Projektarbeit

Thema: „Bewertung und Realisierung einer Public Key Infrastruktur für außendienstorientierte Unternehmen“

Prüfer:
Prof. Dr. Hellberg

Verfasser:
Nicolas Halbach
Strasse
Wohnort

3.Praxisquartal
Studiengang Wirtschaftsinformatik

Eingereicht am:
08 April 2002

Abstract

Das Internet hat sich in den letzten Jahren zu einem so globalen Medium entwickelt. Es wird durch Unternehmen nicht nur als Marketing-Instrument verstanden, sondern es werden zunehmend auch die Geschäftsprozesse mit Geschäftspartnern und Kunden Schritt für Schritt auf das Internet verlagert. Da das Internet einer ganzen Reihe von Gefahren unterliegt, werden an den Schutz der Kommunikation über das öffentliche Netz hohe Anforderungen gestellt.

Ziel dieser Arbeit ist es, die Verfahren aufzuzeigen, welche die Kommunikationswege schützen. Dazu werden die Kryptographieverfahren erläutert und einer rechtlichen Betrachtung unterzogen. Dabei wird festgestellt, dass kryptographische Verfahren allein keinen im Sinne der Kommunikationssicherheit hinreichenden Schutz bieten. Aus diesem Grund werden verschiedene Vertrauensmodelle untersucht. Es stellt sich heraus, dass nur mit Hilfe des hierarchischen Vertrauensmodells eine einigermaßen sichere Umgebung geschaffen werden kann, wobei eine vollkommende Sicherheit gerade im IT-Bereich eine Illusion bleibt. Auf diesem hierarchischen Vertrauensmodell basiert die Public Key Infrastruktur (PKI), die in dieser Arbeit im Mittelpunkt steht. Eine PKI findet ihre Grundlagen in den asymmetrischen Kryptographieverfahren und darf nicht als eigenständige Technologie verstanden werden. Vielmehr wird eine PKI als eine Organisationsform betrachtet, die Anwendungen, die auf Verschlüsselungstechniken aufbauen, ein zusätzliches Maß an Sicherheit gewährleistet. Dazu werden die Verfahren und Komponenten einer PKI erläutert. Dabei stellt sich heraus, dass der Aufbau und Betrieb der PKI weniger eine Frage von Aufwand in Hard- und Software ist, als vielmehr eine optimal abgestimmte Organisation erfordert. Eine Return-on-Investment Untersuchung soll verdeutlichen, dass mit einer PKI nicht nur ein höheres Maß an Sicherheit erreicht werden kann, sondern dass durch eine Vielzahl von Geschäftsprozessen, die durch die PKI verbessert werden können, auch erhebliche Einsparungen realisiert werden können.

Die anfängliche Euphorie auf dem PKI-Markt ist aber aufgrund fehlender Interoperabilität der PKI-Produkte einer gewissen Ernüchterung gewichen. Die verschiedenen Problembereiche werden in dieser Arbeit besprochen. Dabei zeigt sich, dass erst durch vorgeschriebene Standards und international kooperierende Arbeitsgruppen ein einheitlicher Maßstab, sowohl in gesetzlicher als auch in technischer Hinsicht, gefunden werden muss, damit eine PKI mittelfristig den Einsatz in der Breite der Unternehmen findet.

Inhaltsverzeichnis

Seite

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ARPANET ..... Advanced Research Projects Agency Network
B2B ..... Business to Business
B2C ..... Business to Consumer
BDSG ..... Bundesdatenschutzgesetz
BSI ..... Bundesamt für Sicherheit in der Informationstechnologie
BVG ..... Bundesverfassungsgericht
CA ..... Certification Authority
DES ..... Data Encryption Standard
DSL ..... Digital Subscriber Line
EDV ..... Elektronische Datenverarbeitung
EESSI ..... European Electronic Signature Standardisation Initiative
GG ..... Grundgesetz
HGB ..... Handelsgesetzbuch
ISDN ..... Integrated Services Digital Network
ISIS ..... Industrial Signature Interoperability Specification
IT ..... Information Technology
IuKDG ..... Informations- und Kommunikationsdienste-Gesetz
KontraG ..... Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
LAZ ..... Lösungs- und Angebotszentrum
LAN ..... Local Area Network
LDAP ..... Leightweight Directory Access Protocol
NSA ..... National Security Agency
PIN ..... Persönliche Identifikationsnummer
PKCS ..... Public Key Cryptography System
PKI ..... Public Key Infrastruktur
PKIX Public-Key-Infrastruktur-X.509v3-Arbeitsgruppe
PSE ..... Personal Security Environment
RA ..... Registration Authority
RegTP ..... Regulierungsbehörde für Post und Telekommunikation
RSA-Verfahren ..... Rivest-, Shamir-, Adleman-Verfahren
SigG ..... Signaturgesetz
SSL ..... Secure Socket Layer
TC ..... Trust Center
TCO ..... Total-Costs-of-Ownership
TCP/IP ..... Transmission Control Protocol/Internet Protocol
VPN ..... Virtuelles Privates Netzwerk

1 Einleitung

EDV-unterstützte Prozesse sind aus der heutigen Unternehmenswelt nicht mehr wegzudenken. Dabei spielen auch der Einsatz von Netzwerken und die Datenübertragung zwischen verteilten Standorten eine immer wichtiger werdende Rolle. Die klassische Nutzung des Internets durch Unternehmen tritt immer mehr in den Hintergrund. Stattdessen führt die Verlegung von Geschäftsprozessen im Kontakt mit Kunden und Partnern zu umfangreichen Synergieeffekten Fehlende Kommunikationssicherheit stellt bei derartigen Prozessen aber ein nicht zu unterschätzendes Risiko dar. Sensible Daten müssen während der Übertragung über das Netz (i.a. das Internet) geschützt werden. Unbefugten Dritten muss dadurch der Zugriff auf vertrauliche Firmen- oder Kundendaten unterbunden werden.

In dieser Projektarbeit werden die Sicherheitsmechanismen betrachtet und bewertet, die Kommunikationssicherheit gewährleisten. Dabei wird zunächst erklärt, warum die Kommunikationssicherheit aufgrund der Entwicklung des Internets einen sehr wichtigen Status eingenommen hat. Kryptographische Verfahren, die Kommunikationssicherheit gewährleisten werden aufgezeigt und aus rechtlicher und sicherheitstechnischer Sicht betrachtet. Folgend wird beschrieben, warum kryptographische Verfahren alleine heute nicht mehr ausreichen, um rechtlichen Bestimmungen zu erfüllen. Im Mittelpunkt dieser Arbeit steht dabei die „Public Key Infrastruktur“ (PKI), die derzeitig den bestmöglichen Schutz für eine – im Sinne der Kommunikationssicherheit - sichere Datenübertragung bietet. Der Aufbau und die Komponenten einer PKI werden besprochen und die technisch erforderlichen Applikationen und Anschaffungen erklärt. Daran schließt sich eine kritische Betrachtung des derzeitigen PKI-Marktes an und es werden die Synergieeffekte mittels eine Kosten-Nutzen-Analyse beschrieben, die sich bei einem PKI-Einsatz ergeben.

Im Anhang A dieser Projektarbeit wird ein konkretes Angebot einer PKI für einen Kunden, der außendienstorientiert tätig ist, erarbeitet. Dabei wird zum einen auf die technische Realisierung eingegangen und zum anderen wird ein konkretes preisliches Angebot für die entwickelte Lösung erstellt.

Die technische Realisierung der PKI Lösung finden bei der Deutschen Telekom AG in der Abteilung „Lösungs- und Angebotszentrum“ (LAZ) im Team E-Business statt.

2 Sicherheitsaspekte

In diesem Kapitel wird auf die Entwicklung des Internets zum globalen Medium eingegangen und es werden die mit dem rasanten Wachstum dieses Kommunikationsnetzes einhergehenden Gefahren und Sicherheitsmängel aufgezeigt. Weiter wird der Begriff Kommunikationssicherheit eingeordnet und die Grundbegriffe

der sicheren Kommunikation erklärt. Die Erläuterung der rechtlichen Empfehlungen und Vorschriften beschließen dieses Kapitel.

2.1 Entwicklung des Internets zum globalen Medium

Das Internet hat sich in den vergangenen Jahren wie kein anderes Medium in der Gesellschaft verbreitet. Es offenbart inzwischen revolutionäre Kommunikationsmöglichkeiten und bietet ein nahezu unübersehbares Spektrum an geschäftlichen und privaten Anwendungen. Die Entwicklung des Internets basiert auf den Anfängen des ARPANET (Advanced Research Projects Agency Network) im Jahre 1969.[SEL00, S.7] Ziel war es damals, die Datentechnik und die Übertragungsqualität der damaligen Kommunikationstechnik zu verbessern und die Kosten zu verringern. Militärisch versprach man sich, das Netz durch die neue, heterogene Struktur unempfindlich gegen jegliche Art von Netzausfall zu machen, also auch gegen mögliche atomare Gegenschläge. Mit der ersten graphischen Bedienungsoberfläche Anfang der 90er Jahre verbreitete sich das Internet auch in der Masse der Bevölkerung, während die Nutzung vorher nur den Universitäten oder dem Militär vorbehalten war. Ende 2001 nutzten bereits 43,6% der Deutschen das Internet.[1] Auch gilt es als Schlüsseltechnologie für die gesamte Wirtschaft. Kaum ein anderes Medium hat in so kurzer Zeit die Geschäftsprozesse der Unternehmen so grundlegend verändert. Es gibt kaum noch Wirtschaftsbranchen, die auf die Nutzung des weltweiten Datennetzes verzichten. Während die Unternehmen das Internet Mitte der 90er Jahre hauptsächlich als Marketing-Instrument benutzten, ist es inzwischen zu einem allumfassenden Informations- und Kommunikationsmedium geworden. Der Handel über das Internet (e-commerce) zwischen verschiedenen Unternehmen (business to business) oder zwischen Unternehmen und Endverbraucher (business to consumer) ist stark ansteigend, Unternehmensfilialen werden über das Internet vernetzt und in 83% der Unternehmen gehört die e-Mail Nutzung mittlerweile zum Geschäftsalltag.[2]

2.2 Gefahren des Internets

Das signifikante Wachstum und die steigenden Benutzerzahlen des Internets bergen zahlreiche Risiken und Gefahren. Die Einführung von IT-Systemen in allen wichtigen Tätigkeitsbereichen, die starke Zunahme der Datenverbindungen und Übertragung von Daten führen dazu, dass jedes Unternehmen heutzutage auf das reibungslose Funktionieren der EDV-Infrastruktur angewiesen ist. Folgeschäden bei Störungen und Ausfällen beschränken sich nicht nur mehr auf betroffene Einzelorganisationen, sie betreffen aufgrund der steigenden Vernetzung und Interdependenz auch die Kooperation mit Geschäfts- und Kommunikationspartnern. Letztlich seien es sogar Arbeitsplätze, die direkt vom Funktionieren der IT abhängen würden. [BSI01, S.7] Die größte Gefahr geht im Bereich der IT-Sicherheit von der Computerkriminalität aus.

[1] Vgl. hierzu http://www.golem.de/0201/17753.html
[2] Vgl. hierzu http://www.ecin.de/news/2001/08/27/03056/

Abbildung 1 zeigt den monetären Schaden, unterteilt nach Angriffstypen, der im Jahr 2000 durch unautorisierten Zugriff auf ein PC-System entstanden ist. Befragt wurden 538 US-Unternehmen. Der direkte Schaden durch Computerkriminalität geht inzwischen in die Millionen, wobei viele Unternehmen ihren Schaden aus Angst vor Schädigung des Firmenimage nicht anzeigen - oder im schlimmeren Fall - gar nicht bemerken. Der indirekte Schaden, der durch oben beschriebene Angriffe ausgeht, ist aber noch viel größer. Jedes zweite deutsche Unternehmen fürchtet „Hacker" als größtes Sicherheitsrisiko für sein e-Commerce-System, stellte ECIN[3] fest. Abbildung 2 zeigt eine Umfrage unter amerikanischen Unternehmen zu den Hindernissen des e-Commerce. Der volkswirtschaftliche Schaden liegt jedoch weitaus höher. Die Unternehmen halten sich mit Investitionen in den e-Commerce zurück und der Verbraucher ist - angesichts der erhöhten Anzahl von Sicherheitsvorfällen - zurückhaltend.[4] Allein Computerviren hätten im letzten Jahr ca. 14 Milliarden Euro volkswirtschaftlichen Schaden verursacht.[5] Das „Computer Security Institute" weist darauf hin, dass ein Großteil der Angriffe mächtigen, finanzstarken Organisationen zuzurechnen ist. „Dem Vernehmen nach sind nicht nur Konkurrenzunternehmen aktiv, sondern es wird in Fachkreisen davon ausgegangen, dass auch andere staatliche Stellen versuchen, die Datennetze zu kontrollieren."[6] Der Bereich der Wirtschaftsspionage ist in der Tat nicht zu unterschätzen. So wurde davor gewarnt, dass „jedes Kommunikationsmedium von Telefon und –fax über Fernschreiber bis zur Datenautobahn im Internet fest im Griff des amerikanischen Nachrichtendienst NSA ist." Schätzungen zufolge würden täglich bis zu drei Milliarden Sendungen abgefangen.[7]

Ein in der Literatur zu Recht immer wieder angeführtes Beispiel für die nachteiligen monetären Auswirkungen von Wirtschafts- bzw. Konkurrenzspionage ist das Abhören einer Nachricht der Firma Siemens im Jahre 1993. [ULF99, S.32] Der Großkonzern hatte sich um den Bau eines Hochgeschwindigkeitszuges in Südkorea nach dem Vorbild des ICE beworben. Jedoch fing der französische Geheimdienst ein Fax mit dem Angebot von Siemens ab. Die Franzosen waren nun in der Lage, das Angebot zu unterbieten. Für Siemens entstand dadurch ein Milliardenschaden. Auch die Existenz „eines globalen Abhörsystems für private und wirtschaftliche Kommunikation" (Abhörsystem ECHELON) wird im Europäischen Parlament nicht mehr verschwiegen.[8] Aber nicht nur Großkonzerne sind von den Gefahren der Kommunikation betroffen. Auch Kleinstunternehmen oder sogar einzelne Personen sind durch Manipulation der Kommunikation gefährdet. Ein gefälschter Absender einer e-Mail kann nicht nur eine

[3] Electronic Commerce InfoNet http://www.ecin.de/news
[4] Vgl. hierzu http://www.ecin.de/news/2000/04/06/00722
[5] Vgl. hierzu http://www.afp.com/ext/deutsch/presdok/presdokinet/011123142231.115gfv8k.html
[6] Bundesministerium für Wirtschaft und Technologie, Sicherheit im Internet: http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=57&tdid=1148
[7] http://www.ndr4.de/forum/archiv/20000311.html
[8] siehe hierzu „Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echolon)" unter www2.europarl.eu.int

Schädigung des Image hervorrufen. Durch das Vortäuschen[9] von Nachrichten kann auch ein erheblicher finanzieller Schaden entstehen. Ein Beispiel einer Internetseite, die das Absenden von anonymen e-Mails ermöglicht, ist in Abbildung 3 zu sehen. Abbildung 4 stellt den Empfang der anonymen e-Mail dar.

2.3 Schwächen von TCP/IP

Die Protokollfamilie TCP/IP (Transmission Control Protocol/Internet Protocol), die die im Internet verwendeten Protokolle zusammenfasst, weist zudem zahlreiche Schwächen auf. Zahlreiche Mängel, die sich auch in der Praxis zeigten, konnten nicht behoben werden, da es nicht einfach war, Protokolle, die von Millionen Computern verwendet wurden, durch neuere Versionen auszutauschen, ohne dabei ein Chaos zu verursachen. „Zu den zahlreichen Mängeln, die TCP/IP ursprünglich aufweist, gehört durchweg der Mangel an Sicherheit." [SCH01, S.28] Als wichtigster Nachteil für diese Arbeit ist zu nennen, dass in TCP/IP nicht verschlüsselt wird.

2.4 Anforderungen an die Sicherheit verteilter Standorte

Die Sicherheitsrisiken einzelner Desktop-Arbeitsplätzen oder bei einem Intranet, also einem Netzwerk, das auf Basis der Internettechnologie eine leistungsfähige Infrastruktur für Informationsaustausch, Kommunikation und Applikationen innerhalb eines Unternehmens bildet und dessen Daten nur einer geschlossenen Benutzergruppe verfügbar sind [Det01], sind überschaubar. Dagegen ist die Angriffsfläche bei verteilten Standorten und verteilten Systemen weitaus größer. Unter verteilten Systemen versteht man eine Kollektion unabhängiger Computer, die den Benutzern als Einzelcomputer erscheinen. Es wird impliziert, dass die Computer miteinander verbunden sind und dass die Ressourcen wie Hardware, Software und Daten gemeinsam benutzt werden.[10] Große Vorteile bieten verteilte Systeme in Bezug auf Wirtschaftlichkeit, Zuverlässigkeit und Wachstumspotential, während die mangelnde Sicherheit einen großen Nachteil darstellt. Zur Realisierung von Electronic-Commerce-Systemen im Internet sei der Einsatz von verteilten Technologien jedoch unerlässlich. Dies gelte insbesondere für Anwendungsbereiche wie Online-Portale, Online-Auktionen, Online-Shops und e-Procurement.[11] Anwendungen dieser Art müssen also besonders geschützt werden. Dieselbe Sicherheitsproblematik gilt für verteilte Standorte. Bisher ging es bei der Computersicherheit hauptsächlich um die Begrenzung von Zugriffen Unbefugter. Mittlerweile ist die „Maximierung des Zugriffes für berechtigte Personen" [NAE99] das Hauptziel in Unternehmensnetzwerken, um Partnern den Zugriff auf Unternehmensdaten zu gewährleisten. So gibt es keine stark geschützten Grenzen mehr und es muss deshalb, neben der Sicherheit vor Eindringlingen in das System, bei verteilten Systemen und verteilten Standorten das

[9] zu Englisch: „Spoofing"
[10] nach Andrew Tanenbaum
[11] Vgl. hierzu http://vsys-www.informatik.uni-hamburg.de/teaching/kvvtext.phtml/52

Augenmerk in besonderem Maße auf die Sicherheit der Kommunikation, also der Übertragung von Daten jeglicher Art zwischen den Kommunikationspartnern, gelegt werden.

2.5 Kommunikationssicherheit

Die Sicherheit, die für die Übertragung von Daten zwischen zwei Kommunikationspartnern nötig ist, wird Kommunikationssicherheit genannt. Sie ist ein Teilgebiet der Computersicherheit und lässt sich wie folgt einordnen.

2.5.1 Einordnung der Kommunikationssicherheit

Der Begriff Kommunikationssicherheit ist eine Teilmenge der Computer- oder IT-Sicherheit. Da der Begriff Sicherheit im Deutschen eine zu allgemeine Bedeutung hat, wird im Englischen differenziert zwischen Computer-Security und Computer-Safety unterschieden. Mit Computer-Safety wird der Schutz vor unbeabsichtigten Schäden bezeichnet. Dazu zählt man das unbeabsichtigte Löschen, falsche Bedienung, defekte Geräte oder höhere Gewalt z.B. durch Unwetter. Unter Computer-Security wird dagegen den Schutz vor vorsätzlichen bzw. geplanten Schäden wie Sabotage, Hackereinbrüche oder das Ausspähen geheimer Daten verstanden. Da die Sicherheit unvernetzter Rechner eine inzwischen eher untergeordnete Rolle spielt[12], legt man das Augenmerk stärker auf die Netzwerksicherheit, die sich in die „Sicherheit vor Eindringlingen“ und „Kommunikationssicherheit“ unterteilt. In Abbildung 5 ist die Kommunikationssicherheit genauestens eingeordnet.

2.5.2 Definition der Kommunikationssicherheit

Die Kommunikationssicherheit befasst sich mit dem Schutz von Kommunikationsverbindungen zwischen zwei oder mehreren Partnern.[13] Darunter ist die Sicherung der Information und der Daten während ihrer Übertragung mittels Telekommunikation (Funk, leitungsgebundene oder optische Kommunikation) zu verstehen.

2.6 Grundlagen der Kommunikationssicherheit

In offenen Netzen sind Daten prinzipiell jedem zugänglich. Darum müssen Daten und Informationen auf verschiedene Arten und Weisen geschützt und abgesichert werden. Damit sollen folgende Szenarien verhindert werden:

- Vortäuschung und Verfälschung von Nachrichten und Informationen
- Online-Shopping und Online-Banking Betrug
- Illegale, unseriöse Online-Geschäftspraktiken
- Verstöße gegen den Datenschutz

[12] Vgl. Gliederungspunkt 2.3
[13] siehe hierzu http://www.kes.info/_lexikon/lexdata/kommunikationssicherheit.htm

- Rechtsunsicherheit im Cyberspace [KYC, S.30]

Abbildung 6 zeigt die Bedrohungen des Internets, unterteilt nach Schadenshöhe und Eintrittswahrscheinlichkeit. Die Kommunikationssicherheit sieht für die Sicherung von Informationen und Daten vier grundlegende Prinzipien vor.

2.6.1 Vertraulichkeit

Bei der Übertragung von Daten darf ein Unbefugter keine Einsicht in die Daten bekommen. Nur der designierte Empfänger soll die Daten lesen können.

2.6.2 Integrität

Integrität[14] bedeutet, dass Daten auf dem Übertragungsweg nicht verändert werden dürfen. Damit ist gemeint, dass ein nicht autorisierter Dritter die Daten nicht unbemerkt verfälschen darf.

2.6.3 Authentizität

Authentizität[15] bedeutet, dass der Urheber von Daten eindeutig zu identifizieren sein muss. Damit soll verhindert werden, dass Daten unter falschem Absender versendet werden und der Empfänger der Daten getäuscht wird.

2.6.4 Verbindlichkeit

Der Urheber einer Nachricht muss für diese auch verantwortlich gemacht werden können. Nachrichten sollen im Nachhinein also nicht abgeleugnet werden können (Non-Reputation)[16]. Damit soll eine Rechtssicherheit zwischen Sender und Empfänger sichergestellt werden.

2.7 Rechtliche Situation

Der Gesetzgeber sieht für den Schutz der Kommunikation zahlreiche Empfehlungen und Gesetze vor. Während das IT-Grundschutzhandbuch des „Bundesamt für Sicherheit in der Informationstechnologie“ (BSI) nur empfehlende Wirkung besitzt, müssen vor allem Kapitalgesellschaften sowie Branchen, in denen der Datenschutz eine besondere Rolle spielt, entsprechende Gesetze beachten.

2.7.1 Empfehlungen des BSI

Im IT-Grundschutzhandbuch wird vom „Bundesamt für Sicherheit in der Informationstechnologie“ (BSI) auf denkbare Sicherheitslücken in der IT-Sicherheit hingewiesen und erforderliche Maßnahmen empfohlen. Als Grundbedrohungen gelten neben fehlerhafter Hardware, Sabotage und Computerviren auch das unberechtigte Mitlesen von Informationen. Das BSI spricht jedoch lediglich Empfehlungen aus, die sich bei Nichteinhaltung nur im Schadensfall nachteilig für die Unternehmen auswirken. Als sogenanntes Maßnahmenbündel empfiehlt das BSI für den Bereich der Kommunikationssicherheit im organisatorischen Bereich u.a. die „Entwicklung eines

[14] Integrität *lat*. *Integritas*: Makellosigkeit, Unbescholtenheit, Unversehrheit (Quelle: Duden, Das große Fremdwörterbuch)
[15] Authentizität: Echtheit, Zuverlässigkeit, Glaubwürdigkeit [DUD]
[16] Non-Reputation = Nicht Anerkennung

Kryptokonzeptes“ und die „Auswahl geeigneter kryptographischer Verfahren“ und im personellen Bereich die „Schulungen zu IT-Sicherheitsmaßnahmen und die „Einführung in kryptographische Grundbegriffe“. Als weitere Sicherheitsmaßnahmen werden u.a. der „Einsatz eines Verschlüsselungsproduktes für tragbare PCs“, der „Einsatz von Verschlüsselung und digitaler Signaturen“ sowie „sicherheitstechnische Anforderungen an den Kommunikationsrechnern“ definiert. [BSI01, Abs. 3, S.17]

2.7.2 Vorschriften durch die Gesetze

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KontraG) ist ein Artikelgesetz, das insbesondere das Aktiengesetz und das Handelsgesetzbuch (HGB) mit dem Ziel ändert, die Unternehmenskontrolle zu verbessern. „Der Vorstand einer Kapitalgesellschaft hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“[17] Mit dem im Mai 1998 verabschiedeten Gesetz werden Geschäftsführer und Vorstände im Schadensfall gegenüber den Anteilseignern persönlich schadensersatzpflichtig gemacht. Als besonders gefährdend werden sensible Bereiche wie Wirtschaft, Polizei, Justiz, Finanzverwaltung, Gesundheitswesen, Behörden und Verwaltung, Politik, Bundeswehr, Schulwesen, Universitäten und Banken angesehen.[18] Gerade in diesen Bereichen hat der Datenschutz, der im Bundesdatenschutzgesetz (BDSG) geregelt wird, eine wichtige Bedeutung. In §9 BDSG werden zur Vorsorge entsprechende technische und organisatorische Maßnahmen verlangt . So soll verhindert werden, dass „Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden.“[19] In verschiedenen Berufszweigen, wie im Gesundheitswesen, postulieren spezielle Gesetze darüber hinaus überaus strenge datenschutzrechtliche Maßnahmen. So werde die Gewährleistung der ärztlichen Schweigepflicht und die Gesundheit des Patienten zunehmend von der fehlerfreien und nachweislich nicht manipulierten Telekommunikation abhängig sein.[20] Beide Gesetze fordern, in erster Linie zum Gläubigerschutz, dass Unternehmen umfangreiche Maßnahmen zum Schutz der eigenen Ressourcen und zum Schutz der zu verwaltenden Daten treffen. Auch das Informations- und Kommunikationsdienste-Gesetz (IuKDG) regelt das „Ausspähen von Daten“ und die „Verletzung von Privatgeheimnissen.[21]

2.8 Zusammenfassung

Die Entwicklung und das unaufhaltsame Wachstum des Internets und die damit verbundenen Gefahren, die zum einen auf technische Mängel und zum anderen auf die rasante Entwicklung des Internet zurückzuführen sind, erfordern, dass Unternehmen Maßnehmen treffen, um ihre Kommunikationswege abzusichern.

[17] siehe hierzu: BGBl I 1998/24
[18] Siehe hierzu „Pannen beim Probelauf“, Der Spiegel 7/1998, Seite 75
[19] http://www.funkschau.de/heftarchiv/pdf/1999/fs16/f9916066.pdf
[20] Vgl. hierzu „Europäisches Institut für Systemsicherheit“ Report 98/3 1998, S.5
[21] siehe hierzu IuKDG §202a und §203

Rechtliche Vorschriften verpflichten Unternehmen dazu. Es gibt kaum Fälle, in denen digitale Informationen keinen Wert besitzen. Weiterhin führen ungeschützte Kommunikationswege zu einem Vertrauensverlust und Imageschaden in der Öffentlichkeit und bei Partnern, der nicht quantifizierbar ist.

3 Kryptographie

Die für die Kommunikationssicherheit erforderlichen Prinzipien, Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit, spielen auf unterschiedliche Art und Weise im täglichem Geschäftsleben eine Rolle. Ziel ist es, diese Prinzipien auch in der Welt des e-Business bereitzustellen. Die Techniken zur Bereitstellung der elektronischen Pendants zu diesen Prinzipien basieren auf der Kryptographie. Es wird eine Einführung in die Kryptographie gegeben und die Arbeitsweise der verschiedenen kryptographischen Verfahren, insbesondere unter mathematischen Gesichtspunkten, erläutert. Außerdem werden die Verfahren aus sicherheitstechnischer Sicht kritisch untersucht.

3.1 Einordnung und Definition

„Kryptographie[22] ist die mathematische Wissenschaft, die sich mit der Absicherung von Nachrichten – ursprünglich nur zum Zwecke der Geheimhaltung, inzwischen aber weit vielfältiger eingesetzt – beschäftigt.[BUC98] Inzwischen ist unter der Kryptographie neben der Vertraulichkeit auch die Datenintegrität, Authentizität und Verbindlichkeit zu verstehen. Damit soll die Sicherheit elektronischer Transaktionen erhöht werden. Die Kryptographie ist, wie in Abbildung 5 zu sehen, das wichtigste Teilgebiet der Kommunikationssicherheit. Kryptographie und Kryptoanalyse, welche sich nicht mit der Verschlüsselung, sondern mit der unbefugten Entschlüsselung von bereits verschlüsselten Daten beschäftigt, werden unter dem Oberbegriff Kryptologie zusammengefasst.[SCH01, S.14]

3.2 Verschlüsselungsverfahren

In der Kryptographie gibt es im Wesentlichen zwei unterschiedliche Verfahrensweisen, die symmetrischen Verfahren und die asymmetrischen Verfahren. Beide Verfahren basieren auf sogenannten Schlüsseln. Unter Schlüsseln wird je nach Verfahren ein Passwort, eine Geheimnummer oder eine Folge von Bits verstanden. Mit Hilfe des Schlüssels ist es ohne weiteres möglich, eine verschlüsselte Nachricht zu entschlüsseln. Ohne Kenntnis des Schlüssels soll die Entschlüsselung jedoch unmöglich sein, selbst wenn das Verfahren bekannt ist. Auf diese Weise kann bei jeder Kommunikation das gleiche Verschlüsselungsverfahren verwendet werden; dabei werden nur verschiedene Schlüssel genutzt. Abbildung 7 verdeutlicht diesen Zusammenhang. Kryptographie basiert auf dem Konzept, dass sich bestimmte

[22] Kryptographie *gr*. : kryptein = verstecken, graphein = schreiben

Berechnungen zwar problemlos in eine Richtung durchführen lassen, aber nur sehr schwer reversibel sind. Der mathematische Hintergrund dieser sogenannten Einwegfunktionen sind Primzahlen, die multipliziert werden. Die Bildung des Produktes ist ohne weiteres möglich, die spätere Primfaktorenzerlegung ist unter der Annahme sehr großer Zahlen jedoch ein anerkanntes komplexes, mathematisches Problem. Kryptographische Algorithmen besitzen jedoch eine „Falltür", welche die Lösung des Problems in umgekehrter Richtung ermöglicht, sofern das Geheimnis, also der Schlüssel, bekannt ist.

3.2.1 Symmetrische Verfahren

Bei den symmetrischen Verfahren, auch „Secret-Key-Verfahren" genannt, benutzen Sender und Empfänger einer Nachricht den gleichen Schlüssel zum Ver- bzw. Entschlüsseln einer Nachricht. Symmetrische Schlüssel bestehen lediglich aus Zufallszahlen, die künstlich erzeugt werden. Dieser Schlüssel darf nur dem Sender und Empfänger bekannt sein, damit ein unautorisierter Zugriff von außen unterbunden wird. Problematisch gestaltet sich dabei die Schlüsselübergabe, da die Übertragung des Schlüssels vorher über einen unsicheren Kommunikationskanal erfolgen muss. Aus diesem Grund eignet sich das symmetrische Verfahren *allein* nicht für den Einsatz in öffentlichen Netzen. Zudem ist die Schlüsselverwaltung extrem aufwendig, da für jede Kommunikation ein neuer Schlüssel verwendet werden muss. Bei 100 beteiligten Personen sind schon 4950 Schlüssel zur sicheren Kommunikation nötig (n/2) * (n-1). Vorteilhaft wirkt sich bei den symmetrischen Verfahren aus, dass sie auf bewährten, jahrelang geprüften Algorithmen basieren und somit ziemlich sicher sind. Außerdem sind sie schnell und ermöglichen damit die schnelle Verschlüsselung größerer Datenmengen ohne wesentliche Beeinträchtigungen. Die zu übertragende Botschaft bzw. Daten sind damit kompakt und haben fast die gleiche Größe wie der ursprüngliche Klartext. Das bekannteste symmetrische Verschlüsselungsverfahren ist der DES („Data Encryption Standard"), der in den 70er Jahren von IBM entwickelt wurde und mit einer Schlüssellänge von 56 Bit arbeitet. Seit der DES-Schlüssel im Januar 1999 in nur etwa 22 Stunden berechnet werden konnte, gilt er als nicht mehr sicher.

3.2.2 Asymmetrische Verfahren

Asymmetrisches Verfahren, auch „Public-Key-Verfahren" genannt, stellen den Kommunikationspartnern zwei unterschiedliche Schlüssel zur Verfügung. Der Sender benutzt einen Public-Key, einen allgemein zugänglichen, öffentlichen Schlüssel des Empfänger, zum Verschlüsseln einer Nachricht. Nur der Besitzer des zum öffentlichen Schlüssel gehörigen Private-Keys, einem privaten Schlüssel, ist in der Lage, die Nachricht zu dechiffrieren. Durch den Einsatz des Public-Key-Verfahrens werden die Gefahren eines unsicheren Schlüsselaustausches umgangen, da eine vorherige Beziehung zwischen Sender und Empfänger beim Public-Key-Verfahren keine Voraussetzung ist.

Weniger umständlich als beim symmetrischen Verfahren ist daher auch die Schlüsselverwaltung. Da jeder Kommunikationsteilnehmer nur einen öffentlichen Schlüssel besitzen muss, ist die Anzahl der zu verwaltenden Schlüssel nur so groß wie die Anzahl der Teilnehmer selbst. Negativ muss die Struktur des asymmetrischen Verfahrens bewertet werden. Privater und öffentlicher Schlüssel sind zwar unabhängig, mathematisch jedoch miteinander verknüpft. Deshalb ist in der asymmetrischen Kryptographie im Allgemeinen ein längerer Schlüssel erforderlich. Dies wirkt sich nachteilig auf die Geschwindigkeit und die Kompaktheit der Datenübertragung aus. Asymmetrische Algorithmen können zwischen 10 und 100 mal langsamer als symmetrische Algorithmen sein. Genauso ist eine Datenmenge, die asymmetrisch verschlüsselt wird, weit aus größer als der ursprüngliche Klartext. Ronald Rivest, Adi Shamir und Leonard Adleman entwickelten 1978 das RSA-Verfahren, eines der bekanntesten Public-Key-Verfahren.

3.2.3 Hybride Verfahren

Beim Vergleich des symmetrischen mit dem asymmetrischen Verfahren fällt auf, dass in jedem Bereich, in dem eine Algorithmenklasse eine Schwäche besitzt, die andere ihre Stärke hat. Das asymmetrische Verfahren kann gerade bei langen Botschaften oder großen Datenmengen zeit- und ressourcenaufwendig sein. Dagegen sorgt das symmetrische Verfahren für Geschwindigkeit und Kompaktheit. Andererseits sorgt das asymmetrische Verfahren für Skalierbarkeit und einfache Schlüsselverwaltung. Sogenannte Hybridverfahren kombinieren deshalb die Vorteile der symmetrischen und asymmetrischen Verfahren. Die Ideallösung sieht wie folgt aus:

- Die Lösung muss sicher, schnell, kompakt und skalierbar sein
- Die Lösung darf nicht durch das Abfangen der Schlüssel gefährdet sein
- Die Lösung muss digitale Signatur und Nicht-Abstreitbarkeit unterstützen

Nachstehend wird das Verfahren beschrieben:

Nachdem der Empfänger einer Nachricht sein Schlüsselpaar, bestehend aus privatem und öffentlichen Schlüssel, generiert hat, muss er den öffentlichen Schlüssel bekannt machen. Der Sender bzw. der Computer des Senders erstellt nun einen symmetrischen Schlüssel und chiffriert die Nachricht, die übertragen werden soll. Um den Schlüssel sicher zu übertragen, wird dieser nun mit dem asymmetrischen Verfahren verschlüsselt. Der Sender verschlüsselt dazu den symmetrischen Schlüssel mit dem öffentlichen Schlüssel des Empfängers. Diese Operation wird als „Key-Wrapping“ bezeichnet. Als nächstes wird der eingepackte Schlüssel an die verschlüsselte Botschaft angehängt. Das Synonym für diese Kombination ist der „digitale Umschlag“. Der digitale Umschlag kann nun gefahrlos z.B. über das Internet gesendet werden, ohne dass eine Gefahr besteht. Selbst wenn der Umschlag abgefangen wird, kann ein Dritter keine Einsicht in die Nachricht nehmen. Erst der rechtmäßige Empfänger und Besitzer des privaten Schlüssels ist in der Lage, die

Nachricht zu entschlüsseln. Zunächst werden dazu die verschlüsselte Botschaft und der verpackte Schlüssel voneinander getrennt. Um auf die symmetrisch verschlüsselte Botschaft zugreifen zu können, muss der Empfänger den symmetrischen Schlüssel mit seinem privaten Schlüssel dechiffrieren. Der symmetrische Schlüssel wird nun zur Entschlüsselung der verschlüsselten Botschaft eingesetzt. Das asymmetrische Schlüsselpaar kann bei der nächsten Kommunikation wiederverwendet werden, der symmetrische Schlüssel, der deshalb auch Sitzungsschlüssel genannt wird, hat seine Aufgabe erfüllt. Abbildung 8 soll das Verfahren verdeutlichen: Der beschriebene Prozess bildet die Basis der meisten modernen Verschlüsselungslösungen, von verschlüsselten e-Mails oder Web-Sessions (z.B. SSL) bis hin zu Virtuellen Privaten Netzwerken (VPN).

3.3 Digitale Signatur

Die Vertraulichkeit ist mit dem oben beschriebenen Verfahren erfüllt. Zur sicheren Kommunikation ist aber auch ein Mechanismus nötig, der sicherstellt, dass Daten auf dem Übertragungswege nicht verändert wurden und wirklich vom vermeintlichen Absender bzw. von der vermeintlichen Entität[23] stammen und damit verbindlich sind. Um eine Nachricht auch digital zu unterschreiben, also zu signieren, muss das Public-Key-Verfahren nur umgekehrt werden. Dies zeigt, wie vielseitig das in den 70er Jahren von Whitfield Diffie und Martin Hellman eingeführte Verfahren ist. Die digitale Signatur hat ihre Grundlage im sogenannten Hashing[24].

3.3.1 Hashing

Hash-Algorithmen komprimieren große Datenabschnitte in einen sogenannten Fingerabdruck bzw. Digest. Dabei haben sie folgende Eigenschaften. Die Zeichenfolge ist für die Nachricht eindeutig. Selbst die Änderung eines einzigen Bits ergibt einen völlig anderen Hash. Die ursprüngliche Nachricht kann aus dem Hash nicht rekonstruiert werden. Es soll unmöglich sein, zwei Nachrichten zu finden, die den gleichen Hash ergeben. Hash-Werte dienen deshalb zur Sicherung der unverfälschten Übertragung von Dokumenten. Zu den wichtigsten Hash-Algorithmen gehören MD2, MD5 und SHA-I-Hash.[NAS01, S.41]

3.3.2 Der Einsatz der digitalen Signatur

Der Einsatz der digitalen Signatur erfolgt fast analog zum Verschlüsseln. Oft wird die digitale Signatur als Umkehrfunktion der Verschlüsselung bezeichnet. Während zum Verschlüsseln der öffentliche Schlüssel des Empfängers benutzt wird, wird zum Signieren der eigene private Schlüssel verwendet. Mit seinem eigenen privaten Schlüssel kann jeder Schlüsselinhaber mathematische Operationen durchführen, die kein anderer durchführen kann. Diese Fähigkeit bildet die Grundlage für die digitale Signatur. Mit dem privaten Schlüssel wird der Fingerabdruck bzw. Digest, der mit

[23] Eine Entität kann sowohl eine menschliche Person als auch ein Router oder ein Netzwerkknoten etc. sein
[24] zu deutsch: zerhacken

einem entsprechenden Hash-Algorithmus erstellt wurde, verschlüsselt und an die Nachricht angehängt. Nachricht und Digest werden zusammen versendet. Die Software des Empfängers trennt nun die Nachricht vom verschlüsselten Digest. Mit Hilfe des Public-Keys des Senders entschlüsselt der Empfänger nun den Fingerabdruck. Im nächsten Schritt erstellt der Empfänger aus der Klartext-Nachricht mit dem gleichen Hash-Algorithmus des Senders ebenfalls einen Digest. Beide Fingerabdrücke werden nun verglichen. Stimmen sie überein, so wurde die Nachricht auf dem Übertragungswege nicht verändert und stammt auch wirklich vom vermeintlichen Absender, der den Versand nun nicht mehr abstreiten kann. Abbildung 9 verdeutlicht den Vorgang der digitalen Signatur. Da es sich beim Thema „digitale Signatur“ um ein relativ junges Betätigungsfeld handelt, treten bei der Verwendung des Begriffes „digitale Signatur“ immer wieder Missverständnisse auf. Unter den oft synonym verwendeten Begriffen „elektronische Signatur“ oder „elektronische Unterschrift“ ist keinesfalls dasselbe zu verstehen, was mit dem Begriff „digitale Signatur“ gemeint ist. Mit einer eingescannten Unterschrift hat die digitale Signatur nämlich gar nichts zu tun. Eine digitale Signatur wird – wie oben beschrieben – mittels Einsatzes spezieller Verschlüsselungstechniken erzeugt und umgeht dadurch der Manipulation durch Dritte.[25]

3.4 Rechtlicher Hintergrund von Verschlüsselung und Signatur

Die oben beschriebenen kryptographischen Verfahren, Verschlüsselung und digitale Signatur, bedürfen vor dem Einsatz einer rechtlichen Betrachtung. Unterschiedliche Beschränkungen versagen manchem kryptographischen Algorithmus den Einsatz. Länderspezifische Gesetze erlauben nicht überall den Einsatz von Verschlüsselungstechniken. Die digitale Signatur unterliegt dagegen fast keinen rechtlichen Vorschriften. Dennoch muss vor dem Einsatz der digitalen Signatur geprüft werden, in welcher Form sie eingesetzt werden soll. Der Gesetzgeber stellt hier lediglich Anforderungen, die eine digitale Signatur, vor allem für die rechtliche Gleichsetzung mit der realen handschriftlichen Unterschrift, erfüllen muss.

3.4.1 Verschlüsselung

Im Zusammenhang mit der staatlichen Überwachung und Kontrolle der Verschlüsselung von Kommunikationsverbindungen stellt sich nicht erst seit den Terroranschlägen vom 11.September 2001 die Frage, inwieweit staatliche Organisationen und Geheimdienste Einfluss auf Beschränkungen in der Kryptographie nehmen dürfen. Kontrovers sind die Diskussionen schon vorher gewesen. Nicht immer wurden sie sachlich geführt. Die Ursache liegt vor allem in der großen Zahl der Interessensgruppen. Vertreten wurden die grundsätzlichen Thesen, ob eine wirksame Verschlüsselung für jeden frei verfügbar sein sollte oder die Politik den Gebrauch von Kryptographie weiterhin beschränken sollte. Jahrelang war die Verschlüsselung nur

[25] Vgl. hierzu http://www.digital-law.net/knupfer/intro.htm

Reaktionen: „Signtrust“ beurteilt diese These als „interessante Aussage“, da diese quasi die einem Public-Key-Verfahren zugrundeliegende Methodik in Frage stellen würde. Laut SigG seien die Sicherheitsvorkehrungen aber so hoch, dass dieses Szenario auszuschließen sei. Bei Nicht-SigG-konformen Lösungen sei diese Sicherheitslücke aber durchaus vorhanden.

7.4 Zusammenfassung

Einige der in den Fachkreisen und Medien angesprochenen Risiken konnten von den Unternehmen relativiert werden. Jedoch gibt es in der Tat noch eine ganze Reihe von Schwierigkeiten, mit denen die Anbieter von Zertifizierungsdiensten und PKI zu kämpfen haben. Angefangen bei organisatorischen Problemen, die in der Wachstumsphase des PKI-Geschäftes sicherlich nicht unüblich sind, über ein bisher nur geringes Kundenpotential bis hin zu technischen Problemen, die z.T. sogar etwas elementarer sind und sich kurzfristig nicht beheben lassen. Die Interoperabilität zwischen den einzelnen Anwendungen ist dabei das Hauptproblem. Insgesamt vertreten aber alle TC die Meinung, dass Unternehmen in der mittleren Zukunft auf eine verlässliche PKI angewiesen seien und dass e-Business und e-Commerce auf Dauer ohne diese gemeinsame Vertrauensbasis nicht auskommen würden. Um die Probleme der Interoperabilität zu lösen, gibt es in Deutschland verschiedene Standardisierungsaktivitäten. Die wichtigste ist derzeit die „Spezifikation zur Interoperabilität der Trust-Center ISIS (Industrial Signature Interoperability Specification). Auf europäischer Ebene ist die European Electronic Signature Standardisation Initiative (EESSI) zu nennen.[43]

8 Gesamtbetrachtung

Es wurde in dieser Arbeit untersucht, wie durch die Verlagerung der heutigen Unternehmenskommunikation auf das Internet neue Risiken entstanden sind. Die Gefahren wurden bewertet und es wurde gezeigt, dass ein Unternehmen ohne hinreichende Schutzmechanismen im Wettbewerb enorme Nachteile erfahren kann. Die Wichtigkeit von Kommunikationssicherheit wurde gezeigt und unter Betrachtung der rechtlichen Vorschriften genauestens eingeordnet.

Die kryptographischen Verfahren, um Kommunikationssicherheit zu gewährleisten, wurden aufgezeigt, sowohl aus mathematischer Sicht als auch unter dem Aspekt einer sicherheitskritischen Begutachtung. Anhand der grundlegenden Problematiken der Kryptographieverfahren wurde verdeutlicht, dass ein Vertrauensmodell nötig ist, um den höchsten Sicherheitsstandard zu erfüllen. Die Vertrauensmodelle wurden untersucht und verglichen und es wurde erklärt, warum das hierarchische Modell, welches in einer Public Key Infrastruktur verwendet wird, die bestmögliche Lösung darstellt. Die Beschreibung der Aufgaben und der Einsatzgebiete einer PKI sowie die

Hauptkomponenten CA, RA und Zertifikate-Server schloss sich daran an. In einer Umfrage wurde untersucht, inwieweit sich Unternehmen gegenüber den Risiken der heutigen Kommunikation abgesichert haben und wie ihr Wissensstand bezüglich grundlegender PKI-Begriffe ist.

Danach wurden die wichtigsten Prozesse und Anwendungen innerhalb einer PKI beschrieben. Eine Return on Investment-Untersuchung und die Betrachtung der gegenwärtigen PKI-Probleme schlossen diese Arbeit ab.

Es stellte sich heraus, dass eine PKI für Unternehmen in Zukunft eine Schlüsselrolle im Wettbewerb einnehmen kann, da der Verzicht auf Kommunikationssicherheit inzwischen einen eindeutigen Nachteil auf dem Markt darstellt. Viele Branchen werden mit einer derartigen Lösung enorme Einsparungen realisieren können, wie die Return on Investment-Untersuchung gezeigt hat.

Der Erfolg der Einführung einer Public Key Infrastruktur für elektronische Unterschriften nach dem Deutschen Signaturgesetz bzw. der EU-Richtlinie in der Breite hängt wesentlich davon ab, ob eine genügend große Zahl von Anwendern das Rationalisierungspotential erkennen und für sich erschließen wollen. Neben der Einsatzfähigkeit elektronischer Unterschriften in bestehende oder neue Anwendungen ist dabei entscheidend, dass für den Endanwender eine komfortable Nutzung ermöglicht wird.

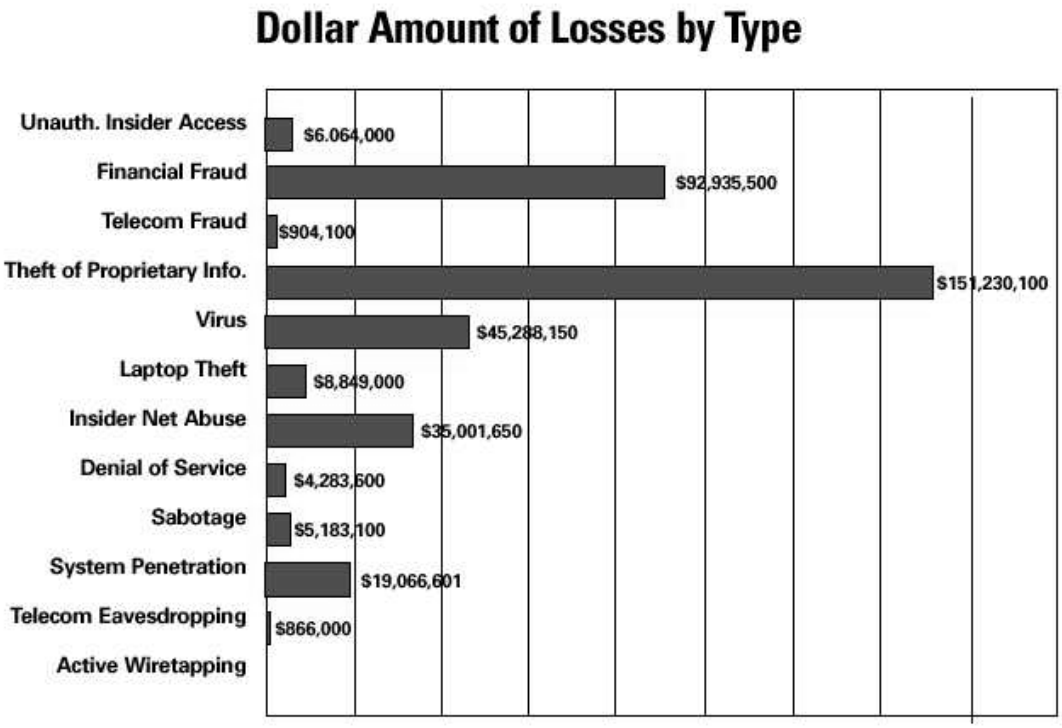
Eine Grundvoraussetzung für die flächendeckende Einführung einer PKI wird sein, dass die entstehenden unterschiedlichen Hierarchien untereinander operabel werden und dass sowohl die technische als auch die gesetzliche Interoperabilität verbessert wird.

Die Entwicklung der Public Key Infrastrukturen steht erst am Anfang. Die in diesem Zusammenhang auftretenden Probleme sind für eine derart komplexe Infrastruktur nicht selten. Allerdings muss unter den verschiedenen Herstellern in der Zukunft ein Konsens gefunden werden, um die recht vielfältigen Einsatzmöglichkeiten einer PKI zu fördern und zu beschleunigen, damit sich Unternehmen zumindest mittelfristig für den Einsatz einer Public Key Infrastruktur entscheiden.

[43] http://www.bsi.de/literat/tagung/cebit01/elekunt.pdf

B Abbildungen

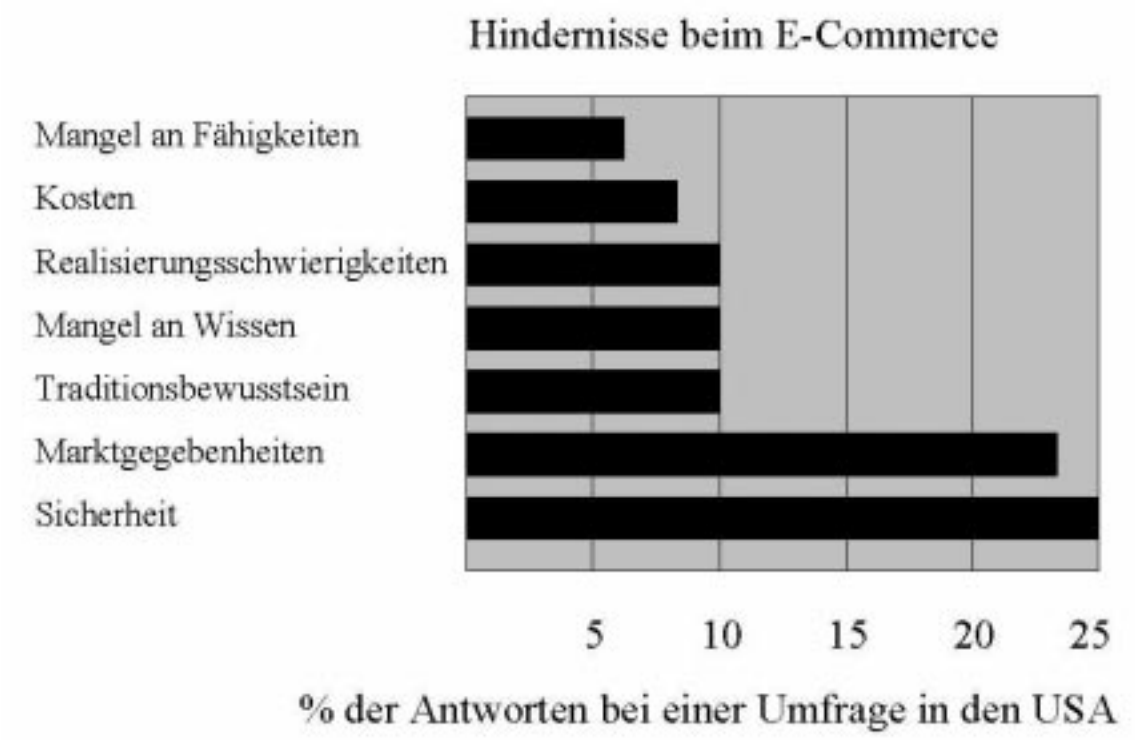
Abbildung 1: Monetäre Verluste durch IT-Sicherheitsverletzungen



Quelle: Computer Security Institute, 2001

Die Abbildung 1 zeigt den monetären Schaden, der durch den unberechtigten Zugriff nicht autorisierter Dritter auf ein IT-System erfolgt. Den größten Schaden verursacht der Diebstahl vertraulicher Informationen, gefolgt von dem Betrug bei finanziellen Transaktionen.

Abbildung 2: Hindernisse beim E-Commerce



Quelle: Abgeänderte Vorlage Computer Security Institute, 2001

Abbildung 2 zeigt die von Unternehmen genannten Hindernisse beim e-Commerce. Neben Marktgegebenheiten, die von vielen Unternehmen als Hindernis angesehen werden, ist die mangelnde Sicherheit die größte Schwelle für Investitionen in den e-Commerce.

Quellenverzeichnis

[BSI01] Bundesamt für Sicherheit in der Informationstechnik, Band 3, Juli 2001

[BUC98] Buchmann „Einführung in die Kryptographie“, 2., erweiterte Auflage, 1998

[DET01] Kai-Oliver Detken „Extranet, VPN-Technik zum Aufbau sicherer Unternehmensnetze“ 2001

[DUD95] Duden, Das große Fremdwörterbuch, 1995

[HAM99] Volker Hammer „Die 2.Dimension der IT-Sicherheit“,1999

[KYC99] Othmar Kyas und Markus a Campo „IT-Crackdown, Sicherheit im Internet“, 1999

[NAE99] Michael Näf (Hrg.) „Risiko Internet?, Sicherheitsaspekte bei der Internet-Benutzung“, 1999

[NAS01] Andrew Nash (Hrg.) „PKI: Implementing and Managing E-Security“, 2001

[PIO99] Jakup Piotrowski „LDAP – Übersicht über das Chaos“, 1999

[SCH01] Klaus Schmeh „Kryptographie und Public Key Infrastrukturen im Internet“, 2001

[SEL00] Jörg Schumacher und Eike Elser „Sicherheit im Internet, 2000

[STR97] Bruno Struif (Hrg.) „Digitale Signatur & Sicherheitskritische Anwendungen“, 1997

[ULF99] Udo Ulfkotte „Marktplatz der Diebe“ C. Bertelsmann, München , 1999

Ehrenwörtliche Erklärung

"Hiermit versichere ich, diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quelle benutzt zu haben.

Wörtliche und sinngemäße Zitate sind kenntlich gemacht. Über die Zitierrichtlinien bin ich schriftlich informiert worden."