Bedrohungen und Risiken im Internet

Diplomarbeit im Fach Informatik

vorgelegt

von

Philippe Maurer

von Zürich, Vechigen BE und Zumikon ZH, Schweiz

Matrikelnummer 93-719-573

Angefertigt am

Institut für Informatik

der

Universität Zürich

Prof. Dr. K. Bauknecht

Betreuer: Philipp Kirsch

Abgabe der Arbeit: 13. Februar 1998

Inhaltsverzeichnis

1. Einleitung

1.1 Problemstellung der Arbeit

Ursprünglich wurde das Internet in den 60er Jahren von den USA für militärische Zwecke entwickelt. Damals suchte das US-Militär nach einer Lösung, in einer Krisensituation flächendeckend Informationen austauschen zu können und zwar so, dass bei einem Ausfall eines Netzteils die übrigen angeschlossenen Computer weiterhin miteinander kommunizieren konnten. Inzwischen hat das Internet jedoch an militärischer Bedeutung verloren.

Zu Beginn waren nur die Wissenschaft und die Forschung am Netz vertreten. Mit der Einführung des World Wide Web im Jahre 1992 wurde die Nutzung des Internet jedoch für immer mehr Unternehmungen zu einem wichtigen Geschäftsfeld und Marketinginstrument[1]. Besonders kleine und mittlere Unternehmungen erhalten die Chance, durch die Nutzung des Internet zu profitieren, denn die Internet-Dienste sind hervorragend geeignet, um die Unternehmungen in der Informationsbeschaffung, der Informationsbereitstellung, bei Geschäftsbeziehungen und in ihrer Zusammenarbeit zu unterstützen.

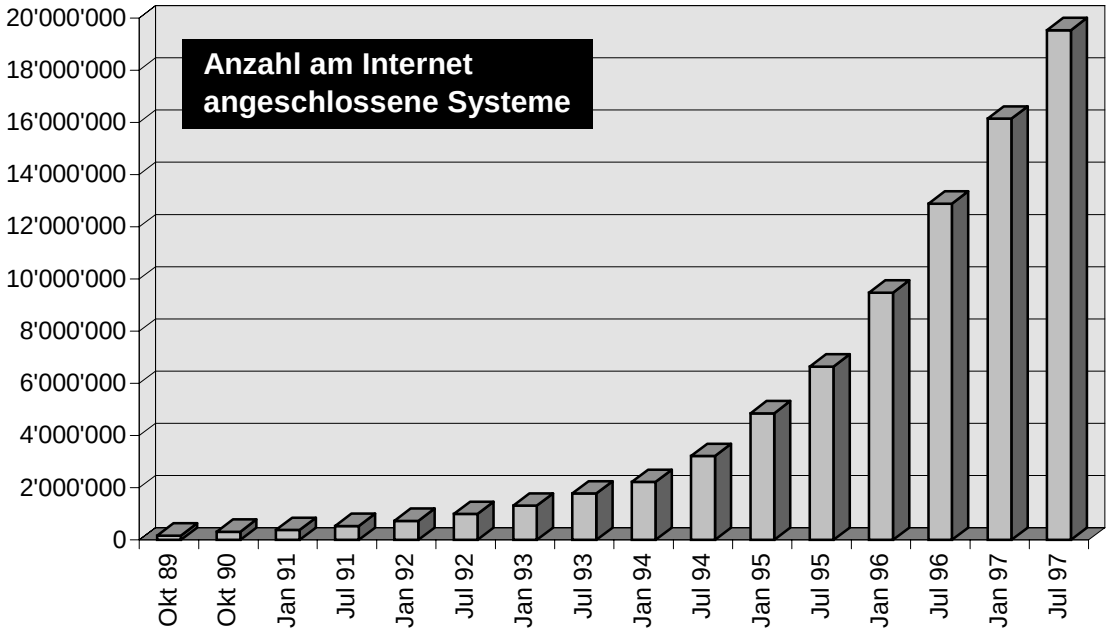

Abbildung 1: Internet-Wachstum[2]

Diesen vielfältigen Möglichkeiten des Internet stehen jedoch ernstzunehmende Risiken im Sicherheitsbereich gegenüber. Sobald nämlich das Firmennetz mit dem weltweiten Internet verbunden wird, entstehen oft unbeachtete Risiken für die Unternehmungen.[3] Proportional zum rasanten Wachstum des Internet (vgl. Abbildung 1) nehmen auch die Einbrüche in Computer-Systeme zu. Dies zeigt u.a. die steigende Anzahl von Sicherheitsvorfällen (vgl. Abbildung 2), welche CERT[4], eine 1988 gegründete Organisation für Sicherheit im Internet, jährlich meldet. Im Vergleich zur Anzahl Systeme, welche am Internet angeschlossen sind,

---

1 Vgl. [Maurer 97].
2 Vgl. http://www.nw.com/zone/
3 Vgl. [Kirsch et. al. 97a] und [Kirsch et. al. 97b].
4 Computer Emergency Response Team

sank jedoch die Quantität der gemeldeten Sicherheitsvorfälle. Dies liegt daran, dass nicht alle Sicherheitsvorfälle gemeldet werden (z.B. aus Angst vor Imageverlusten) und ein Grossteil der Angriffe immer auf dieselben Unternehmungen (z.B. AT&T) ausgerichtet sind.

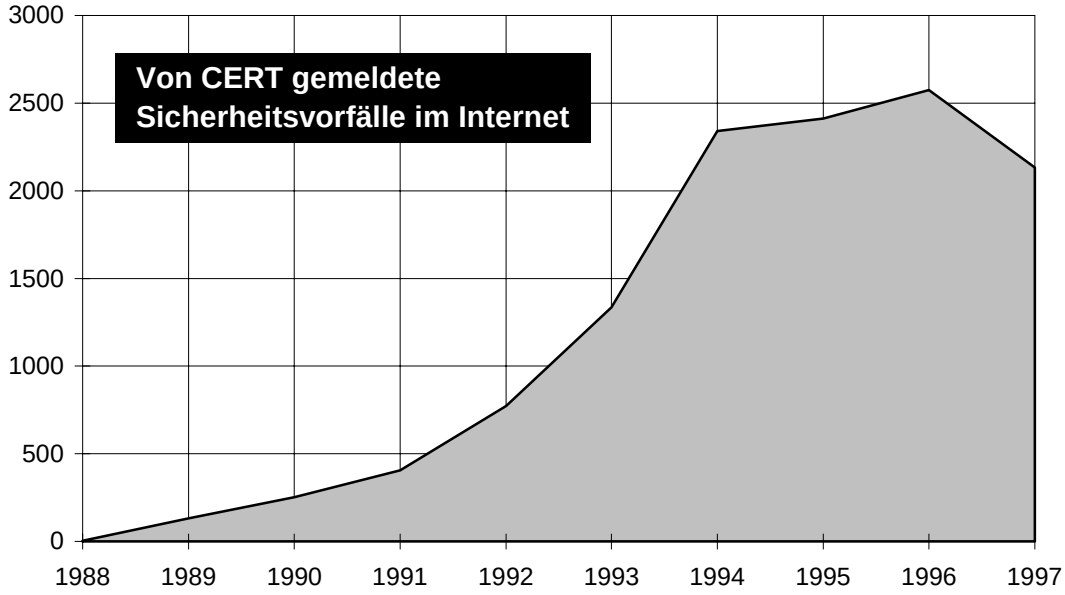

Abbildung 2: Von CERT gemeldete Sicherheitsvorfälle im Internet[5]

1.2 Stand der Forschung

Das Institut für Informatik der Universität Zürich führt in Zusammenarbeit mit SWITCH[6] und der Telekurs AG das SINUS-Projekt[7] durch. Dieses Projekt beschäftigt sich mit den Sicherheitsaspekten beim Anschluss einer Unternehmung an das Internet auf personeller, organisatorischer und technischer Ebene. Zu diesem Zweck wird untersucht, wie die Nutzung von Online-Diensten, das Angebot von Informationen, die Durchführung von Geschäftsbeziehungen und die Zusammenarbeit über das Internet in das Sicherheitskonzept und die informationstechnische Infrastruktur einer Unternehmung eingebettet werden können. Das Projektziel ist die Entwicklung eines integrierten Sicherheitsmanagement-Ansatzes, welcher sowohl organisatorische als auch technische Aspekte berücksichtigt.[8]

1.3 Ziele der Arbeit und Vorgehenskonzept

Ausgehend von den vorhandenen Nutzungspotentialen und Diensten im Rahmen der Sicherheitskonzeption des SINUS-Projekts, hat diese Arbeit das Ziel, die aktuellen Bedrohungen und Schwachstellen im Internet aufzuzeigen. Den identifizierten Bedrohungen und Schwachstellen werden danach personelle, organisatorische und technische Massnahmen gegenübergestellt. Zudem findet eine Untersuchung und Evaluation von Systemen statt, welche die Unternehmung bei der Anbindung an das Internet auf der Suche nach Sicherheitslücken unterstützen.

---

5 Vgl. http://www.cert.org/pub/cert-stats/cert_stats.html
6 Swiss Academic and Research Network
7 Security in Usage of Online Services
8 Vgl. [Weidner 97].

Nach einigen erläuternden Begriffsabgrenzungen und einer Kurzbeschreibung der Nutzungspotentiale des Internet und seiner Dienste wird in den nachfolgenden Kapiteln eine Risikoanalyse durchgeführt. In einem ersten Schritt werden anhand einer Bedrohungsanalyse die Bedrohungspotentiale, welche die Anbindung einer Unternehmung an das Internet mit sich bringt, erarbeitet. Anhand einer Schwachstellenanalyse werden die in einer Unternehmung vorhandenen Schwachstellen in Bezug auf das Internet herauskristallisiert. Aufgrund der sich ergebenden Risiken werden geeignete Massnahmen abgeleitet. Abschliessend werden Werkzeuge zusammengestellt und evaluiert, welche die Unternehmung bei der Erkennung von Schwachstellen unterstützen.

2. Grundlagen

2.1 Begriffsabgrenzungen

2.1.1 Überblick

In der Literatur existieren zahlreiche Ansätze zur Ermittlung des Risikos und zur Ableitung geeigneter Massnahmen gegen diese Risiken. Der grösste Teil dieser Ansätze ist jedoch zu theoretisch bzw. zu komplex und deshalb in der Praxis kaum nachvollziehbar. Bei der Erarbeitung verschiedener Fachliteratur entstand deshalb das in Abbildung 3 gezeigte Modell.

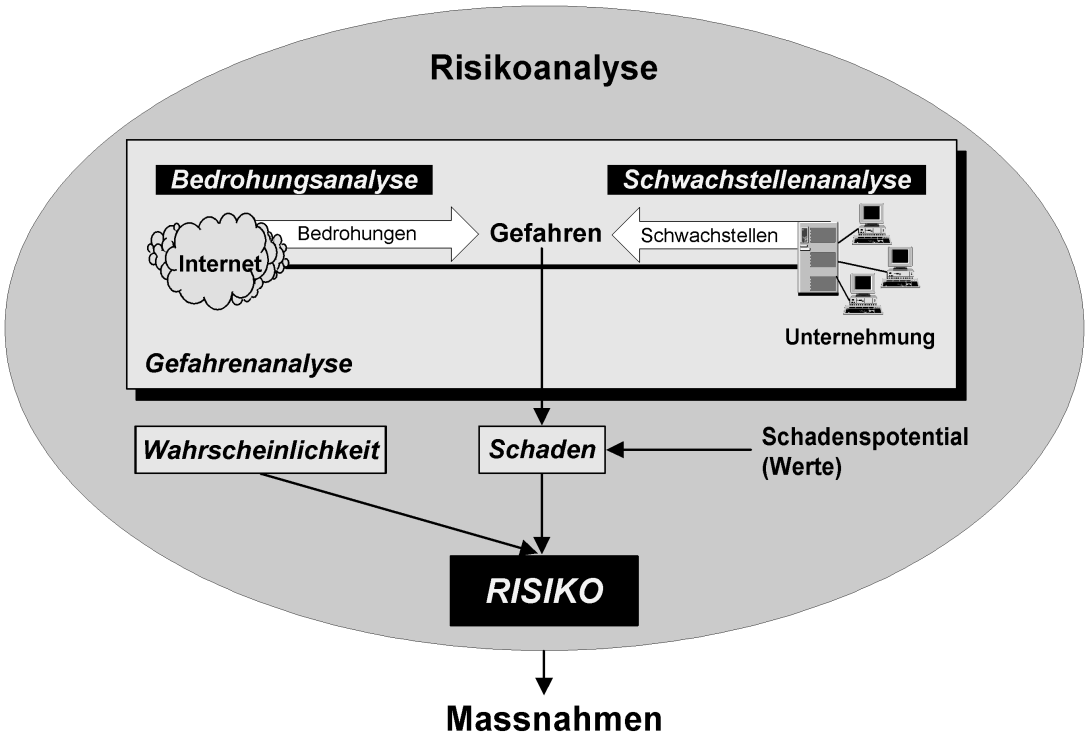

Abbildung 3: Von den Bedrohungen zum Risiko[9]

Das in Abbildung 3 dargestellte Modell veranschaulicht, wie Bedrohung und Risiko miteinander verknüpft sind. Eine Bedrohung entwickelt sich für eine Unternehmung erst dann zu einer Gefahr bzw. zu einem Risiko, wenn das Unternehmungssystem eine oder mehrere Schwachstellen aufweist. Ein Hacker[10] beispielsweise stellt für eine Unternehmung keine grosse Gefahr dar, wenn das Computersystem der Unternehmung eine hohe Sicherheit aufweist (z.B. keine Verbindung zur Aussenwelt). Treffen hingegen die Bedrohungen und die Schwachstellen der Unternehmung aufeinander, so entstehen Gefahren. Durch die Bewertung der negativen Auswirkungen der Gefahren (= Schadenspotential) kann der Schaden (z.B. Wert der Daten) eruiert werden. Das Risiko ergibt sich schliesslich aus der Schadenswahrschein-

---

[9] Vgl. [Alpar 96], S. 159-161; [Bauknecht et. al. 96a], S. 7-15; [Borer 96], S. 7-8; [Heinrich 96], S. 454-465; [Holthaus et. al. 95], S. 24-25; [Kersten 91], S. 45-59; [Kirsch 97], S. 16; [Kirsch et. al. 97a]; [Meli-Isch 95], S. 9-23; [Siyan et. al. 95], S. 116-121; [Stelzer 93], S. 29-40; [Wojcicki 91], S. 24-29.

[10] Personen, welche in fremde Computersysteme, zu denen sie keinen Zugriff haben, eindringen, um dort Daten zu manipulieren.

lichkeit und dem Schadensausmass. Aufgrund des ermittelten Risikos können danach für die einzelnen Bedrohungen die entsprechenden Massnahmen getroffen werden.

2.1.2 Internet

Obwohl der Begriff des Internet aufgrund dessen Popularität weit verbreitet ist, wird er im Alltag immer noch oft falsch verwendet. Ausdrücke wie *"ich möchte einen Computer mit Internet kaufen"* und *"Internetverbindungen in die USA sind teuer"* sind keine Seltenheit. Die folgende Definition des Internet soll deshalb an dieser Stelle Klarheit schaffen:

> *"Das Internet ist eine sich selbst organisierende Ansammlung von verschiedenen Netzwerken und Computern in der ganzen Welt, welche Daten über ein gemeinsames Protokoll (TCP/IP[11]) austauschen."*[12]

Wie die obige Definition präzisiert, erlaubt das Internet (vgl. Abbildung 4) eine Kommunikation zwischen verschiedenen Rechnerarchitekturen. Grundvoraussetzung dafür ist das gemeinsame TCP/IP-Netzprotokoll, mit dessen Hilfe die Daten über das Netz geschickt werden. Dieses Protokoll teilt die zu versendenden Daten in kleine Pakete auf und ergänzt sie mit den erforderlichen Adressinformationen. Dazu gehören Sende-, Empfangsadresse und Sequenznummer. Die Datenpakete legen je nach Verfügbarkeit der Leitungen, Verkehrsbelastung und Übertragungszeit verschiedene Wege zurück. Aufgrund der Adressinformationen wird garantiert, dass jedes Datenpaket den richtigen Empfänger findet, und die Daten schliesslich wieder in der richtigen Reihenfolge zusammengesetzt werden können.[13]

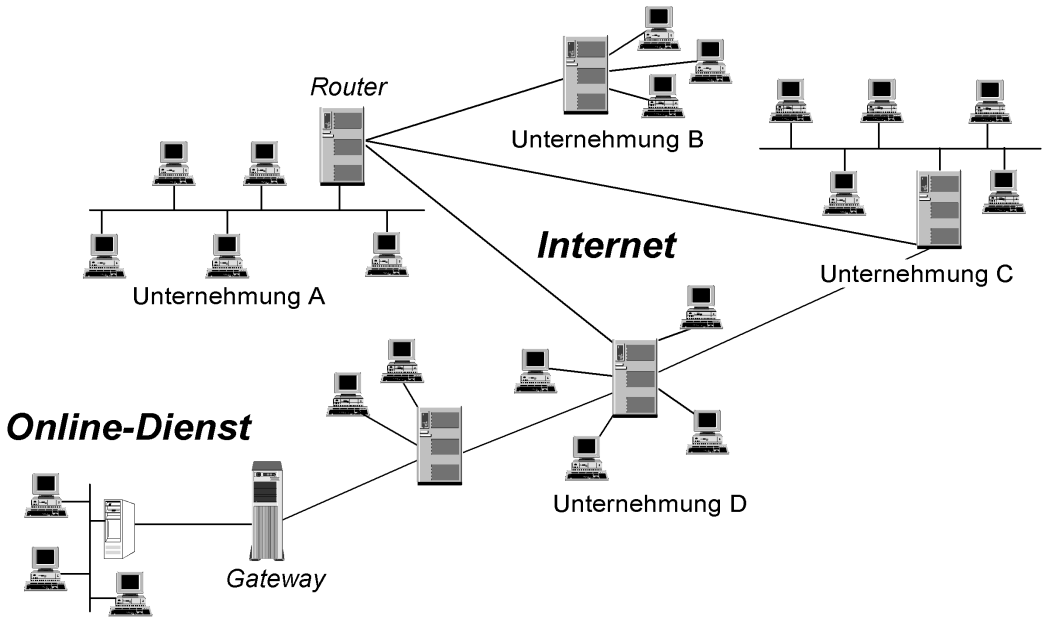

Abbildung 4: Internet und Netze

Damit die Datenpakete ihr Zielnetzwerk auch finden, wird jeder am Netz angeschlossene Rechner über eine eindeutige und unverwechselbare IP-Adresse (z.B. 130.60.48.8) identifiziert. Da diese Dezimalzahlen-Semantik für den Benutzer nur schwer zu durchschauen ist, wurde das bisherige IP-Adressensystem 1986 durch das Domain Name System (DNS), eine

---

[11] Transmission Control Protocol / Internet Protocol

[12] [Marine et. al. 96], S. 1 und [Lampe 96], S. 21-24, zit. in: [Maurer 97], S. 4.

[13] Vgl. [Alpar 96], S. 23-34; [Klau 95], S. 55-65; [Koch 97], S. 48-53; [Kyas 96b], S. 74-97; [Tanenbaum 97], S. 51-54; [Zimmermann 96], S. 4-12.

Methode der Namensverwaltung, ergänzt. Bei der Herstellung einer Verbindung werden die Buchstabenversionen der Adressen (z.B. claude.ifi.unizh.ch) mittels eines Domain-Name-Servers wieder in die äquivalenten IP-Adressen umgewandelt. Jeder Domain-Name-Server verwaltet die Adressen in seinem Bereich. Der SWITCH-Server verwaltet beispielsweise die Domain-Adressen der Schweiz (z.B. unizh.ch), die Universität Zürich wiederum verwaltet die Adressen ihrer Subnetze (z.B. ifi.unizh.ch), die Subnetze ihrerseits verwalten die Adressen der einzelnen Rechner (z.B. claude.ifi.unizh.ch).[14]

Die paketorientierte Übertragung von Daten, wie sie im Internet stattfindet, erfordert eine geeignete Hardwarearchitektur, welche den Übergang zwischen den einzelnen Netzwerken sicherstellt. Zu diesem Zweck gibt es an der Verbindungsstelle von zwei oder mehreren Netzen spezielle Rechnersysteme, die nach festgelegten Regeln einen geeigneten Weg der Daten zum Zielnetzwerk bestimmen können. In der Internet-Architektur wird dabei zwischen Router und Gateways unterschieden. Unter einem *Router* ist ein Rechner zu verstehen, welcher zusammen mit dem IP-Protokoll dafür sorgt, dass die Daten zwischen den Netzwerken ihren Weg zum gewünschten Ziel finden. Sollen jedoch Netzwerke mit unterschiedlichen Kommunikationsprotokollen miteinander verbunden werden, kommen sogenannte *Gateways* zum Einsatz. Ein Gateway verbindet zwei Netze mit komplett verschiedenen Protokollen und ermöglicht den Datentransfer von einem Netz in das andere.[15]

Wird die Internet-Technologie für die innerbetriebliche Kommunikation verwendet, so spricht man von einem **Intranet**[16] . Das Intranet verfügt über dieselben Protokolle und Standards wie das Internet. Die Besonderheit liegt jedoch darin, dass sich die Daten auf einem vom Internet getrennten Server befinden.[17] Eine Erweiterung des Intranet stellt das sogenannte **Extranet** dar, welches ausgewählten Geschäftspartnern der Unternehmung den Zugriff auf interne Web-Applikationen ermöglicht.[18]

2.1.3 Bedrohung

Unter einer Bedrohung versteht man jedes potentielle, negative Ereignis auf ein System von aussen, das zu einem Schaden führen kann.[19]

In der Literatur[20] finden sich folgende Grundbedrohungen, die auf ein System der Informationstechnik einwirken können:

- Verlust der **Vertraulichkeit**
- Verlust der **Integrität**
- Verlust der **Verfügbarkeit**
- Verlust der **Authentizität**
- Verlust der **Verbindlichkeit**

In Kapitel 3 werden diese Grundbedrohungen genauer betrachtet.

---

[14] Vgl. [Alpar 96], S. 49.
[15] Siehe dazu auch [Weidner 97].
[16] lat.: ”intra” = innerhalb
[17] Vgl. [Pohlmann 97], S. 261-265.
[18] Vgl. [Calzo 97], S. 11 und [Rohner 96], S. 63.
[19] Vgl. [Heinrich 96], S. 245 und [Piveteau et. al. 94], S. 149.
[20] Vgl. [Bauknecht et. al. 96a]; [Borer 96], S. 8-9; [Kersten 91], S. 49-52; [Meli-Isch 95], S. 12; [Schaumüller-Bichl 92], S. 41; [Wildhaber 93], S. 19-15.

2.1.4 Risiko

Das Risiko definiert sich als Produkt der Eintrittswahrscheinlichkeit eines unerwünschten Ereignisses in einem bestimmten Zeitraum und dem damit verbundenen potentiellen Schaden (= Auswirkung).[21]

Risiko = Eintrittswahrscheinlichkeit (E) · Auswirkung (A)

2.2 Nutzungspotentiale des Internet für Unternehmungen

Für Unternehmungen ergeben sich im Internet folgende grundlegende Nutzungsmöglichkeiten:

- **Informationsbereitstellung**: Wenn eine Unternehmung im Wettbewerb bestehen will, kommt der Kommunikation zu ihren Stakeholdern[22] eine immer grössere Bedeutung zu. Durch die Bereitstellung von Informationen im Internet kann diesem Punkt Rechnung getragen werden. Die Informationen können dabei die Unternehmung selber, ihre Produkte oder ihre Beziehungen betreffen.
- **Informationsbeschaffung**: Bei der Informationsbeschaffung werden im Internet bereitgestellte Informationen abgerufen. Die Initiative geht dabei von der informationssuchenden Person aus, d.h. die Informationen fliessen nicht automatisch vom Informationsanbieter zum Informationsuchenden, sondern müssen bewusst abgerufen werden.
- **Handel** (*Electronic Commerce*): Diese Kooperationsform bezweckt den Austausch von Gütern, Dienstleistungen und Werten. Der Informationsfluss erfolgt in beide Richtungen, d.h. es besteht ein Angebot und eine Nachfrage.
- **Zusammenarbeit** (*Group Support*): Diese Form der Kooperation umfasst Beziehungen zu Kunden (z.B. Lead-Users[23]), Partner- und Tochterfirmen. Im Gegensatz zum Handel steht bei der Zusammenarbeit die Erfüllung einer gemeinsamen Aufgabe bzw. ein gemeinsames Ziel im Zentrum. Der Informationsfluss erfolgt jedoch, wie beim Handel, in beide Richtungen.[24]

Zur Realisierung dieser Nutzungspotentiale genügen in der Regel die vorhandenen Internet-Dienste.[25] Beispielsweise kann die Bereitstellung von Informationen durch die Nutzung des World Wide Web erwirkt werden. Im Folgenden werden diejenigen Internet-Dienste besprochen, welche die Unternehmungen bei der Realisierung ihrer Nutzungspotentiale unterstützen und deshalb auch gewisse Risiken darstellen.

2.3 Internet-Dienste

2.3.1 Telnet

Telnet stammt ursprünglich aus der UNIX-Welt und ist einer der ältesten Dienste im Internet. Unter Verwendung von Telnet kann ein Benutzer auf einen entfernten Rechner zugreifen,

---

[21] Vgl. [Stelzer 93], S. 41.
[22] Anspruchsgruppen einer Unternehmung (z.B. Kunden)
[23] In vielen Branchen ist das umfassendste Verständnis für Produkte und deren Anwendungsfelder bei einigen wenigen gegenwärtigen Anwendern zu finden.
[24] Vgl. [Borer 96], S. 71-73 und [Griese et. al. 96], S. 21-22.
[25] Vgl. [Kirsch et. al. 97a]

d.h. Tastatur und Bildschirm des Benutzers werden zum zeichenorientierten Terminal des entfernten Rechners. Es ist dazu lediglich ein Zugriffsrecht in Form eines Passwortes nötig.[26]

2.3.2 FTP

Der Transport von Daten aller Art erfolgt im Internet mit dem Programm FTP (File Transfer Protocol). Mit diesem Dienst können Dateien aller Art zwischen zwei Computersystemen übertragen werden. Während Telnet nach dem Aufbau der Verbindung zwischen Client und Server lediglich das interaktive Ausführen von Programmen auf dem Zielsystem ermöglicht, können mit FTP Dateien zwischen den Systemen kopiert werden.[27]

Um ihre Kunden auf gewisse Dateien (z.B. Treiber) zugreifen zu lassen, richten viele Unternehmungen ihren Server als Anonymous-FTP-Server ein, d.h. sie geben einen Bereich des Servers für die Allgemeinheit frei. Für den Zugang zu einem Anonymous-FTP-Server genügt in der Regel der Benutzername "*anonymous*" und als Passwort die eigene E-Mail-Adresse.

2.3.3 E-Mail

Die Electronic Mail, kurz E-Mail genannt, repräsentiert einen der beliebtesten und elementarsten Internet-Dienste. Dieser Dienst ermöglicht die zeitversetzte Übermittlung von Informationen und Nachrichten zwischen zwei oder mehreren Kommunikationspartnern.[28]

Der Transport elektronischer Post wird im Internet durch das SMTP-Protokoll (Simple Mail Transfer Protocol) übernommen, einem auf TCP basierenden Protokoll.[29]

2.3.4 World Wide Web

Telnet, FTP und E-Mail stellen eigentliche Erweiterungen von Diensten dar, die bereits angeboten wurden, als das Internet noch gar nicht existierte. Das World Wide Web (WWW) hingegen ist ein neues, vollständig auf das Internet ausgerichtetes Konzept, das auf bestehenden Diensten und einem neuen Protokoll, dem Hypertext Transfer Protocol (HTTP), beruht.[30] Das World Wide Web basiert auf dem Prinzip des Hypertexts und kommt der Arbeitsweise des menschlichen Gehirns sehr nahe. Hypertextdokumente sind Textdateien, die über sogenannte Links[31] mit einem oder mehreren anderen Textdokumenten verknüpft sind. Hypertextdokumente werden im reinen ASCII-Textformat verfasst und mit Hilfe von HTML[32] gestaltet. HTML ist eine ausgabegerätunabhängige Dokumentenbeschreibungssprache[33], welche die einzelnen Strukturelemente eines Textes beschreibt. In Form eines Hypertextdokumentes können Bild, Ton und formatierter Text in einem Dokument vereint werden.[34] Dies ist auch der Grund für den grossen Erfolg des World Wide Web.

Nachdem das Kernforschungsinstitut CERN[35] in Genf im Jahre 1989 die Entwicklung des World Wide Web in Angriff nahm, entwickelte sich das Internet erstmals auch für kommerzielle Anbieter zu einem wichtigen Geschäftsfeld.[36]

---

[26] Vgl. [Kyas 96b], S. 157-165.
[27] Vgl. [Lamprecht 96], S. 24-25.
[28] Vgl. [Alpar 96], S. 49-50.
[29] Vgl. [Weidner 97], S. 31-33.
[30] Vgl. [Chapman et. al. 96], S. 37-39 und [December et. al. 95], S. 80-95.
[31] Schlüsselwörter, Verbindungen, Verweise
[32] HyperText Markup Language
[33] Vgl. [Perrochon 95], S. 3-7.
[34] Vgl. [Kyas 96b], S. 255-289.
[35] Conseil Européen pour la Recherche Nucléaire
[36] Vgl. [Maurer 97], S. 6-7.

2.3.5 Berkeley r-Tools

Die Befehle rlogin, rsh und rcp waren ursprünglich Bestandteil von BSD[37] , welches von der Universität Berkeley entwickelt wurde.[38]

- **rlogin** (*remote login*): Vom Prinzip her funktioniert rlogin wie Telnet, ist jedoch nur für Verbindungen zwischen UNIX-Systemen vorgesehen. Wie bei Telnet ist eine Berechtigung für das fremde System notwendig, ausser wenn der Zielrechner dem Ursprungsrechner vertraut ist.[39]
- **rsh** (*remote shell*): Dieser Befehl erlaubt es, auf einem fremden Rechner Befehle auszuführen, sofern eine Berechtigung für das fremde System vorhanden ist.
- **rcp** (*remote copy*): Mit dem Befehl rcp können Dateien zwischen Rechnern übertragen werden. Auch hier muss der Benutzer Zugang zum anderen System haben.

2.3.6 Secure Shell

Secure Shell (SSH) ist ein Software-Paket, welches erlaubt, sichere Verbindungen zwischen verschiedenen Rechnern im Internet aufzubauen. Es gilt als sicherer Ersatz für rlogin, rsh, rcp und telnet. Im Gegensatz zu den Berkeley r-Tools findet die Authentisierung nicht anhand von IP-Adressen statt, sondern unter Einsatz von kryptographischen Verfahren. Die Software wurde 1995 von Tatu Ylönen an der Helsinki University of Technology in Finnland entwickelt und ist im Internet frei verfügbar. Das Programm muss sowohl auf dem Server als auch auf den Clients installiert sein.[40]

2.3.7 Weitere Internet-Dienste

Neben den soeben erläuterten Internet-Diensten, existieren eine Reihe weiterer Dienste (z.B. Newsgroups, Internet Relay Chat, Gopher, Archie, Finger, Wais), welche an dieser Stelle nicht näher behandelt werden, da sie für die Analyse der Bedrohungen und Risiken im Internet von geringer Bedeutung sind.

---

37 Version des UNIX-Betriebssystems
38 Vgl. [Weidner 97], S. 35.
39 Vgl. [Luthiger 96], S. 78-80.
40 Vgl. http://www.ssh.fi/ und http://www.cs.hut.fi/ssh/

3. Bedrohungsanalyse

3.1 Aufgabe der Bedrohungsanalyse

Die Grundaufgabe der Bedrohungsanalyse umfasst die Identifikation des aktuellen Bedrohungspotentials. Deswegen werden alle möglichen Bedrohungen und Angreifer ermittelt, denen die sicherheitsrelevanten Elemente[41] einer Unternehmung ausgesetzt sind.[42] Die Bedrohungsanalyse ist ein Bestandteil der Risikoanalyse. Im Rahmen dieser Arbeit werden Bedrohungen betrachtet, welche sich für Unternehmungen durch die Nutzung des Internet ergeben (vgl. Abbildung 5).

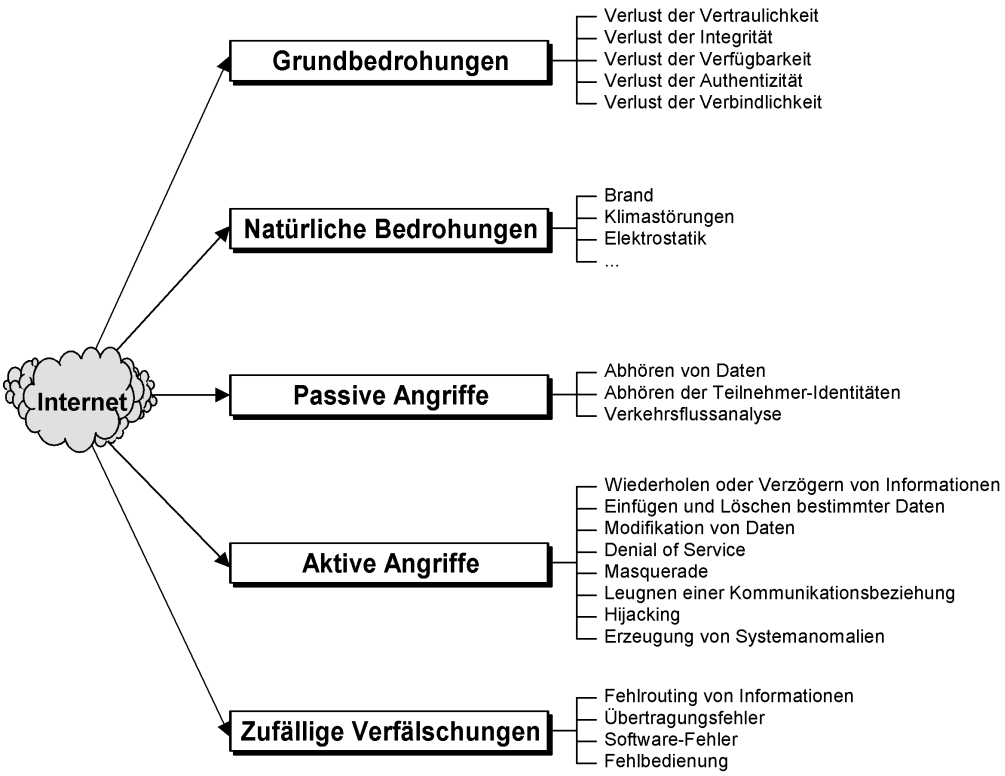

Abbildung 5: Bedrohungen im Internet

Einleitend werden in diesem Kapitel die Grundbedrohungen veranschaulicht, welche auf das informationstechnische System der Unternehmung einwirken können. Da diese Klassifizierung für die Analyse der Bedrohungen allein nicht genügt, wurde zudem eine Einteilung in natürliche Bedrohungen, aktive Angriffe, passive Angriffe und zufällige Verfälschungsmöglichkeiten vorgenommen. Anschliessend an die Schilderung der verschiedenen Bedrohungen werden die verschiedenen Arten von Angreifern bzw. deren Motive beleuchtet.

3.2 Grundbedrohungen

Die klassische Sicht der Informationstechnik sieht nur den Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit als Grundbedrohungen. Im Zusammenhang mit Geschäftsab-

---

41 Alle Elemente der Informationsverarbeitung, die durch Bedrohungen (z.B. Viren) unmittelbar oder mittelbar beeinträchtigt (z.B. Daten) werden können.

42 Vgl. [Schaumüller-Bichl 92], S. 36-37 und [Holbein et. al. 96], S. 272-273.

schlüssen im Internet spielen jedoch die Authentizität und die Verbindlichkeit eine ebenso entscheidende Rolle.

3.2.1 Verlust der Vertraulichkeit

Unter Vertraulichkeit versteht man, dass lediglich berechtigte Personen auf bestimmte Informationen bzw. Daten oder Systeme zugreifen dürfen. Soll die Vertraulichkeit gewahrt werden, dürfen Subjekte, die nicht in den Besitz von Informationen gelangen sollen, technisch gesehen keine Zugriffrechte haben.[43] Beispielsweise musste das BIGA[44] kürzlich sein Arbeitsvermittlungsprogramm im Internet schliessen, weil persönliche Informationen über Arbeitslose für jedermann abrufbar waren. In diesem Fall kam der Verlust der Vertraulichkeit durch ein fehlerhaftes Suchprogramm zustande.[45]

3.2.2 Verlust der Integrität

Mit der Integrität wird der Zustand eines Systems umschrieben, welches das unbefugte oder unabsichtliche (z.B. fehlerhafte Software) Verändern von Daten und Programmen nicht zulässt. Integrität bedeutet, dass alle sicherheitsrelevanten Objekte vollständig, unverfälscht und korrekt sind.[46] Als Beispiel eines möglichen Verlustes der Integrität sollen an dieser Stelle die Computerviren erwähnt werden. Ein Virus kann durch seine Fähigkeit, Daten und Programme zu verändern, die Integrität eines Systems verletzen, sofern es nicht rechtzeitig durch ein Virenschutzprogramm erkannt wird.

3.2.3 Verlust der Verfügbarkeit

Die Verfügbarkeit eines Systems liegt vor, wenn einem Benutzer sowohl Daten als auch das ganze System zu einem bestimmten Zeitpunkt in ihrer vollen Funktionalität zur Verfügung stehen.[47] Der Internet-Wurm ist das Paradebeispiel, wie ein System seine Verfügbarkeit verlieren kann. Innerhalb von wenigen Stunden legte dieses Programm mehrere am Internet angeschlossene Computer lahm, indem es sich Sicherheitslücken von UNIX zunutze machte. Die Verletzung der Integrität führt in der Regel zur verminderten Verfügbarkeit.

3.2.4 Verlust der Authentizität

Authentizität bedeutet, dass verifizierbar ist, ob eine behauptete Identität mit der tatsächlichen Identität übereinstimmt. Die Authentizität befasst sich mit der Echtheit bzw. Glaubwürdigkeit von Kommunikationspartnern und Daten bzw. Informationen. Besonders im Zusammenhang mit dem Internet ist es wichtig, dass nachgewiesen werden kann, ob eine Information vom angegebenen Sender oder Erzeuger stammt. Entscheidungen, die aufgrund von Fehlinformationen gefällt werden, können schwerwiegende Konsequenzen haben. Der Nachweis der Authentizität kann entweder durch elektronische Merkmale (z.B. Chipkarte) oder auf nichtelektronischem Wege (z.B. Identitätskarte) erfolgen. Im Gegensatz zur Integrität, welche sich mit dem Zustand des Systems befasst, beschäftigt sich die Authentizität mit der Übereinstimmung von äusseren Zuständen. Ein Verlust der Authentizität kann jedoch zum Verlust der Integrität führen.[48]

---

[43] Vgl. [Kersten 91], S. 50.
[44] Bundesamt für Industrie Gewerbe und Arbeit
[45] Vgl. [Somm 97], S. 11.
[46] Vgl. [Heinrich 96], S. 245.
[47] Vgl. [Stelzer 93], S. 35.
[48] Vgl. [Wildhaber 93], S. 22.

3.2.5 Verlust der Verbindlichkeit

Seitdem vertragliche Transaktionen über das Internet abgewickelt werden können, stellt sich die Frage nach der Verbindlichkeit. Die Verbindlichkeit kann als Eigenschaft eines Versprechens verstanden werden, denn sie verbindet den Schutz der Urheberschaft und die Integrität einer Information. Dies beinhaltet den eindeutigen Nachweis einer Verbindung oder Transaktion. Die Bedrohung, welche sich zum Beispiel aus dem Nichtanerkennen von Vereinbarungen ergibt, kommt vor allem dann zum Zuge, wenn vom klassischen Datenträger Papier auf ein anderes Medium gewechselt wird und daraus Rechtsunsicherheiten entstehen.[49] Der Verlust der Verbindlichkeit in einem Kommunikationssystem kann auftreten, wenn einer der Kommunikationspartner abstreitet, an einer Kommunikation, wie beispielsweise dem Empfang einer E-Mail, teilgenommen zu haben. E-Mail-Veträge werden vor dem Gesetze einem mündlichen Vertrag gleichgestellt.[50]

3.3 Natürliche Bedrohungen

Jedes System der Informationstechnik unterliegt unabhängig davon, ob es am Internet angeschlossen ist oder nicht, natürlichen Bedrohungen. Zu den natürlichen Bedrohungen zählen Brand, Erdbeben, Blitzschlag, Klimastörungen, Unterbruch der Stromversorgung, Elektrostatik, Bauschäden, Explosionen, Chemieunfälle, Sturm, Wasser, Datennetzausfälle, Störstrahlungen, Fahrzeugunfälle und Tiere. Da diese Ereignisse die Kommunikationssysteme einer Unternehmung auch ohne Anbindung an das Internet bedrohen, werden sie an dieser Stelle nicht weiter behandelt.[51]

3.4 Passive Angriffe

Passive Angriffe verändern die übertragenen Daten und den Betrieb eines Kommunikationssystems nicht. Sie werden jedoch bewusst und gezielt durchgeführt und dienen der unerlaubten Informationsbeschaffung. Der Angreifer verfolgt dabei Übertragungswege und somit die Daten, welche er sogar kopieren kann, ohne Änderungen vorzunehmen. Da bei einem solchen Angriff Personen zu Informationen kommen, die nicht für sie bestimmt sind, handelt es sich bei einem passiven Angriff um eine Verletzung der Vertraulichkeit.[52]

3.4.1 Abhören von Daten

Durch diese Art des Angriffes gelangt ein Angreifer in den Besitz der übertragenen Daten und kann diese für seine eigenen Zwecke verwenden.[53] Um einen solchen Angriff durchzuführen, bedarf es eines Sniffer-Programmes[54] und eines Rechners mit “root”-Privilegien[55]. Das Sniffer-Programm arbeitet rein passiv und erhält alle Daten, welche an den Rechner und seine Subnetze übertragen werden. Eine Erkennung des Abhörprogrammes ist nur auf demjenigen Rechner möglich, auf dem es läuft. Die Programme ETHLOAD und NETWATCH sind Beispiele solcher Snifferprogramme.[56] Ein Provider[57] kann demnach durch die Installation eines

---

[49] Vgl. [Wildhaber 93], S. 21 und [Kersten 91], S. 52.
[50] Vgl. [Maurer 97], S. 22-23.
[51] Vgl. [Panzer 88], S. 57-74.
[52] Vgl. [Wojcicki 91], S. 30-34.
[53] Vgl. [Pohlmann 97], S. 72-73.
[54] Kleine Programme, die auf einen Internet-Host eingeschleust werden und mit denen der ganze Datenverkehr überwacht werden kann, welcher über diesen Host läuft.
[55] Rechte, die es einem Benutzer ermöglichen unbeschränkten Zugriff auf ein System zu haben.
[56] Vgl. dazu auch http://www.cert.dfn.de/infoserv/dsb/dsb-9403.html
[57] Unternehmungen, deren Hauptgeschäft die Anbindung anderer an das Internet ist, werden als Provider bezeichnet.

Sniffer-Programmes den Datenverkehr seiner Kunden abhören und für seine eigenen Zwecke missbrauchen.

3.4.2 Abhören der Teilnehmer-Identitäten

Dieser Angriff dient dazu herauszufinden, welche Teilnehmer untereinander eine Datenverbindung aufbauen und Daten austauschen. Aufgrund dieser Tatsachen, wer zu welchem Zeitpunkt mit wem welche Daten ausgetauscht hat, sind Rückschlüsse über die ausgetauschten Daten und das Verhalten der Benutzer möglich.[58] Ein reger Datenaustausch zwischen den Geschäftsführern zweier Unternehmungen, die bisher keine Kommunikation miteinander pflegten, kann zum Beispiel auf eine Kooperation der beiden hinweisen.

3.4.3 Verkehrsflussanalyse

Werden die Informationen verschlüsselt übertragen, können diese nicht mehr ohne weiteres abgehört werden. Ein Angreifer kann sich aber durch eine Verkehrsflussanalyse Angaben über die Kommunikation der Teilnehmer beschaffen sowie über Informationen, die ihm bei der Entschlüsselung der übertragenen Daten nützlich sein können. Mit Hilfe einer Verkehrsflussanalyse erfährt der Angreifer Zeit, Grösse, Häufigkeit und Richtung eines Datentransfers.[59] Diese Angaben können zum Beispiel für Börsentransaktionen von Interesse sein.

3.5 Aktive Angriffe

Im Gegensatz zu den passiven Angriffen, wird bei aktiven Angriffen der Betrieb eines Kommunikationssystems verändert. Zu den aktiven Angriffen werden sämtliche Aktionen gezählt, welche Daten durch unberechtigtes Nutzen von Ressourcen und Prozessen verändern, löschen oder einfügen.[60]

3.5.1 Wiederholen oder Verzögern von Informationen

Dieser Angriff soll den Empfänger einer Nachricht verunsichern oder zu einer falschen Aktion veranlassen. Die Nachricht wird dabei entweder mehrere Male an den Empfänger geschickt oder es wird eine Verzögerung des Empfangs herbeigeführt, indem die Nachricht aufgezeichnet und zu einem späteren Zeitpunkt wieder eingespielt wird. Der Angreifer kann demnach Benutzeraktionen, ohne Wissen des Benutzers, wiederholt ausführen. Ausserdem können bestimmte Informationen, die über das Netzwerk transportiert werden, solange verzögert werden, bis sie wertlos sind.[61]

So kann zum Beispiel ein Angreifer einen Kaufauftrag eines Grossaktionärs verzögern. Dies wirkt sich für den Angreifer darum positiv aus, weil er gewisse Aktien erwerben kann, bevor dies ein Grossaktionär tut, der eine Übernahme plant. Der Angreifer profitiert durch diese Verzögerung des Kaufauftrages von einem Kursanstieg der Aktien.

3.5.2 Einfügen und Löschen bestimmter Daten

Um eine Systemmanipulation durchzuführen, fügt ein Angreifer bestimmte Daten in bestehende Daten ein oder löscht sie. Der Empfänger wird durch die fehlenden Informationen oder zusätzlich eingefügten Daten zu einem falschen Verhalten veranlasst.[62]

---

[58] Vgl. [Chapman et. al. 96], S. 401-402 und [White et. al. 96], S. 286.
[59] Vgl. [Kimmins et. al. 95], S. 11 und [Bellovin 97], S. 56.
[60] Vgl. [Meli-Isch 95], S. 29.
[61] Vgl. [Wojcicki 91], S. 32.
[62] Vgl. [Pohlmann 97], S. 77.

3.5.3 Modifikation von Daten

Bei einer Modifikation findet eine Veränderung der Daten bei der Übertragung statt. Diese Veränderung ermöglicht es dem Angreifer, falsche Handlungen zu veranlassen.[63] So kann beispielsweise eine Modifikation eines Zahlungsauftrages dazu führen, dass eine andere als die ursprünglich beabsichtigte Person begünstigt wird.

3.5.4 Boykott des Kommunikationssystems (Denial of Service)

Dieser Anschlag wird dazu benutzt, die Verfügbarkeit eines Kommunikationssystem zu stören. Zu diesem Zweck unterbricht der Angreifer entweder die Kommunikationsverbindung oder legt einzelne Dienste und Funktionen lahm.

Bei der einfachsten Form eines solchen Angriffs wird versucht, die Festplatten durch die Übermittlung sehr grosser Datenmengen (z.B. E-Mail-Bombe[64]) zum Überlaufen zu bringen.[65]

Andere Formen des Computervandalismus zielen darauf, die Kommunikation mittels gefälschter ICMP[66]-Pakete zu stören. Im Normalfall dient das ICMP-Protokoll, ein Internet-Steuerprotokoll, dazu, dem Absender eines IP-Paketes Fehlermeldungen anzuzeigen. Diese falschen Fehlermeldungen können entweder einen Abbruch der Verbindung, eine Erhöhung der Netzlast oder eine Umleitung der IP-Pakete über andere Rechnersysteme, verursachen.[67]

3.5.5 Vortäuschen einer falschen Identität (Masquerade)

Um die Authentifizierung zu unterlaufen wird dem System eine falsche Benutzeridentität vorgetäuscht. Dadurch kann der Angreifer Datenmanipulationen durchführen, welche sonst nur einem bestimmten Benutzer zustehen. Auf diese Weise werden Manipulationen an Systemsoftware und Daten möglich.

Eine falsche Identität erlangt ein Angreifer zum Beispiel durch das Ausspähen von Benutzer-ID und Passwort, die Manipulation des Absenderfeldes einer Nachricht oder durch die Manipulation der Kartenadresse der Netzwerkkarte.

Die Erlangung einer falschen Identität kann beispielsweise durch die Duplikation der Authentifizierungs-Sequenz oder durch das Einspeisen gefälschter Daten (Spoofing[68]) in das Netzwerk bewerkstelligt werden.[69] Beispiel: Ein Benutzer verschafft sich unerlaubten Zugang zu einer Firmendatenbank.

3.5.6 Leugnen einer Kommunikationsbeziehung

Einer der Kommunikationsteilnehmer leugnet, dass eine bestimmte Kommunikation oder ein Informationsaustausch stattgefunden hat. Dabei kann es sich entweder um den Sender handeln, welcher abstreitet, eine Nachricht gesandt zu haben oder um den Empfänger, welcher abstreitet, die Nachricht erhalten zu haben. Diese Tatsache führt zu erheblichen Hemmungen

---

63 Vgl. [Pohlmann 97], S. 77.
64 Vgl. http://www.warezdimension.com/mailbmb/
65 Vgl. [Cheswick et. al. 95], S. 199-200 und [Siyan et. al. 95], S. 122.
66 Internet Control Message Protocol
67 Vgl. [Pohlmann 97], S. 101-103.
68 Attacken, welche dem angegriffenen System eine andere Absenderadresse als die eigentlich richtige Absenderadresse vorgeben.
69 Vgl. [Calzo 97], S. 23-24; [Chapman et. al. 96], S. 402-412; [Huber 96], S. 11-13; [Kimmins et. al. 95], S. 11; [Kyas 96b], S. 427-428.

der Geschäftsbeziehungen im Internet.[70] Beispielsweise könnte ein Internet-Benutzer abstreiten, eine Bestellung per E-Mail getätigt zu haben.

3.5.7 Trittbrettfahrer (Hijacking)

Bei einem Hijacking[71] -Angriff schaltet sich der Angreifer in eine bestehende Terminal- oder Login-Sitzung ein, welche vom System bereits authentifiziert wurde, und übernimmt diese. Technisch betrachtet, hängt sich der Angreifer in die Kommunikationsverbindung ein, verfolgt die Login-Prozedur mit und kapert die Login-Bestätigung des Servers. Dem Rechner des autorisierten Benutzer wird ein Verbindungsabbau zugesandt, und der Angreifer verfügt aufgrund des erfolgreichen Login über alle Rechte des autorisierten Benutzers.[72]

3.5.8 Erzeugung von Systemanomalien

Unter Systemanomalien sind solche Situationen zu verstehen, bei denen die Hardware- und Softwarekomponenten die vorgesehene Leistung nicht erbringen. Dies kann einerseits durch Fehler der Systemkomponenten verursacht werden oder es handelt sich um ein beabsichtigtes Fehlverhalten der Systemkomponenten.[73] Die Erzeugung von Systemanomalien wird dazu verwendet, um die unter 3.5 besprochenen Angriffe durchzuführen. Im Wesentlichen existieren folgende Arten von Systemanomalien:

- **Viren**: Als Viren werden sich selbst produzierende Programme bezeichnet, welche sich in andere Programme hineinkopieren und in Verbindung mit diesen bestimmte Funktionen ausführen.[74] Jedes Virus beinhaltet ein Unterprogramm, welches die Vermehrung (z.B. bei jeder Programmausführung) abwickelt und eines, das für die eigentliche Wirkung des Virus (z.B. Löschen von Daten) zuständig ist.[75] Je nach der Form der Infektion wird zwischen Boot-Viren, System-Viren, Programm-Viren, polymorphen[76] Viren, Retro-Viren[77], Stealth-Viren[78] und Daten-Viren unterschieden.[79] Die Wirkungen der Viren sind mit den Möglichkeiten, die ein normales Computerprogramm bietet, zu vergleichen. Im Zusammenhang mit der raschen Zunahme an Internet-Benutzern und dem damit gestiegenen Datenverkehr sind Computerviren nicht mehr bloss für Verwender von Raubkopien eine ernstzunehmende Bedrohung.
- **Würmer**: Ähnlich wie Viren, sind Würmer ebenfalls selbstreproduzierende Programme. Sie sind jedoch im Gegensatz zu Viren eigenständig und laufen deshalb ohne Wirtprogramme. Würmer nutzen sowohl Schwachstellen, Programmierfehler als auch die normalen Mechanismen in Netzwerken und Betriebssystemen aus, um sich fortzupflanzen.[80] Würmer verbreiten sich nur über Netzwerkverbindungen auf andere Computersysteme. Wenn ein Wurm ein System infiziert hat, so sucht er sich die Verbindungen zu andern Computersystemen und kopiert sich selber auf diese noch nicht infizierten Rechner.

---

70 Vgl. [Schaumüller-Bichl 92], S. 44; [Stallings 95a], S. 11; [Wojcicki 91], S. 34.
71 Entführung
72 Vgl. [Chapman et. al. 96], S. 400-401 und [Pohlmann 97], S. 78.
73 Vgl. [Wojcicki 91], S. 34-36.
74 Vgl. [Pohl 93], S. 87-88 und [White et. al. 96], S. 225-235.
75 Vgl. [Schaumüller-Bichl 92], S. 212.
76 Viren, die ihren Programmcode bei jeder Neuinfektion verändern.
77 Viren, welche gezielt Antivirusprogramme beschädigen bzw. löschen.
78 Viren, die ihr Vorhandensein verschleiern (z.B. korrekte Dateilänge des infizierten Programmes).
79 Vgl. [Kyas 96a], S. 113-117.
80 Vgl. [Kersten 91], S. 33.

Neben rein bösartigen Aktionen wie das Löschen von Daten und die Überlastung von Computersystemen, können Würmer auch für die Spionage von Daten eingesetzt werden.[81]

- **Trojanische Pferde**: Programme, welche vorgeben, eine gewisse Aufgabe zu erfüllen, aber in Wirklichkeit eine andere Funktion ausüben, werden als Trojanische Pferde bezeichnet.[82] Ein solches Programm kann beispielsweise aus einer vorgetäuschten Passwortabfrage bestehen, welche ein Passwort nach erfolgter Eingabe speichert und dem Angreifer per E-Mail zusendet. Danach erhält der Benutzer eine Fehlermeldung und das "richtige" Login-Programm wird gestartet.
- **Bomben**: Als Bomben werden solche Programme zusammengefasst, welche den Betrieb eines Rechners stören, sobald sie durch ein bestimmtes Ereignis aktiviert werden. Je nach Typ des Auslösers unterscheidet man zwischen Zeitbomben, welche durch ein bestimmtes Datum oder eine bestimmte Uhrzeit ausgelöst werden und logischen Bomben, die durch bestimmte logische Bedingungen (z.B. Login des Systemadministrators) aktiviert werden.[83]
- **Falltüren**: Als Falltüren werden alle Teile eines Programmes bezeichnet, welche vom Programmierer zu Testzwecken oder in manipulativer Absicht eingebaut wurden.[84] Es ist nur eine Frage der Zeit, bis eine solche Hintertür eines Programmes auch von Angreifern erkannt wird, denn im Gegensatz zu Passwörtern eines Systems, die laufend geändert werden, bleibt eine Hintertür unverändert und entwickelt sich deshalb immer zu einem Risiko.

3.6 Zufällige Verfälschungsmöglichkeiten

Abgesehen von den Bedrohungen, welche die Kommunikationssysteme durch aktive und passive Angriffe erfahren, gibt es auch unbeabsichtigte Verfälschungsmöglichkeiten, die ein System bedrohen.[85]

3.6.1 Fehlrouting von Informationen

Die im Internet übertragenen Informationen können von den Routern an falsche Teilnehmer geleitet werden. Dieses Fehlrouting ist auch schon beim Verbindungsaufbau möglich, wobei eine Verbindung zu einem falschen Teilnehmer hergestellt wird.

3.6.2 Übertragungsfehler

Durch ein Übersprechen von Nachbarkanälen oder Wählgeräusche können Übertragungsfehler entstehen. Die Wahrscheinlichkeit eines solchen Bitübertragungsfehlers liegt jedoch zwischen 10^{-4} und 10^{-7} und ist somit relativ gering.

3.6.3 Software-Fehler

Ein Grossteil der Software (ca. 99%) ist nicht verifiziert. Dies bedeutet, dass jede Software Fehlern unterliegt, welche in gewissen Situationen zu Fehlreaktionen führen können.

3.6.4 Fehlbedienung

"Irren ist menschlich", besagt ein altes Sprichwort. Viele Bedrohungen gehen von Benutzern aus, die Aktionen auslösen, welche aus einer Fehlbedienung resultieren. So wird beispiels-

---

81 Vgl. [White et. al. 96], S. 235-241.
82 Vgl. [Schaumüller-Bichl 92], S. 214.
83 Vgl. [Kersten 91], S. 32.
84 Vgl. [Cheswick et. al. 95], S. 194-196.
85 Vgl. dazu [Pohlmann 97], S. 79-80.

weise eine vertrauliche E-Mail der Personalabteilung, statt an den Personalchef, an einen Mitarbeiter geschickt.

3.7 Typen von Angreifern

Im Anschluss an die Besprechung der Bedrohungen, welche vom Internet ausgehen, soll nun eine Übersicht über die verschiedenen Haupttypen von Angreifern gegeben werden.[86]

3.7.1 Joyrider

Als Joyrider werden Leute bezeichnet, die aus Langweile oder zur Abwechslung in Computersysteme eindringen. Diese Personen handeln grundsätzlich nicht böswillig. Um ihre Spuren eines Einbruchs zu verwischen, richten sie in den Systemen jedoch häufig Schaden an. Je bekannter eine Unternehmung bzw. je ungewöhnlicher das Computersystem, desto attraktiver ist ein Angriff für solche Personen.

3.7.2 Vandalen

Vandalen sind Personen deren Hauptziel die Zerstörung eines Computersystems ist. Ihre Motive sind entweder Spass oder Rachegefühle gegenüber einer Unternehmung. Haben Vandalen einmal ihren Feind auserkoren, so setzen sie alles daran, ihren Angriff erfolgreich abzuschliessen. Meistens kommen Vandalen aus dem nahen Umfeld einer Unternehmung. Beispielsweise gibt es immer wieder entlassene Mitarbeiter, die durch einen Vandalenakt ihren Unmut gegenüber der Unternehmung ausdrücken.

3.7.3 Punktejäger

Ein Punktejäger kann als eine Art Casanova[87] der Computersysteme bezeichnet werden. Diese Art der Angreifer haben das Ziel, in möglichst viele unterschiedliche Computersysteme einzudringen. Je sicherer und bekannter das Computersystem ist, in das sie eingedrungen sind, desto mehr Punkte erzielen diese Angreifer.

3.7.4 Spione (Industrie und andere)

Das Ziel der Spionage liegt im Ausspähen von elektronisch gespeicherten Daten und Programmen.[88] Wenn Spione geheime Informationen finden, werden sie nach Möglichkeit versuchen, diese in Geld umzusetzen. Erfolgreiche Spionageangriffe werden relativ selten sofort entdeckt, da die Spione in das System einbrechen und Daten kopieren, ohne etwas zu zerstören.

3.7.5 Erpresser

Im Gegensatz zu den bereits behandelten Angreifern zielen Erpresser nach erfolgreichem Einbruch in ein System, weder auf eine Zerstörung noch auf eine Entwendung von Daten, sondern sie drohen lediglich damit, um eine bestimmte Leistung zu erzwingen.

Der jüngste Fall einer Erpressung im Internet betrifft eine Gruppe von Hackern, welche in die Internet-Suchmaschine Yahoo[89] eingedrungen waren und dort mit einer massenhaften Ver-

---

[86] Vgl. dazu [Chapman et. al. 96], S. 11-15.
[87] Frauenheld
[88] Vgl. [Pohl 93], S. 34-35.
[89] http://www.yahoo.com/

breitung eines Computervirus gedroht hatten, wenn ein inhaftierter Hackerkollege nicht freigelassen würde.[90]

3.7.6 Unbeabsichtigte Angreifer

Ein Grossteil der Katastrophen werden jedoch nicht durch Böswilligkeit hervorgerufen, sondern entstehen als Folge von Unfällen oder dummen Fehlern. Ursache sind naive oder schlecht geschulte Mitarbeiter, die durch ihr unabsichtliches Fehlverhalten den Computersystemen Schaden zufügen. Zum Beispiel gibt es immer wieder Mitarbeiter, die durch mehrmaliges Senden einer E-Mail mit falscher Empfängeradresse den Mailserver überlasten.

3.8 Zusammenfassung und Beurteilung

Durch die Anbindung einer Unternehmung an das Internet setzt sich diese unterschiedlichen Bedrohungen aus. Diese lassen sich in die klassischen Grundbedrohungen, in natürliche Bedrohungen, in aktive und passive Angriffe sowie in zufällige Verfälschungsmöglichkeiten unterteilen. Zum Abschluss dieser Bedrohungsanalyse des Internet werden die klassischen Grundbedrohungen eines Informationssystems den Bedrohungen, welche sich durch einen Einsatz des Internet ergeben, gegenübergestellt (vgl. Abbildung 6). Wie diese Gegenüberstellung zeigt, sind Softwarefehler und Systemanomalien wie z.B. Viren in sämtlichen klassischen Grundbedrohungen enthalten. Dies bedeutet, dass sich die vielfältigsten Bedrohungen aufgrund von Softwarefehlern und Systemanomalien ergeben. Es gilt nun in einem nächsten Schritt, die Schwachstellen einer Unternehmung zu eruieren, die sich aufgrund des Interneteinsatzes ergeben.

	Verlust der Vertraulichkeit	Verlust der Integrität	Verlust der Verfügbarkeit	Verlust der Authentizität	Verlust der Verbindlichkeit
Natürliche Bedrohungen					
z.B. Brand			√		
Passive Angriffe					
Abhören von Daten	√				
Abhören der Teilnehmer-Identitäten	√				
Verkehrsflussanalyse	√				
Aktive Angriffe					
Wiederholen von Informationen	√	√			
Verzögern von Informationen	√	√	√		
Einfügen und Löschen von Daten	√	√	√	√	√
Modifikation von Daten	√	√	√	√	√
Denial of Service			√		
Masquerade	√			√	
Leugnung der Kommunikation					√
Hijacking				√	√
Systemanomalien	√	√	√	√	√
Zufällige Verfälschungen					
Fehlrouting von Informationen	√		√		√
Übertragungsfehler	√		√		√
Software-Fehler	√	√	√	√	√
Fehlbedienung	√	√	√	√	√

Abbildung 6: Grundbedrohungen und Bedrohungen im Internet

[90] Vgl. [NZZ 97], S. 20.

4. Schwachstellenanalyse

4.1 Aufgabe der Schwachstellenanalyse

Nach der Ermittlung der Bedrohungen, welche im Internet anzutreffen sind, gilt es nun die in einer Unternehmung vorhandenen Schwachstellen zu analysieren. Anhand einer Schwachstellenanalyse werden die potentiellen oder bereits bekannten Schwachstellen einer Unternehmung ermittelt. Es wird deshalb eine gezielte und konsequente Analyse und Beschreibung aller Mängel und Fehler, welche beim Interneteinsatz einer Unternehmung auftreten, vorgenommen.[91]

In diesem Kapitel werden die Schwachstellen aus menschlicher, organisatorischer und technischer Sicht besprochen (vgl. Abbildung 7), wobei der Schwerpunkt zweifellos bei den technischen Schwachstellen liegt.

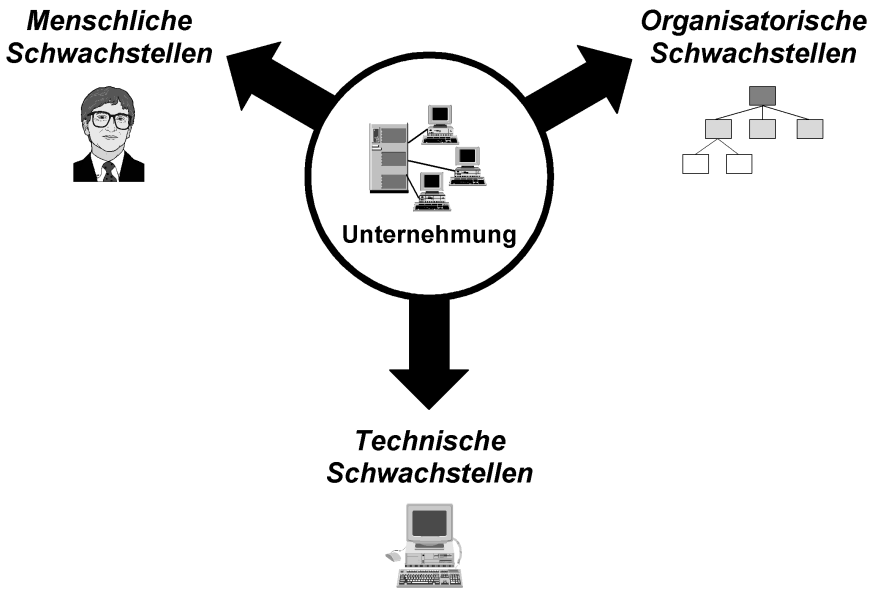

Abbildung 7: Schwachstellenanalyse

4.2 Menschliche Schwachstellen

Unter den menschlichen Schwachstellen werden diejenigen Sicherheitslücken zusammengefasst, welche sich im personellen Bereich ergeben. Als potentielle menschliche Schwachstellen einer Unternehmung gelten alle Personen, die sich durch ihre Arbeit Wissen über das Unternehmungssystem angeeignet haben. Es handelt sich bei diesen Individuen entweder um aktuelle Mitarbeiter oder ehemalige Mitarbeiter der Unternehmung.

4.2.1 Mitarbeiter

Jede Person, die sich den Zugang zu einem System der Unternehmung verschaffen möchte, benötigt dazu eine Berechtigung, zum Beispiel in Form eines Passwortes. Alle Mitarbeiter, welche aufgrund ihrer Arbeit auf einen Zugang zu einem Unternehmungssystem angewiesen sind, bekommen dafür eine Zugangsberechtigung. Da die meisten Zugangsberechtigungen

[91] Vgl. [Schaumüller-Bichl 92], S. 37 und [Wojcicki 91], S. 25-26.

nicht an die Persönlichkeit (z.B. Fingerabdruck) des Mitarbeiters gebunden sind, stellen diese eine potentielle Schwachstelle für das Unternehmungssystem dar.

Sobald Mitarbeiter über eine Zugangsberechtigung zu einem System verfügen, kommen folgende negativen Eigenschaften zum Tragen:

- **Fahrlässigkeit:** Ein überwiegender Teil der Mitarbeiter sind sich des Wertes ihrer Zugangsberechtigung nicht bewusst und gehen deshalb grob fahrlässig damit um. Welche Person würde freiwillig ihre Autoschlüssel, für jedermann zugänglich, herumliegen lassen? Im Gegensatz zu Autoschlüsseln ist dies bei Zugangsberechtigungen mittels Passwort keine Seltenheit, da oftmals zu unsichere Passwörter (z.B. Vorname) gewählt werden. Obwohl sich die Mitarbeiter des unsicheren Passwortes bewusst sind, wählen sie es. Der Grund für die schlechte Passwortwahl liegt in der Vergesslichkeit und Bequemlichkeit des Menschen.
- **Naivität**: In der Fachliteratur wird die Naivität bzw. Gutgläubigkeit des Menschen unter dem Begriff des "Social Engineering" zusammengefasst. Das Social Engineering umfasst alle Methoden eines Angreifers, die darauf zielen, durch geschickte Kommunikation mit Personen den Zugang zu einem System zu erlangen.[92] Beispielsweise täuscht der Angreifer einen Mitarbeiter vor, der sein Passwort vergessen hat und dringend Zugang zum System benötigt, um einen für die Firma immens wichtigen Auftrag zu Ende führen zu können.
- **Wissensmangel**: Fehlendes Know-how der Mitarbeiter stellt eine Schwachstelle der Unternehmung dar. Dieser Wissensmangel äussert sich in Fehlern beim Umgang mit dem Unternehmungssystem. So verschickt beispielsweise ein unerfahrener Mitarbeiter vertrauliche Mitteilungen unverschlüsselt über das Internet.
- **Käuflichkeit**: Mitarbeiter, die über spezifisches Wissen des Unternehmungssystems verfügen, vermitteln dieses Wissen an unternehmungsfremde Personen und erhalten im Austausch dazu eine entsprechende Leistung (z.B. einen besseren Job).

4.2.2 Ehemalige Mitarbeiter

Im Unterschied zu den aktuellen Mitarbeitern einer Unternehmung besitzen die ehemaligen Mitarbeiter im Normalfall keine Zugangsberechtigung zum Unternehmungssystem mehr. Jedoch verfügen einige ehemalige Mitarbeiter über ein umfassendes Know-how über die Systeme der Unternehmung und ihre Sicherheitskonzepte. Die Existenz solcher Wissensträger stellt für die Unternehmung eine Schwachstelle dar, da diese Personen nicht mehr unter Kontrolle der Unternehmung stehen.

4.3 Organisatorische Schwachstellen

Organisatorische Schwachstellen ergeben sich durch die Interaktionen von Mensch und Unternehmung, Technik und Unternehmung sowie Mensch und Technik. Es handelt sich dabei entweder um *logische* organisatorische Schwachstellen (z.B. Passwörter) oder *physische* organisatorische Schwachstellen (z.B. Standorte der sicherheitsrelevanten Elemente). Im Folgenden werden die wichtigsten logischen und physischen organisatorischen Schwachstellen, die im Zusammenhang mit der Anbindung von Unternehmungen an das Internet auftreten, beschrieben.[93]

---

[92] Vgl. [Cheswick et. al. 95], S. 192-194; [Kleiner 97], S. 47; [Pohlmann 97], S. 304; [Resch 96], S. 95.
[93] Vgl. dazu auch [Borer 96], S. 55-56.

4.3.1 Logische organisatorische Schwachstellen

Die logischen organisatorischen Schwachstellen umfassen alle Probleme, die sich aufgrund von Software ergeben.

Als zentrales organisatorisches Problem gilt das Management der Zugangsberechtigungen eines Systems. Es wird dabei geklärt, wie die nicht-physischen Zugriffsrechte eines Systems (z.B. Account auf einem System) auf die Mitarbeiter der Unternehmung verteilt werden sollen.

So ist es beispielsweise nicht sinnvoll, die Zugriffsrechte nach Hierarchiestufen zu verteilen, sondern viel eher nach dem Arbeitsinhalt oder nach den Fähigkeiten im Umgang mit Computersystemen. Jeder Mitarbeiter hat genau diejenigen Zugriffsrechte die er effektiv benötigt.

Eine weitere Schwachstelle sind die Standard-Zugangsberechtigungen (z.B. Guest-Account). Diese bieten den Angreifern eine ideale Basis für ihre Einbrüche in das System.

4.3.2 Physische organisatorische Schwachstellen

Zu den physischen organisatorischen Schwachstellen einer Unternehmung gehören alle Fehler und Mängel, welche die Organisation der materiellen Objekte betreffen. Dazu zählen insbesondere Infrastruktur, Hardware, Datenträger und Dokumentationen.[94]

Der Standort der materiellen Objekte stellt dabei eine der wichtigsten physischen organisatorischen Schwachstellen dar. Es gilt dabei die Frage zu klären, wo die materiellen Objekte aufbewahrt werden sollen. Beispielsweise stellt ein schlecht gesicherter Raum (z.B. Eingangshalle) als Standort eines Servers eine physische organisatorische Schwachstelle dar.

4.4 Technische Schwachstellen

Bei der Analyse der technischen Schwachstellen werden alle Sicherheitslücken ermittelt, die sich durch den Anschluss einer Unternehmung an das Internet auf technischer Ebene (dies betrifft sowohl die Hardware als auch die Software) ergeben. Die technischen Schwachstellen zeigen sich in der Architektur des Datennetzes und in der Implementierung seiner Funktionen.[95] Aufgrund seiner Komplexität ist das Internet, wie auch seine Hard- und Softwarekomponenten, von Programm- und Funktionsfehlern umgeben.[96] Um die technischen Schwachstellen zu untersuchen, empfiehlt sich eine Analyse der einzelnen Schichten des TCP/IP-Schichtenmodells (vgl. Abbildung 8).

Nachstehend werden die Sicherheitslücken, welche der Interneteinsatz mit sich bringt, anhand einer Analyse der Kommunikationsprotokolle und der Internet-Dienste ermittelt.

---

94 Vgl. [Holthaus et. al. 95], S. 25.
95 Vgl. [Wojcicki 91], S. 26.
96 Vgl. [Kyas 96b], S. 425-434.

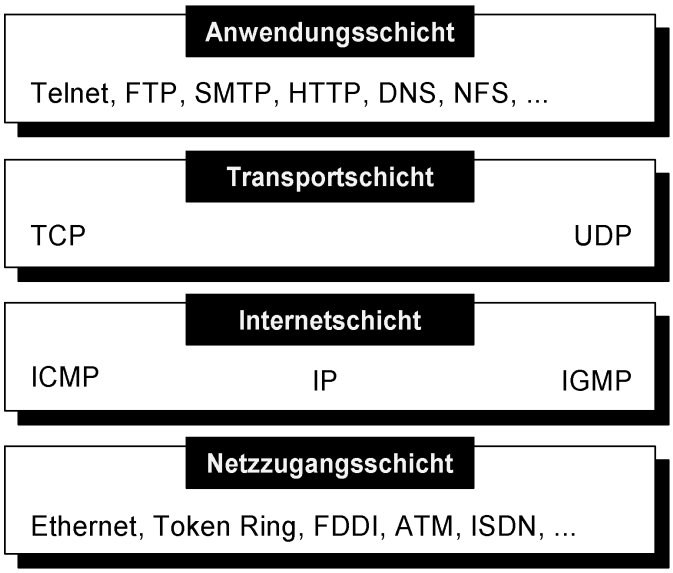

Abbildung 8: Das TCP/IP-Schichtenmodell[97]

4.4.1 Kommunikationsprotokolle

Die Kommunikationsprotokolle beinhalten die Regeln nach denen die Kommunikation zwischen Computersystemen abläuft. Es liegt deshalb auf der Hand, dass diese Protokolle, welche den eigentlichen Transport von Daten im Internet übernehmen, einen Angriffspunkt darstellen.[98]

IP (Internet Protocol): Das IP-Protokoll stellt die Basis für alle höheren Kommunikationsprotokolle dar. Es regelt die Adressierung der Datenpakete im Internet und ermöglicht so den Datentransport zwischen den Rechnern. Das IP-Protokoll verfügt jedoch weder über eine Fehlererkennung noch eine Fehlerkorrektur, d.h. es wird nicht überprüft, ob die Daten ebenso empfangen werden, wie sie abgeschickt wurden. Zudem findet die Übermittlung der Daten unverschlüsselt statt.[99] Diese Sicherheitslücken des IP-Protokolls bieten potentiellen Angreifern die Möglichkeit, die übertragenen IP-Pakete abzuhören (IP-Sniffing), fehlzuleiten, zu modifizieren oder zu fälschen (IP-Spoofing).[100]

ICMP (Internet Control Message Protocol): Da das IP-Protokoll keine Möglichkeit bietet, den Absender zu informieren, ob ein Datenpaket die vorgesehene Lebensdauer überschritten, ob der Empfänger erreichbar ist oder die Daten unterwegs verloren oder zerstört wurden, werden ergänzend zum IP-Protokoll verschiedene Steuerprotokolle verwendet. ICMP, eines dieser Steuerprotokolle, hat die Aufgabe, den Sendern von IP-Paketen Fehler- und Steuerungsmeldungen (z.B. “Destination Unreachable”) zukommen zu lassen.[101] Da diese Meldungen die Konfigurationen von Hosts oder Routern beeinflussen können, ergeben sich daraus potentielle Angriffsmöglichkeiten. Diese Angriffe beeinträchtigen entweder die

---

97 Vgl. [Heinzmann et. al. 97], S. 78; [Holfelder 95], S. 43-45; [Stevens 95], zit. in: [Calzo 97], S. 6; [Tanenbaum 97], S. 51-54; [Weidner 97], S. 14-21.

98 Vgl. [Kyas 96b], S. 74-78.

99 Vgl. [Chapman et. al. 96], S. 534; [Klau 95], S. 58-60; [Tanenbaum 97], S. 431-434.

100 Vgl. http://www.cert.dfn.de/team/kpk/works95a.html

101 Vgl. [Pohlmann 97], S. 55-57 und [Tanenbaum 97], S. 438-439.

Funktionsfähigkeit des Netzwerks (z.B. Source Quench[102]) oder sie zielen auf eine Veränderung der Vermittlungspfade (z.B. ICMP-Redirect[103]).[104]

IGMP (Internet Group Management Protocol): Die übliche IP-Kommunikation findet zwischen einem Sender und einem Empfänger statt. Bei einigen Anwendungen ist es jedoch nützlich, die Übertragung an mehrere Empfänger gleichzeitig zu ermöglichen. Diese Art der Kommunikation wird durch das IGMP-Protokoll übernommen, welches annäherungsweise dem ICMP-Protokoll entspricht.[105]

TCP (Transmission Control Protocol): Auf der Transportschicht besitzt das Internet zwei Protokollarten, das verbindungsorientierte TCP-Protokoll und das verbindungslose UDP-Protokoll. Im Unterschied zum IP-Protokoll ist das TCP-Protokoll ein verbindungsorientiertes Kommunikationsprotokoll, d.h. vor dem Datentransport wird eine virtuelle Verbindung zwischen Quell- und Zielrechner hergestellt. Zu den Hauptaufgaben des TCP-Protokolls zählen der Transport und die Sicherung einer korrekten Datenübertragung.[106] Wie schon das IP-Protokoll, besitzt auch das TCP-Protokoll keine sicheren Mechanismen zur Identifizierung und Authentisierung im Netz.[107] Der Hauptangriffspunkt dieses Protokolls ist der aus drei Schritten bestehende Verbindungsaufbau. Bei jeder auf TCP basierenden Verbindung wird vom lokalen Host eine Sequenznummer generiert, die über IP an den fremden Host geschickt wird. Dieser antwortet ebenfalls mit seiner eigenen Sequenznummer, der Bestätigungsnummer ("Acknowledgement-Number"). Danach sendet der lokale Host eine Rückbestätigung und beginnt mit der Datenübertragung.[108] Wenn ein Angreifer die Sequenznummer vorhersagen kann, so kann er seinem Opfer eine vertrauenswürdige Verbindung vortäuschen (Sequence Number Attack). Eine weitere Möglichkeit eines Angriffes besteht darin, dass der Angreifer einen Host mit Sequenznummern überflutet, indem er nicht auf die erhaltenen Bestätigungsnummern reagiert (TCP SYN Flooding).[109]

UDP (User Datagram Protocol): Das UDP-Protokoll ist ein verbindungsloses Protokoll, welches die Übertragung roher IP-Datengramme ermöglicht, ohne dass eine Verbindung aufgebaut wird.[110] Da das UDP-Protokoll auf eine Fehlerkorrektur verzichtet, wird es meist bei zeitkritischen Anwendungen (z.B. Video) eingesetzt, bei denen es nicht so wichtig ist, ob wirklich alle Pakete korrekt ankommen.[111] UDP wird ebenfalls verwendet, wenn die Sequenznummer aufgrund kurzer Nachrichten (z.B. Zeitübermittlung) unnötig ist. Aufgrund der fehlenden Sequenznummer und Bestätigungsnummer lässt sich dieses Protokoll noch leichter als das TCP-Protokoll simulieren und bringt deshalb ähnliche Sicherheitslücken mit sich (z.B. UDP-Spoofing).[112]

4.4.2 Internet-Dienste

Nach der Diskussion der Schwachstellen der Internet- und der Transportschicht innerhalb der TCP/IP-Protokollarchitektur werden in der Folge diejenigen Sicherheitslücken untersucht, die

---

[102] Die Nachricht "Source Quench" (Quelle löschen) wird benutzt um Hosts zu drosseln, die zuviele Pakete schicken.
[103] Die Nachricht "Redirect" wird von Routern benutzt, um Hosts, welche mit minimaler Routing-Information neu am Netzwerk aktiv werden, zur Benutzung der optimalen Route zu veranlassen.
[104] Vgl. [Kyas 96a], S. 67-71.
[105] Vgl. [Tanenbaum 97], S. 449-450.
[106] Vgl. [Pabrai et. al. 96], S. 70-80 und [Pohlmann 97], S. 60-62.
[107] Vgl. http://www.cci.de/cci/its/fw-inf03.htm
[108] Vgl. [Kyas 96b], S. 80-82.
[109] Vgl. http://www.student.tdb.uu.se/~t95hhu/secure/outside.html#.B.23
[110] Vgl. [Cheswick et. al. 95], S. 28.
[111] Vgl. [Calzo 97], S. 6.
[112] Vgl. [Kyas 96a], S. 74.

sich innerhalb der Anwendungsschicht aufgrund des Einsatzes der Internet-Dienste ergeben. Zur Anwendungsschicht zählen alle Prozesse, welche zur Datenübertragung die Protokolle der Transportschicht nutzen.[113]

4.4.2.1 Telnet

Der Telnet-Dienst an sich verfügt über keine zusätzlichen Schwachstellen. Da Telnet über TCP arbeitet und deshalb der gesamte Ablauf einer Telnet-Sitzung im Klartext übertragen wird, sind auch die für den Verbindungsaufbau notwendigen Passwörter vor Sniffer-Angriffen[114] nicht geschützt. Eine weitere Sicherheitslücke ergibt sich, wenn das aufgerufene Telnet-Programm manipuliert wurde und so beispielsweise alle Benutzernamen mit zugehörigem Passwort aufzeichnet (Trojanisches Pferd). Diese letztgenannte Schwachstelle im Zusammenhang mit Telnet ergibt sich ebenfalls bei Telnet-Sitzungen, die auf Computern gestartet werden, zu denen kein Vertrauensverhältnis besteht.[115]

4.4.2.2 FTP

Analog dem Telnet-Dienst basiert auch FTP auf dem TCP-Protokoll und hat grundsätzlich ähnliche Sicherheitsprobleme. Die Mehrheit der Schwachstellen, welche der Einsatz des FTP-Dienstes mit sich bringt, ergeben sich jedoch aufgrund falsch konfigurierter Systeme, wie beispielsweise ein Anonymous-FTP-Server mit Schreibberechtigung.[116] Eine weitere Schwachstelle von FTP ist die Tatsache, dass der FTP-Serverdämon (ftpd) für Datenverbindungen den privilegierten Port 20 verwendet und deshalb als Benutzer "root" mit Administratorenrechten gestartet wird. Im Nachhinein ist jedoch auch eine Verwendung von FTP unter einem andern Benutzer möglich. Leider wird aus Gründen der Bequemlichkeit oder Unwissenheit oft nicht daran gedacht. Zudem wurden im Laufe der Zeit immer wieder Sicherheitslücken im FTP-Dämon selber (z.B. FTP Bounce[117]) gefunden.

4.4.2.3 E-Mail

Das E-Mail-System besteht aus zwei Subsystemen, dem Message Transfer Agent (MTA) und dem User Agent (UA). Der MTA übermittelt die elektronischen Nachrichten über die Teilnetzwerke des Internet an ihren Bestimmungsort. Beim UA handelt es sich um die Software auf der Clientseite, mit welcher Benutzer E-Mails erstellen, versenden und empfangen können. Zum Abholen der E-Mails werden Protokolle wie das Post Office Protocol (POP3) oder das Interactive Mail Access Protocol (IMAP) verwendet. Der Versand einer E-Mail wird mit Hilfe des SMTP-Protokoll (Simple Mail Transfer Protocol) realisiert. SMTP ist ein einfaches ASCII-Protokoll, mit dem E-Mails im Internet transportiert werden.[118]

Die verschiedenen Protokolle und Anwendungsprogramme, welche in Verbindung mit dem E-Mail-Dienst stehen, stellen Sicherheitslücken für ein Unternehmungssystem dar. Eine der bekanntesten Schwachstellen findet sich im Programm "sendmail", einer SMTP-Implementierung, welches zur Entgegennahme, Weiterleitung und Zustellung von E-Mails verwendet wird. Sendmail ist sehr umfangreich und deshalb schwierig zu konfigurieren, was auch dazu führt, dass Angreifer immer wieder neue Sicherheitslücken entdecken, durch die sie sogar Zugänge mit Administratorenrechten erlangen können. Obwohl nach Bekanntwerden von Fehlern sofort neue Versionen[119] des Programms verfügbar sind, gibt es immer Unter-

---

[113] Vgl. [Chapman et. al. 96], S. 545-546.
[114] siehe 3.4.1
[115] Vgl. [Cheswick et. al. 95], S. 36-37.
[116] Vgl. [Stallings 95], S. 117-121.
[117] Vgl. http://www.cert.org/pub/advisories/CA-97.27.FTP_bounce.html
[118] Vgl. [Kyas 96a], S. 81-85; [Pohlmann 97], S. 65-66; [Tanenbaum 97], S. 662-682; [Weidner 97], S. 31-33.
[119] Vgl. http://www.sendmail.org/

nehmungen, welche noch über alte Versionen von Sendmail verfügen. Zudem beinhalten neue Versionen von Sendmail teilweise auch zusätzliche Probleme.[120]

Da die Protokolle SMTP, POP3 und IMAP ebenfalls wie TCP über keinen Verschlüsselungsmechanismus verfügen, ist es für einen Angreifer möglich, Kenntnis über den Inhalt einer E-Mail sowie Benutzernamen und Passwort eines Benutzers zu erhalten.[121]

Eine weitere Schwachstelle stellt die Vermittlung der Nachrichten zwischen den Message Transfer Agents dar, da diese eine Fälschung von E-Mail-Adressen zulassen (Mail Spoofing).[122] Diese Schwachstelle öffnet die Tür zu Angriffsmöglichkeiten wie Mail-bomben[123] und Social Engineering.

Im Zusammenhang mit dem E-Mail-Dienst kursieren Gerüchte, dass durch das Lesen von E-Mails (z.B. Goodtimes[124]) Viren verbreitet werden. Dies stimmt allerdings nur bedingt, denn damit sich ein Virus verbreiten kann, muss zuerst Programmcode ausgeführt werden. Neuere E-Mail-Programme bieten jedoch die Möglichkeit Programmcode auszuführen, indem sie beim Lesen einer E-Mail gewisse Zusatzprogramme (z.B. Ghostscript), welche Programmcode verstehen, automatisch ausführen. Fehler in diesen Zusatzprogrammen bieten deshalb wiederum Optionen für Angriffe (z.B. Postscript-Angriffe).

4.4.2.4 World Wide Web

HTTP: Das HyperText Transfer Protocol (HTTP) ist das Standardprotokoll im WWW zur Übertragung von HTML-Dokumenten. Innerhalb des WWW-Browser können jedoch auch andere Protokolle wie Telnet, FTP, etc. verwendet werden.[125] Jedes im WWW verfügbare Dokument wird über den Universal Resource Locator (URL)[126] angesprochen. Abgesehen davon, dass auch HTTP alles unverschlüsselt überträgt, finden sich im HTTP-Protokoll keine zusätzlichen Sicherheitslücken. HTTP zeigt erst im Zusammenhang mit einem HTTP-Server Schwachstellen. Beispielsweise gibt es HTTP-Server, die Angreifern den Zugang zu Verzeichnissen erlauben, die nicht für den WWW-Zugriff freigegeben wurden. Eine weitere Schwachstelle stellen die im Zusammenhang mit dem HTTP-Server verwendeten CGI-Scripts dar.[127]

CGI: Das Common Gateway Interface (CGI) bietet vielfältige Möglichkeiten für Angriffe. Ein CGI-Script erlaubt einem Benutzer, interaktive Prozesse (z.B. Antwort auf eine Anfrage) vom Browser auslösen zu lassen.[128] Da Scripts als kleine Programme angesehen werden können und Programme bekanntlicherweise selten fehlerfrei sind, bieten diese eine grosse Anzahl möglicher Sicherheitslücken. Die Angriffe äussern sich meist darin, dass versucht wird, ein CGI-Script durch diverse Eingaben zu einem Fehlverhalten (z.B. Abbruch) zu zwingen, um danach das System kontrollieren zu können (z.B. Ausführen von Befehlen). Bei der jüngsten CGI-Attacke wurde eine Schwachstelle im weit verbreiteten CGI-Script “Count.cgi” (Zugriffszähler) dazu benutzt, Befehle mit den Privilegien des HTTP-Dämons (httpd) auszuführen.[129]

---

120 Vgl. ftp://ftp.cert.org/pub/cert_advisories/CA-97.05.sendmail
121 Vgl. [Müller-Späth 97], S. 41 und [Cameron 97], S. 48-49.
122 http://home4.swipnet.se/~w-48299/AnonyMail.exe
123 Grosse E-Mail (bzw. viele kleine E-Mails), welche die Störung der Funktionsfähigkeit des Mail-Servers zum Ziel hat.
124 Vgl. http://www.mcafee.com/support/hoax.asp
125 Vgl. [Pohlmann 97], S. 66-69.
126 Die allgemeine Form einer URL lautet: Service://Rechner/Pfad/Datei
127 Vgl. [Stallings 95], S. 90-92.
128 Vgl. [Eike 97], S. 42-43.
129 Vgl. http://www.cert.org/pub/advisories/CA-97.24.Count_cgi.html

HTML: Dokumente, die in HTML erstellt wurden, können verschiedene Dateitypen (z.B. Java-Programme) umfassen. Diese Möglichkeit kann aber durch Angreifer auch negativ, z.B. in Form von Viren, ausgenutzt werden.[130] Allerdings sind für solche Angriffe spezielle Dokumentenformate (z.B. JavaScript) nötig sowie ein Browser, der diese ohne weiteres akzeptiert. Zudem bieten Schwachstellen innerhalb des Browsers (z.B. Internet Explorer 3.0) eine gute Angriffsmöglichkeit.

PlugIns: Unter einem PlugIn (z.B. Realaudio) ist ein Programm zu verstehen, das die Funktionsfähigkeit eines Browsers erweitert. Da PlugIns alle Fähigkeiten des Browsers, die Ressourcen des Clients und alle Netzwerkressourcen, zu denen der Client Zugriff hat, ausnutzen können, stellen sie eine grosse Sicherheitslücke für das Unternehmungssystem dar. Das Risiko eines PlugIns ist jedoch gleich hoch einzustufen, wie das Risiko jedes andern Programmes, das auf den lokalen Rechner geladen wird.

JavaScript: JavaScript ist eine Programmiersprache, mit welcher der Programmcode direkt in ein HTML-Dokument eingebunden und ausgeführt werden kann. Theoretisch beschränkt sich die Wirkungsfähigkeit eines Javascripts im Wesentlichen nur auf das Browser-Fenster.[131] Jedoch können Angreifer unter Verwendung eines Javascripts Beobachtungen über besuchte HTML-Dokumente, Formulardaten (z.B. Passwörter) und Werte von Cookies[132] durchführen.[133]

Java: Die Programmiersprache Java, welche von Sun Microsystems entwickelt wurde, ist von der Syntax her vergleichbar mit C++. Das Hauptziel von Java besteht darin, Programme (Java-Applets) über das Netz zu einem angeschlossenen Rechnersystem zu transportieren und dort unabhängig von der verwendeten Hardwareplattform in einem abgegrenzten System ablaufen zu lassen. Da einige Implementierungen von Java-Interpretern allerdings mit Fehlern behaftet sind, finden sich auch hier Sicherheitslücken.[134] JavaScript und Java können übrigens in neueren Browserversionen optional deaktiviert werden. Diese Lösung erweist sich jedoch als nicht akzeptabel, da der WWW-Dienst so an Funktionalität verliert.

ActiveX: Im Gegensatz zu Java läuft ActiveX von Microsoft nicht in einem abgegrenzten System, sondern ist ein Teil des Betriebssystems. Wenn eine ActiveX-Komponente einmal aktiv ist, unterliegt sie keinen Sicherheitsmechanismen mehr d.h. das ActiveX-Programm kann beispielsweise auch Daten löschen. Um der fehlenden Sicherheitsarchitektur Rechnung zu tragen, werden sogenannte Zertifikate verwendet, welche die Herkunft eines Programmes bestätigen.[135]

4.4.2.5 Berkeley r-Tools und SSH

Die Tatsache, dass die r-Befehle nur ausgeführt werden, wenn der Zielrechner dem Ursprungsrechner vertraut, bietet keine Sicherheit, denn - wie bereits erwähnt - können IP-Adressen gefälscht (IP-Spoofing) werden.

Secure Shell (SSH), welches als Ersatz der r-Tools gedacht ist, besitzt derzeit keine bekannten Sicherheitsprobleme.

---

[130] Vgl. [Borer 96], S. 51.
[131] Vgl. [Luckhardt 97], S. 171.
[132] Textzeile, in der Zustandsinformationen (z.B. Uhrzeit des letzten Web-Seiten-Besuches) über einen Benutzer gespeichert werden.
[133] Vgl. http://www.cert.org/pub/advisories/CA-97.20.javascript.html
[134] Vgl. [Pilz 97], S. 17-22; [Waldburger 98], S. 75; [Weidner 97], S. 34.
[135] Vgl. [Luckhardt 97], S. 174 und [Pohlmann 97], S. 337-338.

4.5 Abschliessende Bemerkungen zur Schwachstellenanalyse

Wie in diesem Kapitel gezeigt wurde, sind die vielfältigsten Schwachstellen im technischen Bereich anzutreffen. Dies heisst aber nicht, dass die menschlichen und die organisatorischen Schwachstellen von untergeordneter Bedeutung sind. Es ist jedoch nicht möglich im Rahmen dieser Arbeit alle Schwachstellen aufzuzeigen. Vielmehr wurden einige wichtige Schwachstellen dargestellt, welche für eine Unternehmung gefährliche Sicherheitslücken darstellen.

Nachdem bereits eine Bedrohungs- und eine Schwachstellenanalyse vorgenommen wurde, findet im nächsten Kapitel die Gegenüberstellung von Bedrohungen und Schwachstellen in Form einer Gefahrenanalyse statt.

5. Gefahrenanalyse

5.1 Aufgabe der Gefahrenanalyse

Sobald die auf eine Unternehmung einwirkenden Bedrohungen (z.B. Ausführen von Programmen mit unerwünschter Wirkung) mit den in der Unternehmung vorhandenen Schwachstellen (z.B. ActiveX) zusammentreffen, ergeben sich Gefahren. Das Ziel der Gefahrenanalyse (vgl. Abbildung 9) ist deshalb, die Wechselwirkungen von Bedrohungen und Schwachstellen festzustellen, um rechtzeitig Massnahmen zur Risikoreduzierung ergreifen zu können.[136]

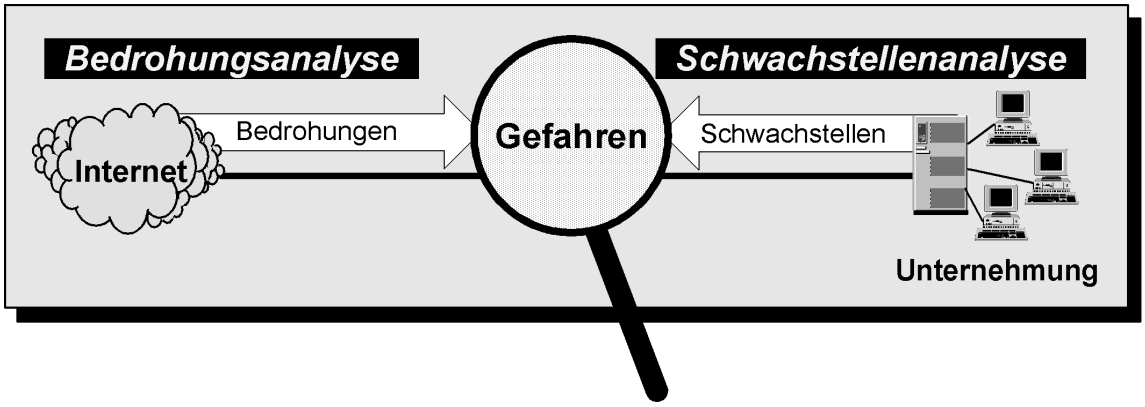

Abbildung 9: Gefahrenanalyse

5.2 Zuordnung von Bedrohungen und Schwachstellen

Bei der Ermittlung von potentiellen Gefahren wird analysiert, welche Schwachstellen innerhalb einer Unternehmung mit welchen Bedrohungen seitens des Internet zusammentreffen können. Abbildung 10 zeigt eine Gegenüberstellung der Bedrohungen und Schwachstellen, die bei der Internetnutzung von Bedeutung sind. Wie aus dieser Gefahrenanalyse ersichtlich ist, entstehen viele Gefahren aufgrund eines Zusammentreffens von Bedrohungen auf eine Kombination von Schwachstellen (vgl. Abbildung 11). Beispielsweise werden bei einem Einbruch in ein System menschliche (z.B. Fahrlässigkeit), organisatorische (z.B. Standort) und technische (z.B. IP-Protokoll) Schwachstellen ausgenutzt.

Die Gegenüberstellung von Bedrohungen und Schwachstellen erläutert, dass viele Gefahren im Internet durch menschliche und organisatorische Schwachstellen ausgelöst werden können. Obwohl die technischen Schwachstellen in der Schwachstellenanalyse am umfassendsten vertreten sind, stehen diese nicht allein da. Es braucht immer einen Menschen, der eine Schwachstelle (z.B. schwache Passwörter) überhaupt zulässt und damit Angriffe auf die Unternehmungssysteme ermöglicht. So sind beispielsweise viele Angriffe gar nicht denkbar, wenn sich die Mitarbeiter nur von unternehmungseigenen Computern aus mit dem Unternehmungssystem verbinden dürfen.

[136] Vgl. [Heinrich 96], S. 457-459.

Bedrohungen / Schwachstellen			Passive Angriffe			Aktive Angriffe									Zufällige Verfälschungen			
		Natürliche Bedrohungen (z.B. Brand)	Abhören von Daten	Abhören der Teilnehmer-Identitäten	Verkehrsflussanalyse	Wiederholen von Informationen	Verzögern von Informationen	Einfügen und Löschen von Daten	Modifikation von Daten	Denial of Service	Masquerade	Leugnung der Kommunikation	Hijacking	Systemanomalien	Fehlrouting von Informationen	Übertragungsfehler	Software-Fehler	Fehlbedienung
Mensch																		
aktuelle Mitarbeiter		√	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	–	–	–	√
ehemalige Mitarbeiter		*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	–	–	–	–
Organisation																		
Logische Schwachstellen		–	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	–	–	*o*	–
Physische Schwachstellen		√	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	*o*	√	√	–	√
Technik																		
Kommunikationsprotokolle																		
IP		–	√	√	√	√	√	√	√	√	√	√	–	√	√	√	–	–
ICMP		–	*o*	*o*	*o*	*o*	*o*	*o*	*o*	√	–	–	–	–	–	–	–	–
IGMP		–	*o*	*o*	*o*	*o*	*o*	*o*	*o*	√	–	–	–	–	–	–	–	–
TCP		–	√	√	√	√	√	√	√	√	√	√	√	√	–	–	–	–
UDP		–	√	√	√	√	√	√	√	√	√	√	√	√	√	√	–	–
Internet-Dienste																		
Telnet	Client	–	√	√	√	√	√	√	√	√	√	–	√	√	–	–	–	–
	Server	–	√	√	√	–	–	–	–	√	√	–	√	–	–	–	–	–
FTP	Client	–	√	√	√	√	√	√	√	√	√	–	√	√	–	–	–	–
	Server	–	√	√	√	–	–	–	–	√	√	–	√	√	–	–	–	–
E-Mail	UA	–	√	√	√	√	√	√	√	√	√	√	√	√	–	–	–	–
	MTA	–	√	√	√	–	–	–	–	√	√	√	√	–	–	–	–	–
World Wide Web	HTML	–	–	–	–	–	–	–	–	√	–	–	–	–	–	–	–	–
	PlugIns	–	*o*	*o*	*o*	√	√	√	√	√	√	√	√	√	–	–	–	–
	JavaScript	–	*o*	–	–	–	–	–	–	√	–	–	–	√	–	–	–	–
	Java	–	*o*	–	–	√	√	√	√	√	√	√	√	√	–	–	–	–
	ActiveX	–	√	*o*	*o*	√	√	√	√	√	√	√	√	√	–	–	–	–
	CGI	–	√	√	√	*o*	*o*	*o*	*o*	√	√	–	√	√	–	–	–	–
Berkeley r-Tools	Client	–	√	√	√	√	√	√	√	√	√	–	√	√	–	–	–	–
	Server	–	√	√	√	–	–	–	–	√	√	–	√	–	–	–	–	–
SSH	Client	–	–	√	√	√	√	√	√	√	–	–	–	*o*	–	–	–	–
	Server	–	–	√	√	–	–	–	–	√	–	–	–	–	–	–	–	–

√ direkter Einfluss
o indirekter Einfluss
– kein Einfluss

Abbildung 10: Zuordnung von Bedrohungen und Schwachstellen[137]

[137] Vgl. dazu auch [Kirsch et. al. 97a].

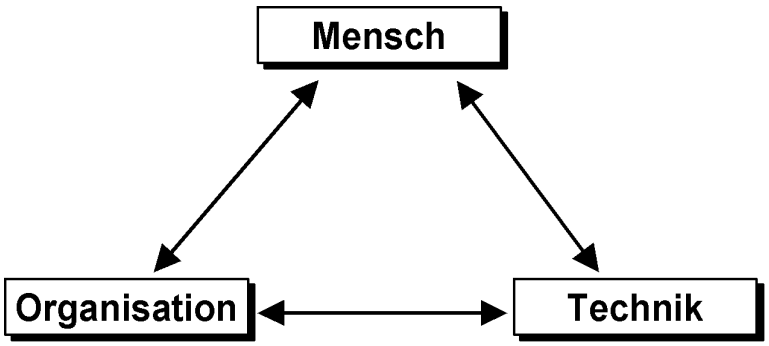

Abbildung 11: Wechselbeziehungen von Mensch, Organisation und Technik

Unzählige Gefahren haben jedoch ihren Ursprung im Fundament des Internet, repräsentiert durch die Kommunikationsprotokolle. Da diese Protokolle eine unverschlüsselte Übertragung der Daten vorsehen und zudem über keine Sicherheitsmechanismen zur Identifizierung und Authentisierung verfügen, bilden sie die ideale Grundlage jedes Angriffes im Internet. Damit wird deutlich, dass alle Anwendungen, welche auf diesen Protokollen aufbauen, ähnlichen Bedrohungen ausgesetzt sind, sofern die in den Protokollen verkörperten Sicherheitslücken nicht durch zusätzliche Sicherheitsmechanismen (z.B. Verschlüsselung von E-Mails) geschlossen werden.

Eine weitere Gefahr geht von den Benutzungsschnittstellen aus, welche den direkten Zugriff auf die Ressourcen des Unternehmungssystems erlauben (z.B. ActiveX). Obwohl sich solche Ressourcenmanipulationen durchaus als sinnvoll erweisen können, stellen sie bei missbräuchlicher Verwendung eine grosse Gefahr für das Unternehmungssystem dar. Es gilt daher allgemein der Grundsatz, dass alles, was einen bestimmten Nutzen (z.B. Löschen von alten Daten) bietet, ebenfalls auch missbräuchlich (z.B. Löschen aller Daten) eingesetzt werden kann. Wenn beispielsweise eine Unternehmung ihren Mitarbeitern den Zugriff auf ihr Netzwerk von zu Hause aus erlaubt, so steht diese Türe grundsätzlich auch einem Hacker offen.

Was ebenfalls auffällt, ist die Tatsache, dass sich sämtliche Kommunikationsprotokolle und Internet-Dienste stören lassen (Denial of Service). Ebenso ist das Auftauchen von Systemanomalien (z.B. Viren) bei allen Internet-Diensten möglich.

5.3 Weiteres Vorgehen

Nachdem eine Unternehmung die potentiellen Bedrohungen seitens des Internet sowie ihre eigenen Schwachstellen ermittelt hat, kennt sie die Gefahren, denen das Unternehmungssystem ausgesetzt ist. Um nun das weitere Vorgehen planen zu können, ist das Risiko, dem die Unternehmung gegenübersteht, zu berechnen. Dazu ist eine Bewertung der sicherheitsrelevanten Elemente (z.B. Daten) in Form einer Wertanalyse[138] notwendig. Eine derartige Bewertung der zu schützenden Objekte ist stark von der Struktur und der Branche der Unternehmung abhängig.

Nach der Berechnung der Werte der sicherheitsrelevanten Objekte einer Unternehmung können diese den einzelnen Gefahren zugeordnet werden. Eine Unternehmung ermittelt so beispielsweise, wie hoch der Schaden ist, der verursacht wird, wenn ihre Daten abgehört werden (vgl. Abbildung 12).

---

[138] Vgl. [Borer 96], S. 11-13 / S. 32-35 und [Schaumüller-Bichl 92], S. 36.

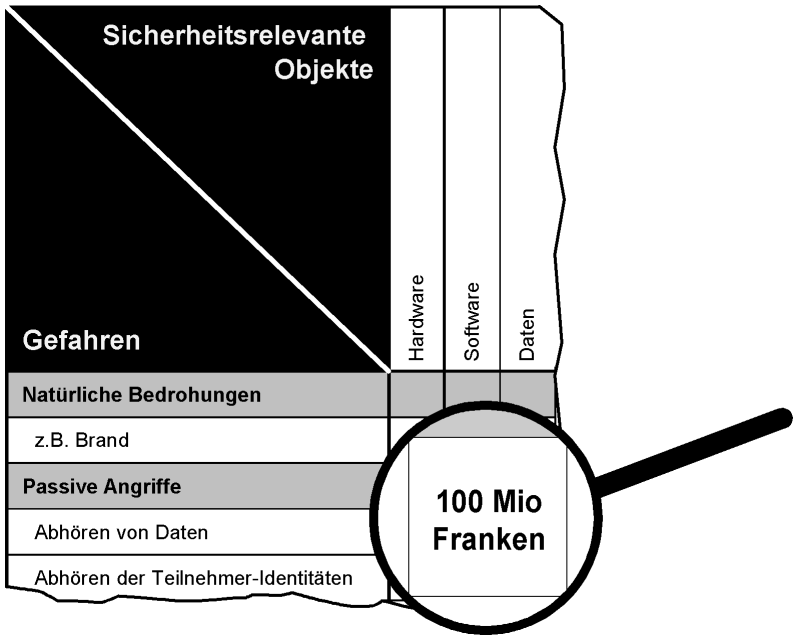

Abbildung 12: Beispiel einer Schadensanalyse

Sobald der Schaden beziffert ist, der sich durch das Zusammentreffen von einer Bedrohung auf eine Schwachstelle der Unternehmung ergibt, wird die Eintrittswahrscheinlichkeit eines solchen Schadenfalls eruiert. Da sich das Internet erst seit drei Jahren im Aufschwung befindet, sind viele Unternehmungen neu am Netz vertreten. Sie können sich deshalb noch nicht auf Erfahrungswerte bei ihren Berechnungen der Eintrittswahrscheinlichkeiten stützen. In einem solchen Fall muss die Unternehmung entweder selber schätzen, wie hoch die Wahrscheinlichkeit eines bestimmten Schadenfalles ist, oder sie greift auf bereits publizierte Schätzungen (z.B. CERT-Mitteilungen[139]) zurück. Wird auf publizierte Schätzungen zurückgegriffen, ist es von grösster Bedeutung, dass diese noch speziell angepasst werden, da jede Unternehmung eine andere Infrastruktur und andere Sicherheitsmechanismen aufweist.

Laut einer Schätzung des CERT ist eine Domäne alle 0.8 Jahre und ein Host alle 45 Jahre in einen Zwischenfall verwickelt. Dabei ist jedoch zu beachten, dass es Internet-Hosts gibt, welche als attraktivere Angriffsziele gelten als andere und deshalb in mehrere Zwischenfälle pro Jahr verwickelt sind.[140]

Für eine Unternehmung ist jedoch nicht von grösster Bedeutung, dass die Eintrittswahrscheinlichkeiten der einzelnen Schadenfälle genau stimmen, sondern vielmehr, dass Risikotendenzen innerhalb des Unternehmungssystems erkannt werden können. Wichtig ist, dass für Ereignisse mit hohem Risiko sobald als möglich entsprechende Gegenmassnahmen getroffen werden.

Abbildung 13 zeigt eine Möglichkeit, wie durch die Einteilung von Ereignissen in sogenannte Risikoklassen der streng mathematische Weg zur Ermittlung des Risikos umgangen werden kann.

---

[139] Vgl. http://www.cert.org/research/JHThesis/index.html
[140] Vgl. http://www.cert.org/research/JHThesis/Chapter16.html

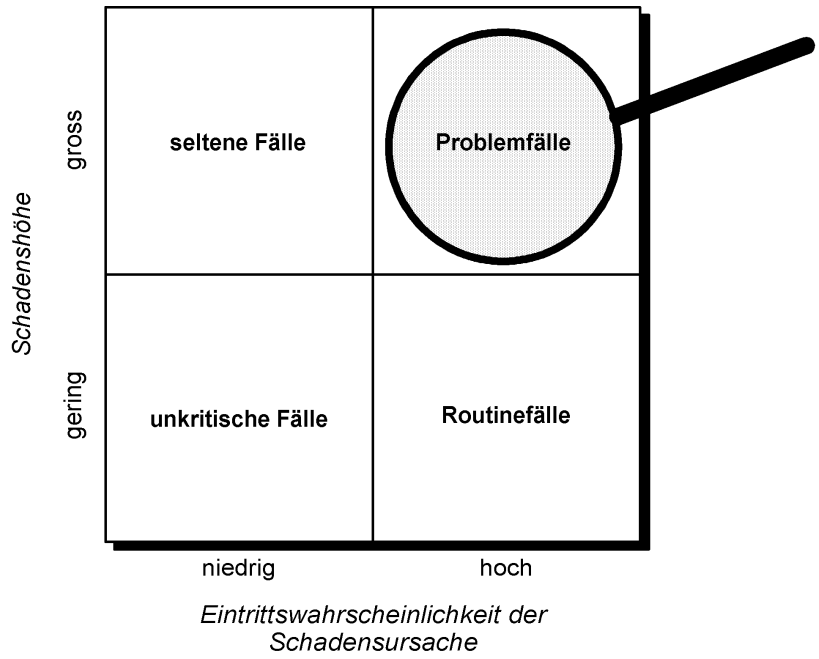

Abbildung 13: Risikoklassen[141]

In diesem Kapitel wurde demonstriert, wie eine Unternehmung anhand ihrer gesammelten Daten aus der Bedrohungs-, Schwachstellen- und Wertanalyse das Risiko eines Ereignisses bestimmen kann. Das nächste Kapitel widmet sich den Massnahmen, die zur Reduzierung von Schwachstellen in der Unternehmung dienen.

[141] Vgl. [Krallmann 89], S. 136.

6. Massnahmen

6.1 Überblick

Im Anschluss an die Analyse der Risiken sind passende Massnahmen zur Risikoreduzierung zu ergreifen. Diese Massnahmen dienen der Schwachstellenminimierung in einer Unternehmung und bieten somit Schutz gegenüber den Bedrohungen, die ein Interneteinsatz bewirkt. Ziel dieser Gegenmassnahmen ist eine stufenweise Einschränkung des Gesamtrisikos (vgl. Abbildung 14).

Trotzdem bleiben auch nach der Umsetzung aller Gegenmassnahmen immer noch gewisse Restrisiken bestehen, die nicht durch entsprechende Massnahmen abgedeckt werden konnten und von der Unternehmung selber getragen werden müssen. Deshalb streben Unternehmungen mit der Durchsetzung möglichst vieler Massnahmen ein Restrisiko mit sehr kleiner Eintrittswahrscheinlichkeit an. Dabei ist jedoch der finanzielle Aspekt ebenfalls im Auge zu behalten, denn eine bestimmte Massnahme lohnt sich nur, wenn sie einen geringeren Aufwand beinhaltet, als ein potentieller Schaden auslösen könnte.[142]

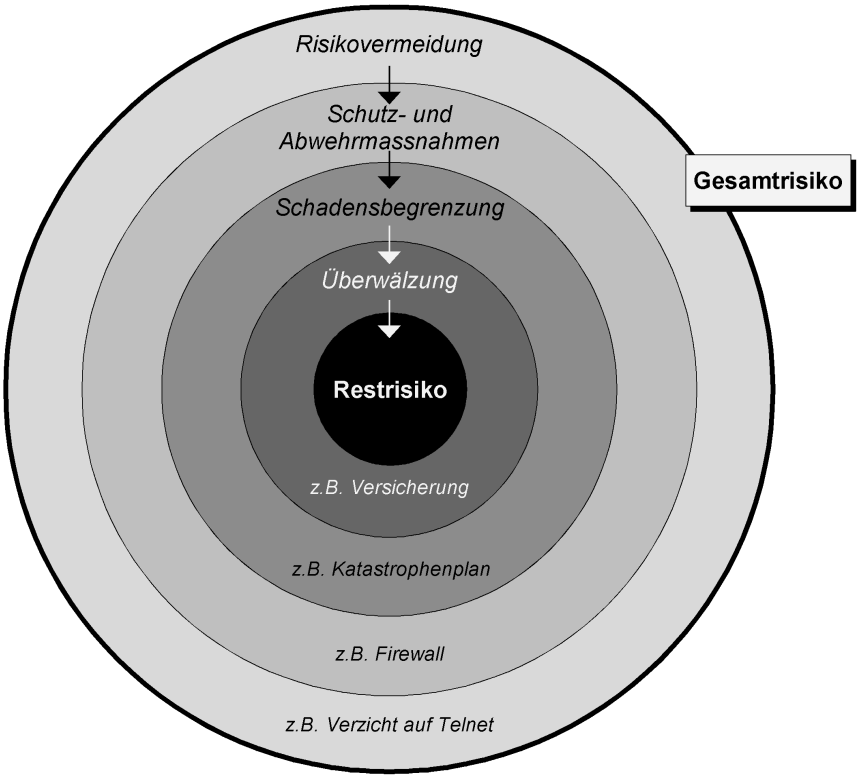

Abbildung 14: Stufenweise Reduktion des Gesamtrisikos[143]

Anschliessend werden die verschiedenen Massnahmen zusammengestellt, die einer Unternehmung zur Schwachstellenbekämpfung auf personeller, organisatorischer und technischer Ebene zur Verfügung stehen. Es wird zudem gezeigt, welche Massnahmen zur Reduktion welcher Risiken eingesetzt werden können.

---

[142] Vgl. [Borer 96], S. 3-4; [Holthaus et. al. 95], S. 26; [Maurer 95], S. 18-23; [Schaumüller-Bichl 92], S. 33-40.
[143] Vgl. [Schaumüller-Bichl 92], S. 34.

6.2 Personelle Massnahmen

6.2.1 Schulung

Die Schulung des Personals leistet einen grossen Beitrag zur Erhöhung der Sicherheit des Unternehmungssystems. Eine bessere Ausbildung der Mitarbeiter gewährleistet, dass Sicherheitslücken, die sich durch fehlendes Wissen ergeben (z.B. Konfigurationsfehler), vermieden werden. Ein weiteres Ausbildungsziel bildet die Vermittlung des richtigen Verhaltens in einem Ernstfall (z.B. Virenbefall eines Computers) zur Schadensreduzierung bzw. -elimination. Das Hauptziel der Schulung besteht in der Information der Mitarbeiter über potentielle Bedrohungen und Schwachstellen in einer Unternehmung sowie Problemlösungen zu deren Behebung. Leider wird die Schulung von Sicherheitsmechanismen in Unternehmungen oft vernachlässigt, da sie keinen direkten Nutzen bringt, sondern eher präventiven Charakter hat. Sobald jedoch eine Unternehmung einmal einen Schaden aufgrund von personellen Schwachstellen erlitten hat, wird sie, leider zu spät, auf das Instrument der Schulung nicht mehr verzichten wollen.[144]

6.2.2 Verbote

Selbst wenn Mitarbeiter bestens geschult sind und eine grosse Erfahrung auf dem Gebiet der Informationssicherheit besitzen, gibt es immer wieder Situationen (z.B. Stress), in denen sie das Gelernte bewusst oder unbewusst vergessen. Verbote helfen mit, Mitarbeiter zu einem sicherheitsbewussteren Verhalten (z.B. Verwendungsverbot “fremder” Disketten) zu erziehen. Damit unternehmungsspezifische Informationen über die Sicherheitsmechanismen nicht an die Öffentlichkeit gelangen, empfiehlt sich, eine sogenannte Geheimhaltungsbestimmung im Arbeitsvertrag einzuschliessen. Allerdings führt eine zu starke Sicherheitsbetonung zu einer sinkenden Innovationsfähigkeit der Mitarbeiter.

Bei Kündigungen von Mitarbeitern mit grossem Insiderwissen[145] (z.B. Security Administrator), ist eine sofortige Freistellung des Mitarbeiters von Vorteil. Sonst besteht die Gefahr, dass sich dieser durch einen Sabotageakt (z.B. logische Bombe) bei der Unternehmung zu rächen versucht.[146]

Um die Gefahr zu eliminieren, dass ehemalige Mitarbeiter mit grossem unternehmungsspezifischem Wissen (z.B. Kenntnisse der Sicherheitsmechanismen) der Unternehmung schaden könnten, sind hohe Konventionalstrafen[147] eine geeignete Gegenmassnahme.

6.2.3 Förderung des Sicherheitsbewusstseins

Um das Sicherheitsbewusstsein[148] innerhalb einer Unternehmung nachhaltig zu fördern, ist es notwendig, dass allen Mitarbeitern die Gefahren, denen eine Unternehmung durch den Einsatz des Internet ausgesetzt ist, klar aufgezeigt werden. Je persönlicher sich die Mitarbeiter angesprochen fühlen, umso eher werden sie auch einen Beitrag zur Sicherheit leisten. Als erste Massnahme in diesem Zusammenhang ist jeder Mitarbeiter gehalten, sein Passwort hinsichtlich Sicherheit nochmals zu überdenken. Dabei ist zu beachten, dass Passwörter gewählt werden (z.B. S18mEaNiDl), die selbst mit umfangreichen Wortbibliotheken und Analysen der persönlichen Umgebung des Mitarbeiters (z.B. Geburtsdatum der Freundin), nicht eruiert werden können.

---

144 Vgl. [White et. al. 96], S. 25-27; [Pohlmann 97], S. 304; [Schaumüller-Bichl 92], S. 261-262.
145 Vgl. [Siyan et. al. 95], S. 141.
146 Vgl. [Schaumüller-Bichl 92], S. 262.
147 Vgl. Art. 160-163 OR.
148 Vgl. [Heinrich 96], S. 252.

Insbesondere müssen die Mitarbeiter auch für "systemfremde" Angriffe, wie das Social Engineering[149], sensibilisiert werden. Prinzipiell gilt der Grundsatz, dass keine sicherheitsempfindlichen Informationen, wie beispielsweise Passwörter, auf irgendeinem Weg (z.B. Passwörter als Post-it auf dem Bildschirm) weitergegeben werden dürfen. Ausserdem ist immer höchste Vorsicht beim Ausführen von unbekannten Programmen geboten, selbst wenn diese angeblich vom "Systemadministrator" stammen.[150]

6.3 Organisatorische Massnahmen

6.3.1 Physikalische Trennung

Der beste Schutz des Unternehmungsnetzwerkes kann sicherlich durch eine physikalische Trennung der Internetzugangsrechner vom Firmennetz erreicht werden. Allerdings schränkt eine solche Massnahme den Benutzerkomfort erheblich ein, da immer ein Wechsel zwischen Rechnern des internen- und des externen Datenaustausches stattfindet. Zudem ist keine Integration von Daten und Anwendungen (z.B. Datenbank) der beiden Netze möglich. Aus diesem Grund eignet sich diese Lösung auch nur für Unternehmungen (z.B. Anwaltsbüro), welche das Internet nur gelegentlich benutzen oder in einem ersten Schritt den Nutzen des Internet erkunden und deshalb keine aufwendigen und teuren Sicherheitsmassnahmen ergreifen wollen bzw. rechtfertigen würden.[151]

6.3.2 Situative Rechtevergabe

Indem die Benutzungsrechte des Unternehmungssystems nach Aufgabengebieten vergeben werden, ergibt sich für die Unternehmung eine Vermeidung von Risiken. So wird bei einer situativen Rechtevergabe beispielsweise nur denjenigen Mitarbeitern Zugriff auf eine Unternehmungsdatenbank gewährt, welche diesen Zugang für ihre unternehmerischen Tätigkeiten benötigen. Um jedoch eine solche restriktive Vergabe von Benutzerrechten zu ermöglichen, ist die Ernennung von Mitarbeitern mit untergeordneten Administratorenrechten notwendig. Damit ist eine rasche und restriktive Vergabe von Zugriffsrechten möglich. Dies bedeutet aber auch, dass die aufgabenspezifischen Zugriffsrechte der Mitarbeitern nach Beendigung ihrer Projekte wieder aufgehoben werden.[152]

6.3.3 Sicherheit einzelner Rechner

Jedes Unternehmungssystem besitzt gewisse Rechner (z.B. Server), ohne die das Unternehmungssystem nicht existieren kann. Da ein Angriff auf einen solchen Rechner für eine Unternehmung schwerwiegende Konsequenzen hat, ist ein spezieller Schutz dieser Rechner notwendig. Es handelt sich dabei um physische organisatorische Massnahmen, wie beispielsweise die Bestimmung eines sicheren Standortes der Rechner, sowie logische organisatorische Massnahmen, wie zum Beispiel die Verwendung von Zugangspasswörtern für einzelne Rechner.

6.3.4 Zuständigkeiten

Die Festlegung der Verantwortung, die jeder einzelne Teilnehmer für den Schutz der Systemsicherheit trägt, stellt eine wichtige Massnahme innerhalb der Sicherheitspolitik dar. So ist beispielsweise jeder Benutzer dafür verantwortlich, dass er sein Passwort geheimhält und

---

[149] Vgl. ftp://ftp.cert.org/pub/cert_advisories/CA-91%3A04.social.engineering
[150] Vgl. [Luckhardt 97], S. 173 und [Resch 96], S. 95.
[151] Vgl. [Alpar 96], S. 162.
[152] Vgl. [Wojcicki 91], S. 59-61.

regelmässig ändert. Die Systemadministratoren sind für die Sicherheit im Unternehmungssystem zuständig.

Ausserdem sind die verantwortlichen Mitarbeiter für Notfälle (z.B. Stellvertretungen) klar festzulegen. Es muss für jeden Arbeitnehmer ersichtlich sein, an welche Personen er sich zu wenden hat, wenn er beispielsweise einen Angriff auf das Unternehmungssystem lokalisiert.[153]

6.4 Technische Massnahmen

6.4.1 Firewalls

Um das interne Unternehmungsnetzwerk gegen Angriffe aus dem Internet zu schützen, werden sogenannte Firewalls eingesetzt. Ein Firewallsystem besteht aus einer Kombination von Hard- und Softwarekomponenten, die zwischen das zu schützende Unternehmungsnetz und das unsichere Internet geschaltet werden (vgl. Abbildung 15). Es wird sichergestellt, dass die Kommunikation zwischen den beiden Netzen ausschliesslich über das Firewallsystem erfolgt. Auf diese Weise findet eine Kontrolle des Datenaustausches statt, und damit können unerlaubte Verbindungen unterbunden werden. Firewalls bedienen Funktionen der Internet-, der Transport- und der Anwendungsschicht.[154]

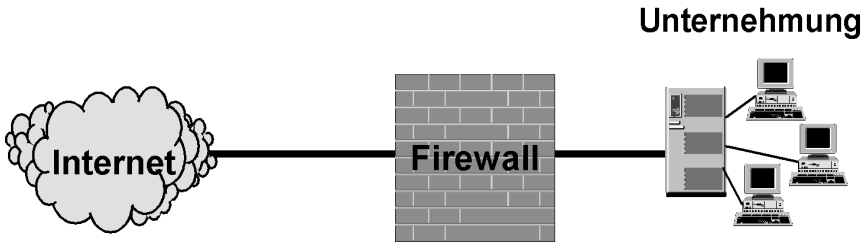

Abbildung 15: Firewall[155]

Je nach Architektur des Firewalls wird zwischen *Paketfiltern* und *Application-Gateways* unterschieden.

Paketfilter (Screening Router, Screening Filter, Route Filters, Packet Filters):

Der Paketfilter (vgl. Abbildung 16) ist die einfachste Variante eines Firewallsystems. Paketfilter analysieren die ein- und ausgehenden Datenpakete auf der Internetschicht sowie der Transportschicht. Aufgrund vorgegebener Regeln (z.B. Zugang nur für IP-Adressen der Unternehmung) werden die Datenpakete entweder weitergeleitet oder verworfen. Die Datenpakete können nach IP-Adressen, Protokolltypen, Portnummern, Benutzern oder Datenmengen gefiltert werden. Entsprechende Verstösse gegen die Regeln des Filters werden automatisch protokolliert. Vielfach werden Paketfilter als Vorfilter für weitere Firewallkomponenten benutzt.[156]

---

[153] Vgl. [Schaumüller-Bichl 92], S. 257-259 und [Siyan et. al. 95], S. 116.

[154] Vgl. [Cheswick et. al. 95], S. 61-64; [Ellermann 94], S. 122; [Fehling et. al. 97], S. 65-66; [Kyas 96a], S. 133-142; [Kyas 96b], S. 434-443; [Lamprecht 96], S. 179-183; [Macgregor et. al. 96], S. 5-9; [Maurer 95], S. 18-20; [Pohlmann 97], S. 36; [Resch 96], S. 88-96; [Siyan et. al. 95], S. 194-195; [Weidner 97], S. 45-46.

[155] Vgl. [Lampe 96], S. 220 und [Pohlmann 97], S. 37.

[156] Vgl. [Chapman et. al. 96], S. 67-69; [Cheswick et. al. 95], S. 64-89; [Kyas 96b], S. 436; [Macgregor et. al. 96], S. 5-6; [Pohlmann 97], S. 110-135; [Resch 96], S. 92.

Die Vorteile von Paketfiltern liegen in der Einfachheit der Installation und deren Administration. Ausserdem müssen keine zusätzlichen Konfigurationen seitens des Benutzers durchgeführt werden. Ein Nachteil der Paketfilter bildet die Möglichkeit, dass ein Angreifer Pakete mit gefälschter Adresse senden kann, um so den Firewall zu umgehen.[157]

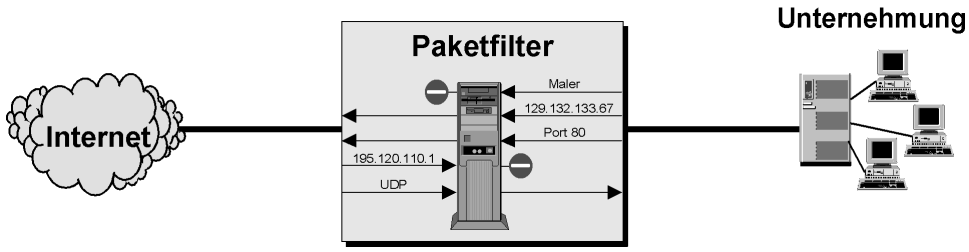

Abbildung 16: Paketfilter[158]

Application-Gateways: (Proxy-Firewalls[159])

Bei einem Application-Gateway wird das Internet so mit dem internen Unternehmungsnetzwerk gekoppelt, dass keine direkte Kommunikationsverbindung auf Protokollebene zwischen den internen und externen Rechnern stattfindet (vgl. Abbildung 17). Eine Kommunikation zwischen dem lokalen Netzwerk und den Rechnern des Internet ist dabei nur über den Application-Gateway möglich. Dieser prüft zuerst die Verbindung auf ihre Zulässigkeit und baut dann eine Verbindung zum angeforderten externen System auf. Auf diese Weise ist mit einem Application-Gateway eine Überwachung bzw. Protokollierung der übertragenen Daten möglich.

Da der Application-Gateway das einzige vom Internet aus erreichbare Rechnersystem einer Unternehmung ist, muss es besonders geschützt werden. Es wird deshalb auch als *Bastion-Host* bezeichnet. Wenn der Application-Gateway, wie hier beschrieben, mit zwei Netzwerk-Anschlüssen arbeitet, spricht man von einem *Dual-Homed-Gateway*, ansonsten von einem *Single-Homed-Gateway*.

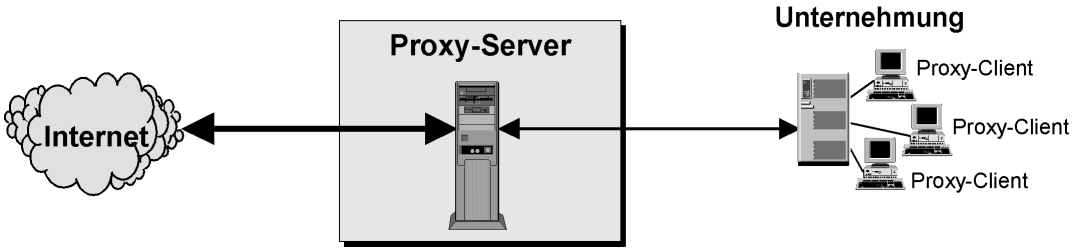

Abbildung 17: Application-Gateway[160]

Grosse Vorteile eines Application-Gateways zeigen sich in seiner hohen Sicherheit. Der Nachteil eines Application-Gateways liegt darin, dass für jeden Internet-Dienst ein Proxy-Server[161] konfiguriert werden muss. Zudem müssen die einzelnen Clients so eingerichtet werden, dass sie ihre Verbindungen über den Proxy-Server aufbauen, da eine direkte

---

157 Vgl. [Maurer 95], S. 19.
158 Vgl. [Chapman et. al. 96], S. 67.
159 Vgl. [Resch 96], S. 92.
160 Vgl. [Pohlmann 97], S. 136.
161 Programm, das stellvertretend für interne Clients mit externen Servern kommuniziert.

Verbindung unmöglich ist. Ein weiterer negativer Punkt ist die Tatsache, dass sich viele Mitarbeiter durch die Überwachung ihres Datenverkehrs in ihrer Persönlichkeit eingeschränkt fühlen.[162]

6.4.2 Kryptographische Massnahmen

Mit kryptographischen Verfahren (vgl. Abbildung 18) werden Daten so verändert (Verschlüsselung), dass sie nur noch für autorisierte Personen verständlich sind (Entschlüsselung).[163] Damit ist eine sichere Kommunikation auch über ein unsicheres Netz, wie das Internet, durchführbar. Neben der Geheimhaltung eignen sich kryptographische Verfahren ferner zur Sicherung der Authentizität, der Integrität und der Verbindlichkeit von Nachrichten.[164] Der Einsatz von kryptographischen Verfahren ist auf allen Schichten des TCP/IP-Schichtenmodells möglich. Nachstehend werden die verschiedenen Konzepte kryptographischer Verfahren und ihre Einsatzmöglichkeiten charakterisiert.

Abbildung 18: Ver- und Entschlüsselung[165]

6.4.2.1 Private-Key Kryptosysteme (Symmetrische Algorithmen)

Private-Key Kryptosysteme, oft auch konventionelle Verschlüsselung genannt, basieren auf symmetrischen Algorithmen, d.h. der Schlüssel für die Verschlüsselung und Entschlüsselung ist identisch.[166] Einer der bekanntesten Standards eines symmetrischen Verschlüsselungsverfahrens ist der Data Encryption Standard (DES) auf dem auch das Kerberos-System[167], ein Netzwerk-Authentifikationssystem, aufbaut.[168] Weitere Verfahren, die auf symmetrischen Algorithmen aufbauen, sind MD5[169] und IDEA[170]. Für den Einsatz im Internet sind jedoch Private-Key Kryptosysteme nur bedingt oder in Verbindung mit anderen Kryptosystemen geeignet, da die sichere und schnelle Verteilung der Schlüssel einen Engpass darstellt.[171]

6.4.2.2 Public-Key Kryptosysteme (Asymmetrische Algorithmen)

Um die Schlüsselverteilung zu vereinfachen, wurden Verfahren mit öffentlichen Schlüsseln (public-keys) entwickelt. Solche Public-Key-Verfahren basieren auf einem asymmetrischen Algorithmus und haben den Vorteil, dass die Kommunikationspartner keinen gemeinsamen geheimen Schlüssel vereinbaren müssen.[172]

Diese Verschlüsselungsart beruht auf einem privaten (private-key) und einem öffentlichen (public-key) Schlüssel. Will der Sender dem Empfänger eine Nachricht übermitteln, so codiert

---

[162] Vgl. [Alpar 96], S. 167; [Cheswick et. al. 95], S. 89-91; [Kyas 96a], S. 166-168; [Weidner 97], S. 49-50.
[163] Vgl. [Schaumüller-Bichl 92], S. 52.
[164] Vgl. [Hoburg 96], S. 50-51 und [Schneier 96], S. 2.
[165] Vgl. [Schneier 96], S. 1.
[166] Vgl. [Chapman et. al. 96], S. 398.
[167] Vgl. [Latanzio 96], S. 16-20.
[168] Vgl. [Kyas 96b], S. 444-446.
[169] Vgl. [Tanenbaum 96], S. 636-637.
[170] Vgl. [Schneier 96], S. 370-377.
[171] Vgl. [Resch 96], S. 83.
[172] Vgl. [Pohlmann 97], S. 199.

er die Botschaft mit dem öffentlichen Schlüssel des Empfängers. Dieser kann die Nachricht mit seinem geheimen Schlüssel entziffern.[173]

Die wohl bekannteste Umsetzung eines Public-Key Kryptosystems findet sich im RSA-Algorithmus, der im Jahre 1978 von Ronald Rivest, Adi Shamir und Leonard Adleman erfunden wurde und deshalb die Anfangsbuchstaben der Namen der Erfinder trägt. Der Algorithmus eignet sich sowohl für die Verschlüsselung als auch für digitale Signaturen.[174] Da dieser Algorithmus auch in vielen Programmen (z.B. SecureNet, SafeLine[175] , SSH) implementiert ist, jedoch in der Fachliteratur oft zu theoretisch abgehandelt wird, soll das nachstehende einfache Beispiel die Funktionsweise von RSA[176] erläutern.[177]

Beispiel zur Erläuterung des RSA-Algorithmus:

Die Kreditkartennummer **"5409 5364 2828 0225"** soll unter Verwendung des RSA-Algorithmus sicher über das Internet übermittelt werden. Es existieren nur die Ziffern 0-9, Leerzeichen werden nicht berücksichtigt.

1. Wähle zwei Primzahlen *p* und *q*, die grösser als 10^{100} sind
   p = 5, q = 19 (zur Vereinfachung des Beispiels sind die Primzahlen kleiner als 10^{100})
2. Berechne $n = p \cdot q$ und $z = (p-1) \cdot (q-1)$
   n = $p \cdot q = 5 \cdot 19 =$ **95**
   $z = (p-1) \cdot (q-1) = (5-1) \cdot (19-1) = 4 \cdot 18 =$ 72
3. Wähle eine Zahl *e* (= Chiffrierschlüssel), die teilerfremd zu *z* ist
   Wenn e zu z teilerfremd ist, dann haben e und z keine gemeinsamen Faktoren.
   Beispielsweise ist **e = 5** teilerfremd zu z = 72
4. Finde d (= Dechiffrierschlüssel), so dass $e \cdot d = 1 \bmod z$ gilt
   $e \cdot d = 1 \bmod z$ bedeutet, wenn $e \cdot d$ und 1 durch *z* dividiert werden, haben sie denselben Rest. Wird beispielsweise **d = 29** gewählt, dann ist diese Bedingung mit $(5 \cdot 29)/72 = 2$ Rest 1 und 1/72 = 0 Rest 1 erfüllt.
5. Der **öffentliche Schlüssel** (public-key) besteht aus dem Wertepaar **(e,n)**.
6. Der **private Schlüssel** (private-key) besteht aus dem Wertepaar **(d,n)**.
7. Verschlüsselungsfunktion: $C = P^e \pmod n$
   C ist der Rest der Division von P^e durch n.
8. Entschlüsselungsfunktion: $P = C^d \pmod n$
9. Die optimale Blockgrösse *i* ergibt sich aufgrund von $10^{i-1} < n < 10^i$
   n = 95 => **i = 2**

Nachdem der öffentliche Schlüssel (5, 95) und der private Schlüssel (29, 95) des Empfängers errechnet wurde, teilt dieser dem Sender seinen öffentlichen Schlüssel mit. Die Kreditkartennummer wird vom Sender mit dem öffentlichen Schlüssel in Blöcken der Grösse 2 verschlüsselt.

Klartext: 54 09 53 64 28 28 02 25

Verschlüsselung: $54^5 \bmod 95 =$ **04**, $09^5 \bmod 95 =$ **54**, $53^5 \bmod 95 =$ **78**, $64^5 \bmod 95 =$ **49**, ...

Chiffretext: 04 54 78 49 73 73 32 05

Entschlüsselung: $04^{29} \bmod 95 =$ **54**, $54^{29} \bmod 95 =$ **09**, $78^{29} \bmod 95 =$ **53**, $49^{29} \bmod 95 =$ **64**, ...

Klartext nach der Entschlüsselung: 54 09 53 64 28 28 02 25

---

[173] Vgl. [Imper 98], S. 78-79.
[174] Vgl. [Kyas 96b], S. 446-450 und [Schneier 96], S. 531-541.
[175] SecureNet und SafeLine wurden von der Firma r3 entwickelt, um sichere Banktransaktionen zu ermöglichen.
[176] http://www.rsa.com/
[177] Vgl. [Beutelspacher et. al. 95], S. 18-21; [Schneier 96], S. 531-541; [Tanenbaum 96], S. 618-620.

Eine bekannte Implementierung des RSA-Algorithmus findet sich im Programm **PGP**[178] (Pretty Good Privacy) des Amerikaners Phil Zimmermann. PGP ist ein E-Mail-Sicherheitspaket, welches den Datenschutz, die Benutzer-Authentifikation, digitale Unterschriften und die Datenkompression unterstützt. Allerdings schützt PGP nicht vor einer Verkehrsflussanalyse. Das Programm stellt eine Mischform zwischen dem Private-Key-Verfahren und dem Public-Key-Verfahren dar, da es intern sowohl mit RSA als auch mit IDEA und MD5 arbeitet.[179]

Das **S-HTTP**-Protokoll (Secure HyperText Transfer Protocol), eine Weiterentwicklung von HTTP, wurde von Enterprise Integration Technologies Corporation (EIT) ausgearbeitet. Es enthält im Gegensatz zu HTTP zusätzliche Sicherheitsfunktionen wie Absender-Authentifikation, Ursprungsnachweis sowie Unversehrtheit und Vertraulichkeit der Daten. Im Gegensatz zum SSL-Protokoll setzt S-HTTP wie PGP auf der Anwendungsebene an.[180]

Um eine sichere Kommunikation im World Wide Web zu ermöglichen, entwickelte der Softwarehersteller Netscape Communications das **SSL**-Protokoll (Secure Socket Layer). SSL setzt auf der Transportschicht auf und kann alle gebräuchlichen Anwendungsprotokolle (z.B. HTTP) sicher übertragen. Wenn über SSL eine Verbindung zu einem Server aufgebaut wird, findet einerseits eine Authentizitätsprüfung statt, andererseits werden Verschlüsselungsalgorithmus und Sitzungsschlüssel bestimmt. Alle mit SSL eingesetzten Algorithmen verwenden digitale Signaturen, die mit dem MD5[181] Hash-Algorithmus und dem RSA-Unterschriftsalgorithmus erstellt wurden.[182]

Weitere Einsatzmöglichkeiten der Verschlüsselung auf Anwendungsebene finden sich bei den elektronischen Zahlungsmitteln (z.B. CyberCash), auf die aber an dieser Stelle nicht näher eingegangen wird.[183]

In Zukunft werden Sicherheitsmechanismen, auf der Ebene der Kommunikationsprotokolle das Sagen haben. Seit 1995 wird am neuen IP-Protokoll **IPv6** gearbeitet. Im Gegensatz zu dem momentan im Internet verwendeten Protokoll IPv4 mit 32-Bit-Adressen, haben IP-Adressen zukünftig eine Länge von 128 Bit. Ausserdem erlaubt das neue Protokoll verschiedene Varianten von Verschlüsselungen sowie die eindeutige Identifizierung eines Absenders von IP-Paketen. Durch die Authentizität der IP-Pakete wird auch die Programmierung von sicheren Firewallsystemen möglich. Allerdings ist bei der Umstellung mit einem Zeitraum von 10 bis 20 Jahren zu rechnen. Ebenfalls mit kryptographischen Verfahren soll zukünftig auch die Authentizität und die Integrität von DNS-Informationen in Form von **Secure-DNS** sichergestellt werden.[184]

6.4.2.3 Digitale Unterschriften

Mit einer digitalen Unterschrift werden die wesentlichen Eigenschaften einer handschriftlichen Unterschrift in elektronischer Form verwirklicht.[185] Eine Nachricht, die eine digitale Unterschrift aufweist, kann nur von einem bestimmten Kommunikationsteilnehmer erzeugt worden sein. Damit ist auch die Authentizität der Nachricht sichergestellt. Im Gegensatz zu handgeschriebenen Unterschriften weisen digitale Unterschriften bei jeder Unterzeichnung

---

[178] http://www.pgp.com/ und http://www.pgpi.com/
[179] Vgl. [Pabrai et. al. 96], S. 335-347; [Resch 96], S. 85; [Stallings 95], S. 179-194; [Tanenbaum 96], S. 682-686.
[180] Vgl. [Alpar 96], S. 158-159 und [Pohlmann 97], S. 370-373.
[181] Vgl. [Tanenbaum], S. 636-637 und [Weidner 97], S. 11.
[182] Vgl. [Köhntopp 97]; [Kyas 96a], S. 105-107; [Pohlmann 97], S. 373- 375.
[183] Vgl. [Himmelspach et. al. 96], S. 18-25 und [Maurer 97], S. 26-30.
[184] Vgl. [Pohlmann 97], S. 50 und http://www.cert.dfn.de/team/kpk/dud9704.html
[185] Vgl. [Beutelspacher et. al. 95], S. 16-18 und [Meli-Isch 95], S. 48.

eine andere Ausprägung auf und sind demzufolge vom Inhalt der zu unterzeichnenden Daten abhängig.[186] Die Umsetzungen digitaler Unterschriften arbeiten normalerweise mit dem Public-Key-Verfahren. Neben dem RSA-Verfahren existiert auch noch der DSA[187]-Algorithmus (Digital Signature Algorithmus), welcher ebenfalls für digitale Signaturen eingesetzt werden kann. DSA ist aber im Gegensatz zu RSA langsamer und unsicherer.[188]

6.4.2.4 Benutzerauthentifikation

Durch den Nachweis der Authentizität (z.B. kryptographischer Schlüssel) kann sich ein Benutzer Zugang zu einem System verschaffen. Da über das Internet Passwörter unverschlüsselt übertragen werden, empfiehlt sich bei "gefährlichen" Diensten wie Telnet, der Einsatz von Einmal-Passwörtern. Eine weitere Möglichkeit der Authentifikation bieten sogenannte Challenge-Response-Verfahren, bei denen dem Benutzer eine zufällige Frage gestellt wird, auf die er eine richtige Antwort geben muss.[189]

6.4.2.5 Zertifizierung

Damit die Authentizität eines öffentlichen Schlüssels überprüft werden kann, besteht die Möglichkeit, diesen mit dem geheimen Schlüssel einer zentralen Zertifizierungsstelle signieren zu lassen. Der Benutzer generiert ein Schlüsselpaar und verschickt den öffentlichen Schlüssel mit seinen persönlichen Daten an die Zertifizierungsstelle. Um einen Missbrauch auszuschliessen, wird die Identität des Antragstellers jedoch vor der Signierung nachhaltig überprüft.[190]

6.4.3 Redundante Einrichtungen

Wenn gewisse Teile eines Systems mehrfach vorhanden sind, so spricht man von Redundanz. Mit redundanten Einrichtungen (z.B. Datensicherungssystem) wird garantiert, dass beim Verfügbarkeitsverlust einer Systemkomponente sofort eine Ersatzkomponente greifbar ist, um das System wieder instand zu setzen. Um bei einem erfolgreichen Angriff aus dem Internet den Schaden in Grenzen zu halten, helfen redundante Einrichtungen wie regelmässige Backups, Plattenspiegelungen sowie der Einsatz von Parallelsystemen.[191]

6.4.4 Virenschutzprogramme

Durch den Einsatz von Internet-Diensten (z.B. E-Mail) steigt das Risiko eines Virenbefalls von Daten und Programmen in Unternehmungen. Um sich gegen Viren zu schützen, gibt es Virus-Wächter-Programme (z.B. VirusShield) , Virus-Detektionsprogramme[192] (z.B. Virus-Scan) und Virus-Killer-Programme. Virus-Wächterprogramme laufen im Hintergrund und melden dem Benutzer verdächtige Aktionen, die auf ein Virus hindeuten. Virus-Detektionsprogramme und Virus-Killerprogramme werden vom Benutzer eigens gestartet um in der Software und den Daten bestimmte Virenmuster zu erkennen. Ist ein System tatsächlich mit einem Virus infiziert, so kann dieser mit einem Virus-Killerprogramm entfernt werden.[193]

Da Viren jedoch immer durch das Fehlverhalten von Personen (z.B. Verwendung von nicht virengeprüften Programmen) in das Unternehmungssystem eingeschleust werden, müssen primär die Mitarbeiter gegenüber Viren sensibilisiert werden.

---

[186] Vgl. [Käding 91], S. 85-90.
[187] Vgl. [Schneier 96], S. 553-570.
[188] Vgl. [Schneier 96], S. 41-52 und [White et. al. 96], S. 215-216.
[189] Vgl. [Alpar 96], S. 162-163 und [Schaumüller-Bichl 92], S. 173-191.
[190] Vgl. [Kyas 96b], S. 449 und [Pohlmann 97], S. 202-205.
[191] Vgl. [Pohl 93], S. 98.
[192] http://www.mcafee.com/ und http://www.f-prot.com/
[193] Vgl. [Bauknecht et. al. 96a], S. 12-13.

6.4.5 Protokollierung

Der Protokollierung von Systemaktivitäten kommt eine grosse Bedeutung zu, da sie die Funktion der Beweissicherung erfüllt. Wichtig ist dabei, dass die Protokolldaten nicht gefälscht bzw. zerstört werden können. Im Zusammenhang mit dem Internet dient ein Protokoll hauptsächlich zur Erkennung von Sicherheitsverletzungen (z.B. fehlerhafter Authentifikationsprozess) und zur Beweissicherung der Handlungen von Benutzern (z.B. Internetvergnügen statt Arbeiten). Anhand der protokollierten Ereignisse kann die Unternehmung bei schwerwiegenden Verletzungen der Systemsicherheit entsprechende Gegenmassnahmen einleiten.[194]

6.5 Beurteilung

Die Gegenüberstellung von Bedrohungen und Massnahmen zeigt (vgl. Abbildung 19), dass kryptographische Massnahmen den grössten Beitrag zur Reduktion des Risikos im Internet leisten. Kryptographische Massnahmen können die Sicherheitslücken, welche das Internet mit sich bringt, schon auf Protokollebene schliessen. Durch den Einsatz von Protokollen mit Verschlüsselungsmechanismen (z.B. IPv6) wird eine sichere Übertragung von Daten über das Internet möglich. Zudem wird die Vertraulichkeit, Integrität und Authentizität der übertragenen Daten sichergestellt. Da jedoch die Einführung eines neuen Internetprotokolls viel Zeit in Anspruch nimmt, müssen Verschlüsselungsmechanismen bis zur vollständigen Umstellung vorerst noch auf der Anwendungsebene (z.B. PGP) eingesetzt werden. Um umfassende Verkehrsflussanalysen zu verhindern sowie die Daten des internen Unternehmungsnetzwerk gegen Angreifer aus dem Internet abzusichern, bieten sich Firewalls in Kombination mit Verschlüsselungstechniken als ideale Massnahme an.

Neben den technischen Massnahmen, die sicherlich die grösste Bedeutung haben, dürfen aber auch die personellen und die organisatorischen Massnahmen nie vernachlässigt werden. Eine umfassende Schulung der Mitarbeiter, die darlegt, wie sich diese in kritischen Situationen zu verhalten haben, hilft oft viele Angriffe zu vermeiden. Um jedoch die Mitarbeiter und die technischen Möglichkeiten optimal aufeinander abzustimmen, bedarf es einer guten Organisation innerhalb der Unternehmung. Zudem fördert eine gute Organisation das Sicherheitsbewusstsein der Mitarbeiter.

Die Analyse der verschiedenen Massnahmen zur Bekämpfung der Risiken des Interneteinsatzes hat zudem ergeben, dass momentan keine Bedrohungen bzw. Angriffe seitens des Internet existieren, denen nicht durch eine entsprechende Massnahmen begegnet werden kann. Sollte jedoch einmal eine ernstzunehmende Angriffsmöglichkeit auftauchen, für die es keine Gegenmassnahme geben sollte, bleibt der Unternehmung nur noch die physikalische Trennung der gefährdeten Systeme bis eine Lösung gefunden wird.

Wie die Unternehmung bei der Suche nach geeigneten Massnahmen, insbesondere bei der Erkennung von Bedrohungen und Schwachstellen, mit technischen Hilfsmitteln unterstützt werden kann, wird im nächsten Kapitel dargestellt.

---

[194] Vgl. [Pohl 93], S. 97 und [Pohlmann 97], S. 317-330.

Massnahmen / Bedrohungen	Mensch			Organisation				Technik							
	Schulung	Verbote	Sicherheitsbewusstsein fördern	Physikalische Trennung	Situative Rechtevergabe	Sicherheit einzelner Rechner	Zuständigkeiten	Firewalls	Verschlüsselung	Digitale Unterschriften	Benutzerauthentifikation	Zertifizierung	Redundante Einrichtungen	Virenschutzprogramme	Protokollierung
Natürliche Bedrohungen															
z.B. Brand	√	√	√	–	–	√	–	–	–	–	–	–	–	–	–
Passive Angriffe															
Abhören von Daten	–	–	–	√	*o*	*o*	*o*	–	√	–	–	–	–	–	–
Abhören der Teilnehmer-Identitäten	–	*o*	–	√	*o*	*o*	*o*	√	–	–	–	–	*o*	–	–
Verkehrsflussanalyse	–	*o*	–	√	*o*	*o*	*o*	√	–	–	–	–	*o*	–	–
Aktive Angriffe															
Wiederholen von Informationen	*o*	*o*	*o*	√	*o*	*o*	*o*	–	–	–	–	–	–	√	–
Verzögern von Informationen	*o*	*o*	*o*	√	*o*	*o*	*o*	–	–	–	–	–	*o*	√	–
Einfügen und Löschen von Daten	√	√	√	√	*o*	*o*	*o*	–	√	√	√	–	√	√	–
Modifikation von Daten	√	√	√	√	*o*	*o*	*o*	*o*	√	√	*o*	–	√	√	–
Denial of Service	*o*	–	–	√	*o*	*o*	*o*	*o*	–	–	–	–	√	–	–
Masquerade	*o*	–	–	√	*o*	*o*	*o*	*o*	√	√	√	–	–	√	–
Leugnung der Kommunikation	√	–	*o*	–	–	–	–	–	*o*	√	√	√	*o*	–	√
Hijacking	√	√	√	√	*o*	*o*	*o*	√	√	–	√	–	√	*o*	√
Systemanomalien	√	√	√	*o*	*o*	*o*	*o*	*o*	–	*o*	*o*	*o*	–	√	√
Zufällige Verfälschungen															
Fehlrouting von Informationen	–	–	–	–	–	–	–	–	–	–	–	–	√	–	√
Übertragungsfehler	–	–	–	–	–	–	–	–	–	–	–	–	√	–	√
Software-Fehler	–	–	–	–	–	–	–	–	–	–	–	–	–	–	√
Fehlbedienung	√	√	√	–	*o*	*o*	*o*	–	–	–	–	–	√	–	√

√ direkter Einfluss
o indirekter Einfluss
– kein Einfluss

Abbildung 19: Zuordnung von Bedrohungen und Massnahmen

7. Audit-Tools zur Erkennung von Schwachstellen

7.1 Überblick

Nachdem in den vorhergehenden Kapiteln gezeigt wurde, welche Risiken sich aus dem Interneteinsatz ergeben und welche Gegenmassnahmen daraus abgeleitet werden können, stellt sich die Frage, wie die Unternehmung in diesem Prozess unterstützt werden kann. Im Internet selber finden sich eine Reihe von Audit-Tools, die helfen, das System zu überwachen und Konfigurationsfehler aufzuspüren. Wenn die Unternehmung diese Werkzeuge nicht selber einsetzt, so werden diese von potentiellen Angreifern missbraucht, um die Schwachstellen im Unternehmungssystem ausfindig zu machen. Es ist deshalb von grösster Wichtigkeit, dass die Unternehmung ihr System auf allgemein bekannte Sicherheitslücken untersucht (z.B. CERT-Mitteilungen[195]).

Ursprünglich wurde der englische Begriff "Audit" im Rechnungswesen für die Rechnungsprüfung verwendet. In der Informatik kann jedoch das Audit als Revision und Controlling von sicherheitsrelevanten Ereignissen gesehen werden. Die Revision dient der sporadischen Überprüfung, das Controlling hingegen der laufenden Überwachung des Unternehmungssystems.

Audit-Tools lassen sich je nach Funktionalität in Angriffssimulatoren, in Programme zur Prüfung der Systemsicherheit und in Überwachungsprogramme (Intrusion Detection) einteilen (vgl. Abbildung 20).

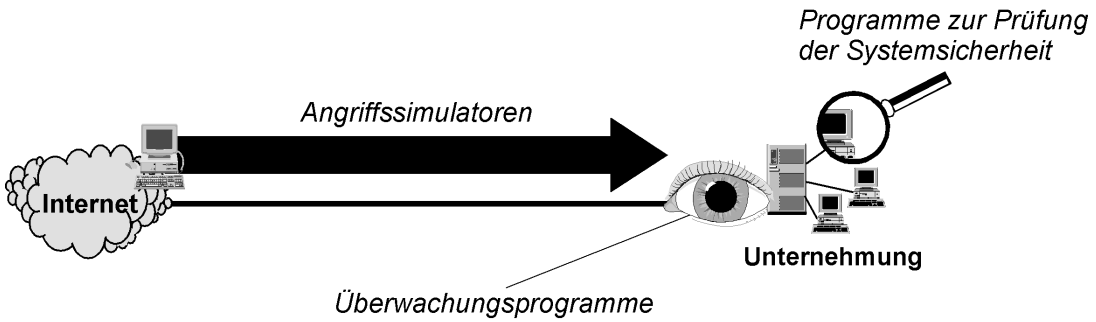

Abbildung 20: Arten von Audit-Tools[196]

Angriffssimulatoren (z.B. SATAN) sind Programme, welche auf einem am Internet angeschlossenen Rechner ausgeführt werden, um einen Angriff auf ein anderes System im Internet zu simulieren. Im Gegensatz zu den Angriffssimulatoren werden die Programme zur Prüfung der Systemsicherheit (z.B. COPS) lokal auf dem zu untersuchenden System eingesetzt. Während Angriffssimulatoren und Programme zur Überprüfung der Systemsicherheit manuell gestartet werden müssen, laufen Überwachungsprogramme (z.B. IP-Watcher) aktiv im Hintergrund und helfen Angriffe auf das System zu erkennen.

In der Fachliteratur finden sich jedoch nur wenige Hinweise über solche Tools. Dies erstaunt nicht, denn erst im Jahre 1995, als erste erfolgreiche Versuche mit dem Angriffssimulator SATAN bekannt wurden, begann sich auch die breite Öffentlichkeit für diese Sicherheitstools zu interessieren.[197] Die Informationen zur Evaluation dieser Tools stammen deshalb vorwiegend aus dem Internet sowie aus eigenen Erfahrungen.

---

[195] Vgl. http://www.cert.org/
[196] Vgl. [Kyas 96a], S. 180-184; [Siyan et. al. 95], S. 77-78; [White et. al. 96], S. 91-115.
[197] Vgl. ftp://ftp.cert.org/pub/cert_advisories/CA-95%3A06.satan

Die Liste der vorgestellten Tools kann ohne weiteres ergänzt werden, da ähnlich wie bei den Programmiersprachen, beinahe jede Universität ihr eigenes Werkzeug entwickelt hat. Um jedoch trotzdem einen Einblick in das vielfältige Angebot der Audit-Tools zu verschaffen, wurden nur diejenigen Tools berücksichtigt, die entweder einen hohen Bekanntheitsgrad aufweisen oder sich durch ihre speziellen Funktionen von den anderen differenzieren.

7.2 Angriffssimulatoren

7.2.1 SATAN (Security Administrator Tool for Analyzing Networks)

Das Programm SATAN[198] dient der Überprüfung von allgemein bekannten Schwachstellen auf einem System. Entwickelt wurde SATAN von Wietse Venema, dem Autor des TCP-Wrappers und von Dan Farmer, dem Autor von COPS. SATAN läuft unter dem Betriebssystem UNIX und benötigt zudem die Interpreter-Sprache Perl 5.0 sowie einen Web-Browser für die graphische Darstellung der Resultate. Entgegen vielen Befürchtungen, die vielleicht auch aufgrund des negativ klingenden Namens hervorgerufen wurden, nützt SATAN die erkannten Schwachstellen nicht aus. Das Tool bietet jedoch für jede erkannte Schwachstelle ein Tutorial an, welches das Problem sowie mögliche Auswirkungen erläutert. Zudem erklärt das Tutorial, welche Gegenmassnahmen zur Behebung der erkannten Schwachstellen getroffen werden können (vgl. Abbildung 21).[199]

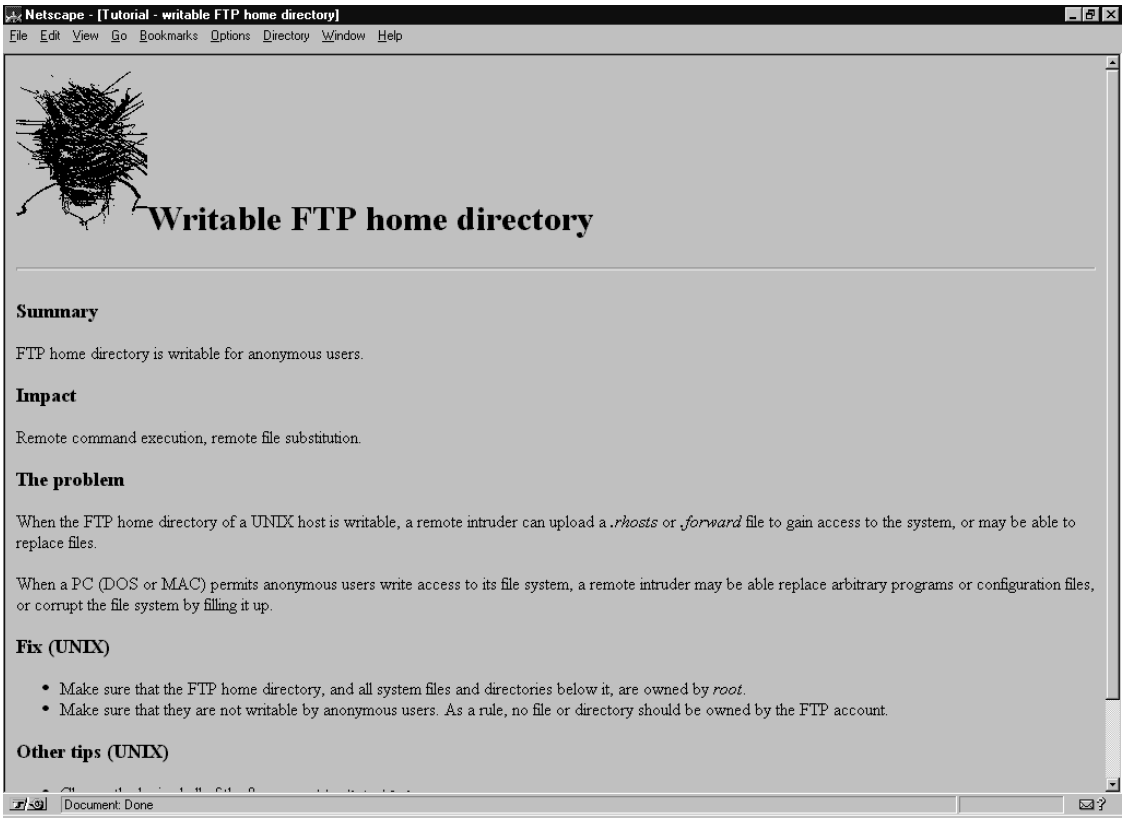

Abbildung 21: SATAN-Tutorial

[198] Vgl. http://www.fish.com/satan/
[199] Vgl. [Chapman et. al. 96], S. 518 und [Macgregor et. al. 96], S. 165-167.

SATAN kennt nur etwa zehn verschiedene Arten von Sicherheitslücken.[200] Das Programm kann jedoch problemlos um weitere Regeln ergänzt werden, damit auch neuere Sicherheitslücken erkannt werden können.[201] Standardmässig überprüft SATAN die folgenden potentiellen Sicherheitslücken eines Unternehmungssystems: NFS[202] -Dateisystem, NIS[203] -Passwortdateizugriff, rexd-Zugriff, sendmail-Fehler, Zugriffsrechte von Anonymous-FTP, Dateizugriffe via TFTP[204] , rsh-Zugriffe, rlogin-Zugriffe, Zugriffsrechte auf X-Server.

Bezugsquelle von SATAN im Internet:

ftp://ftp.win.tue.nl/pub/security/satan.tar.Z

7.2.2 ISS (Internet Security Scanner)

Der Name “Internet Security Scanner” steht für die im Internet frei verfügbare Version des kommerziellen Netzschwachstellenanalysepaketes SAFEsuite der Firma Internet Security Systems (ISS). SAFEsuite besteht aus den drei Produkten, “Internet Scanner”, “System Security Scanner” und “RealSecure”.

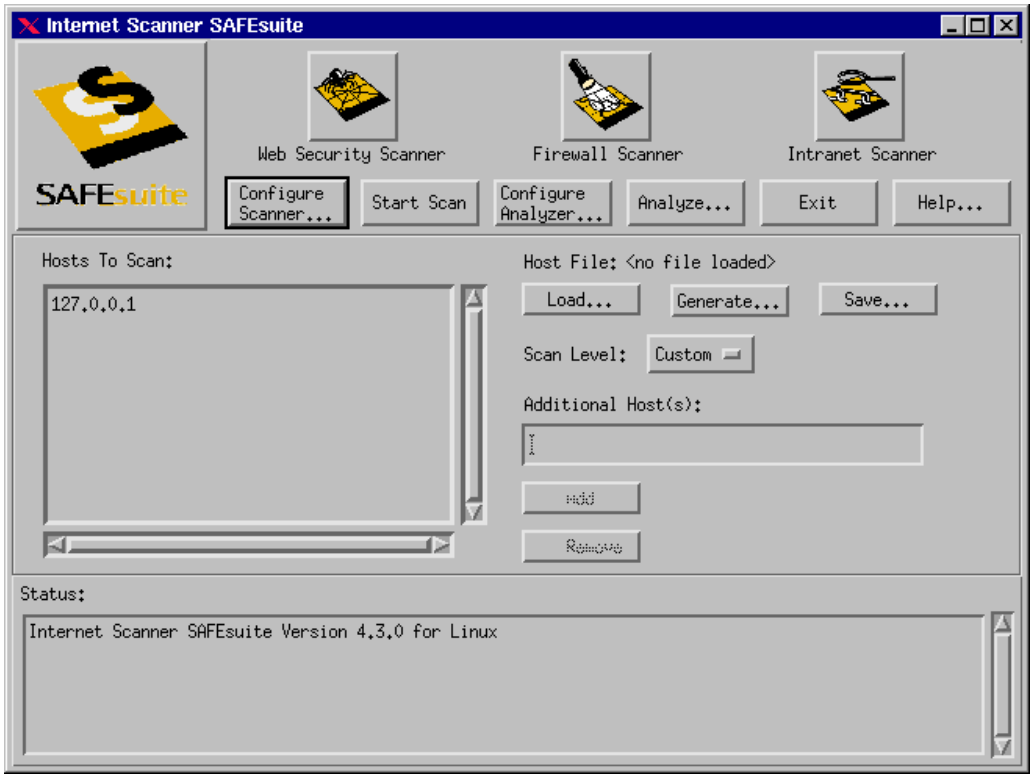

Abbildung 22: Internet Scanner[205]

Der **Internet Scanner** untersucht das Unternehmungsnetzwerk nach allgemein bekannten Sicherheitslücken. Die Datenbank des Programmes beinhaltet 287 Schwachstelleneinträge und ist somit viel umfangreicher als SATAN. Mit dem Internet Scanner werden Schwachstellen der Betriebssysteme UNIX, Windows NT, Windows 95 und Windows for Workgroups

---

200 Vgl. http://www.datamation.com/PlugIn/issues/1996/march1/03ainfc1.html
201 Vgl. http://www.cert.dfn.de/team/wl/papers/satan/
202 Network File System
203 Network Information Service
204 Trivial File Transfer Protocol
205 Vgl. http://www.iss.net/

untersucht.[206] Das Werkzeug besteht aus drei Modulen, die Intranets, Firewalls und Webserver überprüfen (vgl. Abbildung 22).[207]

Nach der Analyse des Systems auf Schwachstellen liefert der Internet Scanner Problembeschreibungen der Sicherheitslücken sowie Lösungsvorschläge zu deren Behebung.

Der **System Security Scanner** erlaubt es, Schwachstellen in der Konfiguration des Betriebssystem zu untersuchen (vgl. Abbildung 23). Dies beinhaltet potentielle Schwachstellen wie Dateiberechtigungen, Dateibesitz, leicht zu erratende Passwörter und Benutzer-Account-Konfiguration. [208]

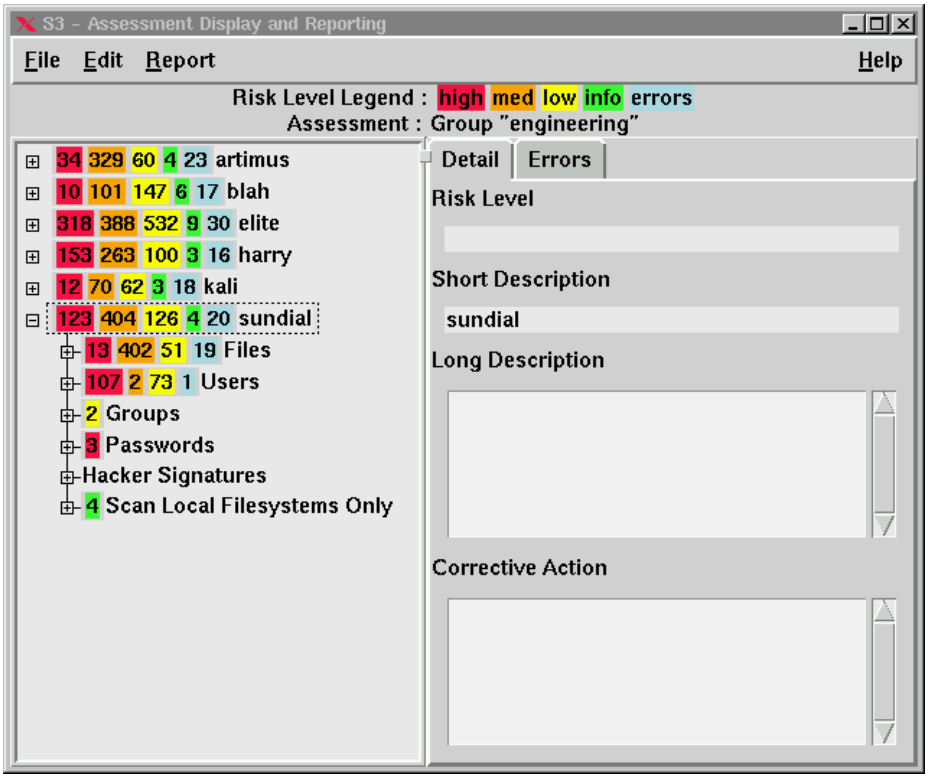

Abbildung 23: Schwachstellenreport des System Security Scanner

RealSecure ist ein Überwachungsprogramm, das Angriffe auf das Unternehmungssystem erkennt und den Systemadministrator via E-Mail benachrichtigt. Das Programm beendet die Verbindung bei einem erkannten Angriff automatisch.[209]

Die frei verfügbare Version des Internet Security Scanners ist gegenüber der kommerziellen Version stark eingeschränkt. Sie bietet daher lediglich einen Bedienungsumfang ähnlich dem Programm SATAN. Im Unterschied zu SATAN werden jedoch zusätzlich die Benutzeraccounts auf schwache Passwörter untersucht.[210]

Bezugsquelle des Internet Security Scanners im Internet:

http://www.iss.net/ (Kommerzielle Version)

ftp://ftp.iss.net/pub/iss/ (Freie Version)

---

206 Vgl. http://www.zdnet.com/products/content/pcwk/1451/pcwk0026.html
207 Vgl. http://www.iss.net/eval/manual/iss/chap1.html
208 Vgl. http://www.winmag.com/library/1997/1001/ntent017.htm
209 Vgl. http://www.iss.net/prod/rs.html
210 Vgl. ftp://ftp.cert.org/pub/cert_advisories/CA-93%3A14.Internet.Security.Scanner

7.2.3 Pingware

Pingware, ein kommerzielles Sicherheitstool der Firma Bellcore[211], identifiziert die Sicherheitslücken eines Systems und generiert einen Bericht, welcher die Schwachstellen des Unternehmungsnetzwerkes und ihre Behebung aufzeigt. Das Sicherheitswerkzeug simuliert einen Angreifer, welcher versucht, durch bekannte Konfigurationsfehler und Schwachstellen der auf TCP/IP basierenden Dienste, Zugang zum System zu bekommen. Nachdem Pingware gestartet wurde, läuft das Programm im Hintergrund und untersucht mehr als 400 IP-Adressen pro Stunde. Pingware untersucht dabei Schwachstellen wie finger, ftp, http, NFS, rlogin, rsh, rpcinfo, sendmail, tftp, xhost und Passwörter. Neu bekanntwerdende Sicherheitslücken werden vom Hersteller überprüft und sofort in die aktuellen Programm-Versionen aufgenommen.[212]

Bezugsquelle von Pingware im Internet:

http://www.bellcore.com/BC.dynjava?PingwarePDGeneralProductDescription

7.2.4 NetProbe

Das kommerzielle Netzwerksicherheitsanalysetool NetProbe stammt von der Firma Qualix Group[213] und untersucht die Netzwerke auf allgemein bekannte Schwachstellen und unsaubere Konfigurationen. Das Programm läuft ebenfalls im Hintergrund und führt über 85 Tests auf 100 Rechnern in weniger als 5 Minuten durch. Die Testresultate enthalten Beschreibungen der gefundenen Schwachstellen sowie Lösungsvorschläge, um die Sicherheitslücken zu schliessen.[214] Die Testresultate enthalten zudem Verweise auf die Advisories von CERT und CIAC. NetProbe führt jedoch keine selbständige Korrektur der Schwachstellen durch. Ausserdem können die neu bekanntwerdenden Sicherheitslücken ohne Neuinstallation der Software implementiert werden.[215] Die Software funktioniert übrigens nur auf dem Rechner, dessen IP-Adresse lizenziert ist. Damit wird verhindert, dass Angreifer das Tool auf anderen Rechnern anwenden.[216]

Bezugsquelle von NetProbe im Internet:

http://www.qualix.com/html/netprobe.html

7.3 Programme zur Prüfung der Systemsicherheit

7.3.1 COPS (Computer Oracle and Password System)

Da Betriebssystem UNIX beinhaltet eine Reihe von kritischen Bereichen, die für die Sicherheit des Systems von Bedeutung sind. Das Überprüfen dieser Bereiche ist zwar relativ einfach, aber zeitaufwendig. Das Programm COPS besteht aus einer Anzahl von Shellscripten, welche diese Aufgabe übernehmen. Es werden sicherheitsrelevante Bereiche wie Zugriffsrechte, Passwortdateien, Systemdateien, FTP-Installationen sowie die CERT-Advisories überprüft.[217] COPS versucht jedoch nicht, die gefundenen Sicherheitslücken zu korrigieren oder auszunutzen; der Benutzer wird lediglich gewarnt.[218]

---

[211] http://www.bellcore.com/
[212] Vgl. http://www.bellcore.com/BC.dynjava?PingwarePDGeneralProductDescription
[213] http://www.qualix.com/
[214] Vgl. http://www.datamation.com/PlugIn/issues/1996/march1/03ainfc1.html
[215] Vgl. http://www.qualix.com/html/netprobe.html
[216] Vgl. http://www.qualix.com/html/nprb_faqs.html
[217] Vgl. http://www.cert.dfn.de/infoserv/dib/dib-9305.html und [Pabrai et. al. 96], S. 201-206.
[218] Vgl. ftp://ftp.cert.dfn.de/pub/tools/admin/Cops/COPS-README.1

Bezugsquelle von COPS im Internet:

ftp://coast.cs.purdue.edu/pub/tools/unix/cops/

7.3.2 TAMU-Tiger

TAMU-Tiger besteht, wie COPS, aus verschiedenen Shellscripts, welche die Sicherheit des eigenen UNIX-Systems untersuchen. Das Programm wurde an der Texas A&M University (TAMU) entwickelt und diente ursprünglich dazu, die UNIX-Systeme der Universität zu überprüfen, bevor der Paketfilter im Firewall auch Zugriffe von aussen zuliess. Im Gegensatz zu COPS nimmt der TAMU-Tiger an, dass der Angreifer bereits Zugang zum System hat und nach Wegen sucht, wie er Administratorenrechte erlangen kann. Tiger prüft cron-Einträge, Mail-Aliases, NFS, inetd-Einträge und PATH-Zuweisungen. Das Tool überprüft auch die rhosts- und netrc-Dateien sowie Datei- und Verzeichnisberechtigungen. Ausserdem meldet der TAMU-Tiger, wenn er Programmdateien findet, für die es inzwischen verbesserte Versionen der Hersteller gibt.[219]

Bezugsquelle von TAMU-Tiger im Internet:

ftp://net.tamu.edu/pub/security/TAMU/

7.3.3 Crack und CrackLib

Um das UNIX-Betriebssystem auf unsichere Passwörter zu untersuchen, kann das frei verfügbare Programm “Crack” von Alec Muffett verwendet werden. Das Programm versucht die verschlüsselten Passwörter des Systems mit Hilfe von Wörterlisten (können problemlos erweitert werden!) zu erraten. Erratene Passwörter werden von Crack gemeldet; sie werden jedoch nicht automatisch geändert.[220] Im Zusammenhang mit Crack muss auch das Programm CrackLib[221] des gleichen Autors erwähnt werden. CrackLib verhindert, dass Benutzer Passwörter auswählen, die mit Crack erraten werden können.[222] Programme zur Prüfung von Passwörtern finden sich beinahe für jedes Betriebssystem. Unter Windows NT hat sich beispielsweise das Programm ScanNT etabliert.[223]

Bezugsquelle von Crack und CrackLib im Internet:

http://www.users.dircon.co.uk/~crypto/

7.4 Überwachungsprogramme

7.4.1 IP-Watcher

Der IP-Watcher ist ein kommerzielles Werkzeug, das dem Benutzer die Möglichkeit gibt, alle Verbindungen im eigenen Netzwerk zu überwachen und zu kontrollieren (vgl. Abbildung 24). Auf diese Weise können verdächtige Aktivitäten auf dem System erkannt werden und die bösartigen Benutzer gestoppt werden, bevor sie einen Schaden anrichten können. Ausserdem kann mit dem IP-Watcher genügend Beweismaterial gegen Angreifer protokolliert werden.

Der IP-Watcher ist in der Lage, alle IP-Verbindungen, die auf seinem Subnet laufen, zu überwachen, indem eine Technik namens “IP-Hijacking” verwendet wird.[224] Damit können bestehende IP-Verbindungen sowohl überwacht als auch übernommen werden. Da diese

---

[219] Vgl. http://www.itp.ac.ru/books/UNIX/unx44.htm#I38
[220] Vgl. ftp://ftp.cert.org/pub/tools/crack/README
[221] Weitere Programme zur Überprüfung der Passwortsicherheit sind Npasswd und Passwd+.
[222] Vgl. http://www.users.dircon.co.uk/~crypto/cracklib,2.7.txt
[223] Vgl. http://www.ntsecurity.com/Products/ScanNT/index.html
[224] Vgl. http://www.engarde.com/software/ipwatcher/

Technik auch von Angreifern zur Überlistung eines Firewalls genutzt wird, stellt der IP-Watcher in falschen Händen eine nicht unerhebliche Gefahr dar.[225] Ein Provider beispielsweise kann unter Verwendung des IP-Watchers alle Tastatureingaben und Passwörter, welche ein Kunde während einer Telnetverbindung macht, überwachen.

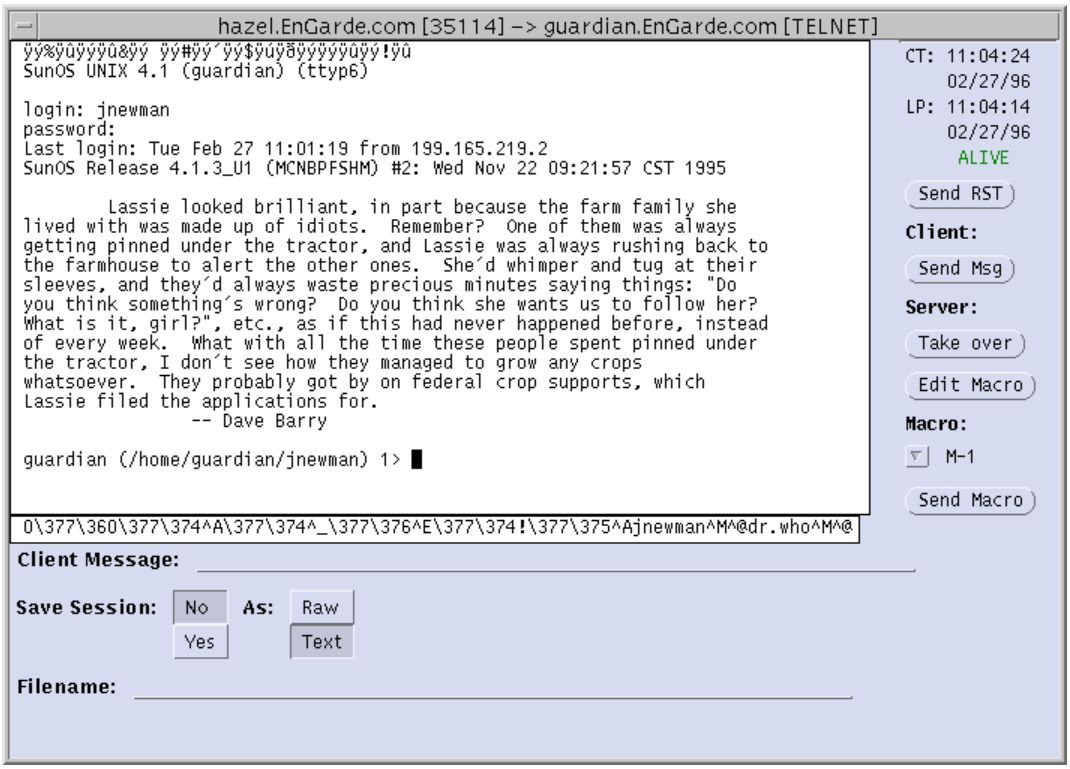

Abbildung 24: IP-Watcher beim Überwachen einer Telnet-Sitzung[226]

Bezugsquelle des IP-Watchers im Internet:

http://www.engarde.com/software/

7.4.2 TTY-Watcher

Beim TTY-Watcher handelt es sich um die frei verfügbare Version des IP-Watchers. Allerdings ist der TTY-Watcher in seinem Bedienungsumfang eingeschränkt und kann deshalb nur einen einzelnen Rechner überwachen. Wie der IP-Watcher kann auch der TTY-Watcher jede Tastatureingabe des TTY-Fensters auf dem überwachten System aufzeichnen und modifizieren. Der Hauptunterschied zum IP-Watcher besteht darin, dass der TTY-Watcher nur TTY-Verbindungen kontrollieren kann und nicht wie der IP-Watcher TCP/IP-Verbindungen.[227]

Bezugsquelle des TTY-Watchers im Internet:

ftp://coast.cs.purdue.edu/pub/tools/unix/ttywatcher/

---

[225] Vgl. [Kyas 96a], S. 183.
[226] Vgl. http://www.EnGarde.com/software/ipwatcher/images/session_xview.gif
[227] Vgl. http://nswt.tuwien.ac.at/htdocs/internet/unix/sys_admin/TTY-Watcher.html

7.4.3 TCP-Wrapper

Mit dem TCP-Wrapper kann die Nutzung von Netzwerkdiensten (z.B. Telnet) überwacht und kontrolliert werden. Der TCP-Wrapper nutzt dabei die Tatsache aus, dass die meisten TCP/IP-Anwendungen auf dem Client-Server-Modell basieren. Im Normalfall übernimmt der Internetdämon inetd die Kontrolle über die Serverprogramme. Um die von inetd gestarteten Server-Dienste zu überwachen, wird statt dem jeweiligen Original-Server (z.B. telnetd), der TCP-Wrapper (tcpd) gestartet. Dieser übernimmt danach die Kontrolle über die Server und startet diese nur, wenn eine Zugangsberechtigung vorhanden ist. Die Zugangsberechtigung ergibt sich aufgrund der in /etc/hosts.allow und /etc/hosts.deny gespeicherten Regeln. Zuerst werden die Regeln in /etc/hosts.allow, danach die Regeln in /etc/hosts.deny berücksichtigt. Wenn keine Regel gefunden wird, erlaubt der TCP-Wrapper den Zugriff auf den jeweiligen Dienst. Damit der TCP-Wrapper lauffähig ist, müssen alle Original-Server (z.B. ftpd) durch den TCP-Wrapper ersetzt und die Datei inetd.conf entsprechend angepasst werden (vgl. Abbildung 25).[228]

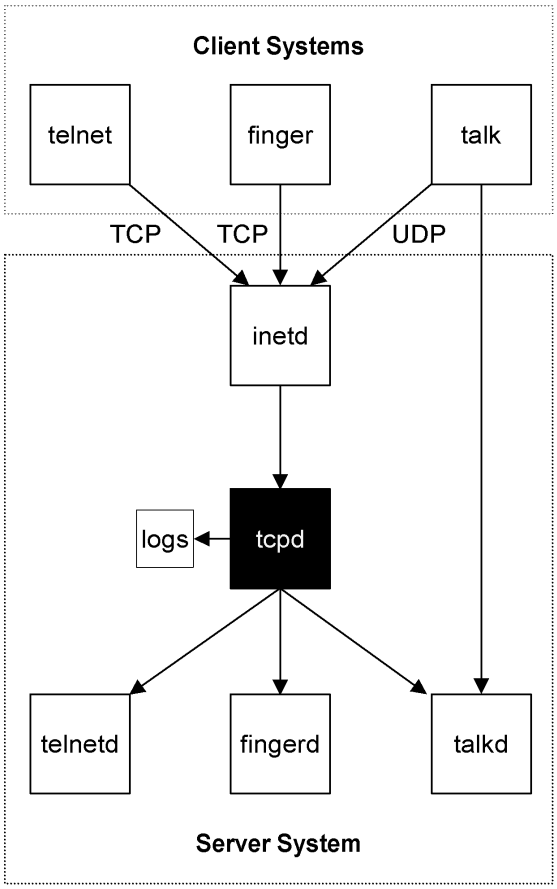

Abbildung 25: Funktionsweise des TCP-Wrappers[229]

Bezugsquelle des TCP-Wrappers im Internet:

ftp://ftp.win.tue.nl/pub/security/

[228] Vgl. http://www.cert.dfn.de/infoserv/dib/dib-9307.html und [Hughes 95], S. 316-320.
[229] Vgl. [Hughes 95], S. 317.

7.4.4 Tripwire

Tripwire wurde an der Purdue University von Gene Kim und Gene Spafford entwickelt. Das Programm überprüft die Integrität von Dateisystemen, indem es Dateien und Verzeichnisse mit Informationen vergleicht, welche in einer zuvor generierten Datenbank gespeichert wurden. Es werden alle Dateien gemeldet, die sich vom Zustand in der Datenbank unterscheiden. Dazu gehören unerwünschte Programmänderungen (z.B. durch Viren) sowie hinzugefügte, gelöschte und modifizierte Dateien.[230]

Bezugsquelle von Tripwire im Internet:

ftp://coast.cs.purdue.edu/pub/COAST/Tripwire/

7.4.5 Gabriel

Gabriel, von Los Altos Technologies, ist ein Detektor, welcher Netzwerkuntersuchungen mit Angriffssimulatoren wie SATAN wahrnimmt. Sobald unerlaubte Netzwerkuntersuchungen entdeckt werden, benachrichtigt das Programm den Systemadministrator. Zudem speichert das Programm, woher der Angriffssimulator gestartet wurde.[231] Dasselbe Ziel strebt auch das vom CIAC[232] entwickelte Programm Courtney[233] an.

Bezugsquelle von Gabriel im Internet:

ftp://ftp.lat.com/gabriel-1.0.tar.Z

7.4.6 Argus

Argus ist ein IP-Netzwerküberwachungstool der Carnegie Mellon University, welches aus dem Dämon “argus” und den Programmen “ra” und “services” besteht. Der Dämon “argus” protokolliert die auf dem Netzwerk übertragenen Pakete in eine Logdatei, welche anschliessend mit den Programmen “ra” und “services” ausgewertet werden kann. Da jedoch bei der Überwachung aller übertragenen Pakete, der Festplattenspeicher bald einmal an seine Grenzen stösst, führt Argus jeweils eine Aktualisierung der gespeicherten statischen Daten durch.[234]

Die Logdatei von Argus enthält Einträge über Ethernet-Adressen, IP-Adressen, TCP-Ports, UDP-Ports, den Zeitpunkt des ersten und des letzten empfangenen Paketes sowie die Anzahl der übertragenen Bytes pro Richtung.[235]

Bezugsquelle von Argus im Internet:

ftp://ftp.sei.cmu.edu/pub/argus-1.5/

7.4.7 Swatch

Das an der Stanford University entwickelte Programm Swatch ist ein Werkzeug, mit dem Logdateien überwacht und gefiltert werden können. Ausserdem kann Swatch bestimmte Aktionen (z.B. Schicken einer E-Mail) an Protokolleinträge binden.[236]

Bezugsquelle von Swatch im Internet:

ftp://ftp.stanford.edu/general/security-tools/swatch/

---

[230] Vgl. http://www.cert.dfn.de/infoserv/dib/dib-9304.html; [Chapman et. al. 96], S. 518; [Cannady et. al. 96].
[231] Vgl. http://www.lat.com/gabe.htm
[232] http://ciac.llnl.gov/
[233] ftp://ciac.llnl.gov/pub/ciac/sectools/unix/courtney/
[234] Vgl. http://www.cert.dfn.de/infoserv/dib/dib-9602.html
[235] Vgl. ftp://ftp.net.cmu.edu/pub/argus-1.5/argus-1.5.announce
[236] Vgl. [Cheswick et. al. 95], S. 330 und http://www.cert.dfn.de/infoserv/dib/dib-9306.html

7.4.8 NID (Network Intrusion Detector)

Das Programm NID ist eine Entwicklung des Computer Security Technology Centers (CSTC). Es beinhaltet eine Reihe von Werkzeugen, um einen Angreifer zu entdecken und Beweismaterial zu sichern. NID arbeitet im Hintergrund eines auf dem IP-Protokoll basierenden Netzwerks.

Das Tool wird in einem gesicherten Bereich des Netzwerkes eingesetzt und unterstützt die Erkennung von Einbrüchen in das Unternehmungssystem. Dazu gehört die unberechtigte Nutzung von Computern durch Personen, die entweder gar keinen Zugang zum System haben oder denjenigen Personen, die zwar Zugang zum System haben, aber unerlaubte oder verdächtige Handlungen durchführen.[237]

Bezugsquelle von NID im Internet:

http://ciac.llnl.gov/cstc/nid/nidavl.html

[237] Vgl. http://ciac.llnl.gov/cstc/nid/intro.html

8. Beurteilung der Audit-Tools

8.1 Überblick

Im vorhergehenden Kapitel wurden verschiedene Audit-Tools zur Erkennung von Schwachstellen vorgestellt. Abschliessend werden nun die in Kapitel 7 dargestellten Tools evaluiert. Die in der vorliegenden Arbeit identifizierten Bedrohungen, Schwachstellen und Massnahmen fliessen als Bewertungsgrundlagen in den Kriterienkatalog der Evaluation. Ausserdem findet eine Gegenüberstellung von kommerziellen und nicht-kommerziellen Programmen statt. Zum Abschluss wird untersucht, welche Betriebsysteme durch die verschiedenen Audit-Tools unterstützt werden.

8.2 Evaluation

Bei der Evaluation eines Audit-Tools geht es darum herauszufinden, welches Produkt die Anforderungen der Unternehmung am besten erfüllt. Diese Anforderungen werden von der Unternehmung in einem sogenannten Pflichtenheft festgehalten.

Je nach Funktionalität der Audit-Tools, erkennen diese entweder Bedrohungen oder Schwachstellen und treffen daraufhin geeignete Massnahmen (vgl. Abbildung 26). Um das Risiko eines erfolgreichen Angriffes möglichst klein zu halten, empfiehlt sich für eine Unternehmung der Einsatz eines Audit-Tools, das sowohl Bedrohungen erkennen, als auch Schwachstellen im Unternehmungssystem identifizieren kann. Auf diese Weise wird ein aktiver Schutz vor potentiellen Angreifern in Form von Überwachungsprogrammen und ein passiver Schutz mit Hilfe von Programmen zur Überprüfung von Schwachstellen gewährleistet.

Audit-Tools / Funktionen	Angriffs-simulatoren	Programme zur Prüfung der Systemsicherheit	Überwachungs-programme
Erkennung von Bedrohungen	–	–	√
Erkennung von Schwachstellen	√	√	–
Treffen von Massnahmen	√	√	√

Abbildung 26: Hauptfunktionen von Audit-Tools

Abbildung 27 zeigt die Bewertung der in Kapitel 7 besprochenen Audit-Tools. Als Bewertungskriterien agieren primär die verschiedenen Bedrohungen und Schwachstellen, die von den Audit-Tools erkannt werden. Ausserdem treten die Massnahmen, welche ein Audit-Tool umsetzt, im Kriterienkatalog auf. Ebenfalls nicht zu vernachlässigen sind Bewertungskriterien, die sich nicht auf die technische Funktionen der Audit-Tools beziehen (z.B. Service). Bewusst nicht in den Kriterienkatalog aufgenommen wurden die Kosten der jeweiligen Audit-Tools, denn Kosten dürfen nie ein Entscheidungskriterium sein, ein Sicherheitstool nicht zu wählen. Vielmehr hat die Unternehmung zu überprüfen, ob die Audit-Tools auf dem neusten Stand der Technik sind und ob diese die unternehmungsspezifischen Sicherheitslücken erkennen.

Audit-Tools / Funktionen	Angriffssimulatoren				Programme zur Prüfung der Systemsicherheit				Überwachungsprogramme							
	SATAN	ISS (SAFEsuite)	Pingware	NetProbe	COPS	TAMU-Tiger	Crack	CrackLib	IP-Watcher	TTY-Watcher	TCP-Wrapper	Tripwire	Gabriel	Argus	Swatch	NID
Bedrohungserkennung																
IP-Verbindungen überwachen	–	√	–	–	–	–	–	–	√	–	–	–	–	√	–	√
TTY-Verbindungen überwachen	–	√	–	–	–	–	–	–	√	√	–	–	–	√	–	√
Kontrolle über Netzwerkdienste	–	√	–	–	–	–	–	–	√	–	√	–	–	√	–	√
Erkennen von Programmveränderungen	–	√	–	–	–	–	–	–	–	–	–	√	–	–	–	–
Angriffssimulatorenerkennung	–	√	–	–	–	–	–	–	*o*	–	*o*	–	√	*o*	–	*o*
Denial of Service	–	√	–	–	–	–	–	–	*o*	–	*o*	–	–	*o*	–	*o*
Überwachung der Log-Dateien	–	√	–	–	–	–	–	–	–	–	–	–	–	–	√	–
Schwachstellenerkennung																
NFS	√	√	√	√	√	√	–	–	–	–	–	–	–	–	–	–
NIS	√	√	–	√	–	–	–	–	–	–	–	–	–	–	–	–
rexd	√	√	–	√	√	–	–	–	–	–	–	–	–	–	–	–
rsh	√	√	√	√	–	√	–	–	–	–	–	–	–	–	–	–
rlogin	√	√	√	√	–	–	–	–	–	–	–	–	–	–	–	–
X-Windows	√	√	√	√	–	–	–	–	–	–	–	–	–	–	–	–
sendmail	√	√	√	√	–	–	–	–	–	–	–	–	–	–	–	–
FTP	√	√	√	√	√	√	–	–	–	–	–	–	–	–	–	–
TFTP	√	√	√	√	√	√	–	–	–	–	–	–	–	–	–	–
Passwörter	–	√	–	√	√	–	√	√	–	–	–	–	–	–	–	–
Webserver	–	√	√	–	–	–	–	–	–	–	–	–	–	–	–	–
Firewalls	–	√	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Durchgeführte Massnahmen																
Problembeschreibung	√	√	√	√	–	–	–	–	–	–	–	–	–	–	–	–
Massnahmenvorschlag	√	√	√	√	–	–	–	–	–	–	–	–	–	–	–	–
Ergreifen von Massnahmen	–	√	–	–	–	–	–	–	–	–	*o*	–	–	–	√	–
Automatische Alarmierung	–	√	–	–	–	–	–	–	–	–	–	–	√	–	√	√
Sonstige Funktionen																
Verwendung nur auf lizenzierten Netzwerken	–	√	–	√	–	–	–	–	–	–	–	–	–	–	–	–
Regelmässige Updates	–	√	√	√	–	–	–	–	√	–	–	–	–	–	–	√
Kommerzielle Version	–	√	√	√	–	–	–	–	√	–	–	–	–	–	–	√

√ direkter Einfluss
o indirekter Einfluss
– kein Einfluss

Abbildung 27: Evaluation der Audit-Tools

Die Evaluation der in Abbildung 27 dargestellten Audit-Tools lässt das Programmpaket SAFEsuite der Firma Internet Security Systems als Sieger hervorgehen. Das Produkt beinhaltet sowohl einen Angriffssimulator als auch ein Überwachungsprogamm und ist auf dem neusten Stand der Technik. Zudem sprechen ein hoher Bekanntheitsgrad sowie ein ausgezeichneter Support für dieses Tool.

Auf einem ähnlich guten technischen Stand wie SAFEsuite befinden sich die Programme Pingware und NetProbe, die allerdings nicht als Überwachungsprogramme eingesetzt werden können. Pingware überprüft das System nicht auf schwache Passwörter und bietet zudem keine Firewallüberprüfung an. NetProbe verzichtet auf eine Webserverüberprüfung als auch auf eine Firewallüberprüfung. Das ebenfalls als Angriffssimulator aufgeführte Programm SATAN eignet sich nur für eine elementare Überprüfung des Systems und kann den Systemverantwortlichen ein erstes Mal auf mögliche Sicherheitslücken aufmerksam machen.

COPS und TAMU-Tiger untersuchen das Unternehmungssystem auf Sicherheitslücken, die im UNIX-Betriebssystem begründet sind. Um das System lediglich auf unsichere Passwörter zu untersuchen eignen sich die Programme Crack und CrackLib.

Eine Überwachung von IP-Verbindungen lässt sich mit den kommerziellen Tools IP-Watcher und NID realisieren. Möchte eine Unternehmung jedoch nur einmal die Möglichkeiten eines Überwachungstools testen, so kann diese die frei verfügbaren Programme TTY-Watcher oder Argus einsetzen. Um allfällige Programmveränderungen auf dem System zu erkennen, eignet sich der Einsatz von Tripwire. Ist eine Unternehmung jedoch nur an einer Überwachung der Log-Dateien interessiert, so verfügt sie mit Swatch über eine geeignete Lösung.

8.3 Kommerzielle versus nicht-kommerzielle Audit-Tools

Bei der Auswahl eines Audit-Tools stellt sich für eine Unternehmung natürlich die Frage, ob sie ein frei verfügbares oder ein kommerzielles Produkt einsetzen soll. Von der Qualität und den Möglichkeiten, die viele frei verfügbare Produkte[238] bieten, sind diese einem kommerziellen Produkt sicherlich ebenbürtig. Im Gegensatz zu kommerziellen Produkten kann jedoch der Benutzer bei Programmfehlern den Autor nicht haftbar machen. Ausserdem ist der Autor nicht verpflichtet, dem Benutzer bei spezifischen Problemen irgendwelche Auskünfte zu erteilen.

Die Entwickler nicht-kommerzieller Tools stammen meistens aus dem universitären Umfeld. Sobald jedoch diese Programmautoren die Universität verlassen, schwindet auch der Support für diese Produkte. Da immer wieder neue Programme in Umlauf kommen, müssen diese von der Unternehmung zuerst einmal gefunden und evaluiert werden. Die Unternehmung sieht sich gezwungen, ständig nach neuen Programmen zu suchen und muss sich deshalb immer wieder mit anderen Programmautoren auseinandersetzen. Zudem variiert die Qualität der einzelnen nicht-kommerziellen Produkte relativ stark.

Bei kommerziellen Produkten werden in der Regel in regelmässigen Abständen Updates der Programme angeboten. Ausserdem übernimmt der Anbieter die Verantwortung für sein Programm und gewährleistet einen entsprechenden Support. Aufgrund ihres hohen Preises werden jedoch die kommerziellen Audit-Tools hauptsächlich von Unternehmungen eingesetzt.

Entscheidend für die Auswahl des geeigneten Audit-Tools ist jedoch nicht, ob es sich um ein kommerzielles oder ein nicht-kommerzielles Programm (vgl. Abbildung 28) handelt, sondern vielmehr ob das Programm den momentan vorhandenen Gefahren gewachsen ist. Zudem ist es für eine Unternehmung wichtig, dass sie im Sicherheitsbereich immer auf dem neusten Stand der Technik ist, denn nur so kann sie den Sicherheitsrisiken begegnen.

[238] oft auch “Public Domain Software” oder “Freeware” genannt

AUDIT-TOOLS	*kommerzielle*	*nicht-kommerzielle*
Kosten	hoch	gering
Funktionalität	umfangreich	eingeschränkt bis umfangreich
Dokumentation	selten ungenügend	vielfach schlecht
Support bei Fragen	gewährleistet	oft nicht gewährleistet
Updates	regelmässig	unregelmässig
Produktlebenszeit	lang	oft kurz
Haftung	beschränkt	keine

Abbildung 28: Kommerzielle versus nicht-kommerzielle Audit-Tools

8.4 Betriebssysteme

Die Zusammenstellung in Abbildung 29 zeigt, welche Betriebsysteme durch die verschiedenen Audit-Tools unterstützt werden. Es fällt dabei auf, dass mit Ausnahme von SAFEsuite alle untersuchten Audit-Tools nur das UNIX-Betriebssystem unterstützen. Dies ist damit begründet, dass UNIX lange Zeit das einzige Betriebssystem war, welches eine TCP/IP-Anbindung integriert hatte. Bis vor kurzem waren deshalb auch nur Server und Clients für UNIX erhältlich.

Betriebssystem / Audit-Tools	UNIX	Windows NT
Angriffssimulatoren		
SATAN	√	–
ISS (SAFEsuite)	√	√
Pingware	√	–
NetProbe	√	–
Programme zur Prüfung der Systemsicherheit		
COPS	√	–
TAMU-Tiger	√	–
Crack	√	–
CrackLib	√	–
Überwachungsprogramme		
IP-Watcher	√	–
TTY-Watcher	√	–
TCP-Wrapper	√	–
Tripwire	√	–
Gabriel	√	–
Argus	√	–
Swatch	√	–
NID	√	–

Abbildung 29: Unterstützte Betriebssysteme der Audit-Tools

9. Schlussfolgerungen und Ausblick

Den zahlreichen Chancen, die sich für eine Unternehmung durch den Anschluss an das Internet ergeben, stehen eine grosse Anzahl von Risiken gegenüber. Im Rahmen dieser Arbeit wurde deshalb untersucht, welchen Bedrohungen eine Unternehmung bei der Anbindung an das Internet gegenübersteht und welche Risiken sich daraus ergeben. Ferner wurde nach geeigneten Massnahmen gesucht, um diese Risiken zu reduzieren. Abschliessend wurden diejenigen Werkzeuge zusammengestellt und evaluiert, welche der Erkundung von Sicherheitslücken im Unternehmungssystem dienen.

Durch den Einsatz des Internet wird das Unternehmungsnetzwerk verschiedenen Bedrohungen ausgesetzt. Es handelt sich dabei um natürliche Bedrohungen (z.B. Brand), passive Angriffe (z.B. Verkehrsflussanalyse), aktive Angriffe (z.B. Hijacking) sowie zufällige Verfälschungsmöglichkeiten (z.B. Übertragungsfehler). Sobald diese Bedrohungen auf die Schwachstellen im Unternehmungssystem treffen, ergeben sich daraus Gefahren für die Unternehmung. Die momentan grösste Schwachstelle bildet das im Internet verwendete IP-Protokoll (IPv4), welches ein Abhören, Fehlleiten, Modifizieren und Fälschen von Datenpaketen zulässt. Da auch andere Protokolle und Anwendungen auf diesem unsicheren Protokoll aufbauen, tauchen die Sicherheitslücken des IP-Protokoll an diesen Stellen ebenfalls auf. Neben den technischen Schwachstellen (z.B. Kommunikationsprotokolle) sind jedoch die organisatorischen (z.B. Zugangsberechtigungsmanagement) und die menschlichen Schwachstellen (z.B. Naivität) nicht zu vernachlässigen.

Werden die negativen Auswirkungen der Gefahren bewertet, welche sich durch das Zusammentreffen von Bedrohungen und Schwachstellen ergeben, kann der Schaden ermittelt werden. Die Kombination von Schaden und der Schadenswahrscheinlichkeit ergibt schliesslich das Risiko. Um das Risiko möglichst gering zu halten, trifft die Unternehmung entsprechende Gegenmassnahmen (z.B. Schulung der Mitarbeiter). Dennoch bleibt auch nach Umsetzung aller Massnahmen ein gewisses Restrisiko bestehen, das von der Unternehmung selbst getragen werden muss.

Als personelle Massnahmen kommen Schulungen, Verbote sowie die Förderung des Sicherheitsbewusstseins in Frage. Die organisatorischen Massnahmen umfassen eine physikalische Trennung der Internetzugangsrechner vom Firmennetz, die Vergabe von aufgabenspezifischen Zugriffsrechten und die besondere Sicherung einzelner Rechner. Neben den personellen und organisatorischen Massnahmen sind jedoch die technischen Massnahmen am vielfältigsten. Um das Unternehmungsnetzwerk gegenüber dem Internet abzusichern, sind sogenannte Firewalls eine geeignete technische Lösung. Eine sichere Übertragung von Daten wird mit kryptographischen Massnahmen (z.B. Verschlüsselung) erreicht. Weitere technische Massnahmen finden sich in redundanten Einrichtungen, Virenschutzprogrammen und in der Protokollierung der Systemaktivitäten.

Um die Unternehmung bei der Erkennung von Sicherheitslücken zu unterstützen, bieten sich eine Reihe von Audit-Tools an. Diese lassen sich in Angriffssimulatoren (z.B. SATAN), Programme zur Prüfung der Systemsicherheit (z.B. Crack) und Überwachungsprogramme (IP-Watcher) einteilen. Diese Werkzeuge sind jedoch nur solange wirksam als sie sich auf dem neusten Stand der Technik befinden.

In naher Zukunft wird die Umstellung auf das neue IP-Protokoll (IPv6) erfolgen. Da dieses Protokoll auch Verschlüsselungstechniken unterstützt, ist eine sichere Übertragung von Daten möglich, sofern die kommunizierenden Systeme selber keine Sicherheitslücken aufweisen. Ein Grossteil der heute im Internet durch das IP-Protokoll verursachten Sicherheitsprobleme werden mit dem neuen IP-Protokoll gelöst. Da es jedoch einen längeren Zeitraum in Anspruch

nimmt, bis alle am Internet angeschlossenen Systeme das neue Protokoll unterstützen, müssen die Sicherheitslücken des momentan verwendeten IP-Protokolls weiterhin durch zusätzliche Sicherheitsmechanismen abgedeckt werden.

Ferner gilt zu beachten, dass eine hundertprozentige Sicherheit nie erreicht werden kann, da es nur eine Frage der Zeit ist, bis sogar ausgefeilte Sicherheitstechniken umgangen werden können. Angreifer entdecken durch ständiges Experimentieren immer wieder neue Sicherheitslücken und treiben so die Erfindung von immer neueren Sicherheitstechniken voran. Um das Risiko eines erfolgreichen Angriffes zu minimieren, ist es die Aufgabe der Unternehmung, sich stets über den aktuellsten Stand der Technik im Sicherheitsbereich sowie über potentielle Angriffsmöglichkeiten zu informieren.

10. Literaturverzeichnis

[Alpar 96] Alpar, P.: Kommerzielle Nutzung des Internet, Springer, Berlin, 1996.

[Bauknecht et. al. 96a] Bauknecht, K.; Tschudin, C.: Sicherheit in der Informationstechnik, Skript, Universität Zürich, Zürich, 1996.

[Bauknecht et. al. 96b] Bauknecht, K.; Teufel, St.; Gaugler, Th.: Informationssysteme, Skript, Universität Zürich, Zürich, 1996.

[Bellovin 97] Bellovin, St.M.: Probable Plaintext Cryptanalysis of the IP Security Protocols, in: Proceedings of the 1997 Symposium on Network and Distribute System Security, IEEE Computer Society Press, California, 1997, S. 52-59.

[Beutelspacher et. al. 95] Beutelspacher, A.; Schwenk, J.; Wolfenstetter, K.-D.: Moderne Verfahren der Kryptographie, Vieweg-Verlagsgesellschaft, Braunschweig / Wiesbaden, 1995.

[Borer 96] Borer, M.: Potentielle Bedrohungen und Schwachstellen für Unternehmungen am Internet, Diplomarbeit, Universität Zürich, Zürich, 1996.

[Calzo 97] Calzo, P.: Internet Banking, Semesterarbeit, Universität Zürich, Zürich, 1997.

[Cameron 97] Cameron, D.: Security Issues for the Internet and the World Wide Web, Computer Technologiy Research Corp., Revised Edition, Charleston, 1997.

[Cannady et. al. 96] Cannady, J.; Harrell, J.: A Comparative Analysis of Current Intrusion Detection Technologies, Fourth Technology for Information Security Conference'96 (TISC'96), Houston, 1996, http://iw.gtri.gatech.edu/Papers/ids_rev.html.

[Chapman et. al. 96] Chapman, D.B.; Zwicky, E.D.: Einrichten von Internet Firewalls, deutsche Übersetzung von Katja Karsunke & Thomas Merz, O'Reilly, International Thomson-Verlag, Bonn, 1996.

[Cheswick et. al. 95] Cheswick, W.R.; Bellovin, St.M.: Firewalls und Sicherheit im Internet, Addison-Wesley, Bonn, 1996.

[December et. al. 95] December, J.; Randall, N.: World Wide Web für Insider, Markt und Technik, Haar bei München, 1995.

[Eike 97] Eike, U.: Die Bombe tickt im Skript, in: Internet Professionell, Nr. 12, Ziff-Davis Verlag GmbH, 1997, S. 42-43.

[Ellermann 94] Ellermann, U.: Firewalls Klassifikation und Bewertung, in: Bauknecht, K.; Teufel, St. (Hrsg.): Sicherheit in Informationssystemen - Proceedings der Fachtagung SIS ‘94 Universität Zürich-Irchel, Institut für Informatik, Verlag der Fachvereine, Zürich, 1994, S. 121-139.

[Fehling et. al. 97] Fehling, Th.; Harnisch, B.: Firewalls, in: Computermarkt, Nr. 2, M+K Computer Verlag AG, 1997, S. 65-66.

[Griese et. al. 96] Griese, J. (Hrsg.); Sieber, P.: Internet - Nutzung für Unternehmungen, Verlag Paul Haupt, Bern, 1996.

[Haldimann et. al. 96] Haldimann, U. et. al.: netguide 2.0, in: Sonntags Zeitung, 30. März 1997.

[Heinrich 96] Heinrich, L.J.: Informationsmanagement: Planung. Überwachung und Steuerung der Informationsinfrastruktur, 5. Auflage, Oldenbourg, München, 1996.

[Heinzmann et. al. 97] Heinzmann, P.; Schoebi, P.: Am Puls des Bits, in: Prozess- und Informationssicherheit, Broschüre zur Informationstagung Sicherheit 97, Zürich, November 1997, S. 69-83.

[Himmelspach et. al. 96] Himmelspach, A.; Zimmermann, H-.D.: Elektronische Zahlungssysteme als kritischer Erfolgsfaktor des Electronic Commerce in offenen Telematikinfrastrukturen, in: INFORMATIK, Nr. 6, 1996, S. 18-25.

[Hoburg 96] Hoburg, C.: Der Schlüssel zur IT-Sicherheit, in: Der Monat, Nr. 6, 1996, S. 50-51.

[Holbein et. al. 96] Holbein, R.; Winzeler, St.: Verfahren zur Auswahl von zertifizierten IT-Systemen unter dem Aspekt der Wirtschaftlichkeit, in: Bauknecht, K.; Karagiannis, D.; Teufel, St. (Hrsg.): Sicherheit in Informationssystemen - Proceedings der Fachtagung SIS ‘96 Universität Wien, Institut für Angewandte Informatik und Informationssysteme, Verlag der Fachvereine, Zürich, 1996, S. 269-289.

[Holfelder 95] Holfelder, W.: Multimediale Kiosksysteme, Vieweg-Verlagsgesellschaft, Braunschweig, 1995.

[Holthaus et. al. 95] Holthaus, M; Teufel, St.: Ein Wegweiser zur IT-Sicherheit, in: INFORMATIK, Nr. 3, 1995, S. 23-27.

[Huber 96] Huber, W.: IP Spoofing Attacke und deren Abwehr, in: SWITCHjournal, Nr. 1, 1996, S. 11-13.

[Huber 97] Huber, M. O.: Internet und (Rechts-) Sicherheit, in: Computer Forum, Nr. 2, 1997, S. 6-7.

[Hughes 95] Hughes, L.: Actually Useful Internet Security Techniques, New Riders Publishing, Indianapolis, 1995.

[Imper 98] Impter, P.: Vorsicht: Feind im Netz, in: Bilanz, Nr. 1, 1998, S. 78-80.

[Käding 91] Käding, M.: Sicherheitsarchitektur für Verteilte Systeme, Dissertation, Technische Universität Berlin, Berlin, 1991.

[Kersten 91] Kersten, H.: Einführung in die Computersicherheit, Oldenbourg, München, 1991.

[Kimmins et. al. 95] Kimmins, J.; Dinkel, Ch.; Walters, D.: Telecommunications Security Guidelines for Telecommunications Management Network, U.S. Government Printing Office, Washington, October 1995.

[Kirsch 97] Kirsch, Ph.: Chancen und Risiken der Internetnutzung, in: K. Bauknecht, St. Teufel. Sichere Nutzung von Inter- und Intranet-Diensten. Fortbildungsseminar, Institut für Informatik, Universität Zürich, Zürich, März 1997.

[Kirsch et. al. 97a] Kirsch, Ph.; Weidner, H.: Online-Dienste im Internet - eine kombinierte Anforderungs- und Risikoanalyse, in: Proceedings VIS'97, Freiburg (Hrsg.), September 1997.

[Kirsch et. al. 97b] Kirsch, Ph.; Teufel, St.; Weidner, H.: Security in Usage of Online Services, in: 2nd International Small System Security Conference, Copenhagen, May 1997.

[Klau 95] Klau, P.: Das Internet, IWT-Verlag, Bonn, 1995.

[Kleiner 97] Kleiner, M.: Die Angst vor Online-Gangstern, in: OUTPUT, Nr. 11, Fachpresse Verlag, Zürich, 1997, S. 46-48.

[Koch 97] Koch, M.: Grundkurs Internet, 2. überarbeitete Auflage, Beluga Verlag, Wettingen, 1997.

[Köhntopp 97] Köhntopp, F.: Sichere Zahlungen im Internet, in: Tagungsdokumentation, Marktplatz Internet: Von der Präsenz zum Business - a practical approach, Schweizerische Vereinigung für Datenverarbeitung, Zürich, 14. Januar 1997.

[Krallmann 89] Krallmann, H.: EDV-Sicherheitsmanagement - Integrierte Sicherheitskonzepte für betriebliche Informations- und Kommunikationssysteme, Schmidt Verlag, Berlin, 1989.

[Kuhm 96] Kuhm, V.: Electronic Commerce, in: IBM Businesspower, Herbst 1996, S. 28-32.

[Kyas 96a] Kyas, O.: Sicherheit im Internet, Datacom, Bergheim, 1996.

[Kyas 96b] Kyas, O.: Internet professionell, Thomson Publishing, Bonn, 1996.

[Lampe 96] Lampe, F.: Business im Internet, Vieweg-Verlagsgesellschaft, Braunschweig, 1996.

[Lamprecht 96] Lamprecht, St.: Marketing im Internet, Haufe, Freiburg, 1996.

[Latanzio 96] Latanzio, B.: Sicherheitsanforderungen und Lösungspotentiale für die Realisierung elektronischer Märkte, Diplomarbeit, Universität Zürich, Zürich, 1996.

[Luckhardt 97] Luckhardt, N.: Surfer's Hai Security, in: c't magazin für computer technik, Nr. 13, Verlag Heinz Heise GmbH, 1997, S. 166-174.

[Luthiger 96] Luthiger, J.: UNIX Vertiefungskurs, ETH Informatikdienste, 1996.

[Macgregor et. al. 96] Macgregor, R.; Setton, A.; Ueno, K.; Curtiss, J.: Building a Firewall with the IBM Internet Connection Secured Network Gateway, IBM, New York, 1996.

[Marine et. al. 96] Marine, A. et. al.: Internet: Getting Started, Englewood Cliffs, New Jersey, 1993.

[Maurer 95] Maurer, U.; Cachin, Ch.: Sicherheit im Internet: Illusion oder Realität?, in: INFORMATIK, Nr. 2, 1995, S. 18-23.

[Maurer 97] Maurer, Ph.: Das Internet als Marketinginstrument, Semesterarbeit, Universität Zürich, Zürich, 1997.

[Meli-Isch 95] Meli-Isch, H.: Sicherheitsmanagement in offenen Kommunikationssystemen - Sicherheitsarchitektur für eine Electronic Mall, Dissertation, Hochschule St. Gallen, 1995.

[Merz 96] Merz, M.: Elektronische Märkte im Internet, International Thomson Publishing, Bonn, 1996.

[Müller-Späth 97] Müller-Späth, M.: Sicherheitsrisiko E-Mail, in: Internet Professionell, Nr. 12, Ziff-Davis Verlag GmbH, 1997, S. 38-41.

[NZZ 97] Epressung im Internet, in: Neue Zürcher Zeitung, 11. Dezember 1997, S. 20.

[Oenicke 96] Oenicke, J.: Online-Marketing: kommerzielle Kommunikation im interaktiven Zeitalter, Schäffer-Poeschel, Stuttgart, 1996.

[Pabrai et. al. 96] Pabrai, U. O.; Gurbani, V. K.: Internet and TCP/IP Network Security, McGraw-Hill Book Company, New York, 1996.

[Panzer 88] Panzer, Th.E.: EDV-Sicherheit, Verlag Industrielle Organisation, Zürich, 1988.

[Perrochon 95] Perrochon, L.: World Wide Web: Konzepte und Grundlagen, in: INFORMATIK, Nr. 2, 1995, S. 3-7.

[Pilz 97] Pilz, M.: Das Sicherheitskonzept von Java, in: INFORMATIK, Nr. 3, 1997, S. 17-22.

[Piveteau et. al. 94] Piveteau, J.-M.; Riess, H.P.: Eine generische Sicherheitsarchitektur für Telekommunikationsnetze, in: Bauknecht, K.; Teufel, St. (Hrsg.): Sicherheit in Informationssystemen - Proceedings der Fachtagung SIS '94 Universität Zürich-Irchel, Institut für Informatik, Verlag der Fachvereine, Zürich, 1994.

[Pohl 93] Pohl, H.: Einführung in die Informationssicherheit, Oldenbourg, München, 1993.

[Pohlmann 97] Pohlmann, N.: Firewall-Systeme, International Thomson Publishing, 1. Auflage, Bonn, 1997.

[Resch 96] Resch, J.: Marktplatz Internet, Microsoft Press, Unterschleissheim, 1996.

[Rohner 96] Rohner, K.: Internet, Intranet und Extranet - Instrumente für Management und Unternehmen, in: io Management 65 (1996), Nr. 12, S. 63- 66.

[Schaub et. al. 97] Schaub, B; Sennhauser, M: Internet von A-Z, Hallwag AG, 1. Auflage, Bern, 1997.

[Schaumüller-Bichl 92] Schaumüller-Bichl, I.: Sicherheitsmanagement - Risikobewältigung in informationstechnologischen Systemen, BI Wissenschaftsverlag, Mannheim, 1992.

[Scherer 96] Scherer, J.: Wenn die Zukunft zur Gegenwart wird, in: NewsServer, Ausgabe 3, 1996, S. 30-32.

[Schmitt 96] Schmitt, P.-A.: Total vernetzt, in: FACTS, Nr. 34, 1996, S. 40-45.

[Schneier 96] Schneier, B.: Angewandte Kryptographie, Addison-Wesley, Bonn, 1996.

[Siyan et. al. 95] Siyan, K.; Hare, C.: Internet Firewalls und Netzwerksicherheit, SAMS, Haar bei München, 1995.

[Somm 97] Somm, M.: Betreut depressiven Ehemann, in: Tages-Anzeiger, 1. Oktober 1997, S. 11.

[Stallings 95] Stallings, W.: Internet Security Handbook, McGraw-Hill Book Company, London, 1995.

[Stallings 95a] Stallings, W.: Network and Internetwork Security: Principles and practice, Englewood Cliffs, New Jersey, 1995.

[Stelzer 93] Stelzer, D.: Sicherheitsstrategien in der Informationsverarbeitung, Deutscher Universitäts-Verlag, Wiesbaden, 1993.

[Stevens 95] Stevens, W.R.: TCP/IP Illustrated, Addison-Wesley, Vol. 1, Massachusetts, 1995.

[Tanenbaum 97] Tanenbaum, A. S.: Computernetzwerke, 3. Auflage, Prentice Hall, München, 1997.

[Waldburger 98] Waldburger, D.: Internet: Die besten Tricks gegen Schnüffler, in: Sonntags Zeitung, 11. Januar 1998, S. 75.

[Weidner 97] Weidner, H.: Sicherheit im Internet: Stand der Technik, Institutsbericht, Institut für Informatik, Universität Zürich, Zürich, 1997.

[White et. al. 96] White, G.B.; Fisch, E.A.; Pooch, U.W.: Computer System and Network Security, CRC Press, Boca Raton, New York, London, Tokyo, 1996.

[Wildhaber 93] Wildhaber, B.: Informationssicherheit - Rechtliche Grundlagen und Anforderungen an die Praxis. Schulthess Polygraphischer Verlag, Zürich, 1993.

[Wojcicki 91] Wojcicki, M: Sichere Netze: Analysen, Massnahmen, Koordination, Hanser Verlag, München, 1991.

[Zimmermann 96] Zimmermann, R.: Selbstorganisation im Internet, Diplomarbeit, Universität Zürich, 1996.