

Universität Leipzig
Fakultät für Mathematik und Informatik
Institut für Informatik

Versicherbarkeit von Internetrisiken

Das Bedrohungspotenzial von Netzwerken
durch widerrechtliche Handlungsweisen

Diplomarbeit

vorgelegt von: Daniel Paul
Betreuer: Prof. Dr. Gottfried Koch

Leipzig, August 2002

Inhaltsverzeichnis

1	Einführung.....	1
2	Übersicht und Klassifizierung von Netzwerken.....	3
2.1	Aufgaben, Ziele und Funktionen von Netzwerken	4
2.2	Arten von Netzwerken.....	7
2.2.1	Physische Klassifikation von Netzwerken	9
2.2.1.1	Local Area Network (LAN)	9
2.2.1.2	Wide Area Network (WAN)	11
2.2.1.3	Drahtlose Netze	11
2.2.2	Logische Klassifikation von Netzwerken	12
2.2.2.1	Internet	12
2.2.2.2	Intranet und Extranet.....	13
2.2.2.3	Virtual Private Network (VPN).....	14
2.3	Protokollhierarchien in Netzwerken.....	15
2.3.1	Grundlagen von Netzwerkprotokollen	15
2.3.2	Das OSI-Referenzmodell	17
2.3.3	Das TCP/IP-Referenzmodell.....	18
2.3.4	Anwendungsbereiche von verschiedenen Protokollen.....	21
2.4	Strukturierung von Netzwerken	22
2.4.1	Technische Sicht	23
2.4.2	Logische Sicht	24
2.5	Management von Netzwerken.....	24
3	Sicherheitsrisiken in Netzwerken.....	26
3.1	Risikovergleich vernetzter und alleinstehender Systeme.....	26
3.2	Allgemeine Definition von Computer- und Netzwerkkriminalität	29
3.3	Ausprägungen von Computer- und Netzwerkkriminalität	30
3.4	Motivation für Computer- und Netzwerkkriminalität	32
3.4.1	Grundlegende Intention eines computerkriminalistischen Angriffs	32
3.4.2	Auswahl eines geeigneten Angriffszieles	34
3.4.3	Hacker und Cracker.....	35

3.4.4	„Skriptkiddies“	36
3.5	Spezielle Formen von Computer- und Netzwerkkriminalität	37
3.5.1	Malware.....	37
3.5.1.1	Viren und Würmer	37
3.5.1.2	Trojanische Pferde.....	39
3.5.2	„Spoofing“	41
3.5.3	DoS-Attacken	43
3.5.4	Interne Attacken	46
3.5.5	„Social Engineering“	46
3.6	Authentifizierung und Autorisierung	47
3.6.1	Passwortgestützte Mechanismen.....	47
3.6.2	Key Exchange – Verfahren	50
3.6.3	Zugriffskontrolle (Autorisierung) in vernetzten Systemen	50
3.7	Risiken durch installierte Software	51
3.7.1	SANS-Liste	53
3.7.2	Serverseitige Dienste.....	53
3.7.2.1	Telnet und Secure Shell (SSH).....	54
3.7.2.2	File Transfer Protocol (FTP).....	55
3.7.2.3	Simple Mail Transfer Protocol (SMTP).....	56
3.7.2.4	Domain Name Service (DNS).....	57
3.7.2.5	Simple Network Management Protocol (SNMP).....	58
3.7.2.6	HyperText Transfer Protocol (HTTP).....	59
3.7.3	Clientseitige Applikationen.....	59
3.7.3.1	Browsertechnologien, Skriptsprachen.....	60
3.7.3.2	Java-Applets	61
3.8	Risiken bei der Datenübertragung im Netzwerk	61
3.8.1	Netzwerk-Sniffer	62
3.8.2	Datenübertragung im Internet	63
3.9	Betriebssystemspezifische Risiken.....	63
3.9.1	Microsoft Windows.....	64
3.9.2	UNIX-basierte Systeme.....	65
3.10	Hardwarespezifische Risiken	69
3.11	Interne Sicherheit	69

4	Schutzmechanismen für vernetzte Systeme	72
4.1	Grundlegende Risikoanalyse	72
4.2	Bedeutung eines Schadenfalls für das Unternehmen	73
4.3	Systemmanagement als Sicherheitsgrundlage.....	73
4.4	Einsatz sicherheitsrelevanter Technologien	74
4.4.1	Schwachstellen-Scanner	74
4.4.2	Firewall-Systeme.....	75
4.4.3	Verschlüsselungsmechanismen	77
4.5	Überwachung von kritischen Systemen	80
4.6	Fortbildung und Schulung der Mitarbeiter	81
5	Versicherbarkeit von Internetrisiken	83
5.1	Juristische Grundlagen	83
5.2	Aktuelle Gefahrenpotenziale	84
5.3	Generelle Betrachtung des Versicherbarkeitsbegriffs	85
5.3.1	Kriterien aus Sicht des Versicherers	85
5.3.2	Kriterien aus Sicht des Versicherungsnehmers	87
5.4	Grundlegende Versicherbarkeit von Internetrisiken	87
5.4.1	Einschätzung der Risikosituation im Unternehmen	88
5.4.1.1	Risk-Management im Unternehmen	88
5.4.1.2	Konkrete Einschätzung eines zu versichernden Risikos	89
5.4.2	Versicherungstechnische Analyse der IT-Sicherheit im Unternehmen	91
5.5	Abdeckung durch traditionelle Herangehensweisen	91
5.5.1	Traditionelle Haftpflichtdeckungen	91
5.5.2	Vertrauensschaden-Versicherung.....	92
5.5.3	Problematik bestehender Versicherungsprodukte	93
5.5.4	Problematik der Kumulbetrachtung	94
5.6	Alternative Versicherungskonzepte	95
5.7	Neue Versicherungsprodukte	95
5.7.1	ACE – „Data Guard“	96
5.7.1.1	Deckungsbausteine des Versicherungsproduktes.....	96
5.7.1.2	Vorgehensweise bei der Zeichnung des Produktes	97
5.7.1.3	Obliegenheiten des Versicherungsnehmers und explizite Ausschlüsse	98
5.7.2	Chubb – „CyberSecurity for Financial Institutions“	99

5.7.2.1	Deckungsbausteine des Versicherungsproduktes.....	99
5.7.2.2	Vorgehensweise bei der Zeichnung des Versicherungsproduktes	101
5.7.2.3	Obliegenheiten des Versicherungsnehmers und explizite Ausschlüsse.....	102
5.7.3	Bewertung der vorgestellten neuen Versicherungsprodukte.....	102
6	Zusammenfassung und Fazit.....	104
	Anhang A – Literaturverzeichnis	vi
	Anhang B – Verzeichnis der Abbildungen und Tabellen.....	xi
	Anhang C – Glossar zu Internetrisiken	xii
	Erklärung.....	xxi

1 Einführung

Das Internet und die mit ihm verbundenen lokalen Unternehmensnetzwerke spielen in der heutigen Zeit eine zentrale Rolle für den globalen Datenaustausch und die tägliche Beschaffung von wichtigen Informationen. Fast jedes Unternehmen – unabhängig von Größe und Strukturierung – nutzt das Internet, um über einen Webauftritt sich und seine Produkte dem Kunden vorzustellen. Ein hoher Prozentsatz betreibt über diesen Distributionskanal auch den Verkauf von Artikeln und die Bereitstellung von Unterstützungsleistungen. In den meisten Firmen genießen die Mitarbeiter einen freien Internetzugang, der sie bei der weltweiten Informationsbeschaffung zur Bewältigung der täglich anfallenden Aufgaben unterstützt. Die Koordination von Mitarbeitern und Kapazitäten im Unternehmen wird durch den Versand von elektronischer Post (e-Mail) sowie durch Diskussionen in themenbezogenen Foren (Newsgroups) wesentlich unterstützt.

Doch das Internet mit seinem unbeschränkten und unkontrollierbaren Charakter bringt auch erhebliche Sicherheitsrisiken für Unternehmen mit sich. Einer Studie von Price Waterhouse Coopers über neu eingerichtete Webauftritte im Internet zufolge werden diese nach durchschnittlich 28 Sekunden erstmals aufgerufen und bereits nach fünf Stunden zum ersten Mal Opfer eines versuchten Angriffs. In 60 Prozent aller bestehenden Netzwerke wird pro Jahr mehr als 30 Mal versucht einzudringen. Eine entsprechende Absicherung, sowohl technischer als auch versicherungswirtschaftlicher Natur, ist hier dringend erforderlich.

Die vorliegende Arbeit hat zum Ziel, diese oftmals unterschätzten Risiken und das durch sie entstehende Gefährdungspotenzial aufzuzeigen. Dabei können in dieser Arbeit nicht alle existierenden Risikoarten in der Informationstechnologie betrachtet werden, vielmehr wird eine Fokussierung auf alle diejenigen Arten vorgenommen, die durch die sogenannte „widerrechtliche Nutzung“ von Netzwerk-Infrastrukturen charakterisiert sind. Häufig werden die so abgegrenzten Gefahren auch mit dem Begriff „Internetrisiken“ umschrieben. Die Fokussierung dieser Arbeit soll dabei weder auf eine minimale Verbreitung noch auf ein geringfügiges Gefährdungspotenzial der ausgenommenen Risiken schließen lassen, vielmehr würde eine Gesamtdarstellung eine nur oberflächliche Betrachtung nach sich ziehen. Daher werden Risiken wie Stromausfälle allgemein sowie Netzwerkstörungen durch Naturkatastrophen (Sturm, Erdbeben), Wasserschäden, Kurzschluss oder Überspannung nicht in dieser Arbeit betrachtet, obwohl sie durchaus Relevanz für die Funktionsweise von Netzwerk-Infrastrukturen besitzen. In dieser Arbeit soll ein Abriss der bisherigen Bemühungen um die Versicherbarkeit derartiger Risiken versucht werden, wobei eine methodische Vorgehensweise beginnend mit der

Erklärung der grundlegenden Begriffe der Thematik sinnvoll erscheint. Hierzu wird zunächst eine Einführung in bestehende Netzwerke gegeben (Kapitel 2), bevor die vorherrschenden Risiken (Kapitel 3) und darauf aufbauende Maßnahmen zum Schutz (Kapitel 4) vorgestellt werden. In Kapitel 5 werden die mit der Versicherbarkeit von Internetrisiken verbundenen Probleme hinsichtlich fehlender Quantifizierbarkeit durch eine ungenügende Datenlage erläutert. Es wird auf bestehende Versicherungslösungen eingegangen, ebenso werden neue Produkte und die damit verbundenen Sicherheitsanforderungen für Unternehmen vorgestellt.

Die dabei in dieser Arbeit betrachteten sicherheitsrelevanten Probleme und Risiken sind keinesfalls als vollständige und ausschließliche Auflistung zu betrachten, es handelt sich vielmehr um die Gefahren, denen Unternehmen bei einer durchaus normalen bzw. durchschnittlichen Nutzung des Internets sowie einer daran angeschlossenen internen Netzinfrastruktur alltäglich ausgesetzt sind – wissentlich und unwissentlich.

2 Übersicht und Klassifizierung von Netzwerken

Zunächst ist eine Einführung in die verschiedenen Arten von Netzwerken und deren Klassifizierung nach bestimmten Gesichtspunkten zwingend angebracht, da unterschiedliche Strukturen von Netzwerken ebenso unterschiedliche Gefährdungspotenziale besitzen. Dies betrifft auch die von ihnen ausgehenden Formen der Bedrohung bei einer widerrechtlichen Nutzung. Für die Erstellung einer ersten Übersicht über Netzwerke im Allgemeinen ist zunächst die Begriffsklärung des Wortes „Netzwerk“ notwendig, wobei man hierbei zwei Sichten einnehmen kann: eine übergeordnete Allgemeinsicht sowie eine technisch geprägte Untersicht. Daneben existieren noch Definitionen für Netzwerke aus anderen Bereichen, so u.a. für den Begriff des unternehmerischen oder auch des neuronalen Netzwerkes¹. Da für die allgemeine Sichtweise keine eindeutige Definition des Begriffes Netzwerk existiert, soll dieser zunächst aus der technologischen Sicht heraus definiert und danach der Versuch einer Abstrahierung auf die Allgemeinebene unternommen werden.

In der Informationstechnologie bezeichnet der Begriff (Computer-) Netzwerk gemeinhin eine bestimmte Menge von autonomen, miteinander verbundenen Computern, wobei zwei Computer als miteinander verbunden gelten, wenn sie in der Lage sind, untereinander Informationen auszutauschen². Hier spielt es keine Rolle, welcher Art die Verbindung zwischen den Computern ist, Beispiele hierfür sind Kupfer- oder Glasfaserkabel, aber auch Funkwellen können für die Kommunikation genutzt werden. In der Literatur besonders hervorgehoben wird dabei der Begriff der autonomen Computer, d.h. des Ausschlusses von Konstrukten mit einer klaren Master/Slave-Relation. Diese Abgrenzung schließt Systeme aus, bei denen ein Rechner einen anderen beliebig ein- und ausschalten oder steuern kann. Sehr wohl als Computernetze gelten dagegen Konstrukte, bei denen von ihrer Funktionalität her ein Verhältnis wie Client und Server besteht³.

Eine verallgemeinerte Definition des Begriffes Netzwerk lässt sich ableiten als eine bestimmte Menge von wohldefinierten Punkten oder Knoten, die durch bestimmte Wege miteinander verbunden sind. Dabei können Netzwerke wiederum mit anderen übergeordneten oder gleichrangigen Netzen verbunden sein und auch selbst untergeordnete Netzwerke enthalten⁴.

In dieser Arbeit soll der Term Netzwerk, sofern nicht anders vermerkt, im Sinne der Definition eines Computernetzwerks gebraucht werden, dies schließt auch die heute gebräuchlichen

¹ Vgl. dazu [VentureNet 2002], [Aventis 2001]

² Vgl. dazu [Tanenbaum 2000], S. 18

³ Vgl. Definition [Techtarget 2002 Client/Server]

⁴ Vgl. Definition [Techtarget 2002 Network]

Workstation/Server-Konstellationen mit ein. Es werden nur Netzwerke zwischen verschiedenen Computern betrachtet, nicht jedoch Strukturen innerhalb verteilter Systeme⁵, da es sich hier nicht um autonome Teilnehmer innerhalb einer gegebenen Netzstruktur handelt, sondern um ein virtuelles Einprozessorsystem, wobei für den Nutzer die Verteilung der Systemressourcen auf bestehende Aufträge vollständig transparent ist. Dieser Fall kann vollständig herausgelassen werden, weil der Sicherheitsaspekt im herkömmlichen Sinne – d.h. eine vom Nutzer geforderte Absicherung anhand der in den folgenden Kapiteln erläuterten Gesichtspunkte – nicht relevant ist.

2.1 Aufgaben, Ziele und Funktionen von Netzwerken

In diesem Abschnitt sollen zunächst die Ziele bei der Entwicklung von Netzwerkstrukturen erläutert werden, die grundlegend mit den ihnen übertragenen Aufgaben und Funktionalitäten korrespondieren.

Das Hauptziel bei der Planung und beim Aufbau von Netzwerken war vor allem die Möglichkeit der gemeinsamen Nutzung von Ressourcen der beteiligten Computer und des gegenseitigen Datenaustauschs, der bis dahin nur manuell über Datenträger erfolgte. Ein weiteres Ziel war die Erhöhung der Verfügbarkeit von Daten und anderen Ressourcen durch mehrere alternative Standorte im Netzwerk. Innerhalb des Netzwerks konnten auch kleinere Computer eingesetzt werden, die trotzdem durch ihr Zusammenwirken annähernd die gleiche Leistung erbrachten wie ein einzelner Großrechner. Da letztere auch ein erheblich schlechteres Preis-Leistungs-Verhältnis aufwiesen, war eine Einsparung von Geldmitteln ebenfalls ein Ziel des Aufbaus von Netzwerkstrukturen. In vielen Netzwerken steht daher jedem Benutzer ein vergleichsweise billiger Personalcomputer (PC-Client) zur Verfügung, während die Daten zentral auf Dateiservern verwaltet werden. Die folgende Abbildung 2.1 zeigt das Verhältnis von Client- und Server-Rechner bei einer Anfrage über das Netzwerk.

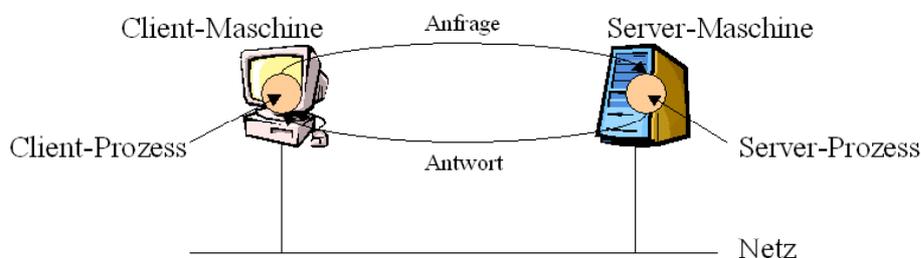


Abbildung 2.1 - Client/Server-Modell

Quelle: Vgl. [Tanenbaum 2000], S. 20

⁵ Vgl. dazu [Tanenbaum 2000], S. 853

Einen weiteren Nutzenzuwachs brachte der Zusammenschluss von kleineren Netzen (z.B. Abteilungsnetzwerken) zu übergeordneten Strukturen. Auch bei der mit der Zeit ansteigenden Arbeitslast konnten vernetzte Systeme besser den veränderten Bedingungen angepasst werden: durch die Verwendung des Client-/Server-Modells konnten in solch einer Situation einfach zusätzliche Clients oder Server dem bestehenden Netzwerk hinzugefügt werden. Bei einem Großrechner dagegen wäre eine komplette Ersetzung desselben durch eine leistungsfähigere Variante, verbunden mit einem erheblichen finanziellen Aufwand und einer – wahrscheinlich noch gravierenderen – Betriebsunterbrechung, die Folge gewesen⁶.

Heutzutage haben Netzwerke vielfältige Aufgaben zu erfüllen, im Vordergrund steht jedoch eindeutig das Übertragen von Informationen aller Art, wobei das Wort Information hierbei sowohl für Daten als auch für Sprache, Videosequenzen, Programme, Metadaten u.a. stehen kann. So gestatten es Netzwerke zwei oder mehr räumlich voneinander getrennten Personen, ein beliebiges Dokument gemeinsam zu verfassen. Die von einer Person durchgeführten Änderungen an dem Dokument sind für die anderen Beteiligten sofort sichtbar. Auch das Grundprinzip, warum häufig Netzwerke beim Zugriff auf weiter entfernte Computer eingesetzt werden, ist klar: Es ist billiger, eine Verbindung zu einem anderen Computer über ein Netzwerk herzustellen, als diesen direkt anzusprechen⁷. Diesem Prinzip folgen auch die Topologien von Netzwerken wie dem heutigen Internet bzw. darauf aufbauenden Applikationen (z.B. dem World Wide Web⁸). Der vermeintlich direkte Zugriff des Internet-Browsers eines Client-Computers auf den angesprochenen Web-Server läuft in der Realität über viele Netzwerkknoten innerhalb des Internets ab. Somit sind alle Computer im Internet lediglich virtuell direkt miteinander vernetzt.

In der Arbeit wird häufig auf den Begriff des ARPANET eingegangen werden, eine Schöpfung im Auftrag der Advanced Research Projects Agency (ARPA) des Verteidigungsministeriums der USA. Diese hatte bereits in den späten 60er Jahren in vielen Universitäten der USA die Forschung auf dem Gebiet der Netzwerke vorangetrieben. Erklärtes Ziel war dabei der Aufbau eines experimentellen Netzwerks zur Kommunikation von Wissenschaftlern mit entfernten Computerressourcen. Dieses Netz sollte so robust beschaffen sein, dass es selbst einen Atomkrieg überleben könne, daher sollte jeder Knoten des Netzwerks mit mindestens zwei weiteren Knoten verbunden sein. Nachrichten sollten automatisch über Ausweichpfade geführt werden, falls einige Leitungen oder Knoten zerstört wären. Im Dezember 1969 wurde ein experimentelles Teilnetz mit Knoten an vier Universitäten der USA in Betrieb genommen.

⁶ Vgl. dazu [Tanenbaum 2000], S. 19 f.

⁷ Vgl. dazu [Tanenbaum 2000], S. 20

⁸ Vgl. dazu Definition [Techtarget 2002 WWW]

Das ursprüngliche Design sah den Anschluss von Großrechnern (Hosts) an einen Vermittlungspunkt (Interface Message Processor, IMP) vor, wobei die verbundenen IMPs das eigentliche ARPANET darstellten. Abbildung 2.2 zeigt eine schematische Darstellung des damaligen Designs.

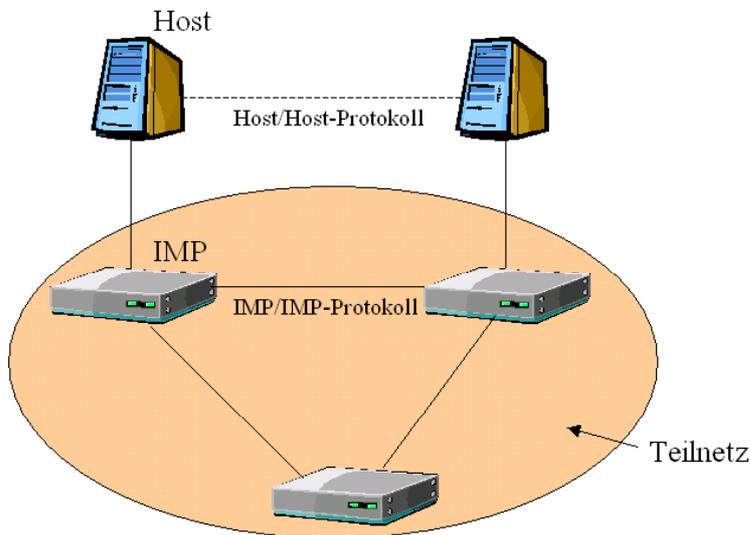


Abbildung 2.2 - das ursprüngliche ARPANET Design

Quelle: Vgl. [Tanenbaum 2000], S. 66

An die mit dem ARPANET verbundenen Hosts wurden schließlich die Terminals angebunden, um eine Interaktion der Benutzer über das Netzwerk zu ermöglichen. Spätere Änderungen des Designs betrafen die Möglichkeit, mehrere Hosts pro IMP anzuschließen (Einsparung von Geldmitteln) sowie aus Gründen der Ausfallsicherheit einen Host mit mehreren IMPs zu verbinden.

Ein Experiment in den 70er Jahren, in Folge dessen auch mobile paketvermittelte Netze, z.B. über Satelliten, an das ARPANET angeschlossen werden sollten, zeigte schnell auf, dass die genutzten Protokolle nicht für den Betrieb über mehrere Netze geeignet waren. Dies führte zu protokollrelevanten Forschungstätigkeiten, die schließlich 1974 in der Entwicklung des Protokolls TCP/IP mündeten⁹. Wissenschaftler der Universität Berkeley integrierten das Protokoll in ihr Netzwerkbetriebssystem UNIX¹⁰ und entwickelten eine Programmschnittstelle zur Netzwerkprogrammierung sowie Hilfs- und Verwaltungsprogramme, um die Vernetzungsaufgabe von bestehenden ersten Universitätsnetzwerken mit dem ARPANET zu vereinfachen. Diese Umstände trugen maßgeblich zum späteren Erfolg von TCP/IP bei.

⁹ Die Abkürzung TCP/IP steht für die im Internet wichtigste Protokollfamilie Transmission Control Protocol / Internet Protocol und wird in einem späteren Kapitel noch näher besprochen.

¹⁰ Das Netzwerkbetriebssystem UNIX wurde bereits Mitte der 70er Jahre entwickelt und existiert inzwischen in vielen, kostenfreien und kommerziellen Versionen, vgl. dazu auch [Berkeley 2002]

Im Jahre 1983 – das ARPANET umfasste mehr als 200 IMPs mit Hunderten von angeschlossenen Hosts – wurde der militärische Teil des Netzes abgetrennt und in ein eigenes gesichertes Netzwerk, das MILNET, überführt. Außerdem wurde mit dem NSFNET der National Science Foundation ein weiteres wissenschaftliches Fernnetzwerk mit Zugang zum ARPANET geschaffen, welches inzwischen mehrmals aufgerüstet wurde und mittlerweile von verschiedenen kommerziellen Anbietern betrieben wird. In anderen Ländern der Erde wurden ähnliche Netzwerke geschaffen, in Europa z.B. das EBONE und das EuropaNET. In Deutschland bildet das Deutsche Forschungsnetz (DFN) das Rückgrat für den Netzverkehr.

Das ARPANET selbst existierte noch bis in das Jahr 1990, als es schließlich von neueren und leistungsfähigeren Netzen überholt und damit überflüssig wurde. Obwohl das ARPANET in seiner damaligen Form nicht mehr existiert, bildet es doch die zumindest „ideelle“ Basis für das heutige Internet sowie dessen wissenschaftliche Grundlage – das heutige Wissen über Netzwerke resultiert zumeist direkt aus diesem Projekt¹¹.

2.2 Arten von Netzwerken

In diesem Abschnitt soll auf die einzelnen Arten von Netzwerken eingegangen werden. Eine Charakterisierung kann anhand verschiedenster Gesichtspunkte wie Größe, Ausbreitung oder Zugänglichkeit, aber auch anhand logischer Funktionalität oder der zugrunde liegenden technischen Merkmale erfolgen. Die wichtigsten Charakterisierungskriterien sind in der untenstehenden Tabelle 2.1 aufgeführt.

Tabelle 2.1 - Merkmale zur Charakterisierung von Netzwerken

Quelle: eigene Darstellung

Charakterisierendes Merkmal	Beispiele
Datenübertragungstechnologie	TCP/IP, Systems Network Architecture (SNA) u.a.
Übertragene Signale	Daten, Sprache oder beides
Zugänglichkeit	öffentlich, beschränkt oder privat
Art der Verbindungen	Punkt-zu-Punkt (exklusiv), permanent, temporär, bei Anruf (Dial-Up)
Verbindungstechnologie	kabelgebunden (Kupfer, Glasfaser) oder kabellos (z.B. Radiowellen, Funkwellen / Bluetooth)

¹¹ Vgl. dazu [Tanenbaum 2000], S. 65 ff.

Dieses Wissen ist für die spätere Analyse und den Aufbau eines Netzwerkes von essentieller Bedeutung, da dieses nicht nur sicherheitstechnisch richtig geplant, sondern vor allem technisch machbar sein muss¹².

Ein Netzwerk besitzt grundlegend die folgende Struktur: mehrere Computer – die zum Zweck die Ausführung von Nutzerapplikationen haben – sind innerhalb eines Kommunikationssubnetzes miteinander verbunden. Das Subnetz hat die Aufgabe, Nachrichten zwischen den Computern zu transportieren, wobei ein solches Netz wiederum aus Übertragungsleitungen und Verbindungselementen besteht. Diese – in der originalen ARPANET Terminologie als Interface Message Processors (IMP) bezeichneten – Verbindungselemente sind spezialisierte Computer, welche zwei oder mehrere verschiedene Übertragungsleitungen miteinander verknüpfen. Einem solchen Subnetz können zwei Designtypen zugrunde liegen: Point-to-Point- oder Broadcast-Channels. Ersteres Modell basiert darauf, dass ein Netzwerk eine gewisse Anzahl von Übertragungskanälen enthält, die die Knoten des Netzes (IMPs) miteinander verbinden. Wenn zwei IMPs nicht miteinander verbunden sind, aber trotzdem Informationen austauschen wollen, so kann dieser Austausch nur indirekt über andere Knoten des Netzes erfolgen. Da ein Paket meist über verschiedene Routen gesendet werden kann, spielt bei diesem Modell die Wahl des Übertragungsweges anhand verschiedenster Kriterien eine wichtige Rolle. Netzwerke, die dieses Modell benutzen, haben z.B. eine Stern-Topologie.

Das zweite Modell beruht auf einer simpleren Methode – hierbei wird der IMP auf einen einzigen Chip innerhalb des Computers selbst reduziert. Nach diesem Prinzip arbeitende Netzwerke haben einen gemeinsamen Übertragungskanal, der von allen Computern innerhalb des Subnetzes abgehört wird. Je nachdem, ob ein Datenpaket für einen Computer bestimmt ist oder nicht, wird es von diesem angenommen und ausgewertet oder einfach ignoriert. Die hierbei zugrunde liegenden Topologien sind z.B. die Bus- oder Token-Ring-Topologie.

Vereinfacht kann man die Regel aufstellen, dass kleinere bzw. geographisch enger zusammenliegende Netzwerke die Broadcasting- und weiter gestreute Netze die Punkt-zu-Punkt-Technologie verwenden¹³.

Viele lokale Netzwerke werden heutzutage als Zusammenschluss der einzelnen Teilnehmer über einen zentralen Netzwerkknoten, einen sogenannten Hub, ausgeführt. Obwohl hier die Stern-Topologie zum Einsatz kommt, werden Datenpakete nicht auf einer Punkt-zu-Punkt Verbindung zwischen den betreffenden Computern gesendet, sondern gehen als Broadcast an alle angeschlossenen Rechner, daher ist der Hub nicht als IMP bzw. aktives Gerät im Netz-

¹² Vgl. dazu [Hunt 1995], S. 21 ff.

¹³ Vgl. dazu [Tanenbaum 2000], S. 24 f.

werk anzusehen. Anders verhält sich ein statt des Hubs eingesetzter Switch – dieser stellt für die Zeit der realen Datenübertragung eine echte Punkt-zu-Punkt-Verbindung zwischen den Verbindungsteilnehmern her.

Ein so beschriebenes lokales Subnetz kann wiederum eine Verbindung zu einem anderen Netzwerk besitzen. So entstehen durch Zusammenschluss von kleineren (lokalen) Netzwerken übergeordnete und leistungsfähigere Netzwerkstrukturen.

2.2.1 Physische Klassifikation von Netzwerken

In den folgenden Abschnitten geht es um die Kategorisierung von Netzwerken anhand ihrer physischen Merkmale. Dazu zählt vor allem deren geographische Ausbreitung. Dagegen wird auf dieser Klassifikationsebene die Funktion und Zielstellung eines Netzwerkes bzw. der daran angeschlossenen Computer sowie Ressourcen nicht betrachtet.

Neben den hier dargestellten Netzarten gibt es noch sogenannte Verbundnetze, die z.B. durch den Zusammenschluss zweier lokaler Netzwerke entstehen.

2.2.1.1 Local Area Network (LAN)

Als Local Area Network wird per Definition eine Gruppierung von Computern und damit verbundenen Geräten bezeichnet, die auf einer gemeinsamen Kommunikationsebene miteinander vernetzt sind und typischerweise die Dienste und Ressourcen eines einzelnen Servers innerhalb einer geographisch kleinen Umgebung, z.B. einem Büro oder einem einzelnen Gebäude, nutzen¹⁴. Gewöhnlich stellt dieser eine Server sowohl bestimmte softwareseitige Dienste, d.h. Applikationen und gemeinsame Daten, als auch hardwareseitige Ressourcen, d.h. Speicherplatz und Rechenleistung, zur Verfügung. Dabei ist die Anzahl sowohl der am Netzwerk angeschlossenen Computer bzw. Geräte als auch der bedienten Nutzer irrelevant für den Gebrauch dieser Bezeichnung. Ein LAN kann zwei oder drei Nutzer bedienen (z.B. in einem privaten Hausnetz), aber auch Tausende angeschlossene Teilnehmer haben, wenn ein FDDI-Netzwerk¹⁵ als technologische Grundlage benutzt wird.

LANs unterscheiden sich von anderen Netzarten nicht nur durch die Größe, sondern auch durch die Übertragungstechnik und die Topologie. In einem LAN sind meist alle Maschinen an ein (logisches) Kabel angeschlossen und kommunizieren mit einer Geschwindigkeit von 10 bzw. 100 Megabit/s. Hierbei kamen in der Vergangenheit häufig die Topologien des linearen

¹⁴ Vgl. dazu Definition [Techtarget 2002 LAN]

¹⁵ FDDI-Netzwerke basieren auf der Token-Ring-Technologie und können eine Gesamtlänge von 200 km überbrücken, daher können Tausende Nutzer an ein FDDI-Netzwerk angeschlossen werden.

Busses sowie des Ringes vor¹⁶. Dies gilt jedoch nicht für die meisten der heutigen modernen LANs. Hier findet man am häufigsten eine Stern-Topologie, wobei die einzelnen Maschinen an einen Hub oder Switch angeschlossen werden. Diese Topologie hat sich vor allem aufgrund der in den letzten Jahren stark gesunkenen Preise für die 10Base-T-/100Base-TX-Netzwerktechnik¹⁷ durchgesetzt. Auch die erheblich vereinfachte Verkabelungstechnik und Wartbarkeit spricht für diese Wahl. Von der Übertragungstechnik her entsprechen LANs dem im letzten Kapitel angeführten Broadcast-Modell, d.h. jedes Datenpaket wird an alle am Netzwerk angeschlossenen Rechner gesendet. In einem LAN gibt es außerdem statische und dynamische Übertragungsarten. Von ersterem spricht man, wenn jede Maschine nur in einem bestimmten Zeitintervall senden darf, wobei dieser Zeitschlitz in Beginn und Dauer nach einem genauen Algorithmus berechnet wird. Bei der dynamischen Übertragungsart dagegen kann jede Maschine zu jeder Zeit Daten verschicken, wobei spezielle Algorithmen oder eine zentrale Steuerung dafür sorgen, dass ein zufällig gleichzeitiges Senden von Daten zweier Maschinen erkannt und die so gestörte Übertragung wiederholt wird.

Eine von der Struktur des Local Area Network abgeleitete geographisch größere Form wird als Metropolitan Area Network (MAN) bezeichnet. Dieser Begriff steht für ein Netzwerk, welches Benutzer und deren Computer-Ressourcen miteinander verbindet und zwar über eine Fläche, die größer als ein ausgedehntes Local Area Network, jedoch gemeinhin kleiner als ein Fernnetzwerk (Wide Area Network, WAN), ist¹⁸. Meist wird dieser Terminus für die breitbandige, d.h. leistungsfähige Verbindung kleinerer Netzwerke – z.B. innerhalb einer Stadt – in ein weiteres, größeres Netzwerk gebraucht. Diese breitbandigen Verbindungen tragen ob ihrer Rückgrat-Funktion für die vernetzten Systeme die Bezeichnung „Backbones“. Die Form des Metropolitan Area Network findet ebenfalls Anwendung in internen Netzwerken von Universitäten (sogenannten „Campus Networks“).

Weiterhin kann man die Bezeichnung MAN auch für neue digitale Kabelfernnetze, welche z.B. einen Internetanschluss beinhalten, gebrauchen. Diese können auch spezielle Busse nutzen, die zwei Flussrichtungen für Daten bereitstellen (Distributed Queue Dual Bus, DQDB¹⁹). Das Netzdesign ist ähnlich einem LAN sehr einfach, da es sich auch bei einem MAN um ein Broadcast-Medium handelt.

¹⁶ Vgl. dazu [Tanenbaum 2000], S. 26

¹⁷ 10Base-T und 100Base-TX bezeichnen von der IEEE definierte Standards für Ethernet über Kupferkabel (Twisted Pair). Dabei arbeitet 10Base-T mit Übertragungsgeschwindigkeiten von bis zu 10 MBit/s, während 100Base-TX bis zu 100 MBit/s im Normal- und 200 MBit/s im Vollduplexbetrieb erreicht.

¹⁸ Vgl. dazu Definition [Techtarget 2002 MAN]

¹⁹ Der noch recht junge Distributed Queue Dual Bus ist im IEEE-Standard 802.6 festgeschrieben.

2.2.1.2 Wide Area Network (WAN)

Mit dem Begriff „Wide Area Network“ (WAN, Fernnetzwerk) wird allgemein ein geographisch weitflächig ausgedehntes Telekommunikationsnetzwerk bezeichnet²⁰. Obwohl der verwendete Terminus lediglich ein besonders großes lokales Netzwerk suggeriert, unterscheidet sich eine solche größere Telekommunikationsinfrastruktur davon erheblich. Vielmehr liegt einem WAN das bereits erklärte Point-to-Point-Modell bei der Datenübertragung zugrunde, d.h. es gibt Übertragungsleitungen und Vermittlungselemente, welche in modernen Netzwerken allgemein als Router²¹ bezeichnet werden. Ein Paket wird an jedem zwischengespeicherten Router zunächst vollständig empfangen, gespeichert und – wenn die benötigte Ausgangsleitung frei ist – entsprechend weitergesendet.

Ein solches Netzwerk kann sowohl in Privatbesitz als auch gemietet bzw. öffentlich sein. Große Telefonnetzwerke – und damit auch Netze, die deren Infrastruktur nutzen (wie z.B. das Internet) – haben oft Vereinbarungen zur gemeinsamen Nutzung und zum Informationsaustausch untereinander getroffen, so dass virtuelle weltumspannende Netzwerkstrukturen entstehen²².

2.2.1.3 Drahtlose Netze

Ein noch sehr junge Netzwerktechnologie stellen die drahtlosen Netze dar, wobei hier meist der Begriff des „mobilen Rechners“ gleichgesetzt wird. Allerdings ist die Installation eines LAN in einem Gebäude, in dem die Verlegung von Netzkabeln unmöglich ist, zwar drahtlos, keinesfalls sind solche Computer aber mobil. Eine andere – diesmal mobile – Anwendung eines drahtlosen Netzes ist dagegen der Personal Digital Assistant (PDA), mit dem der Nutzer im Internet surft.

Obwohl oder gerade weil diese Netze noch keine lange Historie haben, gibt es hier einige besonders gravierende Sicherheitsprobleme. Wenn die technische Entwicklung dieser Netzwerke – vor allem in Bezug auf Fehlertoleranz und mögliche Übertragungsgeschwindigkeiten – mit der Zeit fortschreitet, wird allgemein eine weitere Erhöhung der Zahl bekannter Sicherheitslücken erwartet. Dies betrifft vor allem die mangelnde Abhörsicherheit drahtloser Datenetze – da die Daten nicht kabelgebunden laufen, benötigt ein Eindringling keinen Zugangspunkt zum Netzwerk mehr, sondern kann durch die bloße Anwesenheit eines von ihm kon-

²⁰ Vgl. dazu Definition [Techartget 2002 WAN]

²¹ Ein Router ist ein Gerät, welches zwei oder mehr Übertragungsleitungen miteinander verbindet und ankommende Pakete dahingehend weitervermittelt, dass es entscheidet, auf welchem der möglichen Ausgangsleitungen die Daten gesendet werden sollen (Routing Decision), vgl. dazu auch [Techartget 2002 Router]

²² Vgl. dazu [Tanenbaum 2000], S. 28 ff.

trollierten Gerätes (Computer, PDA, etc.) in das Netzwerk einbrechen. Dessen Möglichkeiten wurden gegenüber drahtgebundenen Netzen damit stark vereinfacht²³.

Drahtlose Netze gibt es mittlerweile in verschiedensten Anwendungsbereichen, vor allem wird versucht, die in der Telekommunikationsbranche schon seit vielen Jahren existierenden Netzstrukturen auch für die Übermittlung von digitalen Daten zu nutzen. Hierbei kommen verschiedene Übertragungstechnologien wie GPRS (General Packet Radio Service), HSCSD (High Speed Circuit Switched Devices) oder auch künftig UMTS (Universal Mobile Telecommunication Service) zum Einsatz, wobei der jeweilige Mobilfunknetzbetreiber die Art der zu verwendenden Technologie wählt und seinen Nutzern zur Verfügung stellt.

2.2.2 Logische Klassifikation von Netzwerken

In diesem Kapitel soll es um die Gliederung von Netzwerken anhand ihrer logischen Funktionalität gehen. Die dadurch entstehenden Abgrenzungen sind jedoch meist nicht über längere Zeit scharf getrennt, da die Begriffe häufig unterschiedlich gebraucht werden und daher verschiedene Definitionen existieren. Die hier zur Unterscheidung gebrauchten Merkmale sind nicht objektiv messbare Größen.

2.2.2.1 Internet

Das Internet wird selbst häufig als ein Wide Area Network bezeichnet – allerdings zu unrecht, da es ist nicht als Netzwerk im physikalischen Sinne vorhanden ist. Weiterhin wird mit dem Begriff Internet heutzutage häufig die Gesamtmenge aller weltweit vorhanden Webauftritte charakterisiert und somit das, was der Nutzer „im Internet-Browser sehen kann“. Auch diese Abgrenzung ist falsch, da dies nur einen kleinen Teil des Internets ausmacht, nämlich das durch die Benutzung des Protokolls HTTP²⁴ umgrenzte „World Wide Web“. Andere Technologien und Protokolle, die im Internet vorhanden sind und ebenso häufig genutzt werden (z.B. e-Mail, Telnet oder FTP), werden dabei vernachlässigt.

Vielmehr ist das Internet ein virtuelles Netzwerk, welches öffentlich zugänglich ist und vollständig autark arbeitet. Physisch gesehen ist es ein weltweit einzigartiges System von einzelnen, jedoch zusammenwirkenden Kommunikationsnetzwerken, vor allem öffentlichen Telekommunikationsnetzen. Technisch unterscheidet das Internet von anderen Strukturen die Benutzung der TCP/IP Protokollfamilie, auf die sich nahezu die gesamte Funktionalität des Internets stützt, wobei diese Protokolle mittlerweile auch den Einzug in andere Adaptionen des

²³ Vgl. dazu [Tanenbaum 2000], S. 30 f.

²⁴ HTTP steht für Hypertext Transfer Protocol und bietet ein Verfahren zur schnellen Navigation auf Webseiten im Internet über sogenannte „Hyperlinks“. Beim Anklicken eines Hyperlinks wird auf die dort angegebene Ressource im Internet gewechselt.

Internets, wie das Intranet bzw. Extranet, gefunden haben. Auf diese Protokollfamilie stützen sich wiederum höhere Anwendungsprotokolle im Internet, welche bestimmte Applikationen (Dienste) zur Verfügung stellen – e-Mail, Milliarden von Webseiten, Live-Chats (IRC) und vieles mehr.

2.2.2.2 Intranet und Extranet

Intranets und Extranets stellen eine Adaption der Technologie des Internets dar und haben daher viele Merkmale mit diesem gemeinsam. Genau genommen unterscheiden sich die drei Begriffe nur anhand der Funktionalität ihrer Strukturen, dies soll im Folgenden kurz erläutert werden.

Der Begriff Intranet steht für ein Netzwerk innerhalb einer Firma oder ähnlicher Organisationsform, welches lediglich intern genutzt wird. Der Hauptzweck der Implementierung eines Intranets ist dabei die gemeinsame Nutzung von Informationen und Computerressourcen unter den Mitarbeitern der Firma. Die durch ein Intranet zur Verfügung gestellten Applikationen bzw. Dienste umfassen Teile derer des Internets, meist eingeschlossen sind eine unternehmensinterne Webseite sowie ein elektronisches Nachrichtensystem, welches e-Mail-, sowie eventuell Instant-Messaging- und Chat-Funktionen einbringt. Zusätzlich nur in einem Intranet vorhandene Dienste sind fast immer die zentralisierte Verwaltung von Nutzerinformationen (Namen, Passwörter) sowie die Bereitstellung von Speicherplatz sowohl für unternehmensweite als auch mitarbeiterinterne Daten. Die genannten Funktionalitäten werden von „Intranetservern“ zur Verfügung gestellt, die auch Berechtigungen für zentral gespeicherte Daten und Benutzerprofile vergeben sowie Zugriffe darauf überwachen und protokollieren²⁵.

Technologisch ist ein Unternehmensintranet gekennzeichnet durch eine streng kontrollierte Verbindung zu daran angrenzenden Netzwerken wie z.B. dem Internet, aber auch andere (Abteilungs-) Intranets. Dies wird i.d.R. durch spezialisierte Gateway²⁶-Systeme verwirklicht.

Demgegenüber bezeichnet ein Extranet ein Netzwerk mit Internetmerkmalen, das jedoch vom Internet selbst durch gewisse Sicherheitsmechanismen logisch abgeschirmt ist. Damit kann es als eine Art „ausgelagertes Intranet“ der Firma gesehen werden. Ein Extranet umfasst typischerweise die folgenden Merkmale: die Abgrenzung gegenüber anderen Netzen – besonders dem Internet – durch Firewall-Systeme²⁷, die Verwendung von digitalen Sicherheitszertifikaten und Verschlüsselungstechnologien zur Datenübertragung sowie die mögliche Nutzung

²⁵ Vgl. dazu Definition [Techartget 2002 Intranet]

²⁶ Gateway-Systeme stellen eine Schnittstelle zwischen verschiedenen Netzen dar, welches meist mit zusätzlichen Sicherheitsfunktionen wie Paketfilterung oder anderen Möglichkeiten zur Zugriffskontrolle ausgestattet ist.

²⁷ Firewall-Systeme sind mit speziellen Sicherheitsfunktionen ausgestattete Gateway-Systeme, auf sie wird in Kapitel 4.4.2 noch näher eingegangen werden.

eines im folgenden Gliederungspunkt näher erläuterten Virtual Private Network (VPN) zum Tunneln des Datenverkehrs zwischen einem Extranet²⁸ und entfernten Netzstrukturen.

Häufig wird der Begriff auch – in einem einfacheren Sinne – lediglich für ein zwischen dem Intranet und dem Internet (siehe Abbildung 2.3) liegendes Netzwerk, welches durch Firewall-Systeme auf beiden Seiten geschützt ist, gebraucht. Ein auf solche Weise abgetrenntes Netzwerk erlaubt die genaue Kontrolle der Zugriffe auf dessen Ressourcen durch ein entsprechendes Protokollieren von Informationen auf den es begrenzenden Firewall-Systemen. Dadurch wird das schnelle Erkennen von Sicherheitslöchern, auch bei Angriffen von eigenen Mitarbeitern aus dem Intranet des Unternehmens heraus, möglich.

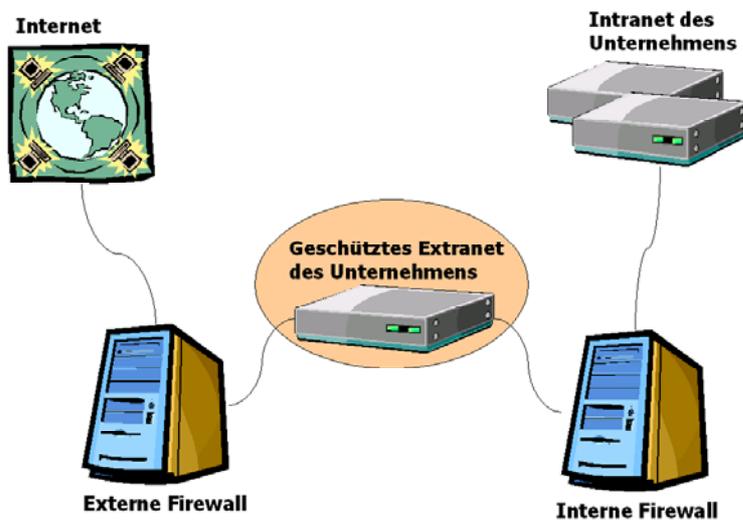


Abbildung 2.3 - Schema der Implementierung eines Extranets

Quelle: eigene Darstellung

2.2.2.3 Virtual Private Network (VPN)

Wie der Begriff Virtual Private Network (VPN) schon beinhaltet, handelt es sich bei dieser Art von Netzwerken um lediglich virtuell vorhandene Strukturen, die auf einem beliebigen öffentlichen Telekommunikationsnetzwerk aufbauen. Man kann VPNs von ihrer Funktionalität her mit einem weitflächigen privaten Netzwerk, welches von einem Unternehmen betrieben wird, vergleichen. Auch dieses ist gegen jeden unbefugten Zugriff von außerhalb seiner Strukturen entsprechend abgeschirmt. Ein VPN unterscheidet sich von einem solchen Konstrukt jedoch durch seine Nutzung eines öffentlich zugänglichen Kommunikationsnetzwerks als Übertragungsmedium. Dadurch braucht ein Unternehmen keine eigenen (und damit kostspieligen) weitflächigen Netzstrukturen zu errichten und betreiben. Die Sicherheit des VPN

²⁸ Vgl. dazu Definition [Techartget 2002 Extranet]

wird dabei durch die Tunnelung²⁹ des öffentlichen Netzwerks erreicht. Dieser Begriff umschreibt die Verschlüsselung der zu übertragenden Datenpakete vor ihrem Eintritt in das öffentliche Netzwerk. Die Daten werden praktisch durch einen logischen Tunnel geleitet. In Abbildung 2.4 ist die Nutzung eines VPN zur Einbindung eines Laptops (z.B. eines Außendienstmitarbeiters) in das Intra- oder Extranet der Firma schematisch dargestellt.

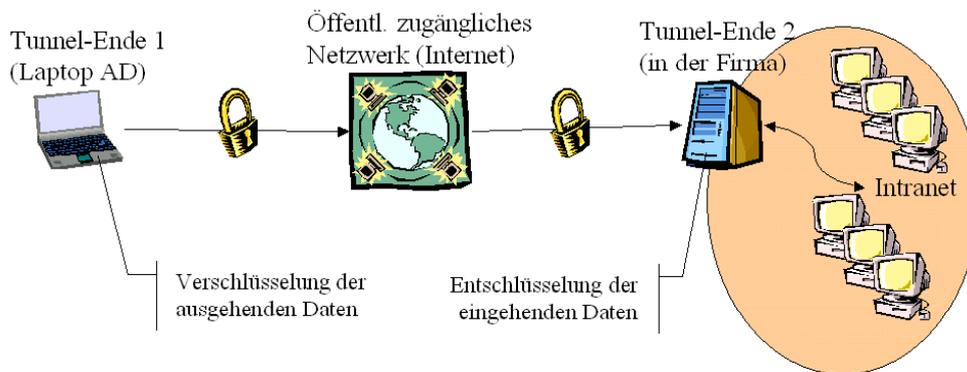


Abbildung 2.4 – Nutzung eines Virtual Private Network zur Datenübertragung

Quelle: eigene Darstellung

Typischerweise ist, wie auch aus der Abbildung ersichtlich wird, die notwendige Software für das VPN auf dem Gateway zum Firmen-Intranet und auf dem entsprechenden Laptop des Außendienstmitarbeiters selbst installiert. Der Laptop fungiert hierbei gleichzeitig als Tunnel-Ende (Gateway) und zu schützendes Subnetz³⁰.

2.3 Protokollhierarchien in Netzwerken

Während in den vorangegangenen Gliederungspunkten die bestimmten Netzwerken zugrunde liegende Hardware näher erläutert wurde, soll im folgenden Kapitel die darauf aufbauende Netzsoftware, d.h. die verwendeten Protokolle, eine Rolle spielen.

2.3.1 Grundlagen von Netzwerkprotokollen

Protokollhierarchien werden vor allem zur Verringerung der Komplexität von Netzwerken aufgestellt, wobei dies bei den meisten Netzen als Reihe von übereinander angeordneten Schichten geschieht. Alle Schichten – mit Ausnahme der obersten – haben stets die Aufgabe, der jeweils darüber liegenden Schicht bestimmte Dienste (Services) zur Verfügung zu stellen. Analog dazu verlässt sich jede Schicht – mit Ausnahme der untersten – auf die Dienste, die

²⁹ Tunnelung meint hierbei die Kommunikation von zwei Systemen über ein öffentlich zugängliches Kommunikationsnetzwerk, z.B. das Internet, durch einen abgeschirmten Übertragungskanal (Tunnel). Vor ihrem Eintritt in den Tunnel werden die Daten zunächst verschlüsselt. Zudem werden die Absender- und Zieladresse der verschlüsselten Pakete umgeschrieben.

³⁰ Vgl. dazu Definition [Techartget 2002 VPN]

ihr die jeweils darunter liegende Schicht zur Verfügung stellt³¹. Dabei existieren zwischen den Schichten genau festgelegte Schnittstellen. Dabei muss jede Schicht die Schnittstelle der darunter liegenden Schicht kennen, um deren Dienste in Anspruch nehmen zu können. Sie muss jedoch nicht über deren darüber angesprochene interne Verarbeitungsprozesse Bescheid wissen. Die Definition sauberer Schnittstellen ist beim Design einer Netzarchitektur einer der wichtigsten Aspekte. Das Beispiel in Abbildung 2.5 zeigt die Zusammenhänge zwischen Schichten, Protokollen und Schnittstellen.

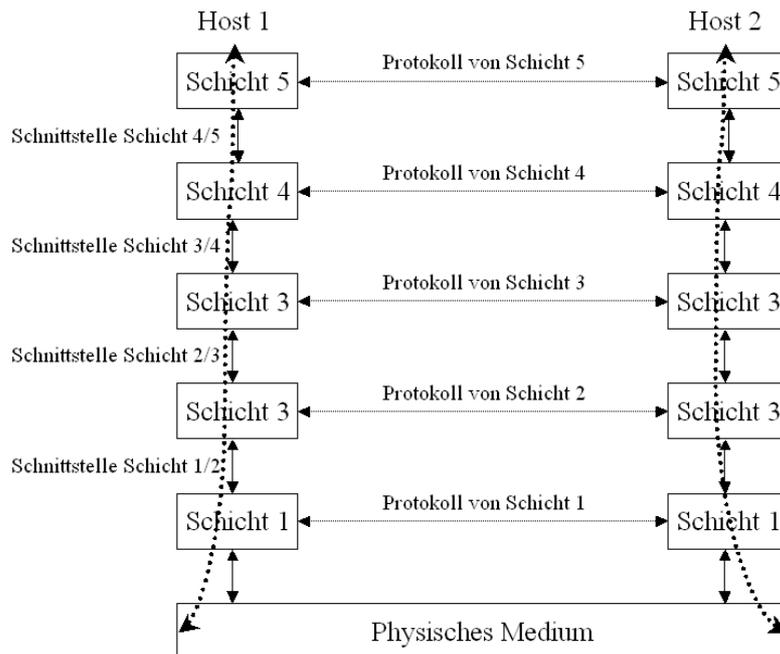


Abbildung 2.5 – Netzarchitektur: Schichten, Protokolle und Schnittstellen

Quelle: nach [Tanenbaum 2000], S. 34

Zwischen den gleichrangigen Schichten zweier kommunizierender Maschinen findet in Wirklichkeit keine Datenübertragung statt. Stattdessen leitet jede Schicht Daten und Steuerinformationen an die unmittelbar darunter liegende Schicht weiter, bis die unterste Schicht erreicht ist. Unter Schicht eins liegt das physische Medium (Datenkabel), über das die Kommunikation stattfindet³². Beim Kommunikationspartner werden die Daten in der umgekehrten Richtung verarbeitet.

Beim Design eines Protokolls muss eine Vielzahl von Variablen betrachtet werden, die hier nur stichpunktartig erwähnt werden sollen. Es handelt sich hierbei u.a. um Regeln für den Datenfluss (Richtung, Vorrangigkeit, Folgesteuerung) sowie die Fehlerüberwachung sowie möglicherweise eine zu garantierende Dienstgüte. Die Funktionen und Leistungen, die ein

³¹ Vgl. dazu [Hein 1995], S. 18

³² Vgl. dazu [Tanenbaum 2000], S. 34 ff.

Protokoll erbringt, lassen seine Kategorisierung in zwei grundlegende Protokollklassen zu: verbindungslose und verbindungsorientierte Protokolle.

Bei den verbindungslosen Protokollen wird jedes Datenpaket als unabhängiges Datagramm durch das Netz zum Empfänger übermittelt, wobei für jedes der Datagramme einzeln der optimale Übertragungsweg (Route) berechnet wird. Pakete können unmittelbar, ohne vorherigen Verbindungsaufbau und abschließenden Verbindungsabbau, über das Netz übertragen werden. Dadurch kann sich die Reihenfolge der Datagramme auf ihrem Weg ändern und Pakete können unbemerkt verloren gehen, wodurch einer höhere Schicht die Aufgabe zuteil wird, diese wieder zu ordnen und nicht empfangene Pakete neu anzufordern. Der Vorteil dieser Art, wie z.B. dem UDP-Protokoll³³, liegt in ihrem geringen Overhead³⁴ und damit höheren Nettodatenrate bei der Übertragung und rechtfertigt damit ihre Nutzung für Anwendungen, bei denen die Schnelligkeit der Datenzustellung wichtiger als deren Genauigkeit ist.

Bei den verbindungsorientierten Protokollen werden verschiedene zusätzliche Dienste bereitgestellt: gesicherter Verbindungsaufbau und –abbau sowie Aufrechterhaltung der Verbindung während des gesamten Datentransfers. Die übertragenen Datenpakete werden durchnummeriert, auf Fehler überprüft und zeitlich überwacht. Fehlerhafte und verloren gegangene Pakete werden neu gesendet. Durch diese zusätzlichen Funktionalitäten ergibt sich ein größerer Protokoll-Overhead und damit auch eine langsamere Datenübertragung (geringere Performance). Verbindungsorientierte Protokolle bieten jedoch Vorteile bei großen Datenmengen bzw. einer Übermittlung über fehleranfällige Transportmedien, wie z.B. Telefonnetzwerke³⁵.

2.3.2 Das OSI-Referenzmodell

Die wohl bekannteste Netzarchitektur bildet das 1983 standardisierte (ISO-) OSI³⁶-Referenzmodell. Die diesem zugrunde liegenden sieben Schichten entstanden aufgrund von verschiedenen wohlgedachten Prinzipien³⁷, z.B. zu (abstrahierten) Funktionen, bestehenden internationalen Normen und Definitionen sowie genauen Abgrenzungen der Schichten in ihrer Funktionalität. Die genaue Beschreibung der Schichten soll hier jedoch nicht weiter Gegenstand der Betrachtung sein.

³³ User Datagram Protocol, verbindungsloses Protokoll aus der Transportschicht, welches vor allem für einmalige Abfragen und Streaming von Audio-/Videodaten genutzt wird

³⁴ Mit Overhead bezeichnet man die Differenz zwischen den Nettodaten (eigentliche Nutzdaten) und der tatsächlich übertragenen Datenmenge einer Verbindung.

³⁵ Vgl. zur Thematik auch [Tanenbaum 2000], S. 40 ff. und [Hein 1995], S. 404 f.

³⁶ OSI steht für Open Systems Interconnection, das Modell beschäftigt sich damit, (für die Kommunikation mit anderen Systemen) offene Systeme zu verbinden. ISO bezeichnet dessen Standardisierung durch die International Standards Organization.

³⁷ Vgl. dazu [Tanenbaum 2000], S. 45 f.

Auf dem OSI-Referenzmodell wurden wiederum verschiedene Protokollsätze definiert (OSI-Protokolle), welche zwar in zahlreichen Produkten implementiert sind, sich aber wegen der Vielfalt und Funktionsmächtigkeit nicht als „das Kommunikationsprotokoll“ durchgesetzt haben. Dagegen stellen die unter der Bezeichnung TCP/IP³⁸ subsummierten Protokolle aktuell den De-facto-Standard im Bereich der LAN- und WAN-Netzwerke dar und sollen im folgenden Abschnitt erläutert werden.

2.3.3 Das TCP/IP-Referenzmodell

Das TCP/IP-Modell wurde aufgrund der bereits im Abschnitt 2.1 erläuterten Schwierigkeiten bei der Zusammenarbeit von Satelliten- und Funknetzen mit dem damaligen ARPANET im Jahre 1974 als Referenzarchitektur entwickelt und nach seinen zwei primären Protokollen benannt. Die bei der Entwicklung vordergründige Zielstellung bestand in der Fähigkeit zur nahtlosen Zusammenschließung mehrerer unterschiedlicher Netzstrukturen. Ein zweites Ziel war die Sicherstellung der möglichst vollständigen Funktionsfähigkeit eines Netzes auch bei Ausfall mehrerer Knoten und Verbindungsleitungen.

Anhand dieser Anforderungen entschied man sich für ein paketvermitteltes Netz auf der Grundlage einer verbindungslosen Vernetzungsschicht, der Internet-Schicht³⁹. Sie ermöglicht es, Pakete in jedes beliebige Netz einzubringen und einem Zielsystem in einem wiederum beliebigen Netz zuzustellen. Dabei wird nicht sichergestellt, dass die Pakete in der bei der Absendung vorherrschenden Reihenfolge beim Zielsystem ankommen – diese Kontrolle obliegt entsprechend höheren Schichten. Durch die Internet-Schicht wird das IP-Protokoll als ein Teil der TCP/IP-Protokollfamilie definiert. Die zu übertragenden Daten werden darin als IP-Datagramme (logische Sicht) bzw. IP-Pakete (technische Sicht) bezeichnet. Seine Aufgabe besteht im ordnungsgemäßen Transport der IP-Pakete vom Absender zum Empfänger, wobei die Zuständigkeit des IP-Protokolls immer nur im Ausführen des jeweils nächsten Schrittes auf dem Übertragungsweg liegt⁴⁰. Ein weiterer durch das IP-Protokoll zur Verfügung gestellter Dienst ist die Fragmentierung (Zerlegung) von Paketen – wenn gewisse Netzwerke dies erfordern – und deren korrekte Zusammenfügung auf dem nächsten Host. Die Internet-Schicht ähnelt der Netzschicht (Vermittlungsschicht) im OSI-Referenzmodell.

³⁸ TCP/IP steht für Transmission Control Protocol / Internet Protocol

³⁹ Der Begriff „Internet“ ist in diesem Zusammenhang nicht als das bekannte globale Netzwerk zu verstehen, sondern als eine allgemeine Schicht, die u.a. auch im Internet vorhanden ist, vgl. dazu [Tanenbaum 2000], S. 53

⁴⁰ In RFC 791, worin IP definiert wird, heißt es dazu: “(to) provide the functions necessary to deliver a package of bits (an Internet datagram) from a source to a destination ... (but) no ... end-to-end data reliability, flow control, sequencing, or other services ...”, vgl. dazu [IETF 1981].

Oberhalb der Internet-Schicht liegt im Design des TCP/IP-Referenzmodells die Transportschicht, welche zwei Point-to-Point-Protokolle definiert. Das Transmission Control Protocol (TCP) stellt ein verbindungsorientiertes Protokoll dar, welches den empfangenen Bytestrom aus der darüber liegenden Schicht in einzelne Nachrichten zerlegt und an die Internet-Schicht weiterleitet. Zu seinen Funktionalitäten zählen auch die Flusssteuerung⁴¹ sowie auf der Empfängerseite die Zusammensetzung der empfangenen Nachrichten in der korrekten Reihenfolge. Somit wird TCP überall dort genutzt, wo die genaue Zustellung der übertragenen Daten wichtiger ist als deren Übertragungsgeschwindigkeit.

Das zweite auf der Transportschicht definierte Protokoll ist das User Datagram Protocol (UDP), welches im Gegensatz zu TCP verbindungslos arbeitet. Bei Verwendung dieses Protokolls muss die darüber liegende Anwendung selbst Funktionalitäten zur Flusssteuerung und Paketabfolge bereitstellen. UDP kommt überall da zum Einsatz, wo die Geschwindigkeit der Datenübertragung primäres Ziel ist und nicht deren Genauigkeit, z.B. im Bereich des Audio- und Videostreaming.

Da das TCP/IP-Referenzmodell keine Sitzungs- und Darstellungsschicht wie das OSI-Modell beinhaltet – für die meisten Anwendungen besteht hierfür kein Bedarf mehr – folgt oberhalb der Transportschicht bereits die Verarbeitungsschicht, welche alle höherschichtigen Protokolle umfasst. Neben vielen anderen zählen hierzu die bekannten Protokolle zum Datentransfer (FTP), e-Mail-Versand (SMTP, POP, IMAP) sowie das vom Browser verwendete HTTP zum Abrufen von Webseiten aus dem Internet. Alle diese Protokolle werden später noch ausführlich besprochen.

Am TCP/IP-Modell kann man jedoch auch viele kritische Punkte bemerken. Zum einen werden die unterhalb der Internet-Schicht fehlenden Funktionalitäten zur Datenübertragung nicht genau im Modell beschrieben. Dort wird lediglich die Aussage getroffen, dass sich „ein Host ... über ein bestimmtes Protokoll am Netz anschließen (muss), um IP-Pakete darüber versenden zu können“. Damit ist diese „Host-an-Netz-Schicht“ eigentlich keine Schicht im üblichen Sinn. Es wird also nicht – wie im OSI-Modell – deutlich zwischen den Termini „Dienst“, „Schnittstelle“ und „Protokoll“ unterschieden. Ebenfalls findet keine Teilung zwischen der Bitübertragungs- und der Sicherungsschicht statt. Beide sollen in der „Host-an-Netz-Schicht“ gemeinsam vorhanden sein, obwohl sie aufgrund ihrer Differenzen separat definiert werden

⁴¹ Mit Flusssteuerung bezeichnet man die Beeinflussung des Datenstroms, wenn ein langsamer Empfänger von einem schnellen Sender mehr Daten empfängt, als er verarbeiten kann.

sollten. Außerdem ist das Modell sehr speziell gehalten, was die Beschreibung anderer Protokollstapel mit dem TCP/IP-Modell (im Gegensatz zum OSI-Modell) unmöglich macht⁴².

In einem IP-basierten Netzwerk hat jeder Kommunikationsteilnehmer eine weltweit eindeutige Bezeichnung, die IP-Adresse genannt wird. Diese besteht aus vier durch Punkte getrennten Zahlen (Oktetten), wobei jede Zahl einen Wert von 0 bis 255 annimmt. Aufgrund seiner IP-Adresse lässt sich jedes mit dem Internet verbundene Computersystem eindeutig bestimmen⁴³. In auf der Grundlage des darüber liegenden Transportprotokolls TCP oder UDP arbeitenden Netzwerken besitzt wiederum jeder Rechner sogenannte Ports. Jeder Port stellt eine eindeutige Adresse für einen Dienst dar, welcher von dem Rechner darüber bereitgestellt werden kann. Wenn eine Anfrage an den betreffenden Port des Systems gestellt wird, reagiert die dafür zugeordnete Serveranwendung darauf und antwortet. Die Ports selbst werden numerisch mit Zahlen zwischen 0 und 65535 bezeichnet, außerdem existiert ein Standardsystem für die feste Zuordnung bestimmter Ports zu darauf gemeinhin erwarteten Anwendungen⁴⁴.

Das hier in Version 4 beschriebene IP-Protokoll deckt mittlerweile nicht mehr alle notwendigen Belange in Netzwerken ab, ein Zustand, der zur – noch andauernden – Entwicklung von IPv6 (IP Version 6) führte. IPv6 hat derzeit den Status eines „Draft Standard“ und findet in einigen Computersystemen bereits testweise Anwendung. Da jedoch die weitaus meisten Systeme auch in den kommenden Jahren die derzeit aktuelle Version 4 des IP-Protokolls einsetzen werden, soll in folgenden Kapiteln die Bezeichnung IP stets für IPv4 stehen.

Im Folgenden soll noch kurz das im TCP-Protokoll festgelegte Modell des Verbindungsaufbaus skizziert werden, da dies für das weitere Verständnis der Arbeit wichtig ist. Im Gegensatz zu anderen auf IP aufbauenden Protokollen (z.B. UDP), verfügt TCP über eine Art „zuverlässiges Kommunikationsmodell“, in dem die Herstellung, die eigentliche Datenübertragung und auch die Beendigung einer Verbindung genau festgelegt sind.

Zur Herstellung einer TCP-Verbindung⁴⁵ schickt der Client zuerst ein Paket⁴⁶ an den Server, bei dem lediglich das SYN-Flag⁴⁷ gesetzt ist und teilt diesem so mit, dass er eine Verbindung aufbauen möchte. Das Paket enthält außerdem eine bestimmte Startsequenznummer (Initial Sequence Number, ISN), welche zur Identifizierung der Verbindung genutzt wird. Der ange-

⁴² Vgl. dazu [Tanenbaum 2000], S. 61 f.

⁴³ Vgl. dazu [anonymous 2001], S. 93

⁴⁴ Vgl. dazu [anonymous 2001], S. 97 f.

⁴⁵ Die Herstellung einer TCP-Verbindung wird ihrem Wesen nach als „Drei-Wege-Handshake“ bezeichnet.

⁴⁶ Der Begriff Paket soll in diesem Abschnitt ausschließlich für ein TCP-Paket stehen.

⁴⁷ Ein TCP-Paket enthält an einer genau definierten Stelle in seiner Paketstruktur (innerhalb des Headers) sechs Bits (0 oder 1), die bestimmte Flags, d.h. Kennzeichnungen bedeuten. Dabei stehen die Werte 1/0 für die Bedeutung Flag gesetzt / Flag nicht gesetzt. Beispiele dafür sind das SYN-Flag (Synchronize Flag, Verbindungsaufbau), das ACK-Flag (Acknowledge Flag, Bestätigung) sowie das FIN-Flag (Finite Flag, Verbindungsabbau). Ein TCP-Paket, bei dem z.B. das SYN-Flag gesetzt ist, wird auch kurz als TCP-SYN-Paket bezeichnet.

sprochene Server antwortet mit einem Paket, bei dem das SYN- und ACK-Flag gesetzt sind (SYN-ACK-Paket) und übermittelt eine ISN, die um genau den Wert „Eins“ höher ist als die des empfangenen Pakets. Der Client sendet daraufhin ein Paket, bei dem lediglich das ACK-Flag gesetzt ist (ACK-Paket), wobei er wiederum die ISN um „Eins“ erhöht und mitsendet. Ab diesem Zeitpunkt gilt eine TCP-Verbindung als hergestellt, wobei es sich um eine Voll-duplexverbindung handelt, d.h. beide Verbindungsteilnehmer können gleichzeitig Daten senden und empfangen. Client und Server senden von nun an Datenpakete (ACK-Pakete, bei jedem Paket wird die ISN jeweils um „Eins“ erhöht), wobei der empfangene Host jedes Paket mit einem leeren ACK-Paket bestätigt. Der Abbau einer TCP-Verbindung erfolgt nach einem ähnlichen Schema wie der Aufbau, anstelle des SYN-Flags kommt diesmal jedoch das FIN-Flag zum Einsatz. Außerdem müssen – aufgrund des Vollduplexbetriebes – beide Verbindungsteilnehmer einer Beendigung zustimmen, daher ergibt sich folgendes Schema: Der Client sendet ein FIN-Paket an den Server, dieser antwortet mit einem FIN-ACK-Paket und bestätigt damit den Abbau der Verbindung. Zusätzlich sendet er ein FIN-Paket an den Client, der ebenfalls mit einem FIN-ACK-Paket antwortet und seinerseits den Verbindungsabbau abschließt⁴⁸.

Die genannten Merkmale der verschiedenen Schichten des TCP/IP-Referenzmodells soll hier nur als Einführung in dessen Arbeitsweise und keineswegs als vollständige Beschreibung dienen. In anderen Kapiteln werden bestimmte Teilaspekte des Modells – vor allem hinsichtlich ihrer sicherheitsrelevanten Eigenschaften und mit ihnen zusammenhängende Probleme – noch näher betrachtet.

2.3.4 Anwendungsbereiche von verschiedenen Protokollen

Obwohl man hierzu keine generelle Übersicht geben kann, soll an dieser Stelle trotzdem eine grundlegende Aufzählung der gebräuchlichen Technologien versucht werden.

In lokalen Netzwerken kommen heutzutage fast ausschließlich das vorstehend besprochene Protokoll TCP/IP sowie das von Novell entwickelte Client-/Server-Netzsystem NetWare zum Einsatz. Dieses basiert auf einem herstellereigenen Protokollstapel, welcher aus dem Vermittlungsprotokoll Internetwork Packet Exchange (IPX) sowie den Transportprotokollen Network Core Protocol (NCP) und Sequenced Packet Exchange (SPX) aufgebaut ist. Dabei können Anwendungen zwischen der Verwendung der beiden letztgenannten Protokolle wählen. Noch im Jahr 2000 wurde Novell NetWare als das weltweit populärste System für vernetzte PCs angesehen, insbesondere für Unternehmen, welche von einer Großrechnerarchitektur auf Per-

⁴⁸ Vgl. dazu auch [anonymous 2001], S. 94 ff.

sonalcomputer umstellen wollten⁴⁹. Andererseits belegen Statistiken bereits 1999 einen dramatischen Einbruch im Marktanteil von NetWare-basierten Netzwerken⁵⁰ im Bereich lokaler Netze. Der Nachteil von NetWare liegt in der notwendigen Umsetzung von IPX in IP-Pakete bei der Anbindung an das Internet oder ein anderes TCP/IP-basiertes Netzwerk. Der Vorteil TCP/IP-basierter lokaler Netzwerke dagegen ist, dass nur ein höheres Protokoll Verwendung findet, sowohl im LAN als auch bei einer Anbindung an das Internet.

In lokalen Netzwerken wird als darunter liegende Technologie meist (Fast-) Ethernet genutzt und somit CSMA/CD⁵¹ als Protokoll der Sicherungsschicht. Nur einige LANs benutzen nicht die Ethernet-Technologie, sondern ein anderes Mitglied der unter der IEEE-Norm 802⁵² zusammengefassten Protokolle, nämlich Token-Ring (IEEE 802.5).

Im Internet wird ausschließlich das höhere Kommunikationsprotokoll TCP/IP verwendet, während hier jedoch andere Protokolle in der darunter liegenden Sicherungsschicht zum Einsatz kommen. Dies liegt daran, dass das Internet nicht – wie die lokalen Netzwerke – ein Broadcast-, sondern ein Punkt-zu-Punkt-Netzwerk darstellt. Dieses wird aus Routern gebildet, welche meist über Mietleitungen miteinander verbunden sind. Die Funktionsweise von Routern wurde bereits ausführlich in Kapitel 2.2.1.2 beschrieben. Zwei Protokolle kommen bei der Router-Router-Kommunikation am häufigsten zum Einsatz, zum einen das ältere SLIP-Protokoll⁵³ und zum anderen das moderne, flexiblere PPP-Protokoll. Es vereint mehrere Vorteile⁵⁴ gegenüber SLIP und wird dieses bald vollständig ablösen.

2.4 Strukturierung von Netzwerken

Die Strukturierung von Netzwerken, also das Netzdesign, ist eine weitgehende Entscheidung hinsichtlich seiner späteren Verwaltbarkeit und möglicher Absicherung und soll daher in diesem Abschnitt näher betrachtet werden. Dabei sind vor allem die Kriterien der Netzwerkgröße sowie Schnittstellen zu anderen lokalen Netzwerken und vor allem zum Internet zu beachten.

⁴⁹ Vgl. [Tanenbaum 2000], S. 62

⁵⁰ Vgl. dazu [Informationweek 2002]

⁵¹ CSMA/CD steht für Carrier Sense Multiple Access (with) Collision Detection und bildet die Grundlage für das Ethernet (IEEE 802.3) als wichtigste Technologie für lokale Netzwerke.

⁵² Das Institut of Electrical and Electronics Engineers (IEEE) ist der weltweit größte Fachverband und beschäftigt sich auch mit der Entwicklung von Normen in der Informatik. IEEE-Norm ist der wichtigste Standard für LANs und beinhaltet u.a. CSMA/CD (Ethernet), Token-Bus und Token-Ring. Sie wurde auch von der International Standards Organization als Grundlage für die ISO-Norm 8802 genutzt.

⁵³ SLIP steht für Serial Line IP. Das sehr einfache Protokoll wurde 1984 entwickelt und ist in RFC 1055 beschrieben. Es unterstützt nur Netzwerke auf IP-Basis und lediglich feste IP-Adressen. Vgl. dazu auch [Tanenbaum 2000], S. 255 f.

⁵⁴ PPP steht für Point-to-Point-Protocol und ist in RFC 1661-1663 definiert. Im Gegensatz zu SLIP unterstützt PPP mehrere Protokolle (IP, NCP u.a.) und kann mit dynamischen IP-Adressen umgehen. Es beherrscht auch Fehlererkennung und Authentifizierungsmechanismen. Vgl. dazu auch [Tanenbaum 2000], S. 256 ff.

Im Folgenden sollen lediglich die lokalen Netzwerke, insbesondere Intranets bzw. Extranets von Unternehmen betrachtet werden, da auf außerhalb gelegene Netzstrukturen im Regelfall kein Einfluss möglich sein wird. Als zugrunde liegendes Protokoll bzw. Technologie wird im Regelfall das am weitesten verbreitete TCP/IP mit darunter liegendem Ethernet-LAN angenommen.

Dabei befasst sich die technische Sicht mit der physischen Teilung von Netzwerken anhand von verschiedenen Netzwerksegmenten, welche nur über eine exklusive Anzahl von Verbindungen (im Normalfall eine) miteinander verknüpft sind, währenddessen die logische Sicht auf die Erstellung funktional getrennter Netzwerksegmente eingeht.

2.4.1 Technische Sicht

Bei der Planung des Netzwerks eines mittleren bis großen Unternehmens sollte eine Segmentierung, z.B. nach den Unternehmensfunktionen der Mitarbeiter (Abteilungen), erfolgen. Dies ermöglicht die Einrichtung von gesicherten Schnittstellen zwischen den Segmenten und damit eine gezielte und automatisierte Überwachung des Netzverkehrs im Intranet. Ein positiver Nebeneffekt ist z.B. die Möglichkeit der Auslastungsfeststellung des Intranet für Controlling-Zwecke, wiederum getrennt nach Teilbereichen des Unternehmens. Die weitaus wichtigere Abgrenzung liegt jedoch in der Planung einer exklusiven Verbindung (Gateway) zu öffentlichen Netzwerken wie dem Internet. Hier sollte in jedem Fall eine sogenanntes Firewall-System errichtet werden, das den gesamten Netzverkehr an dieser Schnittstelle überwacht, filtert und protokolliert. Hierbei ist der Datenverkehr in beiden möglichen Flussrichtungen als relevant anzusehen.

Ebenfalls zur sicherheitstechnischen Strukturierung von Netzwerken zählen Aspekte wie die Absicherung kritischer Komponenten (Server, Hub oder Switch) gegenüber unbefugtem Zugriff oder die genaue Festlegung aller erlaubten MAC-Adressen⁵⁵ im lokalen Netzwerk.

Eine weitere Art der Strukturierung kann bei der Verbindung nicht kompatibler Rechnernetze notwendig werden, wobei diese Strukturierung nicht vordringlich sicherheitsrelevant ist. Auch hierfür werden als Protokollkonverter Gateway-Systeme eingesetzt. Dabei findet eine logische Umsetzung zwischen den Protokollen auf der obersten Ebene der jeweiligen Hierarchien statt⁵⁶. Eine weitere Möglichkeit der Verbindung nicht IP-basierter Netzwerke über das Internet ist das TCP/IP-Tunneling. Hierbei werden die inkompatiblen Pakete in TCP/IP-Pakete

⁵⁵ Bei der MAC-Adresse (auch Hardware-Adresse, Ethernet-Adresse) handelt es sich um eine weltweit eindeutige, 48-bit lange Nummer, die in jedem Netzwerk-Controller fest encodiert ist. Alle Komponenten eines Netzwerks kommunizieren anhand dieser Nummer miteinander, so dass über eine vom Netzwerkadministrator festgelegte Tabelle mit Einträgen der verschiedenen MAC-Adressen als Zugriffsbeschränkung dienen kann.

⁵⁶ Vgl. dazu auch [Hein 1995], S. 378 ff.

verpackt und danach über das IP-Netzwerk vermittelt. Fast alle Router-Hersteller unterstützen dieses Verfahren in ihren Produkten.

2.4.2 Logische Sicht

Bei der logischen Strukturierung eines Netzwerks geht es um die Definition eines Netzwerksegments hinsichtlich seiner Funktion im Unternehmen, eine solche bildet z.B. die Einrichtung eines Unternehmensintranet sowie –extranet. Häufig ist die logische Sicht der physischen Strukturierung zwar nicht deckungsgleich, jedoch ähnlich. Wichtig bei der Einrichtung eines Unternehmensintranet ist die Verwendung von nicht-routbaren IP-Adressen⁵⁷ für alle Komponenten (Workstations und Intranetserver) innerhalb des Netzwerksegments. Somit wird sichergestellt, dass jede dieser Komponenten nicht direkt mit (obwohl physikalisch verknüpften) Ressourcen im Internet kommunizieren kann und ein potenzielles Sicherheitsloch entsteht. Lediglich über die bereits besprochene exklusive Schnittstelle zum Internet ist eine Verbindung möglich, wobei dieser Gateway die private IP-Adresse aus dem Intranet auf eine weltweit gültige, routingfähige IP-Adresse umsetzt. Weiterhin wichtig ist die genaue logische Abgrenzung eines eventuell vorhandenen Extranets und dessen bereitgestellter Dienste und Ressourcen gegenüber dem Internet.

2.5 Management von Netzwerken

In diesem Abschnitt sollen nur kurz die Grundprinzipien des Netzwerkmanagements beschrieben werden, während in späteren Kapiteln entsprechend detaillierter auf Teilaspekte des Managements eingegangen werden wird. Eigentlich lässt die Bezeichnung Netzwerkmanagement nur auf ein Teilgebiet der Administrationsaufgaben schließen. Besser ist in diesem Zusammenhang der Gebrauch des Begriffs „Sicherheitsmanagement“, da dieser die komplexe Aufgabenstellung in ihrer Gesamtheit erfasst.

Der wichtigste Punkt hierbei ist die genaue Bestimmung von Zuständigkeiten bestimmter Mitarbeiter für wiederum genau festgelegte Aufgabenbereiche innerhalb des Netzwerkmanagements. Folgende Abstufungen bei der Zuständigkeit sind möglich und auch gebräuchlich. Ein Mitarbeiter kann für das gesamte Management – und damit auch das Sicherheitsmanagement – des Unternehmensnetzwerkes verantwortlich sein. Dies ist die häufigste Management-

⁵⁷ Nicht-routbare (sogenannte private) IP-Adressen wurden aufgrund der stetig bedrohlich sinkenden Anzahl freier Bereiche weltweit gültiger IP-Adressen entwickelt und sind in RFC 1918 definiert, vgl. dazu [IETF 1996]. Diese Adressbereiche dürfen nicht auf Computersystemen direkt im Internet Verwendung finden, sondern müssen durch eine logische Trennung (z.B. Firewall-System) und Einsatz einer Adresstransformation (Network Address Translation, NAT) auf weltweit gültige Adressen umgesetzt werden, bevor Pakete über das Internet versandt werden können.

form in kleineren bis mittleren Netzwerkstrukturen. Bei letzteren findet man häufig auch eine Teilung der Managementzuständigkeiten einzelner Mitarbeiter, entweder getrennt nach Aufgabengebieten⁵⁸ oder nach zuvor erstellten Netzwerksegmenten. Eine dritte Form, bei der verschiedene Mitarbeiter dieselben Managementaufgaben durchführen – leider immer noch eine gerade in kleineren Unternehmen gebräuchliche Form – soll hier lediglich als Negativbeispiel Erwähnung finden, da sie mehrere gravierende Probleme mit sich bringt. Zum einen gibt es keinen exklusiv verantwortlichen Mitarbeiter für die anfallenden administrativen Aufgaben, zum anderen sind sichere Passwortvergaben, Rechteverwaltung usw. so nur schwer realisierbar. Auch die Dokumentation durchgeführter Tätigkeiten ist in solch einer Konstellation meist nicht oder nur rudimentär vorhanden.

Oberstes Grundprinzip bei der Vergabe von Managementaufgaben sollte deren absolut regelmäßige Ausführung sein, wobei dies auch die Erarbeitung einer Rückfallebene bei Urlaub, Krankheit oder einem Ausscheiden aus der Firma der diese Aufgaben übernehmenden Mitarbeiter einschließt. Die absolute Integrität und Verantwortungsbewusstheit der betreffenden Mitarbeiter sollte ebenfalls zu jedem Zeitpunkt garantiert sein. Ein weiteres Prinzip betrifft die genaue Dokumentation der durchgeführten administrativen Tätigkeiten.

Bei Beachtung der o.a. Gesichtspunkte kann ein Netzwerkmanagement (bzw. Sicherheitsmanagement) effizient durchgeführt werden.

⁵⁸ Einzelne Aufgabengebiete können z.B. das Anschließen neuer Netzwerkkomponenten, die Vergabe von Trust Accounts für Windows-Workstations, die Verlegung von Kabeln oder das Installieren neuer Systemsoftware sein.

3 Sicherheitsrisiken in Netzwerken

In diesem Kapitel sollen bekannte und vor allem eher weniger bekannte Sicherheitsrisiken bei vernetzten Systemen vorgestellt werden. Dazu wird zunächst ein Risikovergleich von vernetzten gegenüber alleinstehenden Systemen vorgenommen sowie eine historische Abhandlung des Themas versucht. Als nächstes soll eine Definition der Begriffe Computerkriminalität bzw. Netzwerkkriminalität zur genauen Abgrenzung der Materie beitragen. Anschließend wird auf deren verschiedene Formen, wie z.B. Einschleusen von Malicious Software, Unterwandern von Authentifizierungsmechanismen und bestehenden Autorisationen sowie weitere Risiken, u.a. installierte Software und die Übertragung von Daten im Netzwerk eingegangen. Zuletzt wird noch ein oft verschwiegenes, weil unangenehmes Sicherheitsproblem angesprochen – die unternehmensinternen Mitarbeiter.

Das Kapitel soll Sicherheitsrisiken erkennen helfen und damit die Grundlage für eine objektiv richtige Risikoeinschätzung vernetzter Computersysteme in einem Unternehmen schaffen.

3.1 Risikovergleich vernetzter und alleinstehender Systeme

In diesem Abschnitt soll ein Vergleich von vernetzten und alleinstehenden Computersystemen hinsichtlich ihrer Sicherheitsprobleme versucht werden.

Wenn viele Kritiker der weltweiten Vernetzung von Computersystemen über deren mangelnde Sicherheit diskutieren, wird häufig nicht beachtet, dass auch nicht vernetzte, alleinstehende Systeme keinesfalls als vollkommen sicher gelten können. Auch ein solches System besitzt Schnittstellen nach außen und damit potenzielle Gefährdungskanäle, wie z.B. das Diskettenlaufwerk, CD-Laufwerk oder sogar einen CD-Brenner. Somit können über Disketten oder CDs ebenfalls Viren und andere bösartige Programme in das System eingeschleust werden und auch – über dieselben Kanäle – Daten unbefugt aus dem Computersystem entwendet werden (Datenspionage). In Verbindung mit der Verfälschung dieser Daten und einem Wiedereinspielen in das ursprüngliche System können auch Daten eines solchen Systems bewusst manipuliert werden, außerdem ist – wie bei jedem Computer – das unbefugte Löschen von wichtigen Daten, ohne jeden Bezug zu einer möglichen Vernetzung des Systems, möglich. Daraufhin sollte man sich die Frage stellen: „Gibt es überhaupt ein vollkommen abgesichertes Computersystem?“

Solch ein vollständig sicherer Computer könnte ungefähr so beschrieben werden⁵⁹: „Ein in einem dicken, nicht zu öffnenden Metallcontainer verpacktes System, mit soliden Stahlbändern an einer Betonmauer verankert und von einer autonomen Batterie betrieben; ohne irgendeine Form menschlichen Zugriffs und Vernetzung mit der Außenwelt; rund um die Uhr geschützt von bewaffneten, ständig wechselnden Wächtern mit der Anweisung, niemanden an das System heranzukommen zu lassen.“ Ein solcher Computer wäre vollkommen sicher – und vollkommen nutzlos. Eine andere Definition hierzu besagt⁶⁰: „Sicher ist ein Computer nur, wenn er ausgeschaltet und der Stecker aus der Steckdose gezogen ist“. Auch dies kann kaum eine brauchbare Definition für ein abgesichertes System darstellen. Man kann also zusammenfassend sagen, dass es einen vollständig abgesicherten Rechner nicht gibt.

Miteinander vernetzte Computersysteme, besonders Systeme mit Anschluss zu verschiedenen Netzwerken, sind natürlich stärker gefährdet als jene im letzten Abschnitt betrachteten. Genau genommen, kommt hier jedoch lediglich das (oder im Falle eines multiplen Anschlusses die) Netzkabel als mögliche Eingangs- und Ausgangskanäle für sicherheitsrelevante Probleme in Frage. Obwohl nur ein zusätzlicher Kanal entsteht, ist dessen Gefährdungspotenzial für das System weitaus höher als das der bisher beschriebenen Kanäle, wie Disketten- oder CD-Laufwerk. Dies liegt vor allem an der Möglichkeit, den Kanal ohne einen physischen Zugang zum System zu benutzen, meist sogar ungewollt und unerkannt von einer den betreffenden Computer überwachenden Person⁶¹.

Hieraus lässt sich auch eine historische Betrachtung des Begriffs Sicherheitsrisiken vernetzter Systeme ableiten. In den Anfängen der Computertechnologie waren deren Systeme und auch erste Netzwerke – wie das ARPANET – nur einzelnen Wissenschaftlern und Spezialisten sowie Hard- und Softwareentwicklern vorbehalten. Damit war der Nährboden für Computerkriminalität sehr viel geringer als heute ausgeprägt. Mit der Reifung der Technologie kamen jedoch große Teile der Bevölkerung (in den Industrienationen) in den Besitz von Computersystemen. Die Gründe hierfür sind vielfältig, stark sinkende Preise für Rechner und verwandte Technologien, immer wiederkehrende Präsenz in den Medien und natürlich das steigende Interesse am Internet, vor allem an den Anwendungen e-Mail und World Wide Web können hierfür angegeben werden. Somit ist seither eine große Anzahl von „Nicht-Fachkräften“ an der Nutzung von Computersystemen und bestehenden Netzstrukturen beteiligt.

⁵⁹ aus: [Geodsoft 2002]

⁶⁰ aus: [anonymous 2001], S. 216

⁶¹ Als „Person“ kann hierbei sowohl der reguläre Nutzer des Computers als auch ein eventuell vorhandener Systemadministrator gesehen werden. Dabei liegt der Fokus des Terms „Überwachung“ bei ersterem auf dem Bemerken eines ungewöhnlichen Systemverhaltens bei dessen normaler Nutzung, bei letzterem dagegen auf dem Feststellen eines ungewöhnlichen Ereignisses in einer entsprechend protokollierenden Datei.

Eine weitere, nicht unerhebliche Steigerung von Computerkriminalität konnte nach dem Zusammenbruch der Regierungen in osteuropäischen Staaten Anfang der neunziger Jahre festgestellt werden. Dort waren viele Fachleute der IT-Branche, vor allem Programmierer, innerhalb kürzester Zeit arbeitslos und ohne Chance auf Zukunft in einem neuen Betätigungsfeld. In Ermangelung dessen und auch als eine Art Rachefeldzug begannen viele mit der Entwicklung von zerstörerischer Software (Viren, Würmer oder Trojanischer Pferde)^{62,63}.

Weitere Gründe für ansteigende Computerkriminalität sind z.B. in dem immer stärker zunehmenden Austausch von geschäftskritischen Daten über öffentlich zugängliche Netzwerke sowie im Aufleben des Electronic Commerce, also des Handels im Internet zu sehen. Hier treten vor allem Möglichkeiten der aktiven Geschäftsschädigung und der Profitbeschaffung als Motive auf.

Man kann zusammenfassend sagen, dass die Computer- und Netzwerkkriminalität seit den ersten Anfängen dieser Technologie bis in die heutige Zeit zunimmt, und das mit exponentiellem Wachstum. Angaben des CERT/CC⁶⁴ zufolge, welches seit 1988 Statistiken über kriminelle Vergehen in Zusammenhang mit Computertechnologien führt, stieg deren Zahl von damals 6 auf mittlerweile 52658 im Jahre 2001. Das CERT/CC gibt seit 1995 regelmäßig Warnungen vor entdeckten Sicherheitsproblemen in Soft- und Hardware heraus und fungiert dahingehend als zentrale Anlaufstelle im Internet.

In Deutschland untersucht das Bundesministerium des Inneren jährlich die Anzahl der gemeldeten Fälle von Computerkriminalität als ein Teil der allgemeinen Kriminalstatistik. Dabei wurde in der am 02. Mai 2002 veröffentlichten Statistik für das Jahr 2001 ein Anstieg der Computerkriminalität um 39,9 Prozent gegenüber dem Vorjahreszeitraum festgestellt⁶⁵. Die genauen Zahlen sind in Tabelle 3.1 aufgeführt.

⁶² Vgl. dazu [SZ-Newsline 2002] sowie [Fuhs 1993]

⁶³ Die Begriffe Virus, Wurm und Trojanisches Pferd werden in Abschnitt 3.5.1 ausführlich vorgestellt.

⁶⁴ Das CERT/CC (CERT Coordination Center, CERT steht für die frühere Bezeichnung Computer Emergency Response Team) ist das führende Informationszentrum für Computersicherheit im Internet und wird vom Software Engineering Institut der Carnegie Mellon University, Pennsylvania betrieben, <http://www.cert.org>

⁶⁵ Vgl. dazu [Heise 2002]

Tabelle 3.1 - Statistik zu Fällen der Computerkriminalität in Deutschland für 2001

Quelle: aus [BMI 2001 Kriminalstatistik], Abschnitt 5.6

Bereich	Jahr	Erfasste Fälle	Änderung in v.H.	Häufigkeitszahl *)
Bundesrepublik Deutschland (Gebietsstand vor 03.10.90)	1987**)	3 355		5,4
	1990	5 004		8,0
alte Länder mit Gesamt-Berlin	1991	7 928		12,2
	1992	11 265		17,1
Bundesrepublik Deutschland (Gebietsstand seit 03.10.90)	1993	13 898		17,2
	1994	20 998	51,1	25,8
	1995	27 902	32,9	34,2
	1996	32 128	15,1	39,3
	1997	39 331	22,4	48,0
	1998***)	46 076		56,2
	1999	45 359	-1,6	55,3
	2000	56 684	25,0	69,0
	2001	79 283	39,9	96,4

*) Häufigkeitszahl: Fälle pro 100 000 Einwohner

**) Beginn der gesonderten Erfassung

***) Inhaltsänderung: Einbeziehung von Betrug mit Zugangsberechtigung zu Kommunikationsdiensten

3.2 Allgemeine Definition von Computer- und Netzwerkkriminalität

Einer bereits aus dem Jahr 1986 von der OECD⁶⁶ aufgestellten Definition des Begriffs zufolge, bezeichnet Computerkriminalität „jedes illegale, unethische oder unautorisierte, mit der automatischen Verarbeitung und Übertragung von Daten verbundene Verhalten“⁶⁷. Diese Definition erscheint jedoch zu weitreichend bzw. ungenau und damit für eine schlüssige Erläuterung des Begriffes nicht geeignet.

Eine weitere Definition des Begriffs Computerkriminalität bzw. Hochtechnologie-Kriminalität hat das Bundesministerium des Inneren (BMI) aufgestellt, bei der es heißt: „Der Begriff umfasst alle Straftaten ..., bei denen Daten, Datenträger, die Datenverarbeitung oder Datenverarbeitungsanlagen in den Tatmerkmalen enthalten sind bzw. ... die automatische Datenverarbeitung zur Planung, Vorbereitung oder Ausführung eingesetzt wird. Des weiteren

⁶⁶ Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

⁶⁷ engl. Originalfassung in [Heinegg 1997]

... Straftaten im Zusammenhang mit Datennetzen ... sowie ... rechtswidrige Handlungen ... (zur Beeinträchtigung der) Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von elektronisch (und) magnetisch ... gespeicherten Daten“⁶⁸. Bei der Netzwerkkriminalität – als Teil der o.a. Hochtechnologie-Kriminalität – handelt es sich nach der Definition des BMI um diejenigen Fälle von Computerkriminalität, die „in oder über öffentliche Computernetze erfolgen“. Das Ministerium nennt als Beispiele für Computerkriminalität sowohl Angriffe auf Datensysteme als auch Straftaten wie die Verbreitung von rechtswidrigen Inhalten und Informationen. Dabei spielt die Technologie bei der zweiten Form nur als Mittel zur Tatbegehung eine Rolle, nicht als Zielobjekt einer kriminellen Aktion. Obgleich auch die zweite Form von Computerkriminalität sehr wohl eine zu verhindernde bzw. zu verfolgende Straftat darstellt, ist sie für diese wissenschaftliche Arbeit nicht von Belang. Der Fokus liegt dagegen eindeutig bei der erstgenannten Form, dem Angriff auf beliebige Systeme. Die dabei vorkommenden Ausprägungen sollen im nächsten Abschnitt näher charakterisiert werden.

3.3 Ausprägungen von Computer- und Netzwerkkriminalität

Im Folgenden soll ein Computersystem vor allem als Bereitsteller von Informationen bzw. Dienstleistungen angesehen werden. Somit existiert generell ein Informationsfluss von einer beliebigen Quelle zu einem beliebigen Ziel, wie z.B. von einer Datei zu einem Benutzer⁶⁹. Dieser normale Informationsfluss ist in Abbildung 3.1 dargestellt.



Abbildung 3.1 - Normaler Informationsfluss

Quelle: aus [Stallings 1995], S. 8

Für einen sicheren Datenaustausch sind zusammenfassend – und analog zur Definition von Computerkriminalität i.S.d. Bundesministeriums des Inneren – vier Voraussetzungen bzw. Merkmale zu nennen. Gewährleistet sein muss zum Ersten die Vertraulichkeit und Integrität der Daten. Dies bedeutet, dass die zu übertragenen Daten in ihrer ursprünglichen, nicht modifizierten Form verbleiben und nur denjenigen Personen zugänglich sind, die am Kommunikationsprozess teilnehmen. Weiterhin muss die Authentizität der an der Kommunikation Beteiligten sichergestellt sein. Als letztes ist eine genaue Protokollierung des Kommunikationspro-

⁶⁸ aus: [BMI 2002 Hochtechnologie-Kriminalität]

⁶⁹ Vgl. dazu [Stallings 1995], S. 7

zesses notwendig. Dies hat in einer Form zu geschehen, die es später ermöglicht, das Stattfinden des Datenaustauschs sowie die Identitäten der daran beteiligten Personen genau nachzuweisen.

Durch einen Angriff wird der normale Informationsfluss verändert, wobei die folgenden vier Kategorien von Angriffen unterschieden werden müssen: die Unterbrechung des Informationsflusses sowie das Abfangen, Modifizieren bzw. Generieren von Daten. Diese Fälle sollen im Folgenden kurz erläutert werden.

Die einfachste Art der vorgestellten Angriffe stellt das bloße Unterbrechen des Informationsflusses dar. Dabei wird entweder die Informationsquelle selbst (Festplatte des Computersystems, Dateisystem) oder Teile des Kommunikationsnetzwerks (Netzwerkanschluss, Verbindungskabel) in einer Weise geschädigt, dass daraufhin kein Informationsfluss vom diesem System aus – meist zu verschiedenen Zielsystemen – möglich ist. Die Art der Schädigung kann dabei physischer oder logischer Art sein, wobei letztere z.B. die Abänderung der Adresse des Computersystems, so dass dieses für einen bestimmten Zeit nicht erreichbar ist, darstellt. Es handelt sich demnach hierbei um einen Angriff auf die Verfügbarkeit (des Systems). Eine schematische Darstellung dieser Angriffsart findet sich in Abbildung 3.2, Punkt (a).

Das Abfangen wiederum ist ein Angriff auf die Vertraulichkeit der betroffenen Daten. Bei der angreifenden Seite kann es sich entweder um eine natürliche Person oder ein Programm bzw. einen Computer handeln. Diese Angriffe werden häufig unter dem Begriff „Sniffen“⁷⁰ zusammengefasst, eine Darstellung findet sich in Abbildung 3.2, Punkt (b).

Das Modifizieren von Daten ist eine Erweiterung des eben angeführten Falls. Hierbei werden die zuvor abgefangenen Daten auf eine Weise verändert, die den Nutzen des Informationsflusses für den Angreifer – verglichen mit dem ursprünglich übertragenen Informationen – erhöht, oder aber den Nutzen für den rechtmäßigen Sender oder Empfänger verringert. Im Regelfalle handelt es sich dabei um die Manipulation von Zahlen, z.B. Überweisung größerer Geldbeträge oder die Erweiterung von bestimmten (Zugriffs-)rechten. Die so veränderten Daten werden zum vorher bestimmten Zielsystem geschickt und erreichen dort ihre vom Angreifer gewünschte Wirkung. Zusätzlich wird der Absender der betreffenden Informationen dahingehend fingiert, dass es sich scheinbar um die (dem Zielsystem vertraute) ursprüngliche Informationsquelle handelt. Da die Originaldaten vorsätzlich modifiziert wurden, handelt es dabei um einen Angriff auf die Informationsintegrität. Der Ablauf einer solchen Aktion ist schematisch in Abbildung 3.2, Punkt (c) dargestellt.

⁷⁰ Das „Sniffen“ von Daten in einem Netzwerk wird noch ausführlich in Abschnitt 3.8.1 behandelt und soll daher hier nicht Gegenstand weiterer Erklärungen sein.

Die vierte Kategorie, das Generieren von (falschen) Informationen ist mit dem im letzten Absatz vorgestellten Modifizieren vergleichbar, hierbei erfolgt jedoch nicht eine Abänderung von zuvor abgefangenen Informationen, vielmehr werden bewusst falsche Daten erstellt und an ein ausgewähltes Zielsystem gesendet. Zusätzlich wird wiederum die Absenderadresse entsprechend fingiert. Eine schematische Darstellung eines solchen Angriffs findet sich in Abbildung 3.2, Punkt (d).

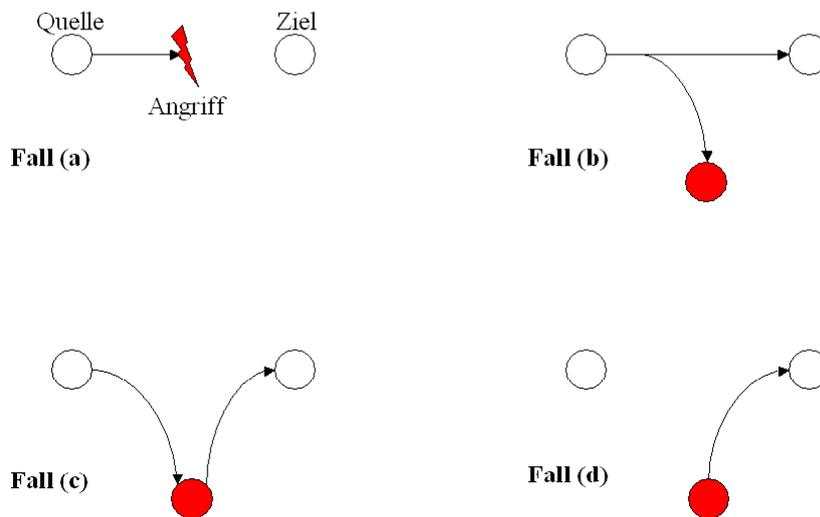


Abbildung 3.2 - Kategorisierung sicherheitsrelevanter Angriffe auf Computersysteme

Quelle: aus [Stallings 1995], S. 8 (vgl. hierzu auch Abbildung 3.1, normaler Informationsfluss)

3.4 Motivation für Computer- und Netzwerkkriminalität

Unter dem Stichwort „Motivation“ soll in diesem Abschnitt untersucht werden, aus welchen allgemeinen und speziellen Gründen ein Angreifer computerkriminalistisch relevante Aktionen überhaupt durchführt. Eine Angabe aller Gründe würde allerdings den Rahmen dieses Kapitels sprengen, daher soll im Folgenden nur eine kurze Aufzählung erfolgen.

3.4.1 Grundlegende Intention eines computerkriminalistischen Angriffs

Einen Angreifer treiben zumeist Motive wie das Erreichen unautorisierten Zugangs zu Informationen, das Vorspielen einer anderen Identität (zum Ausnutzen eventueller Mehrrechte), das Protokollieren des Zugriffs auf bestimmte Informationen durch Dritte (zur späteren Verwendung gegen sie) oder das Unterbinden oder Verfälschen der Kommunikation zwischen zwei Nutzern (zum eigenen Vorteil)⁷¹.

Die bisher genannten Gründe liefen zumeist auf die dahinterstehende Bereicherungsabsicht (Diebstahl von Daten bzw. Informationen) hinaus. Dieser stellt jedoch nicht die Majorität an

⁷¹ Eine vollständigere Liste von Gründen findet sich in [Stallings 1995], S. 6, Tabelle 1.2

Angriffsmotiven dar. Andere Beweggründe können Faktoren wie Eitelkeit, Zerstörungsabsicht, aber auch (politische) Meinungsäußerung beinhalten.

Das Motiv der Bereicherung ist zunächst klar, hierbei geht es dem Angreifer um die illegale Beschaffung eines materiellen oder ideellen Gewinns. Die häufigsten Ausprägungen sind wahrscheinlich der Diebstahl „elektronischen“ Geldes, das unerlaubte Aneignen von fremdem geistigen Eigentum – z.B. in Form von Industriespionage – und der Kreditkartendiebstahl. Die letztere Form ist aufgrund ihrer einfachen Ausübung leider besonders verbreitet, da Kreditkartendaten⁷² i.d.R. zwar verschlüsselt über das Internet übertragen werden, jedoch nicht festgelegt ist, in welcher Form sie bei der erhaltenden Firma als Teil der Transaktionsdaten abgespeichert werden. Hierbei sind Fälle bekannt, in denen eben jene Kreditkartendaten unverschlüsselt auf dem ungeschützt im Internet stehenden Web-Server des Unternehmens abgelegt worden waren, so dass ein Angreifer lediglich einen Zugang auf den Server finden musste, um alle dort gespeicherten Kreditkartendaten zu erlangen.

Eitelkeit steht dagegen zumeist im Vordergrund, wenn es um das Erlangen einer bestimmten Berühmtheit in der Crackerszene gilt. Dieses Motiv treibt vor allem Neulinge und sogenannte „Skriptkiddies“⁷³, die Angreifer werden oft auch als „pubertierende männliche Jugendliche“ klassifiziert.

Angreifer, die dagegen aus Zerstörungswut handeln, setzen nach dem Einstieg in ein fremdes Computersystem alles daran, dieses für den Nutzer unbrauchbar zu machen. Dies erreichen sie durch das Aussetzen von destruktiven Viren, Formatieren von Datenträgern oder auch das gezielte Löschen offensichtlich persönlicher Daten des Systemnutzers. Da das Zerstören von fremdem Eigentum für diese Klasse Angreifer eine Art innere Befriedigung darstellt, kann man nur sehr schwer etwas gegen sie unternehmen. Ein Sonderfall der vorgenannten Gruppe stellt der „verärgerte Mitarbeiter“ da und zwar dahingehend, dass er es – im Gegensatz zum externen Cracker – aus dem Unternehmensintranet heraus wesentlich einfacher hat, Daten zu manipulieren oder zu zerstören⁷⁴.

Ein bisher nicht angeführtes, aber ebenso einfaches Motiv ist die Suche nach Wissen um die internen Funktionen von fremden Systemen. Dabei handelt es sich meistens um Administratoren oder Programmierer, die ihre Intelligenz und abstraktes Denken unter Beweis stellen wollen. Zumeist teilen sie das dabei gewonnene Wissen mit anderen, so dass bei einem solchen

⁷² Der Begriff „Kreditkartendaten“ umfasst dabei den Namen des Besitzers, die Nummer der Kreditkarte und deren Ablaufdatum. Diese Daten genügen bereits, um mit der Kreditkarte im Internet einzukaufen.

⁷³ Begriffe wie „Cracker“ oder „Skriptkiddies“ werden in den folgenden Abschnitten noch näher erläutert. Vorerst sollen diese nur der Seite der „Bösen“ im Internet zugeordnet werden.

⁷⁴ Der Einfluss von Mitarbeitern des Unternehmens auf sicherheitsrelevante Probleme wird noch im Kapitel „Interne Risiken“ (3.11) ausführlich behandelt werden.

Einbruch genutzte Sicherheitslücken in Systemen schnell publik werden. Genau genommen tragen diese Angreifer eher zum Prozess der Stärkung von Datensicherheit bei und werden daher als wertvolle Erkenntnisbringer für die Thematik Computer- und Netzwerksicherheit angesehen⁷⁵.

3.4.2 Auswahl eines geeigneten Angriffszieles

Natürlich wird ein Computersystem nicht in dem Moment als Angriffsziel interessant, in dem es eingeschaltet wird und einen Netzwerkzugang erhält⁷⁶. Vielmehr erfolgt – zumindest bei Privatpersonen oder kleineren Unternehmen – die zufällige Einbeziehung in eine Liste von IP-Adressen⁷⁷, die dann vom Angreifer der Reihe nach untersucht werden. Dies erfolgt in fast allen Fällen mit einem sogenannten „Portscanner“⁷⁸.

Der Begriff Portscanner bezeichnet ein Programm, das einen bestimmten Bereich von IP-Adressen und Ports auf deren Status (offen, geschlossen, gefiltert) untersucht. Die so entstehende Datenbasis kann der Angreifer zur Entscheidungsfindung nutzen, welche Computersysteme sich für einen Angriff eignen. Dabei geht er nach Kriterien wie vermutetes Betriebssystem, installierte (angebotene) Dienste und sich daraus ergebenden Sicherheitslücken vor. Einen Portscan auf einen beispielhaft ausgewählten Windows 2000 – Rechner zeigt die untenstehende Abbildung 3.3.

```
{The 1526 ports scanned but not shown below are in state: closed}
Port      State    Service
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    open     http
110/tcp   open     pop3
111/tcp   filtered sunrpc
135/tcp   open     loc-srv
139/tcp   open     netbios-ssn
161/tcp   filtered snmp
162/tcp   filtered snmptrap
445/tcp   open     microsoft-ds
1068/tcp  open     instl_bootc
1433/tcp  open     ms-sql-s
1993/tcp  filtered snmp-tcp-port
8007/tcp  open     jserv
8080/tcp  open     http-proxy
9876/tcp  open     <d

Remote OS guesses: Windows Me or Windows 2000 RC1 through final release, Windows Millenium Edition v4.90.3000
```

Abbildung 3.3 - Beispiel für einen Portscan mit dem Programm "nmap"

Quelle: eigene Darstellung

Selbst über eine Modem- oder ISDN-Wählleitung dauert ein solcher umfassender Portscan einer IP-Adresse nur Sekunden, außerdem filtert der Portscanner das Ergebnis bereits vor, so dass lediglich für eine Klassifizierung interessante Ports angezeigt werden. Ein solcher Scan wird zumeist nicht mit einer bestimmten IP-Adresse durchgeführt, sondern hat einen be-

⁷⁵ Vgl. zu den Motiven auch [anonymous 2001], S. 232 ff.

⁷⁶ Vgl. dazu [anonymous 2001], S. 216 ff.

⁷⁷ Begriffe wie IP-Adresse und Port wurden bereits im Kapitel „Das TCP/IP-Referenzmodell“ (2.3.2) ausführlich beschrieben und sollen hier nicht Gegenstand weiterer Erläuterungen sein.

⁷⁸ Beispiel für einen Portscanner ist das weit verbreitete „nmap“ (<http://www.nmap.org>)

stimmten Adressbereich zum Ziel. Die Ergebnisse kann der Angreifer in einer Datei ablegen und mit geeigneten Programmen weiter ausfiltern, bis er schließlich eine Liste mit endgültigen Angriffszielen erhält.

Welche Informationen lassen sich aus dem in Abbildung 3.3 gezeigten Portscan herauslesen? Man kann erkennen, dass auf dem betreffenden Rechner ein Microsoft SQL-Server (Zeile 1433/tcp, Dienstname ms-sql-s), ein beliebiger Webserver (Zeile 80/tcp, Dienst http) sowie viele weitere Dienste aktiv sind und auf eine Verbindungsanfrage warten. Außerdem hat „nmap“ den Typ des darauf laufenden Betriebssystems mit Windows 2000 oder Millennium Edition bereits eingegrenzt. Aufgrund weiterer gelisteter Ports (53, 25, 110) lässt sich mit fast vollständiger Sicherheit als Betriebssystem Windows 2000 bestimmen.

Hat der Angreifer auf die Weise ein Computersystem ausgewählt, muss er lediglich dieses System und die darauf laufenden Dienste mit den laufend aktualisierten Listen für bekannte Sicherheitsprobleme (Exploits) vergleichen und kann schließlich den Computer zielgenau angreifen. Hat der verantwortliche Systemadministrator für den zum Angriff benutzten Exploit noch keine Updates installiert, wird der Angreifer sicherlich Erfolg haben und in das System eindringen können.

Die große Tragweite dieses Sicherheitsproblems erkennt man u.a. daran, dass für die Ausnutzung eines Exploits i.d.R. bereits fertige Skripten und Programme für vielfältige Betriebssysteme vorliegen, aus denen der Angreifer nur noch auswählen muss. Außerdem existieren neben den reinen Portscannern auch spezielle Schwachstellen-Scanner⁷⁹, die ein beliebiges System auf bekannte Sicherheitslücken hin überprüfen, meist mit einem Hinweis zur Ausnutzung derselben kombiniert.

Neben den genannten gibt es noch weitere Faktoren, die einen Computer für einen Angriff interessant machen, und die größtenteils selbsterklärend sind. Dazu zählen z.B. die Bekanntheit eines Unternehmens (die Firma Microsoft gilt als beliebtes Angriffsziel) sowie die Frage, ob der Computer ständig oder nur zeitweise am Internet angeschlossen ist (Standleitung oder Wählleitung). Bei einer Wählleitung hat der Angreifer naturgemäß wenig Zeit, einen Angriff zu planen und auszuüben, außerdem erhält ein so an das Internet angebundenes Computersystem bei jeder Einwahl eine andere IP-Adresse, woraus eine gewisse Schutzwirkung resultiert.

3.4.3 Hacker und Cracker

Die beiden Begriffe werden häufig verwechselt und ihre Unterscheidung ist seit vielen Jahren ein heftiger Diskussionspunkt. Meist wird die Linie zwischen den beiden Bezeichnungen wie

⁷⁹ Schwachstellen-Scanner werden noch in Kapitel 4.4.1 ausführlich erläutert.

folgt gezogen: Hacker sind Individuen, welche zwar in fremde Computersysteme eindringen, jedoch nicht um Schaden anzurichten, sondern um Sicherheitsprobleme aufzudecken und die gewonnenen Erkenntnisse mit anderen zu teilen. Insofern rechnet man die Hacker zu den „guten“ Mitgliedern der Internetgemeinde⁸⁰. Viele von Ihnen sind als professionelle Berater in Sicherheitsfragen tätig. Cracker dagegen dringen in fremde Computersysteme ein mit der Absicht, diese zu schädigen, Daten zu manipulieren bzw. zu löschen und die Weiterarbeit des Systems unmöglich zu machen. Sie verhalten sich dabei meist so unauffällig wie möglich, um keine Spuren ihres Einbruchs zu hinterlassen. Cracker rechnet man also zur Seite der „Bösen“ im Internet. Beide Personengruppen verbindet i.d.R. ein langjähriges Verhältnis zu Computern und Programmierung, vor allem Netzwerksicherheit und –administration.

Obwohl viele eine andere Definition der beiden Begriffe gebrauchen, ist die genannte Einteilung sehr verbreitet, vielfach werden jedoch alle Personen, die in Computersysteme eindringen, ungeachtet ihrer Motivation als „Hacker“ bezeichnet und somit auch der Vorgang als solcher als „in ein System hacken“. Neben den beiden Gruppierungen lassen sich noch weitere Klassifizierungen von Eindringlingen in Computersysteme bilden, z.B. nach der Angriffsmethode oder den Angriffsmotiven⁸¹.

3.4.4 „Skriptkiddies“

Diese stellen den wohl zur Zeit erfolgreichsten Typ von Eindringlingen dar und können mit den vorhandenen Begriffen „Hacker“ bzw. „Cracker“ nicht ausreichend beschrieben bzw. klassifiziert werden. Meist handelt es sich hierbei um sehr junge Leute, die in der Internetgemeinde kursierende fertige Angriffs-Skripten von erfahrenen Crackern ausprobieren. Der Reiz des Verbotenen spielt hierbei wohl die wesentliche Rolle, er ist wahrscheinlich auch für die Beharrlichkeit und Ausdauer dieser Gruppe bei der Suche nach anfälligen Rechnern im Internet verantwortlich. Obwohl nur sehr wenige der von ihnen geführten Angriffe erfolgreich sind, richten sie aufgrund einer besonderen Boshaftigkeit der Mitglieder dieser Gruppe – die wahrscheinlich in nicht unerheblichem Maße aus einer gewissen Sorglosigkeit und Naivität gegenüber ihrem Tun entsteht – in einigen Fällen erheblichen Schaden an.

Selbst in der Gemeinde professioneller Cracker sind Skriptkiddies eher verachtet, da sie selbst keine (der zweifelhaften) Leistungen erbringen, sondern auf bestehende, von anderen erstellte Programme und Techniken zurückgreifen und diese zur ihrem eigenen Vorteil nutzen.

⁸⁰ Häufig werden die Guten auch als „White Hats“, die Bösen dagegen als „Black Hats“ bezeichnet, vgl. dazu auch [anonymous 2001], S. 224

⁸¹ Vgl. hierzu auch [Stallings 1995], S. 208

3.5 Spezielle Formen von Computer- und Netzwerkkriminalität

In den folgenden Abschnitten sollen die gebräuchlichen Formen, in denen Computer- und Netzwerkkriminalität speziell gesehen vorkommt, näher vorgestellt werden. Dazu zählen sowohl bekannten bösartige Programme wie Viren, Trojaner und Würmer als auch verschiedene Angriffsmethoden wie DoS-Angriffe und Spoofing.

3.5.1 Malware

Mit dem Begriff „Malware“ (kurz für Malicious Software) bezeichnet man gemeinhin jegliche Form von Software, welche eine „böartige Absicht“ verfolgt, d.h. deren Zweckbestimmung das vorsätzliche Anrichten eines definierten Schadens ist⁸². Eine genauere Definition besagt, dass es sich um Software oder Hardware handelt, welche vorsätzlich in ein System eingebracht wird zum Zwecke der Schädigung bzw. Außerkraftsetzung desselben und eines unautorisierten Zugriffs darauf. Hinter dem allgemeinen Begriff verbirgt sich meist ein kleiner und deswegen unauffälliger Programmcode, der im Internet meist in Form von sogenannten Viren, Trojanern oder Würmern kursiert⁸³.

Fast alle Formen von Malware sind dabei spezifisch für bestimmte Ausführungsumgebungen (Betriebssysteme, installierte Programme und Dienste) geschrieben.

3.5.1.1 Viren und Würmer

Gerade in Zeiten des Internets sind Viren und Würmer als häufigste Formen von Malware eine ernsthafte Sicherheitsbedrohung für jedes Computersystem⁸⁴. Besonders der massive Anstieg des täglichen e-Mail-Verkehrs führte zu Verbreitungsgeschwindigkeiten und einer Anzahl infizierter System, die vor der Entstehung weltumspannender, öffentlicher Netzwerke nicht für möglich erachtet wurden.

Von der Definition her ist ein Computervirus „ein Programm, das sich repliziert, indem es andere Programme »infiziert«, so dass diese eine (möglicherweise erweiterte) Kopie des Virus enthalten“⁸⁵. Die Arbeitsweise von Viren ist i.d.R. nicht daraufhin angelegt, dass bereits infizierte Wirtsprogramm zu zerstören, vielmehr wird der Virencode anstelle des normalen Codes des Wirtsprogramms zuerst ausgeführt und erst nach dessen Beendigung die Kontrolle dem Wirtsprogramm zurückgegeben. In der Definition wird zwar die Infizierung als Weg der Replikation beschrieben, nicht jedoch ein zwingend vorhandenes destruktives Merkmal.

⁸² Vgl. dazu Definition [Techtarget 2002 Malware]

⁸³ in [Stallings 1995], S. 238, findet sich eine grafische Darstellung der verschiedenen Typen von Malware, wobei nur die genannten drei Formen relativ bekannt und weithin verbreitet sind.

⁸⁴ Vgl. dazu auch [anonymous 2001], S. 400 ff.

⁸⁵ aus [anonymous 2001], S. 401

Trotzdem führt jeder Virus (oder Wurm) in dem von ihm infiziertem System zu eingeschränkten Systemressourcen, weiterhin verursachen sie in fast allen Fällen entweder unbeabsichtigte oder vorsätzliche Zerstörungen, wobei Fälle existieren, in denen Daten auf eine so subtile Weise modifiziert wurden, dass die Veränderung und damit die Infizierung des Systems erst lange nach ihrem Stattfinden bemerkt werden konnte. Einige an sich harmlose, da über keinerlei vorsätzliche zerstörerische Funktionalität verfügende Viren können aufgrund ihre bloßen Anwesenheit im System Probleme durch ungewollte Interaktionen mit installierten Diensten und laufenden Prozessen hervorrufen, so dass man nicht wirklich von „gutartigen“ und „böartigen“ Viren sprechen kann.

Im Computeralltag besonders relevant ist jedoch nicht die Anzahl an insgesamt weltweit verbreiteten Viren, sondern den als „In-the-Wild“ bezeichneten, z.Zt. einigen Hundert Viren umfassenden Gruppe, die in der ständig aktualisierten „Wildlist“ erfasst sind. Obwohl die Gesamtzahl aller Computerviren im Jahr 2001 zwischen 50000 und 60000 lag, sind nur diese ItW-Viren bzw. -Würmer wirklich bedeutsam.

Neben der am meisten verbreiteten Art von Viren – den Dateiviren – gibt es noch weitere, in der Praxis ebenso anzutreffende Arten. Hierzu zählen die Makroviren, besonders für Microsoft Office – Dokumente, die Skriptviren – normalerweise für die Sprache VBScript oder JavaScript sowie die Bootsektor-Viren, die mittlerweile allerdings eine eher unbedeutende Rolle spielen. Die meisten heutzutage vorkommenden Viren sind von ihrem Prinzip her gesehen „normale“ Dateiviren, d.h. sie infizieren bestimmte ausführbare Dateien im Betriebssystem und breiten sich auf diese Weise aus. Meist sind sie gekoppelt mit einer Komponente zur Verbreitung über Netzwerkstrukturen (z.B. Anhang an e-Mail-Programm).

Eine weitere Art von Viren sind sogenannte Hoaxes. Diese werden zwar als „memetische Viren“ bezeichnet, sind jedoch keine Viren im ursprünglichen Sinne, sondern von ihrer Natur her Kettenbriefe in Form von e-Mails, die mit einem ganz bestimmten, den Empfänger erschreckenden Betreff und ebensolchem Inhaltstext aufwarten. Sie beruhen auf der einfachen Intention, dass die jeweiligen Empfänger – wie in der Nachricht des Hoaxes verlangt – diese e-Mail an möglichst alle ihnen bekannten e-Mail-Adressen weiterleiten. Durch die entstehenden Massen von e-Mails werden häufig Mailserver überlastet und außer Kraft gesetzt, wodurch man dieser Art von Viren ebenfalls eine destruktive Wirkung zuschreiben kann. Sie sind jedoch keine Viren im eigentlichen Sinne, weil sie sich nicht ohne Benutzereinwirkung vermehren können.

Ein Wurm unterscheidet sich von einem Virus durch seine Fähigkeit, sich selbsttätig über Netzwerke oder verteilte Systeme zu replizieren, ohne (wie der Virus) dafür ein legitimes

Trägerprogramm zu benötigen⁸⁶. Genau wie bei Hoaxes kann es bei Würmern durch die Produktion eines großen e-Mail-Aufkommens zu einer Überlastung und Außerkraftsetzung von Mailservern kommen. Die Einteilung in Viren und Würmer kann bei neueren Exemplaren nicht mehr vollständig vorgenommen werden, da auch sogenannte „Virus/Wurm-Hybriden“ existieren. Viele Würmer fallen heutzutage in diese Kategorie. Da sich Würmer meistens nur mit Benutzerbeteiligung replizieren können (z.B. die heutigen VBScript-Würmer), wird eine Interaktionsstrategie mit dem Benutzer erforderlich. Hierfür werden dem Nutzer oft falsche Inhalte eines e-Mail-Anhanges suggeriert, die ihn dazu verleiten sollen, diesen auszuführen. Neben der Installation und ständigen Aktualisierung eines Antivirus-Programms besteht das einzige wirksame Mittel im Kampf gegen eine Infektion mit einem Virus oder Wurm in der Nichtausführung von unbekanntem Dateianhängen in e-Mails. Dies gilt insbesondere dann, wenn die e-Mail von einem gänzlich Unbekannten kommt oder der Anhang einen sicherheitstechnisch problematischen Typ besitzt (ausführbare Dateien, Bildschirmschoner, Skriptdateien).

3.5.1.2 Trojanische Pferde

Der Begriff „trojanisches Pferd“ (oder kurz „Trojaner“) sagt schon einiges über das Wesen dieser Malware-Form aus: Es handelt sich hierbei um ein „Programm, das vorgibt, eine wünschenswerte oder notwendige Funktion auszuführen und das möglicherweise auch tut, aber außerdem eine oder mehrere Funktionen ausführt, die die Person, die das Programm ausführt, weder erwartet noch wünscht“⁸⁷. Trojaner lassen sich dabei in drei Kategorien klassifizieren. Zum einen gibt es Programme, die unerlaubten (unautorisierten) Zugriff auf Informationen erhalten wollen, wobei diese sich vor allem auf Passwörter oder andere persönliche Daten spezialisiert haben. Andere wollen eine bestimmte Verfügbarkeit unterbinden (z.B. einen Dienst abschalten). Der dritten Kategorie gehören Programme an, die ohne eine vorherige Autorisierung Daten und Systeme modifizieren oder zerstören wollen.

Problematisch ist vor allem die Abgrenzung, ob ein bestimmtes Programm ein Trojaner ist oder nicht. Die Einordnung soll daran erfolgen, ob ein Programm genau das tut, was der Benutzer von ihm erwartet hat. Niemand kann jedoch genau sagen, was der Benutzer von einem Programm genau erwartet, daher ist eine Abgrenzung nicht besonders scharf umrissen.

Eine sehr gefährliche Art von Trojanern stellen – auch als „Remote Access Tools“ bezeichnete – Programme wie Netbus und BackOrifice dar, da es sich dabei scheinbar um ganz legale Programme zur Systemadministration und Fernwartung bzw. –steuerung von Computersys-

⁸⁶ Vgl. dazu [anonymous 2001], S. 403

⁸⁷ aus [anonymous 2001], S. 433

temen handelt. Hierbei wird ein Server auf dem Rechner des Opfers installiert, der auf einem bestimmten Port auf die Konnektierung eines zugehörigen Clients – den des Angreifers - wartet. Diese Programme werden auch als „Hintertür-Trojaner“ bezeichnet.

Eine weitere Variante stellen die sogenannten „Rootkits“, Sammlungen von mit Trojanern versetzten Systemprogrammen, dar. Mit deren Hilfe kann ein Eindringling ohne Superuser-Rechte⁸⁸ eigentlich geschützte Systemprogramme mit modifizierten Versionen ersetzen, die dann beispielsweise Passwörter im System ausspionieren. Zu den Rootkit-Programmen gehören fast immer spezielle Versionen von bestimmten Standard-Werkzeugen, die z.B. nicht legitime Prozesse vor dem Benutzer verbergen und Einträge in Log-Protokollen modifizieren oder löschen. Rootkits für das UNIX-basierte Betriebssysteme werden noch ausführlich in Kapitel 3.9.2 vorgestellt.

Eine letzte Ausprägung von Trojanern, welche als „DDoS-Tools“⁸⁹ bezeichnet werden, sind häufig mit den oben angeführten Rootkits verwoben, um ihre eigene Existenz zu verbergen. Diese Tools sind nach der Installation zunächst inaktiv und warten auf einen zentralisiert gegebenen Befehl zum Angriff des als Opfer ausgesuchten Internetserver.

Zum Schutz vor trojanischen Pferden gilt – da diese meist per e-Mail, gekoppelt mit einem Wurm oder Virus verschickt werden – dass der Benutzer, gerade in einem ansonsten geschützten Unternehmensintranet, keine Dateianhänge öffnen oder speichern darf, von deren Sicherheit er nicht vollständig überzeugt ist. Mit den beschriebenen Antivirus-Programmen (und deren heuristischen Erkennungsmaßnahmen) sind Trojaner meist nur schwer zu entdecken, so kann es durchaus sein, dass ein nicht erkannter Trojaner zu einer vollständigen Unterwanderung eines Systems führen kann. Bevor er entdeckt und beseitigt wird, kann der diesen Trojaner benutzende Cracker bereits weitere Hintertüren installiert haben – als einzige Möglichkeit bleibt dann die Neueinrichtung des kompletten Systems.

Als wirksames Mittel gegen die gesamte Malicious Software bietet sich das Ermitteln und Ablegen von sogenannten Prüfsummen („digitaler Fingerabdruck“) für jede Datei des zu untersuchenden Systems an, wobei die Erstellung der Prüfsummen zu einem Zeitpunkt stattfinden muss, an dem das System noch keinen Kontakt mit einem irgendwie gearteten Netzwerk

⁸⁸ Superuser bezeichnet allgemeinen den Benutzeraccount, welcher generell über alle Rechte im System verfügt und der ob dieser Rechte auch besonders gefährdet ist (oft wird versucht, diesen Account zu cracken). Unter Windows NT/2000 heißt dieser Account „Administrator“, unter UNIX/Linux-Varianten „root“. Andere Betriebssysteme haben weitere Bezeichnungen, i.d.R. ist ein solcher Benutzeraccount jedoch immer existent.

⁸⁹ DDoS ist die Abkürzung für „Distributed Denial of Service“ und bezeichnet die von mehreren, meist gecrackten Rechnern ablaufende gezielte Überlastung eines Internetserver (Mailserver, Webserver) mit immer neuen Verbindungsanfragen. Diese Technik der Paketüberflutung wird auch als „Flooding“ bezeichnet.

hatte. Die dafür verwendeten Funktionalitäten werden noch ausführlich in Kapitel 3.9.2 besprochen werden.

3.5.2 „Spoofing“

Mit „Spoofing“ bezeichnet man die vorsätzlich falsche Authentifizierung an einem System mit Hilfe gefälschter Datenpakete, wodurch man diesem System eine andere Herkunft (IP-Adresse) bzw. Identität (Benutzername) vorspiegelt. Meist werden dafür vertrauenswürdige Absenderinformationen verwendet⁹⁰.

In diesem Kapitel werden die zwei Begriffe „Vertrauensstellung zwischen zwei Computern“ sowie „Authentifizierung“ näher beleuchtet. Der erstere Begriff steht hierbei für die Art der Beziehung zwischen zwei Computern, der letztere hingegen für die gegenseitige Identifizierung und das mögliche Nachprüfen der dabei angegebenen Identitäten.

Der Prozess der Authentifizierung menschlicher Nutzer gegenüber einem Computersystem ist hinlänglich bekannt, es handelt sich hierbei zumeist um die Eingabe einer Benutzername / Passwort – Kombination⁹¹. Meist werden diese Daten auf unverschlüsseltem Wege zwischen den zwei am Authentifizierungsprozess verwendeten Parteien (Benutzer und entfernter Computer) übertragen, nur in einigen Fällen kommt eine verschlüsselte Verbindung zum Tragen. Dies wird noch in Kapitel 3.7 ausführlich erläutert.

Die Authentifizierung zwischen zwei Computersystemen funktioniert dagegen auf andere Art. Hier wird häufig eine Identifizierung aufgrund von IP-Adressen oder Hostnamen vorgenommen. Bei dem auf UNIX-Systemen immer noch gebräuchlichen RHOSTS-System wird über zuvor in speziellen Dateien festgelegten IP-Adressen bzw. dazugehörigen Hostnamen bestimmten Rechnern und deren Benutzern eine uneingeschränkte Vertrauensstellung eingeräumt, d.h. diese Benutzer (bzw. Computer) können sich mit dem betreffenden System ohne irgendeinen vorgelagerten Authentifizierungsmechanismus verbinden. Für eine solche Verbindung stehen dem Angreifer verschiedene Anwendungen zur Verfügung, die häufig auch als „r-Dienste“ bezeichnet werden. Diese Remote-Anwendungen umfassen die Dienste Login zum Initiieren einer Anmeldesitzung, Shell und Command zur entfernten Befehlsausführung sowie Copy zum Kopieren von Dateien zwischen dem lokalen und dem entfernten System⁹².

⁹⁰ Vgl. dazu [anonymous 2001], S. 164 ff.

⁹¹ Die Kombination Name/Passwort steht dabei meist für einen künstlichen Benutzernamen, z.B. auch eine e-Mail-Adresse oder eine Kundennummer, welcher ein bestimmtes Passwort zugeordnet ist. In jedem Fall identifiziert der für die Authentifizierung verwendete Name auf dem jeweiligen System eindeutig einen bestimmten Benutzer. Man spricht hier auch von einem (Benutzer-)Account. Vgl. dazu auch [anonymous 2001], S. 164 f.

⁹² Die genannten Remote-Anwendungen werden über die Eingabe der Befehle rlogin, rsh, rcmd und rcp auf dem lokalen System angesprochen. Für die Authentifizierung, d.h. die Überprüfung der Vertrauensstellung gegenüber dem entfernten Computersystem wird ausschließlich das RHOSTS-System verwendet.

Der Angreifer braucht somit nur dem entfernten System eine andere, demjenigen vertraute Identität vorzuspiegeln und erlangt allein daraufhin vollständigen Zugriff auf dessen Ressourcen. Basierend auf dem schon beschriebenen Aufbauverfahren einer TCP-Verbindung⁹³ muss der Angreifer die folgenden zwei Probleme lösen: Erstens muss er die Ausgangsadresse der Verbindung fälschen (IP-Adresse) und zweitens die zur Herstellung einer TCP-Verbindung bereits hinlänglich erklärten Initial Sequence Numbers (ISN) berechnen bzw. erraten.

Zunächst einmal identifiziert der Angreifer seine potenziellen Angriffsziele und legt daraufhin den Host still, welcher er zu sein vorgeben will. Dies ist notwendig, weil alle Antwortpakete nicht an den Rechner des Angreifers, sondern an den Rechner, dessen Identität übernommen wurde, geleitet werden und dessen Reaktion darauf den Angriff unmöglich machen würde. Genauso sieht der Angreifer nicht den Paketaustausch zwischen den beiden angesprochenen Systemen, deswegen wird die Methode häufig als „blindes Spoofing“ bezeichnet. Das Stilllegen dieses Computersystems wird zumeist mit einer Art Überlastung vorgenommen, dem sogenannten SYN-Flooding⁹⁴. Vor dem letzten Schritt muss der Angreifer mehrere Testverbindungen zum Zielsystem durchführen, wobei er von diesem jedes Mal entsprechende Sequenznummern für die Verbindung genannt bekommt. Diese Sequenznummern werden auf dem System des Angreifers protokolliert und die Verbindung wird wieder getrennt. Der Angreifer versucht nun, mithilfe von bestimmten Algorithmen die Abfolge der Sequenznummern vorausszusehen. Wenn er dies erreicht hat, kann er zuverlässig voraussagen, welche Sequenznummern für eine künftige Authentifizierung zum Einsatz kommen. Nun stellt er wiederum eine Verbindung zum ausgesuchten Zielsystem her und gibt sich dabei als der von ihm stillgelegte Computer (IP-Adresse) aus. Die Verbindung kommt – aufgrund der zuvor ermittelten Sequenznummer – zustande. Ein letzter Schritt besteht nun meist im Eintragen der realen IP-Adresse des angreifenden Rechners in die RHOSTS-Dateien des Zielsystems und somit in der Schaffung eines bequemeren Zugangs des Angreifers zum Zielsystem.

Angriffe, die auf IP-Spoofing basieren, können z.B. auch für das sogenannte „Session Hijacking“, d.h. das Entwenden einer bestehenden TCP-Verbindung genutzt werden. Insbesondere sind UNIX-basierende Systeme anfällig für alle Arten des IP-Spoofing. Hier hilft nur die Deaktivierung der Dienste, die über IP-Adressen eine Vertrauensstellung anbieten. Neben den

⁹³ Vgl. dazu Kapitel 2.3.2

⁹⁴ SYN-Flooding ist eine Methode des DoS (Denial of Service) und hat die vollständige Blockierung des angegriffenen Systems zum Ziel, so dass dieses keine Anfragen mehr beantworten kann. Eine genaue Beschreibung der Methode findet sich im nächsten Abschnitt 3.5.3. Im Moment reicht es aus zu wissen, dass der auf diese Weise angegriffene Rechner für einen gewissen Zeitraum nicht mehr in der Lage ist, auf eingehende Pakete zu antworten.

genannten R-Diensten betrifft dies vor allem (Sun-) RPC-Dienste⁹⁵ und das grafische X-Window-System des Massachusetts Institute of Technology (MIT). Einen wirksamen Schutz vor IP-Spoofing bietet neben der angesprochenen Deaktivierung betroffener Dienste, und somit dem Abschalten der für Angreifer interessanten Ziele, eine saubere Netzwerkkonfiguration. Hierzu kann man sagen, dass ein Netzwerk prinzipiell so konfiguriert werden sollte, dass es Pakete aus dem Internet zurückweist, die eine lokale Absenderadresse vorweisen (und umgekehrt). Generell sollten netzwerkfremde Hosts niemals als vertrauenswürdig im Sinne des RHOSTS-Systems erachtet werden, da eine wirkliche Kontrolle der Identität außerhalb des Intranets nicht sicher erscheint.

Bereits seit 1995 stellt das Spoofing eine ständig anwachsende Angriffsmethode dar, wobei die Zielsysteme meist Nameserver und Routersysteme sind. Besonders das DNS-Spoofing als Sonderform des Spoofing ist eine erfolgreiche Methode. Hierbei werden vom Angreifer die Tabellen, welche für die Auflösung von Hostnamen (wie www.microsoft.com) zu IP-Adressen (wie 1.2.3.4) zuständig sind, derart abgeändert, dass ein bekannter und vertrauenswürdiger Hostname statt zu der real zugeordneten IP-Adresse auf den Rechner des Angreifers zeigt. Somit wird bei Eingabe dieses Hostnamens der Rechner des Angreifers statt dem vertrauenswürdigen Zielsystem angesprochen. Wenn der Angriff nicht sofort bemerkt wird, hat DNS-Spoofing sehr weitreichende Folgen. Da die für das DNS-System zuständigen Server in bestimmten Zeitabständen eine Synchronisation ihrer Datenbanken durchführen, können sich die gefälschten DNS-Tabellen über mehrere Server verteilen und somit eine Behebung des Problems stark verzögern.

Eine damit verwandte Sonderform des Spoofing wird als ARP-Spoofing bezeichnet und hat die Auflösung von IP-Adressen zu Hardwareadressen (MAC-Adressen) zum Angriffsziel⁹⁶.

3.5.3 DoS-Attacken

Die bereits kurz vorgestellten DoS-Attacken (Denial of Service, Dienstverweigerung) stellen eine der am meisten verbreiteten Sicherheitsprobleme im Bereich der Netzwerke dar. Ihr Ziel ist in jedem Fall die Außerkraftsetzung eines bestimmten Systems oder Dienstes. Diese wird z.B. durch einen übermäßigen Datenstrom verursacht, der zu einer gewollten Überlastung des betreffenden Dienstes oder auch einer bestimmten Netzwerkverbindung führt.

Meist tritt ein solcher Angriff in Form einer „DDoS-Methode“ (Distributed DoS, verteilter DoS) auf. Bei dieser Form attackieren mehrere Rechner gleichzeitig und koordiniert das als

⁹⁵ Das RPC-System von Sun Microsystems bietet einen Standard für den entfernten Aufruf von Systemprozeduren (Remote Procedure Calls) und ist in RFC 1057 definiert, vgl. dazu auch <http://www.ietf.org/rfc/rfc1057.txt>.

⁹⁶ Vgl. dazu [anonymous 2001], S. 176 f.

Angriffsziel ausgesuchte Computersystem, was die korrekte Identifizierung der angreifenden Rechner fast unmöglich macht. Die zwei Engpässe bei einer DoS-Attacke stellen prinzipiell die Netzwerkanbindung des betroffenen Systems sowie seine Leistungsfähigkeit, eingehende Anfragen zu beantworten, dar. Kommt es bei einem der beiden zu einer Überlastung, ist das betroffene System für eine bestimmte Zeit nicht in der Lage, gestellte Anfragen zu beantworten⁹⁷.

Die erste bedeutende DoS-Attacke stellte 1988 der Morris-Wurm dar, welcher für einige Stunden 5000 Rechner von Universitäts- und Forschungseinrichtungen lahm legte. Im Gegensatz zu damals, wo außer den betroffenen Einrichtungen niemand den Angriff bemerkte, werden vergleichbare DoS-Attacken gegen bedeutende Webseiten wie Yahoo! oder Amazon.com (so geschehen im Februar 2000) in Minutenschnelle populär und ziehen Verluste in Millionenhöhe nach sich. DoS-Angriffe kommen heutzutage sehr oft vor, wobei ein wichtiger Grund dafür wohl die Existenz vielfältiger Hilfsprogramme für die Initiierung eines solchen Angriffs gibt. Diese Programme zielen zumeist auf die nicht oder schlecht implementierten Sicherheitsfunktionen in bestimmten Betriebssystemen ab.

Ein DoS-Angriff hat charakteristisch mindestens eine der folgenden Erscheinungen zur Folge: Bandbreitenverschwendung, Ressourcensättigung sowie die Herbeiführung von System- und Anwendungsabstürzen⁹⁸.

Der Begriff Bandbreitenverschwendung umfasst dabei die Überschreitung einer für jede Art von Netzwerkverbindung existente maximale (endliche) Menge von Daten, welche über diese Netzwerkverbindung transportiert werden können, wobei sich der Term Netzwerkverbindung sowohl auf Leitungen als auch auf Verbindungsknoten wie Router oder Switches bezieht. Generell ist dieser Typ von Angriffen aktiver Natur, d.h. die blockierten Verbindungen sind nur solange nicht verfügbar, wie der Bandbreitenkonsum aktiv stattfindet.

Der zweite Begriff, Ressourcensättigung, kann analog dem ersten aufgezeigt werden, wobei es sich bei den betroffenen Komponenten hierbei um Computersysteme handelt. Auch diese verfügen nur über eine endliche Anzahl von sogenannten Ressourcen (Prozessorleistung, Speicherkapazität etc.). Wenn eine dieser Ressourcen vollständig belegt ist, sind für andere Anwendungen des Systems keine nutzbaren Kapazitäten mehr verfügbar. Eine bekannte Methode dieser DoS-Angriffe ist das bereits vorgestellte „SYN-Flooding“, bei dem der betroffene Rechner mit Verbindungsanfragen überschwemmt wird, was zu einer Belegung aller verfügbaren Netzwerkressourcen des Systems führt. Hierbei werden an das Angriffsziel vermehrt

⁹⁷ Vgl. dazu [anonymous 2001], S. 227 und 374 ff.

⁹⁸ aus [anonymous 2001], S. 375

TCP-SYN-Pakete mit ungültigen Absenderadressen übermittelt, woraufhin der Server für jede dieser Anfragen ein SYN-ACK-Paket sendet. Da er auf diese Pakete aufgrund der ungültigen Absenderadressen keine Antworten erhält, wartet er eine bestimmte definierte Zeitspanne ab, bevor er die sogenannte „halboffene“ Verbindung schließlich von sich aus beendet (Timeout-Prinzip). Da der Timeout i.d.R. eine längere Zeitspanne darstellt, sammeln sich in kurzer Zeit viele halboffene Verbindungen an, wodurch der Server neue, gültige Verbindungsanfragen nicht mehr akzeptiert. Ein besonders beliebtes Ziel für solche DoS-Attacken sind Webserver, die für jede auszuliefernde Webseite meist mehrere Einzelverbindungen aufrechterhalten müssen, z.B. wird jedes auf der Webseite enthaltene Bild auf einer einzelnen Verbindung übertragen. Eine Verteidigung gegen diese Art DoS-Angriffe ist meist nicht möglich, da eine automatisierte Entscheidung, ob es sich bei den Ursprüngen der TCP-Pakete um ein nicht erreichbares System handelt, unmöglich ist.

Weitere DoS-Angriffe, die ebenfalls auf den Verbrauch von Systemressourcen abzielen, sind z.B. Mailbomben. Hierbei wird meist an eine Mailbox eines Benutzers eine große Menge (Hunderte oder Tausende) e-Mails versandt, was im Endeffekt dazu führt, dass die ankommenden Daten die zur Verfügung stehende Festplattenkapazität des Systems übersteigen. Als Folge davon kann (im günstigsten Fall) der betroffene Benutzer, meist aber alle auf dem Computersystem registrierten Nutzer keine e-Mails mehr empfangen. Im schlimmsten Fall, wenn der zuständige Administrator keine entsprechend differenzierte Partitionierung⁹⁹ der Festplattenkapazität vorgenommen hat, kann dadurch auch das Betriebssystem selbst keine Daten mehr schreiben, ein Systemabsturz wäre die Folge.

Die dritte der genannten Arten, die Herbeiführung von System- und Anwendungsabstürzen, ist eine Variante, bei der sich der Angreifer bekannte Programmierfehler in einer Anwendung ausnutzt, um durch bestimmte Datenpakete¹⁰⁰, die an das Zielsystem gesandt werden, diese zum Absturz zu bringen. Solche Programmierfehler werden auch als „Exploits“ bezeichnet. Das schon in Kapitel 3.1 beschriebene CERT Coordination Center erhält täglich bis zu 200 Meldungen über Sicherheitslöcher in Betriebssystemen und Anwendungen und übernimmt dahingehend auch eine Koordinationsfunktion für die Hersteller der betroffenen Systeme und Anwendungen, die für die möglichst schnelle Bereitstellung entsprechender aktualisierter Software, sogenannter Updates oder Patches, sorgen.

⁹⁹ Die Partitionierung, d.h. Aufteilung der zur Verfügung stehenden Festplattenkapazität ist eine wichtige systemadministratorische Aufgabe, die bereits bei der Einrichtung des Systems bedacht werden sollte.

¹⁰⁰ Hierbei handelt es sich zumeist um Datenpakete, die nicht der jeweiligen Norm entsprechen, wofür aber in der entsprechenden Anwendung eine adäquate Fehlerbehandlung fehlt.

3.5.4 Interne Attacken

Unter dem Begriff „interne Attacken“ versteht man keine eigene Art, vielmehr dient er als Sammelbegriff für alle möglichen Arten von Angriffen, die aus dem internen Netz (zumeist einer Unternehmung) heraus auf Computersysteme eben dieser Firma initiiert werden. Hierbei ist nicht ein entfernt arbeitender Cracker – wie sich die meisten Systemadministratoren den schlimmsten anzunehmenden Feind vorstellen – der Gegenspieler, sondern vielmehr ein, meist unzufriedener, Mitarbeiter aus den eigenen Reihen. Diese Art von Angriffen kann technisch gesehen wiederum ein trojanisches Pferd sein, eine logische Bombe u.a., wichtig ist hier nur der Ursprungsort der Attacke. Interne Attacken kommen häufiger vor als jede Form des externen Angriffs, sind i.d.R. erheblich gefährlicher und werden entweder gar nicht oder erst lange nach ihrer Ausführung entdeckt, da die meisten Sicherheitssysteme auf einen Angriff von außerhalb des Unternehmensnetzwerks ausgerichtet sind. Auf interne Attacken wird noch ausführlich in Kapitel 3.11 eingegangen.

3.5.5 „Social Engineering“

Mit dem Begriff „Social Engineering“ bezeichnet man das bewusste Einwirken eines Angreifers auf firmeninterne Mitarbeiter, welches die Herausgabe sensibler Daten, z.B. Zugriffscodes, Passwörter oder auch von Informationen selbst zum Ziel hat. Die Mitarbeiter werden dabei nicht zur Herausgabe gezwungen (zumindest fällt dies nicht unter den Begriff), der Angreifer setzt vielmehr auf eine gezielte „Überzeugung“ der Mitarbeiter. Zusammenfassen könnte man es unter dem Begriff „clevere Manipulation der menschlichen Gewohnheit Vertrauen¹⁰¹“. Meist handelt es sich dabei um Methoden wie „Systemadministrator, ich habe mein Passwort vergessen, weisen Sie mir doch bitte ein neues zu.“ oder „Mein Schlüssel / meine Identifikationskarte liegt leider zu Hause, lassen Sie mich doch bitte herein.“ Die meisten dieser Tricks funktionieren, der Mensch ist somit das schwächste Glied in der Sicherheitskette eines Unternehmens.

Meist wird Social Engineering entsprechend vorbereitet, so dass der Angreifer informiert ist über Namen, Verantwortlichkeiten, Telefonnummern oder Urlaubszeiten. Diese Informationen werden dann beim eigentlichen Prozess des Social Engineering zur Vorspiegelung einer internen Wissensbasis über das Unternehmen und seine Mitarbeiter genutzt. Die meisten dieser Angriffe werden über Telefon geführt, wobei der Angreifer häufig zusätzlich seine Stimme verstellt. Besonders anfällig sind Mitarbeiter des in fast jeder Firma vorhandenen technischen Support (Help Desk), besonders wenn dieser für die unternehmensinternen Mitarbeiter

¹⁰¹ Vgl. dazu [SecurityFocus 2001]

arbeitet. Die dortigen Angestellten werden geradezu trainiert, besonders freundlich und zuvorkommend zu sein und stellen somit ein ideales Ziel für Social Engineering dar.

Eine abgewandelte Form stellt das „Reverse Social Engineering“ dar, bei dem der Angreifer eine hohe verantwortliche Rolle vorspielt. Ein Beispiel hierfür wäre die absichtliche Zerstörung eines Netzwerks durch den Angreifer, der sich dann selbst als Problemlöser anbietet – und nebenbei die Informationen aus dem Netzwerk mitnimmt, wegen denen er ursprünglich gekommen war.

3.6 Authentifizierung und Autorisierung

In diesem Kapitel sollen die verschiedenen gebräuchlichen Authentifizierungs- und Autorisierungsmechanismen vorgestellt werden, wobei zunächst eine genaue Klärung dieser beiden Begriffe notwendig erscheint.

Authentifizierung steht gemeinhin für das Überprüfen der Identität eines bestimmten Benutzers oder Hosts, wobei diese meist einfach gehalten ist und auf der Anwendungsebene erfolgt (Eingabe einer Kombination aus Benutzername und Passwort)¹⁰². Allerdings kann die Authentifizierung auf diesem Wege nicht gewährleisten, dass der sich authentifizierende Benutzer tatsächlich die damit in Verbindung stehende Identität besitzt. Somit ist die Definition für herkömmliche Passwortverfahren zu weitflächig. Bekannte Authentifizierungsverfahren sind zum einen die bekannte Passwortmethode, weiterhin z.B. persönliche Identifikationsnummern (PIN), Einmalpasswörter, Public-Key-Verfahren, Chipkarten sowie biometrische Verfahren. In dieser Arbeit soll sich auf die wichtigsten zwei Verfahren beschränkt werden: die passwortgestützten und Key-Exchange Mechanismen.

Die Autorisierung ist der Authentifizierung logisch nachfolgend, sie wiederum bezeichnet die entsprechend granulare Rechtevergabe für einen bereits gegenüber dem System authentifizierten Benutzer.

3.6.1 Passwortgestützte Mechanismen

Dieser Abschnitt soll zur Einführung in die Thematik der passwort- oder kennwortgeschützten Authentifizierung dienen. Heutzutage werden Passwörter für alle möglichen Zwecke verwendet, einige Beispiele stellen die Anmeldung am Computer oder Netzwerk, das Einloggen am Mailserver oder die Vergabe von Passwörtern zum Schutz von Office-Dokumenten dar¹⁰³. Man könnte Passwörter als die vorderste Front in der Verteidigung gegen Eindringlinge be-

¹⁰² aus [anonymous 2001], S. 977

¹⁰³ Vgl. dazu [anonymous 2001], S. 320 ff.

zeichnen¹⁰⁴. Fast jedes Mehrbenutzersystem baut heutzutage auf der Anmeldung des Benutzers durch eine Kombination aus Benutzername (häufig auch als User-Account bezeichnet) und einem dazugehörigen Passwort. Der User-Account bestimmt dabei, ob der betreffende Benutzer überhaupt Zugang zu dem Computersystem besitzt und spielt außerdem eine wichtige Rolle in nachgeordneten Autorisierungsmechanismen¹⁰⁵.

Die Passwörter werden auf verschiedenen Betriebssystemen und für verschiedene Anwendungen auf die unterschiedlichsten Arten berechnet, so dass man keine generelle Aussage über die Verwundbarkeit dieser von passwortgestützten Mechanismen genutzten Algorithmen geben kann. Auf eventuell bei bestimmten Betriebssystemen oder Anwendungen dahingehend vorhandene Sicherheitsprobleme wird noch in Kapitel 3.9 näher eingegangen werden. Das schwächste Glied in dieser Beziehung ist jedoch nicht technischer Art, vielmehr stellt der Mensch mit seiner Auswahl von Passwörtern ein bekanntes „Sicherheitsproblem“ dar. Leider gibt es nur bei sehr wenigen Unternehmen klare Vorgaben für die Beschaffenheit, z.B. Länge, Aufbau und mögliche Wortähnlichkeiten von Passwörtern. Für die Auswahl von Passwörtern gibt es einige Grundregeln, die im Folgenden erläutern werden sollen.

Zwei Parameter bestimmen dabei die Qualität, d.h. die Verwundbarkeit eines Passwortes, zum einen ist dies die Passwortlänge, zum anderen die Vermeidung eines Wortes aus dem eigenen Umfeld, einem Wörterbuch oder einer anderen bekannten Wortliste. Bei einem diesbezüglichen Stichprobentest mit fast 14000 Passwörtern besaßen immerhin 3 Prozent von ihnen eine Länge von drei Stellen oder weniger. Solche kurzen Passwörter sind sogar mit sogenannten „Brute-Force-Angriffen“¹⁰⁶ innerhalb kürzester Zeit zu entschlüsseln, daher sollte für jede Software gelten, dass sie ein Passwort nur dann als gültig anerkennt, wenn dieses eine Länge von mindestens acht Zeichen besitzt. Eine solche Sicherheitspolitik wäre sicherlich in den meisten Unternehmen durchsetzbar.

Der zweite Aspekt ist erheblich diffiziler zu betrachten, nämlich die Qualität der als Passwort ausgesuchten Zeichenfolge. Viele Benutzer verwenden hier eine der folgenden Möglichkeiten: ihren eigenen Benutzernamen, Nachnamen oder Vornamen, ihr Geburtsdatum, oft auch die entsprechenden Daten von ihrer Frau oder ihren Kindern. Ebenso beliebt sind Automarke, Haustier, Lieblingessen, Wörter aus dem Systemhandbuch oder allgemeinen Wörterbüchern. Dies bietet dem Angreifer eine zwar große, aber endliche Wortliste als Grundlage für einen

¹⁰⁴ Vgl. dazu [Stallings 1995], S. 213 ff.

¹⁰⁵ Auf Autorisierungsmechanismen wird noch im Kapitel „Zugriffskontrolle“ (3.6.3) eingegangen.

¹⁰⁶ „Brute-Force-Angriffe“ stellen eine recht einfach gestrickte Methode zur Passwortentschlüsselung dar. Hierbei wird einfach jede mögliche Kombination von Buchstaben, Zahlen sowie diversen Sonderzeichen bis zu einer spezifizierten Passwortlänge getestet, egal ob die dadurch zufällig entstehenden Zeichenfolgen einen Sinn ergeben oder nicht.

sogenannten „Wörterbuchangriff“. Bei diesem wird jedes Wort dieser Liste (auch in einigen Permutationen) mit dem gleichen Algorithmus verschlüsselt wie die zu testenden Passwörter. Der Angreifer muss nun nur noch die dabei entstehenden verschlüsselten Passwörter mit der Datenbank des Systems vergleichen. Findet er eine Übereinstimmung, ist die zu diesem verschlüsselten Passwort gehörige Klartextphrase entschlüsselt. Auf diese Art konnten ca. 25 Prozent der oben beschriebenen 14000 Passwörter ermittelt werden¹⁰⁷.

Ein wirklich vollkommen zufälliges Passwort zu wählen, kommt im Regelfalle nicht in Frage, da sich ein solches fast unmöglich merken lässt. Nachahmenswerte Passwortstrategien beinhalten z.B. die Auswahl einer Zeichenfolge aus den jeweils ersten Buchstaben eines Satzes oder eines Liedes und zwar einschließlich der Groß- und Kleinschreibung sowie Interpunktion¹⁰⁸. Ein solches Passwort kann weder über Brute-Force-Angriffe (aufgrund der zu großen Länge) noch über Wortlisten (da diese Phrase mit Sicherheit nicht darin vorkommt) entschlüsselt werden und stellt dahingehend eine sehr sichere Passwortwahl dar¹⁰⁹.

In fast allen Betriebssystemen werden heutzutage Hash-Funktionen benutzt, Passwörter standardmäßig zu verschlüsseln¹¹⁰. Lediglich in älteren UNIX-basierten Systemen wird noch das konventionelle Verschlüsselungsverfahren DES (Data Encryption Standard)¹¹¹ benutzt, während in neueren Systemen dafür das Hash-Verfahren MD5 (Message Digest, Version 5) zum Einsatz kommt.

Zur Charakteristik einer Einweg-Hash-Funktion zählt, dass es unmöglich ist, aus dem erzeugten Hash-Wert den ursprünglichen Klartext wiederzuerlangen, dieser ist nicht einmal darin enthalten. Stattdessen wird die Identitätsprüfung durch die erneute Anwendung der Hash-Funktion auf das vom Benutzer eingegebene Passwort und einen anschließenden Vergleich des dabei erzeugten Wertes mit dem abgespeicherten Hash-Wert, zumeist in einer Passwortdatei, vorgenommen. MD5¹¹² wird in RFC 1321 beschrieben und ist ursprünglich für die Integritätsprüfung von Dateien durch die Erzeugung eines passenden digitalen Fingerabdrucks entwickelt worden.

¹⁰⁷ Vgl. dazu [Stallings 1995], S. 217, Tabelle 6.2

¹⁰⁸ Zum Beispiel würde man aus dem Lied „Er gehört zu mir, wie mein Name an der Tür...“ das folgende, leicht zu merkende Passwort codieren: „Egzm,wmNadT“.

¹⁰⁹ Neben Kriterien für die sichere Auswahl eines Passwortes existieren noch generelle Richtlinien für den Umgang mit Passwörtern, nachzulesen unter [Stallings 1995], S. 225, Tabelle 6.4

¹¹⁰ Vgl. dazu [anonymous 2001], S. 325 f.

¹¹¹ DES wird im Kapitel „Verschlüsselungsverfahren“ (4.4.3) noch ausführlicher vorgestellt.

¹¹² Vgl. zur Funktionsweise [Stallings 1995], S. 286 ff.

3.6.2 Key Exchange – Verfahren

Eine zweite, wesentlich weniger verbreitete Authentifizierungsmethode stellen die sogenannten „Key Exchange – Verfahren“ dar. Einer der meistgenutzten Vertreter dieser Methoden ist das vom MIT entwickelte Kerberos, welches auf der Anwendungsebene arbeitet und auf einem System von Tickets und vertrauenswürdigen Authentifizierungsservern basiert¹¹³.

Kerberos wurde für den Einsatz in offenen verteilten Umgebungen konzipiert, somit für Szenarien, in denen verschiedene Nutzer eine Workstation nutzen und die Identität eines Benutzers nicht anhand des Computersystems festgestellt werden kann¹¹⁴. Die Authentifizierung läuft über einen zentralen Server, der sowohl Benutzer gegenüber Servern als auch Server gegenüber Benutzern authentifizieren kann, wobei das Schema komplett auf konventioneller Verschlüsselung beruht. Kerberos liegt mittlerweile in der Version 5 vor, wobei die mit einigen Sicherheitsdefiziten belastete Vorgängerversion 4 immer noch einschlägig verbreitet ist.

Das Verfahren beruht dabei auf einem sehr strengen Sicherheitsansatz: Benutzer müssen sich für jeden Dienst, den sie in Anspruch nehmen wollen, identifizieren. Umgekehrt implementiert Kerberos auch eine Identifikation der Server gegenüber den Clients. Außerdem achteten die Entwickler von Kerberos auf verschiedene Grundsätze: Das System sollte umfassende Sicherheit dahingehend bieten, dass ein Netzwerkniffer keine verwertbaren Daten beziehen kann, der Dienst sollte vollständig redundant ausgelegt sein und somit ein ausgefallener Authentifizierungsserver automatisch durch ein Backupsystem ersetzt werden. Außerdem sollte der Prozess der Authentifizierung für den Benutzer – bis auf die Eingabe seines Passworts – transparent erscheinen. Kerberos ist dabei aufgrund seiner modularen Struktur hoch skalierbar und kann eine große Anzahl von Clients und Servern verwalten.

Da das Konzept von Kerberos auf einem uneingeschränkten Vertrauensverhältnis (sowohl der Clients als auch der Server) gegenüber den zur Authentifizierung verwendeten Servern beruht, müssen diese in besonderer Weise vor unbefugtem Zugriff geschützt werden.

Ein weiteres Verfahren stellt der Verzeichnisdienst X.509 (X.509 Directory Service) dar, der an dieser Stelle nicht weiter beschrieben werden soll¹¹⁵.

3.6.3 Zugriffskontrolle (Autorisierung) in vernetzten Systemen

Der Begriff Zugriffskontrolle vereint gemeinhin alle Mittel, Geräte oder Techniken, mit der eine zentrale Stelle (i.d.R. ein Administrator) Benutzern den Zugriff auf eine bestimmte Res-

¹¹³ aus [anonymous 2001], S. 983

¹¹⁴ Vgl. dazu [Stallings 1995], S. 315 ff., insbesondere auch das Schema eines Authentifizierungsvorgangs (S. 321 ff.)

¹¹⁵ Weiterführende Informationen finden sich in [Stallings 1995], S. 333 ff.

source erlauben oder verweigern kann. Dabei kann der Term Ressource sowohl für Dateien oder Verzeichnisse als auch für einen Server insgesamt oder sogar ein Netzwerk stehen¹¹⁶.

Die Zugriffskontrolle ist dabei i.d.R. dem Authentifizierungsvorgang nachgeordnet und wird auch als Autorisierung bezeichnet. Beide Begriffe sind miteinander verwandt in der Hinsicht, dass jeder Benutzer eine bestimmte, mit seinem Benutzernamen verknüpfte primäre Gruppenzugehörigkeit besitzt, die in vielen Fällen bereits eine grobe Zugriffskontrolle für Systemressourcen beinhaltet.

Um eine Zugriffskontrolle auf Netzwerke zu erreichen, wird zumeist das detaillierte Regelwerk einer Firewall benutzt, da der Schnittpunkt zweier oder mehrerer Netzwerke die besten Möglichkeiten zu einer entsprechend fein granulierten Zugriffssteuerung bietet. Die Klassifizierung von erlaubten und zu verweigernden Zugriffen wird dabei nach IP-Adressen, angesprochenen Diensten (Ports), Benutzernamen sowie möglicherweise zusätzlichen Aspekten wie Tag, Uhrzeit oder Anzahl der bereits getätigten Zugriffe vorgenommen.

Die meisten Betriebssysteme unterstützen die Aufstellung von Benutzerrechten für allgemeine Gruppen (wie „jeder authentifizierte Benutzer“), spezielle Gruppen (Administratoren, Bereich Controlling, Bereich Vertrieb u.a.) sowie für einzelne Benutzer. Dazu zählen alle UNIX-basierten Betriebssysteme, die Windows-Versionen NT, 2000 und XP Professional von Microsoft sowie das Netzwerkbetriebssystem Novell NetWare. Die Festlegung von Zugriffsrechten auf bestimmte Dateien und Ordner eines Laufwerks muss dabei vom darunter liegenden Dateisystem unterstützt werden.

Einige Betriebssysteme, z.B. Windows 95/98 und Millennium Edition von Microsoft bieten keinerlei dateibasierte Zugriffskontrolle an und sind dahingehend nicht für eine Mehrbenutzerumgebung geeignet.

Die bei der Erstellung von Zugriffsrichtlinien zu beachtenden Aspekte – hinsichtlich Eigentümern und Zugriffsrechten von Dateien – werden am Beispiel von UNIX in Kapitel 3.9.2 ausführlicher beschrieben.

3.7 Risiken durch installierte Software

Ein bestimmtes Computersystem wird, wie schon in Kapitel 3.4.1 angemerkt, durch die von ihm angebotenen Dienste für einen Angreifer interessant. Somit sollte ein wichtiger Grundsatz der Systemadministration darin bestehen, ausschließlich die Dienste auf einem System zu aktivieren, die für seine Funktion innerhalb des Netzwerks wirklich erforderlich sind. Man

¹¹⁶ aus [anonymous 2001], S. 989

kann sogar noch weiter argumentieren und für eine Deinstallation nicht benötigter Software, insbesondere Serverprogramme, plädieren.

Jedes Programm, das auf einem Server (oder auch Client) ausgeführt wird, enthält in der Regel Sicherheitslücken – es ist nur eine Frage der Zeit, bis diese entdeckt werden. Somit kommt der aktiven Beobachtung der sogenannten BUGTRAQ-Mailingliste¹¹⁷ oder den von verschiedenen Stellen herausgegebenen Sicherheitsbulletins eine große Bedeutung zu.

Zur näheren Betrachtung von Risiken durch installierte Software ist zunächst eine Differenzierung nach serverseitigen und clientseitigen Risiken empfehlenswert. Ein als Server fungierendes (d.h. bestimmte Dienste anbietendes) Computersystem kann auch Clientfunktionalitäten besitzen, z.B. beim Initiieren einer FTP-Verbindung durch den dort angemeldeten Systemadministrator. Umgekehrt kann eine Workstation (eigentlich Client) bestimmte wohldefinierte Dienste anbieten, z.B. die Freigabe eines an diesem System angeschlossenen Druckers für alle Netzwerkteilnehmer. In dem Moment, wo ein anderer Benutzer im Netzwerk auf diesen Drucker zugreift, fungiert die eigentliche Workstation als Server.

Bei der Absicherung eines Computersystems hinsichtlich der darauf installierten Software ist daher die vorherige genaue Feststellung, welche Dienste auf dem System angeboten werden (sollen) sowie deren Festschreibung und Versionsbestimmung der einzelnen Programme ein essentieller Schritt. In den meisten kleinen und mittleren Unternehmen existiert hierzu jedoch keinerlei Dokumentation, so dass eine genaue Bestimmung der Anfälligkeit installierter Software für erkannte Sicherheitslücken nur mit großem Aufwand möglich ist. Die Aufstellung sollte zwingend den Hersteller des Programms und eine Lokation für entsprechende Updates beinhalten. Bei Linux-Systemen handelt es sich dabei i.d.R. um den Anbieter der jeweiligen Distribution.

Eine schnelle Übersicht über möglicherweise bei Computersystemen vorhandene fehlerhafte Software bieten sogenannte „Schwachstellen-Scanner“, die noch in Kapitel 4.4.1 ausführlich vorgestellt werden.

¹¹⁷ Mailinglisten stellen einen automatisierten Informationsservice dar, der im Versenden von e-Mails an eine Gruppe von vorher definierten e-Mail-Adressen besteht. Die hinter den e-Mail-Adressen stehenden Benutzer haben die Mailingliste zuvor abonniert und wurden somit in den Verteiler aufgenommen. Es gibt Tausende Mailinglisten, wobei jede einen bestimmten Themenkreis abdeckt. Die genannte BUGTRAQ-Mailingliste berichtet bei Bekanntwerden von Sicherheitslücken in einer zusammenfassenden e-Mail über betroffene Programme und deren Versionen, Art des Angriffes und gibt auch einige Hinweise zum einstweiligen Sichern des Systems. Die gefundenen Sicherheitslöcher werden dabei als Bug bezeichnet. Im Gegensatz zu einschlägigen schwarzen Brettern von Crackern sind in der dabei versandten e-Mail keine Informationen über Möglichkeiten zur Ausnutzung des Bugs in Form von veröffentlichtem Code enthalten. Diese, als Exploits bezeichneten Programme zur Profitierung von solchen Schwachstellen, werden jedoch sehr schnell nach Bekanntwerden einer neuen Sicherheitslücke auf Cracker-Seiten zum Download bereitgestellt. Die BUGTRAQ-Mailingliste kann man unter <http://www.securityfocus.com/forums/bugtraq/intro.html> abonnieren.

3.7.1 SANS-Liste

Die SANS-Gruppe bietet eine ständig aktualisierte „Top-20-Liste“ der schwerwiegendsten Sicherheitslücken in Computernetzwerken auf ihrer Webseite an¹¹⁸. Diese Liste stellt Schwachstellen nach verschiedenen Kategorien (Generelle Probleme, Windows-Systeme, UNIX-Systeme) geordnet dar, wobei die darin genannten sicherheitsrelevanten Probleme die wichtigsten Ansatzpunkte für Systemadministratoren bei der Absicherung ihrer Computersysteme bilden sollten.

Die SANS-Liste benennt die folgenden Zustände als sicherheitstechnisch generell bedenklich: bei der Installation des Betriebssystems oder systemnaher Software mitinstallierte, jedoch nicht benötigte Programme und Dienste, die zumeist noch beim Systemstart automatisch gestartet werden und unnötige Ports im System öffnen (Punkte G.1 und G.4 der SANS-Liste), schwache, nicht gesetzte bzw. auf einem eventuellen Standardwert belassene Passwörter (Punkt G.2, siehe auch Kapitel 3.6.1), die Vernachlässigung einer regelmäßigen Datensicherung (Punkt G.3), inkorrekte Filterregeln bzgl. der Blockierung von IP-Adressbereichen auf einer Firewall (Punkt G.5) sowie ein nicht-existentes oder unpassendes Mitprotokollieren von Systeminformationen (Logging, Punkt G.6). Die unter Punkt G.7 in der SANS-Liste stehenden Schwachpunkte von CGI-Programmen¹¹⁹ auf Webservern werden in Kapitel 3.7.2.6 besprochen.

In den nachfolgenden Abschnitten sollen wichtige serverseitige Dienste sowie clientseitige Applikationen vorgestellt werden, die – zumeist unabhängig vom jeweiligen Betriebssystem – bekannte Sicherheitsprobleme mit sich bringen. Somit handelt es sich bei den vorgestellten Aspekten nicht um einzelne bekannt gewordene Exploits, sondern aufgrund ihrer Funktionalitäten generell sicherheitsrelevante Programme.

3.7.2 Serverseitige Dienste

Einige von Servern häufig angebotene Dienste sind als potenziell gefährlich anzusehen und sollten daher nur bei absoluter Notwendigkeit aktiviert werden. In besonders sicherheitssensiblen Umgebungen sollten diese Programme zusätzlich von den betreffenden Computersystemen deinstalliert werden.

¹¹⁸ Die Liste kann unter <http://www.sans.org/top20.htm> abgerufen werden.

¹¹⁹ CGI steht für „Common Gateway Interface“ und beschreibt eine von jedem Webserver unterstützte und gängige Technik zum Einbinden verschiedener interaktiver Komponenten wie Formulare, Statistikgrafiken, etc. in Webseiten.

3.7.2.1 Telnet und Secure Shell (SSH)

Das Telnet-Protokoll, definiert in RFC 854, bietet einen Netzwerkdienst für die virtuelle Terminalemulation für Clients im Netzwerk an, d.h. der Benutzer erhält auf seinem Client eine Arbeitsumgebung, die so agiert, als wäre der Nutzer direkt am entfernten Computer angemeldet. Der Telnet-Client verbindet sich dabei von einem unprivilegierten Port¹²⁰ aus mit dem Port 23 des Servers. Die Authentifizierung des Benutzers erfolgt dabei über eine Benutzername / Passwort – Kombination, wobei der Benutzer für die Authentifizierung einen gültigen Account auf dem Server haben muss und die eingegebenen Anmeldedaten mit den diesem Account zugeordneten Daten identisch sein müssen.

Ein Telnet-Server ist als extrem unsicher¹²¹ zu betrachten, da alle Daten – Benutzername, Passwort, eingegebene Befehle, Antworten vom Server – unverschlüsselt über die Netzwerkverbindung zwischen den beiden Computersystemen übertragen werden. Durch ein Abhören des Datenverkehrs auf dieser Netzwerkverbindung könnte sich ein Angreifer die im Klartext gesendeten Anmeldedaten aneignen. Solch ein Angriff wird seiner Art nach als „Man in the Middle – Attack“ bezeichnet. Der Angreifer hätte mittels dieser Benutzerdaten freien Zugang zum System, das Ausnutzen einer eventuellen Sicherheitslücke durch einen Exploit ist nicht mehr nötig. Einmal im System, kann der Angreifer leicht andere Benutzerkonten anlegen, unerwünschte Dienste starten, die ihm einen unbegrenzten Zugang sichern und Systemdateien durch gefälschte Versionen ersetzen. Diese Tatsache macht Telnet grundsätzlich für Umgebungen unbrauchbar, in denen die Sicherheit der dem gesamten Datenübertragungsweg zugrunde liegenden Netzwerke nicht gewährleistet werden kann.

Eine weitere Sicherheitslücke des Telnet-Dienstes besteht in der Anzeige eines sogenannten „Banners“ bei der Anmeldung eines Benutzers am Server. Dieses zeigt – am Beispiel einer aktuellen Linux-Distribution – standardmäßig Versionsnummer und Name des Betriebssystems, die Version des Linux-Kernels sowie die Architektur des Servers an. Ein Angreifer kann diese Informationen zur sogenannten „Reconnaissance“, dem Auskundschaften des Zielsystems nutzen, wobei diese Daten i.d.R. eine größere Genauigkeit bieten als die in Kapitel 3.4.1 bei einem Portscan gelisteten Informationen. Die einzige Möglichkeit der Absicherung besteht in der Abschaltung der Banneranzeige, diese ist jedoch den meisten Systemadministratoren

¹²⁰ Alle Ports von 1 – 1024 werden als sogenannte privilegierte Ports bezeichnet, weil Dienste, die an diesen Ports den Netzverkehr abhören, mit root-Rechten ausgeführt werden müssen. Diese, nur unter UNIX-basierten Betriebssystemen vorhandene Einschränkung ist dadurch begründet, dass kein anderer Benutzer bestimmte gefälschte Server wie Telnet oder DNS auf dem dafür bestimmten Port anbieten kann. Benutzer könnten sich in so einem Fall mit dem gefälschten Server verbinden und würden beim Login ihre Passwörter preisgeben. Ports mit Nummern über 1024 werden dagegen als unprivilegierte Ports bezeichnet. Vgl. dazu auch [anonymous 2001], S. 566 ff.

¹²¹ Vgl. dazu [anonymous 2001], S. 570 ff.

ratoren nicht bekannt¹²². Bei Telnet-Servern, die keine Möglichkeit zur Abschaltung des Banners bieten, besteht die einzige Möglichkeit in einem manuellen Überschreiben des Banners in der ausführbaren Datei. Das dahinterliegende Betriebssystem lässt sich zwar trotzdem noch annähernd bestimmen (über Auswertung empfangener Datenströme beim Login-Prozess), für weniger erfahrene Angreifer, z.B. die bereits erwähnten „Skriptkiddies“ ist eine solche Systemanalyse meist schon zu aufwendig, womit trotz allem ein gewisser Schutzeffekt erreicht wird.

Die einzige sichere Variante von Telnet besteht jedoch in der Deaktivierung des Dienstes – wenn möglich, sollte auch die für den Server zuständige ausführbare Datei vom System entfernt werden. Es existieren heutzutage sichere Alternativen zu Telnet, welche funktional dazu identisch sind und ausschließlich eine verschlüsselte Datenübertragung unterstützen. Die meistgenutzte Alternative stellt dabei die Secure Shell (SSH) dar, die für fast alle Betriebssysteme in Client- und Serverversionen zur Verfügung steht.

3.7.2.2 File Transfer Protocol (FTP)

Das FTP-Protokoll¹²³ – spezifiziert in RFC 959 – stellt einen Standard für die Übertragung von Dateien dar und ist damit einer der ältesten Dienste im Internet. Ein FTP-Client verbindet sich von einem unprivilegierten Port aus mit einem auf – dem FTP-Dienst zugeordneten – Port 21 laufenden FTP-Server eines beliebigen Computersystems. Grundsätzlich existieren bei Servern, die einen FTP-Dienst anbieten, die bereits im letzten Kapitel erwähnten Risiken bezüglich der unverschlüsselten Datenübertragung sowie zur Anzeige eines Banners beim Einloggen eines Benutzers. Das FTP-Protokoll stellt Systemadministratoren jedoch vor weitere Probleme, die in sicherheitsrelevanten Umgebungen vor der Entscheidung des Anbietens eines FTP-Dienstes geklärt werden sollten. Dies betrifft vor allem die bei „aktivem FTP“ standardmäßige Benutzung von zwei TCP-Verbindungen auf unterschiedlichen Ports bei der Übertragung von Dateien per FTP. Die zweite Verbindung – initiiert vom Port 20 des angesprochenen Servers zu einem unprivilegierten Port auf dem Client stellt für Firewall-Systeme eine Konfigurationshürde dar, da die Firewall die Kontrollverbindung korrekt decodieren müsste, um den dabei angesprochenen Port auf dem Client zu ermitteln und ihn dynamisch freizuschalten. Eine einfache, auf Paketfiltern beruhende Firewall vermag eine solche Funktionalität jedoch nicht zu leisten, ihr fehlt dabei die erforderliche Intelligenz des Anwendungsschichtprotokolls. In diesem Fall müsste das Firewall-System so konfiguriert sein, von jedem

¹²² Die mit den heutigen modernen Linux-Distributionen ausgelieferten Telnet-Server können mit der Startoption „-h“ zur Unterdrückung der Banneranzeige gebracht werden.

¹²³ Vgl. dazu auch [anonymous 2001], S. 577 ff.

Host im Internet (Port 20) eine Verbindungsiniiierung zu einem System im lokalen Netzwerk (beliebiger unprivilegiertes Port) zuzulassen. Diese Konfiguration ist in einer sicherheitsrelevanten Umgebung jedoch nicht tragbar. Eine Umgehung bietet die Verwendung von sogenanntem „passiven FTP“, wodurch der Client selbst eine beliebige Portnummer berechnet und die Datenverbindung, diesmal zu einem unprivilegierten Port auf dem FTP-Server, vom gesicherten lokalen Netzwerk aus aufbaut.

Das Anbieten eines öffentlich zugänglichen FTP-Servers sollte aus den beschriebenen Gründen auf einem dedizierten, d.h. nur diesem einen Zweck dienenden, Computersystem erfolgen. Eine weitere wichtige Regel besteht in der Einschränkung sowohl der Clients, die diesen Dienst nutzen dürfen (IP-Adresse)¹²⁴, als auch der für eine FTP-Anmeldung zugelassenen Benutzer. In dieser Beziehung zeigen viele Implementierungen von FTP-Servern eine für viele Systemadministratoren verwirrende Konfiguration – in einer speziellen Textdatei werden diejenigen Nutzer aufgeführt, die für eine FTP-Anmeldung nicht erlaubt sein sollen. Diese Vorgehensweise widerspricht dem Prinzip der Mindestprivilegien, da ein neu angelegter Nutzer somit standardmäßig eine Zugriffserlaubnis über FTP erhält.

Wie schon bei Telnet, existiert keine wirkliche sichere Variante, einen FTP-Server im Unternehmensnetzwerk zu betreiben. Er stellt im Gegensatz sogar eine weitergehende Sicherheitslücke für eigentlich sichere Dienste wie SSH dar – wenn für FTP- und SSH-Zugriffe die gleichen Benutzeraccounts und Passwörter verwendet werden. In solch einer Konstellation kann der Angreifer unverschlüsselt übertragene FTP-Anmeldedaten dazu nutzen, um sich über den eigentlich sicheren Secure Shell-Dienst mit dem Zielsystem zu verbinden.

Eine mit dem FTP-Protokoll verwandte Implementierung stellt das Trivial FTP-Protokoll (TFTP) dar, welches ohne eine Authentifizierung arbeitet und z.B. zum Herunterladen von Systemsoftware für festplattenlose Workstations (Thin Clients) oder Netzwerkgeräte wie Switches dient. Eine Sicherung dieses Protokolls ist nicht möglich, so dass ein Aktivieren nur in einer gesicherten Umgebung und bei unbedingter Notwendigkeit gegeben ist.

3.7.2.3 Simple Mail Transfer Protocol (SMTP)

Das in RFC 821 spezifizierte SMTP-Protokoll bietet einige sicherheitsproblematische Funktionen an¹²⁵, die bei entsprechender Fehlkonfiguration des Systemadministrators von Angreifern zur Kompromittierung des Systems genutzt werden können.

¹²⁴ Trotz dieser Maßnahme ist der FTP-Server dann anfällig gegenüber einem Zugriff mit gefälschten Ursprungsadressen (IP-Spoofing), vgl. dazu Kapitel 3.5.2

¹²⁵ Vgl. dazu [anonymous 2001], S. 582 ff.

Einer der wichtigsten Schwachpunkte im ursprünglichen SMTP-Protokoll liegt in der Unmöglichkeit der Authentifizierung von Benutzern, die ihre e-Mail über den Server versenden wollen. Erst vor einigen Jahren wurde diese in einer Erweiterung des Protokolls um wichtige Sicherheitsaspekte, wie z.B. auch eine verschlüsselte Datenübertragung, eingeführt. Diese sind jedoch aufgrund der gewünschten Abwärtskompatibilität, nicht zwingend zur Verwendung festgelegt und können dadurch umgangen werden. Zudem können RFC-konforme SMTP-Server mit bestimmten Befehlen (VRFY, EXPN) zur Preisgabe existierender Benutzernamen gebracht werden, eine für Angreifer wichtige Information für das spätere Eindringen in das Zielsystem.

Zusammenfassend kann man sagen, dass ein SMTP-Dienst nur dann auf einem System aktiviert werden sollte, wenn die Funktionalität der Entgegennahme von e-Mails für Benutzer auf dem System benötigt wird. Das Versenden von e-Mail dagegen benötigt nicht zwingend einen aktivierten lokalen SMTP-Server, stattdessen kann auf die Dienste des Internet Service Providers zurückgegriffen werden.

3.7.2.4 Domain Name Service (DNS)

Dem DNS-Protokoll kommt im Internet eine besondere Bedeutung zu – es ist zuständig für die Auflösung von sogenannten „Fully Qualified Domain Names“ (FQDN, z.B. support.microsoft.com) zu IP-Adressen (z.B. 1.2.3.4) und umgekehrt. Aufgrund dieser Bedeutung ist DNS einer der wichtigsten Teile der Infrastruktur im Internet, ein Ausfall bereits einzelner Knoten der DNS-Struktur kann weitreichende Folgen haben.

Das DNS-Protokoll selbst spezifiziert in der Originalrevision keinerlei Sicherheitsregeln, da seine Aufgabe als eine Art „öffentliche Datenbasis“ gesehen wurde. Entsprechende Zugriffsrestriktionen auf die per DNS verfügbaren Daten wurden in verschiedenen Implementierungen des DNS-Protokolls verwirklicht, trotzdem sind sie nicht Bestandteil des Protokolls selbst.

Ein Beispiel für Sicherheitsprobleme des Protokolls findet sich im „DNS-Spoofing“, welches bereits in Kapitel 3.5.2 erläutert wurde. Weiterhin implementieren fast alle DNS-Server die als Erweiterung zur ursprünglichen Definition in RFC 2136 und 2137 spezifizierte dynamische Aktualisierung von DNS-Einträgen, von denen beispielsweise bei der dynamischen Zuordnung von IP-Adressen in einem lokalen Netzwerk Gebrauch gemacht wird. Diese Updates sollten nur von vertrauenswürdigen IP-Adressbereichen entgegengenommen werden, um dem

Risiko einer Fälschung von DNS-Einträgen entgegenzuwirken. Trotzdem ist die so implementierte Form noch immer anfällig gegenüber IP-Spoofing¹²⁶.

Als Folge der Aufdeckung der genannten Sicherheitsprobleme wurde 1994 von der Internet Engineering Task Force (IETF)¹²⁷ eine Erweiterung des ursprünglichen Protokollstandards um sicherheitsrelevante Aspekte beschlossen und eine entsprechende Arbeitsgruppe eingerichtet. Bis auf das als „Information Leakage“ bekannte Problem der unbeabsichtigten Preisgabe der Beschaffenheit interner Netzwerkstrukturen¹²⁸ werden durch die in RFC 2535 definierte, DNSSEC genannte Erweiterung, vorhandene Sicherheitsprobleme beseitigt. Die DNSSEC-Erweiterungen sind dabei abwärtskompatibel zum bisherigen Protokoll, so dass nicht DNSSEC-fähige Server trotz allem Anfragen weiterleiten und beantworten können.

Generell gilt – analog der Überlegungen zu SMTP-Diensten – dass das Anbieten eines DNS-Dienstes nur nach reiflicher Überlegung der Thematik geschehen sollte, im Zweifelsfall sollte man auch hier auf die Dienste des Internet Service Providers zurückgreifen.

3.7.2.5 Simple Network Management Protocol (SNMP)

Das SNMP-Protokoll¹²⁹ wird in Netzwerken weithin zur Überwachung und zum Management des Netzverkehrs benutzt. Es liegt mittlerweile in zwei Versionen, SNMPv1 und SNMPv2 vor, beide sind gleichermaßen verbreitet.

Das Risiko der Aktivierung eines SNMP-Dienstes (SNMP-Agent genannt), z.B. zur Überwachung eines Webservers, liegt in den standardmäßig vergebenen sogenannten „Community Names“, die ähnlich wie Passwörter funktionieren. Meist werden sie auf den Standardwerten belassen, so dass ein Angreifer sich leicht mit einem laufenden SNMP-Agenten verbinden kann. Die Community Names kommen in den beiden Ausprägungen „Lesezugriff“ und „Lese-/Schreibzugriff“ vor, wobei die letztere Form häufig sogar den Neustart eines Gerätes oder Computersystems erlaubt. Der Zugriff auf SNMP-Agenten wird dabei standardmäßig nicht protokolliert, so dass eine Nachverfolgung von Zugriffen fast unmöglich ist.

Da SNMP nur in den wenigsten Fällen benötigt wird, sollte es in sicherheitskritischen Umgebungen nicht aktiviert werden. In einigen Situationen, wie z.B. dem Betrieb eines verteilten

¹²⁶ Die Auflistung der im Zusammenhang mit dem DNS-Protokoll relevanten Sicherheitsprobleme ist keineswegs als vollständig anzusehen, eine detaillierte Beschreibung der Protokollschwachstellen findet sich in [Dawidowicz 1999].

¹²⁷ <http://www.ietf.org>

¹²⁸ Diese Schwäche ist jedoch nicht auf das Protokoll selbst, sondern auf die grundlegende Definition der DNS-Struktur zurückzuführen.

¹²⁹ Vgl. dazu [anonymous 2001], S. 589 f.

Systems oder Clusters¹³⁰, ist die Verwendung von SNMP-Agenten jedoch zwingend erforderlich, da über SNMP die Zustände und Auslastungsdaten der einzelnen Systemkomponenten ausgetauscht werden. Hier sollte der Systemadministrator möglichst lange Community Names verwenden und zusätzlich SNMP-Traps¹³¹ zur Authentifizierung definieren, um einen Angriff frühzeitig erkennen zu können.

3.7.2.6 HyperText Transfer Protocol (HTTP)

Das HTTP-Protokoll ist in seiner ursprünglichen Version 1.0 in RFC 1945 spezifiziert. Mittlerweile liegt das Protokoll in Version 1.1 (RFC 2068) vor und bildet gemeinhin die Grundlage für das den meisten Benutzern bekannte „Surfen“ auf Webseiten im Internet.

Eine mit dem HTTP-Protokoll zusammenhängende Schwachstelle bilden die auf Webservern im Internet laufenden CGI-Programme oder –Skripte, die aufgrund ihrer direkten Verbindung zu dem darunter liegenden Betriebssystem eine sehr sensible Schnittstelle darstellen. Die Ausnutzung eventuell vorhandener Schwachpunkte verschafft dem Angreifer somit dieselben Zugriffsrechte, die der Webserver selbst besitzt.

Besonders anfällig hierfür sind standardmäßig bei der Installation des Webservers mitkopierte CGI-Skripte, die zumeist dem Testen der Funktionalität des installierten Systems dienen sollen. Diese Skripte sind Angreifern von ihrem Namen her zumeist hinlänglich bekannt und sollten daher nach der Installation vom System entfernt werden.

3.7.3 Clientseitige Applikationen

In diesem Abschnitt soll auf die bei Arbeitsplatzrechnern innerhalb einer Unternehmung installierten Applikationen und die von ihnen ausgehende Gefährdung, sowohl für die daran arbeitenden Benutzer als auch für das Unternehmen selbst, näher eingegangen werden.

Analog zu Kapitel 3.7.2 sind in diesem Abschnitt nur diejenigen Applikationen gelistet, welche unabhängig vom Betriebssystem sicherheitsrelevante Aspekte aufweisen. Dies betrifft vor allem die für mehrere Systeme verfügbaren Internet-Browser und die damit verwandten Skriptsprachen. Einen weiteren, sehr sensiblen Angriffspunkt bilden die auf Arbeitsplatzrechnern installierten e-Mail-Programme (Mail User Agents, MUA). In den meisten Fällen kommen hier die Programme Microsoft Outlook (Express) sowie Netscape Messenger zum Ein-

¹³⁰ Als Cluster bezeichnet man verteilte Systeme, die aus mehreren, voneinander logisch unabhängigen Computern bestehen, jedoch als ein großes Computersystem auftreten.

¹³¹ SNMP-Traps haben ihre Bezeichnung von der Fähigkeit, wie eine Falle zu wirken, die – bei ihrer Auslösung durch ein definiertes Ereignis (wie z.B. eine fehlgeschlagene Authentifizierung) – eine entsprechende Reaktion verursacht (z.B. die Information des Systemadministrators). Nähere Informationen zu SNMP finden sich in [Stallings 1995], S. 412 ff.

satz. Eventuell vorhandene Sicherheitslöcher in diesen Anwendungen bilden eine Öffnung für Viren und Würmer, die daraufhin schnell weitere Computersysteme im Intranet infizieren können. Hier ist unbedingt auf eine entsprechende Absicherung durch regelmäßige Aktualisierung der Software zu achten.

3.7.3.1 Browsertechnologien, Skriptsprachen

Der Internet-Browser als eine Art „Fenster zum Internet“ ist für die tägliche Informationsbeschaffung als Arbeitsmittel unentbehrlich geworden und auf fast jedem Computersystem einer Firma installiert. Die genauen Produkte differieren dabei sowohl zwischen als auch innerhalb der Unternehmen, was aufgrund der unterschiedlichen Funktionsumfänge und damit zusammenhängender Sicherheitsprobleme die Administrierung erheblich erschwert.

Den am häufigsten installierten Internet-Browser stellt dabei der Internet Explorer von Microsoft dar, wobei die verwendeten Versionen von 2.0 bis 6.0 reichen. Dabei ist grundsätzlich zu sagen, dass Versionsnummern kleiner als 5.0 für einen Einsatz nicht zu empfehlen sind, da Microsoft bereits seit 10.08.2000 keinerlei Sicherheitsupdates dafür zur Verfügung stellt¹³².

Der am zweithäufigsten anzutreffende Internet-Browser ist der von der Firma Netscape vertriebene Navigator, allerdings ist seine Verbreitung in Unternehmen wesentlich geringer. Im Gegensatz zu Microsofts Internet Explorer gibt es von Netscape keine zentrale Webseite, wo Sicherheitsupdates für den Navigator angeboten werden. Der Netscape-Benutzer muss sich im Fall einer sicherheitsrelevanten Schwachstelle stattdessen die komplette aktuelle Version des Navigator herunterladen. Obwohl für diesen – verglichen mit dem Internet Explorer – erheblich weniger Sicherheitsprobleme bekannt werden, erscheint das Produkt aufgrund der erschwerten Aktualisierung für einen professionellen Einsatz im Unternehmen ungeeignet.

Neben der ständigen Aktualisierung der verwendeten Technologien ist die Durchsetzung einer zentralen Sicherheitsrichtlinie betreffend die Einstellungen des Internet Explorer oder Navigator und deren Skriptsprachen im Unternehmen anzuraten. Dies geschieht bei Microsoft über die Erstellung eines angepassten Internet-Browsers, der u.a. die Vorkonfigurierung aller sicherheitsrelevanten Optionen ermöglicht sowie deren nachträgliche Änderung verhindert¹³³.

Die angepasste Version kann dann im Unternehmensintranet für eine Installation bereitgestellt werden. Für den Netscape Navigator ist eine ähnliche Funktionalität nicht bekannt, allerdings

¹³² Microsoft stellt im Internet die sogenannte Lifecycles, d.h. die verschiedenen Zyklen, die ein Produkt während seiner Betriebszeit durchläuft, dar. Die relevanten Daten für Betriebssysteme finden sich auf der Seite <http://www.microsoft.com/windows/lifecycle.asp>. Eine weitere Auflistung enthält alle Produkte, für die bereits kein Support seitens Microsoft mehr besteht: <http://support.microsoft.com/default.aspx?scid=fh:en-us:lifecycle>

¹³³ Die Erstellung unternehmensangepasster Versionen des Internet Explorer ist mit dem Internet Explorer Administration Kit (IEAK) möglich: <http://www.microsoft.com/windows/ieak/de/default.asp>

kann eine Standardinstallation beim Starten des Browsers zur Benutzung einer vom Systemadministrator definierten, angepassten Konfiguration gezwungen werden.

Die tatsächlich vorhandenen Sicherheitsprobleme in Zusammenhang mit Internet-Browsern, Skriptsprachen sowie anderen Applikationen aufzuzählen, ist im Rahmen dieser Arbeit nicht möglich. Generell lässt sich nur sagen, dass die auf den Workstations eines Unternehmens installierten Applikationen einer genauen Inventarisierung unterzogen und über eine zentralisierte Architektur regelmäßig und möglichst automatisiert mit Updates ausgestattet werden sollten. Ebenfalls in diese Prozedur mit einbezogen werden sollten die zugrunde liegenden Betriebssysteme.

3.7.3.2 Java-Applets

Java-Applets sind kleine, in der Programmiersprache Java geschriebene Programme, die für die Ausführung in Internet-Browsern entwickelt wurden. Sie werden dabei von einer auf der Webseite angegebenen Adresse auf den lokalen Rechner des Internetnutzers heruntergeladen und dort ausgeführt. Aufgrund der dabei bestehenden Sicherheitsbedenken findet die Ausführung innerhalb einer geschützten Umgebung, der sogenannten „Sandbox“, statt, einer virtuellen Maschine, die gleichzeitig eine Begrenzung für die möglichen Zugriffe des Applets auf das übrige System darstellt.

Java-Applets sind nicht mit JavaScript oder sonstigen Skriptsprachen zu verwechseln, diese werden meist ungeschützt auf dem lokalen System ausgeführt. Häufig sind sie im verwendeten Internet-Browser integriert und mit diesem mitinstalliert worden.

Java-Programme – und damit auch Java-Applets – bieten ein komplexes, jedoch nur schwer zu verstehendes Sicherheitskonzept an, das die Einstufung von Programmen als vertrauenswürdig ermöglicht, ein Beispiel hierfür ist die Signierung eines Applets. Diese vertrauenswürdig anzusehenden Applets können über spezielle Funktionen kontrolliert auf Systemressourcen außerhalb ihrer Sandbox zugreifen und diese nutzen. Sicherheitsrelevant ist auch hier die Wahrung der Aktualität der verwendeten Java-Version.

3.8 Risiken bei der Datenübertragung im Netzwerk

Die Datenübertragung im Netzwerk birgt vor allem Risiken hinsichtlich zweier Aspekte, ihrer maximalen Ausbreitung und der Abhörsicherheit der für die Übertragung verwendeten Datennetze. Beide Aspekte stehen im engen Zusammenhang mit der Segmentierung des Netz-

werks¹³⁴ sowie den Verbindungen zu angrenzenden Netzen und deren Sicherung. Generell kann man hierzu nur verlässliche Angaben für kontrollierbare lokale Netzwerkstrukturen machen. Bei der Datenübertragung über entfernte Netzwerke wie dem Internet, muss man prinzipiell von einem unsicheren Übertragungsweg ausgehen. Deshalb sollte eine Übertragung sensibler Daten über diese Netze nur in verschlüsselter Form, z.B. unter Zuhilfenahme eines Virtual Private Network oder aber anderer gesicherter Kommunikationskanäle, erfolgen.

Eine besondere Stellung hinsichtlich der Sicherheit der Datenübertragung nehmen wegen ihrer Charakteristik der bereits in Kapitel 2.2 besprochenen Broadcast-Verbindungen die häufig als Grundlage für Intranets dienenden Local Area Networks auf Ethernet-Basis ein. Da hier jedes Datenpaket an alle am Netzwerk angeschlossenen Teilnehmer übertragen wird, ist es für den Angreifer einfach, unbemerkt Datenpakete mit möglicherweise sensiblen Daten abzufangen. Dies kann durch Einbruch in ein am Netz angeschlossenes Computersystem erfolgen, aber auch durch einfachen Anschluss eines zusätzlichen Rechners (i.d.R. eines Notebooks) an einen freien Anschlusspunkt. Ist das Netzwerk auf die automatische Vergabe von IP-Adressen eingerichtet, braucht der Angreifer nur eine physische Verbindung zum Netzwerk und wird daraufhin sofort in die Struktur eingebunden. Er kann nun Pakete für andere Teilnehmer abfangen und Datenpakete abspeichern, um sie später ausführlich auf nützliche Daten wie Benutzernamen oder Passwörter zu untersuchen.

Die Aufgabe des Speicherns und der späteren Auswertung von IP-Paketen übernehmen sogenannte „Netzwerk-Sniffer“, die im nächsten Abschnitt näher vorgestellt werden.

3.8.1 Netzwerk-Sniffer

Unter dem Begriff „Netzwerk-Sniffer“ werden gemeinhin alle Arten von Analysevorrichtungen für Netzwerkprotokolle zusammengefasst, wobei moderne Programme zumindest die Protokolle Ethernet sowie TCP/IP und IPX verarbeiten können. Sie sind – obwohl vielfach als Sicherheitsrisiko angesehen – vornehmlich als Hilfe für Netzwerkadministratoren bei der Analyse möglicher Probleme der Datenübertragung im Netzwerk gedacht.

Für die Ausführung ihrer Aufgabe versetzen sie die Netzwerkkarte des betroffenen Systems zunächst in den „Promiscuous Mode“¹³⁵ und beginnen anschließend mit der Speicherung und Analyse aller empfangenen Datenpakete. Da dies eine lediglich passive Tätigkeit darstellt, ist

¹³⁴ Das Design von Netzwerkarchitekturen wurde bereits im Kapitel „Strukturierung von Netzwerken“ (2.4) besprochen, weiterführende Informationen finden sich in [anonymous 2001], S. 764 ff.

¹³⁵ Als „Promiscuous Mode“ (engl. ‘vermischt’) wird die ungebräuchliche Einstellung einer Netzwerkkarte bezeichnet, alle Datenpakete, unabhängig von ihrer Zieladresse, anzunehmen. Das Vorfinden einer Netzwerkkarte in diesem Modus ist entweder Zeichen für eine Fehlkonfiguration oder der sichere Beweis für die Existenz eines Sniffers.

die bloße Existenz von Sniffern nur schwer zu erkennen¹³⁶. Einen ziemlich sicheren Anhaltspunkt bietet die Entdeckung einer Netzwerkkarte im besagten „Promiscuous Mode“.

Meist werden Sniffer eingesetzt, um Authentifizierungsdaten abzufangen, daher sind sie i.d.R. konfiguriert, nur die ersten 200 bis 300 Bytes eines Datenpakets zu untersuchen. Dies ist aus zwei Gründen eine essentielle Einschränkung, zum einen hinsichtlich des beschränkt zur Verfügung stehenden Festplattenplatzes zur Ablage protokollierter Daten, zum anderen aufgrund der möglichst gering zu haltenden Belastung des Netzwerkverkehrs – wichtig zur Vermeidung einer frühen Entdeckung des Sniffers.

Generell gibt es zur Entdeckung eines Sniffers zwar verschiedene Programme, allerdings ist damit nicht in jedem Fall ein garantiertes Ergebnis zu erreichen. Die einzigen wirksamen Strategien gegen Sniffer-Angriffe sind deshalb die Erstellung einer sicheren Netzwerktopologie sowie die Verwendung von verschlüsselten Arbeitssitzungen (z.B. durch Verwendung der Secure Shell).

3.8.2 Datenübertragung im Internet

Für die Risiken bei der Datenübertragung im Internet gilt prinzipiell, dass eine sichere Verbindung nur über eine Verschlüsselung der übertragenen Daten gewährleistet werden kann. Auch hier kann ein Netzwerk-Sniffer an einer strategisch gut positionierten Stelle über die Untersuchung von Datenpaketen vertrauliche Informationen erhalten und für einen späteren Angriff nutzen. Wie im lokalen Netzwerk kann es sich bei den Informationen um Anmeldedaten für einen Benutzeraccount, z.B. die Zugangsdaten zu einer Webseite, handeln. Viel wichtiger ist jedoch der Schutz von übertragenen e-Mails sowie (für den Bereich des e-Commerce) von eingegebenen Kreditkartendaten. Der Versand vertraulicher e-Mails sowie die Tötigung von Transaktionen im Bereich des e-Commerce sollten aus diesem Grund nur über verschlüsselte Datenverbindungen erfolgen, wobei hier auf das Kapitel „Verschlüsselungsmechanismen“ (4.4.3) verwiesen wird.

3.9 Betriebssystemspezifische Risiken

Jedes Betriebssystem bietet spezifische Risiken, die häufig vom grundlegenden Design und ursprünglichen Einsatzzweck des Produktes abhängen. In diesem Kapitel sollen das häufig für Arbeitsplatzrechner eingesetzte System Microsoft Windows sowie – aus dem Serverbereich – UNIX-basierte Systeme auf ihr spezifisches Risikopotenzial untersucht werden. Die Novell Netware – Plattform sowie der besonders für Grafikarbeitsplätze häufig eingesetzte Macin-

¹³⁶ Ein massiver verteilter Angriff mit mehreren Sniffern fand 1994 statt. Er kompromittierte u.a. zahlreiche Hosts und Backbones des Milnet (Netzwerk der Armee), vgl. dazu [anonymous 2001], S. 352 ff.

tosh mit dem darauf laufenden System MacOS werden dagegen nicht Gegenstand der Betrachtung sein¹³⁷.

3.9.1 Microsoft Windows

Generell wird Microsoft-Produkten eine geringe Sicherheitsfunktionalität, verglichen mit klassischen Netzwerkbetriebssystemen, nachgesagt. Dies gilt jedoch nicht oder nur bedingt für die Versionen Windows NT, 2000 bzw. das neu erschienene Windows XP Professional. Diese sind für einen Mehrbenutzerbetrieb ausgelegt und bieten dementsprechende Sicherheitsfunktionen, z.B. eine Benutzerverwaltung und darauf aufbauende Zugriffskontrollen auf lokale oder Netzwerkressourcen. Produkte wie Windows 3.x, 95, 98, Millennium Edition (ME) oder XP Home Edition sind – wie bei letzterem der Name auch ausdrückt – für den Gebrauch in Einzelplatzumgebungen gedacht und bieten keine sicherheitsrelevante Funktionalität¹³⁸. So ist es z.B. einem normalen Benutzer in Windows 98 möglich, Dateien des Betriebssystems zu modifizieren oder zu löschen, so dass dieses bei einem Neustart nicht mehr oder nur eingeschränkt funktionsfähig ist. Für den professionellen Einsatz in Unternehmen sind diese Versionen demnach ungeeignet. Aus Gründen der seitens Microsoft eingestellten technischen Unterstützung für Windows NT 3.5 sollte dieses ebenfalls nicht mehr eingesetzt werden. Für die NT-Version 4.0 hat Microsoft bereits eine Beendigung der Unterstützung zum 30. Juni 2003 angekündigt, eine bei der Neuauswahl eines Betriebssystems zu bedenkende Tatsache. Im Folgenden werden lediglich die Versionen NT 4.0 bzw. 5.0 (Windows 2000) betrachtet, da eine ausführliche Analyse von Windows XP noch nicht möglich ist – hier sollte vor dem Einsatz in sicherheitssensiblen Umgebungen eine gewisse Marktreife und damit Stabilität des Produktes abgewartet werden.

Theoretisch kann man eine anfängliche Installation von Windows NT¹³⁹ in ihrer Stabilität und Sicherheit mit anderen Betriebssystemen vergleichen. Eine wichtige Voraussetzung für diese Aussage besteht darin, dass die Installation auf ein NTFS-Dateisystem¹⁴⁰ erfolgte und eine anschließende Aktualisierung des Betriebssystems mit den aktuellen Service-Packs und Hot-

¹³⁷ Hierzu wird als weiterführende Literatur auf [anonymous 2001], S. 608 ff. bzw. S. 648 ff. verwiesen.

¹³⁸ XP Home Edition besitzt zwar die gleichen Funktionalitäten wie die Professional Edition, jedoch sind diese – zur Vermeidung der Überforderung des normalen Heimanwenders – gut verborgen bzw. überhaupt nicht zugänglich.

¹³⁹ Sofern nicht anders angegeben, bezieht sich die Bezeichnung Windows NT im Folgenden sowohl auf die Versionen NT 4.0 und NT 5.0, wobei letztere die gebräuchliche Bezeichnung Windows 2000 trägt.

¹⁴⁰ Das „New Technology File System“ (NTFS-Dateisystem) ist in der Lage, komplexe Rechtevergaben auf einzelne Dateien oder Ordner auf einem Laufwerk abzubilden. Das bei vorherigen Windows-Versionen gebräuchliche „File Allocation Table“ – System (FAT) bietet dagegen keinerlei Zugriffskontrolle auf Dateisystemebene und kann leider auch heute noch für eine Installation von Windows NT ausgewählt werden

fixes¹⁴¹ vorgenommen wurde. Bei einem so konfigurierten System kann man von einer guten externen Sicherheit ausgehen, zu diesem Zeitpunkt sind aber noch keine weiteren Dienste auf dem Rechner aktiv.

Eine für Systemadministratoren wichtige, jedoch in Windows NT fehlende Funktionalität betrifft die ausführliche Protokollierung von Informationen. Dazu zählen vor allem Ereignisse wie die lokale An- und Abmeldung eines Nutzers sowie der Zugriff auf einen vom System bereitgestellten Netzwerkdienst. Windows NT stellt hierfür lediglich die sogenannte „Ereignisanzeige“ zur Verfügung, deren Einträge jedoch nicht als Datei vorliegen und somit eine automatisierte Auswertung nicht möglich ist. Die zusätzliche Installation eines entsprechenden Hilfsprogramms ist in jedem Fall anzuraten.

In der NT-Version 5.0 wurden von Microsoft zusätzliche Sicherheitsfunktionen integriert, die auf einer neuen, servergespeicherten Verzeichnisdienststruktur, dem sogenannten „Active Directory“, beruhen. Darin sind sowohl Benutzer- und Gruppenkonten als auch Zugriffsrichtlinien für Systemressourcen enthalten. Ebenfalls integriert wurde die Unterstützung von internetbasierten Zugriffsprotokollen wie Key-Exchange-Verfahren (Kerberos) und LDAP¹⁴².

3.9.2 UNIX-basierte Systeme

UNIX ist sowohl eines der ältesten als auch das mit Abstand am häufigsten eingesetzte Server- und Netzwerkbetriebssystem der Welt. Die Bezeichnung steht dabei für eine Familie von Betriebssystemen, deren einzelne Mitglieder als Distributionen bezeichnet werden. Jede Distribution wird von einem bestimmten Hersteller angeboten, der wiederum die zentrale Anlaufstelle für eventuelle Updates zum Betriebssystem darstellt. Trotz oder eben vielleicht wegen der großen Installationsbasis sind alle großen Distributionen mit Sicherheitsproblemen behaftet. Grundsätzlich lassen sich diese in kommerzielle (fast immer sogenannte „Closed-Source-Distributionen“) und nichtkommerzielle Systeme (zumeist „Open-Source-Distributionen“)¹⁴³

¹⁴¹ Die Firma Microsoft veröffentlicht in gewissen Zeitabständen Aktualisierungen von fehlerhaften Systemdateien (sogenannten Updates) als zusammengefasste und mit einem Installationsprogramm ausgestattete „Service Packs“. Davon sollte immer die höchste verfügbare Version für das jeweilige Betriebssystem installiert werden, wobei diese immer die vorangegangenen Versionen enthält. Weiterhin veröffentlicht Microsoft in kurzen Abständen sogenannte „Hotfixes“, die nur eine kurze Testphase durchlaufen und neu entdeckte Sicherheitslöcher im System beheben. Alle diese Updates sind zentralisiert im Internet verfügbar und werden für das jeweilige Betriebssystem in einer Auflistung bereitgestellt: <http://windowsupdate.microsoft.com/>

¹⁴² LDAP stellt einen populären Verzeichnisdienst dar, der vor allem für das Ablegen von Benutzerinformationen wie Nutzernamen oder Passwörter entwickelt worden ist. Sowohl unter Windows als auch unter UNIX-basierten Systemen gibt es entsprechende Implementierungen

¹⁴³ Als Beispiele für „Closed-Source-Distributionen“ kann man SUN Solaris, IBM AIX oder auch Hewlett Packards HP-UX anführen. Charakteristisch für diese Distributionen ist, dass deren Quellcode nicht öffentlich zur Verfügung steht (daher die Bezeichnung). Zu den „Open-Source-Systemen“ gehört z.B. das freie Betriebssystem Linux, welches von verschiedenen Herstellern (Suse, Red Hat, Mandrake) vertrieben wird. Hier steht der Quellcode für den Kernel sowie fast alle Applikationen zur Verfügung.

einteilen. Bei ersteren ist die Sicherheit stark davon abhängig, inwieweit der Hersteller nicht nur neue Funktionen und Programme in das Betriebssystem integriert, sondern auch das bestehende System auf eventuell entdeckte Sicherheitslöcher hin überprüft und gegebenenfalls mit einem Update auf einen sicheren Stand bringt. Bei Distributionen aus der „Open Source“ – Bewegung dagegen werden die Programmzeilen von vielen verschiedenen Programmierern angesehen und auf eventuelle Fehler hin überprüft. Da der Quellcode des Systems frei verfügbar ist, kann auf ein bekannt gewordenes Sicherheitsloch entsprechend schnell reagiert werden – ein unbestreitbarer Vorteil gegenüber den kommerziellen Systemen. In besonders gefährlichen Situationen muss nicht einmal auf ein Update des Herstellers gewartet werden, stattdessen kann man den betreffenden Quellcode – eine gewisse Programmiererfahrung vorausgesetzt – auch selbst modifizieren.

Ein sicherheitstechnisch positives Merkmal von UNIX¹⁴⁴ besteht in der Modularität der Systeme. Das eigentliche Betriebssystem, auch als der UNIX-Kernel bezeichnet, ist nur von geringer Größe – in ihm sind die Kernfunktionen, wie Dateieingabe und -ausgabe, Speicherverwaltung u.a. implementiert. Um den UNIX-Kernel herum werden von den Anbietern Unmengen zusätzlicher Pakete bereitgestellt – die entstehende Gesamtheit bildet dann die vertriebene Distribution. Bei der Installation eines UNIX-Systems sollte von Anfang an darauf geachtet werden, dass nur die wirklich zum Betrieb benötigten Pakete zur Installation ausgewählt werden. Damit entfällt auch die sonst bestehende Notwendigkeit, eigentlich nicht benötigte Pakete ebenfalls auf dem neuesten Stand zu halten. Dieses Paketkonzept – was UNIX auch von anderen Betriebssystemen wie Novell NetWare oder Microsoft Windows abgrenzt – ermöglicht zudem die kurzfristige Deinstallation eines sicherheitstechnisch bedenklich gewordenen Paketes, ohne die Gesamtinstallation zu beeinträchtigen.

Einige Distributionen werden als sogenannte „gehärtete“ Betriebssysteme ausgeliefert, meist bezieht sich dies auf zusätzliche Kriterien wie eine standardmäßig sichere Grundkonfiguration (keine unnötigen Dienste aktiviert) oder auch eine spezielle Vorgehensweise bei der Programmierung und Kompilierung des Systems¹⁴⁵. Einen anderen Ansatzpunkt verfolgen die „Trusted Systems“, hier wird der normalerweise alle Rechte besitzende Administrator (root) auf normale Benutzerprivilegien heruntergestuft. Anstatt auf Benutzerebene über eine granulare Rechtevergabe den Zugriff auf bestimmte Systemressourcen einzugrenzen, wird auf der Betriebssystemebene (im UNIX-Kernel selbst) eine Kontrollinstanz für den Zugriff auf Systemaufrufe – die jedes Programm benötigt, um seine gewünschte Funktion auszuführen –

¹⁴⁴ Wenn nicht ausdrücklich eine Spezifizierung vorgenommen wird, soll der Begriff „UNIX“ im Folgenden für alle Varianten dieser Betriebssystemfamilie gelten.

¹⁴⁵ Das bekannteste Beispiel für eine gehärtete UNIX-Distributionen ist OpenBSD.

implementiert. Dabei werden prinzipiell nur die mindestens nötigen Privilegien für einen bestimmten Benutzer oder ein Programm freigegeben, teilweise geschieht dies auch dynamisch. Hauptabnehmer für diese Arten von Betriebssystemen waren bisher vor allem Militär- und Regierungseinrichtungen, mögliche Einsatzszenarien liegen heutzutage jedoch auch im Bereich von e-Business und e-Commerce.

Welche Art von UNIX-System schließlich seinen Einsatz finden soll, muss im Voraus gründlich überdacht werden, hierbei spielen vor allem Kriterien wie vorhandene Administrationskompetenzen, Sicherheitsanforderungen, gewünschte Flexibilität des Systems und sicherheitsrelevante Einstellung des Herstellers, aber auch die Kosten für die Distribution eine wichtige Rolle. Trotzdem muss man sich bewusst sein, dass jede Distribution, auch ein „Trusted System“ grundsätzlich angreifbar ist, wenn eine sichere Endkonfiguration des Systems unterlassen wurde. Einige administrative Regeln sollten jedoch in jedem Fall bei der Installation und Konfiguration eines UNIX-Systems Beachtung finden, diese sollen im Folgenden aufgeführt werden.

Der Zugriff auf den Superuser-Account (also root) sollte nur einem einzelnen Administrator oder maximal einem privilegierten Personenkreis möglich sein, wobei dafür ein besonders starkes Passwort vergeben werden muss. Für die Erstellung des Passworts sollte ein Kennwortgenerator benutzt werden, der komplett zufällige Zeichenfolgen kreieren kann. Das Passwort sollte zudem regelmäßig geändert werden, um eine eventuelle Kompromittierung einzugrenzen, ebenso sollte das Passwort nur für ein einzelnes Computersystem gültig sein.

Ferner ist das System so zu konfigurieren, dass nur diejenigen Dienste gestartet werden, die der Server auch tatsächlich bereitstellen soll, alle anderen sollten nach Möglichkeit deinstalliert, mindestens aber deaktiviert werden. Der Einsatz von unter Sicherheitsaspekten bedenklichen Diensten¹⁴⁶ sollte generell unterbleiben.

Besondere Aufmerksamkeit sollte der Rechtevergabe im Dateisystem gewidmet werden, welche sich aus den Einzelaspekten Objektbesitzer, Objektgruppe und dazugehörigen Berechtigungen zusammensetzt. Die Rechtevergabe wird vom Systemadministrator vorgenommen und stellt eine sehr komplexe Sicherungsmaßnahme dar¹⁴⁷. Ein über ein öffentliches Netzwerk wie das Internet zugängliches UNIX-System sollte unbedingt mit einer Erkennung für potenzielle Eindringversuche von Angreifern ausgestattet sein. Das am häufigsten eingesetzte Programm dieser Art von Systemen ist das frei verfügbare Werkzeug „Tripwire“¹⁴⁸. Die allgemeine Funktionsweise dieser Programme besteht darin, dass unmittelbar nach dem Zeit-

¹⁴⁶ Vgl. dazu auch das Kapitel „Serverseitige Dienste“ (3.7.2)

¹⁴⁷ Vgl. dazu [anonymous 2001], S. 435 ff. sowie die Dokumentation zu den Befehlen „chmod“ und „chown“.

¹⁴⁸ <http://www.tripwire.org>

punkt der Installation des Betriebssystems, noch bevor der Computer mit irgendeinem Netzwerk verbunden wird, ein digitaler Fingerabdruck jeder einzelnen Datei angefertigt und in einer gesicherten Datenbasis abgelegt wird. In regelmäßigen, meist täglichen Abständen wird der erste Teil dieses Prozesses wiederholt und die dabei erhaltenen Ergebnisse werden mit dem abgespeicherten Referenzabbild verglichen. Jegliche Änderung einer Datei hat dabei unweigerlich die Änderung des dazugehörigen digitalen Fingerabdrucks zur Folge. Die gefundenen Unterschiede werden protokolliert und müssen vom Systemadministrator ausgewertet werden. Abweichungen – ohne dass der Administrator diese selbst zu verantworten hätte, z.B. durch die Installation eventueller Updates zum Betriebssystem – sind ein sicheres Zeichen für eine Kompromittierung des Computersystems. Ist der Angreifer erst einmal in das Zielsystem eingedrungen und hat womöglich Superuser-Rechte erlangt, besteht sein nächster Schritt zumeist in der Installation eines sogenannten „Rootkits“ – eines Softwarepakets, welches verschiedene Ersatzprogramme für gängige Systemwerkzeuge enthält. Diese Ersatzprogramme dienen zum Verbergen jeglicher Spuren des Angriffs, indem sie dem legalen Systemadministrator ein scheinbar intaktes System präsentieren. So werden z.B. laufende Prozesse des Angreifers verborgen, ebenso dessen aktive Netzwerkverbindungen und von ihm installierte Dateien. Häufig verschafft sich der Angreifer sehr schnell einen legalen Zugang zum System (Benutzeraccount) und verschließt gleichzeitig das Sicherheitsloch, durch das er in das System eingedrungen ist, um keine weitere Aufmerksamkeit auf sich zu lenken. Neben den gerade beschriebenen „Benutzer-Rootkits“ ist eine zweite, weitaus gefährlichere Form unter Angreifern sehr gebräuchlich: die „Kernel-Rootkits“. Der Kernel bildet das zentrale Systemprogramm auf der niedrigsten Ebene und stellt die direkte Schnittstelle zur Systemhardware dar. Ein Angreifer, der auf diese Weise den Kernel modifiziert, erlangt nicht nur vollständige Kontrolle über das System, sondern ist zusätzlich nicht mehr zu entdecken. Egal, mit welchem Programm der legale Administrator eine Überprüfung des Systems vornimmt, der modifizierte Kernel selbst wird mit gefälschten Rückgabedaten die Entdeckung des Einbruchs verbergen.

Zusammenfassend kann man sagen, dass ein UNIX-System bereits mit wenigen Konfigurationsänderungen in großem Maße abgesichert werden kann. Hierzu ist vor allem die erwähnte Deaktivierung nicht benötigter Serverdienste sowie die Einrichtung einer Zugriffskontrolle (Ausschlusslisten, Filterprogramme) auf die verbliebenen Services ein erster Ansatzpunkt. Die sicherheitsrelevante Konfiguration des Systems, auch als „Host Lockdown“ bezeichnet, sollte dabei zunächst manuell vorgenommen und generell protokolliert werden. Aufgrund dieser Protokolle ist später die Erzeugung einer automatisiert ablaufenden Skriptsammlung

möglich, die eine identische Konfiguration ohne Benutzereingriff vornehmen kann. Als weiterführenden Schritt kann man die Benutzung eines sogenannten „Hardening-Tools“ in Betracht ziehen, welches speziell für die verwendete Plattform und Version eine Absicherung durchführt¹⁴⁹.

3.10 Hardwarespezifische Risiken

Meist stützt man sich bei der Absicherung von Unternehmensnetzwerken vollständig auf die der vorhandenen Computersysteme und lässt damit die zusätzlich vorhandenen Infrastrukturgeräte wie Router und Switches außer Acht. In diesem Kapitel sollen kurz die damit verbundenen Sicherheitsprobleme beschrieben werden.

Jedes aktive¹⁵⁰ Infrastrukturgerät im Netzwerk besitzt heutzutage eine interne Konfigurationsoberfläche, wobei deren gebräuchliche Formen von einer sehr einfach gehaltenen Textoberfläche bis zu webbasierten Konfigurationslösungen reichen. Dieser Oberfläche liegt in jedem Fall eine von der Hardware selbst unabhängige Software zugrunde, die auch als sogenannte „Firmware“ bezeichnet wird. Diese enthält üblicherweise – wie jede andere Art von Software auch – in ihren anfänglichen Revisionen eine gewisse Anzahl von Fehlern, die vom Hersteller durch die Herausgabe einer neuen Version behoben werden. Da die enthaltenen Fehler – analog zu denen in Betriebssystemen – zum unberechtigten Zugriff eines Angreifers auf das Gerät führen können, ist eine regelmäßige Aktualisierung der Firmware notwendig.

Auf fast allen Routern und Switches wird zudem ein SNMP-Dienst zum Management des Gerätes ausgeführt. Dieser sollte entweder vollständig deaktiviert – was im Regelfall ohne Funktionalitätsverlust möglich ist – oder aber zumindest durch die Vergabe sicherer Passwörter geschützt werden¹⁵¹.

3.11 Interne Sicherheit

Der bisher verwendete Term „Angreifer“ impliziert häufig eine im Vergleich zum Unternehmen externe Rolle der damit bezeichneten Person. Diese Annahme ist – wie schon in Kapitel 3.5.4 kurz dargelegt – nicht nur grundlegend falsch, sie ist im Hinblick auf sicherheitstechnisch notwendige Überlegungen auch besonders gefährlich. Die interne Sicherheit eines Unternehmens stellt vielfach noch immer eine Art „ungeliebtes Stiefkind“ dar und wird dementsprechend vernachlässigt. Einer aktuellen Studie des Computer Security Institute (CSI) zufol-

¹⁴⁹ Beispiele für „Host Hardening – Tools“ findet man in der Literatur: [anonymous 2001], S. 599 ff.

¹⁵⁰ Der Zusatz „aktiv“ trennt gemeinhin konfigurierbare Netzwerkgeräte von nicht anpassbaren Geräten ab.

¹⁵¹ Vgl. dazu auch das Kapitel „Das SNMP-Protokoll“ (3.7.2.5)

ge waren lediglich 25 Prozent der von den Befragten entdeckten Sicherheitsverletzungen externen Personen zuzurechnen¹⁵².

Eine vielfache Ursache von internen Sicherheitsverletzungen stellen falsch konfigurierte Firewall-Systeme dar – diese bieten häufig einen ausschließlichen Schutz vor externem unautorisiertem Zugriff, interne (und damit stillschweigend als autorisiert angesehene) Zugriffe können die Firewall oft ungehindert passieren.

Die internen Risiken sind von ihren Arten her den externen Risiken gleichzusetzen, unterscheiden sich jedoch in zugeordneten „menschlichen Faktoren“, genauer gesagt in ihren organisatorischen Rollen und Intentionen. Erstere lassen sich dabei wie folgt klassifizieren: Unwissenheit (Unabsichtlichkeit), Ignoranz sowie Böswilligkeit (oder Opportunismus). Die Angreifer können dabei in der Rolle von Mitgliedern der Öffentlichkeit, Mitarbeitern auf Zeit, Vollzeitmitarbeitern oder sogar Systemadministratoren auftreten. Die möglichen Kombinationen dieser beiden Faktoren ergibt eine Matrix theoretischer Gefährdungspotenziale, welche in Abbildung 3.4 gezeigt ist.

Intention \ Rolle	unwissentlich, unabsichtlich	ignorant	böswillig, opportunistisch
Mitglieder der Öffentlichkeit (z.B. Kioskanwendung)			
Mitarbeiter auf Zeit			
Vollzeitmitarbeiter in einzelnen Abteilungen			
Administratoren der Infrastruktur			

Abbildung 3.4 - Menschliche Vektoren: Risikostufen

Quelle: nach [anonymous 2001], S. 748

Diesem Gefährdungspotenzial wirksam zu begegnen, bedeutet vor allem die Erarbeitung einer starken, jedoch akzeptablen Benutzerrichtlinie für das Unternehmensnetzwerk sowie deren anschließende Umsetzung. Die Einhaltung der Richtlinie sollte regelmäßig und automatisiert überprüft werden.

Aufgrund ihres breiten Vorkommens stellen ignorante Mitarbeiter das weitaus größte Problem dar, d.h. diejenigen, welche Benutzer- und Sicherheitsrichtlinien bewusst untergraben und (sinnvolle) Beschränkungen umgehen. Dies geschieht meist aus dem Bestreben heraus, der Überwachung des Internetzugangs durch die IT-Abteilung des Unternehmens auszuweichen.

¹⁵² Vgl. dazu [anonymous 2001], S. 746

Beispiele dafür sind die Benutzung von zusätzlichen Einwahlfunktionalitäten (z.B. einem eigenen Modem) oder auch die bewusste Ausführung unbekannter Anhänge von e-Mails.

Zusammenfassend kann man sagen, dass alle in diesem Kapitel dargestellten Risiken und deren Begegnung in besonderem Maße auch für interne Mitarbeiter gelten. Dahingehend ist für die Absicherung eines Unternehmensnetzwerks von innen eine ebenso sorgfältige wie strenge Analyse von kritischen Sicherheitspunkten notwendig, das betrifft sowohl die Errichtung einer physikalischen (d.h. Zugangs-) Sicherheit zu gefährdeten Ressourcen als auch administrative Maßnahmen wie Richtlinien, Zusammenarbeit von Administratoren, Einsatz von Protokollierungsmechanismen zum Nachweis von Zugriffen sowie die regelmäßige Aktualisierung der Software auf den Arbeitsplätzen der Mitarbeiter.

Zusätzlich sollte von Managementseite aus eine gewisse Sensibilität für Sicherheitsfragen bei der Neueinstellung von Mitarbeitern vorhanden sein, eine heutzutage keineswegs selbstverständliche Tatsache.

4 Schutzmechanismen für vernetzte Systeme

In diesem Kapitel sollen stichpunktartig verschiedene Schutzmechanismen gegen die im vorangegangenen Kapitel betrachteten verschiedenen Risiken aufgeführt werden. Dabei ist diese Aufzählung keinesfalls als vollständige Liste zu betrachten, vielmehr ist sie als erster Ansatzpunkt möglicher Absicherungsmethoden zu verstehen. Das (Nicht-) Vorhandensein der hier dargestellten sicherheitsrelevanten Methoden und Systeme hat einen erheblichen Einfluss auf die individuelle Risikosituation des Unternehmens und damit zusammenhängend auch auf die Versicherbarkeit des betreffenden Risikos sowie die zu zahlende Versicherungsprämie.

Leider haben auch heutzutage, wie eine aktuelle Studie der Unternehmensberatung Ernst & Young¹⁵³ aufzeigt, viele Unternehmen essentielle Sicherheitslücken. So denken beispielsweise nur 40 Prozent der befragten Firmen, dass sie einen stattgefundenen Angriff auf ihre Computersysteme entdecken würden, ebenso unternehmen in einem solchen Fall nur rund 60 Prozent einen Versuch der Aufklärung und Analyse. Ein standardisierter Verfahrensplan für die Aufrechterhaltung des Geschäftsbetriebes im Fehlerfall ist nur bei 53 Prozent der Unternehmen vorhanden. Diese Zahlen sind umso mehr beängstigend, als im letzten Jahr über drei Viertel der befragten Firmen eine unplanmäßige Betriebsunterbrechung aufgrund von Computerkriminalität bestätigten.

4.1 Grundlegende Risikoanalyse

Eine grundlegende individuelle Risikoanalyse ist prinzipiell als Ausgangspunkt für den Absicherungsprozess eines Unternehmensnetzwerks zu betrachten. Dabei sollte beachtet werden, dass eine absolute Sicherheit im Netzwerk niemals erreicht werden kann, vielmehr sollten die Möglichkeiten der Minimierung vorhandener Risiken im Mittelpunkt der Betrachtung stehen. Eine Risikoanalyse kann zum einen von einer beauftragten externen Spezialfirma als auch von eigenen Mitarbeitern durchgeführt werden. In letzterem Fall sind eine gewisse Integrität sowie Objektivität und eine gute Ausbildung als Kriterien der Mitarbeiter für eine erfolgreiche Risikoanalyse zwingend erforderlich. Eine vollständige Risikoanalyse sollte dabei mindestens die aktuelle Situation in den Bereichen Systemadministration (vorhandene Sicherheitsrichtlinien), Netzwerksicherheit, System- und Anwendungssicherheit sowie Sicherheitsbewusstsein im Unternehmen widerspiegeln. Für den letzten Punkt ist auf jeden Fall eine aus-

¹⁵³ Ernst & Young führen jährlich eine Umfrage unter ausgewählten US-Unternehmen durch, die deren Wissen und Maßnahmen bezüglich der eigenen IT-Sicherheit widerspiegelt. Die aktuelle Studie kann im Internet heruntergeladen werden: [EY 2002].

fürliche Erfassung, getrennt nach Mitarbeitern und Geschäftsführung des Unternehmens, vorzunehmen.

Sind die einzelnen sicherheitsrelevanten Bereiche analysiert, schließt sich die Ermittlung der zugeordneten Werte, d.h. der individuellen Bedeutung der vorhandenen Objekte für das Unternehmen an. Die Bestimmung eines „Wertes“ für ein gegebenes Objekt, z.B. eines Routers, der das Unternehmen an das Internet anschließt, ist als extrem schwierig und sensibel zu betrachten, hier ist vor allem die Zusammenarbeit von Geschäftsführung und Sicherheitsbeauftragten im Unternehmen wichtig¹⁵⁴. Im Regelfall wird dieser den reinen finanziellen Wert des Objektes um ein Vielfaches übersteigen.

Vielfach wird – unabhängig von der durchgeführten Risikoanalyse und –bewertung – der Prozess der Absicherung des Unternehmensnetzwerks von außen beginnend nach innen angeordnet und ausgeführt. Als effizienter hat sich jedoch die Vergabe von Prioritäten aufgrund der ermittelten Werte für die einzelnen Objekte und zuvor analysierten Bereiche erwiesen.

4.2 Bedeutung eines Schadenfalls für das Unternehmen

Der nächste Schritt bei der Absicherung des Unternehmensnetzwerkes besteht in der Beantwortung der Frage nach der wirtschaftlichen und ideellen Bedeutung eines Schadenfalls für das Unternehmen. Dabei ist ein Bezug auf die bei der Risikoanalyse ermittelten Werte als Grundlage zweckmäßig. Die dort aufgeführten Einzelrisiken mit den ihnen zugeordneten Werten müssen hierfür zu Risikoszenarien zusammengefasst werden, denen sich wiederum Werte zuordnen lassen. Diese Werte sind zumeist zeitvariant und spiegeln somit die Auswirkungen einer Betriebsunterbrechung aufgrund eines Schadenfalls wider. Wichtig ist die Möglichkeit, in den analysierten Fehlerszenarien von Unternehmensseite her effektiv reagieren zu können. Die Planung dieser Reaktionen lässt sich in einem sogenannten „Incident Response – Modell“ festhalten¹⁵⁵.

4.3 Systemmanagement als Sicherheitsgrundlage

Die Implementierung eines funktionierenden Systemmanagements bildet eine grundlegende Voraussetzung für die erfolgreiche Absicherung eines Unternehmensnetzwerks und der darin enthaltenen Computersysteme. Dafür ist die genaue Zuordnung von Verantwortlichkeiten für die vorab definierten Gebiete des Systemmanagements zwingend notwendig. Als wichtige Bereiche sind vor allem das Management von Sicherheitsrichtlinien, das Netzwerkmanage-

¹⁵⁴ Eine Liste von besonders sensiblen Werten im Unternehmen ist in [anonymous 2001], S. 73 aufgeführt.

¹⁵⁵ Weiterführende Informationen zum IR-Modell und seiner Erstellung finden sich in [Allaire 2001].

ment, die Administration der Systeme und Netzwerkgeräte sowie die Protokollierung durchgeführter Arbeiten in den genannten Gebieten zu nennen. Den dafür verantwortlichen Personen muss nicht nur ein genau definiertes Aufgabenfeld zugeteilt sein, sondern auch eine auf ihren Bereich des Systemmanagements beschränkte funktionelle Eigenständigkeit in Bezug auf die Einführung und Umsetzung von notwendigen Maßnahmen. Ein zwar gut gegliedertes, jedoch lediglich mit Pflichten ausgestattetes Systemmanagement ohne weitreichende eigene Entscheidungsrechte ist sowohl in der Ausübung täglicher Aufgaben als auch bei einem eventuellen Schadenfall nur von begrenzter Effektivität.

Ein wichtiger Punkt innerhalb des Systemmanagements besteht in der Erstellung, Propagierung und Umsetzung von unternehmensweit gültigen sicherheitsrelevanten Richtlinien sowie deren regelmäßiger und automatisierter Überwachung¹⁵⁶.

4.4 Einsatz sicherheitsrelevanter Technologien

Heutzutage existiert eine Vielzahl sicherheitsrelevanter Technologien, die jeweils einen bestimmten begrenzten Teil des Sicherheitsmanagements von Netzwerken unterstützen sollen. Die wichtigsten unter ihnen sollen im Folgenden vorgestellt werden, dazu zählen Schwachstellen-Scanner, Firewall-Systeme sowie Verschlüsselungsmechanismen. Als ebenfalls sicherheitsrelevant sind umfassende Lösungen zum Schutz vor Computerviren, die in jedem Unternehmensnetzwerk standardmäßig vorhanden sein sollten, zu betrachten. Diese sollen jedoch nicht in diesem Kapitel betrachtet werden.

4.4.1 Schwachstellen-Scanner

Als Schwachstellen-Scanner bezeichnet man Programme, die auf der Grundlage einer Datenbasis von bekannt gewordenen Sicherheitsmängeln (sogenannten „Exploits“) ein System oder Netzwerk auf seine Sicherheit hin überprüfen. Damit stellen sie eine sinnvolle Ergänzung und Weiterführung zu den bereits im Kapitel 3.4.1 beschriebenen Portscannern dar. In den Überprüfungsprozess ist meist eine Analyse grundlegender Sicherheitsprobleme, wie aktivierter, jedoch im Regelfall unnötiger Netzwerkdienste, mit eingeschlossen. Durch eine entsprechende Variation des Ausgangspunktes für eine System- oder Netzwerküberprüfung lassen sich Angriffe sowohl aus dem Unternehmen heraus als auch von externen Quellen simulieren. Auch die Analyse des jeweils aktuellen Computersystems – analog zur versuchten Kompromittierung durch einen bereits eingeloggten Anwender – ist möglich und anzuraten. Die

¹⁵⁶ Weiterführende Informationen zu Sicherheitsrichtlinien im Unternehmen finden sich in [anonymous 2001], S. 714 ff.

Schwachpunktanalyse gliedert sich dabei in Sicherheitslücken auf der Hostebene (dem Computersystem selbst) und auf der Netzwerkebene (Zugriff von außerhalb des Systems).

Der Nutzen eines Schwachstellen-Scanners steht im engen Zusammenhang mit dessen regelmäßiger Aktualisierung, deshalb sollte immer die jeweils aktuellste Version des Scanners, unter Einbeziehung von eventuell vorhandenen Updates zu dessen interner Schwachstellendatenbank, zum Einsatz kommen. Nur so ist eine zuverlässige Erkennung entsprechender Dienste und deren Schwachpunkte auf dem zu untersuchenden Rechner möglich. Ein wichtiges Kriterium bei der Auswahl des Scanners bildet auch dessen Präsentationsform für die gefundenen Ergebnisse – diese sollten nicht nur die gefundenen Schwachstellen selbst, sondern zusätzlich auch Details zu deren Sicherheitsrelevanz sowie Aktualisierungsmöglichkeiten für das betroffene System enthalten¹⁵⁷.

Eine Schwachstelle aller Scanner – bei deren Einsatz im eigenen Netzwerk – besteht in der Anwendung einfacher Prüftechnologien zur Ermittlung eines auf dem untersuchten Rechner laufenden Dienstes (Dienstname) und dessen Versionsnummer. Viele Dienste gestatten heutzutage eine Änderung dieser Daten. Eine solche Maßnahme, die zwar für die Absicherung eines Dienstes gegenüber unbefugtem Zugriff sehr nützlich sein kann¹⁵⁸, erweist sich für die Prüfung des Systems durch einen Scanner als unpraktikabel – der Scanner wird nicht die für den real installierten Dienst bekannten Schwachstellen testen, sondern sich an den empfangenen Daten zu Dienstname und Versionsnummer orientieren. Vor Einsatz eines Scanners sollten daher die ursprünglichen Identifizierungsdaten des Dienstes wiederhergestellt sein.

4.4.2 Firewall-Systeme

Firewalls bilden eine der ältesten Säulen aller Datensicherungsstrategien und viele Unternehmen verlassen sich fast ausschließlich auf diese Technologie zur Absicherung ihres Netzwerks – ein zumeist schwerwiegender administrativer Fehler.

Grundlegend ist ein Firewall-System eine Einrichtung, die auf der Netzwerkebene einen Zugriffssteuerungsmechanismus bereitstellt, indem sie die Paketübertragung zwischen zwei Netzen entweder gestattet oder verwehrt. Somit bilden Firewalls eine Art „Kontrollpunkt“ im Netzwerk. Durch einen vorab vom Administrator des Netzwerks definierten Satz von Regeln wird über die Zulässigkeit eines Zugriffs entschieden.

¹⁵⁷ Eine ausführliche Liste zu Auswahlkriterien für Schwachstellen-Scanner findet sich in [anonymous 2001], S. 280 f. Ein Beispiel für einen empfehlenswerten Scanner ist das Open-Source-Projekt „Nessus“ (<http://www.nessus.org>).

¹⁵⁸ Ein Angreifer wird immer zuerst anhand der erhaltenen Daten zu Dienstname und Versionsnummer nach bekannten Schwachstellen suchen. Wenn diese Daten vom Administrator vorab geändert werden, wird die „Arbeit“ des Angreifers zumindest erheblich behindert.

Obwohl einige Firewalls zusätzliche Funktionalitäten wie das automatisierte Ausfiltern von Inhalten (bestimmte, vom Unternehmen unerwünschte Webseiten) oder Technologien (Java, ActiveX) bieten, arbeiten die weitaus meisten Firewall-Systeme lediglich als sogenannte „Paketfilter“ für definierte Protokolle. Indem sie Ursprungs- und Zieladresse einschließlich der verwendeten Portnummern sowie zusätzliche Paketmerkmale (z.B. gesetzte Flags) überprüfen, um sie mit dem zugrunde liegenden Regelwerk zu vergleichen, wird eine Filterung der Paketströme erreicht. Konstruktionsbedingt weisen paketfilterbasierte Firewalls einige Sicherheitsdefizite auf, die sie z.B. anfällig für Angriffstaktiken mit ungültigen TCP-Paketen machen (viele DoS-Attacken beruhen auf diesem Prinzip). Außerdem sind sie nicht in der Lage, eine TCP-Sitzung ihrem Status nach zu verfolgen¹⁵⁹.

Eine Weiterentwicklung dieser Technologie bilden die zustandsorientierten Paketfilter (Stateful Packet Filters, SPF), welche grundsätzlich auf dem gleichen Konzept aufbauen, jedoch zusätzlich mittels interner Zustandstabellen den Status einer bestehenden TCP-Verbindung protokollieren und überwachen können. Diese Funktionalität erlaubt auch das sonst nicht mögliche Schließen der unprivilegierten Ports. Aus diesem Grund sollten zustandsorientierte Paketfilter als Mindestanforderung für Firewall-Systeme betrachtet werden.

Einen dritten Ansatz verfolgen die sogenannten „proxybasierten Firewalls“. Diese fungieren als Vermittler zwischen den beiden an einer Netzwerkverbindung beteiligten Partnern und unterbinden somit deren direkte Kommunikation miteinander, wobei eine Untersuchung des Datenstroms nicht auf der Netzwerkebene, sondern auf der Anwendungsebene stattfindet. Dadurch ist eine protokollorientierte Untersuchung und genauere Filterung der übertragenen Daten möglich. Dafür ist jedoch das Vorhandensein eines protokollspezifischen Proxy-Moduls nötig, was bei einigen Anwendungsprotokollen noch nicht der Fall ist.

Generell können Firewalls, gerade im Falle einer strengen Implementierung, erhebliche Funktionalitätseinbußen in Netzwerken nach sich ziehen. Hierbei wird oft eine Lockerung der Vorschriften (bzw. des Regelwerks der Firewall) gefordert und teilweise auch gewährt, mit der Folge, dass sich schon bald erste „Löcher“ in der Firewall aufzeigen. Ein anderes Problem wiederum ist das oftmals von Firewalls erzeugte Gefühl von Sicherheit. Hier muss nochmals angemerkt werden, dass Firewalls lediglich ein Teil des Sicherungsmodells eines Netzwerks bilden, keineswegs jedoch die Absicherung selbst darstellen. Zudem ist eine ordnungsgemäße

¹⁵⁹ Weiterführende Informationen zu paketfilterbasierten Firewalls finden sich in [anonymous 2001], S. 249 ff.

Implementierung und Konfiguration eines Firewall-Systems als äußerst komplex und damit auch als potenziell fehleranfällig zu betrachten¹⁶⁰.

4.4.3 Verschlüsselungsmechanismen

In diesem Abschnitt soll auf den praktischen Nutzen von Verschlüsselungsalgorithmen bezüglich der Sicherheit in Netzwerken eingegangen werden. Neben der bereits in Kapitel 3.6.1 vorgestellten Kennwortverschlüsselung in Betriebssystemen finden diese Mechanismen heutzutage vor allem für die Sicherung der Datenübertragung in Netzwerken Anwendung.

Der Begriff „Verschlüsselung“ steht allgemein für die Transformation eines Klartextes unter Zuhilfenahme einer Zusatzfunktion (Schlüssel) in einen zugehörigen Geheimtext (Chiffre)¹⁶¹. Für diesen Prozess der Verschlüsselung von Daten stehen zwei verschiedene Kategorien von Algorithmen zur Verfügung.

Die erste Gruppe bilden die sogenannten konventionellen oder symmetrischen Verschlüsselungsverfahren, bei denen derselbe Schlüssel sowohl zur Chiffrierung als auch zur Dechiffrierung genutzt wird (Ein-Schlüssel-Verfahren). Dieser Schlüssel muss daher über einen sicheren Kommunikationsweg vom Sender der verschlüsselten Nachricht zu deren Empfänger gelangen, damit dieser eine Entschlüsselung vornehmen kann. Dies impliziert im allgemeinen, dass vor Beginn der verschlüsselten Kommunikation die beteiligten Partner bekannt sind, so dass eine Versendung des Schlüssels vorgenommen werden kann. Für die sichere Kommunikation mit häufig wechselnden Beteiligten ist diese Art der Verschlüsselung daher als ungeeignet zu betrachten.

Das Modell der symmetrischen Verschlüsselungsmethode ist in Abbildung 4.1 dargestellt.

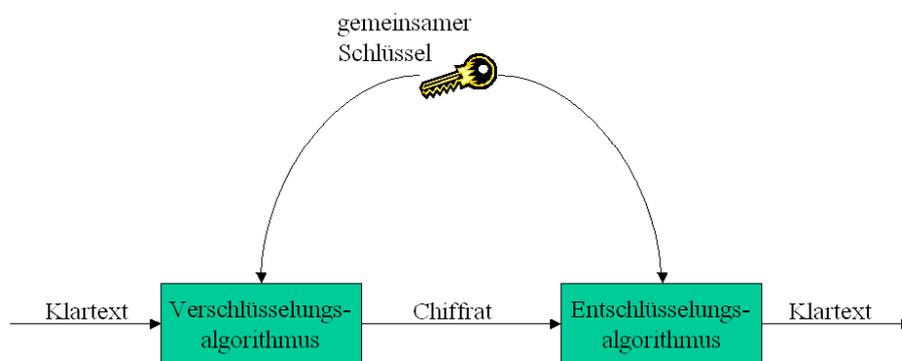


Abbildung 4.1 - vereinfachtes Modell der symmetrischen Verschlüsselung

Quelle: aus [Stallings 1995], S. 22

¹⁶⁰ Eine ausführliche Beschreibung zur Implementierung und Konfiguration von Firewall-Systemen findet sich in [anonymus 2001], S. 256 ff.

¹⁶¹ Vgl. dazu [BSI 2002 GSHB 3023]

Das populärste Beispiel für symmetrische Verschlüsselungsverfahren bildet der Data Encryption Standard (DES)¹⁶², welcher 1974 unter der Federführung von IBM entwickelt und 1977 veröffentlicht wurde. Dieser Algorithmus stellte bis vor kurzem die Standardverschlüsselung der US-Regierung für sogenannte „nichtklassifizierte Daten“ dar. Für DES wurde seit dem Jahr 2000 ein Nachfolger entwickelt (Advanced Encryption Standard, AES), der am 26.05.2002 in Kraft getreten ist und auf dem „Rijndael-Algorithmus“ beruht¹⁶³. Trotz allem ist der DES-Algorithmus nach heutigem Wissensstand als sichere Verschlüsselungsmethode für die private und kommerzielle Nutzung zu betrachten. Als weitere symmetrische Verschlüsselungsalgorithmen sind neben der Abwandlung Triple-DES neuere Algorithmen wie IDEA¹⁶⁴, CAST oder Twofish zu nennen.

Die zweite große Gruppe von Verschlüsselungsalgorithmen bilden die asymmetrischen Verfahren, welche auch als „Public-Key-Verfahren“ bezeichnet werden. Hierbei kommen zwei Schlüssel zum Einsatz, ein öffentlich verfügbarer „Public Key“ sowie ein geheimer „Private Key“, welcher nur dem ihn erzeugenden Benutzer zugänglich sein darf. Die beiden Schlüssel sind zwar mathematisch gesehen verwandt, jedoch ist allein aus dem öffentlichen Schlüssel ein Erraten oder Berechnen des privaten Schlüssels unmöglich.

Das Schema asymmetrischer Verschlüsselungsverfahrens ist in Abbildung 4.2 dargestellt.

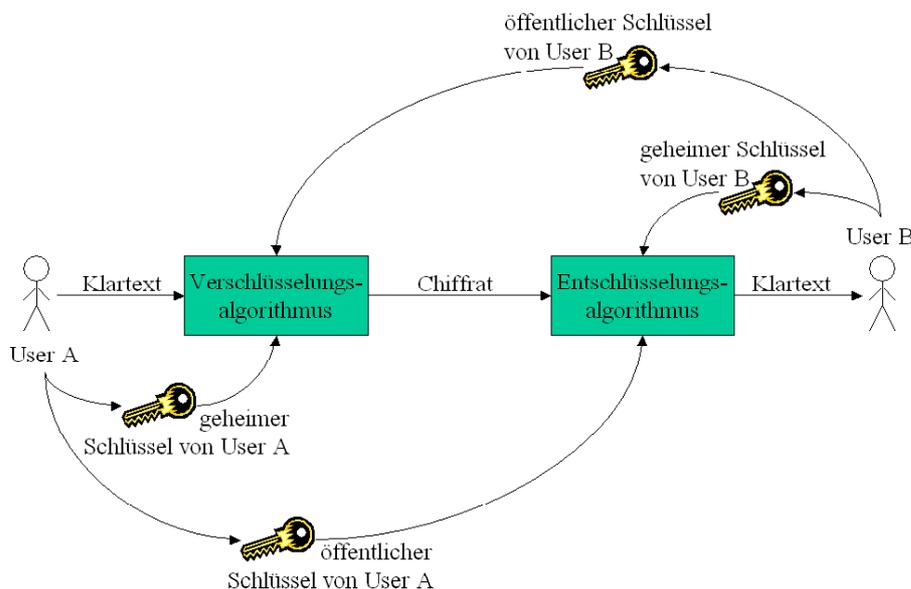


Abbildung 4.2 - vereinfachtes Modell des Public-Key-Verschlüsselungsverfahrens

Quelle: abgeleitet aus [Stallings 1995], S. 110

¹⁶² Vgl. zur Funktionsweise [Stallings 1995], S. 42 ff.

¹⁶³ Weiterführende Informationen zu AES sowie zum Rijndael-Algorithmus finden sich auf den entsprechenden Seiten des National Institute of Standards and Technology (NIST): <http://csrc.nist.gov/encryption/aes/>

¹⁶⁴ Vgl. zur Funktionsweise [Stallings 1995], S. 282 ff.

Asymmetrische Kryptographieverfahren bildeten eine revolutionäre Neuerung in der Welt der Verschlüsselung, zum einen basierten sie auf vollkommen neuen mathematischen Prinzipien (statt der in konventionellen Verfahren verwendeten Substitutions- und Permutationsmethoden), zum anderen sorgten sie für ein Ende der Austauschnotwendigkeit von geheimen Schlüsseln. Der zum Entschlüsseln eines Chiffrats notwendige öffentliche Schlüssel des Absenders der Nachricht wird zumeist in zentralisierten Key-Verzeichnissen (auf speziellen Servern) zur Verfügung gestellt. Das nicht nur besonders sichere, sondern auch einfach zu handhabende Verfahren findet deswegen gerade dort Anwendung, wo Daten in verschlüsselter Form zwischen nicht im Voraus bekannten Kommunikationspartnern erfolgen soll. Als bekanntes Beispiel für ein asymmetrisches Verschlüsselungsverfahren soll der nach einem Konzept von Diffie und Hellman entwickelte RSA-Algorithmus¹⁶⁵ genannt werden.

Neben den genannten existieren in der Praxis noch hybride Verfahren, die sich die Vorteile beider Kategorien zunutze machen: Mittels asymmetrischer Verschlüsselung wird ein einmaliger sogenannter Sitzungsschlüssel erstellt und übermittelt, mit dem zuvor die eigentlichen zu übertragenen Daten mit einem symmetrischen Verfahren verschlüsselt werden. Als Beispiel für eine hybride Technologie soll hier das Programm „Pretty Good Privacy“ (PGP)¹⁶⁶ genannt werden, welches eine verschlüsselte e-Mail-Kommunikation implementiert und in alle gängigen e-Mail-Programme eingebunden werden kann. PGP beruht auf dem asymmetrischen RSA, dem symmetrischen IDEA und beherrscht optional die transparente Komprimierung der zu übermittelnden Daten mit dem populären ZIP-Algorithmus.

Ein zweites Beispiel für hybride Verschlüsselungsverfahren stellt das für den Bereich des e-Commerce sicherheitstechnisch bedeutende SSL (Secure Sockets Layer) dar, welches ursprünglich von Netscape entwickelt wurde und in der HTTP-Protokoll-Erweiterung HTTPS (HyperText Transport Protocol Secure) Anwendung findet. Auch hier wird eine sichere Datenübertragung durch die Verwendung von asymmetrisch verschlüsselten, einmaligen Session Keys erreicht. Dabei ist SSL theoretisch für die Verwendung jedes Verschlüsselungsalgorithmus gedacht, die genaue Unterstützung ist hierbei abhängig vom eingesetzten Internet-Browser. Der Vollständigkeit halber soll in diesem Abschnitt auch die Technologie der digitalen Signatur Erwähnung finden, welche auf verschiedenen der genannten Algorithmen basieren kann. Gängige Verfahren bauen hier auf die Verwendung von RSA zur Verschlüsselung und zum Austausch eines zuvor erzeugten MD5-Hashwertes.

¹⁶⁵ Vgl. zur Funktionsweise [Stallings 1995], S. 121 ff. und S. 340 ff. (Diffie-Hellman Key-Exchange)

¹⁶⁶ <http://www.pgpi.org>, vgl. dazu auch [Stallings 1995], S. 361 ff.

4.5 Überwachung von kritischen Systemen

Eine weitere essentielle Sicherheitsfunktion stellt die automatisierte, auf einem zuverlässigen und – im Falle der Entdeckung einer Unregelmäßigkeit – beweis- und nachvollziehbaren Verfahren basierende Überwachung von im Kapitel 4.1 ermittelten wertkritischen Systemen dar. Dabei beruhen Überwachungsverfahren auf zwei gängigen Methoden, der Auswertung zuvor protokollierter Informationen (Logging) sowie dem Einsatz von Werkzeugen zur Erkennung von Eindringversuchen (sogenannten „Intrusion Detection Systeme“, IDS). Beide Methoden sollen im Folgenden eine kurze Vorstellung finden, wobei auf weiterführende Informationen zum Thema jeweils verwiesen wird.

Das weitaus wichtigste Werkzeug zur Erkennung von Systemmanipulationen stellt die Protokollierung (Logging) sicherheitsrelevanter Informationen sowie deren Auswertung durch den Administrator dar, wobei die genannte Auswertung entweder auf manuellen Vorgehensweisen oder, seltener, auf einem automatisierten Verfahren beruht. Ein vollständig autonom arbeitender Prozess wird in seiner Gesamtheit als „Auditing“ bezeichnet. Der Sinn der Protokollierung ist nicht nur die oben angeführte Erkennung von Systemmanipulationen, sondern auch die spätere Beweisführung des stattgefundenen Angriffs selbst sowie dagegen eingesetzter Sicherungsmaßnahmen – im Extremfall vor Gericht. Dahingehend haben auch Angreifer verschiedene automatisiert ablaufende Werkzeuge entwickelt, die alle Spuren eines Angriffs aus den Protokolldateien entfernen. Hier wird deutlich, dass in einer sicherheitsrelevanten Umgebung zusätzliche Protokollierungsströme zu einem alternativen Speicherort (andere Datei, spezieller Log-Server) essentiell sind. Die Notwendigkeit muss u.a. bei der Entwicklung einer detaillierten Protokollierungsstrategie berücksichtigt werden, wobei diese genau definierte Kriterien zu Programmen und Medien für das Logging sowie Verfahrensstandards für die Auswertung der mitgeschriebenen Informationen enthalten sollte¹⁶⁷. Die optimale Festlegung der angesprochenen Kriterien ist meist erst nach einiger Zeit der Überwachung und Protokollauswertung möglich, da viele Informationen erst im Nachhinein als sicherheitstechnisch relevant erkannt werden (und wiederum andere als nicht unbedingt notwendig). Die Auswahl des richtigen „Levels“, also der Menge der mitprotokollierten Informationen, ist entscheidend für die erfolgreiche Erkennung eines stattgefundenen Angriffs.

Intrusion Detection Systeme stellen eine zweite Methode zur Erkennung von eventuellen Eindringversuchen in Netzwerke bzw. Computersysteme dar. Obwohl der Begriff keine klare

¹⁶⁷ Zum Schutz vor Manipulationen an den Log-Dateien durch Angreifer bietet sich die Einbeziehung der Protokollierungslösung eines Drittanbieters an, da deren Verfahrensweise und Datenformate dem Angreifer i.d.R. weniger vertraut sind als die der systemeigenen Werkzeuge. Weiterführende Informationen sowie Verweise auf Protokollierungslösungen finden sich in [anonymous 2001], S. 306 ff.

Definition besitzt, kann man „Intrusion Detection“ mit „Erkennen unerlaubter Handlungen seitens eines Unbefugten zum Zwecke des Zugriffs auf ein System“ beschreiben¹⁶⁸. Heutige Systeme lassen sich nach ihrer Arbeitsweise in zwei Gruppen klassifizieren: Programme, die ein Computersystem auf einerseits Missbrauch oder andererseits Systemanomalien untersuchen¹⁶⁹. Erstere lassen sich wiederum in netzwerkbasierte (NIDS) und hostbasierte (HIDS) Lösungen einteilen. NIDS arbeiten passiv und suchen im über Netzwerke übertragenen Datenstrom nach für Angriffsversuche charakteristischen Mustern (Signaturen), während HIDS aktive Komponenten im Betriebssystem darstellen, die eine ständige Untersuchung von Systemprotokollen, Benutzeranmeldungen und laufenden Prozessen vornehmen¹⁷⁰.

Vor der Einführung eines IDS sollte zwingend die Implementierung grundlegender Sicherheitsfunktionalitäten (analog Kapitel 4.4) stehen, namentlich der Einsatz von Firewalls, Sicherheitsrichtlinien oder auch Virenschutzmechanismen. Keineswegs können IDS als ein erster Ansatzpunkt im Absicherungsprozess eines Unternehmensnetzwerks gelten.

4.6 Fortbildung und Schulung der Mitarbeiter

Alle der in Kapitel 4.4 aufgezählten Maßnahmen bieten keinen hinreichenden Schutz, wenn die Mitarbeiter des Unternehmens fahrlässig mit den vorhandenen IT-Ressourcen sowie dem Internet umgehen¹⁷¹. Zwar suggeriert die Einführung und Umsetzung von Richtlinien und administrativen Beschränkungen ein hohes Maß an Sicherheit, diese ist jedoch nur als oberflächlich und leicht penetrierbar zu betrachten, solange keine Sensibilisierung der Mitarbeiter hinsichtlich der IT-Sicherheit vorhanden ist.

Als Mittel für diesen Prozess stehen vor allem Fortbildungs- und Schulungsmaßnahmen zur Verfügung, wobei häufig seitens des Managements der Fehler gemacht wird, nur den verantwortlichen Führungskräften in den entsprechenden Abteilungen den Besuch derartiger (meist externer) Weiterbildungen zu ermöglichen. Das Anbieten interner Schulungsmaßnahmen wird dagegen meist sträflich vernachlässigt – auf diese Weise entsteht zwischen den Leitern der IT-Abteilung und den Beschäftigten im Unternehmen ein steiles Informations- und Wissensgefälle hinsichtlich der Bedeutung von Sicherheitsmaßnahmen. Regelmäßige Fortbildungsveranstaltungen könnten dagegen für einen gezielten Wissenstransfer sowie für die Klärung von

¹⁶⁸ aus [anonymous 2001], S. 290

¹⁶⁹ Letztere Methode wird i.d.R. nicht in Produktionsszenarien eingesetzt, da deren vollständige Funktionalität noch nicht nachgewiesen werden konnte, lediglich in Universitäten und Forschungsprojekten finden diese Systeme Anwendung. Einzelheiten zur Klassifizierung von IDS finden sich in [anonymous 2001], S. 290 f.

¹⁷⁰ Weiterführende Informationen zur Arbeitsweise und zu Auswahlkriterien der verschiedenen IDS-Verfahren finden sich in [anonymous 2001], S. 292 ff. sowie [Stallings 1995], S. 224 ff. (allgemeine Techniken zur Entdeckung von Eindringversuchen, insbesondere wird auf Tabelle 6.5, S. 233 verwiesen)

¹⁷¹ Vgl. dazu auch [Schweizer Versicherung 7/2001], S. 64

eventuellem Unverständnis gegenüber bestehenden Richtlinien sorgen. So ist das Erreichen einer hohen Sensibilisierung der Mitarbeiter für das Thema „interne Sicherheit“ möglich – mit dem Effekt, dass gerade die auf der Intention „Unwissenheit“ bzw. „Unabsichtlichkeit“, jedoch auch „Ignoranz“ beruhenden Gefährdungspotenziale für das Unternehmen kontinuierlich abgebaut werden. Dabei können die genannten Maßnahmen sowohl von internen als auch externen Anbietern durchgeführt werden, wobei auf ein hohes Maß an Kompetenz für das Thema „interne Sicherheit“ beim ausführenden Schulungsleiter zu achten ist. Ebenso sollte dieser pädagogische und methodische Erfahrungen besitzen.

Viele Firmen bieten entsprechende Fortbildungsprogramme als „In-House-Seminare“ an. Dabei ist jedoch zu beachten, dass diese niemals einen vollständigen Überblick bezüglich der momentanen Situation im Unternehmen gewährleisten können, so dass hier vorab zumindest eine grundlegende Analyse, z.B. durch Befragung von System- und Netzwerkadministratoren sowie durch Ausfüllen eines anonymen Fragebogens zum Risiko- und Sicherheitsbewusstsein unter den Beschäftigten durchgeführt werden sollte¹⁷².

¹⁷² Weiterführende Informationen zur Durchführung von Schulungsmaßnahmen finden sich im IT-Grundschutzhandbuch des Bundesministeriums für Sicherheit in der Informationsgesellschaft, siehe dazu [BSI 2002 GSHB 3005]

5 Versicherbarkeit von Internetrisiken

Wie schon in der Einführung erläutert, soll der Begriff Internetrisiken alle Arten von Netzwerkrisiken umfassen, d.h. der Begriff „Internet“ wird für die gesamtheitliche der Informationsbeschaffung zugrunde liegende Infrastruktur verwendet. Dies umfasst i.d.R. die Netzstrukturen innerhalb des Unternehmens (d.h. das Intranet), ein eventuell vorhandenes Extranet, sowie das meist über einen Internet Service Provider erreichbare Internet selbst. Mit den von den Risiken betroffenen Objekten sind gemeinhin alle am Netzwerk angeschlossenen Teilnehmer (Netzwerkknoten) und deren Verbindungen untereinander gemeint. Als Knoten im Netzwerk treten sowohl Computersysteme als auch spezialisierte Geräte wie Router, Switches und Gateway-Systeme auf.

5.1 Juristische Grundlagen

Die Absicherung von Internetrisiken eines Internet Service Providers oder einer auf Netzwerke spezialisierten Firma ergibt sich bereits aus dem Bürgerlichen Gesetzbuch. § 631 ff. BGB besagt, dass „jeder Werkleistende ... unbeschränkt für Personen- und sonstige Schäden (haftet) sowie dafür, dass die gelieferte Leistung fehlerfrei funktioniert und nicht mit Mängeln behaftet ist, welcher die Tauglichkeit diese Leistung einschränken“. Weiterhin bestimmt das vor kurzem in Kraft getretene Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), dass Geschäftsführer für vermeidbare Schäden durch mangelnde Netzwerksicherheit in vollem Umfang haftbar sind¹⁷³. Da hierbei nicht auf bestimmte Branchen abgestellt wird, führen heutzutage alltägliche Gefahren wie das Empfangen einer mit einem Virus infizierten e-Mail durch einen Mitarbeiter und dessen Ausbreitung innerhalb des Unternehmensnetzwerks oder sogar die weitergehende Infizierung externer Mailboxen von Geschäftspartnern zur Haftung des Geschäftsführers für entstehende Vermögensschäden¹⁷⁴.

Für Firmen, die Telekommunikationsdienstleistungen für Dritte erbringen (sogenannte „Carrier“, also auch Internet Service Provider), gilt eine unbeschränkte Haftung bei Vermögensschäden, die durch Vorsatz oder Fahrlässigkeit entstanden sind¹⁷⁵. Ein Call-Center, welches durch eine fahrlässige Handlung seitens des Kommunikationsdienstleisters weder über Internet (e-Mail) noch telefonisch erreichbar ist, oder auch ein Internet-Broker, der aufgrund des Ausfalls des Kommunikationsnetzwerks keine Aufträge mehr entgegennehmen und bestehen-

¹⁷³ Vgl. dazu [ZfV Nr.10/2000], S. 320

¹⁷⁴ Die Entstehung eines Sachschadens ist in einem solchen Fall eher unwahrscheinlich, theoretisch haftet der Geschäftsführer jedoch für alle entstehenden Schäden.

¹⁷⁵ Vgl. §40 Telekommunikationsgesetz (TKG) i.V.m. §7 Telekommunikationsdurchführungsverordnung (TKV)

de Order platzieren kann, sind Beispiele für die Entstehung von beträchtlichen Vermögensschäden innerhalb eines extrem kurzen Zeitraums.

Allein durch die genannten juristischen Gegebenheiten werden neue Risikopotenziale aufgebaut – nicht nur bei Unternehmen der IT-Branche, sondern in allen Firmen, in denen eine IT-Unterstützung für den Ablauf der Geschäftsprozesse maßgeblich ist. Herkömmliche Modelle decken diese Risikopotenziale nicht ab. Wenn z.B. eine wichtige Videokonferenz nicht zustande kommt, weil beim Betreiber des Netzwerks ein Server oder eine Verbindung ausfällt, entsteht dem Kunden kein Sach-, sondern ein reiner Vermögensschaden. Als Folge davon ist der Schaden durch die klassische Betriebshaftpflicht nicht gedeckt.

5.2 Aktuelle Gefahrenpotenziale

Einer bereits 1998 von der Kölnischen Rück unter 138 Internet Service Providern durchgeführten Umfrage¹⁷⁶ zufolge, die einen hohen Rückläuferanteil von 83 Prozent erreichte, erlitten davon 33 Prozent wirtschaftliche Schäden durch externe Angriffe und 30 Prozent Schäden durch Serverausfälle oder –überlastung. Weiterhin bestand bei zwei Dritteln der Befragten ein konkreter, bisher entweder nicht abgedeckter oder nicht abdeckbarer Versicherungsbedarf – am häufigsten nachgefragt wurden Versicherungen für externe Angriffe und Betriebsunterbrechungen.

Bei einer im Jahr 2000 in den USA durchgeführten Umfrage des Computer Security Institute (CSI) in Zusammenarbeit mit dem Federal Bureau of Investigation (FBI) wurden 643 Sicherheitsverantwortliche aus verschiedenen US-Unternehmen zu festgestellten sicherheitsrelevanten Problemen befragt. Immerhin drei Viertel der Befragten hatten in den vergangenen zwölf Monaten ernsthafte Angriffe gegen ihr Unternehmensnetzwerk festgestellt¹⁷⁷.

Solche Angriffe auf Unternehmensnetzwerke – und die damit verbundene „elektronische Verletzlichkeit“ eines Unternehmens – werden häufig von den Anlegern mit starken Wertverlusten an der Börse beantwortet. Besonders im heutzutage wichtigen Business-to-Customer-Geschäft (B2C) wirkt sich der entstehende Imageschaden schwerwiegend auf das Umsatzgeschehen aus. Vielfach wird von Unternehmen die Präsenz am Internetmarkt nur als Bereitstellung einer Website gesehen. Weiterführend bedeutet diese jedoch auch, kritische Datensysteme

¹⁷⁶ Internet Service Provider stehen mit dem Betrieb von Internetanbindungen als Bindeglied zwischen dem Internet einerseits und dem Unternehmensnetzwerk andererseits im Mittelpunkt eventueller Haftungsfragen. Vgl. dazu auch [ZfV Nr.13/1998], S. 372 ff.

¹⁷⁷ Vgl. dazu [ZfV Nr.17/2000], S. 604 ff. Als ernsthafte Angriffe werden hierbei (Distributed-) Denial-of-Service-Attacken, gezielte Sabotage von Daten und Netzwerken, sowie Eindringversuche in Computersysteme gewertet.

me mit Kunden, Geschäftsstellen, Zulieferern und privaten Netzwerken zu verbinden – in der Regel über das globale Internet hinweg.

Jedem Unternehmen muss dahingehend bewusst werden, dass – neben den klassischen Größen wie Umsatz – heutzutage zusätzliche Aktiva als kritisch zu betrachten sind: das „geistige Eigentum“ (elektronisch gespeicherte Daten und Know-How) sowie die „öffentliche Reputation“ und Ansprüche Dritter¹⁷⁸.

5.3 Generelle Betrachtung des Versicherbarkeitsbegriffs

Zur Entscheidungsfindung über die Versicherbarkeit von Internetrisiken ist zunächst die generelle Definition des Begriffes „Versicherbarkeit“ und seiner Merkmale wichtig. Nach Farny¹⁷⁹ gibt es keine allgemein bestimmbare Grenze für die Versicherbarkeit von Risiken, vielmehr ist diese von der Entscheidung der beiden am Versicherungsgeschäft beteiligten Parteien, also dem Versicherungsnehmer und dem Versicherer abhängig. Für beide ist dafür i.d.R. die Erzielung eines Nettonutzens aus dem Versicherungsgeschäft, d.h. dem eigentlichen Risikotransfer von Bedeutung.

5.3.1 Kriterien aus Sicht des Versicherers

Für den Versicherer beeinflussen nach Farny allgemein die nachstehenden drei Kriterien seine Entscheidung zur Versicherbarkeit eines bestimmten Risikos. Als erstes ist die jeweilige Entscheidungssituation des Versicherers, d.h. die von ihm aufgestellten Unternehmensziele sowie das Entscheidungsfeld (Erhaltungspolitik), maßgeblich. Ein weiteres Kriterium bildet der bereits vorhandene Versicherungsbestand, d.h. die Erwartungen hinsichtlich der Einfügung des zu versichernden Risikos darin sowie die Frage der vorhandenen Kapazitäten. Als drittes Kriterium dienen die Erfüllung verschiedener Merkmale zur Schadenverteilung des zu versichernden Risikos, namentlich die Zufälligkeit, Schätzung, Eindeutigkeit, Unabhängigkeit und Größenmerkmale. Die verschiedenen Merkmale sollen im Folgenden noch einmal näher erläutert werden.

Zunächst ist das Merkmal der Zufälligkeit der Schadenrealisation, d.h. des Eintritts eines Versicherungsfalls, Voraussetzung. Der Begriff steht für die Ungewissheit hinsichtlich der drei Schadenmerkmale Entstehung, Zeitpunkt und Schadensgröße sowie deren Unabhängigkeit vom (bewussten) Verhalten des Versicherungsnehmers. Da jedoch in der Versicherungspraxis auch fahrlässige, teilweise sogar grob fahrlässige Handlungen sowie von Vorsatz geprägte Ereignisse versichert sind, sind diese Merkmale meist nur in begrenztem Ausmaß erfüllt. Zu-

¹⁷⁸ Vgl. dazu [NZZ 11.04.2000]

¹⁷⁹ Vgl. dazu [Farny 2000], S. 37 ff.

sammenfassend lässt sich sagen, dass eine generell definierbare Grenze bezüglich der „Zufälligkeit“ als Voraussetzung für die Versicherbarkeit nicht existiert.

Eine weitere Voraussetzung, die Schätzung, steht für die Zuordnung numerischer Werte für die Wahrscheinlichkeitsverteilung der versicherten Schäden. Hierbei sind Begriffe wie der Erwartungswert oder die Streuung (Varianz) von Bedeutung. Der Schätzung liegen zumeist verschiedene Quellen, wie Zahlen aus dem innerbetrieblichen Rechnungswesen, Schadenstatistiken und Risikoanalysen, als objektive Werte zugrunde, die letztendlich ein subjektives Bild der zu erwartenden Schadenverteilung ergeben. Die Qualität der entstandenen Schätzungen ist dabei – je nach Qualität des zugrunde liegenden Datenmaterials – schwankend.

Ferner ist nach Farny die Eindeutigkeit der versicherten Schadenverteilung Kriterium der Versicherbarkeit. Dies betrifft die genaue materielle und formalrechtliche Definition sowohl der Merkmale des Versicherungsfalls als auch der versicherten Schäden (Gefahren).

Weiterhin ist die Unabhängigkeit der versicherten Schadenverteilungen untereinander Voraussetzung für die Versicherbarkeit, d.h. die Unmöglichkeit, dass durch ein Ereignis zufällig eine Schadenrealisation bei vielen oder sogar allen versicherungstechnischen Einheiten ausgelöst wird. Die hierbei angesprochene Kumulproblematik wird – im Zusammenhang mit über das Internet sehr schnell übertragbaren Viren und Würmern – noch Gegenstand einer detaillierten Betrachtung in Kapitel 5.5.4 sein. In der Versicherungspraxis wird das Kriterium laut Farny häufig so betrachtet, dass die Abhängigkeiten „ein gewisses Maß nicht überschreiten“ sollten.

Die letzte Voraussetzung stellt die Ausprägung der quantitativen Merkmale der Schadenverteilung dar, besonders die höchstmögliche Schadengröße (Possible / Probable Maximum Loss). Hier gilt i.d.R., dass diese relativ zur Größe des vorhandenen Versicherungsbestands und zu den risikopolitischen Möglichkeiten gesehen angepasst sein muss, da hohe Einzelschäden große und sogar ruinbringende Verluste im Versicherungsgeschäft mit sich bringen können. Dieses Kriterium wird auch als „Kapazitätsproblem“ bezeichnet. Häufig werden für ein diesbezüglich problematisches Risiko die Kapazitäten vieler Versicherer in einer Mitversicherung oder in einem „Versicherungs-Pool“ zusammengefasst.

Grundsätzlich kann man zu begünstigenden Merkmalen der Versicherbarkeit eines Risikos sagen, dass der Versicherer möglichst risikofreudig ist, einen großen – und hervorragend gestreuten – Versicherungsbestand besitzt, über sowohl qualitativ als auch quantitativ ausreichende Kapazitäten verfügt, das Risiko möglichst zufallsbestimmt, gut schätzbar, in den zu versichernden Schadenverteilungen eindeutig abgrenzbar sowie ein eventuell eintretender Schadenfall nach oben begrenzt ist und nicht mit anderen (Folge-) Schäden korrespondiert.

5.3.2 Kriterien aus Sicht des Versicherungsnehmers

Aus der Sicht des Versicherungsnehmers erfolgt meist dann eine negative Entscheidung hinsichtlich der Versicherbarkeit eines Risikos, wenn der Nutzen des Risikotransfers – also des Versicherungsgeschäfts – im Vergleich zur Prämie nur mäßig ist.

Man spricht dann von einem sehr niedrigen Schadenerwartungswert, welcher aus zwei Gründen resultieren kann: Entweder wird die Wahrscheinlichkeit des Schadeneintritts (sogenannte Schadenfrequenz) als minimal betrachtet, oder das sogenannte Schadenausmaß, d.h. die Schadensgröße, ist lediglich gering. In beiden Fällen ist das Verhältnis von Risikoprämie zu dafür erforderlichen Deckungsbeiträgen für Betriebskosten nicht gegeben.

Eine weitere Grenze für die Versicherbarkeit kann aus Sicht des Kunden in einer schwachen Zufallsausprägung der Schadenverteilung bestehen, wobei dies bei fast „sicher auftretenden“ Bagatellschäden der Fall ist. Diese Risiken werden nach Farny als eine Art „Geldwechselgeschäfte“ (Tausch der Prämie gegen eine fast sichere Versicherungsleistung) betrachtet, die jedoch mit einer hohen Belastung durch Betriebskosten einhergehen würden. Deshalb wird auch hier beim Versicherungsnehmer eine Grenze des erwarteten Nettonutzens aus dem Versicherungsgeschäft erzeugt.

5.4 Grundlegende Versicherbarkeit von Internetrisiken

Von Seiten des Versicherungsunternehmens her kann man Internetrisiken als Sicherheits-, Störungs- und Medienrisiken weiter unterteilen. Dabei stellen Sicherheitsrisiken alle Arten von Angriffen dar, die auf die Verletzung der Vertraulichkeit und Unversehrtheit von Daten abzielen – dazu zählen das Ausspionieren, die böswillige Änderung oder Zerstörung sowie die unerlaubte Veröffentlichung. Als Störungsrisiken werden alle – böswilligen und unabsichtlichen – Beeinträchtigungen der Verfügbarkeit von Ressourcen betrachtet, wobei es sich dabei sowohl um Netzverbindungen als auch Computersysteme handeln kann. Die zugrunde liegenden Ursachen für Störungsrisiken können vielfältig sein, Beispiele sind Viren, Stromausfall, Hardwarefehler oder auch Überlastung. Die dritte Kategorie ist heutzutage besonders problematisch, hier spielen vor allem der globale Charakter des Internets und die damit verbundenen Gefahren der Verletzung von Urheber-, Patent- und Markenrechten, wettbewerbsrechtlichen Verstößen sowie die Missachtung fremder Persönlichkeitsrechte (inhaltlich falsche Darstellung) eine bedeutende Rolle¹⁸⁰. Negativ begünstigt wird dies durch die offene Umgebung und interne Gesetzlosigkeit des Internets, außerdem ist es mit minimalem Aufwand für jedermann zugänglich. Da es zusätzlich keinen „Besitzer“ des Internets im engeren Sinne gibt, existiert

¹⁸⁰ Vgl. dazu [VB 06/2001], S. 26

dafür auch kein Verantwortungsträger. Unzählige offene Rechtsfragen, allen voran des anwendbaren Rechts¹⁸¹, komplettieren die heutige Situation.

Eigentlich kann man Internetrisiken dahingehend als nicht versicherbar bezeichnen, da diese nicht quantifizierbar sind und statistische Daten zu Schadenfrequenzen und Schadenausmaßen bislang fehlen. Dazu führt auch, dass viele Fälle von Computerkriminalität entweder nicht entdeckt oder trotz der Entdeckung der Öffentlichkeit nicht zugänglich gemacht werden¹⁸².

5.4.1 Einschätzung der Risikosituation im Unternehmen

Welche Computerrisiken im allgemeinen und Internetrisiken im speziellen sind überhaupt versicherbar? Dazu erarbeitete das Risk Management Magazine bereits im Jahr 2000 eine Studie, welche die verschiedenen Risiken und ihre Versicherbarkeit erläutert¹⁸³.

Zunächst ist für die fundierte Einschätzung der zu versichernden Risiken eine Unterscheidung zwischen geschäftlichen und technischen Risiken notwendig¹⁸⁴. Während bei letzteren – eine ständige Weiterentwicklung der technischen Standards vorausgesetzt – eine Konsolidierung der Gefahrensituation möglich ist, stellen die geschäftlichen Risiken, wie schon in Abschnitt 5.2 erläutert, aufgrund des transnationalen Charakter des Internets und den damit verbundenen komplexen Rechts- und Steuerfragen ein besonders großes Gefahrenpotenzial dar. Doch auch die technische Seite wird zunehmend von neuen Risikoarten geprägt, da einige Unternehmen der „New Economy“ lediglich virtuell im Internet existent sind. Demzufolge ist deren Abhängigkeit von der zugrunde liegenden Infrastruktur als besonders hoch zu bezeichnen¹⁸⁵. Auch die schnellstmögliche Umsetzung von Projekten im e-Business stellt heutzutage erhebliche Anforderungen an technische Gegebenheiten. Die damit verbundene teilweise Auflösung der Wertschöpfungskette trägt zwar zur raschen Erreichung von Ergebnissen bei (schnelles Time-to-Market, Rapid Prototyping), bringt aber auch neue Risiken mit sich, die oftmals – auch aufgrund des eben dargestellten Zeitdrucks – nicht genügend beachtet werden.

5.4.1.1 Risk-Management im Unternehmen

Die Basis für eine korrekte Einschätzung eventuell zu versichernder Risiken von Unternehmensseite aus ist zunächst die Implementierung eines funktionierenden Risk-Managements. Auf dessen Grundlage muss die Aufstellung und Abarbeitung eines Risk-Management-Zyklus

¹⁸¹ Staatsangehörigkeit des Domaininhabers, des Providers oder des Websitebesuchers (Kunden)

¹⁸² Vgl. dazu [ZfV Nr.10/2000], S. 320 ff.

¹⁸³ Die Zusammenfassung der Studienergebnisse steht online im Internet zur Verfügung: [Marsh 2000]

¹⁸⁴ Vgl. dazu [ZfV Nr.13/1998], S. 372 ff.

¹⁸⁵ Vgl. dazu [ZfV Nr.17/2000], S. 603 ff.

erfolgen, welcher genaue Punkte zum Management von Unternehmensrisiken vorgibt. Die wichtigsten sollen im Folgenden genannt werden.

Zum ersten ist eine Standortbestimmung, also eine Analyse der momentanen Situation im Unternehmen erforderlich. An diese schließt sich die Bewertung der dabei gefundenen Punkte an (Assessment), worauf die Erstellung eines Maßnahmenkataloges erfolgt. Die darin verankerten Maßnahmen müssen innerhalb eines vorab festgelegten Zeitraumes eine Umsetzung finden. Der gesamte beschriebene Prozess wird auch als (Risk-) Auditing bezeichnet. Wie schon aus der Bezeichnung „Risk-Management-Zyklus“ ersichtlich, erfolgt in regelmäßigen Zeitabständen ein Re-Auditing, wobei sich der Zeitraum zwischen zwei Durchläufen nach der individuellen Risikosituation im Unternehmen richtet.

Hierfür werden auch, beispielsweise von der ACE Insurance Europe, entsprechende Dienstleistungen¹⁸⁶ angeboten, vor allem in der Beurteilung von Aspekten der theoretischen und organisatorischen Schadenverhütung. Ergänzende Dienstleistungen für die Konfiguration von Firewall-Funktionen, Sicherheit von Servern, die Erarbeitung einer Notfallplanung sowie Lösungen zur Zugangs- und Zugriffskontrolle stehen ebenfalls zur Verfügung¹⁸⁷.

5.4.1.2 Konkrete Einschätzung eines zu versichernden Risikos

Die konkrete Einschätzung eines eventuell zu versichernden Risikos erfolgt i.d.R. in einem individuellen Prozess zwischen dem Unternehmen und dem Versicherungsunternehmen oder einem beauftragten Versicherungsmittler. In einem gemeinsamen Gespräch wird zunächst die Risikolage des Unternehmens analysiert. Das Ergebnis der Analyse können sowohl eine Versicherungslösung, aber auch andere Deckungen sein. Letztere werden häufig unter dem Punkt „Alternativer Risikotransfer“ (ART) zusammengefasst und haben den Charakter von umfassenden Dienstleistungen¹⁸⁸. Für das Funktionieren dieses Prozesses ist vor allem ein reibungsloses Zusammenspiel der Bereiche Risk-Management im Unternehmen und Underwriting auf Versichererseite¹⁸⁹ von Bedeutung.

Verschiedene Firmen bieten die Bewertung neuer Risiken für Versicherungsunternehmen als Dienstleistung an¹⁹⁰. Im Gegensatz zu anderen Groß- oder Kumulrisiken wie Naturkatastrophen, bei denen das Risiko kalkulierbar ist und eine datenbasierte Prämienberechnung nach Wahrscheinlichkeiten möglicher Schäden und möglicher Kosten erfolgen kann, sind Internetrisiken, wie z.B. das Eindringen eines Computervirus in eine Softwarefirma in ihren Auswir-

¹⁸⁶ ACE Risk Management Engineering Services

¹⁸⁷ Vgl. dazu [ZfV Nr.10/2000], S. 319 ff.

¹⁸⁸ Vgl. dazu [Schweizer Versicherung 7/2001], S. 64

¹⁸⁹ Vgl. dazu [Allianz 3/2001], S. 98

¹⁹⁰ In [HB 10.08.2001] wurde als Beispiel die Risqon GmbH vorgestellt: <http://www.risqon.de>

kungen kaum einzuschätzen. In so einem Schadenfall werden möglicherweise mit Viren behaftete Programme an die Kunden ausgeliefert und deren Computersysteme durch die Programminstallation infiziert. Im Endeffekt ist der durch ein derartiges Schadenereignis verursachte Vermögensschaden um ein Vielfaches höher als die Prämie, die der Versicherer über einen langen Zeitraum erwarten kann. Aufgrund der fehlenden statistischen Daten zu Schadenfrequenzen und Schadenhöhe kann zur Prämienberechnung nicht auf bestehende Kalkulationsprogramme zurückgegriffen werden, stattdessen findet eine Berechnung – wie auch im Falle des vorgestellten Unternehmens – mit Hilfe einer selbst entwickelten Computeranalyse der zu versichernden Risiken und Gefahren statt.

Dargestellte Erfahrungsberichte¹⁹¹ aus der Praxis belegen, dass in vielen Fällen zwar intuitiv angemessene Prämien berechnet werden, jedoch in einigen Fällen ein starkes Ungleichgewicht zwischen versichertem Risiko und zu zahlender Prämie besteht. Hierbei sind sowohl Verträge mit zu geringer Prämienzahlung als auch solche mit zu hoch angesetzter Prämie anzufinden. Eine differenzierte Analyse der zu versichernden Risiken bringt – neben ebenso stark differenzierten Prämien – vor allem zielsichere Gewinne und stabilisierte Erträge für das Versicherungsunternehmen. In dieser Hinsicht wird in den kommenden Jahren ein weiteres Aufbrechen der Wertschöpfungskette für Versicherungsunternehmen, gerade im Bereich Produktplanung und Risikobewertung, erwartet. Hier werden zunehmend externe Dienstleister die bislang beim Versicherer selbst vorgehaltenen Kompetenzen übernehmen oder zumindest ergänzen. Besonders im Hinblick auf von noch jungen Unternehmen angebotene Dienstleistungen zeigt sich die Versicherungsbranche jedoch extrem schwerfällig, so dass im Zweifelsfall lieber auf bekannte Geschäftspartner zurückgegriffen wird, ein Umstand, der es neuen, innovativen Unternehmen nicht leicht macht, in der Branche Fuß zu fassen.

Obwohl die bestehende Ungewissheit über Eintrittswahrscheinlichkeiten, Schadenhäufigkeit und Schadenhöhe eine fundierte Prämienkalkulation sowohl für Erst- als auch für Rückversicherer fast unmöglich macht, geht man trotzdem von einer grundsätzlichen Versicherbarkeit fast aller Internetrisiken aus¹⁹².

¹⁹¹ Im Artikel aus [HB 10.08.2001] wurde ein Großauftrag der Bayerischen Versicherungskammer an die Risqon GmbH beschrieben. Diese hatte Haftpflicht-Versicherungen für New Economy – Firmen in der IT angeboten, jedoch im Nachhinein Zweifel über die Prämienberechnung. Risqon nahm eine Neubewertung der zu versichernden Risiken vor, wobei jedes Unternehmen und dessen individuelle Risikosituation (Welche Produkte und Gefahren? Existiert ein Risikomanagement, eine Produktzertifizierung?) analysiert wurde. Am Ende diese Risikobewertungsprozesses steht ein stark differenziertes Bild der einzelnen Risiken.

¹⁹² Vgl. dazu [VW 12/2001], S. 956

5.4.2 Versicherungstechnische Analyse der IT-Sicherheit im Unternehmen

Wie schon in den Kapiteln 4.4 und 4.6 angeführt, besteht in den Unternehmen in zwei Kategorien Handlungsbedarf – zum einen in technischen Belangen, zum anderen in der Frage der Information und Sensibilisierung der Mitarbeiter für Fragen der Sicherheit. Hinsichtlich der letzteren Maßnahmen ist für die versicherungstechnische Frage nach dem spezifischen Risiko eine Klärung der Beachtung von Sicherheitsstandards, eines eventuell vorhandenen Widerstands in der Belegschaft und darauf aufbauenden administrativen und organisatorischen Regelungen, z.B. Sicherheitsschulungen der Mitarbeiter, eine essentielle Voraussetzung. Nur so kann von Versichererseite festgestellt werden, ob Mitarbeiter die Folgen einer Fehlbedienung oder fahrlässigen Handlung richtig einschätzen können.

Bei der Überprüfung von technischen Maßnahmen ist neben den in Kapitel 4.4 genannten Punkten vor allem das Vorhandensein und die Überwachung einer regelmäßigen Datensicherungslösung wichtig, da bei der Generierung, Speicherung, Veränderung und Übertragung von Daten jederzeit Fehler und Störungen eintreten können, die nur durch die Wiederherstellung eines konsistenten Datums behebbar sind¹⁹³.

Für die Bewertung der genannten Kriterien – wie auch zum aktiven Einwirken auf die Sicherheitspolitik im Unternehmen – ist die Einbeziehung von externen Gutachtern und spezialisierten Informationsdienstleistern zumeist unumgänglich¹⁹⁴.

5.5 Abdeckung durch traditionelle Herangehensweisen

Bis vor kurzem konnten reine Vermögensschäden (etwa hervorgerufen durch nachteilige Veränderungen von Daten) ohne einen vorherigen Sachschaden am versicherten Gegenstand nicht abgedeckt werden. Gerade diese Schäden prägen jedoch das typische Erscheinungsbild von Viren, Würmern oder auch DoS-Angriffen. Im Bereich traditioneller Versicherungen existieren lediglich Deckungen im Haftpflichtbereich, die zumeist an einen vorherigen Sachschaden gekoppelt sind, welche im Folgenden kurz vorgestellt werden.

5.5.1 Traditionelle Haftpflichtdeckungen

Um die Bedingungen eines durch die (Betriebs-) Haftpflicht abgedeckten Schadens zu erfüllen, ist zunächst die ausdrückliche Definition eines Schadens an Daten als Sachschaden not-

¹⁹³ Vgl. dazu [ZfV Nr.10/2000], S. 321

¹⁹⁴ Bei Vorhandensein entsprechender interner Kompetenzen beim Versicherer trifft dies nicht zu. Hier ist zudem die Chance des Outsourcing dieser Kompetenzen gegeben, um sie auch anderen Versicherern zur Verfügung stellen zu können.

wendig¹⁹⁵. Dies kann auch im Nachhinein durch die Erweiterung des Versicherungsvertrages geschehen. Die im Haftpflichtbereich angebotenen Produkte umfassen die Elektronikversicherung, die Elektronik-Betriebsunterbrechungsversicherung sowie die (erweiterte) Datenträgerversicherung¹⁹⁶. Dabei ist im Zusammenhang mit Internetrisiken lediglich die letzte der drei Deckungsformen relevant.

Die Datenträgerversicherung ist in Form von zwei Produkten auf dem Versicherungsmarkt anzutreffen. Die erstere, nicht erweiterte Form leistet analog zu den anderen Haftpflichtdeckungen nur bei nachteiliger Veränderung oder Verlust versicherter Daten durch einen dem Grunde nach versicherten Sachschaden am Datenträger oder Computersystem Schadenersatz. In der erweiterten Form ist dagegen – unabhängig von einem Sachschaden – auch bei Schäden durch Viren, Würmer oder vorsätzliche Programm- oder Datenmanipulation Dritter eine Deckung gewährleistet. Voraussetzungen für die Deckung ist die Umsetzung geeigneter Anforderungen an Schadenverhütung bzw. –minderung, z.B. die Durchführung einer regelmäßigen Datensicherung.

Eine Absicherung von Internetrisiken ist durch reine Haftpflichtdeckungen jedoch nicht möglich, da z.B. eine Betriebsunterbrechung nur bei einem vorangegangenen Sachschaden versichert ist, diese jedoch einen Großteil der Kosten bei einem Schadenfall ausmacht. Ebenso ist ein Ausfall externer Netze, wie z.B. das Wegfallen der Internetverbindung des Unternehmens, nicht in der Deckung enthalten. Dies gilt auch für andere Risiken, die außerhalb des Zugriffsbereichs des Versicherungsnehmers liegen¹⁹⁷.

5.5.2 Vertrauensschaden-Versicherung

Die „Vertrauensschaden-Versicherung“ (VSV) bietet dem Versicherungsnehmer, i.d.R. dem Unternehmer, Schutz vor Vermögensschäden, die ihm (oder seinem Unternehmen) insbesondere seine Mitarbeiter zufügen. Dabei umfasst der Versicherungsschutz die Bereiche Betrug, Untreue, Unterschlagung und Diebstahl. Dadurch werden Schäden abgedeckt, die Mitarbeiter Dritten, insbesondere Kunden des Unternehmens, unmittelbar zufügen, und für den das Unternehmen schadenersatzpflichtig ist. Dabei muss die Schädigung zwingend durch einen Vertrauensperson verursacht worden sein, Schäden durch außenstehende Dritte sind ausdrücklich ausgeschlossen¹⁹⁸. Aufgrund der charakteristischen Späterkennung intern verursachter, vorsätzlicher Schäden wird eine Karenzzeit von zwei Jahren zwischen Schadenereignis und Mel-

¹⁹⁵ Vgl. dazu [VB 6/2001], S. 26

¹⁹⁶ Vgl. dazu [VW 23/2000], S. 1856 ff.

¹⁹⁷ Dies schließt z.B. Outsourcing oder Hosting der Website bei einem Provider mit ein.

¹⁹⁸ Der Geschädigte muss in der Lage sein, den Namen des verursachenden Mitarbeiters anzugeben.

derung des Schadens an das Versicherungsunternehmen gewährt. Generell ausgeschlossen sind in der Computermisbrauch-Versicherung Schäden durch entgangenen Gewinn (Betriebsunterbrechung) sowie Risiken, die „üblicherweise“ durch andere Versicherungen, z.B. eine Elektronikversicherung, abgedeckt werden.

Eine spezielle Vertrauensschaden-Versicherung stellt die „Computermisbrauch-Versicherung“ dar, die besonders den Bereich der in Kapitel 3.11 genannten „internen Risiken“ abdecken soll. Sie bietet einen Schutz des Arbeitgebers vor Vermögensschäden aus Daten- bzw. Softwaremanipulationen durch seine Mitarbeiter, z.B. die Nutzer der EDV-Anlage des Unternehmens. Analog zur Vertrauensschaden-Versicherung sind Schäden durch Dritte vom Deckungsumfang ausgeschlossen. Eine weitere Form, die „Datenmissbrauch-Versicherung“, entspricht in ihren Grundzügen der Computermisbrauch-Versicherung, verzichtet jedoch in ihrer Deckung auf die Beschränkung des Kreises der Schadenverursacher auf die autorisierten Benutzer der EDV-Anlage. Somit werden auch Vermögensschäden ersetzt, die dem Unternehmen durch außenstehende Dritte zugefügt werden, eingeschlossen sind u.a. Hacker-Angriffe oder Diebstahl von Firmeninterna. Normalerweise ausgeschlossen dagegen sind Schäden durch unspezifische Gefahren im Internet, wie z.B. Computerviren und trojanische Pferde, sofern deren Eindringen in das Firmennetzwerk nicht vorsätzlich und nur zur Schädigung des betreffenden Unternehmens erfolgte.

5.5.3 Problematik bestehender Versicherungsprodukte

Traditionelle Versicherungsprodukte weisen im Zusammenhang mit der Versicherung von Internetrisiken eine Reihe erheblicher Einschränkungen und Probleme auf, die im Folgenden aufgezählt werden sollen.

Besonders betrifft dies Risiken, die mit herkömmlichen Produkte nicht abgedeckt werden können, für die jedoch ein großer Versicherungsbedarf besteht. Als Beispiele dafür sind u.a. Drittschäden durch Viren, Ansprüche Dritter wegen Nichterfüllung, Patent- sowie Urheberrechtsansprüche zu nennen. Ein weiteres Problem stellen die bislang stark begrenzten Limite für die Zahlung im Schadenfall dar¹⁹⁹. Außerdem sind bestehende Policen in der Deckung oft restriktiv ausgewählt, so dass eine Zahlung bei Schäden durch einen Angriff nur dann erfolgt, wenn von dessen Seite eine Bereicherungsabsicht vorgelegen hat²⁰⁰.

Des Weiteren sind am Markt befindliche Versicherungsprodukte durch generelle, nicht speziell auf die Versicherbarkeit von Internetrisiken beschränkte Mängel gekennzeichnet. Dies

¹⁹⁹ Vgl. dazu [VB Nr. 6/2001], S. 26

²⁰⁰ Vgl. dazu [ZfV Nr. 13/1998], S. 372 ff.

betrifft zum einen deren nach wie vor an der aufsichtsrechtlich geprägten Spartenentrennung ausgerichteten Merkmale. Statt dem damit verbundenen Transfer von singulären Risikoklassen wäre ein dem Bilanzschutz und anderen Unternehmensbedürfnissen angepasstes Produkt, welches den Schutz der Erfolgsrechnung bzw. Bilanz vor negativen Risikoauswirkungen zum Ziel hat, wünschenswert²⁰¹. Zum anderen ist die Auswahl der versicherten Objekte auch heute noch an physischen Eigentümern orientiert. Diese Einstellung ist jedoch nicht mehr zeitgemäß, da Wissen und Reputation eines Unternehmens, also das sogenannte „geistige Eigentum“, einen Großteil des Firmenwerts ausmachen. Im Gegensatz zu klassischen Versicherungsobjekten ist auch deren Wiederbeschaffung meist nicht möglich²⁰².

5.5.4 Problematik der Kumulbetrachtung

Die Kumulbetrachtung stellt bei Internetrisiken ein besonderes, weil nicht mit anderen Risikoarten vergleichbares Problem für die Versicherungswirtschaft dar. Dies resultiert daraus, dass durch Internetrisiken entstehende Schadenszenarien – im Gegensatz zu Naturkatastrophen – in ihren Auswirkungen geographisch unbegrenzt und nicht kontrollierbar erscheinen.

Durch die exponentielle Verbreitung von schadenauslösenden Programmen über das Internet ist die Anzahl der potenziell von einem Schadenfall betroffenen Kunden letztlich nicht eingrenzbare. Als Folge davon versagen die herkömmlichen Berechnungsmodelle für Kumulsituationen²⁰³. Für die Prämienkalkulation von Kumulereignissen nach herkömmlichen Verfahren werden bestimmte Komponenten benötigt, die im Bereich der Internetrisiken nicht genau definierbar sind. Dies betrifft zum einen die genaue Definition des Ereignisses mit seiner Eintrittswahrscheinlichkeit und durchschnittlicher Schadenhöhe, zum anderen die Berücksichtigung zusätzlicher Kumule aus weiteren Versicherungszweigen. Aufgrund dessen ist die Möglichkeit einer Modellbetrachtung nicht gegeben²⁰⁴.

In einer Expertenrunde der „Cyberliability-Gruppe“ der Bayerischen Rück mit externen Fachleuten wurde zudem deutlich, dass eine Modell- bzw. stochastische Betrachtung nicht nur kaum realisierbar, sondern auch lediglich bedingt sinnvoll erscheint. Da bestehende Modelle für die Kalkulation herkömmlicher Risiken, wie z.B. Naturkatastrophen, entwickelt wurden, müssen bei Internetrisiken neue Methoden der Kalkulation gefunden werden. Ein erster Schritt in diese Richtung stellt die grundlegende Kategorisierung der Risiken dar, wobei zwischen sogenannten „Safety Risks“ und „Security Risks“ unterschieden wird. Erstere stellen

²⁰¹ Vgl. dazu [ZfV Nr. 17/2000], S. 605

²⁰² Vgl. dazu [NZZ 11.04.2000]

²⁰³ Vgl. dazu [Allianz 3/2001], S. 97

²⁰⁴ Vgl. dazu [VW 12/2001], S. 956

die rein technischen Risiken dar, d.h. Gefahren, die ohne jede Einflussnahme von Menschen-
seite an Netzwerken oder Computersystemen bestehen. Während diese bereits gut überschaubar
und planbar hinsichtlich ihres Risikopotenzials erscheinen, stellt die zweite Kategorie ein
weit größeres Problem für die Risikokalkulation dar. Dies besteht vor allem darin, dass jegliches
Gefahrenpotenzial, welches durch die Einwirkung eines menschlichen Faktors in nicht
unerheblichem Umfang geprägt ist, nicht genau in seinen Auswirkungen beschrieben werden
kann.

5.6 Alternative Versicherungskonzepte

Wie schon in Kapitel 5.5.3 aufgezeigt, werden von Unternehmensseite heutzutage neue,
„durchgeschriebene“ Versicherungskonzepte²⁰⁵ bevorzugt. Diese besitzen charakteristisch
eine erheblich stärkere Kundenorientierung und zeichnen sich durch ein knapperes, übersichtlicheres
Wording aus. Unsicherheit entsteht jedoch oftmals durch die in diesem Bereich noch
nicht vorhandene Rechtsprechung.

An neue Risikofinanzierungslösungen werden zudem bestimmte Kriterien angelegt. Dies be-
trifft die Bereitstellung größerer Kapazitäten, eine höhere Effizienz des Risikotransfers sowie
das Anbieten ergänzender Serviceleistungen, etwa im Bereich des Risk-Managements. Wei-
terhin wird die Übernahme auch traditionell als „nicht versicherbar“ geltender Risiken gefor-
dert. Daraufhin entstandene innovative und ganzheitliche Lösungen werden auch als „Alterna-
tive Risk Transfer“ (ART) bezeichnet und tragen sehr individuelle Merkmale. Geboten wer-
den mehrjährige Deckungen sowie ein Risikoausgleich über die Zeit und innerhalb des Port-
folios. Somit wird eine wirksame Unterstützung des Bilanzschutzes verwirklicht. Die Produk-
te werden teilweise unter Nutzung des Kapitalmarktes angeboten und schließen z.B. Captives,
Finite-Risk-Lösungen, Multi-Line-/Multi-Year-Lösungen und Multi-Trigger-Produkte ein²⁰⁶.
Voraussetzungen für alle ART-Lösungen stellt das Vorhandensein eines proaktiven, ganzheitlich
ausgerichteten Risk-Managements im Unternehmen dar.

5.7 Neue Versicherungsprodukte

In diesem Kapitel sollen zwei neue Versicherungslösungen, die aktuell am deutschen Markt
verfügbar und zu zeichnen sind, kurz vorgestellt werden. Dabei handelt es sich zum einen um
das Produkt „Data Guard“ von ACE Insurance und zum anderen um die Police „CyberSecurity
for Financial Institutions“ von Chubb.

²⁰⁵ Darunter sollen Produkte verstanden werden, welche eine Versicherungsdeckung unabhängig von der Scha-
denart ermöglichen, diese werden auch als „All-Risk“ Lösungen bezeichnet.

²⁰⁶ Vgl. dazu auch [ZfV Nr.17/2000], S. 607 ff.

Neben den hier genannten existieren am deutschen Markt nur wenige zu zeichnende Produkte zur Versicherbarkeit von Internetrisiken, so z.B. die Versicherungslösung „eComprehensive“ der JLT-Group. Hierbei ist auch anzumerken, dass viele Versicherungsunternehmen ihre Angebote dahingehend nach den gerade für Versicherungsunternehmen geschäftskritischen Ereignissen des 11. September 2001 vorerst eingestellt haben. Dazu zählen u.a. die „Netzverfügbarkeitsversicherung“ der Allianz-Gruppe sowie das Produkt „NetSecure“ des Versicherungsmaklers Marsh.

Weitere Produkte, wie z.B. die „Hacker-Police“ von Hiscox, sind nicht am deutschen Versicherungsmarkt erhältlich und bieten sich daher nicht für eine Betrachtung an.

5.7.1 ACE – „Data Guard“

Mit dem Versicherungsprodukt „Data Guard“ bietet ACE Insurance Europe ein modulares Konzept aus verschiedenen, auch einzeln erhältlichen Deckungsbausteinen an, die je nach individuellem Versicherungsbedarf zu einer Gesamtlösung zusammengestellt werden können. Bei den drei Modulen handelt es sich um die „Computerkriminalitäts-Versicherung“, die „Erweiterte Software-Versicherung“ und das Zusatzmodul „Betriebsunterbrechungsversicherung / Mehrkosten“. Die drei miteinander kombinierbaren Bausteine sollen im folgenden Abschnitt einzeln betrachtet werden.

5.7.1.1 Deckungsbausteine des Versicherungsproduktes

Im ersten Baustein, der „Computerkriminalitäts-Versicherung“, sind als versicherte Objekte Gegenstände des allgemeinen Finanz- und Sachvermögens sowie ausdrücklich Daten, Computer- und Netzwerk-Serviceleistungen sowie Betriebsunterbrechungskosten aufgeführt. Zu den versicherten Schadenursachen aus dem Bereich der technischen Risiken zählt die vorsätzliche (unerlaubte) Benutzung von Computern, Modifizierung von Daten und Zugangsverhinderung („Denial of Service“ bzw. „Denial of Access“). Ebenso sind nicht-technische Ursachen wie Erpressung sowie Betrug, Unterschlagung und Diebstahl von Vermögenswerten abgedeckt. Im Schadenfall werden zunächst die Kosten für Schäden an versicherten Vermögenswerten sowie Wiederherstellungskosten für Daten, Computer und Netzwerkinfrastruktur ersetzt. Bei einer Betriebsunterbrechung entstehende Aufwendungen, zusätzlich auch eventuell entstehende Mehrkosten z.B. durch die kurzfristige Schaltung eines alternativen Internetzugangs, werden ebenfalls vom Versicherer beglichen. Der Einschluss der Betriebsunterbrechung ist allerdings explizit erforderlich. Für den Versicherungsmarkt revolutionär ist der vorgesehene Kostenersatz für einen erhöhten Werbeaufwand, die Zahlung von Honoraren für beauftragte externe Krisenberater sowie von eventuellen Erpressungsgeldern.

Das zweite Modul, die „Erweiterte Software-Versicherung“, schließt grundsätzlich alle Daten und Datenträger als versicherte Objekte ein. Zu den zusätzlich zur „Computer-Kriminalitätsversicherung“ abgedeckten Schadenursachen zählen der Verlust oder die Veränderung von Daten durch fehlerhafte Bedienung, Blitzschlag, Stromausfall oder Ausfall der Telekommunikationsinfrastruktur. Ersetzt werden neben den Wiederherstellungskosten der versicherten Daten eventuelle Ersatzkosten für Programmlizenzen, zusätzliche Betriebskosten sowie Belastungen aus einer aufgrund des versicherten Schadenfalls entstehenden Betriebsunterbrechung.

Innerhalb des dritten und letzten Bausteins, der „Betriebsunterbrechungs-Versicherung“, werden die folgenden Kosten ersetzt, wobei als maximale Haftzeit eine Begrenzung von zwölf Monaten vorgesehen ist. Zum einen sieht die Police den Ersatz des aufgrund der Betriebsunterbrechung entgangenen Gewinns vor, der vor Steuern in dem betreffenden Zeitraum erzielt worden wäre. Zusätzlich dazu werden die laufenden Betriebskosten einschließlich aller Löhne und Gehälter für diesen Zeitraum vom Versicherer übernommen. Weiterhin beinhaltet die Betriebsunterbrechungs-Versicherung den Ersatz von Mehrbelastungen für Maßnahmen zur Begrenzung des Zeitraums der Betriebsunterbrechung. Hierzu zählen u.a. Kosten für die Anwendung alternativer Arbeitsverfahren, die Benutzung zeitweilig angemieteter Ersatzanlagen, die Inanspruchnahme von Dienstleistungen Dritter sowie eventuell entstehenden zusätzlichen Personal- oder Arbeitsaufwand.

5.7.1.2 Vorgehensweise bei der Zeichnung des Produktes

Die „Data Guard“ Police bildet mit einem Volumen von 4.700.000 Euro den größten Vertragsbestand der ACE Insurance in Europa. Dabei liegen nach eigenen Angaben 70 Prozent der Prämien über 100.000 € Als Zielbranchen für das Produkt werden vor allem Finanzinstitute, aber auch Dienstleistungsunternehmen, besonders im IT- und Telekommunikationsbereich, angesehen.

Vor der Angebotserstellung der Police wird eine Analyse des zu versichernden Unternehmens mittels eines Kurzfragebogens vorgenommen, der zur Einschätzung dessen IT-Sicherheitsphilosophie sowie des Kundeninteresses am Versicherungsschutz dienen soll. Weiterhin wird bereits vor Herausgabe eines unverbindlichen Angebots ein Treffen mit dem IT-Sicherheitspersonal des Unternehmens durchgeführt. Ausdrücklich nicht in der Police enthalten ist die Deckung von Schäden durch Computerviren, diese wird jedoch als separater Versicherungsbaustein angeboten. Wird deren Einschluss in die Versicherungslösung gewünscht, müssen noch zusätzliche sicherheitstechnische Mindestvoraussetzungen erfüllt sein.

Die Kapazitäten des Produktes liegen nach Angaben des Versicherungsunternehmens bei 25.000.000 € Jahreshöchstleistung, wobei für vorsätzliche Handlungen ein Sublimit von 10.000.000 € gilt. Ersatzleistungen für Schäden aufgrund von Computerviren sowie Kosten für erhöhte Werbeaufwendungen sind auf eine Höhe von maximal 10 Prozent der vereinbarten Versicherungssumme begrenzt.

5.7.1.3 Obliegenheiten des Versicherungsnehmers und explizite Ausschlüsse

Der Versicherungsnehmer muss zur Aufrechterhaltung des Versicherungsschutzes mindestens einmal wöchentlich eine Sicherung seines Datenbestandes vornehmen und diese an einem sicheren Ort, welcher außerhalb der Betriebsstätte gelegen ist und gegen Feuer und Wassereinbruch hinreichend geschützt ist, verwahren. Ebenso ist die Einhaltung der Vorschriften und Hinweise des Herstellers zur Wartung und Pflege von Computersystemen und Datenträgern in den Versicherungsbedingungen festgeschrieben. Bei Verletzung der genannten Regeln in der Art, dass ein Einfluss auf den Eintritt des Versicherungsfalls im Umfang des eingetretenen Schadens vorliegt, ist der Versicherer von der Leistung frei.

In der Computer-Kriminalitätsversicherung sind – neben Schäden durch Hoheitsakte, Kernreaktion und vorsätzliche Taten durch Organe des Versicherungsnehmers – zum einen Schäden, die durch Zufall oder Fahrlässigkeit verursacht werden²⁰⁷ oder infolge einer Sachbeschädigung am versicherten Gegenstand entstehen, zum anderen alle Aufwendungen, die aus der Haftung gegenüber Dritten entstehen, explizit ausgeschlossen. Der zugrunde liegende Haftungsgrund im letzten Fall ist dabei unerheblich.

In der Erweiterten Software-Versicherung sind im Entwicklungsstadium befindliche Programme generell als versicherte Gegenstände ausgeschlossen. Ein gravierender Einschnitt besteht in der Nichthaftung für Schäden durch böswillige bzw. vorsätzliche Handlungen von jeglichen Personen, wodurch auch Angriffe durch Hacker und Cracker nicht als versicherte Gefahren gelten. Ebenso werden keine Kosten im Zusammenhang mit Programmfehlern, des weiteren Sachschäden an der Computerhardware (mit Ausnahme der versicherten Datenträger) sowie – analog zur Computer-Kriminalitätsversicherung – Kosten aufgrund von Haftungsansprüchen durch Dritte ersetzt.

Für die Betriebsunterbrechungs-Versicherung gilt in jedem Fall ein zuvor vereinbarter Selbstbehalt, der in der Police als eine Anzahl von Tagen festgeschrieben wird. Ausgeschlossene Gefahren innerhalb der Betriebsunterbrechungs-Versicherung sind vor allem Kosten im Zusammenhang mit Programmierungs- oder Softwarefehlern sowie aufgrund von menschlichem

²⁰⁷ Hierzu zählt vor allem die versehentliche oder unrichtige Modifizierung bzw. Löschung von Daten.

Versagen oder fehlerhafter bzw. unbeabsichtigter Dateneingabe. Im letzteren Fall sind jedoch dadurch eventuell entstehende Mehrkosten versichert.

5.7.2 Chubb – „CyberSecurity for Financial Institutions“

Der Fokus des „CyberSecurity for Financial Institutions“ von Chubb liegt – wie schon in der Produktbezeichnung deutlich wird – auf Firmen des Finanzsektors. Durch neue Aktivitäten im Bereich des e-Commerce, neue Möglichkeiten des globalen Transfers und leichte Verfügbarkeit finanzieller Mittel ist diese Branche seit einiger Zeit besonders anfällig für Sicherheitsdelikte. So ist es heutzutage für einen Finanzdienstleister möglich, überall und jederzeit Schäden zu erleiden, ohne dass der verantwortliche Täter physisch in das Unternehmen eindringen muss. Stattdessen hat er die Möglichkeit, sich über das Internet Zugang zu den entsprechenden Netzwerken der Finanzdienstleister zu verschaffen und so strafbare Handlungen zu begehen. Eine Nachverfolgung von dabei hinterlassenen „elektronischen“ Spuren ist sehr schwierig und führt – gerade bei Straftaten aus „Offshore“-Zentren – meist nicht zu den wirklichen Tätern.

Eine spezielle „Cyber-Deckung“ zur Absicherung der genannten Risiken für Finanzdienstleister wird seit Ende 2001 in Deutschland von Chubb angeboten und beinhaltet in einer Police Elemente einer Computer- und Datenmissbrauchs- sowie einer klassischen Sachversicherung. Darüber hinaus sind nicht nur eigene, sondern auch Drittschäden, z.B. bei der widerrechtlichen Nutzung entwendeter Kundendaten, abgedeckt.

Die Police setzt sich aus verschiedenen Deckungsbausteinen zusammen, die das Unternehmen zu einer individuellen Versicherungslösung zusammensetzen kann. Diese Bausteine sind „E-Theft“ (Cyber-Diebstahl), „E-Service – Denial or Impairment of Service“ (Betriebsunterbrechung und Mehrkostendeckung), „E-Communication“ (Elektronische Anweisungen von Kunden und Unternehmen), ferner „E-Vandalism“, „E-Threat“ (Erpressung), „E-Signatur“ sowie „Voice Initiated Funds Transfer Instruction“ (Telefonbanking). Ein letzter Baustein ersetzt eventuelle Schadenfeststellungskosten. Die genannten Bausteine sollen im folgenden Abschnitt näher vorgestellt werden.

5.7.2.1 Deckungsbausteine des Versicherungsproduktes

Der erste Baustein „E-Theft“ (Cyber-Diebstahl) ersetzt dem Finanzdienstleister Vermögensschäden für eine vorgenommene elektronische Überweisung, Auszahlung, Freigabe bzw. Herausgabe von Vermögenswerten, sofern diese unmittelbar auf einen elektronischen Angriff, gefälschte elektronische Anweisung oder betrügerische Dateneingabe zurückzuführen sind. Des Weiteren besteht ein Versicherungsschutz vor elektronischem Diebstahl durch Personen,

die sich unberechtigt Zugriff auf das Computersystem des Finanzdienstleisters verschafft oder – im Falle eines Mitarbeiters – ihre eigenen Autorisierungen überschritten haben. Dabei sind Schadenersatzansprüche Dritter aufgrund von Datenmissbrauch ebenfalls gedeckt.

Im zweiten Deckungsbaustein „E-Service“ (Betriebsunterbrechung und Mehrkostendeckung) werden der entgangene Gewinn sowie eventuelle Mehrkosten für eine Beeinträchtigung oder Unterbrechung der Geschäftstätigkeiten, welche aufgrund einer zielgerichteten Denial-of-Service-Attacke oder eines unberechtigten Zugriffs auf das Computersystem des Finanzdienstleisters notwendig wird, vom Versicherer ersetzt. Der Begriff Mehrkosten umfasst dabei alle für eine baldige Wiederherstellung der Geschäftstätigkeit erforderlichen Gelder. Ebenfalls eingeschlossen sind eventuell notwendige Kosten für Öffentlichkeitsarbeit und Werbung, um das verlorene Vertrauen von Kunden wiederzugewinnen.

Im Modul „E-Communication“ (Elektronische Anweisung) werden alle Vermögensschäden abgedeckt, die den Kunden des Unternehmens oder Dritten dadurch entstehen, dass diese aufgrund einer elektronischen Anweisung Geld oder Vermögenswerte auszahlen, überweisen oder aushändigen, diese Anweisung jedoch entweder gar nicht vom versicherten Unternehmen stammte oder aber in ihrem Inhalt betrügerisch verändert wurde. Mit eingeschlossen sind Kosten zur Abwehr unberechtigter bzw. zur Befriedigung begründeter Schadenersatzansprüche.

Auf die Absicherung von Vermögensschäden aufgrund der böswilligen Veränderung, Löschung oder Zerstörung von Daten und Programmen der Internetpräsenz des versicherten Unternehmens zielt der Baustein „E-Vandalism“ (Cyber-Vandalismus). Hierbei sind Viren, Würmer sowie Verunstaltungen und Veränderungen der Webseite mit eingeschlossen. Ersetzt werden von der Versicherung alle direkten Kosten zur Wiederherstellung der Integrität der Internetpräsenz sowie wiederum Kosten aus Schadenersatzansprüchen Dritter, z.B. gegen zeitweilige Beschränkungen oder Unterbrechungen des Zugangs zum Online-Banking des Finanzdienstleisters.

Das Modul „E-Threat“ (Cyber-Erpressung) deckt das Risiko einer möglichen Schließung der Internetpräsenz aufgrund einer Erpressung des versicherten Unternehmens dahingehend, dass die bei einer angedrohten Umgehung von Sicherheitsmechanismen und anschließenden Kompromittierung von Kundendaten (Veröffentlichung, Modifizierung oder Zerstörung) entstehenden theoretischen Kosten für die Abwendung und Minderung von Schäden vorsorglich ersetzt werden. Einzige Bedingung für die Leistung ist deren theoretische technische Machbarkeit, der eigentliche Schadenfall muss nicht abgewartet werden. Weiterhin versichert sind Gebühren und Aufwendungen für unabhängige Vermittler, Gutachter sowie PR-Berater zur

Klärung des Sachverhaltes. Damit ist dieser Baustein einzigartig in seiner Gestaltung, da eine Leistungserbringung bereits aufgrund der theoretischen Möglichkeit des Eintritts eines Schadenfalls erfolgt. So wird das versicherte Unternehmen vor dem Druck der Schließung seiner Internetpräsenz wegen Sicherheitsbedenken bewahrt.

Der vorletzte Deckungsbaustein „E-Signature“ (Elektronische Signatur) ist lediglich bei Einschluss von Versicherungsschutz für Geschäftstätigkeiten in den USA, und dort wiederum im Bereich von Hypothekendarlehen, von Bedeutung. Durch ihn werden Vermögensschäden, welche aufgrund der unrichtigen Annahme eines hypothekarisch gesicherten Darlehensvertrages entstehen, abgedeckt. Als Bedingung für die Versicherungsleistung muss dieser mit einem elektronisch übertragenen Dokument übermittelt worden sein, welches eine gefälschte elektronische Signatur beinhaltet.

Wenn dem versicherten Unternehmen Vermögensschäden durch eine vorgenommene Überweisung, Auszahlung von Geld oder Vermögenswerten bzw. der unrechtmäßigen Vergabe von Krediten, die aufgrund einer telefonischen Anweisung ausgeführt wurden, entstehen, werden diese durch den Deckungsbaustein „Voice Initiated Funds Transfer Intention“ (Telefonbanking) ersetzt. Dabei muss der Anrufer den Finanzdienstleister vorsätzlich dahingehend getäuscht haben, ein Kunde oder Geschäftspartner zu sein.

Der letzte, die übrigen Deckungsmodule lediglich ergänzende Baustein namens „Schadenfeststellungskosten“ ersetzt dem Versicherungsnehmer Belastungen, die aufgrund der Feststellung der Schadenhöhe eines in diesem Abschnitt beschriebenen Schadens entstehen, sofern diese notwendig und angemessen sind. Hierzu zählen vor allem Kosten, welche dem Unternehmen für die Hinzuziehung eines externen Gutachters oder Sachverständigen entstehen.

5.7.2.2 Vorgehensweise bei der Zeichnung des Versicherungsproduktes

Das Versicherungsunternehmen wird vor der Möglichkeit zur Zeichnung des Versicherungsproduktes eine Risikoanalyse durch ein umfassendes Sicherheits-Audit durchführen. Dabei bleibt offen, ob es sich bei den Durchführenden um externe Gutachter handelt. Laut Chubb ist jedoch die Anfertigung eines unverbindlichen Versicherungsangebots aufgrund der Beantwortung eines detaillierten Fragebogens zur IT-Sicherheit bereits möglich. Abgefragt werden u.a. Angaben zu bisherigen Schäden sowie zum Vorhandensein eines unternehmensinternen Risiko- und Sicherheitsmanagements im IT-Bereich. Allenfalls ist die Notwendigkeit eines tiefergehenden Gespräches zwischen dem Underwriting des Versicherers und dem Finanzdienstleister, abhängig von den Ergebnissen des Fragebogens, möglich, bevor das angesprochene unverbindliche Angebot zur Versicherungslösung erstellt werden kann.

Bei der Prämienkalkulation wird neben der Höhe des Selbstbehalts sowie der gewünschten Schadenssumme auch das Vorhandensein eines Präventionsmanagements im IT-Bereich des Versicherungsnehmers berücksichtigt.

5.7.2.3 Obliegenheiten des Versicherungsnehmers und explizite Ausschlüsse

Explizite Ausschlüsse umfassen z.B. jegliche entgangene Gewinne (Betriebsunterbrechung sowie Mehrkosten), sofern diese nicht eindeutig im Deckungsbaustein „E-Service“ (5.7.2.2) Erwähnung finden, außerdem Schadenfälle aus dem Bereich „E-Theft“ (5.7.2.1) sowie „E-Communication“ (5.7.2.3), welche unter Einflussnahme eines Mitarbeiters des Unternehmens verursacht wurden. Ebenfalls ausgeschlossen sind Vermögensschäden aus sogenannten „Punitive damages“ (Schäden mit Strafcharakter), für die der Versicherungsnehmer gesetzlich haftbar zu machen ist, wobei diese Klausel als typischerweise in US-amerikanischen Versicherungsverträgen enthalten anzusehen ist.

Eine weitere wichtige ausgeschlossene Schadenursache umfasst die klare Abgrenzung der verschiedenen Erscheinungsformen von gefälschten, jedoch vom Finanzdienstleister, einem Partner oder Kunden trotzdem ausgeführten Anweisungen. Dahingehend ist geregelt, dass die Anweisung entweder in elektronischer Form, z.B. als e-Mail, oder aber als Telefax vorliegen muss, im Fall des „Telebanking-Bausteines“ auch in Form eines Telefongesprächs. Alle anderen Formate befreien den Versicherer eindeutig von der Leistungserbringung.

Zuletzt ist der Versicherer bei Vermögensschäden aufgrund von Rechtsverletzungen in Copyright-Fragen, Patenten, Handelsmarken sowie Geschäftsgeheimnissen generell von der Leistung freigestellt.

5.7.3 Bewertung der vorgestellten neuen Versicherungsprodukte

Zur Bewertung der beiden exemplarisch vorgestellten Versicherungsprodukte kann zunächst gesagt werden, dass beide einen ganzheitlichen Ansatz hinsichtlich der Versicherung internet-typischer Risiken verfolgen und somit eine bessere Lösung, verglichen mit traditionellen Deckungen im IT-Bereich, bereitstellen. Die „Data Guard“ Police von ACE ist wegen des Ausschlusses von Haftungsansprüchen Dritter gegenüber dem versicherten Unternehmen nicht als alleinige Lösung empfehlenswert. Hier sollte der Versicherungsnehmer die anderweitige Schließung dieser Deckungslücke anstreben, dafür bieten sich möglicherweise auch Lösungen aus dem Bereich des alternativen Risikotransfers an.

Die Chubb-Police ist, da auf den Bedarf von Dienstleistungsunternehmen aus dem Finanzsektor zugeschnitten, nicht für den IT-Bereich jeder Firma anwendbar. Eine Bewertung der Versicherungslösung fällt zudem schwer, da sie stark auf den amerikanischen Versicherungs-

markt ausgerichtet ist, was vor allem in den verschiedenen Ausschlussklauseln deutlich zum Tragen kommt. Als ebenfalls problematisch ist die Ausschlussklausel für von Mitarbeitern des eigenen Unternehmens verursachte Vermögensschäden in einigen der Deckungsbausteine zu betrachten.

Insgesamt deckt somit keines der beiden Produkte den vollständigen Versicherungsbedarf eines von seiner IT- und Netzwerkinfrastruktur stark abhängigen Unternehmens ab. Sie bieten jedoch eine in vielen Punkten wirksame Ergänzung zu klassischen Haftpflichtdeckungen und sollten nicht als deren Ersatz betrachtet werden.

6 Zusammenfassung und Fazit

In einem abschließenden Fazit soll versucht werden, die in der Arbeit aufgestellten Prämissen hinsichtlich der sicherheitsrelevanten Probleme in der Konstellation von Netzwerken wie dem Internet sowie den Netzstrukturen innerhalb von Unternehmen entsprechend zusammenzufassen²⁰⁸.

Die Angreifbarkeit von Computersystemen und Netzwerken ist heutzutage unbestritten vorhanden, negativ beeinflusst wird sie durch eine schnelle Entwicklung der Informationstechnologien, aber auch durch weltweit vorherrschende Monokulturen im Hard- und Softwarebereich. Das Problem hierfür liegt nicht etwa in einem Mangel an zur Verfügung stehenden Technologien, sondern vielmehr in bestimmten dominierenden, marktpsychologischen und gesellschaftlichen Zusammenhängen. Der weltweite IT-Markt ist ein Angebotsmarkt, in welchem Unternehmen ihre eigenen Vorstellungen von Systemlandschaften nicht oder nur sehr kostenintensiv verwirklichen können. Somit werden oft standardisierte Produkte und Systeme eingesetzt, obwohl diese nicht den gewünschten Sicherheitsvorstellungen entsprechen. Die Hersteller selbst vermitteln ihren Kunden ein Bild absolut sicherer Produkte, wobei den Kunden wiederum häufig ein fundiertes Risikoverständnis fehlt.

Juristisch gesehen wurde in Deutschland mit der Einführung des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) ein erster wichtiger Schritt zur Sensibilisierung der Verantwortlichen für Sicherheitsfragen im Unternehmen getan. Somit kann dieses auch als Grundsteinlegung für das Bewusstmachen der Notwendigkeit eines funktionierenden Risk-Managements gesehen werden.

Zur Risikoabsicherung existiert eine Vielzahl technischer und administrativer Mittel, die in Kapitel 4 vorgestellt wurden. Doch nicht nur Firewall-Systeme, Verschlüsselungsmechanismen oder sinnvoll aufgestellte Zugriffsrichtlinien für Systeme können zum Schutz geschäftskritischer Systeme beitragen, auch der Aufbau redundanter Ressourcen und die weitgehende Vermeidung der Abhängigkeit von Technologien aus Herstellermonopolen hat daran einen nicht zu unterschätzenden Anteil. Weitere wichtige Maßnahmen stellen die unbedingte Bekanntmachung entdeckter Sicherheitsmängel in Systemen und Organisationen sowie der Einsatz ausgereifter Technologien dar.

Hinsichtlich der Koordination und Bündelung verschiedener nationaler Rechte und Normen besteht weltweit ein dringender Regelungs- und Standardisierungsbedarf. Momentan steht dem globalen Charakter des Internets eine national geprägte Sicherheitspolitik in den einzel-

²⁰⁸ Vgl. dazu auch [VW 12/2001], S. 957 ff.

nen Ländern der Welt gegenüber. Hier sind die Politiker aller Industrienationen gefordert, eine einheitliche Rechtsnorm für alle internetbezogenen Geschäftsvorfälle zu schaffen.

Und doch wird, trotz der Beachtung aller theoretisch möglichen Sicherungsmaßnahmen, im Zusammenhang mit Internetrisiken immer ein gewisses, mit technischen und administrativen Mitteln nicht abzudeckendes Restrisiko bleiben, welches zudem häufig von menschlichen Faktoren zusätzlich potenziert wird. Dessen Versicherbarkeit beschäftigt heutzutage jedes Versicherungsunternehmen. Die dabei unweigerlich auftauchenden Fragen nach den genauen zu versichernden Gefahren, nach Eintrittswahrscheinlichkeiten, Schadenhöhen sowie der generellen Quantifizierbarkeit von Risiken und Ereignissen können mit heutigen Mitteln nicht eindeutig beantwortet werden. Sowohl Entscheidungen hinsichtlich der Versicherbarkeit als auch Prämienkalkulationen werden (noch) nicht anhand objektiv analysierter Werte vorgenommen, vielmehr bestimmt die subjektive Einstellung des Underwriting die Haltung der Versicherungsunternehmen. Trotz allem – in Forschungsprojekten und Werkstätten zum Thema wird allmählich die wissenschaftliche Fundierung für den Risikotransfer internetbezogener Gefahren erarbeitet.

Nicht vergessen darf man bei der Frage nach der Versicherbarkeit des erwähnten Restrisikos jedoch, dass die Hauptverantwortung beim Umgang mit dem Internet nach wie vor bei jedem einzelnen Nutzer selbst liegt. Nur ein ausgeprägtes, täglich gelebtes Risikobewusstsein und Sicherheitsverständnis schafft hier einen langfristigen Schutz.

Anhang A – Literaturverzeichnis

[Allaire 2001]

Incident Response, in:

http://www.macromedia.com/v1/documentcenter/partners/asz_aswps_incident_response.pdf,

Abruf: 18.07.2002

[Allianz 3/2001]

Stefan Feldhütter, Daten sind versicherbar: Neue Lösungen für Konzernkunden, Allianz-Report, Heft 3/2001, S. 96-103

[anonymous 2001]

anonymous, der neue hacker's guide, Verlag Markt+Technik, München 2001

[Aventis 2001]

Neuronale Netze, in:

http://www.corp.aventis.com/future/de/fut0102/neural_networks/neural_networks_1.htm,

Abruf: 12.06.2002

[Berkeley 2002]

Berkeley UNIX, in: http://www.coe.berkeley.edu/labnotes/history_unix.html, Abruf: 19.06.2002

[BMI 2001 Kriminalstatistik]

Polizeiliche Kriminalstatistik 2001, in:

http://www.bmi.bund.de/Annex/de_20088/Polizeiliche_Kriminalstatistik_als_PDF-Download.pdf, Abruf: 08.06.2002

[BMI 2002 Hochtechnologie-Kriminalität]

Hochtechnologie-Kriminalität, in:

<http://www.bmi.bund.de/services/lexikon/lexikon.jsp?key=H&hit=Hochtechnologie-Kriminalit%e4t>, Abruf: 08.07.2002

[BSI 2002 GSHB 3023]

IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik, Kapitel 3.23, Einführung in kryptographische Grundbegriffe, in:

<http://www.bsi.de/gshb/deutsch/m/m3023.htm>, Abruf: 15.07.2002

[BSI 2002 GSHB 3005]

IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik, Kapitel 3.5, Schulung zu IT-Sicherheitsmaßnahmen, in:

<http://www.bsi.de/gshb/deutsch/m/m3005.htm>, Abruf: 17.07.2002

[Davidowicz 1999]

Diane Davidowicz, Domain Name System (DNS) Security, in:

<http://compsec101.antibozo.net/papers/dnssec/dnssec.html>, Abruf: 09.07.2002

[EY 2002]

Ernst & Young, Global Information Security Survey 2002, in:

[http://www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_2002/\\$file/FF0210.pdf](http://www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_2002/$file/FF0210.pdf), Abruf: 20.07.2002

[Farny 2000]

Dieter Farny, Versicherungsbetriebslehre, 3. Auflage, Verlag Versicherungswissenschaft, Karlsruhe 2000

[Fuhs 1993]

Computervirenprogrammierer, in: http://www.fuhs.de/buch/2_4.htm, Abruf: 03.07.2002

[Geodsoft 2002]

Myth of total secure, in: <http://geodsoft.com/book/security/fully.htm>, Abruf: 03.07.2002

[HB 10.08.2001]

Julia Latka, Riecher für Risiko, Handelsblatt, Ausgabe vom 10.08.2001

[Hein 1995]

Matthias Hein, Ethernet, International Thomson Publishing, Bonn 1995

[Heinegg 1997]

Computerkriminalität, in: <http://www.rz.uni-augsburg.de/connect/9701/compstrf.html>, Abruf: 05.07.2002

[Heise 2002]

Computerkriminalität in Deutschland erneut kräftig gestiegen, in:

<http://www.heise.de/newsticker/data/wst-02.05.02-004/>, Abruf: 05.07.2002

[Hunt 1995]

Craig Hunt, Networking Personal Computers with TCP/IP, O'Reilly & Associates, Sebastopol 1995

[IETF 1981]

Internet Protocol, in: <http://www.ietf.org/rfc/rfc791.txt>, Abruf: 23.06.2002

[IETF 1996]

Address Allocation for private Internets, in: <http://www.ietf.org/rfc/rfc1918.txt>, Abruf: 27.06.2002

[Informationweek 2002]

Betriebssysteme, in: <http://www.informationweek.de/index.php3?channels/channel17/000210na.htm>, Abruf: 28.06.2002

[Marsh 2000]

Cyberrisk Evaluation, in: <http://www.marsh.com/MarshPortal/resources?id=c9f5f742c9914754a52db324bb61d800>, Abruf: 24.07.2002

[NZZ 11.04.2000]

Pascal Schweingruber, Die Versicherung von Cyber-Risiken, Neue Zürcher Zeitung, Ausgabe vom 11.04.2000

[Schweizer Versicherung 7/2001]

Andreas Luig, Sicherheit im Internet ist machbar, Schweizer Versicherung, Heft 7/2001, S. 64-65

[SecurityFocus 2001]

Social Engineering Fundamentals, in: <http://online.securityfocus.com/infocus/1527>, Abruf: 08.07.2002

[Stallings 1995]

William Stallings, Network and Internetwork Security, Prentice Hall, New Jersey 1995

[SZ-Newsline 2002]

Finstere Rache, in: http://www.sz-newsline.de/m_viren/virus2.htm, Abruf: 03.07.2002

[Tanenbaum 2000]

Andrew S. Tanenbaum, Computernetzwerke, 3. Auflage, Verlag, Prentice Hall, New Jersey 2000

[Techtarget 2002 Client/Server]

Client/Server, in:

http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci211796,00.html, Abruf: 09.06.2002

[Techtarget 2002 Extranet]

Extranet, in: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212089,00.html, Abruf: 14.06.2002

[Techtarget 2002 Intranet]

Intranet, in:

http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci212377,00.html, Abruf: 12.06.2002

[Techtarget 2002 LAN]

Local Area Network, in:

http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212495,00.html, Abruf: 14.06.2002

[Techtarget 2002 Malware]

Malicious Software, in:

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci762187,00.html, Abruf: 04.07.2002

[Techtarget 2002 MAN]

Metropolitan Area Network, in:

http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214083,00.html, Abruf: 14.06.2002

[Techtarget 2002 Network]

Network, in: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212644,00.html, Abruf: 13.06.2002

[Techtarget 2002 Router]

Router, in: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212924,00.html, Abruf: 15.06.2002

[Techtarget 2002 VPN]

Virtual Private Network,

in: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213324,00.html, Abruf:
18.06.2002

[Techtarget 2002 WAN]

Wide Area Network,

in: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213336,00.html, Abruf:
14.06.2002

[Techtarget 2002 WWW]

World Wide Web,

in: http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci213391,00.htm, Abruf:
22.06.2002

[VentureNet 2002]

Netzwerke, in: <http://www.venturenet-online.de/netzwerkmain.htm>, Abruf: 12.06.2002

[VB 6/2001]

Monika Linden, 6. Kölner Versicherungssymposium am Fachbereich Versicherungswesen der Fachhochschule Köln, Versicherungs-Betriebswirt, Heft 6/2001, S. 26-27

[VW 23/2000]

Torsten Lesch / Andreas Richter, Prävention und Versicherung für Gefahren aus dem Internet (II), Versicherungswirtschaft, Heft 23/2000, S. 1856-1858

[VW 12/2001]

Monika Gruber, Kumulgefahr bei IT- und Internet-Risiken – wie sicher ist sicher?, Versicherungswirtschaft, Heft 12/2001, S. 956-958

[ZfV Nr.13/1998]

Jörg Knospe, Gefahrenherd Internet, Zeitschrift für Versicherungswesen, Nr.13/1998, S. 372-373

[ZfV Nr.10/2000]

Andreas Benz / Franz Görge, Computerkriminalität – Ist die Versicherungswirtschaft auf das Risiko vorbereitet?, Zeitschrift für Versicherungswesen, Nr.10/2000, S. 319-322

[ZfV Nr.17/2000]

Frank Romeike, IT-Risiken und Grenzen traditioneller Risikofinanzierungsprodukte, Zeitschrift für Versicherungswesen, Heft Nr.17/2000, S. 603-610

Anhang B – Verzeichnis der Abbildungen und Tabellen

Abbildung 2.1 - Client-/Server-Modell	4
Abbildung 2.2 - das ursprüngliche ARPANET Design	6
Abbildung 2.3 - Schema der Implementierung eines Extranets.....	14
Abbildung 2.4 – VPN-Nutzung zur Datenübertragung zwischen Laptop und Intranet	15
Abbildung 2.5 – Netzarchitektur: Schichten, Protokolle und Schnittstellen.....	16
Abbildung 3.1 - Normaler Informationsfluss	30
Abbildung 3.2 - Kategorisierung sicherheitsrelevanter Angriffe auf Computersysteme.....	32
Abbildung 3.3 - Beispiel für einen Portscan mit dem Programm "nmap"	34
Abbildung 3.4 - Menschliche Vektoren: Risikostufen.....	70
Abbildung 4.1 - vereinfachtes Modell der symmetrischen Verschlüsselung.....	77
Abbildung 4.2 - vereinfachtes Modell des Public-Key-Verschlüsselungsverfahrens.....	78
Tabelle 2.1 - Merkmale zur Charakterisierung von Netzwerken	7
Tabelle 3.1 - Statistik zu Fällen der Computerkriminalität in Deutschland für 2001	29

Anhang C – Glossar zu Internetrisiken

ActiveX: Technik, Anwendungen automatisch um bestimmte Fähigkeiten zu erweitern und ein Interagieren zwischen Anwendungen zu ermöglichen, entwickelt von Microsoft. Im Ansatz eigentlich als Grundlage für ein Komponentenmodell gedacht, hat ActiveX mittlerweile als Möglichkeit zur Darstellung *aktiver Inhalte* in *Internet-Browsern* Bedeutung erlangt. Aufgrund der damit verbundenen massiven Sicherheitsrisiken ist generell vom Ausführen von ActiveX Controls aus unbestimmter Quelle abzuraten.

Administrator: auch als Superuser bezeichneter *Benutzer-Account* auf einem *Computersystem*. Person, die für die Verwaltung eines dieses Systems verantwortlich ist, i.d.R. betraut mit entsprechenden Pflichten (Wartungsarbeiten) und Rechten (Vergabe von *Autorisierungen*). Der Administrator besitzt i.d.R. jedwede Berechtigung im System, z.B. darf er auf dem *Server* abgelegte persönliche Daten von *Benutzern* lesen, modifizieren und löschen. Unter *UNIX* ist die Bezeichnung des entsprechenden *Benutzer-Accounts root*.

Aktive Inhalte: Vielzahl von Programmen, Skripten und Multimediateilen, die nicht auf dem angesprochenen Web-Server im Internet, sondern auf dem lokalen Rechner ausgeführt werden. Dazu gehören z.B. *ActiveX* Controls, Flash-Animationen, *Java-Applets*, *JavaScript*- oder *VisualBasic*-Skriptdateien. Diese sorgen i.d.R. für eine „buntere“ Darstellung der Webseiten, bringen aber immer auch ein erhöhtes Sicherheitsrisiko mit sich.

Antiviren-Software: Programm, das gezielt nach *Viren*, *Würmern*, *trojanischen Pferden* und sonstiger *Malware* sucht und diese unschädlich machen kann. Damit die Schutzwirkung erhalten bleibt, muss in regelmäßigen Abständen die darin enthaltene Signaturdatenbank, welche zur Identifizierung der o.a. Schädlinge dient, aktualisiert werden.

Attachment: eine beliebige an eine *e-Mail* angehängte Datei. Hierbei kann es sich sowohl um vergleichsweise ungefährliche Anhänge handeln (z.B. Urlaubsfoto), als auch um ein potenziell sehr gefährliches Sicherheitsrisiko (z.B. *VisualBasic*-Skript, Bildschirmschoner, ausführbare Datei). Generell sollten nur vom Empfänger erwartete e-Mail-Anhänge, nach gründlicher Einschätzung des wahrscheinlichen Inhalts und Abklärung der Identität des Absenders, geöffnet werden. Im Zweifelsfall sollte das Öffnen in einer abgesicherten Umgebung, am besten einer *Sandbox* erfolgen (siehe auch: *Viren*, *Würmer*).

Authentifizierung: bezeichnet meist die Kombination von Login und Passwort, die einen Benutzer gegenüber einem Service oder *Server* identifizieren soll. Hierbei wird jedoch nicht geprüft, ob die mit den eingegebenen Daten verbundene Person die Authentifizierung tatsächlich selbst vorgenommen hat (siehe auch *Social Engineering*). Ein Problem besteht darin, dass die Daten zur Authentifizierung bei vielen *Servern* unverschlüsselt über das Internet transportiert werden, d.h. ein physikalisch in das Transportmedium geschalteter *Netzwerk-Sniffer* kann hier die Daten im Klartext abfangen und somit Zugriff auf den *Server* erlangen.

Autorisierung: dem Prozess der *Authentifizierung* nachgeordnete Rechtevergabe für Ressourcen in *Computersystemen* und *Netzwerken*. Dabei werden bei der *Authentifizierung* angegebenen Daten, i.d.R. der *Benutzername*, als Identifizierungsgrundlage verwendet

Backdoor: *Server*, der versteckt auf einem Computer läuft und einem Angreifer mehr oder weniger vollständigen Zugriff auf das betreffende System und damit eine Fernsteuerung ermöglicht, meist „eingeschleppt“ durch *trojanische Pferde*. Ohne Wissen des Computernutzers können so Daten gelöscht, verändert oder über das *Internet* übertragen werden (bekanntes Beispiel: „Back Orifice“).

Benutzer: Bezeichnung für Personen, die auf einem *Computersystem* einen *Benutzer-Account* besitzen, der sie zur Nutzung bestimmter *Ressourcen* dieses Systems berechtigt.

Benutzer-Account: meist künstliche, vom System- oder Netzwerk*administrator* vergebene elektronische Identifikation für einen Benutzer. I.d.R. eindeutige Kombination aus einem Benutzernamen, welcher zum *Einloggen* (Anmelden) auf einem System oder im *Netzwerk* dient, verbunden mit einem dazugehörigen *Passwort*.

Bouncer: Programme, die i.d.R. vom Besitzer unbemerkt auf einem Computer mit ständigem Internetanschluss installiert werden. Sie ermöglichen es einem entfernten Benutzer, eine Verbindung mit anderen Rechnern oder auch anderen *Netzwerken*, z.B. dem Internet Relay Chat (IRC), aufzubauen. Der Vorteil für die Benutzer besteht darin, dass nicht deren eigene *IP-Adresse*, sondern die des kompromittierten Bouncers übermittelt und somit eine Anonymisierung eines potenziellen Angreifers möglich wird.

Buffer-Overflow: Stapelüberlauf; ein darauf abzielender Angriff führt zu einem schwerwiegenden Programmfehler, der es letztendlich ermöglicht, beliebigen Programmcode auf dem attackierten Rechner auszuführen, siehe auch *Exploit*.

Client: Programm oder *Computersystem*, das Daten von einem *Server* empfängt. Ein Rechner wird zum Client, wenn eine entsprechende Software darauf ausgeführt wird. Darunter fallen auch alle Programme, die eine Verbindung mit dem Internet ermöglichen, wie z.B. *Internet-Browser*. Umgangssprachlich wird Client auch als Bezeichnung für Rechner, die keine *Dienste* im *Netzwerk* anbieten, gebraucht.

Computersystem: jeder Rechner wird als Computersystem bezeichnet, unabhängig von seiner Funktion als *Client* oder *Server*. Ein weiteres System für den Begriff ist *Host*.

Content-Filter: Software, die nach bestimmten Regelwerken Inhalte zulässt oder verbietet, beispielsweise zur Filterung von *Hoaxes* und *Viren* auf einem *e-Mail-Server* eingesetzt. Als *Proxy* für das Internet kann sie beispielsweise alle *aktiven Inhalte* einer Webseite ausfiltern.

Cracker: einerseits Personen, die Software „knacken“ (Kopierschutz entfernen), in Bezug auf die Sicherheitsthematik aber auch Leute, die sich Zugriff auf fremde Rechner verschaffen, um diese auszuspionieren und ernsthaften Schaden anzurichten. Im Gegensatz zu *Hackern* zeichnen sie sich durch kriminelle Energie aus und ver-

schaffen sich i.d.R. persönliche Vorteile durch einen Angriff. Eine moderne, gefährliche Abwandlung sind die sogenannten *Skriptkiddies*, welche sich mittels vorgefertigten und leicht zu bedienenden Werkzeugen Zugriff auf fremde Computersysteme verschaffen.

Datagramm: siehe *Paket*

Denial of Service (DoS): Attacke mit dem Ziel, die Verbindung eines Rechners an das Internet zu kappen, also seine Funktion im Internet einzustellen. Es gibt zahlreiche Varianten, die zu einem DoS führen können: einfaches *Flooding*, aber auch trickreiche Methoden, die den attackierten Rechner dazu bringen, sich durch exzessive Kommunikation selbst lahm zu legen.

Eine Sonderform des DoS ist der **Distributed DoS (DDoS)**: hier handelt es sich um einen DoS-Angriff, an dem sich mehrere Rechner zugleich beteiligen. Häufig handelt es sich dabei um Rechner, die z.B. durch eine *Backdoor* unter der Kontrolle eines einzelnen *Crackers* operieren. Je nach Intensität – also Bandbreite – können solche DDoS-Angriffe ganze Netzwerksegmente bzw. *Router* lahmlegen.

Dienst: bezeichnet eine bestimmte Funktion, die von einem *Server* im *Netzwerk* angeboten wird. Dazu zählen u.a. das Empfangen und Bereitstellen von *e-Mails* sowie die Bereitstellung von zentralem Speicherplatz oder einem *Login-Mechanismus*.

Distributed Denial of Service (DDoS): siehe *Denial of Service (DoS)*

Domain Name System (DNS): Protokoll zur Auflösung von *Hostnamen* zu *IP-Adressen* und umgekehrt aufgrund von Datenbanken spezialisierter DNS-Server. Das DNS besitzt eine große, hierarchisch aufgebaute Struktur und häufig sind dessen zentrale Rechner Ziele von Angriffen wie z.B. *Spoofing*.

e-Mail: elektronische Post, häufige Gefahrenquelle zum Einschleusen von *trojanischen Pferden*, *Hoaxes*, *Viren* und *Würmern* in ansonsten geschützte lokale *Netzwerke* und private Computer. Das Risiko geht dabei von den mit der e-Mail gesendeten *Attachments* aus.

Exploit: Programm, das eine bestehende, bekannte Sicherheitslücke in einem Computersystem ausnutzt, um dem Angreifer unerlaubte Zugang zum System zu verschaffen. Zumeist wird dabei die Anfälligkeit eines *Dienstes* (oder eines anderen installierten Programms) für einen *Buffer-Overflow* ausgenutzt.

Eine spezielle Form des Exploits stellt der sogenannte **Root-Exploit** dar, bei dem der Angreifer einen uneingeschränkten Systemzugriff erlangen kann, abgeleitet von der Bezeichnung „*root*“ für den Administrator unter *UNIX*-basierten Betriebssystemen.

File Transfer Protocol (FTP): Protokoll zur Übermittlung von Daten über das Internet, aufbauend auf *TCP/IP*. Die Übermittlung der zur *Authentifizierung* notwendigen Benutzerdaten erfolgt dabei unverschlüsselt, was sie anfällig für *Netzwerk-Sniffer* macht. Außerdem gibt es einen seit langer Zeit bekannten und trotzdem noch vielerorts anzutreffenden *Root-Exploit* für FTP-Server.

Firewall: Eine Firewall ist ein speziell eingerichtetes *Gateway-System*, welches ausschließlich dem Zweck dient, den ein- und ausgehenden Datenverkehr zu anderen *Netzwerken* zu überwachen und unerwünschte *Pakete* auszufiltern. Zumeist findet sich eine Firewall an der Schnittstelle zweier *Netzwerke*. Jedes *Paket* zwischen den beiden *Netzwerken* muss dabei die Firewall passieren. Firewalls kommen meist in den Ausführungen von *Paketfiltern* oder auch *Stateful Packet Filters (SPF)* vor. Häufig übernimmt eine Firewall auch die Funktionen von *Network Address Translation (NAT)* und *Masquerading*.

Flooding: Oberbegriff für Angriffsformen, bei denen große Mengen von Daten an ein *Computersystem* geschickt werden, mit dem Zweck, dieses bei der Verarbeitung zu überlasten. Zumeist wird dadurch die Verbindung des *Computersystems* zum *Netzwerk*, z.B. dem *Internet* unterbrochen. Flooding kommt in verschiedenen Arten vor: zu den harmlosen Varianten gehört Text-Flooding (z.B. in einem Chat, hierbei werden große Mengen an Textzeilen schnell hintereinander an den *Client* des Zielrechners geschickt).

Eine gefährlichere Variante stellt dagegen das **SYN-Flooding** dar, bei dem massenhaft *ICMP-Pakete* an die *IP-Adresse* des Zielsystems geschickt werden, so dass dieses die vielen Verbindungsanfragen nicht mehr bearbeiten kann und den Dienst einstellt. Eine weitere Variante ist das Versenden von korrupten, d.h. absichtlich beschädigten *IP-Paketen*, die einen *Buffer-Overflow* in der Implementierung des *IP-Protokolls* beim angegriffenen System zum Ziel hat.

FTP: siehe *File Transfer Protocol (FTP)*

Fully Qualified Domain Name: siehe *Hostname*

Gateway: *Computersystem* oder *Router*, welches zwei oder mehr verschiedene *Netzwerke* miteinander verbindet, zumeist gekoppelt mit einer *Firewall*-Implementierung.

Hacker: Computerspezialisten, die in (eigenen und fremden) *Computersystemen* nach Sicherheitslücken suchen, diese aber nicht nutzen, um sich selbst einen Vorteil zu verschaffen, sondern nach deren Aufdeckung und Behebung, nicht zu verwechseln mit *Crackern*.

Hoax: Bezeichnung für über *Netzwerke* verbreitete Scherze, z.B. in Form von *e-Mails*. Beispiele stellen falsche Warnungen vor *Viren* dar. Hoaxes sind immer verbunden mit dem Hinweis, diese so schnell wie möglich an möglichst viele Personen weiterzuleiten. Sie sind daher mit Kettenbriefen vergleichbar und verbreiten sich nicht selbsttätig. Ihr Ziel ist zumeist die unspezifische Erzeugung von *Netzwerkverkehr*.

Host: siehe *Computersystem*

Hostname: Bezeichnung für ein *Computersystem*, die vor allem in Form eines **Fully Qualified Domain Name (FQDN)**, d.h. der vollständigen Bezeichnung eines Rechners bedeutsam ist, z.B. www.microsoft.com.

HyperText Transfer Protocol (HTTP): hinlänglich bekanntes Protokoll, das aufbauend auf *TCP/IP* im *Internet* zum Übertragen von Webseiten (i.d.R. HTML-Dokumenten) dient. Dieses höherschichtige Protokoll stellt mit Abstand die meistgenutzte Anwendung des *Internets* dar.

Die sichere Variante von HTTP heißt **HyperText Transfer Protocol Secure (HTTPS)** und *verschlüsselt* Daten vor der Übertragung.

HyperText Transfer Protocol Secure (HTTPS): siehe *HyperText Transfer Protocol (HTTP)*

HTTP: siehe *HyperText Transfer Protocol (HTTP)*

ICMP: siehe *Internet Control Message Protocol*

Internet: weltweit operierendes, lediglich virtuell vorhandenes *Netzwerk*, welches physisch gesehen auf der Zusammenwirkung einzelner Telekommunikationsnetze aufbaut.

Internet-Browser: *Client*-Software zur Anzeige von Webseiten auf dem Rechner des *Benutzers* (z.B. „Internet Explorer“ von Microsoft, „Navigator“ von Netscape)

Internet Control Message Protocol (ICMP): Protokoll zum Versenden von Metadaten (Fehler- und Testpaketen) über das *Internet*, wird häufig zum *Flooding* missbraucht (siehe auch *Ping*).

IP-Adresse: numerische Adresse zur eindeutigen Identifizierung von Rechnern im *Internet*, in der z.Zt. aktuellen Version IPv4 wird diese in vier Oktetten (Zahlen von 0-255) dargestellt, z.B. 192.170.0.0. Sie besteht jeweils aus zwei Teilen: der *Netzwerkadresse* (Adresse des zugehörigen *Netzwerks*) und der *Hostadresse* (Adresse des spezifischen Rechners). Hierbei gibt es verschiedene festgelegte Netzklassen, welche sich nach der Größe des zu verwaltenden Netzwerks richten. Ebenfalls gibt es spezielle, für lokale Zwecke einzusetzende IP-Adressen, die keine Gültigkeit im *Internet* besitzen. Da diese Rechner vom *Internet* aus nicht direkt erreichbar sind, besteht hier ein grundlegender Angriffsschutz.

IP-Protokoll: siehe *TCP/IP-Protokoll*

IP-Spoofing: siehe *Spoofing*

Java: Programmiersprache von SUN Microsystems, die besonders im Hinblick auf Netzwerkunterstützung entwickelt wurde. Herausstechendes Merkmal ist die Plattform-Unabhängigkeit. Sie hat vor allem bei der Entwicklung von *Internetanwendungen* und sogenannten *Applets* für den *Internet-Browser* Bedeutung erlangt, wobei Java-Applets auch Risikofaktoren auf Webseiten darstellen, da sie lokal auf dem *Client* ausgeführt werden und möglicherweise unbefugten Zugriff auf dessen Daten gewähren können (siehe auch *aktive Inhalte*).

JavaScript: Von der Firma Netscape entwickelte, nicht mit *Java* verwandte Skriptsprache zur *Internet-Browser*-Erweiterung (siehe auch *aktive Inhalte*).

Joke: Spaßprogramm, welches Anwender von der Arbeit ablenken oder verunsichern soll, indem es virentypische Aktionen vortäuscht. Daher werden solche Programme auch häufig von *Antiviren-Programmen* fälschlich als gefährlicher *Virus* entdeckt.

Login: Begriff für die Anmeldung auf einem *Computersystem* oder im *Netzwerk*, allgemein mit einem *Benutzer-Account*.

Makrovirus: Sonderform von *Viren*, die Makrosprachen von Anwendungen zur Ausführung und Verbreitung nutzt. Heutzutage in der Sprache VBA (VisualBasic for Applications) für Microsoft Office am meisten verbreitet. Einzige Abhilfe besteht im Verneinen der Abfrage nach Ausführung der in einer Datei enthaltenen Makros, außer wenn man sich über deren Funktion und Autor vollständig im Klaren ist.

Malicious Ware (Malware): Oberbegriff für schädliche Software, d.h. *Viren*, *Würmer* und *trojanische Pferde*.

Masquerading: siehe *Network Adress Translation(NAT)*

Network Address Translation (NAT) oder auch **Masquerading:** Umsetzung einer, zumeist reservierten *IP-Adresse* eines Rechner im lokalen Netzwerk auf eine öffentliche, d.h. weltweit gültige) *IP-Adresse*, so dass zugehörige *IP-Pakete* im *Internet* transportiert werden können. Zumeist integrierte Funktionalitäten in *Firewalls*.

Netzwerk: eine bestimmte Menge von autonomen, miteinander verbundenen Computern, wobei zwei Computer als miteinander verbunden gelten, wenn sie in der Lage sind, untereinander Informationen auszutauschen

Netzwerk-Sniffer: ein an einem physikalischen Leitungsweg installiertes Programm, welches dazu gedacht ist, allen an dieser Stelle vorbeikommenden Netzverkehr mitzuhören und zu protokollieren. Obwohl es sich dabei um Rohdaten handelt, lassen sich auf diese Weise z.B. *Passwörter* erschleichen.

Paket: eine bestimmte, genau definierte Menge von Daten, die über ein *Netzwerk* transportiert werden können.

Paketfilter: Software, die *Pakete* nach einem vorgegebenen Regelwerk, meist ausgehend von *IP-Adresse* und *Port* des Absenders und Empfängers, filtert. Vor allem eingesetzt in *Firewalls*. Eine Sonderform stellen **Stateful Packet Filters (SPF)** dar, diese führen zusätzlich zu normalen Paketfiltern eine Zustandstabelle über den Status der aktiven TCP-Verbindungen, somit ist eine erweiterte Filterung des Datenverkehrs möglich.

Passwort: geheime Zeichenfolge, die zur Sicherung eines *Benutzer-Accounts* benutzt wird, sie sollte möglichst lang (minimal acht Zeichen) und ebenso schwer zu durch einen Dritten zu erraten sein

Ping: Umgangssprachliche Bezeichnung für einen *ICMP Echo Request*, häufig dazu eingesetzt, um die Erreichbarkeit eines Rechners im Internet zu überprüfen. Solchen *Hostscans* folgt meist ein eingehender *Portscan* der gefundenen *IP-Adressen*, um darauf laufende Dienste und vorhandene Angriffsmöglichkeiten zu prüfen. Eine

besondere Form ist der sogenannte **Ping of Death**, hierbei wird ein überlanges Ping-Paket verschickt, welches zu einem *Denial of Service* des angegriffenen Rechners führen kann.

Ping of Death: siehe *Ping*

Port: *TCP/IP*-Anwendungen kommunizieren mit anderen Rechnern im Internet über eine Kombination aus *IP-Adresse* und Portnummer (Zahl zwischen 1 und 65535). Diese spezifiziert den Dienst auf dem angesprochenen Rechner, da unter einer einzigen *IP-Adresse* auch mehrere Services (z.B. ein *HTTP*-Server und ein *FTP*-Server) erreichbar sein können. Für diesen Mechanismus gibt es sogenannte „well known ports“, dies sind z.B. Port 80 für *HTTP* oder Port 21 für *FTP*. Dabei werden Portnummern zwischen 1 und 1024 als privilegierte Ports bezeichnet, diese sind für *Server* reserviert und können nicht von einem normalen Benutzerprogramm verwendet werden. Portnummern über 1024 werden als unprivilegierte Ports bezeichnet.

Portscan: Bezeichnung für einen systematischen Test, auf welchen *Ports* eines Rechners Dienste aktiv, d.h. erreichbar sind. Am häufigsten eingesetzt von *Crackern* bzw. *Hackern*, um die Verwundbarkeit eines Rechners und andere Zusatzinformationen wie z.B. darauf laufendes Betriebssystem zu prüfen, meist im Zusammenhang mit einem geplanten Angriff.

Proxy: Ein Proxy übernimmt als „Stellvertreter“ für *Clients* die Kommunikation mit einem *Server* in einem anderen *Netzwerk* (z.B. dem *Internet*). Im Unterschied zu einer einfachen *Firewall* ändert er aber die Datenpakete so ab, dass sie unter seiner eigenen *IP-Adresse* verschickt werden und leitet die Antwort dann an den entsprechenden *Client* zurück. Proxies sind generell dienstspezifisch ausgelegt (*HTTP*-Proxy u.a.).

Ressource: von einem *Server* oder in einem *Netzwerk* zur Verfügung gestelltes Produktions- oder Hilfsmittel, z.B. Speicherplatz, Rechenleistung oder Übertragungskapazität

root: siehe *Administrator*

Root-Exploit: siehe *Exploit*

Router: Ein Rechner oder spezielles Gerät zur Vermittlung zwischen zwei Netzen, z.B. den zweier getrennter Firmenteile. Router können über spezielle Datenpakete den besten Weg zur Weiterleitung von Daten selbständig bestimmen. Es existiert jedoch auch hier ein Sicherheitsrisiko dahingehend, dass mittels gefälschter Redirect-(Umleitungs-) Anweisungen bestimmte Datenpakete nicht zum korrekten Empfänger, sondern zu einem Angreifer hingeleitet werden.

Sandbox: Abgesicherte und klar abgegrenzte Umgebung, darin laufende Programme haben keinen Zugriff auf kritische Systemressourcen und wichtige Dateien. Häufig zum Testen suspekter *Attachments* einer e-Mail auf *trojanische Pferde* u.ä. verwendet.

Secure Shell (SSH): ein mit Verschlüsselungsmechanismen arbeitender Ersatz für das Terminalemulationsprogramm *Telnet*.

Server: Ein Programm, welches für einen *Client* Daten bzw. Dienste zur Verfügung stellt. Häufig wird umgangssprachlich ein diesbezüglich agierender Rechner selbst als Server bezeichnet.

Skriptkiddies: auch als „pubertierende männliche Jugendliche“ bezeichnete, aus Eitelkeit handelnde Sonderform der *Cracker*, die unter Ausnutzung fertiger Programme oder Skripte in fremde *Computersysteme* eindringen und dort Schaden anrichten. Der Zweck besteht hierbei in der Erlangung einer gewissen zweifelhaften Berühmtheit in der Untergrundszene.

Social Engineering: Hierbei handelt es sich um einen von Angreifern angewandten psychologischen Trick, bei dem ein Opfer durch die Vorspiegelung einer falschen Identität überredet wird, Informationen (wie z.B. Kreditkartennummern, Passwörter) herauszugeben oder schädliche Kommandos in seinen Rechner einzugeben.

Spam: Bezeichnung für unaufgefordert verschickte Massenwerbung, meist per e-Mail.

Spoofing: Generell steht das Wort „Spoofing“ für das Vorgeben einer falschen Identität. In der Ausprägung des **IP-Spoofing** spiegelt der Angreifer dem anzugreifenden Computer eine falsche (wahrscheinlich vertrauenswürdige) *IP-Adresse* vor. Eine Möglichkeit ist das „Erraten“ der Initial Sequence Numbers, die bei der Kommunikation zwischen zwei Rechnern zum Identifizieren des TCP-Verbindung zum Einsatz kommen, im Regelfalle in Kombination mit einem *Denial-of-Service*-Angriff auf den Rechner, dessen Identität man übernehmen möchte. Eine weitere Möglichkeit ist das **DNS-Spoofing**, bei der man die Funktion eines *DNS*-Servers übernimmt und falsche Angaben über die bekannten Hostnamen (z.B. *www.microsoft.com*) zugehörigen *IP-Adressen* publiziert.

Stateful Packet Filter: siehe *Paketfilter*

Superuser: siehe *Administrator*

SYN-Flooding: siehe *Flooding*

TCP/IP: siehe *Transmission Control Protocol / Internet Protocol (TCP/IP)*

Telnet: Protokoll für das entfernte Arbeiten an Rechner mit einem Netzwerkanschluß, aufbauend auf dem *TCP/IP* Protokoll. Hierbei *loggt* sich der Benutzer auf dem entsprechenden System ein und kann danach so damit arbeiten, als sitze er an der Tastatur des Rechners selbst. Der Telnet-Server stellt ein bekanntes Sicherheitsrisiko dar, da die zur Autorisierung des Benutzers erforderlichen Daten im Klartext über das Internet übertragen werden und mit einem *Netzwerk-Sniffer* ausgespäht werden können.

Transmission Control Protocol / Internet Protocol (TCP/IP): grundlegende Standard-Protokoll-Suite im Internet, eigentlich handelt es sich hierbei um zwei Protokolle, wobei TCP auf IP aufbaut. IP ist dabei für die

Adressierung und Weiterleitung der Pakete zuständig, während TCP beim Empfänger für die richtige Sortierung der Pakete und für die Absicherung der Kommunikation durch Bestätigung des Paketerhalts sorgt.

Trojanisches Pferd (Trojaner): Bezeichnung für ein unscheinbares Programm, das insgeheim Spionage- oder Schadensausübungsfunktionen enthält. Im Gegensatz zu *Würmern* oder *Viren* verbreiten sich Trojaner nicht selbständig weiter, sondern sind dahingehend auf die (zumeist ahnungslosen) Benutzer angewiesen. Bei der Ausführung installieren sich diese Programme heimlich auf dem System und richtet daran teilweise Schäden an. Meist in Kombination mit *Backdoor*-Funktionalität anzutreffen (z.B. „AOL4Free“).

UDP: siehe *User Datagram Protocol (UDP)*

UNIX: in den 60er Jahren entwickeltes *Netzwerk*betriebssystem, welches für *Server* sehr populär geworden ist. Es bietet von Haus aus sehr viele Funktionalitäten und ist teilweise kostenlos erhältlich (Linux). UNIX ist eine dabei ein Sammelbegriff für eine Familie von Betriebssystemen, die einzelnen Produkte werden als Distributionen bezeichnet.

User Datagram Protocol (UDP): auf IP aufbauendes Protokoll, das aber im Gegensatz zu *TCP* ohne eine direkte Verbindungsaufnahme zwischen Sender und Empfänger funktioniert (verbindungsloses Protokoll) und ebenfalls nicht die korrekte Übertragung der Datenpakete gewährleistet. Es ist jedoch durch die kleinere Paketgröße (geringerer Protokoll-Overhead) besser für kleine Datenmengen (z.B. Abfrage von *DNS*-Servern) geeignet als *TCP*.

Virus: Programm, welches sich selbständig, also ohne Hilfe von außen, vermehrt, indem es andere Programme, Skripte oder Makros infiziert. Anders als ein *Wurm* benötigt es einen Wirt, der dann vom Virus infiziert wird. Klassifizieren lassen sich Viren z.B. nach ihrem Lebensbereich in Datei-, *Makro*-, Skript- und Bootsektorviren oder nach ihren typischen Eigenschaften wie z.B. Massenmailer.

VisualBasic Script (VBS): von Microsoft aus VisualBasic (analog zu VBA, siehe *Makrovirus*) entwickelte Skriptsprache zur Verwendung vor allem in dynamischen Webseiten. VBScript Dateien können eine gewaltiges Sicherheitsloch darstellen, da die entsprechende Datei bei einem Doppelklick sofort ausgeführt wird (Standardaktion). Hier empfiehlt es sich, die verknüpfte Standardaktion das Öffnen mit einem Texteditor zu setzen, um ein unbeabsichtigtes Ausführen des Skriptes zu verhindern.

Wurm: eigenständige Programme, die sich selbständig über Netzwerke vermehren, aber keine anderen Dateien befallen (z.B. „ILoveYou“-Virus, dies ist ein Wurm, anders als es der Name vermuten läßt).

Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Leipzig, den 19.08.2002

.....

(Daniel Paul)