relevanten Sicherheitsmaßnahmen identifizieren und umsetzen und sich dadurch gegen die häufigsten Gefahren beim IT-Einsatz zuverlässig absichern.

[4] Eine solche Festlegung soll in verschiedenen Standardisierungsgremien sowie in einem speziellen EU-Ausschuss vorgenommen werden.

[5] Dieser Entwurf ist ebenfalls unter www.iukdg.de abrufbar.

"Wozu brauche ich ein Zertifikat?" – Verschlüsselung und Signaturen im E-Business/E-Commerce

Gerade im für Privatanwender interessanten Bereich entstehen dadurch praktisch keine zusätzlichen Kosten.

- Einsatz von kryptographischen Technologien

  Nutzen Sie wo immer dies möglich ist den Einsatz kryptographischer Verfahren, um Datenspionen keine Chance zu lassen und um die Verbindlichkeit von Angeboten o.Ä. zu gewährleisten.

- Nutzung transparenter Gütesiegel

  Anbieter, die transparente und sinnvolle Gütesiegel nutzen, geben Ihnen die Möglichkeit, Ihre Entscheidung für einen Anbieter auch unter Sicherheitsaspekten zu begründen. Scheuen Sie sich nicht, bei Unklarheiten über Inhalt und Umfang der Zusagen entsprechend nachzufragen. Sollten Sie keine Antwort erhalten, so ist dies auch eine wertvolle Auskunft!

- Nutzung des "gesunden Menschenverstands"

  Ebenso wie im "normalen" Geschäftsalltag ist auch beim E-Commerce eine gesunde Portion Misstrauen gegenüber allzu verlockenden Angeboten ein guter Ratgeber. So manches extrem günstige "Schnäppchen" hat sich auch hier im nachhinein als sehr teuer erwiesen. Auch im schnelllebigen Internet sollte vor dem Mausklick noch genügend Zeit für eine angemessene Abwägung oder eine entsprechende Nachfrage bein Anbieter sein.

7 Fazit

Moderne kryptographische Verfahren bieten, sofern sie auf der Basis eines sicheren IT-Betriebs im eigenen Bereich aufgesetzt werden, eine vielversprechende Grundlage für verlässliche und vertrauliche Interaktion im offenen Medium Internet.

Die ihnen zugrunde liegenden Zertifikate ermöglichen es, auch in elektronischen Kommunikationsbeziehungen "persönlich" zu agieren.

Die Frage

"Wozu brauche ich ein Zertifikat?"

ist demnach das elektronische Analogon zur Frage

"Wozu brauche ich eine Identität?"

Die Antwort kann daher nur lauten:

"Ich brauche Zertifikate als
'digitale Identität'
und damit als
'Eintrittskarte'
in alle Formen
der anspruchsvollen
elektronischen Interaktion".

E-Commerce, E-Business und E-Government stehen sicherlich erst am Anfang dieser Entwicklung.

Abk.

B	**BSI**	**Bundesamt für Sicherheit in der Informationstechnik**
C	**CA**	**Certification Authority**
	CRL	**Certificate Revocation List**
E	**E-Government**	**elektronische Erbringung von Verwaltungsdienstleistungen**
	EU-RiLi	**EU-Richtlinie**
P	**PKCS**	**Public Key Cryptography Standards**
	PKI	**Public-Key-Infrastructure**
R	**RegTP**	**Regulierungsbehörde für Telekommunikation und Post**
S	**SigG**	**Das deutsche Signaturgesetz**
	SigV	**Signaturverordnung**
Z	**ZS**	**Zertifizierungsstelle**

Thema

"Wenn die Prüfung dahinter steht, muss man sich doch viel intensiver mit allem auseinandersetzen."

Lothar Jahn hat schon früher ("noch hinter der Mauer") Computer-Netzwerke betreut. Heute arbeitet bei der Firma Siemens am Standort Berlin, wo er das Lokale Netz seit 6 Jahren betreut. Vorher war er drei Jahre bei Siemens Dozent für Netzwerke beim Trainingscenter.

Insider: Und warum haben Sie damit aufgehört?

Jahn: Ich wollte mal wieder was praktisches machen. Nun ist aber der Fall eingetreten, dass man, wenn man andauernd nur die Praxis macht, die Theorie dabei wieder verlorengeht.

Insider: Welche Aufgaben haben Sie jetzt?

Jahn: Ich konfiguriere die aktiven Komponenten im Netzwerk, mach in regelmäßigen Abständen, so alle 2 Jahre, ein Redesign von dem Netzwerk. Als ich angefangen hab war das noch so ein Shared Ethernet gewesen, einfach bloß eine Leitung durchs ganze Werk. Dann haben wir angefangen zu switchen und Twisted Pair einzubauen. Die nächste Stufe war dann, dass wir 100 Mbit-Technologie eingeführt haben. Und jetzt bin ich dabei, ein Gigabit Ethernet Backbone aufzubauen.

Insider: Und warum wollten Sie Ihre Kenntnisse jetzt auffrischen?

Jahn: Wenn man sowas aufbaut, das ist alles sehr praktisch. Die meisten Komponenten funktionieren auch ohne allzu großes Hintergrundwissen. Nur man weiß dann nicht, warum sie funktionieren. Und das ist dann bei der Fehlersuche ein bißchen ungünstig, wenn man nicht weiß, warum was funktioniert. Man hat dann so viel zu tun mit dem täglichen Zeug, dann fällt da mal eine Leitung aus, und dann geht mal ein Switch wieder nicht, da kommt man dann in der normalen Arbeit nicht dazu, sich das wirklich zu durchdenken.

Insider: Und deshalb dachten Sie, jetzt mach ich diese Kurse?

Jahn: Ja, ich dachte, jetzt mach ich diese Kurse und dann mach ich auch die Prüfung. Sonst sitzt man doch nur bei dem Seminar, hört sich das an, sagt: alles schön, alles toll, versteh ich alles, ist doch logisch. Aber wenn die Prüfung dahinter steht, muss man

sich doch viel intensiver mit allem auseinandersetzen. Und es hat sich gezeigt, dass das wirklich so ist. Als ich die Fragen das erste Mal gesehen habe, dachte ich, oh, hier muss ich aber noch einiges tun und einiges nochmal durchlesen.

Insider: Wie lange brauchten Sie für die Ausbildung?

Jahn: Ich hab das ziemlich kompakt gemacht. Ich hab im Frühjahr angefangen mit dem ersten Kurs und jetzt bin ich fertig, also ein halbes Jahr.

Insider: Wie ist die Prüfung für Sie gelaufen?

Jahn: Es freut einen schon, wenn der Prüfer sagt: Sie wissen wahrscheinlich mehr, als Sie hingeschrieben haben (lacht). Die Zeit ist ziemlich knapp in der schriftlichen Prüfung, man kann wirklich nur die ganz wesentlichen Schlagworte hinschreiben. Es müssen dann eben genau die passenden sein und wenn man sich etwas mehr ausbreiten kann, hätte man eher die Chance, das richtige zu erwischen.

Insider: Wo sehen Sie den Nutzen des Gelernten für Ihre tägliche Arbeit?

Jahn: Ich bin ja grade dabei den nächsten Technologie-Schritt zu machen mit Gigabit und da haben gerade die Kenntnisse aus dem letzten Kurs Neue Ethernet-Technologien sehr viel geholfen.

Lothar Jahn (links) mit Dr. Jürgen Suppan

Dr. Kauffels Investment Insider

Dr. Kauffels Investment Insider

Der Dr. Kauffels Investment Insider greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends. Auf keinen Fall haftet der Autor oder der Netzwerk Insider für Investments der Leser, die sich aus diesen Darstellungen ergeben. Eine Haftung, weder für Verluste noch für entgangene Gewinne, wird absolut ausgeschlossen.

Und ist der Ruf mal ruiniert ...

Bald macht es keinen Spaß mehr. Schlechte und gute Nachrichten wechseln sich ab, aber es scheint so, als wolle der Markt keine dauerhaft positiven Nachrichten sehen. Es gibt immer so ein Aufbäumen, das unseren Lieblingswerten dann auch meist hilft, aber damit hat es sich auch. Eine kleine Nebenbemerkung in einem hinteren Untersatz ... schon geht es wieder abwärts. Hatte doch Mitte Januar das überaus positive Ergebnis von IBM zusammen mit den Zinsschritten für eine gewisse Entspannung und Zwischenerholung gesorgt, treiben Warnungen alles wieder in den Keller. Am 24.1.2001 meldete der führende Glasfaserhersteller Corning ein überaus gutes Ergebnis, was weit über den Erwartungen lag. Leider wurde auch erwähnt, dass sich wegen zurückhaltendem Ausgabeverhalten der Carrier dieses Ergebnis vielleicht nicht ganz in dem erwarteten Maße steigern ließe. Das hat an dem Tag gereicht, die Aktie wieder 16% in den Keller zu schicken, und weil man im dunklen Keller ja nicht so gerne alleine ist, sind die anderen gleich mitgekommen.

Ihr Franz-Joachim Kauffels

Dr. Kauffels Investment Insider

Positive Signale

Glücklicherweise bin ich schon lange genug dabei und habe auch schon genug Geld gegen die Wand gefahren, um in der jetzigen Situation die eindeutig positiven Zeichen nicht zu übersehen.

Schauen wir zunächst einmal in die Historie. Bullenmärkte beginnen sich zu entfalten, wenn die US-Notenbank die Zinsen senkt. Betrachtet man die Zinsbewegungen seit 1913, gab es 21 initiale Zinssenkungen, also Senkungen der Zinsen nach einem langen Abschnitt von Zinserhöhungen. Betrachtet man anschließenden den Dow Jones Index, ist er im Zwölfmonatszeitraum nach einer Senkung um durchschnittlich 19,92% gestiegen. Man kann vielleicht sagen, das sei doch wenig, aber halten wir bitte fest, daß die großen Ausschläge der letzten Jahre eher exzessiv waren und dass 20% eine hervorragende Rendite für ein Jahr ist. Senkungen der Zinsrate sind aber selten alleine geblieben: in 17 der 21 Fälle wurden die Zinsen weiter gesenkt. Dies erwarten auch alle Beobachter für 2001, denn obwohl Alan Greenspan auch Steuersenkungen befürwortet, könnte ein kleiner Nachbrenner der Wirtschaft nicht schaden. Normalerweise werden die Zinsen solange gesenkt, bis sich die Wirtschaft wieder erholt. Werden die Zinsen zweimal gesenkt, so steigt der Markt im Jahr danach durchschnittlich um 28,4 % an. Aktien reagieren nur auf die erste und zweite Senkung mit diesen Sprüngen, bei weiteren Zinssenkungen lassen sie nach. Wenn die erste Zinssenkung in einer frühen Phase der Rezession erfolgt, reagiert der Markt nicht besonders stark. Das hatten wir 1929, 1957, 1960 und 1981. Und 2001. Gleichermaßen hat der Markt in dieser Situation besonders stark auf die zweite Senkung reagiert.

Wenn nun wie erwartet Ende Januar der Offenmarktausschuss die zweite Zinssenkung beschließt, ist rein statistisch ein vehementes Durchstarten des Marktes zu erwarten.

Sollte das so eintreten wie von allen gewünscht und vorhergesagt, geht es über längere Zeit dramatisch aufwärts. Wie lange das sein wird, darüber streitet man sich trefflich. Manche sprechen von zwei Jahren, andere sagen, dass schon die nächste Ergebnissaison in drei Monaten die Freude wieder verderben wird, weil dann endgültig die Auswirkungen der aktuellen Schwächephase zu spüren sind. Nichtsdestotrotz steht fest, dass Unmengen Geld in frei beweglichen Anlageformen liegt, Geld, das aus dem Aktienmarkt herausgezogen wurde und nur darauf wartet, hier wieder Gewinne zu machen. Man spricht von ca. 2 Trilliarden US-Dollar, das entspricht ca. 16% des Gesamtwertes der an der Nasdaq notierten Firmen.

Was muss man haben?

Wie schon gesagt, hat es unsere strahlenden Lieblinge von letztem Jahr schlimm zerrissen. Dadurch sind sie jetzt alle ziemlich preiswert zu haben, doch es gilt, die Spreu vom Weizen zu trennen. Das wird der Markt nämlich auch machen. 20% Steigerung des Gesamtmarktes bedeutet, dass sich manche Werte schnell wieder mehr als verdoppeln werden und andere vielleicht nur 5% zulegen, bzw. könnte es sogar sein, dass aus einigen Werten Geld abgezogen wird.

Ich stelle jetzt einfach meine zehn persönlichen Favoriten für 2001 vor, und zwar in alphabetischer Reihenfolge. Um der wenn auch gering wahrscheinlichen Möglichkeit Rechnung zu tragen, dass sich der Euro-Raum in einem überschaubaren Zeitraum besser erholt als die US-Wirtschaft, sind auch ein paar Werte, die nicht alleine aus USA kommen, dabei.

Wegen der hohen Volatilität des Marktes, die nichts für jeden Anleger ist, habe ich ausnahmsweise auch das Augenmerk auf Sicherheit gelegt. Vielleicht wird der eine oder andere Leser meine Auswahl nicht besonders originell finden, aber denken Sie immer daran, dass auch Fondsverwalter es nicht besonders originell finden, Geld zu verlieren!

Thema

AOL/Time Warner

Ich finde es ja einfach schrecklich. AOL ist für mich der Schöpfer des WWTW: World Wide Tussi Web. Schriller, bunter und für noch Dümmere konnte man es eigentlich nicht machen. Und ... wie Big Brother und die Bild Zeitung: es brummt. Nicht so sehr hier in Deutschland, wo der Platzhirsch T-Online heißt, aber weltweit. Durch die Vereinigung mit Time Warner können sozusagen unendlich viele, noch buntere Inhalte angeboten werden und sich dauerhaft in den Seelen der Basisbevölkerung verewigen. In 2001 soll der Umsatz um 15% auf 40 Mrd. US$ steigen. AOL bietet den Kunden Content, Info-Dienste, Shops und Services an. Dabei sind sie sehr erfolgreich: Kunden bleiben durchschnittlich täglich 12 Minuten auf den Seiten, während sie sich bei T-Online schon nach 2 Minuten entsetzt abwenden. T-Online ist mit 18 Mrd. Euro Marktkapitalisierung übrigens nur ein kaum wahrnehmbarer Zwerg gegenüber AOL mit über 250 Mrd. Euro. Die Aktie hat im Dezember ihren Tiefpunkt erreicht und sich danach vehement erholt. Mit einem KGV von 85 momentan noch einigermaßen erschwinglich, aber durch die dominante Marktstellung entstehen so viele neue Chancen in neuen Geschäftsfeldern, dass auch langfristig am Erfolg kein Weg vorbeiführt.

Ciena

Der Marktführer bei DWDM-Systemen hat eine erstaunliche Widerstandsfähigkeit gegenüber den Abschlagswellen gezeigt. Im Januar konnte sich das Papier kurzfristig schon wieder über 100 US$ schwingen. Nach wie vor steht einem Wachstum in schwindelnder Höhe auch ein ebensolches KGV gegenüber, immer noch weit über 200 auf Basis der 2001er Erwartungen. Andererseits scheint das aber niemanden zu stören, während andere Werte im Zweifelsfall abgeworfen werden wie Blätter im Herbststurm, bleiben die Besitzer auf Ciena Aktien sitzen und erzeugen so eine phantastische Wertstabilität. Man muss ja nicht das ganze Geld in den Wert legen, aber ein paar können nicht schaden.

Cisco Systems

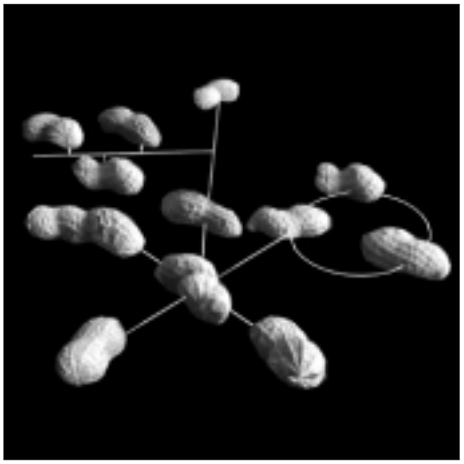
Diese Firma ist ein Basisinvestment, welches man jetzt wieder kaufen kann. Ich rechne fest damit, dass die konzeptionellen Schwierigkeiten des Jahres 2000 überwunden werden und Cisco wieder zur alten Form auflaufen kann. Nachdem die Tiefstände um die 35 US$ mehrfach erfolgreich getestet wurden, ergibt sich zu den heutigen Preisen um 40 US$ ein KGV auf Basis der 2001er Erwartungen von ca. 50. Damit ist die Aktie immer noch nicht billig, aber gerecht bewertet. Ich glaube nicht daran, dass sich der Preis in den nächsten Monaten verringert, eher wird das Gegenteil der Fall sein. Cisco ist mit einer Marktkapitalisierung von knapp 300 Mrd. US$ immer noch mehr als doppelt so groß wie der Verfolger Nortel Networks. Wer in 2000 auf mich gehört hat, ist frühzeitig aus dem Wert gegangen und bekommt jetzt fürs selbe Geld doppelt so viele Aktien.

EMC

Wo man hinsieht, die Welt ist voller Daten. Und dies mit rasant steigender Tendenz. Die Daten müssen irgendwo schlafen. Besonders luxuriös und beliebt sind die Herbergen von EMC. Ausgerüstet mit einer weit vor allen Verfolgern liegenden Software zur Steuerung der Datenkühlschränke greifen vor allem Großanwender immer beherzter zu. Alleine die Deutsche Telekom betreibt 400 EMC Datenhotels. Rechnet man das einmal auf die Größe um, müßte AOL über 5.500 davon herumstehen haben. Mangels wirklicher Konkurrenz im Hochzuverlässigkeitsbereich ist die Kundenhalterate bei über 96%. Die von EMC hauptsächlich verkauften SAN-(Storage Area Networks) Lösungen machen einen Gesamtmarkt von 27 Mrd. US$, der bis 2003 mindestens um 100% wächst. Der NAS-Markt (Network Attached Storage) ist nur 2 Mrd. US$ schwer. Obwohl EMC Marktführer ist, haben sie momentan nur 20% des Marktes, können also durchaus überproportional wachsen.

Extreme Networks

Für meine Begriffe stehen wir erst am Anfang einer langen Erfolgstory. Ich sehe nämlich, dass es Tendenzen bei Kunden gibt, diesen Hersteller als zweite Linie neben Cisco aufzubauen. Man möchte sich nach den schlechten Erfahrungen der Vergangenheit nicht mehr von einem Hersteller abhängig machen. Die "Ethernet Everywhere" Strategie ist sauber durchdacht und setzt sich sogar bis in den Bereich der letzten Meile fort. Darüber werde ich im nächsten Insider in einem Hauptartikel berichten. Der Wert ist ziemlich abgestürzt, sammeln wir ihn auf! Bei einem KGV von 89 auf Basis der 2001er Erwartungen kann auch hier nicht mehr viel passieren.



Netzwerke: für IBM Peanuts

IBM

Die innere Erneuerung dieser Firma ist schon sehr weit vorangeschritten. Dem Mitbewerb ist es auf vielen Feldern nicht gelungen, dauerhaft wirkliche Alternativen auf die Beine zu stellen. Durch eine gradezu beängstigende Politik der Öffnung zu Standards hat man die Grundlage für weiteren, dauerhaften Erfolg geschaffen. Nach wie vor sind in vielen Bereichen Großrechner nicht wegzudenken, vor allem im E-Business. Man greift aber auch Herausforderer wie Sun Microsystems an, die dieser Angriff bis zu 60% des eigenen Firmenwertes gekostet hat. Mit der gleichen unerbittlichen Konsequenz trennt man sich von Bereichen, die man offensichtlich nicht beherrscht, wie PCs und Netzwerke. Die gesamte Firma profitiert von einer enormen Stärke der Firmenführung. Viele Anwender sehen in der Verwendung von IBM-Komponenten einen Investitionsschutz. Grade für die Netzwerker ist dies leider nicht aufgegangen, aber gemessen am Gesamtumsatz waren Netzwerke für IBM Peanuts. In verschiedenen Bereichen hat man es sehr erfolgreich geschafft, sich auch als Lösungsanbieter zu positionieren. Die Aktie von IBM wird nicht durch die Decke gehen, aber man steht auch kaum in Gefahr, Geld damit zu verlieren.

Microsoft

Mit Bush als Präsident ist eingetreten, was ich schon im Frühsommer vermutet hatte: Microsoft gibt eine Spende und das wars. Vielleicht wäre ja eine Spende an eine psychiatrische Anstalt angemessen, wo diejenigen Leute landen, die die Bedienung der Produkte nicht vertragen haben.

Thema

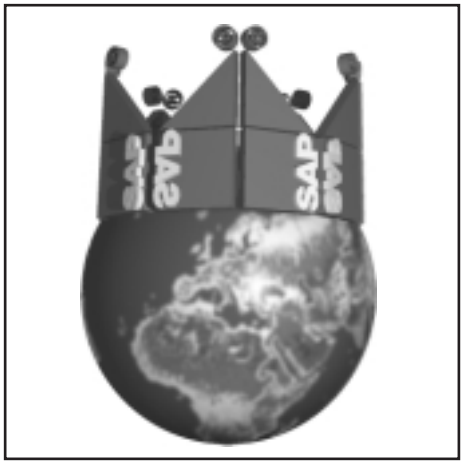
Scherz beiseite, niemand wird in den nächsten Jahren gegen Microsoft anstinken können. Ich gehe sogar noch weiter: wenn Microsoft den Einstieg in die Spielekonsolen schafft, werden sie in ganz geschickter Weise die Bedienung der Konsolen und der PC-Software anpassen. In ein paar Jahren können dann Kids damit besser umgehen als mit dem Lichtschalter. Der Einbruch beim PC-Wachstum könnte damit deutlich kompensiert werden. Mit einem KGV von 30 ist der Wert schon fast den Schwermetallverarbeitern zuzurechnen. Im Gegensatz zu vielen konservativen Analysten rechne ich eher damit, dass der Firma in absehbarer Zeit nochmals ein "Knüller" gelingt, der alle überrascht.

Nortel Networks

Die Nummer zwei der weltweiten Ausrüster hatte einige strukturelle Probleme zu bewältigen. Dies sollte aber "gegessen" sein. In vielen bereichen hat man technologisch die Führung übernommen und macht dem mehr als doppelt so großen Marktführer Cisco Systems das Leben schwer. Man rechnet für 2001 mit einem Umstaz- und Ergebniswachstum von jeweils 30% und im ersten Quartal mit 16 Cents pro Aktie und einem Umsatz von 8,1 Mrd. US$. Die Höchststände im August wurden halbiert, seit Dezember ist Nortel Networks technisch gesehen einer der attraktivsten Werte überhaupt.

SAP

In Walldorf soll ja bald ein künstlicher Fluss angelegt werden, in dem Buchhalter, die



König von Europa: SAP

mit R/3 arbeiten, jedes Jahr eine spirituelle Reinigung erhalten können. Die Erfolgsstory ist einzigartig und es ist einfach so, dass Firmen, die in R/3 investiert haben keinen Grund mehr haben, zu wechseln. Bis das System einmal zur Zufriedenheit läuft, dauert es etwas und kostet viel Geld. Danach verschlingen die Systemkosten vielleicht ein halbes Prozent vom Umsatz. Durch eine andere Software ließen sich nur unbedeutende Promille einsparen, zum Preis einer weiteren Einführungsphase. Man kann davon ausgehen, dass das niemand macht. Das Buchhalten als solches ist vielleicht langweilig, aber erforderlich. Änderungszyklen sind eher langsam. SAP ist in Europa der absolute König und hat weltweit nur noch einen einigermaßen ernst zu nehmenden Konkurrenten, die Fa. Peoplesoft. Baan ist untergegangen. Auf Basis der 2001er Erwartungen ergibt sich ein KGV von ca. 65. Die Aktie hatte sich um Weihnachten bezogen auf ihren Kurs vom März 2000 mehr als halbiert, in den letzten Tagen aufgrund sehr guter Ergebnisse aber einen erheblichen Aufschwung genommen. Bei geringer Rückschlagswahrscheinlichkeit bald einsteigen, bevor der Wert wieder völlig abzieht.

Siemens

Heinrich von Pierer hätte sicherlich allen Grund, seinen 60 jährigen Geburtstag ausgelassen zu feiern. Das würde aber nicht zu einem Mann passen, der es verstanden hat, einem völlig zerfahrenen und diffusen Großkonzern wieder Richtungen zu geben, in denen Welt-Spitzenpositionen aufgebaut, gehalten und genutzt werden können. Siemens hat ein erhebliches Forschungspotential, bei der Kommunikation sind sie Inhaber des aktuellen Rekords mit 10 Terabit/s. über 50 km ohne Zwischenverstärker. Charttechnisch gesehen hat die Aktie Böden erfolgreich getestet und kann jetzt wieder nach oben ausbrechen und dabei bis zu 40% gut machen. Den Spaß verderben könnte der zyklische Halbleitermarkt. Infineon, an der Siemens noch die Mehrheit hält, und Epcos haben sich eher vorsichtig geäußert. Infineon ist aber Marktführer in verschiedenen Sektoren, wie z.B. bei kompakten 10 Gbps Transceivern. Außerdem ist der Konzern also solcher natürlich gut aufgestellt. Bereiche wie z.B. SBS (Siemens Business Services) nehmen führende Positionen im Bereich gehobener Dienstleistungen ein und der Angriff auf die Nebenstellenanlagen durch VoIP konnte zunächst auch einmal abgewehrt werden. Mit einem KGV von 23,8 ein preiswertes Investment.

Dr. Kauffels Investment Insider

Investment Insider Top Performer

Nein, nicht alle Werte, über die ich in den vergangenen Monaten geschrieben habe, sind eingegangen. Es gibt immer noch ein paar Hartnäckige, die allen Tendenzen zum Trotz in der Gewinnzone liegen.

Rang	Company	genannt am:	Kurs	Kurs 28.1.	Gewinn %
1.	BEA Systems	25.5.	34	65	91 %
2.	Extreme Networks	04.05.	30	47	56 %
3.	Coca Cola	25.05.	53	58	9,4 %
4.	Ciena	04.07.	85	90,5	6,5 %
5.	Microsoft	25.05.	62	64	3,2 %

***Extreme Networks und Ciena haben zwischen Nennung und jetzt einen 1:2 Split durchgeführt.**

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebrauchte Netzwerk-Komponenten

Gebrauchte Netzwerk-Komponenten, die im Rahmen eines Redesigns ausgemustert werden, könnten einige Betriebe sehr gut gebrauchen. Hier wollen wir helfen. Wir bauen für unsere Kunden eine Handelsplattform für gebrauchte Netzwerk-Komponenten auf. Die Spielregeln: Sie melden uns, welche Produkte/Komponenten Sie anbieten/suchen mit Ihrer Preisvorstellung. Ihr Angebot wird in anonymer Form auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de und im Netzwerk Insider veröffentlicht. Interessenten melden sich per Mail, mit dem Fax-Formular (unten) oder über den Web-Server bei uns. Wir stellen den Kontakt zwischen Anbieter und Nachfrager her. Wir erhalten vom Verkäufer für diese Leistung 10% Provision auf den erzielten Kaufpreis. Davon stellen wir die Hälfte ausgewählten Schulen als Spende zum Aufbau ihres Internet-Zugangs oder ihres internen Netzwerks zur Verfügung. Der Kaufvertrag entsteht direkt zwischen Käufer und Verkäufer. Wir selber haften in keiner Form für die Qualität oder Nutzbarkeit der Komponenten.

Fax an 02408/955-399

☐ **Ich biete**
☐ **Ich suche**
☐ **Antwort auf Gesuch**
☐ **Antwort auf Gebot**

☐ _____

Produkt/Komponente/Release/Software

_____

_____

_____

_____

Preisvorstellung_____

_____

Ansprechpartner

_____

Firma

_____

Ort

_____

Straße

_____

Telefon, Fax

_____

eMail

Gebote

Adapter

Token Ring Karten ISA und PCI, Olicom, IBM, 50 Stck., DM 20,-- B1201

Hubs, Repeater, Sternkoppler Concentrator Ringleitungsverteiler

Cabletron Repeater Module FOMIN, 5 Stck., DM 100,-- B1205

IBM Token Ring Verteiler, 20fach 4 Stck.; 8fach (passiv), 6 Stck.; 1 Token Ring MAU, zusammen DM 300,-- B1203

Multiplexer Steuereinheiten Controller

IBM 3745-A31A Comm. Contrl. mit 3746-900 Erweiterungseinh. Schaltsystem von Control Ware System Specification auf Anfrage, verfügbar Ende Januar, 5 Stck, VS B0103

Racal Datacom Premnet 5000, jeweils mit: 1x Singlemode 1300 nm, 25 dB, 1x Switch, 5x Ethernet I/O, 1x Dual DS 1A, 1x Network MGT, 2x AC Power Supply, 2 Stck. Gesamtpreis DM 4.000,-- B0104

Switches Brücken

Cabletron 2-Port-Bridges, 5 Stck, DM 20,-- B1206

IMB 8230 TRN-Units, IVS+RJ45 Ports,mehrere Stck., VS B0102

Sonstiges

Cabletron Ersatz-Netzteil für MMAC-3, 8 Stck., DM 350,-- B1204

Gesuche

Hubs, Repeater, Sternkoppler Concentrator Ringleitungsverteiler

Cabletron Repeater Modul TPMIN-22 oder TPMIN-24 (für MMAC), 5 Stck., DM 100,-- S1203

Smart CAU Plus Madge Nr. 55-29, 1 Stck., DM 1000,-- S1202

Smart LAM Plus UTP Madge Nr. 55-50, 3 Stck., DM 700,-- S1201

Router

Cisco 2611 Dual Eth. Modular Router oder Cisco 2621 Dual 10/100 Eth. Router, 2 Stck., DM 1500,-- bzw. DM 2000,-- S1204

Cisco Router, 3000 Serie IOS V. ab. 11.0, 1 Stck., VS S0103

Switches Brücken

Enterasys (Digital) VNSSwitch 900 CG, 1 Stck., VS S0104

Sonstiges

Kabel für 2 Baynetworks BayStack 28115 um sie zu kaskadieren, 1 Stck., VS S0102

Weitere Gebote/ Gesuche

finden Sie auf dem Web-Server der ComConsult Akademie unter www.comconsult-akademie.de