

Medialab: Gefahren und Sicherheitsaspekte bei der Interaktion mit dem Internet

Martin Bacher

Martin.Bacher@student.unisg.ch

Marcel Zeender

Marcel.Zeender@student.unisg.ch

Benjamin Stengl

Benjamin.Stengl@student.unisg.ch

Arbeit zum Thema Internetsicherheit im Kurs Medialab

Universität St. Gallen

Bachelorstufe

Dr. Katarina Stanoevska-Slabeva und Prof. Dr. Beat Schmid

07.02.2003

Inhaltsverzeichnis

1.	Einleitung.....	5
2.	Erläuterungen und Begriffsdefinitionen.....	6
2.1.	OSI-Referenzmodell	6
2.2.	Das Internetprotokoll TCP/IP	6
3.	Gefahren des Internet.....	8
3.1.	Allgemein	8
3.2.	Aspekte der sicheren Datenübertragung.....	8
3.2.1.	Vertraulichkeit	9
3.2.2.	Authentifizierung und Unbestreitbarkeit	9
3.2.3.	Verfügbarkeit	10
3.2.4.	Integrität / Korrektheit	10
3.3.	Schädlinge im Internet	10
3.3.1.	Viren.....	11
3.3.1.1.	Viren allgemein	11
3.3.1.2.	Funktionsweise von Viren	11
3.3.2.	Würmer.....	12
3.3.3.	Cookies.....	12
3.3.4.	Trojaner	13
4.	Mögliche Lösungen	14
4.1.	Organisatorische Lösungen.....	14
4.1.1.	Allgemein	14
4.1.2.	Verhalten der Mitarbeiter	14
4.1.3.	Administrative Aufgaben	16
4.2.	Technische Lösungen.....	16
4.2.1.	Allgemein	16
4.2.2.	Verschlüsselung.....	17
4.2.2.1.	Symmetrische Verschlüsselung.....	17
4.2.2.2.	Asymmetrische Verschlüsselung.....	18
4.2.2.3.	Hybride Verschlüsselung.....	19
4.2.2.4.	Höhe des Verschlüsselungsschutzes	19
4.2.3.	Antivirenprogramme	20
4.2.4.	Firewall.....	21
4.2.4.1.	Komponenten und deren Funktionsweise.....	22
4.2.4.2.	Vor- und Nachteile von Firewall-Systemen.....	24
4.2.4.3.	Firewall-Produkte	25
4.3.	Sicherheit und Sensibilisierung	25
5.	Fazit.....	27
6.	Literaturverzeichnis	28

i. Abbildungsverzeichnis

Abbildung 1: eigene Darstellung der ISO/OSI- vs. TCP/IP - Modelle in Anlehnung an Eckert (2001) .6	
Abbildung 2: schematische Darstellung der Funktionsweise des hybriden Verschlüsselungsverfahrens (eigene Darstellung in Anlehnung an den Text und die darin verwendeten Quellen).	19
Abbildung 3: Idee des Firewall-Systems und deren Positionierung Quelle: eigene Darstellung, in Anlehnung an Pohlmann, N. (2001)	21
Abbildung 4: Aufbau und Arbeitsweise einer Firewall-Komponente	24

Management Summary

Die Aspekte der Sicherheit haben in praktisch allen täglichen Belangen während den letzten Jahren zunehmend an Bedeutung gewonnen. So auch in der virtuellen Welt, wo die Täter nicht Terroristen sondern Hacker genannt werden. Ohne den Teufel gleich an die Wand zu malen: Sobald man sich mit einem PC im Internet befindet, sollten grundlegende Sicherheitsaspekte beachtet werden, um sich vor bösen Überraschungen zu schützen.

Regelmässig erreichen uns Meldungen über neue Viren, Würmer oder anderen Schädlingen, die durch ihr Unwesen weltweit Schäden in zwei bis dreistelligen Millionenbeträgen verursachen. Für die einzelne Firma kann dies, sofern sie ihren Pflichten eines minimalen Sicherheitsstandards nicht nachgekommen ist, sogar zum Untergang führen. Man stelle sich vor, ein Dienstleistungsbetrieb verliere alle digital gespeicherten Daten gänzlich oder deren Wiederherstellung würde Kosten verursachen, die die finanziellen Möglichkeiten der Unternehmung bei weitem übertreffen. Dieses Schreckensszenario gehört nicht ins Reich der Hirngespinnste und stellt für jede Unternehmung eine ernsthafte Bedrohung dar, sobald einzelne oder alle Computer Zugang zum Internet haben und diese miteinander vernetzt sind. Daraus ergibt sich zwangsläufig die Forderung, dass die IT - Sicherheit nicht mehr nur in den Zuständigkeitsbereich der Netzwerk-Spezialisten gehört, sondern dass auch die Mitarbeiter in der Teppichetage Verantwortung übernehmen müssen: Sicherheit ist also Chefsache!

Natürlich findet ein CEO nicht genügend Zeit, um sich eingehend und ausführlich mit den möglichen Gefahren bzw. Vorsichtsmassnahmen auseinanderzusetzen. Er hat aber die Möglichkeit, externe Sicherheitsspezialisten mit der Inspektion der firmeninternen Vorkehrungen zu beauftragen oder diese ermächtigen, gezielte Angriffe aufs firmeninterne Intranet zu starten. Als Beispiel kann der amerikanische Geheimdienst gelten, der von der Polizei aufgegriffene Hacker unter Vertrag nimmt und diese dafür bezahlt, Löcher in ihrem Sicherheitsnetz zu finden. Zwischen dem Anspruch, die besten Talente zu akquirieren und den Sicherheitsvorkehrungen, die bei einigen Firmen immer noch anzutreffen sind, besteht in der Tat eine grosse Diskrepanz. Sollte diese Arbeit dazu beitragen, diese Lücke zu schliessen, hat sie ihren Auftrag erfüllt.

1. Einleitung

In der vorliegenden Arbeit wollen wir der Frage nachgehen, welche Mittel und welches Handeln nötig sind, um die Interaktion zwischen dem globalen und offenen Internet einerseits und den lokalen Firmennetzwerken andererseits so zu gestalten, dass keine Sicherheitsprobleme entstehen bzw. dass Gefahren und Sicherheitslücken mit grösster Wahrscheinlichkeit vermieden werden können. Selbstverständlich ist sich jedermann bewusst, dass es eine hundertprozentige Sicherheit nicht gibt, vor allem bei einem komplexen Gerät wie einem PC; ganz zu schweigen, wenn dieser wie heute mehr und mehr üblich, fast pausenlos mit Millionen anderen Rechnern im Internet direkt verbunden ist. Die völlige Sicherheit bei einem einzelnen PC kann theoretisch und praktisch fast nur noch dadurch gewährleistet werden, wenn er physisch vom Netz abgekoppelt oder vom Stromnetz genommen wird. Aber sobald man mit einem PC arbeitet und auf den Netzwerkzugang oder aufs Internet angewiesen ist, sind solche Strategien unrealistisch. Grundsätzlich geht es darum, die eigenen „Rechnersysteme und Informationen gegen den Verlust von Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit und Authentizität zu schützen“ (Pohlmann, 2001, S. 27).

In einem ersten Teil soll nachfolgend auf wichtige Begriffe im Bereich Netzwerke und Internet eingegangen werden, danach sollen die wichtigsten Gefahren erläutert werden, die vom Internet auf Firmennetzwerke und einzelne PCs ausgehen. Anschliessend folgen mögliche Lösungen oder Lösungsansätze, wobei wir Organisatorisches trotz dessen Bedeutung nur kurz aufgreifen wollen. Mit bestimmten technischen Lösungen werden wir uns eingehend befassen, weil wir glauben, vielen Anwendern sind solche Möglichkeiten noch kaum bekannt oder diese denken, dass man diese als Normalverbraucher nicht nutzen kann. Der Abschluss dieser Arbeit dreht sich dann zentral um die Vermittlung von einem elementarsten Sicherheitsverständnis in unserem Themengebiet.

Zu ergänzen gilt es noch, dass in der ganzen Arbeit bei der Verwendung von männlichen Personenausdrücken immer beide Geschlechter gemeint sind, als auch weibliche Personen.

2. Erläuterungen und Begriffsdefinitionen

2.1. OSI-Referenzmodell

Im Zusammenhang mit der Vernetzung von Systemen werden unterschiedliche Protokolle und Techniken verwendet. Um eine Vereinheitlichung all dieser Varianten zu erreichen, wurde das OSI-Referenzmodell (Open System Interconnection) geschaffen. Primäres Ziel dieses Referenzmodells war es, mittels einheitlicher Schnittstellen den Einsatz herstellerunabhängiger Netzkomponenten gewährleisten zu können. Dieses Referenzmodell besteht aus sieben Schichten und wird deshalb auch 7-Layer-Architektur genannt. Die einzelnen Schichten werden *Physical Layer*, *Data Link Layer*, *Network Layer*, *Transport Layer*, *Session Layer*, *Presentation Layer* und *Application Layer* genannt¹ (Fuhrberg, Häger & Wolf, 2001).

2.2. Das Internetprotokoll TCP/IP

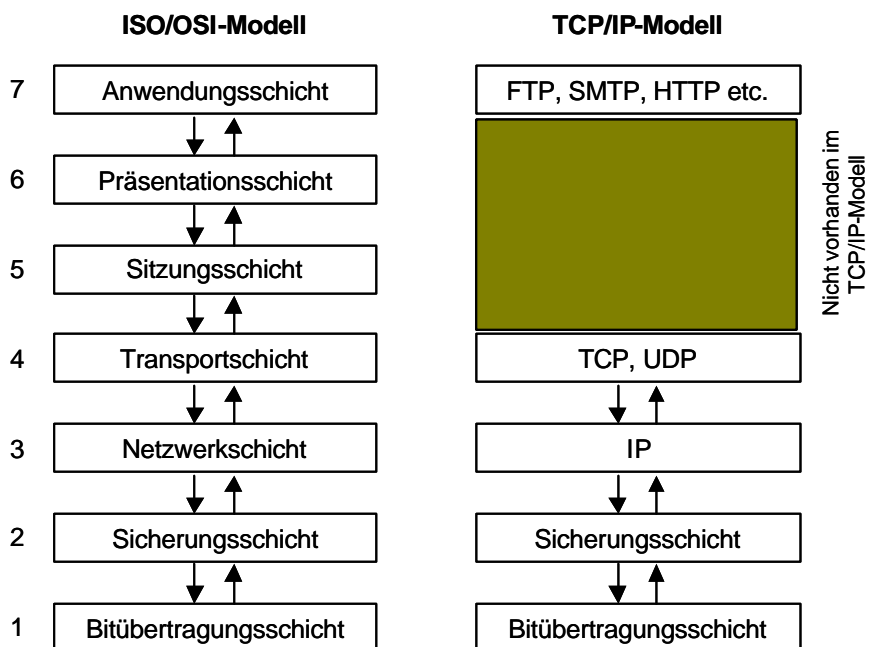


Abbildung 1: eigene Darstellung der ISO/OSI vs. TCP/IP - Modelle in Anlehnung an Eckert (2001)

Im Gegensatz zum ISO/OSI-Modell ist das TCP/IP-Modell von unangefochtener Bedeutung. Es wird oftmals sogar als *TCP/IP-Protokoll* bezeichnet, weil diese beiden Protokolle zusammen das Herzstück der Datenübertragung im heutigen Internet bilden. Abbildung 1 zeigt schematisch den Unterschied zwischen dem *Referenzmodell* und der *Wirklichkeit*: Im TCP/IP-Modell fehlen zwei Schichten (Layer) gänzlich, d.h. auf der Netzwerk- und Transportschicht sind direkt die Anwendungsprotokolle aufgesetzt, entsprechend kann es bei Sicherheitsproblemen in den TCP/IP-Protokollen zu unmittelbaren Auswirkungen auf der Anwendungsschicht kommen, weil mögliche Zwischenschichten bspw. mit Verschlüsselungsfunktionen fehlen.

¹ In dieser Arbeit geht es um die Sicherheit in Unternehmensnetzwerken bei der Interaktion mit dem Internet. Aus diesem Grund wird auf die Erklärungen der einzelnen Schichten verzichtet. Zusätzliche Informationen zu diesem Referenzmodell bieten Fuhrberg, Häger & Wolf (2001).

Das *Internetprotokoll* (IP) ist ein *paketvermittelnder, verbindungsloser* Dienst ohne Übertragungskontrolle. Die Datenpakete werden möglicherweise über x-verschiedene Zwischenrechner zum Ziel geleitet, wobei jedes Paket seinen völlig eigenen Weg gehen kann. Aus diesem Grund braucht jedes Paket einen Header („Paketkopf“), worin alle notwendigen Informationen gespeichert sein müssen (die Sender- und Empfänger-IP-Adresse, Angaben über die Position des Datenpakets, die Paketlänge etc.), erst nach dem Header folgen die zu übertragenden Daten.

Das *Transport Control Protocol* (oder *Transportkontrollprotokoll*, kurz TCP) ist *verbindungsorientiert* und *kontrolliert*, ob alle IP-Pakete auch übertragen werden (d.h. es überprüft fortlaufend die Vollständigkeit der Daten anhand der Sequenznummern der einzelnen Pakete). Das TCP-Protokoll stellt eine End-zu-End-Verbindung nicht einfach nur von Rechner zu Rechner her, sondern von *Port zu Port* (16-bit Adresse), d.h. auf der Anwendungsebene besteht dann die Möglichkeit, dass bestimmte Dienste einen Port überwachen bezüglich eintreffender Nachrichten. Entsprechend enthält jedes TCP-Paket die Information des Sende- und Zielports, dazu wird jedes Paket mit einer Sequenznummer nummeriert, damit ein Paketverlust festgestellt und sofort das verlorene Paket nochmals angefordert werden kann. Der *Verbindungsaufbau* zwischen Client und Server läuft in drei Schritten ab: Der Client schickt ein TCP-Paket mit Empfänger-IP und -Port an den Server. Kann das Paket am gewünschten Port zugestellt werden, wird die Übertragung quittiert. Im dritten Schritt quittiert dann auch der Client nochmals, dass er die Quittierung erhalten hat, anschliessend beginnt der eigentliche Datentransfer.

Auf der Anwendungsschicht gibt es verschiedenste (bekannte) Dienste, welche über das TCP-Protokoll auf der Transportebene arbeiten. Es wären zu erwähnen, das *File Transfer Protocol* (FTP), das *Simple Mail Transfer Protocol* (SMTP) und das *Hypertext Transport Protocol* (HTTP). Ersteres dient zum Hinauf- und Herunterladen von Dateien auf und von Servern (sog. FTP-Server), das Zweite zum Versenden von E-Mails und letzteres ist *das* Internetprotokoll zum Surfen auf dem World Wide Web. *Wichtig zu erwähnen* ist hier, dass auf der Ebene der TCP/IP-Protokolle überhaupt keine Sicherheitsüberwachung stattfindet, also weder über die Korrektheit des Inhaltes von Paketen, noch woher sie kommen oder wohin sie gehen. Auch bieten sie keine *Verschlüsselungsmechanismen*, sondern senden die Daten in den Paketen in Klartext auf dem Internet umher. Auch die einfachen Protokolle auf der Anwendungsschicht bieten keine erhöhte Sicherheit, nur spezielle Abwandlungen wie das *sichere HTTP*, das HTTPS, welches vor allem im Online-Banking vermehrt zu Anwendung kommt, bieten entsprechende Sicherheit. (Eckert, 2001, S. 44-71)

Diese kurze Einführung in die Problematik der TCP/IP-Protokolle, welche in der Praxis im Internet zur Anwendung kommen, soll vor allem als Hintergrund für die in dieser Arbeit zu behandelnden Themen *Firewall* (Kap. 4.2.4) und *Verschlüsselung* (Kap. 4.2.2.) dienen. Bei ersterem geht es darum zu wissen, dass eine Firewall nicht einfach auf einer Protokollebene eingreift, sondern diesen Zugriff sehr differenziert vornehmen kann. Beim Zweiten soll einfach erwähnt sein, dass Daten de facto erst sicher übertragen werden können, wenn diese auf höchster Ebene (also auf oder über der Anwendungsschicht, d.h. in einer Anwendungsapplikation) verschlüsselt werden, andernfalls sendet man seine vertraulichen Daten in Klartext übers Internet.

3. Gefahren des Internet

3.1. Allgemein

Während früher, also bis vor ca. 10-15 Jahren, vorwiegend die Netzwerke und Server von Regierungen und anderen staatlichen Einrichtungen Angriffe von Hackern befürchten mussten, kann heutzutage praktisch jeder Internetbenutzer als potenzielles Opfer eingestuft werden. Beinahe jeder hat auf seinem Computer sensible Daten gespeichert, die ein Dritter zum eigenen Vorteil ausnutzen könnte. Als anfälligen Bereich kann das E-Banking genannt werden, wo der Bankkunde mit seinem PC entweder offline oder online Bankgeschäfte abwickelt und dazu Benutzername, Passwort und Kontrollnummer ins System eintippen muss.

Nicht nur die Angriffsziele haben sich geändert, sondern auch die Vorgehensweise: Hacker verbringen nicht mehr nächtelang vor dem Computer und versuchen, Codes zu knacken und Fährten zu verwischen. Dies geschieht heute meist systematisch und automatisiert mit speziellen Programmen, die das Internet nach offenen Rechnern absuchen und umgehend eine kurze Inspektion der zugänglichen Daten vornehmen bzw. diese aufgrund von vorgegebenen Kriterien analysieren. Damit einem Fremden überhaupt die Möglichkeit geboten werden kann, auf einen anderen PC zuzugreifen, muss das *Microsoft Netzwerk* installiert sein. Diese Systemdienste erweisen sich bei einem alleinstehenden PC jedoch als nutzlos, weshalb empfohlen wird, den Dienst zu deaktivieren, falls er nicht benötigt wird. Der Schutz vor einem Angriff, und sei es nur das Herumstöbern auf dem eigenen Computer durch eine fremde Person, kann dadurch mit wenig Aufwand enorm gesteigert werden.

Die Analyse der Gefahren im Internet wäre unvollständig, wenn nicht auch gefragt würde, vor wem schliesslich zu schützen sei. Als Angreifer könnte sich etwa ein anderer Benutzer des Systems entpuppen, der Betreiber des Systems oder vielleicht sogar der Entwickler des Systems selbst. Jeder Aussenstehende stellt schlussendlich eine potenzielle Gefahr dar und dies sollte vor allem bei der Administration der eigenen Passwörter sorgfältig berücksichtigt werden.

3.2. Aspekte der sicheren Datenübertragung

Grundsätzlich sollten Gefahren betreffend lokal gespeicherter Daten innerhalb einer Unternehmung wie auch Gefahren bei der Übertragung der Daten über ein öffentliches Netz betrachtet werden. Fuhrberg et al. (2001) unterscheiden dabei u.a. Vertraulichkeits- und Integritätsverluste von übertragenen, lokal im Unternehmensnetz gespeicherten und durch Schadprogramme (Anhänge von E-Mails) bedrohte lokal gespeicherte Daten. Vertraulichkeit und Integrität beschäftigen sich mit dem Datenaustausch zwischen zwei Teilnehmern, dem Sender und dem Empfänger. Die Verfügbarkeit, ein weiterer Differenzierungspunkt im Zusammenhang mit sicherer Datenübertragung, befasst sich mit der Beziehung Benutzer-Rechner. Heindl et al. (2001) ergänzen die Anforderungen an eine sichere Datenübertragung und nennen zusätzlich Authentifizierung und Unbestreitbarkeit, die wir im folgenden Abschnitt näher erläutern werden. Hochwertige Verschlüsselungsverfahren müssen zudem den Kriterien der *Nichtwiederholbarkeit* und *eindeutigem Zeitbezug* genügen (Heindl et al., 2001, S. 51), auf die jedoch nicht eingegangen wird.

3.2.1. Vertraulichkeit

Gleich wie im täglichen Briefverkehr wird mit diesem Begriff zum Ausdruck gebracht, dass die Information nur für den Empfänger bestimmt ist bzw. „dass niemand ausser dem intendierten Empfänger die Nachricht lesen kann“ (Heindl et al., 2001, S. 51). Während der Empfänger eines schriftlichen Briefes an der Unversehrtheit des Umschlages prüfen kann, dass niemand vor ihm diesen geöffnet hat, gestaltet sich dies im E-Mail-Verkehr wesentlich komplizierter. Zu beachten ist ferner, dass das Verschicken von vertraulicher Information auch vom Absender einer E-Mail erhöhte Vorsicht abverlangt. Mit *Reply to All* oder *Allen antworten* bieten die E-Mail-Programme (wie bspw. Microsoft Outlook, Netscape Messenger, Eudora, Lotus Notes etc.) die Möglichkeit, eine erhaltene E-Mail an alle Adressaten zu beantworten. Dabei kann es vorkommen, dass auf dem erhaltenen Mail Adressen von Empfängern stehen, die eventuell firmenextern sind oder Daten und am neuen E-Mail angehängt werden, obwohl sie die Nachricht nicht erhalten sollten. Ein unvorsichtiges *Antworten an alle* kann dazu führen, dass sensible Daten in fremde Hände gelangen und diese eventuell zum Nachteil der eigenen Firma eingesetzt werden. Es ist daher ratsam, bei jedem *Reply to all* alle Adressaten genau zu prüfen und abzuklären, ob die Information tatsächlich an die betreffende Person gesendet werden soll. Dieser Problematik muss auch Beachtung geschenkt werden, wenn ein E-Mail mit vertraulichen Daten an eine vordefinierte Benutzergruppe geschickt wird. Oft wird die Administration von Benutzergruppen in grösseren Firmen von der IT-Abteilung vorgenommen. Für den einzelnen Benutzer sind deshalb die Mutationen dieser Empfängerlisten nicht ersichtlich und die Benutzung dieses E-Mailversands sollte deshalb nur angewendet werden, wenn Daten oder Informationen verschickt werden, die keiner vertraulichen Behandlung bedürfen.

3.2.2. Authentifizierung und Unbestreitbarkeit

Auch wenn versendete Informationen das Kriterium der Vertraulichkeit erfüllen, besteht die offene Frage, ob der genannte Absender auch tatsächlich jener Person entspricht, welche das E-Mail verschickt hat oder ob es sich hier allenfalls um eine Täuschung handelt, welche im Fachjargon mit dem Begriff *spoofing* (Clearswift, 2002) bezeichnet wird. Das Wort *spoof* wird im Wörterbuch mit Parodie oder Aprilscherz übersetzt und ist in der Tat alles andere als lustig. Zum Beispiel kann die E-Mail-Adresse eines Vorgesetzten angezeigt werden, obwohl diese von einer anderen Person stammt. Der Empfänger vertraut auf die Richtigkeit des Absenders und kann unter Umständen dazu bewogen werden, sensible oder geheime Daten an die Adresse zurückzuschicken. Eine 1999 in der USA durchgeführte Studie kam zum Schluss, dass 95% der Befragten den Ursprung nicht bezweifeln, die von der Geschäftsleitung oder einem Vorgesetzten stammt (Clearswift, 2002). Für den Anwender mit Basiskenntnissen in Office-Programmen ist es in der Praxis beinahe unmöglich, die Richtigkeit der Absenderadresse anhand des erhaltenen E-Mails zu prüfen. Einzig der Griff zum Telefon könnte Abhilfe schaffen, um den Versand der E-Mail bei der vermeintlichen Person bestätigen zu lassen. Die wesentlich effizientere Lösung ist allerdings das Versenden und Empfangen von E-Mails mittels Verschlüsselungsprogrammen (siehe Kap. 4.2.2).

3.2.3. Verfügbarkeit

Bei der Verfügbarkeit geht es um die Möglichkeit, Daten oder Systeme zu nutzen, wenn dies vom Anwender gewünscht wird. Die steigende Anzahl der Internetnutzer einerseits und die vermehrte Nachfrage nach mehr Übertragungskapazitäten zwingt die Netzbetreiber, ihre Systeme ständig aufzurüsten, um mehr Bandbreite zu schaffen. Ein System, das oft an der Kapazitätsgrenze operiert, ist daher sehr anfällig für Störungen und Unterbrüche. Dies kann nun einfach ausgenutzt werden, indem das System mit zusätzlichem Datentransfer belastet wird, den dieses nicht mehr bewältigen kann und in der Folge abstürzt. Das Verschicken einer riesigen Anzahl von E-Mails, mit dem Ziel, ein Netz oder einen Knoten (ISP) lahmzulegen, wird in der Praxis mit *Spam* bezeichnet (Clearswift, 2002). Damit kann ein Internet Service Provider (ISP), die Anbindungsstelle der einzelnen Nutzer ans Internet, unterbrochen werden, was zu einem DOS (Denial of Service) führt.

Die Verfügbarkeit ist die Voraussetzung der Kommunikation, die im Internet zwischen zwei oder mehreren Teilnehmern stattfindet. Während die Überprüfung der eigenen Verfügbarkeit problemlos möglich ist (kurzes Einloggen beim ISP), ist dies beim Empfänger meiner Daten oder Informationen beinahe unmöglich. E-Mail-Programme bieten die Funktion, eine Bestätigung des Empfängers anzufordern, sobald dieser die E-Mail öffnet. Der Sender ist jedoch auf die Mitarbeiter des Adressaten angewiesen, denn wenn dieser die Bestätigung nicht abschicken will, besteht keine Möglichkeit zur Überprüfung der Verfügbarkeit.

3.2.4. Integrität / Korrektheit

Als letztes Kriterium bei der Prüfung der sicheren Datenübertragung geht es schliesslich um die Integrität bzw. Korrektheit der versandten Informationen. Gegenstand der Untersuchung ist, ob das Dokument genau so empfangen wurde, wie es der Absender verschickt hat oder ob bspw. eine E-Mail unterwegs von einer fremden Person abgeändert wurde. Als zusätzliche Forderung erwähnt Heindl et al. (2001), eine allfällige Änderung mit Sicherheit feststellen zu können. Dazu eignet sich die Verwendung einer digitalen Signatur, die aus dem Dokument einen unverwechselbaren Hash-Wert generiert (Heindl et al., 2001, S. 55). Bereits ein geringfügiger Eingriff in das Dokument verändert den Hash-Wert in unvorhersehbarer Weise und signalisiert dem Empfänger, dass es sich beim vorliegenden Dokument nicht mehr um das Original handelt. Eine Feststellung der Veränderung alleine reicht jedoch noch nicht aus. Neuste Systeme der digitalen Signatur können im Nachhinein auch die genauen Veränderungen während der Übertragung feststellen.

3.3. Schädlinge im Internet

Bei der folgenden Analyse möglicher Angreifer im Internet konzentrieren wir uns auf die Viren, die Würmer, die Cookies und die Trojaner. Diese vier Ausprägungsformen erscheinen unter verschiedenen Gesichtspunkten exemplarisch. Die Viren als die wohl bekanntesten Vertreter von Störprogrammen, die in der Vergangenheit mehrmals für weltweites Aufsehen² sorgten und durch die

² Aus Aktualität (Ende Januar 2003) wäre hierbei die Attacke auf eine Lücke im Microsoft SQL-Server (mit dem sog. *SQL-Slammer*, *Slapper*, *Sapphire* oder *SQL Hell*) zu erwähnen: Der Hauptgrund für die vielen Systemausfälle lag vor allem darin, dass viele Systemadministratoren ein länger verfügbares (Juli 2002) Servicepaket für den SQL-Server noch nicht installiert hatten. (Borchers, 2003, S. 75)

Stilllegung von Servern oder Teilnetzen innerhalb weniger Tage beträchtlichen wirtschaftlichen Schäden anrichteten. Betrachtet werden anschliessend die Würmer, die sich dank der weltweiten Vernetzung von Rechnern erst verbreiten konnten, bevor die Funktionsweise von Cookies erklärt wird, mit denen jeder Internetnutzer konfrontiert ist, wenn er sich mit einem Webbrowser im Internet bewegt. Zuletzt erklären wir die Funktionsweise der Trojaner, vor denen sich besonders die Internetnutzer schützen sollten, die Software von mehr oder weniger vertrauenswürdigen Quellen im Internet beziehen, sei dies gratis oder gegen Entgelt.

3.3.1. Viren

3.3.1.1. Viren allgemein

Die Absicht hinter der Verbreitung von Viren wie *Melissa* oder *ILOVEYOU* war immer dieselbe: Das Beschädigen von Dateien und das automatische Weiterverbreiten durch E-Mail-Programme. Diese Verbreitung kann im Zeitalter des Internets sehr schnell geschehen. Das FBI stellte fest, dass sich bisher noch nie ein Virus so schnell wie der Love Bug verbreitet hat (Electronics today, 2000) und bisher nie so viele Computer gleichzeitig vom selben Virus infiziert wurden. Die Schäden werden dementsprechend auch auf die horrend hohe Zahl von 2.1 Milliarden USD beziffert; die Folgeschäden können dabei möglicherweise auf ein Mehrfaches ansteigen. Dass Viren ein ernstzunehmendes Problem in der vernetzten Computerwelt darstellen, zeigt allein schon die Anzahl dieser heimtückischen Programme: Heutzutage sind ca. 60'000 verschiedene Viren bekannt und monatlich entstehen 600 neue Viren (Lindhorst, 2002, S. 87).

Besonders gefährlich sind die Bootviren, deren Namen dem Englischen Wort *booten* übernommen wurde, das den Start eines Rechners bezeichnet. Diese Viren können über Jahre hinweg unbemerkt auf einer Diskette gespeichert sein. Wird nun ein PC gestartet und befindet sich noch eine Diskette im Laufwerk, so sucht der Computer in der Regel die Systemdateien, die für einen Start benötigt werden, im Laufwerk auf der Diskette. Der Bootvirus wird nun aktiviert und kann zum Ausfall bzw. zum Absturz des Systems führen. Diesem Risiko kann sehr effizient vorgebeugt werden, indem das Booten von der Diskette im BIOS (Grundeinstellung des Computers) unterbunden wird. Der PC versucht nun bei jedem Neustart die Systemdateien von der Festplatte aufzurufen, um das System zu starten. Das gleiche vorsichtige Verhalten gilt natürlich auch gegenüber den zunehmend aufkommenden bootable CD-ROMs.

3.3.1.2. Funktionsweise von Viren

Computerviren funktionieren sehr ähnlich wie medizinische Viren: Sie sind nicht in der Lage, sich selber zu vermehren und benötigen deshalb einen Wirt, der sie aufnimmt und ihnen die Möglichkeit bietet, sich zu vermehren. E-Mail-Programme³ eignen sich hervorragend dafür, weil sie konzipiert sind, Informationen an andere Nutzer zu schicken. Technisch betrachtet sind Viren „winzige Programme, die aus Programmcode bestehen und Störungen hervorrufen“ (Lindhorst, 2002, S. 86).

³ Skriptviren sind eine Hauptgefahr für *E-Mail-Programme*, aber grundsätzlich auch für alle Programme mit *VBA-Unterstützung* (Visual Basic for Applications; bspw. die ganze Office-Familie). Für alle *ausführbaren* Programme (EXE-Dateien) gilt die Gefahr durch Programmviren (welche direkt in den Maschinencode dieser Programme eingreifen und immer mit dem Wirt ausgeführt werden).

Dabei ist zu erwähnen, dass vor allem die Software Microsoft Outlook für Viren anfällig ist, weil dieses VB-Skripte direkt ausführt. Andere Programme wie Netscape Messenger oder Eudora starten diese Skripte nicht automatisch.

Auf die Problematik der Bootviren wurde bereits hingewiesen und mögliche Schutzmassnahmen wurden aufgezeigt. Als nächstes wollen wir den Makrovirus, wie bspw. der Love Bug einer war, näher erläutern. Dieser Virus nutzte gleich zwei Nachlässigkeiten innerhalb der Microsoft-Office-Produkte aus: Zum einen war er ergänzt mit dem Kürzel „.vbs“ mittels dem die Datei problemlos passieren konnte. Dieser Anhang sollte auf die Programmiersprache *Visual Basic Script* hindeuten, welche vor allem bei Hackern und Programmierern sehr verbreitet ist. Zum andern führt die E-Mail-Software Outlook dieses Skript selber aus, wenn das sogenannte *Active Scripting* (Electronic today, 2000) eingeschalten und startet somit die Verbreitung an die Kontaktliste (alle Einträge im Adressbuch) des E-Mail-Programms. Dabei geht es aber lediglich um die Ausdehnung des Virus, die ähnlich wie die der Würmer (siehe Kap. 3.3.2.) funktioniert (Lindhorst, 2002, S. 90). Hat sich aber der Virus erstmals im System eingenistet, so beginnt er, sein Unwesen zu treiben. Er versteckt sich in einem Makro eines Dokuments (bevorzugt Microsoft Word und Excel) und beginnt, Dokumente zu löschen. Besonders für kleine Firmen, die ihre Daten unzureichend schützen, kann der Verlust von wichtigen Daten im Extremfall der Ruin bedeuten. Experten schätzen die Kosten der Wiederherstellung verloren gegangener Daten auf bis zu 500 Euro pro Megabyte. Theoretisch würde also die Wiederherstellung von zehn Gigabyte bereits 5 Mio Euro kosten (Electronics Today, 2000). Der Aufwand für ausreichende Schutzmassnahmen steht also in keinem Verhältnis zu einem möglichen Schaden. Dies wird in der heutigen Computerwelt leider noch zuwenig beachtet.

3.3.2. Würmer

Zu einer weiteren Schadensklasse gehören die Würmer, deren primäres Ziel es ist, sich zu reproduzieren und zu verbreiten. Die vernetzte Computerwelt scheint daher prädestiniert zu sein für das Wirken dieser Schädlinge. Analog zu den Viren bevorzugen auch die Würmer die E-Mail-Programme, um innerhalb kürzester Zeit eine grosse Verbreitung zu erreichen. Dazu werden die Systemdateien auf dem Computer gezielt abgeändert, damit bei jedem Starten des Computers der Wurm von neuem aktiviert wird und im Mailprogramm eine Nachricht an alle im Posteingang befindlichen Adressaten schickt. Doch dieser Vorgang dient nur der Verbreitung. Hat sich ein Wurm erfolgreich in einem System eingenistet, so durchsucht er den Rechner auf Quelldateien von Programmen und setzt diese auf die Länge ,0' womit eine Wiederherstellung beinahe verunmöglicht wird (Lindhorst, .2002, S. 96).

3.3.3. Cookies

Beim Besuch einer Webseite werden Informationen in einer kleinen Textdatei, dem Cookie, auf der Festplatte gespeichert. Darin sind Informationen über den Nutzer und seine Präferenzen enthalten. Zum Beispiel kann die Abfolge der besuchten Seiten beim Aufrufen der Homepage einer Airline gespeichert werden, damit beim nächsten Besuch gewisse Auswahlkriterien und Einstellungen bereits vorgegeben werden. Überdies wird diese Seite beim nächsten Besuch schneller aufgebaut, weil Informationen über das Seitenlayout auf dem eigenen Rechner geladen sind und deshalb nicht erst empfangen werden müssen.

Im Prinzip sollte eine Internetseite nur auf Ihre eigenen Cookies auf der Festplatte des Internetnutzers zugreifen, um die Daten zu pflegen. Allerdings ist es möglich, eine URL-Adresse abzuändern damit diese die gespeicherten Informationen in den anderen Cookies liest oder ändert (Sicherheitsberater, 2001). Ein regelmässiges Löschen der temporären Internet-Dateien kann dazu beitragen, den Schutz vor unliebsamen Lauschangriffen zu begegnen. Allerdings werden harmlose Informationen über andere Seiten, die das Arbeiten am PC durchaus erleichtern, auch gelöscht und müssen anschliessend wieder neu erstellt werden. Erwähnt werden sollte in diesem Zusammenhang, dass nicht nur die temporären Internet-Dateien gelöscht werden sollten, sondern auch die gespeicherten Cookies. Dies ist bei den heutigen Webbrowsern allerdings problemlos möglich.

3.3.4. Trojaner

Trojaner treten meist offen, als Bildschirmschoner, Software für Passwortverwaltungen oder zum Beispiel als Programm zum Komprimieren von Dateien auf. Neben dem Komprimieren führt dieses Programm noch eine zweite Aufgabe aus, nämlich das gleichzeitige Verschicken der Dateien an eine vordefinierte E-Mail-Adresse. Besonders gefährlich werden die Trojaner dadurch, dass diese die gleichen Rechte haben, wie der Benutzer, der das infizierte Programm aufruft (Heindl et al., 2001, S. 67). Vorstellbar wären, dass der PC eines Netzwerkadministrators von einem Trojaner befallen wird und dieser anschliessend einen ferngesteuerten Zugriff auf die Konfiguration des Netzwerkes bietet. Nur von vertrauenswürdigen Quellen Dateien oder Programme zu beziehen, ist sicher ein guter Anfang, um sich vor Trojanern zu schützen. Virens Scanner untersuchen den PC ebenfalls auf Trojaner wobei beachtet werden muss, dass der Scanner periodisch auf den neusten Stand gebracht werden sollte. Die eigentliche Zweckbestimmung der Trojaner, Informationen über das Internet an eine Adresse zu schicken, macht sie für ihr Auffinden besonders anfällig. Zum Beispiel kann die Bewegung des Datentransfers beobachtet werden und bei auffällig hohen Mengen sollte anschliessend der Rechner auf mögliche Trojaner untersucht werden.

4. Mögliche Lösungen

Um die Sicherheit der im LAN verfügbaren und über das Netz zu versendenden Daten gewährleisten zu können, braucht es innerhalb einer Unternehmung sowohl *organisatorische* wie auch *technische* Lösungen. Diese sollten sinnvoll aufeinander abgestimmt werden, so dass ein bestmöglicher Schutz der Daten gewährleistet wird. Es macht wenig Sinn, eine Firewall optimal zu konfigurieren und viel Geld in die Installation und die Wartung des Systems zu investieren, wenn die Mitarbeiter unzureichend über die Stärken und Schwächen der Firewalls informiert sind und nicht wissen, wie man sich verhalten sollte (Sensibilisierung, siehe auch Kapitel 4.3).

In den folgenden Kapiteln sollen nun möglichen Lösungen aufgezeigt werden, wie man sich sinnvoll gegen Hacker bzw. grundsätzlich gegen Angriffe aus dem Internet wehren kann, obwohl natürlich ein Restrisiko immer bestehen bleibt.

4.1. Organisatorische Lösungen

4.1.1. Allgemein

Als kernzentrales Problem bei der Sicherheit in Netzwerken ist der Mensch bzw. der Anwender zu sehen. In Unternehmen steigt die Fahrlässigkeit in bezug auf Netzwerksicherheit mit der hierarchischen Entfernung eines Arbeitsplatzes zur Informatikabteilung: „Humans are, by nature, lazy breeds. To most users, the subject of Internet security is boring and tedious. They assume that security of the Internet will be taken care of by experts” (Anonymous, 1997, S. 83). Das Problem hierbei ist vor allem in der ungenügenden *Sensibilisierung* zu diesem Thema von durchschnittlichen Mitarbeitern⁴, welche selbstverständlich auch einen PC und Zugriff auf verschiedenste Netzwerkgerätschaften haben, zu sehen. Dazu kommt die ständig zunehmende Komplexität von IT-Systemen, was wiederum viele Mitarbeiter entmutigt, sich tiefgehend mit diesen zu beschäftigen. Dies ist bei den heutigen Leistungsanforderungen an die Arbeitnehmer auch nicht verwunderlich, wenn diese schlichtweg keine Zeit mehr finden, dies zu tun. Demgegenüber existiert in vielen Unternehmen ein Informatikbereich (wenn dies auch nur ein Mitarbeiter ist), der für die Administration des Netzwerkes und der einzelnen PCs zuständig ist. Hier besteht das Problem vor allem darin, dass möglicherweise benötigte Ressourcen (zeitlich und finanziell) fehlen, um den gestellten Aufgaben nachzukommen.

Die beiden zentralen und sich ergänzenden Faktoren, um organisatorisch die Sicherheit in einem Netzwerk zu gewährleisten, sind einerseits die *Schulung des Verhaltens* jedes einzelnen Mitarbeiters, gleichgültig welche Stellung er in einem Unternehmen einnimmt. Ausschlaggebend ist nur, ob er an einem PC arbeitet oder in irgendeiner Form Netzwerkzugriff hat oder benötigt. Auf der anderen Seite steht die klassische Aufgabe der Informatik, nämlich die (falls möglich) *lückenlose Administration* eines Firmennetzwerkes. (Dutton, 1994, S. 39)

4.1.2. Verhalten der Mitarbeiter

Eine Person mit Zugriffsmöglichkeit auf bestimmte Netzwerkressourcen (bspw. auf Serverlaufwerke, Drucker und andere Dienste) wird durch eine zentrale Administration mit einer eindeutigen

⁴ *Durchschnittlich* soll in diesem Zusammenhang vor allem auf eine nicht vertiefte Technik- oder Informatikkenntnis hinweisen.

Identifikation versehen (bspw. dem Namen, einem Namenskürzel, einer Mitarbeiternummer etc.). Um den Missbrauch einer solchen Identifikation zu vermeiden, schützt man diese in den in der Regel⁵ mit einem *Password*, damit es nur mit dessen Kenntnis möglich ist, sich mit der entsprechenden Identifikation Zugriff zum gewünschten Dienst zu verschaffen. Dieses Verfahren weist aber eine grosse Schwäche auf, nämlich die Wahl des Passwortes: Den Benutzern wird oftmals die Möglichkeit überlassen, das Passwort selber zu wählen oder dieses auch jederzeit ändern zu können. Je nach Wahl, wird es aber aussenstehenden Personen vereinfacht, ein Passwort zu erraten („knacken“). Diesen Gründen zufolge sollten sie den folgenden Regeln entsprechen: Das Passwort benötigt eine *gewisse Länge*, mindestens acht Zeichen, sollte *kein Wort aus einem Wörterbuch* oder *irgendein Eigennamen* sein und *Sonderzeichen und/oder Zahlen* sollten normale Buchstaben ergänzen. Dazu kommt, dass Passwörter *periodisch geändert* werden sollten, dass beim Anpassen eines solchen die entsprechende Applikation überprüfen sollte, ob die *vorhergehenden Regeln eingehalten werden* und dass nach einer bestimmten Anzahl Fehlversuchen beim Anmelden eine *automatische Sperrung* der Identifikation verfügt wird (Eckert, 2001, S. 307-310). Gemäss Fites und Kratz (1993) muss den Mitarbeitern auch vermittelt werden, dass Passwörter niemals an einem *offensichtlichen Platz niedergeschrieben* werden dürfen bzw. dass das schriftliche Festhalten des Passwortes grundsätzlich nicht erlaubt ist. Denn wenn in einem gut administrierten Netzwerk jemand sein Passwort vergisst, dann kann dieses zumeist problemlos und innerhalb einer nützlichen Frist durch den Systemadministrator geändert werden (S. 5).

Weitere Themen, die mit Mitarbeitern kritisch thematisiert werden sollen:

- das mögliche *Speichern von Passwörtern* auf dem eigenen PC, um diese nicht wieder neu eingeben zu müssen.
- das *Verlassen des Arbeitsplatzes*, ohne sich auszuloggen oder zumindest einen Bildschirmschoner zu aktivieren, den man nur mit einem Passwort deaktivieren kann.
- Der *Umgang mit Daten auf einem portablen Computer* (Laptop), der den Mitarbeitern auf allen geschäftlichen und privaten Reisen um die Welt begleitet und bei Verlust des Gerätes ggf. nicht nur wichtige Firmeninformationen gestohlen werden, sondern auch noch verloren sind, weil nie eine Kopie der entsprechenden Daten angelegt wurde.
- das Erkennen von *möglichen Gefahren beim Surfen im Internet*.

Beispiele dafür finden sich im vorhergehenden Abschnitt über *Gefahren*, wobei von zentraler Bedeutung die Virengefahr ist, aber auch das Preisgeben von vertraulichen Informationen im Internet etc.

Als Ergänzung zu einer Mitarbeiter-Identifikationsnummer können sogenannte *SecurID*-Karten verwendet werden. Gemäss Strobel (1997) berechnen diese „über ein Verfahren aus einem internen Schlüssel, der schon vom Hersteller in die Karten programmiert wurde, der aktuellen Zeit und einer PIN⁶ des Anwenders eine Zahl [...]“ (S. 81), welche wie ein zweites Passwort verwendet wird. Ein Benutzer muss seine Personal Identification Number (den sogenannten PIN-Code), sein Passwort und diese von der SecurID vorgegebene Zahl eingeben, um sich erfolgreich in das Unternehmensnetzwerk einzuloggen, wobei der Einlass erst nach erfolgreicher Überprüfung all dieser Angaben gewährt wird.

⁵ Immer mehr in der Praxis anzutreffen sind zudem *biometrische* Identifikationsverfahren.

⁶ Personal Identification Number.

4.1.3. Administrative Aufgaben

Die Netzwerk-administrativen Aufgaben in einem Unternehmen bestehen nicht nur in der zur Verfügung stellen der physischen Infrastruktur (Server, PCs, Kabeln, Hubs etc.), sondern vor allem in der *Verwaltung* eines gesamten Netzwerkes. Serverbetriebssysteme wie Windows NT oder UNIX bieten dazu umfassende Werkzeuge für eine zentrale Rechteadministration, d.h. an *Subjekte* (bspw. Benutzer, aber auch Prozesse oder einzelne PCs) werden Rechte vergeben, damit sie auf gewünschte oder benötigte *Objekte* (bspw. ganze Server, einzelne Dateien, PCs, Prozesse, bestimmte Ports oder Dienste eines Webservers etc.) zugreifen können. Allgemeinste Rechte sind die Schreib- und Leserechte für Dateien, bei vielen Prozessen reicht diese Unterscheidung aber nicht mehr aus, wenn man bspw. an die verschiedensten Dienste auf einem Webserver denkt oder auch in einer Datenbank, wo man eine Fülle weiterer Rechte vergeben kann. In einem Firmennetzwerk handelt es sich oftmals um *statische Rechte*, d.h. ein Benutzer kann bspw. auf einen Ordner auf einem Server ohne Einschränkungen zugreifen. Es besteht aber auch die Möglichkeit, *dynamische Rechte* zu vergeben, d.h. ein Subjekt kann bspw. nur einmal auf ein Objekt zugreifen und dann ändert sich das entsprechende Zugriffsrecht. Ein möglicher Einsatz für ein solches Recht wäre, wenn ein Mitarbeiter seine neue Arbeitsstelle antritt und dabei ein Einmalpasswort für seine Identität erhält. Das dynamische Recht gibt ihm die Möglichkeit, sich nur einmal mit diesem Passwort ans System anzumelden, falls dabei das Passwort nicht geändert wird, verfallen die vergebenen Rechte. Um die Administration zu vereinfachen und auch zu vereinheitlichen, vor allem wenn viele Subjekte mit ähnlichen Bedürfnissen Zugriff haben oder erlangen sollten, dann wird in der Praxis bei der Rechtevergabe auf *Gruppenrechte* zugegriffen: Nicht jedem Subjekt und Objekt werden einzelne Rechte und Rechtebündel zugeordnet, sondern Subjekte und Objekte werden Gruppen zugeordnet, welche die gewünschten Rechte besitzen. Spezielle Abweichungen gegenüber den Gruppenrechten können problemlos vorgenommen werden. (Eckert, 2001, S. 91-96 & S. 124-130)

Weitere zentrale Aufgaben der Netzwerkadministration bestehen einerseits im Erstellen von *Plänen*, *Prozeduren* und *Informationsunterlagen* für die Mitarbeiter, um einen effizienten Einsatz des Netzwerkes gewährleisten zu können, um auch genügend Planungsreserven zu besitzen, falls das Netzwerk stark wachsen sollte und schlussendlich auch um in einem Notfall schnell und zielgerichtet handeln zu können (Dutton, 1994, S. 39). Auf der anderen Seite müssen Alltagsarbeiten erledigt werden, wie bspw. *Protokolldateien* auszuwerten, um zu wissen, wer im Netzwerk wie agiert, wo Schwachstellen im System bestehen, welche man beheben sollte oder wie die Leistungsfähigkeit verbessert werden kann. Dazu kommt natürlich auch das laufende Überprüfen, inwiefern Rechte gewissen Subjekten überhaupt noch zugeordnet sein müssen oder ob gewissen Subjekten der Zugang gänzlich gesperrt werden soll, weil bspw. ein Mitarbeiter überhaupt nicht mehr in der Firma tätig ist.

4.2. Technische Lösungen

4.2.1. Allgemein

Grundsätzlich kann zwischen *Datensicherheit* und *Datenschutz* unterschieden werden. Unter Datensicherheiten fallen Vorkehrungen im Bereich der Stromversorgung und des Backups; es geht also um die Integrität der Daten sowie die Gewährleistung eines Betriebes – Datenschutz. Beim Datenschutz geht es zudem um das Vorbeugen von Missbräuchen, was man mittels Firewall-Systemen

und Verschlüsselungstechniken zu verhindern versucht (Hochschule für Technik und Wirtschaft Chur [HTW Chur], 2002). In den folgenden Ausführungen wenden wir uns der Verschlüsselung, den Antivirenprogrammen und den Firewall-Systemen zu.

4.2.2. Verschlüsselung

Passwörter, Zugriffsbeschränkungen, Zugriffsrechte etc. auf Systeme können zwar einen Benutzer davon abhalten, bequem und schnell auf bspw. ein vertrauliches Dokument zuzugreifen; liegt dieses aber im *Klartext* auf einem Server gespeichert und kann man bspw. den *Softwareschutz* umgehen, indem man sich physisch einer Festplatte bemächtigt, so ist es oftmals problemlos möglich auf die entsprechenden Daten zuzugreifen, weil auf dem eigenen PC kann man sich schnell volle Zugriffsrechte auf eine neu angeschlossene Festplatte gewähren. Noch problematischer ist der Klartext-Datentransfer in Firmennetzwerken oder übers Internet bspw. in einer E-Mail. Das Abhören von solchen Transfers ist in der Tat keine schwere Aufgabe, gibt es doch in Netzwerken viele Schnittstellen (Hubs, Routers, Switches etc.), wo zentral grosse Datenmengen durchfliessen und man mit entsprechenden Software-Werkzeugen auf den verschiedenen Layer-Ebenen Daten mitlesen bzw. einfach systematisch sammelt und dann später auswerten kann. Die Frage, welche bei diesen Problemstellung zutage tritt, ist, wie man Daten verändern kann, damit sie nur mit einem bestimmten Wissen gelesen werden können. Die Lösung liegt dabei in der Verwendung der *Kryptografie* bzw. *Verschlüsselungstechnik*. Ein *Klartext* (bzw. irgendeine Datei) wird dabei durch einen *Algorithmus* mit Einbezug eines *Schlüssels* in den *Chiffretext* umgewandelt bzw. chiffriert (Geuer-Pollmann, 1999, S. 13). Die verschlüsselte Datei besteht dann aus einer chaotischen Abfolge von Zeichen, welche auch bei detaillierter Analyse nicht auf den Ausgangsklartext zurückzuführen ist. Nur mit dem Wissen des Schlüssels ist es möglich, den Klartext wieder herzustellen. Die Sicherheit heutiger Kryptografieverfahren hängt alleine von der *Geheimhaltung* und der *Grösse* der verwendeten *Schlüssel* ab und nicht, wie vielfach angenommen, vom Algorithmus, denn diese werden laufend weiterentwickelt, zum Testen ihrer Sicherheit weltweit publiziert und somit sind sie auch global bekannt⁷. Zudem müsste ja zur Gewährleistung einer umfassenden Sicherheit für jede Datei ein neuer Algorithmus verwendet werden (Fites & Kratz, 1993, S. 24).

4.2.2.1. Symmetrische Verschlüsselung

In der Praxis wird heute zwischen der *symmetrischen* und *asymmetrischen* Verschlüsselung unterschieden und je nach Anwendung das eine oder das andere Verfahren oder beide Verfahren in Kombination (*hybride* Verfahren) verwendet. Bei der symmetrischen Verschlüsselung wird ein Klartext mit einem *geheimen* Schlüssel sowohl chiffriert als auch dechiffriert. Bei allen Verfahren wird der Klartext in Blöcke bestimmter Grösse zerteilt und danach mit dem Schlüssel durch verschiedenste mathematische Funktionen umgewandelt. Beispiele dazu sind die XOR-Funktion, bitweise Verschiebungen, die MOD-Funktion etc. Bekannteste symmetrische Verfahren sind der *Data Encryption Standard* (DES), obwohl heute wegen der Schlüssellänge von 56 Bit als zu unsicher betrachtet, der *International Data Encryption Algorithm* (IDEA; mit 128-Bit-Schlüssel), *Blowfish*

⁷ Algorithmen, Protokolle, Dateiformate etc. werden auch deshalb publiziert, um heute gespeicherte Daten zukünftigen Generationen lesbar zu machen.

(Schlüssel von 32 bis 488 Bits), sowie der *Rijndael-Algorithmus* (128, 196 oder 256 Bits). Die Sicherheit bei diesen Algorithmen hängt alleine von der *Länge des Schlüssels* ab, weil eine *Kryptoanalyse* zur Entschlüsselung des Chiffretextes nicht möglich ist (regelmässige Streuung der einzelnen Bytes). Um einen Chiffretext zu knacken, muss man alle möglichen Schlüsselkombinationen ausprobieren; dieses Vorgehen wird auch *Brute-Force-Attacke* genannt. Weil sich mit jedem zusätzlichen Bit im Schlüssel die möglichen Kombinationen verdoppelt, muss man bei einem 56-Bit-Schlüssel maximal fast 10^{17} Kombinationen testen, bei 128 Bit mehr als 10^{38} und bei 256 Bit mehr als 10^{77} , entsprechend gestaltet sich auch der Aufwand zum Knacken eines Schlüssels, womit man sagen kann, dass ein 128-Bit-Schlüssel beim symmetrischen Verschlüsseln als sicher betrachtet werden kann. Positiv bei diesem Verfahren ist die relativ hohe Geschwindigkeit gegenüber dem asymmetrischen Verfahren zu sehen. Der grosse Nachteil ist, dass man den geheimen Schlüssel auf einem sicheren Kanal austauschen muss, um zwischen zwei Objekten eine sichere Kommunikation aufbauen zu können. Als Anwendungsbeispiel findet sich die *reine* symmetrische Verschlüsselung beim Speichern von Dateien auf lokalen Laufwerken, Servern oder auch Backupsystemen. Konkret zu nennen wäre hierbei die Software *BestCrypt* von Jetico (www.jetico.com), mit welcher man bspw. auf einer Festplatte eines Computers Container einrichten kann, worin Daten sicher gespeichert werden können. Diese Container können per Passwortabfrage geöffnet (mounten) werden und deren Inhalt wird als eigenes Laufwerk dargestellt, wobei von allen anderen Programmen nun auf die darin enthaltenen Dateien zugegriffen werden kann. (Seide & Hansel, 2001, S. 6-19)

4.2.2.2. Asymmetrische Verschlüsselung

Das *asymmetrische* Verfahren der Verschlüsselung will im Kern das Hauptproblem des symmetrischen Verfahrens umgehen, nämlich die problematische Übertragung des geheimen Schlüssels. Durch sogenannte *Falltürfunktionen* (Berechnung eines diskreten Logarithmus oder Zerlegung eines Produktes von zwei oder mehreren Primzahlen in die entsprechenden Faktoren) kann ein *öffentlicher* und *privater Schlüssel* (*public* und *private key*) generiert werden, wobei ersterer nur für die *Chiffrierung* und der Zweite nur für das *Dechiffrieren* verwendet werden kann. Durch die oben erwähnten mathematischen Funktionen kann sichergestellt werden, dass anhand des öffentlichen Schlüssels, der viel wichtigere private Schlüssel wiederum nur mit grossem Einsatz von Rechnerleistung eruiert werden kann. Die Benutzung ist äusserst einfach, man lässt sich ein Schlüsselpaar generieren, verwahrt den privaten Schlüssel unter aller Vorsicht, kann aber den öffentlichen Schlüssel jedermann zusenden. Der Sender nimmt dann den öffentlichen Schlüssel des Empfängers, verschlüsselt damit die Nachricht und nun kann nur noch der Empfänger mit seinem privaten Schlüssel diese Nachricht entschlüsseln. Als bekannteste Verfahren gelten heute der *RSA-Algorithmus* und das *Diffie-und-Hermann-Verfahren*. Ein grosser Nachteil besteht auch bei der asymmetrischen Verschlüsselung und zwar, dass zur Sicherung des privaten Schlüssels vor dem Knacken mit Hilfe des öffentlichen Schlüssels viel grössere Schlüssel als beim symmetrischen Verfahren verwendet werden müssen, was zu einem 100 bis 1000fach grösseren Rechenaufwand führt. Eine sichere Schlüssellänge wird heute erst bei 512 bis 1024 Bit erachtet, teilweise sind auch schon 2048-Bit-Schlüssel in Anwendung. Der Einsatz dieses Verfahrens konzentriert sich auf die Verschlüsselung kleiner Datenmenge, den Schlüsselaustausch (hybride Verschlüsselung), die Passwortgenerierung und digitale Unterschriften. (Seide & Hansel, 2001, S. 19-24)

4.2.2.3. Hybride Verschlüsselung

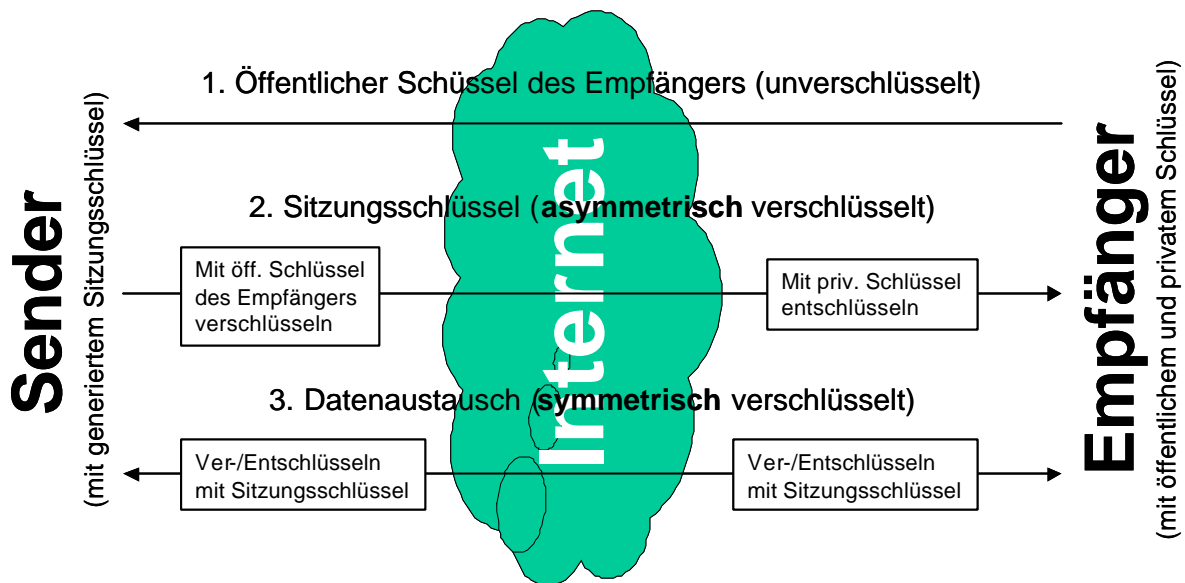


Abbildung 2: schematische Darstellung der Funktionsweise des hybriden Verschlüsselungsverfahrens (eigene Darstellung in Anlehnung an den Text und die darin verwendeten Quellen).

Zur Umgehung der Hauptprobleme der geschilderten Chiffrierungsverfahren verbindet man diese heute vermehrt zur *hybriden* Verschlüsselung (siehe dazu auch die schematische Darstellung dieses Verfahrens in Abbildung 2). Zwischen einem Sender und Empfänger wird dabei *asymmetrisch verschlüsselt* ein vom Sender generierten *Sitzungsschlüssel* (*session key*) dem Empfänger übermittelt. Anschliessend kann die gewünschte Nachricht durch Zunahme dieses Sitzungsschlüssels *symmetrisch chiffriert* und übertragen werden. D.h. das leistungsfähige symmetrische Verfahren wird mit Hilfe der asymmetrischen Verschlüsselung aufgebaut, damit die Sicherheit beim Transfer des geheimen Schlüssels gewährleistet werden kann. Ein Anwendungsbeispiel dafür ist der Zugriff auf eine sichere Webseite bspw. beim Onlinebanking. Aber auch der Einsatz beim Verschlüsseln von E-Mails ist möglich; dabei generiert der Sender einen Sitzungsschlüssel (für jede E-Mail), verschlüsselt damit die E-Mail *symmetrisch* und schickt dann diesen Sitzungsschlüssel mit der gleichen E-Mail aber *asymmetrisch* durch den öffentlichen Schlüssel des Empfängers chiffriert an denselben. Konkret anzufügen wäre hierbei das E-Mail-Verschlüsselungsprodukt *Pretty Good Privacy* (PGP), welches für den nicht-kommerziellen Gebrauch im Netz kostenlos zur Verfügung gestellt wird. Es ist für verschiedenste Betriebssysteme erhältlich und ermöglicht dem Benutzer das Verschlüsseln von E-Mails völlig unabhängig vom verwendeten E-Mail-Client. Zur Generierung des persönlichen Schlüsselpaars stellt diese Software ebenfalls eine Funktionalität bereit, womit gewährleistet ist, dass der private Schlüssel nicht übers Internet auf den eigenen PC transportiert werden muss. (Seide & Hansel, 2001, S. 25-40)

4.2.2.4. Höhe des Verschlüsselungsschutzes

Zusammenfassend kann gesagt werden, dass Verschlüsselungsverfahren einen weitausreichenden Schutz gegen unerlaubten Zugriff auf gespeicherte Informationen oder Informationen in einem Kommunikationsfluss bieten. Der Zugriff kann dabei problemlos stattfinden, denn die entsprechenden Informationen oder Daten sind schlichtweg unlesbar. Nur mit dem *geheimen* (*symmetrisches*

Verfahren) oder *privaten* Schlüssel (*asymmetrische* Verschlüsselung) können die *Chiffretexte* wieder in den ursprünglichen *Klartext* umgewandelt werden. Die folgenden drei wichtigen Faktoren sind zu berücksichtigen, um einen höchstmöglichen Schutz zu erreichen:

1. Verwendung bekannter, getesteter, wenn möglich sogar *zertifizierter Algorithmen*
2. Benutzung einer für das entsprechenden Verfahren *ausreichenden Schlüssellänge*
3. *Absolute Geheimhaltung* des geheimen oder privaten Schlüssels

4.2.3. Antivirenprogramme

Um sich am besten vor Viren zu schützen, ist es sinnvoll, nicht nur Virensuchprogramme zu verwenden, sondern selber vorsichtig zu handeln, indem man beispielsweise vor dem Booten des Computers schaut, ob sich eine Diskette im Laufwerk befindet und diese entfernt, um keinen Boot-Virus zu aktivieren. Dieselbe Vorsicht ist auch geboten, wenn man per E-Mail einen Dateianhang erhält, bei dessen Aufruf der Computer direkt von einem Virus befallen wird oder weitere E-Mails automatisch aus dem eigenen Adressverzeichnis weiterversendet (wie beispielsweise mit dem ILOVEYOU-Virus) und damit weitere Computer mit dem Virus verseucht werden, wobei sich die Viren oft passiv verhalten und erst zu einem späteren Zeitpunkt aktiv Schaden anrichten.

Grundsätzlich kann man verschiedene Antivirenprogramme unterscheiden. Ein Virens Scanner ist das wichtigste Antivirenprogramm. Matzer (1999) definiert einen solchen Virens Scanner folgendermassen: „Ein Virens Scanner ist ein Erkennungsprogramm, das dazu dient, Viren aufzuspüren. Meist geht der Scanner so vor, dass er vorgefundene Dateien im System mit denjenigen Virenmerkmalen vergleicht, die in seinem Katalog im Suchprogramm liegen.“ (S. 26). Um einen möglichst grossen Schutz vor Viren gewährleisten zu können, ist es wichtig, den Katalog immer wieder auf den neusten Stand zu bringen. Dies ist bei den am weitesten verbreiteten Antivirenprogrammen (Norton AntiVirus, McAfee VirusScan) mittels eines Abonnements möglich, indem die neusten Virensignaturen vom Internet heruntergeladen und aktualisiert werden. Beim Norton AntiVirus kann man eine Einstellung vornehmen, sodass die aktuellsten Virenmerkmale nach dem Aufstarten eines Internetbrowsers automatisch auf den Computer herunter geladen werden. Da man allerdings die aktuellsten Merkmale über Internet herunterladen muss, bleibt natürlich auch hier ein Restrisiko vorhanden, ob diese Programm-Updates sicher übertragen werden.

Eine weitere Möglichkeit, Viren aufzuspüren, sind so genannte Prüfsummenprogramme. Diese untersuchen Änderungen an ausführbaren Dateien wie beispielsweise die Dateigrösse. Werden dabei Veränderungen festgestellt, so wird man gleich mittels eines Alarms benachrichtigt. (Matzer, 1999).

Sind irgendwelche Viren durch einen Virens Scanner oder ein Prüfsummenprogramm entdeckt worden, so ist es nun Aufgabe des *Cleaners*, den schädlichen Code zu beseitigen. Vielmals werden diese Codes nach entsprechender Erlaubnis per E-Mail an das Virenforschungszentrum des Antivirenprogrammherstellers gesendet. Dies kann insofern nützlich sein, als damit anderen Kunden Nachrichten über aktuelle Viren im Voraus bekannt gegeben werden können (Matzer, 1999).

Grundsätzlich benutzen Virenprogrammierer stets dieselben Code-Strukturen, sodass ein Antivirenprogramm nicht absolut machtlos gegen unbekannte Viren (d.h. das Virenmerkmal befindet sich nicht im Katalog des Antivirenprogrammes) ist. Wird nun eine solche Code-Struktur vom Programm entdeckt, so ist die Wahrscheinlichkeit hoch, dass es sich hierbei um einen ungewollten Gast im System handelt, das Programm Alarm schlägt und den Virus zu beseitigen versucht. (Matzer, 1999).

4.2.4. Firewall

Grundsätzlich kann zwischen Gefahren im Internet und Gefahren des Internets auf die intern gespeicherten Daten innerhalb eines Unternehmens unterschieden werden. Um den Schutz intern gespeicherter Daten zu erhöhen, können sogenannte Firewall-Systeme installiert werden, die dazu dienen, ein LAN vor Angriffen von aussen, d.h. aus dem Internet, zu schützen. Matzer (1999) definiert eine Firewall als „ein kombiniertes Hard- und Softwaresystem zum Schutz eines lokalen Netzwerks (LAN), das an das Internet angebunden ist“ (S. 178). Ziel eines solchen Systems sollte sein, die Funktionsfähigkeit des LAN zu gewährleisten und intern gespeicherte Daten vor Angriffen, beispielsweise gezielten Attacken von Hackern, abzuschotten..

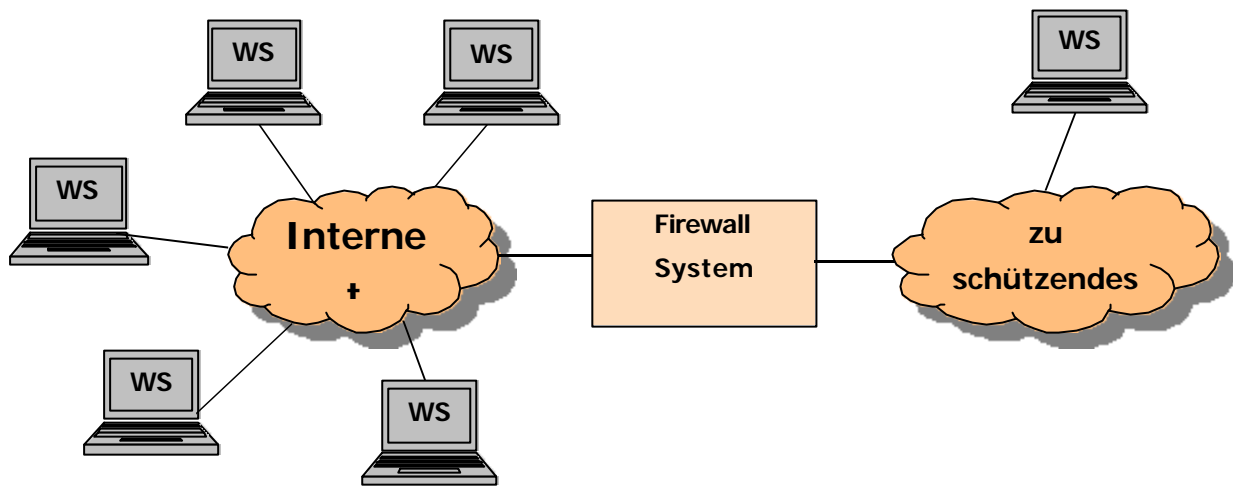


Abbildung 3: Idee des Firewall-Systems und deren Positionierung
Quelle: eigene Darstellung, in Anlehnung an Pohlmann, N. (2001)

Die Idee, die hinter einer Firewall steckt, ist die Verwundbarkeit eines Rechnernetzes auf möglichst einen einzigen Punkt zu begrenzen, da die einzelne Absicherung aller Rechner nicht machbar ist (Kosten- und Organisationsgründe). Deshalb baut man direkt am Internetzugang einer Unternehmung eine Sicherheitsschleuse ein, über welchen „jeglicher Datenaustausch weitergeleitet werden“ (Strobel, 1997, S. 6) muss. Diese Sicherheitsschleuse wird im Fachjargon Firewall genannt. Bei dieser Sicherheitsschleuse können für die Benutzer, Rechner oder Protokolle Kommunikationsrechte definiert werden (Strobel, 1997).⁸

Das Einsatzgebiet einer Firewall ist aber nicht nur auf den Einsatz als Sicherheitsschleuse zwischen einem unternehmensinternen Netzwerk und dem Internet beschränkt. Vielmehr kann sie als Instrument dienen, das firmeninterne Netzwerk zu strukturieren und „Schutzdomänen mit unterschiedlichem Schutzbedarf zu schaffen“ (Pohlmann, 2001, S. 28).

⁸ Pohlmann (2001) sieht die Aufgabe des Firewall-Systems in der Analyse der Kommunikationsdaten, der Kontrolle von Kommunikationsbeziehungen und Kommunikatoren, einem Reglement der Kommunikation, welches auf der unternehmungseigenen Sicherheitspolitik basiert, dem Protokollieren von Ereignissen und einem Alarm an den Security-Administrator bei gravierenden Verstößen.

Innerhalb von Firewall-Systemen kann zwischen zwei verschiedenen Firewall-Architekturen unterschieden werden, nämlich zwischen ein⁹- und mehrstufigen Firewall-Systemen. Dabei bieten die mehrstufigen Systeme eine viel grössere Sicherheit, indem verschiedenen Ebenen nacheinander geschaltet werden. Wird eine erste Ebene durch einen Angreifer überwunden, erkennt eine zweite Ebene diesen Angriff und kann Alarm schlagen. Um diesen Mechanismus in Gang zu setzen, baut man deshalb in die Firewall Überwachungssysteme und Fallen ein, über welche ein Hacker nach Möglichkeit stolpern sollte. Um die Sicherheit vor Angriffen zu erhöhen, geschieht die Implementierung dieser verschiedenen Ebenen auf unterschiedlichen Rechnern (Strobel, 1997).

Zusammenfassend lässt sich den oben geschilderten Aufgaben eines Firewall-Systems entnehmen, dass ein sinnvoll geplantes und gut implementiertes Firewall-System eine Doppelfunktion ausüben kann, nämlich als Schutz vor möglichen externen Gefahren auf ein eigenes Netzwerk sowie als Strukturierungsinstrument für ein Netzwerk inklusive Schutzdomänen.

4.2.4.1. Komponenten und deren Funktionsweise

Nachdem nun die Aufgaben eines Firewall-Systems aufgezeigt und die grobe Positionierung zwischen einem zu schützendem Netzwerk und einem öffentlichen Netz aufgezeigt worden ist, werden nun drei verschiedene zentrale Komponente eines Firewall-Systems (Paketfilter, Application Gateway, Sicherheitsmanagement)¹⁰ und deren Funktionsweise anhand ihres prinzipiellen Aufbaus *kurz* vorgestellt. Die Informationen der folgenden Darlegungen stützen sich auf folgende Quellen: Pohlmann (2001), Strobel (1997), Fuhrberg, Häger & Wolf (2001) und Universität Kaiserslautern (1998).

Paketfilter: Bei der Übermittlung übers Internet werden Daten in Pakete (Datagramme) aufgeteilt. Gelangt ein Paket an einen Filter, so überprüft dieser mittels eines Vergleichs zwischen bestimmten Inhalten der IP-Pakete (normalerweise die Felder des IP-Headers) und den Erlaubnis- oder Verneinungs-Regeln des Paketfilters, ob eine Übereinstimmung der geprüften Werte vorliegt und die Pakete weitergeleitet (geroutet) werden dürfen oder nicht. Ein grosser Nachteil von Paketfiltern ist, dass sie keinen Schutz vor Viren bieten.

Application Gateways bzw. Proxies¹¹: Durch einen Gateway (entspricht einem Rechner) werden zwei Computernetze miteinander verbunden (Bayerischer Rundfunk, 1998). Ein Application Gateway arbeitet, wie dies dem Begriff zu entnehmen ist, auf dem obersten Layer gemässe Referenzmodell (siehe Kapitel 4.1), nämlich der Applikationsebene. Diese Komponente wird in Firewall-Systemen angewendet, da dadurch die Kommunikationsverbindung zwischen einem internen und externen Netzwerk getrennt wird. Strobel (1997) zieht im Vergleich zwischen Application Gateways und

⁹ Die einfachsten Firewallsysteme bestehen aus nur einer Maschine, auf welcher sich z.B. nur Proxies und IP-Filter befinden.

¹⁰ Pohlmann (2001) führt weitere Komponente auf: Stateful Inspection, Proxies und Adaptive Proxies. Auf diese Elemente wird in den Ausführungen dieser Arbeit nicht eingegangen. Zudem werden die drei grundsätzlich zu unterscheidenden Architekturen und deren unterschiedliche Ausgestaltungen (Dual-Homed-Host-, Screened-Host- und Screened-Subnet Architektur) nicht erläutert. Einblicke in diesen Bereich bieten Fuhrberg, Häger & Wolf (2001).

¹¹ In der Literatur werden die Begriffe teilweise als Synonyme verwendet, teilweise werden sie als unterschiedliche Firewall-Komponente betrachtet.

Filtern folgendes Fazit: „Während IP-Filter [...] den Inhalt der Kommunikation nicht berühren und unverändert weiterleiten, kennt der Proxy die Semantik der Verbindung und kann auf der Applikationsebene eingreifen“ (S. 76).¹²

Das *Sicherheitsmanagement* in Form von Programmen oder Rechnern *verwaltet die einzelnen Komponente einer Firewall* und erfüllen u.a. folgende Aufgaben (Auszugsweise aus Pohlmann, 2001, S. 155):

- „Eingabe und Kontrolle der Filterregel
- Eingabe und Kontrolle von Daten, die für den Betrieb der Firewall notwendig sind, z.B. DNS-Informationen, Alias Namen für E-Mails
- Einstellung und Überprüfung der Protokolldaten
- Erstellung und Wiedereinspielen von Backups“

Alle Firewallkomponenten sind prinzipiell gleich aufgebaut und bestehen aus einem Einbindungs- und Durchsetzungsmodul, einem Analysemodul, einem Entscheidungsmodul und einem Regelwerk. Das Einbindungs- und Durchsetzungsmodul ist gemäss Pohlmann (2001) für die „Einbindung des aktiven Firewall-Elements in das Kommunikationssystem sowie die Durchsetzung der im Regelwerk festgehaltenen Sicherheitspolitik“ (S. 30) zuständig. Kommt ein Protokollelement (x_i) in die Firewall-Komponente hinein, so wird es ans Analysemodul weitergeleitet, in welchem die Kommunikationsdaten des Protokollelements analysiert werden. Anschliessend werden die Ergebnisse dem Entscheidungsmodul übergeben. An dieser Stelle kommt nun auch das Regelwerk ins Spiel. Im Entscheidungsmodul werden nämlich die Analyseergebnisse aus dem Analysemodul mit den Definitionen aus dem Regelwerk verglichen. Mit einer Überprüfung wird hier entschieden, ob ein Protokollelement weitergeleitet werden kann oder nicht. Wenn ein Element passieren darf, so wird „das Einbindungsmodul zum Durchlass aktiviert“ (ebd., S. 30). Der Aufbau einer Firewall-Komponente ist in folgender Abbildung dargestellt:

¹² Für differenzierte Ausführungen s. Fuhrberg, Häger & Wolf (2001).

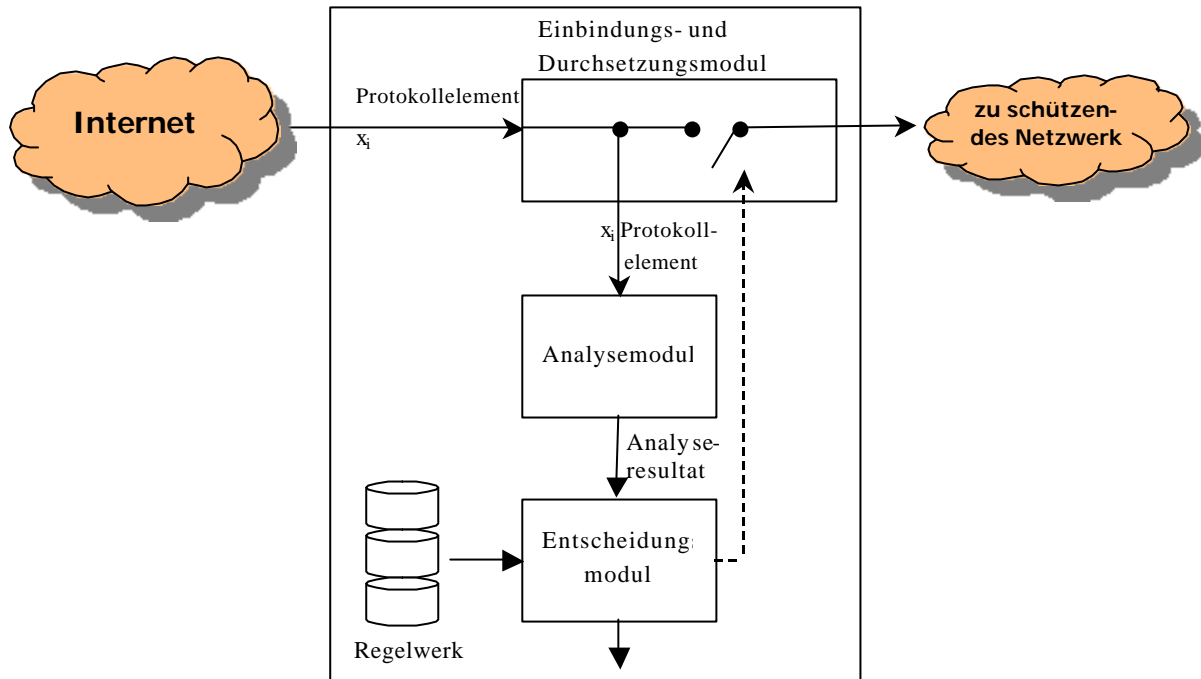


Abbildung 4: Aufbau und Arbeitsweise einer Firewall-Komponente

Quelle: in Anlehnung an Pohlmann (2001).

4.2.4.2. Vor- und Nachteile von Firewall-Systemen

Ein wesentlicher Vorteil¹³ wurde bereits in Kapitel 4.2.4 erwähnt, nämlich die Kostenminimierung eines Firewallsystems, weil damit nicht jeder einzelne Rechner isoliert geschützt werden muss, da mittels einer Firewall die Verwundbarkeit eines Rechnernetzes auf möglichst einen einzigen Punkt begrenzt wird. Zudem sieht Pohlmann (2001) die Protokolliermöglichkeiten als weiteren Vorteil dieses „common point of trust“ (S. 34). Des Weiteren führt er an, dass mit Hilfe einer Firewall die Organisationssicherheitspolitik zentral durchgesetzt werden könne und durch die reduzierte Funktionalität weniger Angriffspunkte bestünden, da sich Angriffe auf diesen einen Übergangspunkt konzentrieren würden und nur dieser auch zu schützen sei (Pohlmann, 2001).

Doch neben diesen Vorteilen existieren natürlich auch Nachteile. Eine der Schwierigkeiten besteht darin, unglücklicherweise in einer Unternehmung Computer mit Modems zu verwenden, die die ganze Idee einer Firewall zunichte machen. Es ist deshalb nötig, die Firewall-Konzepte konsequent umzusetzen und jeden einzelnen Rechner an die Firewall anzubinden. Pohlmann (2001) spricht in diesem Kontext von der Wichtigkeit, dass es neben dem Firewall als zentralen Kommunikationspunkt keinen weiteren Übergang vom Internet zum internen Netzwerk geben sollte. Zudem werden nur Aktivitäten zwischen den OSI-Layern 2 und 7 überwacht (Matzer, 1999). Matzer stellt hierzu fest: „Daten, die innerhalb von Applikationen transportiert werden und unter Umständen in Form von Viren [...] das interne Netzwerk bedrohen, können von ihr nicht blockiert werden“ (S. 182). Als Lösung dieses Problems liegt eine Integration von Antivirenprogrammen in das Firewall-System auf der Hand. Doch auch hier stellt sich wiederum das Problem, dass bei der Konzepterstellung und darauf

¹³ Die Aufzählung von Vor- und Nachteilen erhebt keinen Anspruch auf Vollständigkeit.

basierenden Implementierung eines Systems oft kaum auf derartige Problembereiche geachtet wird. Als letzten Nachteil wollen wir einen von Pohlmann (2001) erwähnten Punkt aufführen, der in diesem Kontext schnell vernachlässigt wird. Bisher wurde jeweils nur von Gefahren von ausserhalb berichtet, doch eigentlich können auch interne Angriffe gestartet werden, wobei Firewall-Systeme zu deren Abwehr kaum geeignet sind und eher „Personal Firewalls und/oder Intrusion Detection Systeme“ (Pohlmann, 2001, S. 35) verwendet werden sollten.

4.2.4.3. Firewall-Produkte

Metagroup (1999) bezeichnet in ihrem „Firewall Evaluation Report 1999“ die Firewallsysteme „AltaVista Firewall 98 4.0, Axent Raptor 5.0, CheckPoint FireWall-1 4.0, Cisco PIX 4.2 sowie SunScreen EFS 2.0x“ als die fünf wichtigsten Firewall-Produkte. Dabei schnitt das Produkt Axent Raptor 5.0 am besten ab, nach einer Bewertung anhand von 300 Kriterien. Diese Untersuchung dauerte zwar sehr lange und in Bezug zur hohen Kriterienzahl kann man doch von einer repräsentativen Untersuchung sprechen, insgesamt darf allerdings nicht vernachlässigt werden, dass der Testsieger auch das für die eigene Unternehmung beste Produkt stellt. Vielmehr muss aufgrund vorgegebener Kriterien dasjenige Produkt ausgewählt werden, welches den eigenen Anforderungen am ehesten genügen kann.

4.3. Sicherheit und Sensibilisierung

Pohlmann (2001) stellt fest, dass eine absolute Sicherheit nicht erreicht werden kann, da eine solche bis dato nicht nachgewiesen werden konnte. Ziel müsse es sein, die Unsicherheit zu kennen und so gering wie möglich zu halten. Gemäss seiner Ausführungen können sich verantwortliche Personen einer Unternehmung vier Sicherheitsziele ins Auge fassen, welche bei der Umsetzung eines Firewall-Systems befolgt werden können. Diese Sicherheitsziele umfassen:

- „alle Unsicherheiten mit grosser Wahrscheinlichkeit vollständig eliminieren.
- möglichst vielen Unsicherheiten mit passenden Sicherheitsmechanismen entgegenzuwirken und damit die Wahrscheinlichkeit eines Schadens durch einen erfolgreichen Angriff auf eine praktisch nicht vorkommende Grösse zu minimieren.
- Unsicherheiten, die nicht verhindert werden können, zu erkennen, um im Angriffsfall im nachhinein angemessen reagieren zu können, mit dem Ziel der Schadensminimierung.
- Angriffe im Vorfeld zu erkennen, damit erst gar kein Schaden auftreten kann“ (S. 29).

Prägende Elemente dieser vier Punkte sind die *Wahrscheinlichkeit, Schadensminimierung und Fokussierung auf mögliche Risiken, um zukünftigen Schäden vor auszusehen*. Es wäre deshalb sinnvoll, vor der Implementierung einer Firewall bzw. eines Firewall-Systems differenziert Anstrengungen zu unternehmen und sich dabei ausreichend Zeit zu genehmigen, um ein möglichst optimales System zu konzipieren, welches den oben genannten Sicherheitsziele nachkommt, um bei grösstmöglicher Sicherheit ein kleinstmögliches Risiko eines möglichen Schadenseintritts einzugehen. Doch wie diese Ausführungen gezeigt haben, wird es nie möglich sein, ein Unternehmensnetzwerk vollkommen zu schützen, wenn man bedenkt, dass hinter allen Sicherheitskonzepten, seien sie organisatorischer

und/oder technischer Art, Menschen stehen, welchen Fehler unterlaufen können¹⁴. In diesem Zusammenhang ist es einmal mehr wichtig zu erwähnen, dass eine Sensibilisierung der Mitarbeiterinnen und Mitarbeiter stattfinden soll, wobei die Sicherheitsphilosophie einer Unternehmung vor allem durch die Geschäftsleitung gestützt werden sollte – dem Management kommt demzufolge eine Vorbildfunktion zu. Insgesamt geht es um eine Philosophie, welche durch die ganze Unternehmung wie eine Kultur ‚gelebt‘ werden müsste. Gemäss unserer Ansicht wäre es durchaus angebracht, Sicherheitsaspekt den einzelnen Angestellten an einer Sitzung, einem Workshop oder im Idealfall mittels einer Schulung nahe zu bringen und ein schriftliches Sicherheitskonzept zu erstellen, ohne dabei gross auf technische Details einzugehen. Vielmehr soll die grundlegende Sicherheitspolitik dargelegt und Zusammenhänge zwischen den einzelnen Sicherheitskomponenten (Passwort, Verschlüsselung, Firewall etc.) aufgezeigt werden. Fuhrberg, Häger & Wolf (2001) umschreiben die Wichtigkeit und Überbringung sicherheitspolitischer Ideen an die Angestellten wie folgt: „Gerade um Akzeptanzprobleme beim Einsatz einer Firewall zu verringern, ist es sehr empfehlenswert, eine Benutzerordnung zu verfassen, die für die Benutzer mehr Informationen als Ver- oder Gebote enthält, da eine Firewall nur ein Hilfsmittel sein kann, um die Sicherheit in einem Netz zu erhöhen. Im Einzelfall sollte sogar die Durchführung von Schulungen geprüft werden, insbesondere dann, wenn spezielle Authentisierungsverfahren eingesetzt werden.“ (S. 139).

¹⁴ Firewall-Systeme sind nur so gut wie die Personen, welche es konfiguriert haben bzw. wie diese von Firewall-Herstellern vorprogrammiert worden sind.

5. Fazit

Wie im Laufe dieser Arbeit gezeigt worden ist, birgt das Internet und dessen Benutzung eine Vielfalt an Gefahren in sich, welche für Unternehmungen aber auch für Privatpersonen hohe Kosten, seien diese finanzieller oder zeitlicher Art, verursachen können. Viren, Würmer oder generell Hackerangriffe usw. aus dem Internet können kleinere Schäden anrichten, aber auch ganze Systeme lahm legen, worunter Geschäftstätigkeiten stark leiden können. Obwohl es insgesamt keine hundertprozentige Lösung gegen diese Gefahren gibt, sollte doch versucht werden, diesen mittels geeigneter *organisatorischer* und *technischer* Vorkehrungen oder Lösungen entgegenzutreten und wenn möglich die entstehenden Schäden zu minimieren.

Entsprechende Vorkehrungen gegen Schnüffeleien, Datenspionage und Datenverluste können ohne grossen Aufwand, beispielsweise in der EMail-Kommunikation, mittels entsprechender Verschlüsselungsverfahren erreicht werden. Für einzelne Computer und Server stehen verschiedene Antivirenprogramme zu Verfügung, die man auch in Firewall-Systeme integrieren kann, um ganze Netzwerke vor Angriffen aus dem Internet abzuwehren. Die einzelnen Komponenten und Instrumente müssen jedoch sinnvoll aufeinander abgestimmt werden. Es nützt im Endeffekt wenig, wenn man ein sehr gutes Firewall-System besitzt, dieses aber nicht durch geeignete Antivirenprogramme und Verschlüsselungstechniken ergänzt. Zusätzlich müssen die gewählten Sicherheitskonzepte stets hinterfragt und bei Bedarf überarbeitet und den aktuellen Bedürfnissen und Gefahren angepasst werden.

Neben diesen technischen Instrumenten sind vor allem für Unternehmen ganzheitliche Sicherheitskonzepte aus organisatorischer Sicht von Bedeutung. Insgesamt geht es darum, neben ausgeklügelten Schutzsystemen und –software die *Sensibilisierung der Mitarbeiter* bezüglich dieser Themenbereiche zu erhöhen und auf die Gefahren des Internet aufmerksam zu machen. Geeignete Vorgehensweisen stellen beispielsweise online verfügbare Massnahmekataloge und Bestimmungen dar, nach denen sich die Mitarbeiter richten müssen. Oft werden jedoch im täglichen Geschäftsverkehr solche Bestimmungen vernachlässigt oder gehen im Stress unter. In solchen Fällen braucht es gegenseitige Aufmerksamkeit, um den Kollegen auf die Sicherheitsbestimmungen aufmerksam zu machen. Als Ergänzung zu schriftlich verfügbaren Informationen eignen sich auch Mitarbeiterschulungen, in welchen die Mitarbeiter, ohne auf technische Einzelheiten einzugehen, auf Gefahren hingewiesen und mögliche Verhaltensregeln aufgezeigt werden.

An dieser Stelle bleibt uns die Erkenntnisse, dass sich ein gezielt eingesetztes, eventuell auf den ersten Blick sehr hohes, Sicherheitsbudget in einer Unternehmung lohnt. Aktuelle Kosten und Folgekosten, die entstehen, wenn Angriffe auf Unternehmen erfolgreich erfolgen, sind meistens höher, als wenn genügend Sicherheitsvorkehrungen getroffen wurden. Deshalb darf die *Prävention* bezüglich Sicherheitsfragen in Unternehmungen nicht zu kurz kommen.

6. Literaturverzeichnis

- Anonymous (1997). *Maximum Security. A Hacker's Guide to Protecting Your Internet Site and Network*. Indianapolis: Sams.net Publishing.
- Bayerischer Rundfunk. (1998). *Internet-Lexikon*. Gefunden am 20.12.2002 unter <http://www.br-online.de/alpha/global/lexikon.html>
- Borchers, D. (2003, 31. Januar). Computerwurm zerfrisst SQL-Server - Microsofts Trustworthy Computing feiert Geburtstag. *Neue Zürcher Zeitung*, S. 75.
- Clearswift. (2002). *Homepage der Firma Clearswift Ltd.*. Gefunden am 11. November 2002 unter <http://www.clearswift.de>
- Dutton, E. (1994). *LAN Security Handbook*. New York: M&T Books.
- Eckert, C. (2001). *IT-Sicherheit. Konzepte - Verfahren - Protokolle*. München: Oldenburg.
- Electronics Today (2000). *Welt in Panik*. Gefunden am 31. Januar 2002 unter http://electronics-today.de/computer-web/welt_in_panic_17-05-00.htm
- Fites, P. & Kratz, M. P. J. (1993). *Information System Security. A Practitioner's Reference*. New York: Van Nostrand Reinhold.
- Fuhrberg, K., Häger, D. & Wolf, S. (2001). *Internetsicherheit. Browser, Firewalls und Verschlüsselung*. (3. Auflage). München/Wien: Carl Hanser Verlag.
- Geuer-Pollmann, Ch. (1999). *Kryptografie, Netzwerk- und Datensicherheit*. Gefunden am 11. Dezember 2002 unter <http://www.nue.et-inf.uni-siegen.de/~geuer-pollmann/publications/Schulen-ans-Netz/Skriptum.pdf>
- Heindl, E., Bücking, J., Emmert, U., (2001). *Der IT-Sicherheitsexperte: Rechtliche und technische Aspekte der Internetnutzung*. München: Addison-Wesley.
- Hochschule für Technik und Wirtschaft Chur [HTW Chur]. (2002). *Theorie*. Gefunden am 05.12.2002 unter <http://www.tlab.ch/praktika/serieIII/c15/theorie/index.html>
- Lindhorst, A. (2002). *Das Einsteigerseminar: Sicherheit im Internet*. Bonn: Moderne Industrie Buch AG.
- Matzer, M. (1999). *Sicherheitsrisiko Internet. Schutzmechanismen beim Surfen, Homebanking, Shopping etc.* München: Beck.
- Metagroup. (1999). *Firewall Evaluation Report 1999*. Gefunden am 25. Dez. 2002 unter <http://www.metagroup.de/studien/Firewall/index.htm>
- Pohlmann, N. (2001), Möglichkeiten und Grenzen von Firewall-Systemen. In: Horster, P. (2001) (Hrsg.): *Kommunikationssicherheit im Zeichen des Internet. Grundlagen. Strategien. Realisierungen. Anwendungen*. Braunschweig/Wiesbaden: Vieweg & Sohn.
- Seide, S. & Hansel, M. (2001). *Dokumenten-Management. Kryptographie beim Dokumenten-Transport*. Gefunden am 11. Dezember 2002 unter http://www.f4.fhtw-berlin.de/people/s0291025/doc/dm_crypto.pdf
- Sicherheitsberater. (2001). *Neues von der Virenfront*. Gefunden am 18. November 2002 unter <http://www.sicherheits-berater.de/2001/0123inews.htm>
- Strobel, S. (1997). *Firewalls für das Netz der Netze. Sicherheit im Internet: Einführung und Praxis*. Heidelberg: dpunkt.
- Universität Kaiserslautern. (1998). *Grundbausteine für Firewalls*. Gefunden am 20.12.2002 unter <http://www.cck.uni-kl.de/~orth/Diplom-Arbeit/Grundbausteine.html>