Seminararbeit zum Thema:

„Anonyme Dienste, Copyright-Schutz und Internet-Kriminalität“

Lehrstuhl für Allgemeine und Industrielle Betriebswirtschaftslehre
Prof. Dr. Dr. h.c. Ralf Reichwald

Betreuer: Robert Goecke

Eingereicht von:

Holger Mattheis Astrid Werner

München, den 18. März 2002

Inhaltsverzeichnis

1. Einleitung

E-commerce, E-mail, Internet, World Wide Web.
Vor wenigen Jahren noch nicht existent sind diese Worte heute zu einem Bestandteil des täglichen Lebens geworden. Sie gehören zu einer neuen Realität, die weitläufig als das Internet bezeichnet wird.
Die virtuelle Welt hat unsere reale Welt verändert. Zum ersten Mal in der Geschichte haben wir Zugriff auf alle erdenklichen Informationen, jederzeit erreichbar mit einem Mausklick. Das birgt neue Möglichkeiten bezüglich Bildung, Kommunikation und unternehmerischer Vielfalt.
Aber wie bei nahezu jeder neuen Technologie hat auch das Internet zwei Seiten. Denn die vorhandenen Potentiale bergen nicht nur Chancen, sondern auch die Gefahr des Missbrauchs. Datenschutz, Betrügereien, Pornographie sind nur einige Schlagworte, die auf die neuen Gefahren verweisen und Gegenstand der Diskussion besorgter Bürger sind.
Im Rahmen dieser Arbeit werden einige dieser Themen angesprochen. Wegen der komplexen Sachverhalte kann jedoch nur auf einige wenige Themen detaillierter eingegangen werden.

2. Anonyme Dienste

2.1 Die Privatsphäre

Nicht erst seit den Zeiten des Internet ist der Schutz der Privatsphäre ein häufig diskutiertes Thema. Eine Aufweichung dieses Schutzes kann den Bürger zum sogenannten „gläsernen Menschen“ und damit angreifbar machen. Persönliche Nachteile, Rufschädigung bis hin zur Zerstörung von Existenzen sowie Verbrechen etwa in Form des Diebstahls von Kreditkartennummern sind nur ein Thema. Ein weiteres ist Spionage, bei der Unternehmen durch Verbreitung von Informationen Nachteile im Wettbewerb entstehen können.
Dennoch sind Menschen und Institutionen immer wieder bereit, Informationen über sich weiterzugeben, wenn sie ihnen von Nutzen sein können. Diese Nutzung ist sehr vielfältig, wie es beispielsweise bei der freiwilligen Freigabe von Bankdaten im Rahmen des „Homeshopping“ geschieht. Auch Formen der Gesundheitsvorsorge und Lebensrettung sind denkbar, wenn z.B. ein Arzt sämtliche Daten des Patienten sofort

abrufen oder einen Verletzten jederzeit und überall lokalisieren kann. Eine weitere Möglichkeit ist die Personalisierung von Diensten, z.B. durch den Einsatz von Cookies bei der Internetnutzung, so dass der Nutzer immer nur die für ihn interessanten Informationen angeboten bekommt.
Auch im Rahmen der Verbrechens- und Terrorismusbekämpfung müssen Bürger oft Eingriffe in die Privatsphäre hinnehmen , wie z.B. die Kameraüberwachung an öffentlichen Plätzen oder sogar das Abhören der Privatwohnung.
Auch Firmen geben zur Zusammenarbeit mit anderen Unternehmen interne Daten an diese weiter.
Objektiviert man die hier aufgeführten Beispiele, lassen sich zwei entscheidende Forderungen aufstellen.

1. Der Bürger / die Geschäftsleitung muss selbst entscheiden können, welche Informationen man über sich freigibt. Diese Subjektivität lässt sich am Beispiel der personalisierten Dienste illustrieren, bei denen sich dem Nutzer die Frage stellt, wie viel Privatsphäre er für den Service aufzugeben bereit ist.
2. Die potenzielle Weiterverbreitung von preisgegebenen Informationen muss streng überwacht werden. Deutlich wird dies zum Beispiel an der Zahlungsweise mit Kreditkarten, die einerseits als beliebtes und bequemes Zahlungsmittel eingesetzt werden, andererseits durch die Preisgabe der Kartennummer leicht missbraucht werden können.

Zu beachten ist in allen hier aufgeführten Fällen, dass die Preisgabe von Informationen theoretisch „für immer“ erfolgt, das heißt durch den, der sie preisgibt, aber auch für den der betroffen ist, nicht mehr revidierbar ist.

2.2 Formen der Angriffe auf die Privatsphäre

Im Internet kommunizierte Informationen sind auch für dritte, unautorisierte Personen oder Institutionen oft mit nur geringem technischen Aufwand recherchierbar.
Am bekanntesten hierfür sind wohl e-mails, deren Fähigkeiten, Daten zu verbergen, oft mit denen einer Postkarte verglichen werden. Auch so genannte „trojanische Pferde“, Programme die Daten des Opfers ausspionieren und übermitteln, machen immer wieder von sich reden.
Generell sind Daten, die im Klartext über das Internet transportiert werden, weitgehend ungeschützt und können überall entlang des Übertragungswegs, z.B. von den Betreibern der Zwischenstationen mitgelesen oder sogar verfälscht werden. Besonders prägnant dabei ist, dass der Absender in der Regel noch nicht einmal weiß, welchen Weg seine Nachrichten nehmen.

Sämtliche Arten dieser Angriffe auf die Privatsphäre beziehen sich aber auf Dateninhalte.
Demgegenüber weniger bekannt sind allerdings die Möglichkeiten, die sich aus der Überwachung von Kommunikationsbeziehungen ergeben.
So hinterlässt jeder Nutzer, technisch bedingt, bei seinen Onlinestreifzügen im Internet zahlreiche Datenreste. Jedem Nutzer wird bei der Einwahl in das Internet eine IP-Adresse zugewiesen und die entsprechenden Ports für einen möglichen HTML-Zugriff werden überprüft. Beim Zugriff auf Web-Server werden die Kontakte in ein internes Logfile eingetragen, mit dem dann Statistiken ausgewertet werden können. Und dies ist nur der Beginn des Onlinestreifzuges, bei dem der Nutzer beobachtet werden kann.
Auf diese Art und Weise können einer IP-Adresse zahlreiche Eigenschaften zugewiesen werden, wie z.B. Datum und Uhrzeit, verwendeter Browser und Betriebssystem sowie besuchte Websites.
Auch im e-mail-Verkehr und in Chat-Rooms können unabhängig vom Inhalt der ausgetauschten Informationen Kommunikationsbeziehungen überwacht und Daten bezüglich Zeitpunkt, Dauer der Interaktion, Absender und Empfänger, Lokalisierung sowie Datenvolumen gesammelt werden.
Solche und ähnliche Maßnahmen ermöglichen es Benutzerprofile anzulegen. Von hoher Brisanz werden diese Informationen aber erst, wenn sie einer Person zugeordnet werden. Dies kann, wenn nicht schon durch die Bekanntgabe von Absender und Empfänger bei e-mails geschehen, z.B. auch dadurch gelingen, dass auf Websites gesammelte Informationen in ihrer zeitlichen Korrelation verkettet, ausgewertet und interpretiert werden.

2.3 Interessensgruppen an Informationen aus der Privatsphäre

Die Interessenten für Informationen jeglicher Art sind zahlreich. Und genauso zahlreich sind auch die Informationen, die sie sammeln, welche Institutionen bzw. Personen deren Opfer werden und die Art und Weise, wie Informationen gesammelt werden, d.h. legal oder illegal. Es gibt zum einen kommerzielle Interessenten, zu denen beispielsweise Werbefirmen zählen, die Daten zu Interessen und Gewohnheiten der Kunden, zwar legal, aber zum Teil auch gegen deren Willen, sammeln.
In Fällen von Industriespionage sammeln Unternehmen Informationen z.B. über die Produkte der Konkurrenz, um sich Wettbewerbsvorteile zu sichern.
Ähnlich verhält es sich mit ausländischen Geheimdiensten, die beispielsweise militärische Produkte ausspionieren.

Kriminelle können z.B. versuchen an persönliche Daten zwecks Erpressung oder Betrug zu gelangen.
Aber auch der eigene Arbeitgeber oder Systemadministrator könnte die Angestellten überwachen, sei es aus reiner Neugierde oder um die Arbeitsleistung der Mitarbeiter zu überprüfen.

2.4 Maßnahmen zum Schutz der Privatsphäre

Bevor die wichtigsten Maßnahmen zum Schutz der Privatsphäre aufgezeigt werden, sollen noch einmal die wesentlichen Kategorien von Angriffen auf diese erwähnt werden:

1. Erlangen von Kenntnissen über den Dateninhalt
2. Erlangen von Kenntnissen über die Kommunikationsbeziehungen

Ersterem kann durch die Verwendung von Verschlüsselungstechniken vorgebeugt werden. Deren Sicherheit beruht vom Prinzip her auf mathematischen Funktionen, durch die nur der Nutzer , der den zugehörigen Schlüssel kennt, Daten im Klartext lesen kann. Darüber hinaus bilden Kryptoverfahren die Basis für die digitale Signatur, die es ermöglicht, eine Nachricht dem Absender zuzuordnen, so dass nachträgliche Manipulationen erkennbar werden.
Für den e-mail-Verkehr bietet sich z.B. das Programm „PGP“ (Pretty Good Privacy) (→ http://www.pgpi.org) an, welches das am meist verbreitete Verfahren ist.
Allerdings lässt sich auch mit solchen Verschlüsselungsverfahren keine hundertprozentige Sicherheit erzielen. Nach derzeitigem Erkenntnisstand würde aber selbst modernste Computertechnologie statistisch gesehen viele Jahrhunderte benötigen, um den Code zu knacken[1].
Der zweiten Art von Angriffen kann mit Verschleierungstechniken begegnet werden. Dazu bieten sich sogenannte Anonymisierer im Internet an, deren Aufgabe es ist, Informationen, die einen Personenbezug ermöglichen, abzuschneiden.
Oft geschieht dies durch den Einsatz von Proxy-Servern, die, stellvertretend für den Nutzer, die Anfrage am eigentlich gewählten Server durchführen.
Im Bereich der e-mail-Kommunikation können „Remailer-Systeme“ eingesetzt werden. Es handelt sich dabei um Computer, die mit einer speziellen e-mail-Software arbeiten, um e-mails an den eigentlichen Empfänger weiterzuleiten, wobei allerdings sämtliche Informationen wie der „header“ oder die Adresse, die den Absender identifizieren, entfernt werden.
Weitere Techniken um Kommunikationsbeziehungen zu anonymisieren sind der Einsatz von:

- „Dummy traffic“ (Senden bedeutungsloser Nachrichten, in denen sich die eigentliche Nachricht sozusagen verbirgt)
- Steganographie (die Nachricht wird in einer anderen verborgen)
- Mix-Netze (Kombination von hintereinandergeschalteten Proxies und verschiedenen Techniken wie „dummy traffic“, Verschlüsselung usw.)

Anbieter, welche die dazu erforderliche Software zur Verfügung stellen, lassen sich beispielsweise auf folgenden Internetseiten finden:

• http://www.netreal.de/• http://www.freedom.net/• http://www.onion-router.net/• http://www.anonymizer.com/

2.5 Fazit

Bei jeder Art von Kommunikation werden Informationen ausgetauscht, die unter Umständen verfolgt werden können. Ein absoluter Schutz vor „Mitwissern“ ist von daher vor allem im Internet eine Illusion. Die hier angesprochenen Möglichkeiten der Angriffe auf die Privatsphäre und Anonymität von Internetnutzern, die Motivation der Angreifer sowie deren Abwehr stellen nur einen Abriss des Gesamtproblems dar, zeigen aber doch, dass die Sicherung und Wahrung des Datenschutzes eine eklatant wichtige Bedeutung hat.

Nicht aufgezeigt wurden hier die Nachteile von Anonymisierungsmöglichkeiten. Denn diese bieten nicht nur unbescholtenen Bürgern die Möglichkeit, sich vor kriminellen Übergriffen zu schützen, sondern schützen auch Kriminelle vor staatlichem Zugriff. So stellt sich nämlich die Frage, ob Remailer-Systeme nur von oppositionellen Gruppen in totalitären Systemen verwendet werden, oder auch von Kriminellen in freiheitlichen Demokratien, um sich zu schützen.

3. Copyright-Schutz

3.1 Virtuelle Welt und Copyright-Schutz

Der Copyright-Schutz hat in den letzten Jahren durch die Digitalisierung von Informationen zunehmend an Bedeutung erlangt. Dies liegt an der Eigenschaft von Informationen, nämlich dass sie oftmals in ihrer Form mit einfachen Techniken kostengünstig beliebig oft vervielfältigt und verbreitet werden können. Dieses Problem ist nicht neu und bescherte beispielsweise der Musikindustrie spätestens seit dem Zeitpunkt Umsatzeinbußen, als zum ersten Mal Schallplatten auf Tonbandkassetten

[1] Vgl.: http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/pgp/index.htm (Stand 17.03.02)

kopiert wurden. Solche Probleme waren allerdings meistens auf lokale Märkte beschränkt und konnten so durch nationale Maßnahmen gezielt bekämpft werden.
Seit der Ära des Internet und der digitalisierten Weitergabe von Informationen hat diese Problematik allerdings eine neue Dimension erhalten. Für das Kopieren von Daten ist kein persönlicher Kontakt zwischen Anbieter und Empfänger mehr nötig. Daten werden im großen Rahmen über das Internet über nationale Grenzen hinweg ausgetauscht. Nationale Schutzbestimmungen können im Internet nicht greifen, da sie zu unterschiedlich sind und vor allem nationale Behörden keinerlei Einfluss auf das Verhalten von Internetnutzern in anderen Ländern nehmen können.
Dadurch haben sich große Tauschbörsen im Internet entwickelt, deren Nutzer Musiktitel unentgeltlich über den ganzen Globus austauschen.
Im Jahr 2001 hat dies den Musikkonzernen weltweit Umsatzeinbrüche von 10 bis 20 Prozent gebracht.[2]

3.2 Internettauschbörsen

Die wohl bekannteste Musiktauschbörse im Internet ist Napster. Darüber hinaus gibt es aber zahlreiche weitere Tauschbörsen, wie Audiogalaxy, eDonkey, Aimster, Gnutella, um nur einige davon aufzuzählen.
Diese Tauschbörsen haben verschiedene Gemeinsamkeiten. Zum einen verwenden sie das vom Fraunhofer-Institut entwickelte Audiocodierverfahren MP3, welches eine höchst effektive Datenreduktion bei der Übertragung und Speicherung von Audiosignalen ermöglicht.
Außerdem läuft der Austausch der Daten bei den Tauschbörsen nach der Technik des „Peer-to-peer File-Sharing“.

3.3. Peer-to-Peer

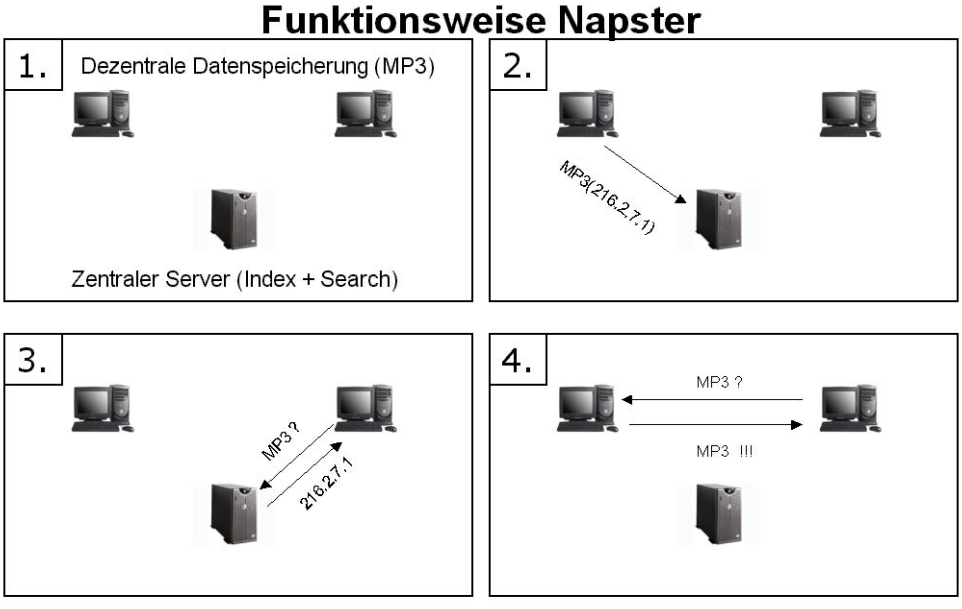
Die Idee des Peer-to-Peer ist in der Computerwelt nicht neu und beschreibt eine Idee, nach der „Kumpel“ die vorhandenen Ressourcen gemeinsam nutzen. In der einfachsten Form geschieht das durch die gemeinsame Nutzung von Netzwerkdruckern, in technisch anspruchsvolleren Anwendungen durch die gemeinsame Verwendung von ungenutzten Prozessorkapazitäten eines Rechners (z.B. www.setiathome.ssl.berkeley.edu).
Die Definitionen für Peer-to-Peer sind vielfältig, beschreiben aber im wesentlichen ein Netzwerk, in dem „intelligente“ Clients kommunizieren. In diesem Netzwerk sind somit Client und Server dasselbe, sogenannte „Servents“. Jegliche Form der Zentralisierung

[2] Die Rheinpfalz, 26. Januar 2002, Nr. 22

fehlt und „das Netzwerk selbst ist der Computer“. Nicht jede Definition geht aber so weit und oftmals wird auch eine Netzwerkarchitektur als Peer-to-Peer betrachtet, die einen zentralen Server und unabhängige Clients nutzt. Beide Formen, „Servents“ und Server mit Clients finden sich in der Praxis.
Der feine Unterschied, der zukünftig signifikante Auswirkungen auf die Durchsetzung eines internationalen Copyright-Schutzes haben könnte, wird im folgenden an den Beispielen Napster und Gnutella erläutert werden.

3.3.1 Napster

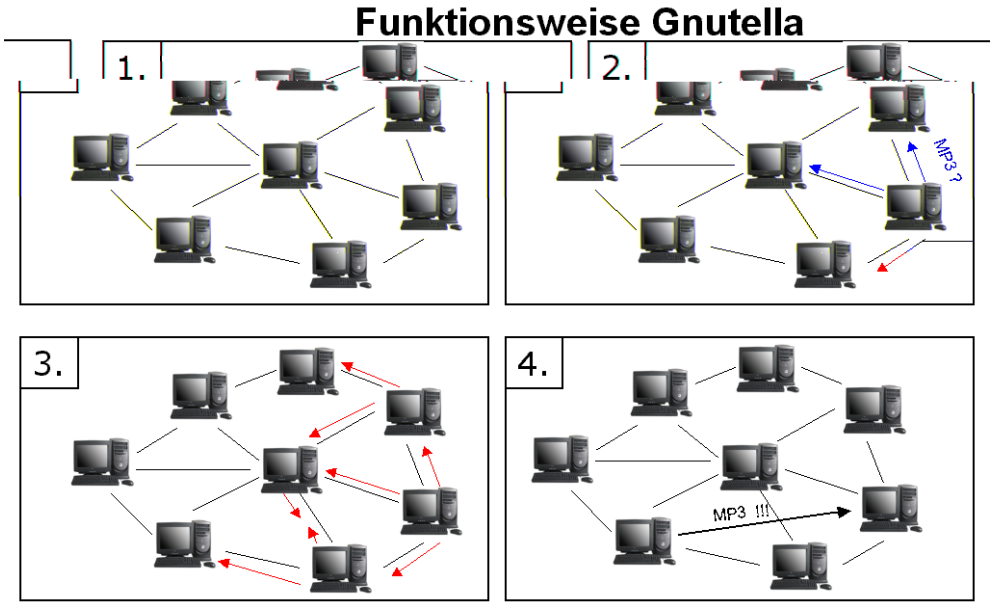
Napster wurde 1999 von dem amerikanischen Studenten Shawn Fanning gegründet, der nach einer Möglichkeit suchte, Musiktitel mit Kommilitonen über das Internet auszutauschen. Erste Gerichtsverfahren wegen Urheberrechtsverletzungen waren bereits im selben Jahr anhängig. Trotzdem überstieg die Anzahl der Nutzer im September 2000 die Anzahl von 38 Millionen. Unter dem Druck der Gerichte und der Musikindustrie ging Napster eine Allianz mit der Bertelsmann Music Group ein, zu der im späteren Verlauf noch EMI und WARNER Music stießen. Im Jahr 2002 soll Napster zu einem kostenpflichtigen Angebot werden.
Das Napster Peer-to-Peer-Netzwerk involviert einen zentralen „directory server“. Die Speicherung der Musiktitel erfolgt dezentral auf den Client-Rechnern. (→ 1.) Ein Client, der ans Netz geht, übermittelt dem Server die Titel, die er zur Verfügung stellt. (→ 2.) Ein weiterer Client, der sich auf der Suche nach bestimmten Titeln ans Netz begibt, übermittelt dem Server eine Suchanfrage, woraufhin dieser ihm die Daten eines weiteren Clients übermittelt, der über den gesuchten Titel verfügt. (→ 3.) Der Austausch des Titels erfolgt dann direkt über die Clients. (→ 4.)



Entscheidend dafür, dass Musikindustrie und Behörden gegen Napster vorgehen konnten, war, dass es einen zentralen Server gibt. Dieser ist lokalisierbar und kann jederzeit abgestellt werden, woraufhin das Peer-to-Peer-Netzwerk faktisch stillgelegt wird.

3.3.2 Gnutella

Gnutella wurde von Justin Frankel entwickelt und erlaubt im Gegensatz zu Napster den Austausch jeglicher Daten, so dass über Gnutella-Netzwerke nicht nur Musik, sondern auch Filme, Software und pornographisches Material ausgetauscht werden können.
Das Gnutella-Protokoll wurde seinerzeit nur wenige Stunden auf der Website von American Online angeboten, in dieser Zeit aber von Tausenden Internetnutzern auf deren Rechner heruntergeladen.
Dieses Protokoll ist frei verfügbar und wird auf freiwilliger Basis weiterentwickelt. Der entscheidende Unterschied zu Napster besteht darin, dass es auch ohne zentralen Server funktionsfähig ist, da alle beteiligten Rechner als „Servents“, d.h. als Server und Clients fungieren und miteinander verbunden sind. (→ 1.)
Bei der Suche nach Musiktiteln richtet der erste „Servent“ eine Suchanfrage an die umliegenden „Servents“. Diese überprüfen die eigene Verfügbarkeit der Titel (→ 2.) und richten, falls sie selbst nicht über die gesuchten Daten verfügen, weitere Suchanfragen an „umliegende“ „Servents“. (→ 3.) Diese Prozedur schreitet solange fort, bis ein „Servent“ mit dem gesuchten Titel gefunden wird. Eine Meldung mit den Daten des gesuchten „Servents“ geht über die ganze Kette zurück zum ursprünglichen „Servent“, woraufhin eine direkte Verbindung zwischen beiden hergestellt wird. (→ 4.)



Der Wegfall eines zentralen Servers verhindert, dass nationale Behörden durch einen lokalen Zugriff das gesamte Netzwerk stilllegen können. Darüber hinaus ist das Gnutella-Protokoll mittlerweile zur Basis zahlreicher Tauschbörsen geworden. Selbst wenn die Behörden auf zahlreiche Rechner zugreifen würden, blieben immer noch Millionen anderer Rechner, die weiterhin über das Gnutella-Protokoll verfügen und dies jederzeit wieder zum Herunterladen anbieten könnten.
Dies hat aber nicht nur Bedeutung für die Musikindustrie, sondern bereitet auch Systemadministratoren Sorgen.
Denn Gnutella arbeitet wie bereits dargestellt nach einem „Schneeballprinzip“, und eine einzige Suchanfrage kann ein enormes Datenaufkommen, auch innerhalb von Firmennetzwerken, induzieren. Eine besondere Bedrohung stellt darüber hinaus die Fähigkeit Gnutellas dar, Firewalls zu umgehen. Geht beispielsweise eine Suchanfrage von Rechner A aus und Rechner C, der über die gesuchten Informationen verfügt, befindet sich hinter einer Firewall, durch die er eigentlich keine fremdindizierten Verbindungen aufbauen kann, wird eventuell über den Umweg des Rechner B Rechner C dazu veranlasst, eine Verbindung nach A selbst zu iniziieren.
Dabei kann Gnutella, wie bereits erwähnt, nicht nur Musikdateien übermitteln, sondern beispielsweise auch Viren.

3.4 Fazit

Nicht nur für die Musikindustrie, sondern für alle Branchen, deren Produkte in digitaler Form angeboten werden, stellen Internet-Tauschbörsen aus Sicht des Copyright-Schutzes eine große Bedrohung dar.
Napster war eine vergleichsweise geringe Gefahr. Viel gravierender sind Gnutella-basierte Anwendungen, da diese durch ihre dezentrale Organisation kaum angreifbar sind. Eine geringe Hoffnung kann für die Musikindustrie darin liegen, dass die Tauschbörsen in der Regel von verhältnismäßig wenigen Nutzern leben, die ihre Titel bereitwillig zur Verfügung stellen, während der Großteil der übrigen Nutzer vorwiegend Titel herunterlädt. Ein Zugriff auf die Hauptanbieter könnte so, zumindest für eine gewisse Zeit, das Angebot an freien Titeln einschränken.
Bisher ist allerdings nicht bekannt, dass überhaupt gegen Nutzer von Tauschbörsen vorgegangen wurde. Dies verwundert auch nicht, da z.B. unter deutschen Juristen umstritten ist, ob nur das Bereitstellen von kopierrechtlich geschützten Daten oder auch das Herunterladen strafbar ist. Ungeklärt ist auch, wie sich die Lage darstellt, wenn sich die Nutzer untereinander kennen, was einige Tauschbörsen bereits dazu veranlasst hat, auch Chatrooms einzurichten.

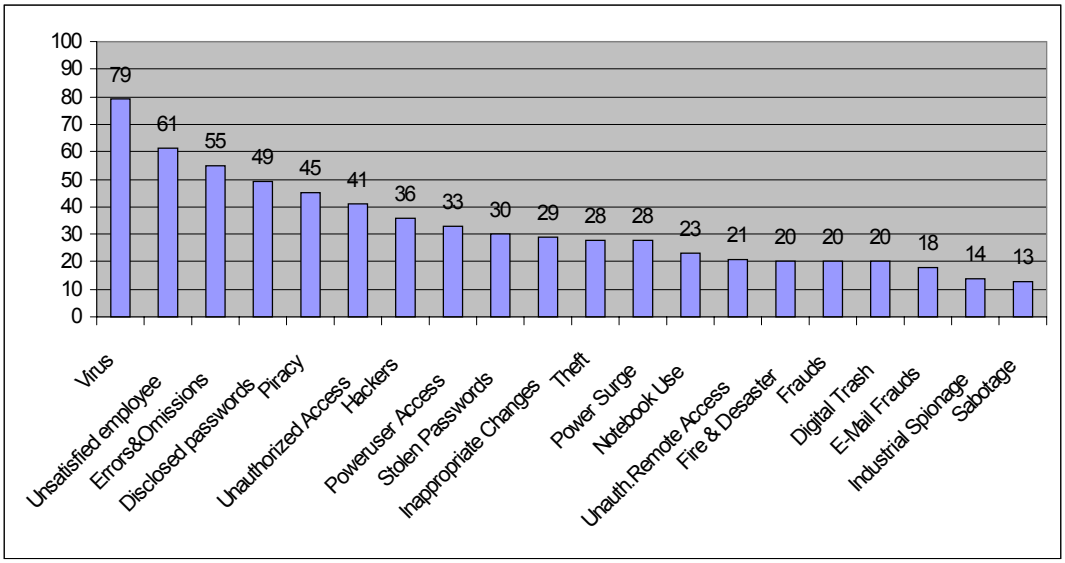
Auch in den USA scheint die Rechtslage nicht eindeutig zu sein. So wurde Napster stillgelegt, während in Texas Audiogalaxy, einer der zahlreichen Klone von Napster, weiterhin aktiv ist.

Auch ist fraglich, ob Nutzer von Tauschbörsen bereit sind, zukünftig für Napster zu bezahlen, wenn sie die gleichen Titel auch über Gnutella eben mit weniger Komfort erhalten können. Dies wird umso fraglicher, da sich die Musikkonzerne bisher noch nicht einmal auf eine Tauschbörse einigen konnten, so dass deren Nutzer, im Gegensatz zu Gnutella, nur Zugriff auf die Interpreten haben, die beim jeweiligen Konzern unter Vertrag sind.

4 Internetcrime: Neue Dimensionen der Kriminalität

Die kommerzielle Bedeutung des Internets wächst von Tag zu Tag, die Anzahl seiner Nutzer steigt rasant an. Doch mit der Zunahme der Bequemlichkeiten, die das Netz mit sich bringt, häufen sich auch die kriminellen Handlungen im Cyberspace.[3] Nicht nur für den Nutzer, auch für die Kriminalität eröffnet die weltweite Vernetzung neue Dimensionen. Dabei reichen die Vergehen von von Computersabotage und Softwarepiraterie über herkömmliche Wirtschaftkriminalität wie Kreditkartenbetrug und Konkursdelikte bis hin zur organisierten Kriminalität wie Geldwäsche und Industriespionage.[4] Abbildung 1 gibt einen Überblick über die vielen Möglichkeiten der Internetkriminalität:

Abbildung 1: Varianten der Internetkriminalität



Quelle: ARC Advisory Group.

Die Begriffe Internetkriminalität und Computerkriminalität werden im Sprachgebrauch nicht voneinander abgegrenzt. Während sich für „Internetkriminalität“ kein Eintrag im Duden findet , wird „Computerkriminalität“ wie folgt definiert: „Die Gesamtheit der Straftaten, die mit Hilfe einer Computeranlage begangen werden.“[5] Der Begriff umschreibt also alle Straftaten,die im und mit Hilfe des Netzes begangen werden:

[3] Vgl. o.V.: Reale Angriffe aus der digitalen Welt. In: Creditreform 9/2000, S.18. downloaded am 16.11.2000.
[4] Vgl. ebenda, S.18.
[5] Vgl. o.V.: Stichwort Computerkriminalität. In: Duden- Deutsches Universalwörterbuch. Aus: www.xipolis.de vom 10.03.02;.

4.1 Formen der Internetkriminalität

Im Allgemeinen sind die Formen der Kriminalität, die durch das Internet auftreten, schon vor dem Internet vorhanden gewesen. Es wurde nur der Nutzen des neuen Mediums erkannt und umgesetzt. Dazu zählen Urheberrechtsverletzungen (Raubkopien z.B. in der Musikbranche), Geldwäsche über online-banking und Kinderpornographie, aber auch technische Eingriffe durch Viren, Trojaner u.ä. Im Folgenden wird auf die Wichtigsten Formen kurz eingegangen.

Eine neue Form eines alten Phänomens stellt der **Cyber-Terrorismus** dar. Vor allem in den Vereinigten Staaten werden Anschläge auf öffentliche Einrichtungen über das Internet befürchtet. Unter Cyber- Terrorismus wird der Gebrauch von Computer-Ressourcen verstanden, um eine Regierung oder Zivilbevölkerung zu einzuschüchtern oder durch Bedrohung eine Handlungsweise zu erzwingen.[6] Ein Beispiel für Cyber-Terrorismus ist der unautorisierte Eingriff in das Computersystem eines Krankenhauses, um die Medikamenten-verteilung oder -dosierungen der Patienten zu verändern.

Eine neue Dimension hat auch die **Industriespionage** erreicht. Während in Deutschland hauptsächlich „spielerische“ Angriffe von Hackern durch die Presse gehen, ist es in den USA inzwischen gang und gäbe, als Unternehmen professionelle Hacker damit zu beauftragen, die Konkurrenz auszuspionieren.[7]

Softwarepiraterie wird in der Bevölkerung oft als Kavaliersdelikt eingestuft. Tatsächlich entstehen gerade der Musikbranche durch unautorisiertes Kopieren von Musikdaten immense Schäden. Auf das illegale Kopieren von Musik wurde in den vorhergehenden ausführlich eingegangen. Aber auch Softwarehersteller haben durch private oder gewerbliche Schwarzkopien ihrer Produkte Verluste hinnehmen müssen. CD- Brenner werden aufgrund der potentiellen Urheberrechtsverletzung, die ihre Nutzung mit sich bringt, beim Verkauf mit einer Sonderabgabe belastet.

Die bekannteste Form der technischen Computerkriminalität ist sicherlich die Computersabotage durch **Viren, Würmer oder Trojaner**. Dies sind alles Namen für kleine Computerprogramme, die kreiert wurden, um in einen Computer ohne das Wissen oder die Erlaubnis des Eigners einzudringen und unerwünschte, (für den

---

[6] Vgl. o.V.: cyber-terrorism. Aus: www.-cs.etsu.edu/gotterbarn vom 23.11.2000, S. 1.

7 Vgl. o.V.: Geliebter Feind. In: Magazin Kriminalität. Internet World Nr.06 vom 01.06.2000, S. 078.

Eigner) nutzlose und schädigende Maßnahmen vorzunehmen.[8] Der Unterschied zwischen den einzelnen Formen liegt vor allem in der Art und Weise, wie die Programme von Computer zu Computer weitergegeben werden.

Viren sind Codefragmente, die sich an andere Daten anhängen oder Teile von ihr löschen und sich ausschließlich bei deren Ausführung oder Bearbeitung vermehren.[9] Viren gelangen über Datenträger, durch das Downloaden eines Programmes oder das Öffen einer e-mail auf einen Rechner. Sie benötigen also menschliche „Hilfe“.

Besondere Formen von Viren sind Würmer, Trojanische Pferde oder auch eine Hoax. Würmer sind „intelligente“Viren, die sich selbst verbreiten können, z.B. verschicken sie sich selbständig über e-mail. Als ein Trojanische Pferd bezeichnet man ein Programm, das zum Ausspähen von Passwörtern, Geheimnummern, u.ä. geschrieben wurde, indem Tastaturfolgen gespeichert und dem Schöpfer des Trojaners übermittelt werden.[10] Trojaner laufen im Hintergrund ab, ohne daß der Nutzer es bemerkt. Eine weiterentwickelte Form ist ein Server /Client -System. Der Trojaner als Server ermöglicht es dem Klienten, auf den befallenen Rechner zuzugreifen. Trojaner werden meist an ein Program angehängt, das dem Nutzer einen Vorteil bringt, z.B an einen Bildschirmschoner, den man sich kostenlos downloaden kann.

Eine **Hoax** ist kein Virus im eigentlichen Sinne, sondern ein falsche Warung vor einem Virus. Sie tritt in Form von e-mails auf, die vor einem besonders bösartigem Virus warnen und an alle Freunde und Bekannte weitergeschickt werden sollen. Als Absender wird gerne eine bekannte Firma oder vertrauenswürdige Institution, z.B. die Polizei, angegeben.

4.2 Einfluß der Internet-Kommunikation auf die Kriminalität

Durch die globale Vernetzung wird die Welt kleiner. Nutzer können Informationen quasi von ihrem Schreibtisch aus rund um den Erdball austauschen. Kontakte mit anderen „wildfremden“ Menschen sind kein Problem mehr. Die Dimensionen der Kommunikation verändern sich. Und die Kriminalität weiß ihren Nutzen daraus zu ziehen.

---

[8] Vgl. Nixon: Computer Crime. Internet Service & Technology, Telecommunications. Aus: ZT FIZ W, Mch P vom 24.11.2000, S. 1.
[9] Vgl. www.trojaner-info.de/viren vom 10.3.02.
[10] Vgl. www.trojaner-info.de/trojanerwas vom 10.3.02.

Das Bundeskriminalamt geht davon aus, daß durch das Internet keine neuen Kriminalitätsformen entstanden sind, sondern die Täter sich nur eines neuen Mediums bedienen.[11] Jedoch die Dimensionen, die durch dieses neue Medium erreicht werden, sind enorm. Die Kriminalität wird virtuell, der früher nötige physische Einsatz durch das Netz überflüssig.

Diese Körperlosigkeit erleichert auch in der Kriminalität vieles. Der Täter muß seinem Opfer nicht mehr gegenüber stehen, Täuschungen werden einfacher. Geldkartenbetrug gibt es schon lange. Doch mußte früher die Geldkarte gestohlen und mit der Karte im Geschäft der Verkäufer getäuscht werden oder am Bankautomaten angestanden werden. Heute können Betrüger durch Käufe im Internet erheblich schneller weitaus höheren Schaden anrichten.

Auch der Warenbetrug hat sich das Internet zunutze gemacht. Die Täter bieten im Netz etwas gegen Vorkasse an, das entweder nicht vorhanden war oder nicht geliefert wurde. Die Wahrscheinlichkeit, daß der Täter gefaßt wird, ist gering. Eine Website ist schnell gelöscht und der ehemaliger Anbieter nicht mehr auffindbar.

Auch in der Industriespionage eröffnete die virtuelle Welt neue Möglichkeiten.Wo sich ein Täter früher an den Ort begeben mußte, um Informationen zu stehlen, kann er heute vom Sofa aus über das Netz in eine Firma einbrechen. Die Entdeckungsgefahr ist wesentlich geringer, im Höchstfall wird angezeigt, daß ein Eindringungsversuch vonstatten geht. Die Rückverfolgung zum Täter oder gar seine Ergreifung ist nahezu unmöglich. Denn wie soll auf einen Menschen zugegriffen werden, der vielleicht tausende von Kilometern entfernt sitzt?

Die durch die Virtualität des Netzes abstrahierte Straftat bedarf geringerer Hemmschwellen und ist deutlich leichter und schneller zu begehen; Schäden, die durch unautorisierte Informationsweiterleitung entstehen, sind nicht mehr rückgängig zu machen. Hinzu kommt, daß laxe Sicherheitsvorstellungen Hackern Tür und Tor öffnen. So sahen noch in einer Umfrage 67% der befragten Unternehmen keine Notwendigkeit, die ihnen wohlbekannten Sicherheitsmängel ihres Systems zu beseitigen.[12] Es befürchten nur 20% der Befragten einen Mißbrauch von Benutzerrechten, obwohl schon 70% einen solchen tatsächlich registriert haben [13] Da

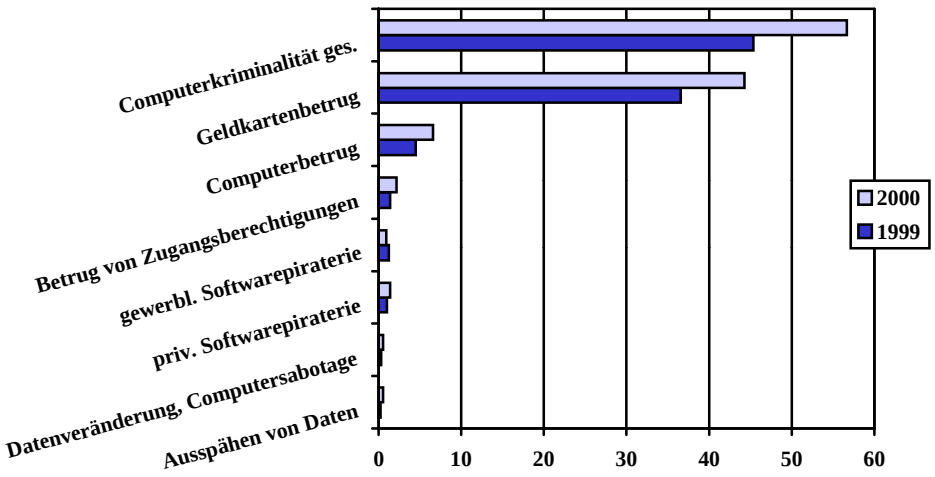
[11] Vgl. o.V.:Geliebter Feind. In: Magazin Kriminalität. Aus: Internet World Nr.06 vom 01.06.2000, S. 078.

12 Vgl. o.V.: Geliebter Feind. In: Magazin Kriminalität. Internet World Nr.06 vom 01.06.2000, S. 079.

[13] Vgl. ebenda, S. 079.

verwundert es nicht, daß die Computerkriminalität von 1999 auf 2000 um 20% gestiegen ist:

Abbildung 2: Comuputerkriminalität in Deutschland



Quelle: Kriminalstatistik des Bundeskriminalamtes; erfaßte Fälle in Tausend

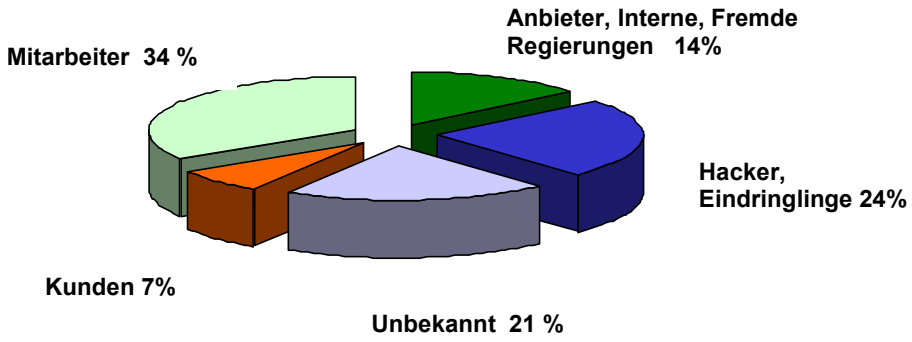
4.3 Sicherheitsrisiken

Das e-business bringt es mit sich, daß sowohl Unternehmen als auch Kunden mehr und mehr von ihrer Privatsphäre preisgeben müssen. Nur so läßt sich aus gegenseitigem Informationsaustausch ein optimaler Nutzen ziehen.[14] Leider kümmern sich die Unternehmen nicht genügend um den Schutz ihrer Firmendaten. Unautorisierte Zugriffe von außen sehen viele Unternehmen zwar als Gefahr an. Bei Angriffen von innen sind die meisten ungeschützt. Diese Tatsache mag auch darauf zurückzuführen sein, daß interne Sicherheitsmaßnahmen die Mitarbeiter nicht bei der Erfüllung ihrer Aufgaben behindern dürfen, da dies die Arbeitsmotivation negativ beeinflußt.

Doch die Schäden, durch die Sabotage unzufriedener Mitarbeiter entstehen, machen 34% der Gesamtschäden eine Unternehmens aus. Dies sind 10% mehr als durch Hacker-Angriffe von außen.

14 Vgl. ARC Advisory Group (Hrsg.): E-Security Strategies for Enterprises. In: ARC Strategies 5/2000, S. 2.

Abbildung 3: Registrierte Sicherheitsübertritte in Prozent



Quelle: ARC Advisory Group

Dies zeigt, daß in naher Zukunft die Firmen deutlich in interne Sicherheit investieren müssen. Um so mehr, da die Statistiken ein allgemeines Ansteigen von Datenmißbräuchen, interne sowie externe Angriffe, anzeigen.[15] Nur durch verstärkte Sicherheitsmaßnahmen werden die Unternehmen die damit steigende Verunsicherung ihrer Kunden unterbinden können.

15 Vgl. ARC Advisory Group (Hrsg.): E-Security Strategies for Enterprises. In: ARC Strategies 5/2000, S. 2.

5 Maßnahmen der Sicherheit

In der näheren Vergangenheit wurden einige bekannte Unternehmen Opfer von Computerattacken. Durch das wachsende Interesse der Öffentlichkeit und die damit verbundene zunehmende Bedeutung des e-Commerce steigen auch die Bedürfnisse der Nutzer und Kunden nach Sicherheitsmaßnahmen.[16] Dabei kommen grundsätzlich zwei Ansatzweisen in Betracht: Zum einen die Netzwerk-Sicherheit, bei der der Schutz von Computern, Druckern und andrem Computer-Zubehör direkt oder indirekt den Web-Server betrifft oder zum anderen die Übertragungs-Sicherheit, die bei online-Kommunikation während der Transaktion greift .[17]

Sicherheitsmaßnahmen können von technischer oder organisatorischer Natur sein. Der Gesetzgeber versucht außerdem, die Gesellschaft durch entsprechende Vorschriften zu schützen und Betreibern und Nutzern gewisse Sicherheitsmaßnahmen abzubedingen.

5.1 Technische Sicherheitsmaßnahmen

Der Markt für Sicherheitsmaßnahmen ist stetig am wachsen. Die Technologie hat sich den Bedürfnissen angepaßt und bietet mehrere Möglichkeiten. Die Kathegorien werden nach den Ansatzpunkten der technischen Maßnahme unterschieden.[18] Es gibt jedoch Produkte, die eine Kombination darstellen.

1. Zutrittssicherungen (Netzwerksicherung)

Vertrauliche Daten sollen durch Barrieren gegen unautorisierte Zugriffe geschützt werden. In diese Kathegorie gehören Firewalls und alle Arten der Zugangsberechtigung (Authentication) durch z.B. Passwörter und PIN-Nummern. Eine Firewall bildet eine starke Barriere zwischen einem privaten Netzwerk und dem Internet. Diese Technologie kann auch eingesetzt werden, um eine bestimmte Zahl eigener Ports zu beschränken, so daß z.B nur bestimmte Protokolle passieren können. Die Installation von Firewalls ist relativ gebräuchlich, aber wiegt Unternehmen manchmal in einer falschen Sicherheit.[19] Wenn diese Zugriffssicherungen Mitarbeiter

16 Vgl. Tran-Minh (ohne Vorname): The market for network and e-commerce secuirty and their services. In. FIZ Wirtschaftsinformationen 10/2000, S.1.

17 Vgl. ARC Advisory Group (Hrsg.): E-Security Strategies for Enterprises. In: ARC Strategies 05/2000, S. 6.

18 Vgl. Titterington, Graham et al.: E-business Security. New Directions and Sucsessful Strategies. Hrsg. Ovum Ltd. London usw. 2000, S. 154.

19 Vgl. Tran-Minh (ohne Vorname): The market for network and e-commerce security and their services. In:FIZ Wirtschaftsinformationen 10/2000, S. 3.

zu sehr behindern, wird häufig versucht, diese zu umgehen oder zu „durchlöchern“, wodurch die Firewall natürlich auch wieder durchlässig für Dritte wird.

2. Kommunikationssicherung (Transaktionssicherung)

Beim Übertragen werden Daten für einen Dritten unkenntlich gemacht, indem sie verschlüsselt werden. Viele Unternehmen nutzen den Spielraum, der durch Verschlüsselungsprotokolle bei Browsern (SSL) oder OSs (PPTP) angeboten werden. Diese bieten deutliche Kosten- und Entwicklungsvorteile, haben aber noch Kontrollschwierigkeiten und müssen als Standards noch weiter entwickelt werden.[20] Bei beiden Protokollen sind vor kurzem bisher noch ungeklärte Mängel aufgetreten.

Pretty Good Privay (PGP) gilt als das sicherste Verschlüsselungssystem im e-mail-Verkehr. Hier wird mit zwei „Schlüsseln“ gearbeitet, eimem Verschlüssler, der nur bei dem Absender verbleibt und einem Entschlüsseler, der dem Adressat zugesendet wird. Jedoch sind im letzten Jahr Fälle von Hackern bekannt geworden, die PGP „geknackt“ haben sollen.

Eine weitere Möglichkeit zur Sicherung von Transaktionen im Netz bieten VPNs (Virtual Private Networks), die in Kombination mit einer Firewall oder als „Standalone“-Server hinter einer Firewall eingerichtet werden können. Ein VPN ist ein privates Netz, das über das öffentliche Netz Nutzer oder/und Branchen-Geschäftsstellen verbindet, indem es Verschlüsselung und Tunneling gebraucht. Es stellt quasi ein nicht wirkliche „Privatisierung“ bestimmter Verbindungen, einer Vermietung vergleichbar, im Internet her. Ein gut konstruiertes VPN kann eine strake Unterstützung eines Unternehmens darstellen, da es neben dem Sicherheitsaspekt noch viele andere Vorteile bietet, wie die Ausweitung der geographische Verbindungen, Vereinfachung der Netzwerk-Topographie und Reduktion der Transaktions- und Transportkosten für weit entfernte Nutzer. Dier Branche des VPNs ist trotz der nicht unerheblichen Kosten ein rasantes Wachstum vorhergesagt.

Dies gilt ebenfalls für die Public Key Infrastrukture (PKI). Hier wird eine asymetrische Verschlüsselung verwendet.

Versicherungen verwendet, es wird jedoch eine deutliche Zunahme auch in anderen Branchen erwartet.[22]

3. Inhaltssicherung

Die größte Bedrohung ihres Unternehmens sehen viele IT- Manager in Viren. Die Anti-Virus- Technologie ist ausgereift und ist bei geringen Kosten leicht zu installieren. Nachteilig ist sicherlich, daß eine regelmäßige Wartung und Erneuerung nötig ist und eine Anti-Virus -Einrichtung nicht präventiv agieren kann.

4. Sicherheitsmanagement

Durch Zugriffskontrollen wie Firewalls oder Authentication werden Dritte, hauptsächlich Verbraucher, als potentielle Hacker angesehen. Als Konsequenz daraus entstanden Real-Time-Überwachungsprodukte, die unautorisierte Angriffe auf das System sofort melden. Jedoch konnten auch diese bisher überlistet werden, indem der Hacker viele Angriffe gleichzeitig simulierte und damit das System überfordete, das dann überhaupt nicht mehr reagierte. Zu dieser Kathegorie gehören neben der Intrusion Detection auch alle anderen Beobachtungs- und Überwachungsprodukte und Risk-Management-Anwendungen. Auf diesem Sektor ist die Fähigkeit, aktiv Schwachstellen aufzuspüren, Viren zu erkennen und die Sicherheitsprodukte entsprechend zu rekonfigurieren von höchster Bedeutung.[23]

5. Architektur

Zur Sicherung ist es neben technischen Barrieren möglich, in der Struktur internen Netzwerks eine Sicherung zu implementieren: Die DMZ („demilitarized zone“) stellt die beste Möglichkeit dar, Zugriffe von Dritten auf Daten zu sichern.[24] Bei dieser Kostruktion wird das Datensegment, das einem Zugriff von außen freigegeben werden soll, durch eine Firewall vom restlichen internen Netzwerk isoliert. Synkronisationsprobleme und Applicationsstrukturen zwingen viele Unternehmen jedoch, ihr gesamtes Netzwerk zu öffnen.

Die Anbieter für Sicherheitsprodukte kommen aus allen Bereichen, die in irgendeiner Form mit Sicherheit oder Informatik in Berührung stehen. edoch auch aus anderen Sektoren, z.B. der Telekommunikationsbranche, strömen Anbieter auf den Sicherheits-Markt, da dieser im Wachstum begriffen ist und große Gewinnmöglichkeiten verspricht.

22 Vgl. Dataminor (Hrsg.): Network Security 1998- 2003. London, New York 1999, S. 132.

23 Vgl. Titterington, Graham et al.: E.business Security. New Directions and Successful Strategies. Hrsg. Ovum Ltd. 2000, S. 155.

Generell sind vier Gruppen von Anbietern zu identifizieren.[25] Zu den **Anbietern von Sicherheitssoftware** und -produkten gehören Network Associates, Checkpoin und Entrust Technologies. Aus dem IT-Service-Bereich kommen **traditionelle Anbieter** wie IBM Global Service, Nortel Networks und PricewaterhouseCoopers. Viele Firmen aus der **Telekommunikation** wie die Deutsche Telekom, WorldCom u.a. bieten ebenfalls Sicherungsprodukte an. Eine weitere Gruppe bilden die **Anbieter von End-to-End-Sicherheitssystemen**, die nur vereinzelt verbreitet sind, sich aber im Wachstum befinden.

5.2 Organisatorische Einrichtungen

Die Bedrohung aus dem Internet hat zahlreiche Organisationen ins Leben gerufen, die sich aktiv und passiv am Schutz gegen die Netzwerkkriminalität beteiligen. Sowohl von privater als auch von öffentlicher Seite sind vor allem in den Vereingten Staaten verschiedene Guppierungen entstanden. An dieser Stelle soll exemplarisch auf einige eingegangen werden.

24 Vgl. Meta Group (Hrsg.): Global Networking Strategies (GNS), File 623. 26.09.2000, S.1.

25 Vgl. Titterington, Graham et al.: E.business Security. New Directions and Successful Strategies. Hrsg. Ovum Ltd. 2000, S. 155.

1. Internet Fraud Complaint Center

Das Internet Fraud Complaint Center (IFCC) ist aus einer Kooperation von FBI und dem National White Crime Center (NW3C) entstanden, um jedliche Art von über das Internet begangenen Bertug zu bekämpfen.[26] Im Rahmen dieser Zusammenarbeit werden zunächst alle Informationen über diese Thema gesammelt, organisiert und ausgewertet. Verbraucher dürfen landesweit von ihren Beschwerden und Befürchtungen (USA) berichten. So können neue Trends frühzeitig erkannt und eine Gegenmaßnahmen entwickelt werden. Es ist das Ziel des IFFC, eine „nationale Strategie“ gegen den Internetbetrug zu entwickeln.[27]

Das NW3C betreibt ein nationales Netzwerk zur Unterstützung von Regierungseinrichtungen, staatlichen Regulationskörperschaften, Staatsanwaltschaften und anderen Organisationen, die sich mit Prevention, Nachforschung oder Verfolgung von Wirtschaftskriminalität in der High-Technolgie befassen.[28] Durch die logische Zusammenstellung von Ressourcen ist es dem NW3C gelungen, diese verschiedenden Einrichtungen zu verbinden und so ihre effektivität zu maximieren.

Eine ähnliche Einrichtung ist auch die Computional Immunology Fraud Detection. Dieses Projekt ist eine Zusammenarbeit von PostOffice, Kings College Londen und Anite Government Systems in Großbritannien.[29]

2. Internet Fraud Watch

Der Internet Fraud Watch ist eine Abteilung auf der NFIC- Website, die 1996 von der der National Comsumers League (NCL) eingerichtet wurde, um die Verbraucher bei ihren Beschwerden und Fragen zu unterstützen.[30] Da die Zahl der Verbraucher, die im Internet einkaufen, ständig steigt, wurde die Bekämpfung von Betrügereien im Internet schnell zu einem Hauptanliegen. Die Internet-Seite stellt Artikel, Tips und andere Informationen zur Verfügung, wie man vermeidet, das Opfer eines Bertug zu werden, die Privatsspäre sichern und sich sicher im Netz bewegen kann.[31]

Die National Comsumers League (NCL) Anfang des letzten Jahrunderts als Amerikas erster Verein zum Schutz der Verbraucher gegründet. Die NCL beschäftigt sich u.a.

[26] Vgl. www.fbi.gov/programs/ifcc/fbinw3cpartnership.htm vom 17.11.2000.
[27] Vgl. ebenda.
[28] Vgl. www.fbi.gov/programs/ifcc/aboutnw3c.htm vom 17.11.2000.
[29] Vgl. Reuters. Business briefing vom 17.11.2000.
[30] Vgl. www. fraud.org/internet/intalert.htm vom 23.11.2000.

Verbesserung der Nahrungsverarbeitung (vor allem im Hygienebereich) und unzumutbaren Arbeitsbedingungen und angagiert sich gegen Kinderarbeit.

3. Internet-Streife

Um der Kriminalität im neuen medium Internet besser begegnen können, richtete die Polzei (CIA, aber auch das BKA) Internet-Streifen ein. Dies sind Arbeitsgruppen, die sich mit einen bestimmten Sachverhalt im Internet beschäftigen und kriminelle Handlungen im Netz verfolgen. Während sich in Deutschland diese Gruppen hauptsächlich mit Kinderpornographie konfrontiert sehen, bemühen sich ihre Kollegen in den Vereinigten Staaten immermehr um illegale Geldgeschäfte, Geldwäsche und Verstöße gegen das Urhebergesetz.

5.3 Gesetzliche Regulation

Gesetzliche Bestimmungen haben in verschiedenen Ländern die Implementation von Sicherheitsmaßnahmen vorangetrieben, vorallem im bereich der Banken und Versicherungen.[32] 2000 wurde von den Mirgliedern der Europäischen Union die cyber Crime Convention verabschiedet, an der sich auch die USA, Kanada und Süd Afrika beteiligten. Die ínternationale Zusammenarbeit zwischen den Staaten bei der Bekämpfung der Internetkriminalität soll gestärkt werden. Die Konverntion enthält auch eine sogenannte Preservation Order. Diese beeinhaltet eine Lockerung des Privatschutzes der Gestalt, daß die Polzei bei begründetem Verdacht die Provider anweisen kann, die Kommunikation der Verdachtspersonen einzufrieren, also die e-mails und Verbindungen zu speichern. Die Polizei kann mit einem richterlichen Durchsuchungsbefehl Einsicht in das Material nehmen.

Diese Regelung ist eine Gradwanderung zwischen dem Datenschutz und dringend notwendigen Maßnahmen, um Straftäter im Internet verfolgen zu können. Tatsächlich hat die EU eine Datenschutzrichtlinie erlassen, die in der Bundesrepublik mit dem Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste umgesetzt wurde. Darin wurde festgelegt, daß die Institutionen, die mit den Daten Dritter umgehen, nur notwendige Daten speichern dürfen und diese nach einer gewissen Zeit wieder löschen müssen. Die Unternehmen müssen alles in ihrer Macht Stehende tun, um die gespeicherten Daten zu sichern. Der Privatmann hat das Recht, jederzeit Einblick in seine gespeicherten Daten nehmen zu

[31] vgl. www.fraud.org/internet/intinfo.htm vom 23.11.2000.

können, bei überflüssiger Speicherung und beim Wegfallen der Speichungsgrundlage sofort die Löschung und sofortige Berichtigung falscher Daten zu verlangen.

Auch in anderen Ländern sind Tendenzen zu weitgreifenden Überwachungsmaßnahmen im Internet zu beobachten. In Frankreich ist eine weiterentwickelte Verschlüsselung gesetzlich verboten, da Verschlüsslungen natürlich auch die kriminellen Handlungen schützt und ihre Verfolgung bzw. Aufklärung erschwert.[33] Die Erfolge der Ermittler und der Zwang zum Datenschutz haben diese Bedenken in anderen Ländern entkräftet.

In Großbritannien wurden verschiedene Regelungen und Vorschriften zur Kontrolle von Datenflüssen und Sicherheitsmaßnahmen den Security-Standard BS7799 aufgenommen. In den USA sind Strömungen verhanden, die nach dem 11. September die „totale Kontrolle und Überwachung“ im Internet ermöglichen wollen.

32 Vgl. Baccari-Edler, Sandra: Security- Services. Protecting the eBusiness Infrastrukture. Hrsg. international Data Cororation. 2000, S. 29.

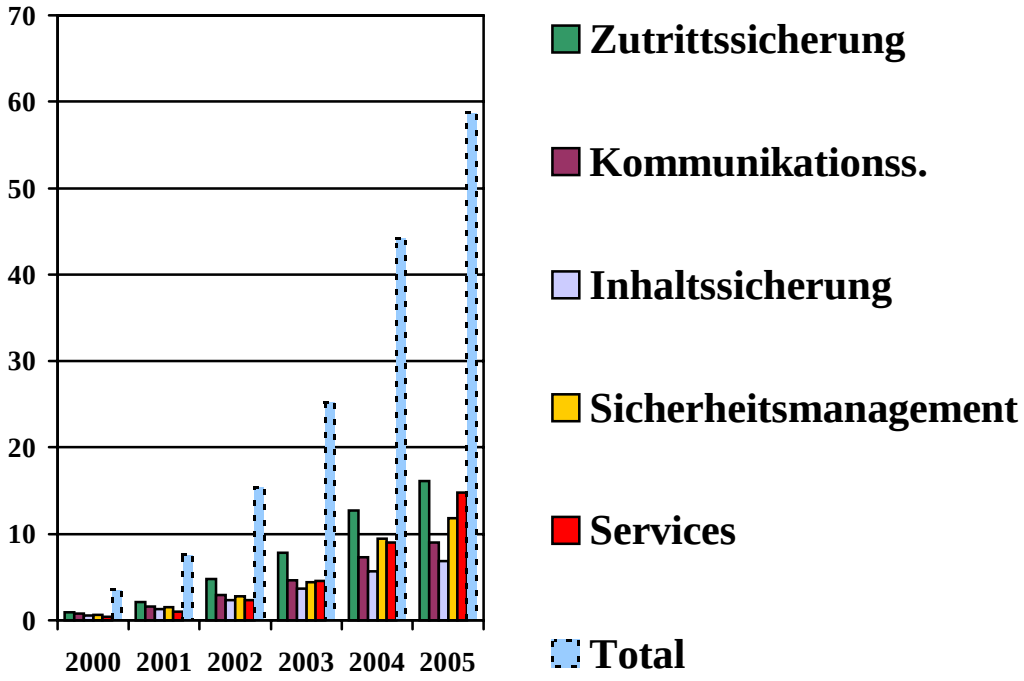
33 Vgl. Denning, Dorothy und Baugh, William: Hiding Crimes in Cyberspace. In: Information, Communication and Society. Vol.2, No.3, Herbst 1999, S. 2.

6 Bedeutung des Sicherheitsmarktes in der Zukunft

Die globale Vernetzung verbindet die Welt, bringt jedoch nicht nur Nutzen sondern auch Schaden. Die Kriminalität hat mit dem Internet neue Türen aufgestoßen, hinter denen ungeahnte Möglichkeiten zum Vorschein kamen. Doch kein Unternehmen wird am e-Business auf lange Sicht vorbeikommen. Zu groß sind die Vorteile, die dem Geschäft und den Verbrauchern daraus erwachsen. Der Druck auf die Unternehmen wächst, stärker in Sicherheitsmaßnahmen zu investieren. Zu groß ist die Gefahr eines Imageverlustes und die damit verbundenen Wettbewerbsnachteile. Zusätzlich verlangen immer mehr Regierungen, höchstmöglichem Datenschutz zu garantieren.

Daher ist ein immenses Wachstum auf dem Markt der E-Business-Sicherheiten zu erwarten, und dies in allen Sektoren:

Abbildung 4: Prognose der weltweiten Entwicklung am Sicherheitsmarkt



Quelle: Ovum Ltd.

Grundsätzlich ist es sicher, daß weitere Sicherheitsmaßnahmen im Internet notwendig

und um die Möglichkeiten bereit zustellen, preventiv zu agieren und nicht nur zu reagieren. Doch Sicherheit und Datenschutz sind zwei Seiten einer Medaille. Die absolute Sicherheit im Netz wird es nicht geben. Und wer die Vorteile der weltweiten Vernetzung und der verschiedenen Dienste in Anspruch nehmen will, wird einen Teil seiner Privatsphäre öffnen müssen. Es gilt abzuwägen zwischen notwendigem Schutz und Funktionalität.

Quellenverzeichnis:

Internet:

http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/pgp/index.htm (Stand 17.03.02)

http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/download/1zwwau.pdf (Stand 02.02.02)

http://www.inf.tu-dresden.de/~hf2/security/8DSfrdlT.pdf (Stand 02.02.02)

http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/download/anonfalt.pdf (Stand 02.02.02)

http://www.inf.tu-dresden.de/~hf2/publ/2000/BeFK2000cfp2000/BeFK2000.pdf (Stand 02.02.02)

http://www.cato.org/pubs/briefs/bp54.pdf(Stand 02.02.02)

http://securityresponse.symantec.com/avcenter/reference/p2pnetworking.pdf (Stand 02.02.02)

http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/presse/anon.htm (Stand 02.02.02)

http://www.tik.ee.ethz.ch/~rennhard/publications/WetIce2001.pdf (Stand 02.02.02)

http://www.bsi.de/ (Stand 02.02.02)

http://vsys-www.informatik.uni-hamburg.de/teaching/ws-01.02/seminar/p2p.pdf (Stand 02.02.02)

http://netresearch.ics.uci.edu/researchclass/243D/week%209%20lectures/Suzuki%20kun/napster.pdf (Stand 02.02.02)

http://www.cs.princeton.edu/courses/archive/fall01/cs109/lect15.pdf (Stand 02.02.02)

http://www.ncmag.com/2001_09/pdf91/gnutella91.pdf (Stand 02.02.02)

http://www.nwconnection.com/2001_12/pdfd1/catchd1.pdf (Stand 02.02.02)

http://www.carnet.hr/cuc/cuc2001/papers/b4.pdf (Stand 02.02.02)

http://cs.engr.uky.edu/~fei/teaching/cs685/slides/21.peer.pdf (Stand 02.02.02)

http://www.namics.com/namics/home.nsf/vFile/iex_2001/$FILE/2000FEB09_IEXs-3MPeertopeer.pdf (Stand 02.02.02)

www.fbi.gov/programs/ifcc/fbinw3cpartnership.htm
vom 17.11.2000.

www.fbi.gov/programs/ifcc/aboutnw3c.htm
vom 17.11.2000.

www.fraud.org/internet/intalert.htm
vom 23.11.2000.

www.fraud.org/internet/intinfo.htm
vom 23.11.2000.

www.trojaner-info.de/viren
vom 10.3.02.

www.trojaner-info.de/trojanerwas
vom 10.3.02.

Zeitungen / Zeitschriften:

www.xipolis.de: Stichwort Computerkriminalität. In: Duden- Deutsches Universalwörterbuch. 10.03.02

Die Rheinpfalz, 26. Januar 2002, Nr. 22

ARC Advisory Group (Hrsg.): E-Security Strategies for Enterprises. In: ARC Strategies 05/2000

Baccari-Edler, Sandra: Security- Services. Protecting the eBusiness Infrastrukture. Hrsg. international Data Cororation. 2000.

Dataminor (Hrsg.): Network Security 1998- 2003. London, New York 1999.

Denning, Dorothy und Baugh, William: Hiding Crimes in Cyberspace. In: Information, Communication and Society. Vol.2, No.3, Herbst 1999.

Meta Group (Hrsg.): Global Networking Strategies (GNS), File 623. 26.09.2000.

Nixon: Computer Crime. Internet Service & Technology, Telecommunications. Aus: ZT FIZ W, Mch P vom 24.11.2000.

o.V.: Geliebter Feind. In: Magazin Kriminalität. Internet World Nr.06 vom 01.06.2000.

o.V.: Reale Angriffe aus der digitalen Welt. In: Creditreform 9/2000, S.18. downloaded am 16.11.2000.

o.V.: cyber-terrorism. Aus: www.-cs.etsu.edu/gotterbarn vom 23.11.2000.

o.V.: Geliebter Feind. In: Magazin Kriminalität. Internet World Nr.06 vom 01.06.2000.

Reuters. Business briefing vom 17.11.2000.
Titterington, Graham et al.: E-business Security. New Directions and Sucsessful Strategies. Hrsg. Ovum Ltd. London usw. 2000.

Tran-Minh (ohne Vorname): The market for network and e-commerce security and their services. In:FIZ Wirtschaftsinformationen 10/2000.