INHALTSVERZEICHNIS

1 Einleitung

"Das Internet wird heute bereits als das "Netz der Netze" bezeichnet. Es stellt einen Zusammenschluß autonomer Rechner dar, die Informationen über das Protokoll TCP/IP austauschen. Mittlerweile gibt es weltweit ca.30 bis 40 Millionen Internet Anwender, und die Zuwachsraten sind enorm." [1] " Die Wirkung der Vernetzung geht weit über die enge Informationsverarbeitungs (IV)- und Kommunikationssicht hinaus. Wir erleben derzeit tiefgreifende Veränderungen, die sowohl das Arbeitsleben betreffen (z.B. Automatisierung) als auch weite Teile des gesellschaftlichen Zusammenlebens berühren (z.B. Online - Shopping)." [2] Der zunehmende Ausbau des Internets schafft neue Dimensionen des Computermißbrauchs. Die ausschließliche Reduzierung der Sicherheitsmaßnahmen auf verschlossene Computerräume und Paßwortschutz ist nicht mehr ausreichend. Die steigende Komplexität und Öffnung der Systeme läßt neue Methoden der Computerkriminalität zu. Im Rahmen dieser Arbeit soll ein Überblick über Sicherheitsrisiken des Internet und mögliche Schutzmaßnahmen gegeben werden. Besondere Aufmerksamkeit richtet sich dabei auf die Virenproblematik.

Das folgende Kapitel zeigt zunächst auf, wie man dem Problem "Sicherheit im Internet" effizient begegnen kann. Das vorgestellte Konzept des Risikomanagements ist auf Unternehmen konzipiert. Anhand der einzelnen Phasen soll modelliert werden, wie man der Gefahr durch das Internet vorbeugen kann. Mit Hilfe von Beispielen innerhalb des Punkts Risikobewertung soll die Bedrohung durch Computer Kriminalität im Internet durch Zahlen verdeutlicht werden.

Gliederungspunkt drei gibt einen Überblick der Sicherheitsrisiken des Internet sowie der Maßnahmen, die zum Schutz eingeleitet werden können.

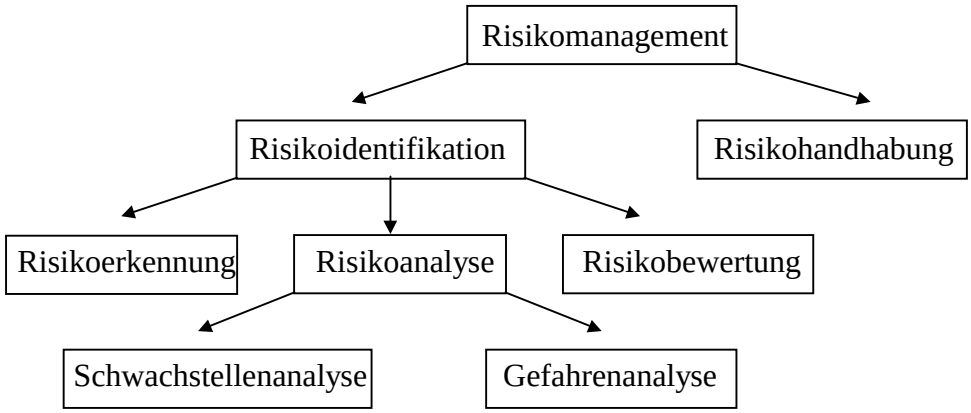
Nachdem ein Überblick gegeben worden ist befaßt sich Kapitel vier mit dem Risikofaktor Viren. Die Computer Anomalien werden zunächst definiert, um im nächsten

[1] Mertens, Grundzüge der Wirtschaftsinformatik, S.38
[2] Mertens, Grundzüge der Wirtschaftsinformatik, S.39

Schritt ihre Funktionsweise genauer zu erläutern. Anschließend werden mögliche Vorsichts- und Gegenmaßnahmen vorgestellt.
Der letzte Gliederungspunkt der Arbeit spricht Sicherheitslücken innerhalb des Unternehmens an. Dazu wird auf Sicherheitsrichtlinien verwiesen, die verhindern, daß Gefahrenquellen entstehen.

2 Risikomanagement

Die gesamten Aktivitäten, die sich mit der Identifikation und Bewältigung von Risiken beschäftigen, können im Rahmen des Risikomanagements betrieben werden. Das Risikomanagement ist eine Methode, mit der Unternehmen den vielfältigen Gefahren und Risiken, die die Verarbeitungs- und Kommunikationssysteme bedrohen, effektiv entgegenwirken. Es untergliedert sich in die Teilbereiche Risikoidentifikation und Risikohandhabung.[3]



Quelle: Wojcicki, Sichere Netze, München 1991

2.1 Risikoidentifikation

Aus der Risikoidentifikation werden Handlungsmaßnahmen abgeleitet. Sie erfolgt somit vor der Risikohandhabung und unterteilt sich in die Teilbereiche Risikoerkennung, Risikoanalyse und Risikobewertung, die im folgenden betrachtet werden sollen.

[3]vgl. Wojcicki, Sichere Netze, S.24

2.1.1 Risikoerkennung

Erster Teil der Risikoidentifikation ist die Risikoerkennung. Es wird zunächst der Bereich abgegrenzt, für den die Risikoanalyse durchgeführt werden soll. Die Analysen werden aufgrund ihrer Komplexität nur für Teilbereiche der EDV - Infrastruktur durchgeführt. Es werden Schnittstellen zwischen den einzelnen Analysebereichen definiert, an denen in einer späteren Phase die Teilergebnisse aneinandergefügt werden können. Nachdem der Analysebereich festgelegt ist, versucht man alle Risiken detailliert zu beschreiben und auf ihre Auswirkungen zu untersuchen. Für die Risikoerfassung können entweder Szenarioanalysen oder Simulationsstudien angewandt werden. Bei Szenarioanalysen werden hypothetische Ereignisse konstruiert, die einen Sicherheitsvorfall zur Folge haben können. Man beschränkt sich auf die Erörterung von wichtigen Fallbeispielen. Im Gegensatz dazu bilden Simulationsstudien den Analysebereich detailgetreu nach und simulieren danach die Einwirkung von Gefahrenquellen. Sie sind wesentlich aufwendiger und erfordern die Unterstützung durch entsprechende Spezialprogramme wie ASIS von Siemens Nixdorf.[4]

2.1.2 Risikoanalyse

Die zweite Phase nach der Risikoerkennung ist die Risikoanalyse, durch die die objektive Risikolage ermittelt wird. Man kann die Risikoanalyse in die Teilbereiche Schwachstellenanalyse und die Gefahrenanalyse untergliedern. “Die Schwachstellenanalyse befaßt sich mit der gezielten und konsequenten Analyse und Beschreibung aller Mängel und Fehler innerhalb eines Rechnersystems.“ [5] Bezüglich Datenkommunikationssystemen ist eine Zweiteilung der möglichen Schwachstellenbereiche in technische und organisatorische Schwachstellen ausreichend. Nach organisatorischen Schwachstellen ist innerhalb der das System umhüllenden Aufbau- und Ablauforganisation zu suchen. Technische Schwachstellen können in der Architektur des Datennetzes und in der Implementierung seiner Funktionen festgestellt werden.[6] Die Gefahrenanalyse soll Gefahrenarten aufzeigen, die auf die Schwachstellen einwirken. Potentielle Risiken, die durch einen Internet-Zugang zu den bestehenden Gefahren

[4]vgl. Kyas, Sicherheit im Internet, S.22
[5]vgl. Wojcicki, Sichere Netze, S.25
[6]vgl. Wojcicki, Sichere Netze, S.26

hinzukommen sind das Eindringen von nichtautorisierten Personen in das Informationsnetzwerk. Mögliche Folgen könnten sein der Verlust von Daten oder vertraulichen Informationen, sowie die Störung der Netzverfügbarkeit beispielsweise durch Viren. Eine weitere Gefährdung besteht in der Vortäuschung falscher Identität (z.B. Adress Spoofing[7]). Letztlich wäre noch die Bedrohung durch das Einschleusen von "Trojanischen Pferden" und Viren durch Datenübertragung aus dem Internet auszufügen.[8] Die verschiedenen Risikofaktoren, die einkalkuliert werden sollten, wenn man an das Internet angeschlossen ist, werden im Verlauf dieser Arbeit belichtet. Zunächst soll aber über die dritte Phase der Risikoidentifikation, die Risikobewertung, ein Einblick über Folgen und Eintrittswahrscheinlichkeit von Sicherheitsschäden bedingt durch das Internet gegeben werden.

2.1.3 Risikobewertung

Im Verlauf der Risikobewertung werden den jeweiligen Risiken, aufbauend auf die Erfassung, Eintrittswahrscheinlichkeiten und Schadenspotentiale zugeordnet. Bei einer kardinalen Risikobewertung wird für jeden Sicherheitsvorfall die Höhe des Schadens (in Währungseinheiten) mit der Eintrittswahrscheinlichkeit pro Jahr multipliziert.

Das folgende Rechenbeispiel (Tab 1) soll die Methode verdeutlichen:

direkte und indirekte Folgeschäden des Datenverlusts	Ereigniseintritt	Berechnung	Risiko
DM 500.000,-	einmal in zehn Jahren	DM 500.000,- x 0,1 Jahre	DM 50.000,- / Jahr

Abb.: Tab 1

Generell ist zur kardinalen Risikobewertung festzuhalten, daß sie mit Hilfe von Tabellen und Kategorien, die auf Grundlage von Statistiken erstellt wurden, die Quantifizierung der jeweiligen Ergebnisse erleichtert. Die Ergebnisse täuschen jedoch eine Exaktheit vor, die in der Realität nicht gegeben ist. Im Vergleich dazu werden bei der

[7] mißbräuchliche Verwendung der eigenen Internet-Adresse durch dritte

ordinalen Risikobewertung die Informationssysteme zunächst in Objekte zerlegt, denen mit Hilfe von Listen und Matrizen Risiken zugeordnet werden. Die Risiken berechnet man im Gegensatz zur kardinalen Methode nicht, sondern man teilt sie in Kategorien wie Tragbarkeit oder Untragbarkeit, bzw. sehr wahrscheinlich bis hin zu sehr unwahrscheinlich ein.[9]

2.1.3.1 Detaillierte Bewertung

Unter Verwendung einer Risikomatrix läßt sich eine detaillierte ordinale Risikobewertung durchführen. Mit Hilfe dieser Matrix können konkrete Aussagen über das Sicherheitsrisiko eines Unternehmens getroffen werden. Potentielle Sicherheitsvorfälle werden darin in Abhängigkeit von den Parametern "Folgekosten" und "Eintrittswahrscheinlichkeit" angeführt. Die Eintrittswahrscheinlichkeit der jeweiligen Einbruchsszenarien ist von den eingesetzten Computer- und Netzwerksystemen, der bestehenden Infrastruktur (z.B. Internet-Anschluß) sowie den bestehenden Sicherheitsvorkehrungen (z.B. Firewalls) abhängig. Weitere Faktoren, die auf das "Sicherheitsgrundrisiko" Einfluß nehmen sind die Attraktivität des Unternehmens als Angriffsziel, die geographische Lage des Betriebs und die Größe bzw. die Anzahl der Mitarbeiter. [10] "Zweck der Risiko- oder Präferenzmatrix ist die Aggregation von Einzelmerkmalen, die ordinal skaliert sind, zu abstrakten Merkmalen."[11] Dies muß durch logische Kombination, sogenannte "Boole`sche Algebra", erfolgen, da eine arithmetische Aggregation bei Ordinalskalen nicht zulässig ist. Im Rahmen der Boole`schen Allgebra werden Wenn-dann- Aussagen nach dem Muster: "WENN Merkmal A den Wert 1 hat und B den Wert 1, DANN wird der aggregierte Wert 1 zugeordnet."[12]
Die einfache Risikomatrix verknüpft zwei Merkmale. Folgende Abbildung[13] zeigt die theoretische Vorgehensweise bei jeweils dreistufig klassifizierten Merkmalen:[14]

n1

[8]vgl. Kyas, Sicherheit im Internet, S.21
[9]vgl. Kyas, Sicherheit im Internet, S.23
[10]vgl. Kyas, Sicherheit im Internet, S.27
[11]URL am 22.12.1998, http://www.laum.uni-hannover.de/ilr/lehre/Ptm/Ptm_BewMatrix.htm
[12]vgl. URL am 22.12.1998, http://www.laum.uni-hannover.de/ilr/lehre/Ptm/Ptm_BewMatrix.htm
[13]URL am 22.12.1998, http://www.laum.uni-hannover.de/ilr/lehre/Ptm/Ptm_BewMatrix.htm
[14]vgl. URL am 22.12.1998, http://www.laum.uni-hannover.de/ilr/lehre/Ptm/Ptm_BewMatrix.htm

		1	2	3
n2	1	1	2	2
	2	2	2	3
	3	2	3	3

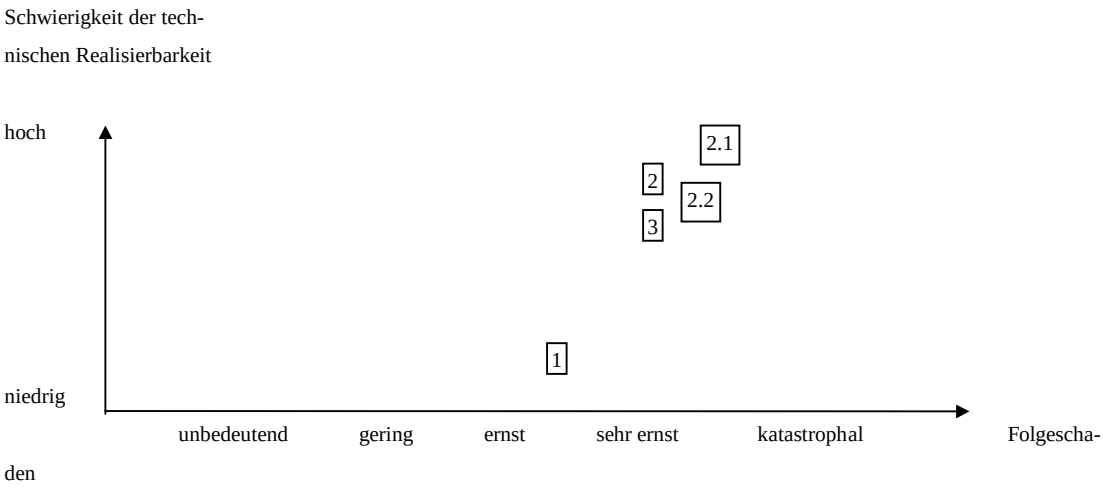
“Die Matrix ist wie folgt zu lesen: WENN Merkmal n1 den Wert 1 hat und Merkmal n2 den Wert 1, DANN ergibt sich für das aggregierte Merkmal N der Wert 1. WENN Merkmal n1 den Wert 1 hat UND Merkmal n2 den Wert 3, DANN ergibt sich für das aggregierte Merkmal der Wert 2. ACHTUNG! Dies wurde nicht als arithmetisches Mittel (1+3/2=2) errechnet, sondern aus der Matrix abgelesen.“[15]

Hat Merkmal n1 den Wert 1 UND Merkmal n2 den Wert 2, DANN ergibt sich für das aggregierte Merkmal N der Wert 2. Das Ergebnis 1,5 wäre falsch, da es einer Kardinalskalierung entspricht. Ob die Kombination 1 UND 2 in der Aggregation 1 oder 2 ergibt, ist keine Frage der Mathematik, sondern eine Wertsetzung. Seine beispielsweise 1 eine gute und 3 eine schlechte Ausprägung, dann bedeutet die Aggregation von 1 UND 2 zu 2, daß dem Vorsorgeprinzip gefolgt wird und im Zweifel aufgrund der Unsicherheit über Auswirkungen vorsichtig vorangegangen wird (im Zweifel für eine Sicherheitsmaßnahme). Im Gegensatz dazu steht die Aggregation von 1 UND 2 zu 1 eher für eine Orientierung an der Gefahrenabwehr (im Zweifel gegen eine Sicherheitsmaßnahme).[16]

“Bei der Aufstellung der Matrix werden zunächst die Eckwerte besetzt (im Beispiel 1 UND 1 ergibt 1, 3 UND 3 ergibt 3, 1 UND 3 ergibt 2, 3 UND 1 ergibt 2). Weitere Wertepaare können durch Kenntnis von Kausalzusammenhängen, also indikativ, besetzt werden, wenn solche Kausalzusammenhänge bekannt sind. Ansonsten (und das ist in der Praxis die Regel) ist normativ vorzugehen (siehe oben). Bei einer großen Risikomatrix schlagen Boese et al. (1981, 50f.) vor, die verbleibenden Werte durch lineare Interpolation zwischen den bekannten bzw. den gesetzten Werten zu gewinnen. Die Präferenzmatrix ist eine Operationalisierung des Paarvergleichs, der intuitives menschliches Bewerten zugrunde liegt. Der Paarvergleich wird im obigem Schema in 3x3=9 Regeln aufgelöst.“[17]

[15]vgl. URL am 22.12.1998, http://www.laum.uni-hannover.de/ilr/lehre/Ptm/Ptm_BewMatrix.htm
[16]vgl. URL am 22.12.1998, http://www.laum.uni-hannover.de/ilr/lehre/Ptm/Ptm_BewMatrix.htm
[17]URL am 22.12.1998, http://www.laum.uni-hannover.de/ilr/lehre/Ptm/Ptm_BewMatrix.htm

Die Risikomatrix wird in der Praxis auf ein bestimmtes Unternehmen konzipiert. Eine Vorgehensweise könnte folgendermaßen aussehen:
Als Ausgangspunkt der Analyse werden zuerst sämtliche Angriffsmöglichkeiten aufgelistet und der Schwierigkeitsgrad für deren Durchführung bewertet. Um eine exakte Beurteilung erstellen zu können, müssen sämtliche Angriffsmöglichkeiten berücksichtigt werden (Oft ist eine Untergliederung der Punkte erforderlich). Ein Ausschnitt der Lösung durch ein Koordinatensystem sieht wie folgt aus:



Legende:

1 = Einschleusen von Viren
2 = Angriff auf Kommunikationsprotokolle
2.1 = TCP-Sequenzummernraten
2.2 = Routing Angriff
3 = Überwindung von Authentifikationssystemen

Ist das Koordinatensystem fertiggestellt, dann können daraus Risikofaktoren abgeleitet werden, mit Hilfe deren dann die aus den unterschiedlichen Angriffsformen resultierenden Sicherheitsvorfälle nach dem beschriebenem Konzept in die Risikomatrix eingetragen werden können. Dabei gilt, je schwieriger die technische Reali-

sierbarkeit eines Angriffs ist, desto geringer ist die Wahrscheinlichkeit eines erfolgreichen Eindringens.[18]

Eine Bewertung bzw. die Ableitung von Maßnahmen aus den Ergebnissen der Risikobetrachtung kann durch die folgende Tabelle (Tab 2)[19] vorgenommen werden:

Folgekosten

katastrophal	2	2	1	1	1
sehr ernst	2	2	2	1	1
ernst	3	2	2	2	1
gering	3	3	3	2	2
unbedeutend	3	3	3	2	2
	sehr gering	gering	mittel	hoch	sehr hoch

Eintrittswahrscheinlichkeit

Abb.: Tab 2

Legende:

1= Mit höchster Priorität behandeln
2= Mit mittlerer Priorität behandeln
3= Nicht oder bei Gelegenheit behandeln

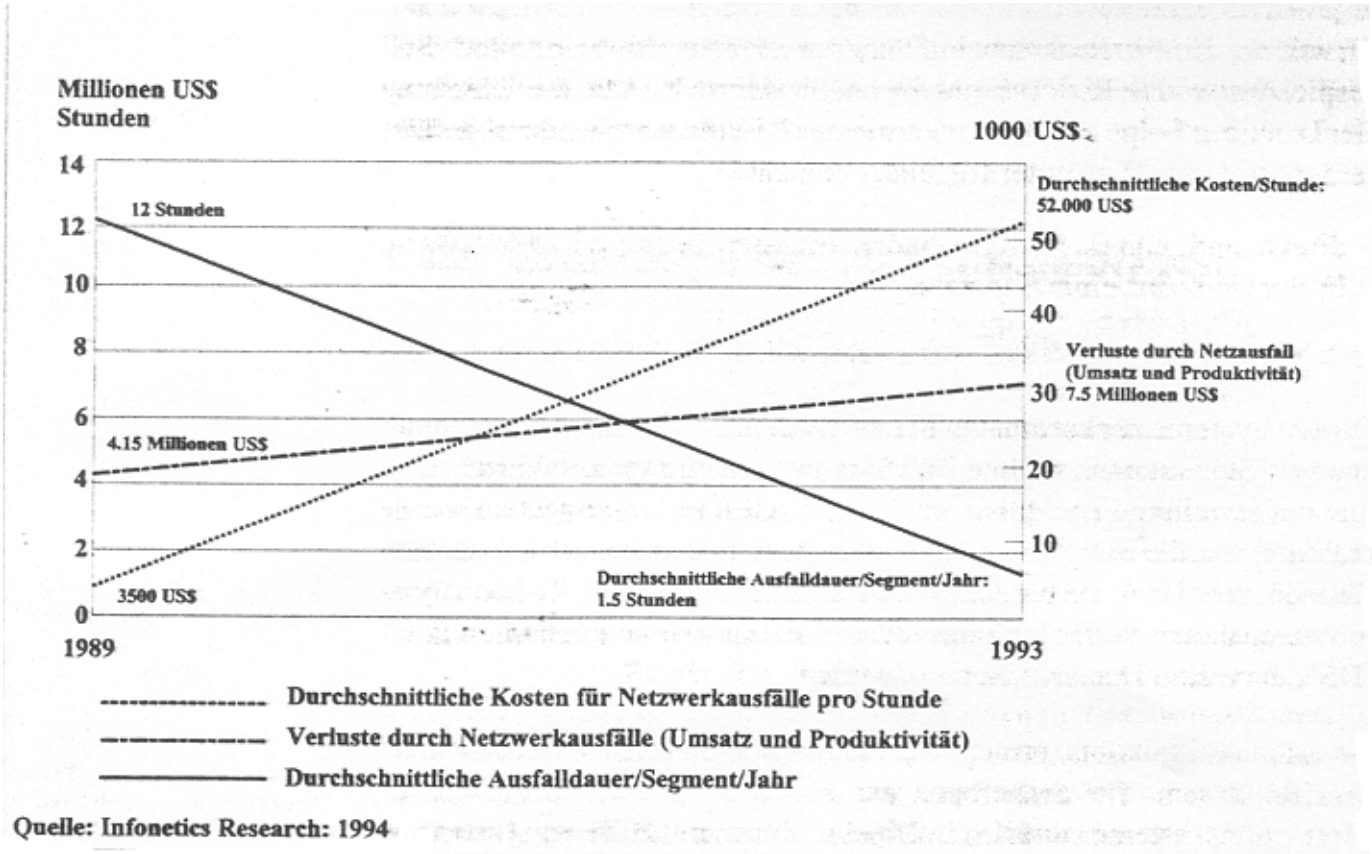
Basierend auf der Aussage, die aufgrund des Ausschnitts aus dem Koordinatensystems und der Handlungsempfehlung (Tab 2) getroffen werden kann, sollten die Präferenzen der Matrix so gewählt werden, daß im Fall von unklaren Werten z.B. bei hoher Eintrittswahrscheinlichkeit und sehr ernsten Folgeschäden der aggregierte Wert eine sofortige Sicherheitsmaßnahme befürwortet. Gibt es beispielsweise einen

[18]vgl. Kyas, Sicherheit im Internet, S.29
[19]Kyas, Sicherheit im Internet, S.27

unklaren Wert bei niedriger Eintrittswahrscheinlichkeit und geringen Folgeschäden, so sollten durch die Präferenzen der Matrix eine Sicherheitsmaßnahme nicht unbedingt empfohlen werden.

2.1.3.2 Netzwerkprobleme und der Verlust von Datenintegrität

Die folgende Grafik[20] zeigt die Entwicklung der Netzausfallkosten von 1989 -1993.



Betrachet man die Grafik, so erkennt man, daß die duchschnittlichen Kosten für einen Netzwerkausfall zwischen 1983 und 1993 von 3500 US$ auf 52000US$/Stunde angestiegen sind. Auch bei den Verlusten durch Netzwerkausfälle bezüglich Umsatz

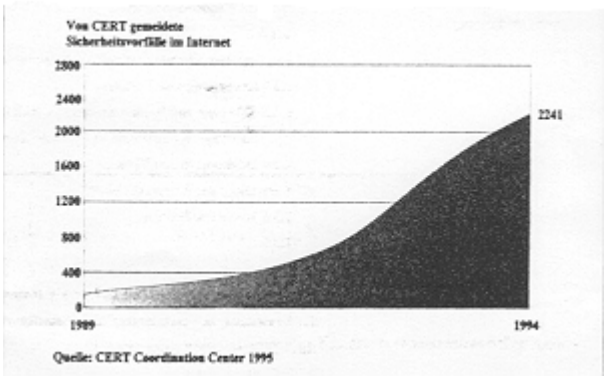
[20]Kyas, Sicherheit im Internet, S.24

und Produktivität läßt sich eine steigende Tendenz erkennen. In einem Zeitraum von vier Jahren stiegen die Verluste von 4,15 Millionen US$ auf 7,5 Millionen US$. Diese Statistik belegt, daß es Ziel eines jeden Unternehmens sein muß, das Netzwerk zu schützen. In der folgenden Bewertung soll vedeutlicht werden, daß Sicherheitsmaßnahmen vor allem in Verbindung mit Internet-Aktivitäten getroffen werden müssen.[21]

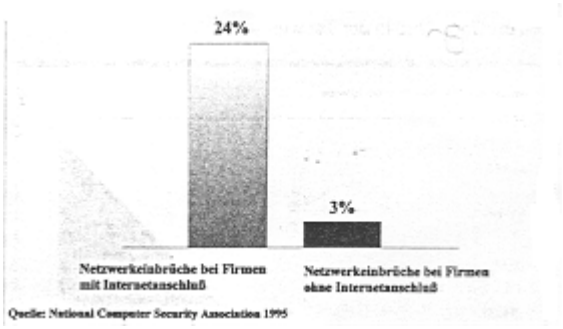
2.1.3.3 Eintrittswahrscheinlichkeit

Die unten angeführten Grafiken geben Aufschluß über die Eintrittswahrscheinlichkeit eines Einbruchs in Computer-Systeme über das Internet.

Grafik 2.3.2.1 [22]



Grafik 2.3.2.2 [23]



Grafik 2.3.2.1 zeigt die Anzahl der gemeldeten Sicherheitsvorfälle im Internet von 1989-1994. Aus der Grafik des Computer Emergency Response Team[24] ist ersichtlich, daß die Vorfälle rasant von 132 auf 2241 gestiegen sind, wobei die Zahl der betroffenen Netzwerke bei mehr als 40000 lag. Nach einer Schätzung des Nationalen Zentrums für Computerkriminalität liegt die Dunkelziffer um ein vielfaches darüber,

[21]vgl. Kyas, Sicherheit im Internet, S.24
[22]Kyas, Sicherheit im Internet, S.25
[23]Kyas, Sicherheit im Internet, S.20
[24]CERT (Organisation für Sicherheit im Internet)

da nur ein Prozent aller Computerdelikte entdeckt wird und davon lediglich 14% zur Anzeige gelangen.[25] Grafik 2.3.2.2 verdeutlicht, daß hauptsächlich Firmen mit Internetanschluß von Netzwerkeinbrüchen betroffen sind. Die Abbildung basiert auf einer Untersuchung der National Computer Security Association vom Mai 1995, nach der Firmen mit Internet-Zugang im Durchschnitt acht mal so häufig Angriffen auf interne Datennetze ausgesetzt sind, wie vergleichbare Unternehmen ohne Internetanschluß.[26]

2.2 Risikohandhabung

Die Erkenntnisse, die im Prozeß der Risikoidentifikation gewonnen wurden, werden nun in der Risikohandhabung verwertet. Es wird abgewogen, ob es ökonomisch sinnvoll ist, diversen Risiken vorzubeugen. Gegebenenfalls wird ein Reaktionsplan erstellt.

3 Zusammenfassung von Sicherheitsrisiken und Gegenmaßnahmen

Die Gefahren des Internet sind vielfältig. Nicht nur Unternehmen werden durch Computer-Mißbrauch in Mitleidenschaft gezogen, sondern auch der private Internet Nutzer muß gegen mögliche Gefahren geschützt sein, um der Computer-Kriminalität vorzubeugen. Die folgenden Punkte geben eine Übersicht von Sicherheitsrisiken und möglichen Gegenmaßnahmen.

3.1 Zugangsberechtigung

Die Zugangsberechtigung ist ein wichtiger Teil von Zugangskontrollsystemen. Diese Systeme haben drei Hauptaufgaben, nämlich die Identifikation, die Legitimierung und die Ermächtigung des Benutzers. Die Identifikation durchwandert der Nutzer, in dem er sein persönliches Login eingibt. Es ist im Normalfall nicht geheim und entspricht einem persönlichem Pseudonym wie dem Familiennamen. In Verbindung mit

[25]vgl. Kyas, Sicherheit im Internet, S.25
[26]vgl. Kyas, Sicherheit im Internet, S.20

dem Login wird das Paßwort des Nutzers abgefragt. Über das geheime Paßwort prüft das System, ob die angemeldete Person zugangsberechtigt ist. Stimmen Paßwort und Login überein, so erhält der Nutzer im letzten Schritt die Ermächtigung, die Programme und Dateien zu verwenden, die für seinen Zugang freigeschaltet wurden.[27] Die Legitimierung wird auch durch andere Mechanismen geprüft (z.B. Stimmenkontrolle). Das Paßwort ist aber der am meisten genutzte Identifikationsmechanismus. Die meisten Systemeinbrüche erfolgen durch Paßwortangriffe, die ein Versagen des Mechanismus für die Zugangsberechtigung hervorrufen. Um Paßwörter zu entschlüsseln werden von den Angreifern unterschiedliche Strategien[28] angewandt:

Erraten des Paßworts

→ trivialste und einfachste Methode

Systematisches Paßwortraten mit Hilfe der Paßwortdatei "passwd"

→ Versuch in Besitz der Datei "passwd" zu gelangen

→ Erfolgt mit Rateprogrammen (z.B. Cracker Jack), die in kurzer Zeit einen Teil der Paßwörter enttarnen

Protokollanalyse mit Paßwortfilterung (Sniffer Angriff)

→ Nutzung der Netzstation als "verräterisches" Analysesytem durch Einschleusung bzw. Aktivierung diverser Protokollanalyseprogramme (z.B. etherfind)

Login/Paßwort-Monitoring durch TSR-Programme und Trojanischen Pferde

→ Installation von TSR-Programmen bzw. Trojanischen Pferden um in den Besitz von Passwörtern zu gelangen

Um die Sicherheit des Gesamtsystems zu erhöhen, sollten für das Paßwort des Nutzers folgende Eigenschaften[29] gelten:

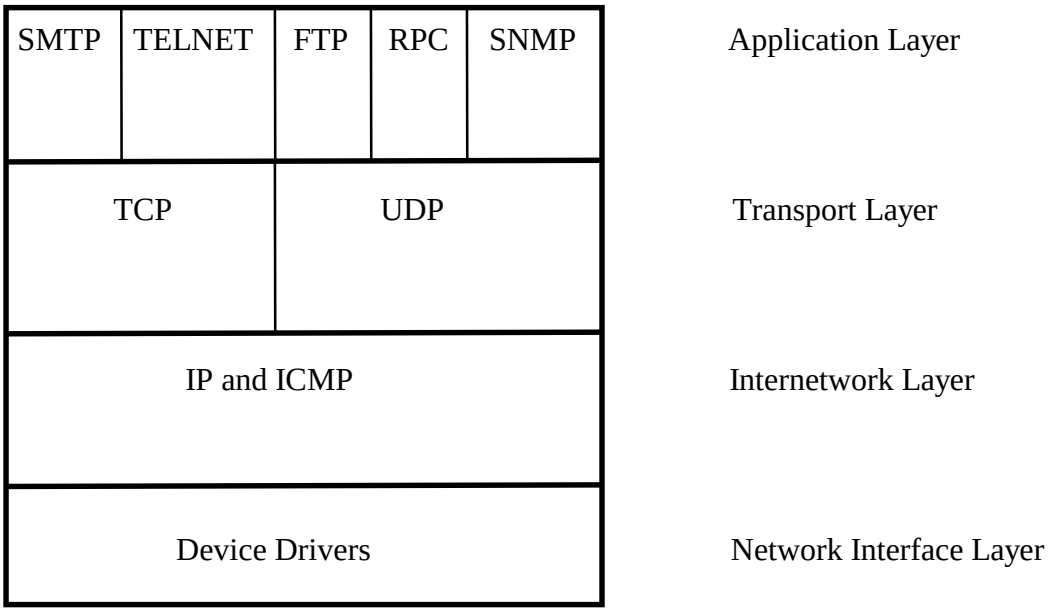
- Das Paßwort sollte alle drei bis sechs Monate geändert werden
- Das Paßwort sollte sowohl Groß- als auch Kleinbuchstaben beinhalten

[27] vgl. Lobel, Foiling the System Breakers, S.111
[28] vgl. Kyas Sicherheit im Internet, S.48ff
[29] vgl. Kyas, Sicherheit im Internet, S.52ff

- Das Paßwort sollte eine mindestlänge von acht Zeichen haben
- Es sollte selbst mit umfangreichen Wortbibliotheken nicht zu erraten sein
- Das Paßwort sollte gut geschützt am Zielsystem gespeichert sein- eventuell Abkürzungen erfinden (z.B. low2basN = I only want to be a small number)

3.2 Kommunikationsprotokolle

Die Rechner kommunizieren im Internet über das TCP/IP Protokoll.[30] Es ist naheliegend, daß sie als eigentliche Elemente des Transportmechanismus Ziel der Angriffe von Hackern sind. TCP steht für *Transport Control Protocol*, IP für *Internet Protocol*. TCP/IP ist eine Kombination von Netzwerkprotokollen und Applikationen, die durch die folgende Grafik[31] veranschaulicht werden soll.



Für die unterste Schicht (Netzwerk Schnittstellen Schicht) läßt sich kein einzelnes TCP/IP Protokoll spezifizieren. TCP/IP ermöglicht aber den Gebrauch von fast allen Netzwerkschnittstellen wie z.B. Token Ring, Ethernet oder X.25. Die "Internetwork"-Schicht besteht aus *Internet Protocol* (IP) und *Internet Control Message Pro-*

[30] vgl. Buhl, Wirtschaftsinformatik II, Folie EC 1.24
[31] Ahuja, Network and Internet Security, S.208/209

tocol (ICMP). Während die Kommunikation über die Netzwerk- Schnittstellen-Schicht durch physikalische Adressen erfolgt, werden bei allen höheren Ebenen IP-Adressen verwendet. Die Transportschicht besteht aus den auf IP aufsetzenden verbindungsorientierten (TCP) und verbindungslosen (*User Datagram Protocol* -UDP) Protokollen. Verbindungsorientierte Protokolle (TCP) garantieren die Übertragung von Daten im Rahmen einer virtuellen Verbindung im Gegensatz zu Verbindungslosen Protokollen, wie UDP oder IP, deren Übertragung verbindungslos ist und nicht garantiert wird. Oberste Ebene ist die der Applikationen und der höher geschichteten Protokolle die TCP/IP verwenden (u.a. FTP-File Transfer Protocol).[32]
TCP/IP-Angriffe[33] können auf sämtlichen Schichten erfolgen. Im wesentlichen handelt es sich dabei um:

Internet Adress Spoofing

→ Erzeugen von synthtetischen Datenpaketen mit gefälschter IP-Sendeadresse, die das Paket einer internen Station vortäuschen

TCP-Sequenznummern-Angriff

→ Angriff während des TCP-Verbindungsaufbaus, der Adress Spoofing voraussetzt

ICMP-Angriffe

→ Versenden von manipulierten, künstlich erzeugten ICMP-Paketen

→ Beeinträchtigung der Funktionsfähigkeit des Netzes

→ Veränderung der Vermittlungspfade mit darauffolgendem Systemeinbruch

Internet-Routing-Angriffe

→ Durch Simulation der IP-Adresse eines internen Systems stehen dem Eindringling alle Möglichkeiten dieses Systems zur Verfügung

Um sich speziell vor solchen Attacken zu schützen, können folgende Maßnahmen[34] hilfreich sein:

[32]vgl. Ahuja, Network and Internet Security, S.209ff.
[33]vgl. Kyas, Sicherheit im Internet, S.64ff
[34]vgl. Ahuja, Network and Internet Security, S.218/219

1. **Datenintegrität** zum Schutz von FTP oder E-Mail-Files bei der Übertragung im Internet. (→Sicherheit, daß Daten unverändert übertragen werden)
2. Inanspruchnahme eines Gateways, um Nachrichten, die über das Internet gesendet werden zu untersuchen oder eventuell abzufangen. Diese Gateways, sogenannte **Firewalls,** legalisieren die Quellen der Nachrichten, indem sie Pakete herausfiltern, die auf IP-Adressen basieren.
3. Einrichten eines **Zugangskontrollsystems**
4. Verschlüsselung der Dateien durch einen **Chiffrierschlüssel**

3.3 Sicherheitsrisiken durch Informationsdienste

Ziel von Informationsdiensten ist es, einen einheitlichen Informationszugriff in heterogen verteilten Systemen zu ermöglichen. Der wohl bekannteste Anwenderdienst ist das World Wide Web (WWW). Es ist ein multimediales, interaktives Hypertextinformationssystem, daß Informationen über Hyperlinks verknüpft.[35] Der Server stellt WWW-Seiten als Hypertext Markup Language[36] Dokument bereit. Der Client ruft Seiten ab, lädt sie, arbeitet sie zur grafischen Bilddarstellung auf und zeigt sie dem Benutzer an.[37] Zum Transport zwischen WWW-Clients und -Servern wird das Protokoll HTTP[38] benutzt. Die angebotenen Daten umfassen alles von Texten und Dokumenten über Bücher, Audio und Bilder bis hin zu Video. Weder das Hypertext Transport Protocol noch die Seitenbeschreibungssprache HTML enthalten besondere Mechanismen, die WWW-Server gegen Angriffe schützen. Es besteht die Gefahr sogenannter Common Gateway Interface (CGI) Angriffe. CGI ist verantwortlich für die Kommunikation zwischen WWW-Server und den entsprechenden Programmen. Variablen und Daten werden vom WWW-Server an die Programme übergeben. Die Ergebnisse der Verarbeitung durch die Programme werden wieder an den Server weitergeleitet. Angreifer versuchen diesen Prozeß für ihre Zwecke zu manipulieren.

[35]vgl. Buhl, Wirtschaftsinformatik II, Folie EC 1.27
[36]HTML
[37]vgl. Buhl, Wirtschaftsinformatik II, Folie EC 1.28

Seit kurzer Zeit erst sind mit Kryptographie- und Authentifikationsmechanismen versehene Protokolle verfügbar, die die sichere Übertragung von HTML und anderen Internet-Applikationsprotokollen ermöglichen. Als Beispiel seien Secure Socket Layer (SSL), Shen und S-HTTP genannt.[39]

SSL und Shen funktionieren ähnlich, da aber Shen wenig verbreitet ist soll kurz die Arbeitsweise des Secure Socket Layers erklärt werden. SSL setzt auf TCP/IP auf und ist in der Lage, alle im Internet gebräuchlichen Applikationsprotokolle wie HTTP (WWW), Telnet, Gopher und NNTP sicher zu übertragen. [40] WWW-Clients wie der Netscape Navigator und der Microsoft Internet Explorer unterstützen seit Version 2.0 den Secure Socket Layer, so daß dieses Sicherheitsprotokoll bereits eine enorme Verbreitung im Netz besitzt. Eine mittels SSL abgesicherte WWW- Seite kann anhand der Adresse HTTPS://... anstelle von HTTTP://... sowie dem auf der linken unteren Ecke eingeblendeten Schlüssel erkannt werden. Zum Betreiben des eigenen WWW-Servers mit SSL - gesicherten Dokumenten ist neben der entsprechenden Serversoftware (z.B. Netscape Commerce Server) die Zertifizierung des eigenen Servers bei der Zertifizierungsstelle (RSA Certificate Services für Netscape Server) erforderlich. [41] Der Unterschied zwischen dem SSL und dem S-HTTP Protokoll besteht darin, daß SSL ein Vermittlungsprotokoll erstellt, um eine sichere Verbindung zur Anschlußebene zu gewährleisten. S-HTTP Protokolle dagegen sind im HTTP-Protokoll integriert. Sicherheit wird über sogenannte Header und Zeichen, mit denen die Seite ergänzt wird, gewährleistet.[42]

Nach diesem kurzen Überblick über mögliche Sicherheitsrisiken und Maßnahmen der Vorbeugung soll nun eines der größten Sicherheitsprobleme im Internet, der Befall durch Viren, diskutiert werden.

4 Virenproblematik

[38]HTTP
[39]vgl. Kyas, Sicherheit im Internet, S.105ff
[40]vgl. Kyas, Sicherheit im Internet, S.105/106
[41]vgl. Kyas, Sicherheit im Internet, S.106
[42]vgl. Ahuja, Network and Internet Security, S.245

Mit dem rasanten Wachstum des Internet hat auch die Verbreitung von Viren neue Dimensionen angenommen. 1989 waren 15 von ihnen bekannt, 1990 ca. 100, im Jahr 1995 1500 und heute sind es weltweit ca. 20000. Ein Ende dieser Entwicklung ist nicht in Sicht. Weiterhin werden jedes Monat 300-350 neue Varianten gemeldet.[43]
Das provisorische Schutzmaßnahmen nicht ausreichend sind, um effizienten Schutz gegen Viren zu gewährleisten, wird in den nächsten Abschnitten ersichtlich.

4.1 Definition der Computer Anomalien 2.Art

Viren gehören neben Würmern und trojanischen Pferden zu den Computer-Anomalien 2.Art. Sie unterscheiden sich nach der Art der Ausbreitung, dem Ortsverhalten und der Eigenschaft selbständig zu sein. [44]

Die folgende Tabelle soll eine Übersicht der wesentlichen Merkmale geben.

	selbständig	ortsfest	Vermehrung
trojanisches Pferd	X	X	-
Wurm	X	-	X
Virus	-	X	X

Quelle: H.Brobeil , Software-Andriffe auf PC`s und Netzwerke, 1991

Weitere Charakteristika der Computer-Anomalien 2.Art sind den angeführten Definitionen zu entnehmen.

4.1.1 Viren

“Als Computervirus bezeichnet man eine Befehlsfolge, deren Ausführung bewirkt, daß eine Kopie oder eine weiterentwickelte Version ihrer selbst in einem Speicherbe-

[43]vgl. Enskat, Hochschul-Anzeiger/Nr.40, S.20

reich, der diese Sequenz nicht enthält, reproduziert wird. Diesen Vorgang bezeichnet man als Infizierung. Die Befehlsfolge kann neben dieser Minimalanforderung der Reproduzierbarkeit auch noch beliebige weitere Funktionen bewirken.“[45]

Viren sind demnach Programmstücke, deren Ausführung nach sich zieht, daß sie sich selbst als Ganzes oder in modifizierter Form ihrer selbst in ein anderes Programm kopieren.[46] Computer-Viren benutzen den Rechner als Wirt (→ortsfest). Der Benutzer ermöglicht ohne es zu wissen die Verbreitung der Viren, indem er sein System benutzt.[47]

Ein Virus kann aus folgenden Elementen bestehen:[48]

1. Kennung

→ ermöglicht es dem Virus festzustellen, ob eine bestimmte Datei bereits von ihm infiziert wurde

2. Infektionsteil

→ Implementation des Virus in ein anderes Programm

3. Schadensfunktion

→ Programmstück, indem der Virus seine Wirkung entfaltet

4. Ereignissteuerung

→ Gewährleistet ungestörte Ausbreitung des Virus

5. Aufruf des Wirtsprogramms

→ Um unentdeckt zu bleiben wird nach Abarbeitung des Virencodes wieder zum ursprünglichen Code des Wirtsprogrammes verzweigt.

[44]vgl. Brobeil, Software-Angriffe auf PC`s und Netzwerke, S.49
[45]Gleissner, Manipulation in Rechnern und Netzen, S.32
[46]vgl. Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.55
[47]vgl. Slade, Slade´s Guide to computer viruses, S.187
[48]vgl. Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.55/56

Ein Virus muß nicht alle Teile besitzen, essentiell sind lediglich Infektionsteil und Schadensfunktion.[49]

4.1.2 Trojanische Pferde

"Unter einem trojanischen Pferd versteht man ein Programm, das einerseits die spezifizierte Funktion ausführt, andererseits aber unzulässige und vom Manipulateur beabsichtigte Nebenwirkungen hat."[50]
Die Erkennung dieser Anomalie wird erschwert, da es sich bei trojanischen Pferden um selbständige, ortsfeste Programme handelt. Der Benutzer wird getäuscht, indem er ein Programm startet, das offensichtlich seinen Anforderungen entspricht. Die gewünschte Leistung wird jedoch nur vorgetäuscht, bzw. das funktionelle Codestück in Form eines korrekten Programms enthält eine nicht dokumentierte Routine, die eine unerwartete Zusatzfunktion (den trojanischen Teil) ausführt. Meistens haben trojanische Pferde Namen, welche die Neugier des Benutzers wecken, wie sexylady, log-in.neu, info.sys. Ebenso können sie Namen gängiger Kommandos (z.B. DIR, DEL) oder von Anwendungsprogrammen tragen (z.B. von Spielen).[51]

4.1.3 Würmer

"Ein Wurmsegment ist ein lauffähiges Programm (oder eine Ansammlung von lauffähigen Programmen und Dateien), das in der Lage ist, sich -über ein Netzwerk auch in andere Rechner- zu vervielfältigen. Dies geschieht selbstgesteuert in Kommunikation mit anderen Segmenten. Ein Wurm ist die Vereinigung aller seiner Segmente."[52]
Würmer sind ortsunabhängig und treten bevorzugt in vernetzten Systemen auf, in die sie durch Systemfehler oder Sicherheitslücken eindringen können. Als eigenständige Programme, die sich im Arbeitsspeicher fortbewegen, attackieren sie Computersysteme direkt. Würmer erzeugen Prozesse und versuchen illegale Aktivitäten auszu-

[49]vgl. Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.55
[50]Gleissner, Manipulation in Rechnern und Netzen, S.17
[51]vgl. Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.49/50
[52]Gleissner, Manipulation in Rechnern und Netzen, S.23

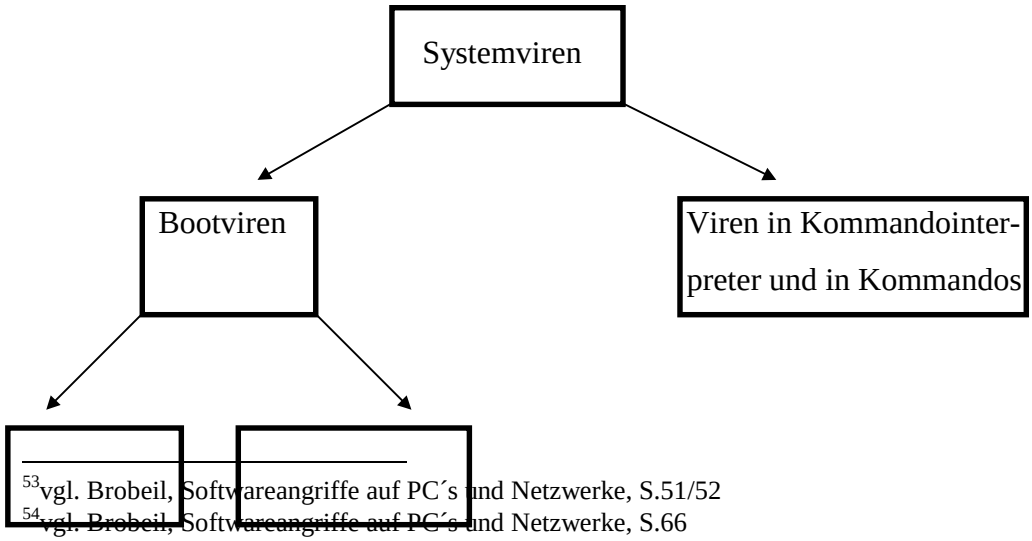
führen. Zur Verbreitung nutzen sie auch Mechanismen, die über das Netz bereitgestellt werden. Charakteristisch für einen Wurm ist, daß er explizit aufgerufen werden muß.[53] Anhand von Standardbeispielen soll das vermittelte Wissen bezüglich der Computeranomalien 2.Art nun vertieft werden.

4.2 Funktions- und Wirkungsweise von Computeranomalien 2.Art

Die Vielfalt von Computeranomalien darf bei der Erläuterung der Funktions-und Wirkungsweise nicht irritieren, weil die überwiegende Zahl der verschiedenen Anomalien lediglich Varianten von bereits bekannten Typen sind. Aus diesem Grund lassen sich die Virenkategorien sehr gut an Standardbeispielen erklären.
Im Rahmen dieser Arbeit werden Beispiele erwähnt, um die wichtigsten Kategorien, Systemviren, trojanische Pferde und Würmer bezüglich ihrer Funktionsweise und Wirkung zu erläutern.

4.2.1 Systemviren

Um zu veranschaulichen, wo sich Viren einnisten und wie sie funktionieren, werden unter diesem Gliederungspunkt einige Arten von Systemviren besprochen. Wie sich Systemviren unterteilen lassen soll durch folgende Grafik veranschaulicht werden.[54]



[53] vgl. Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.51/52
[54] vgl. Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.66

Bootsektor-viren Partitionsektor-viren

Systemviren lassen sich nach Bootviren bzw. Viren in Kommandointerpreter und in Kommandos unterteilen. In der nachfolgenden Ausführung wird die Kategorie Bootviren in Bootsektorviren und Partitionsektorviren unterteilt.

4.2.1.1 Bootsektor Viren

Bootsektorviren schreiben sich vor das eigentliche Bootsektorprogramm[55]. Fährt man das System hoch, dann wird der Virusprogrammteil vor dem Bootsektor Programm des Rechners ausgeführt.[56] Der Ablauf läßt sich folgendermaßen darstellen. Der Computer prüft zuerst, ob sich eine Diskette für den Boot[57]-Vorgang in Laufwerk A befindet. Ist das nicht der Fall, liest er von Laufwerk C (Festplatte). Während dieses Prozesses wird der Bootsektorvirus implementiert. Er setzt seinen Code an den Platz des eigentlichen Programms und lagert dieses an einer beliebigen Stelle des Speichermediums.[58] Ein Virus, der auf diese Weise funktioniert, ist der Italian.[59]
Seine Verbreitung wird ermöglicht, indem eine infizierte Diskette beim herunterfahren des Systems im Diskettenlaufwerk bleibt. Um den Virus zu implementieren muß die Diskette nicht unbedingt eine Boot-Diskette sein. Wird das System das nächste mal hochgefahren, erscheint die Nachricht: “Keine System Diskette. Bitte legen sie eine Systemdiskette ein und versuchen sie es erneut.“ Der Virus befindet sich jetzt bereits im Speicher und bleibt dort, auch wenn der Startvorgang über ein anderes Speichermedium (Festplatte) fortgeführt wird. Jede Diskette, mit der gearbeitet wird, sowie die Festplatte werden nun mit dem Italian infiziert. Der Virus setzt seinen Code an die Stelle des üblichen Startsektors und schiebt diesen an eine andere Stelle des Speichermediums. Befallene Disketten verlieren 1K Speicher an den implementierten Italian, die Festplatte 2K. Dieser Vorgang wiederholt sich bei jedem Neustart,

[55]Bootsektorprogramme laden bestimmte Betriebssystemkonfiguration
[56]vgl.Gleissner, Manipulation in Rechnern und Netzen, S.37ff.
[57]Boot=Start
[58]vgl. Enskat, Hochschul-Anzeiger/Nr.40, S.20
[59]wird auch Ping Pong oder Bouncing Ball genannt

bis das gesamte System langsam und unauffällig lahmgelegt worden ist.[60] Diese Aussage soll jedoch nicht mißverstanden werden. Der Bootsektor Virus infiziert nur das Bootsektor Programm (der Diskette / Festplatte), nicht das ganze System. Weil aber die Betriebssystemkonfiguration durch das Bootsektor Programm geladen wird, ist es der Schlüssel für ein funktionierenden Rechner.
Das Internet kann übertragendes oder weiterleitendes Medium von Bootviren sein, zu denen auch Partitionsektorviren gehören. Die ähnliche Arbeitsweise wird nachfolgend dargestellt..

4.2.1.2 Partitionsektor Viren

“Der physikalisch erste Sektor einer Festplatte ist bei PC´s für den partition record reserviert, der Informationen über die Partitionierung der Festplatte und den Code für einen Kaltstart enthält. Dieser ist nicht identisch mit dem Bootsektor, der sich auf dem logisch ersten Sektor der Festplatte befindet. Bei Disketten entspricht der physikalisch erste Sektor dem logisch ersten. Der Stoned- oder Marihuana Virus legt seinen Code in diesem Bereich ab.“[61]
Die Implementierung und der Kopiervorgang des Stoned entsprechen dem des Italian. Einziger Unterschied ist, daß der Marihuana Virus auch in den Partitionsektor der Festplatte geschrieben wird. Wird eine Diskette infiziert, ist der Prozeß exakt der gleiche wie bei Bootsektorviren, weil bei Disketten der physikalisch erste Sektor dem logisch ersten entspricht.[62] Ebenso wie Bootviren nisten sich auch Systemviren in Kommandos und im Kommandointerpreter sehr früh in das System ein. Ein Beispiel für sogenannte File-Viren ist der Vienna Virus.

4.2.1.3 Systemviren in Kommandos und im Kommandointerpreter

Diese Viren infizieren Kommandoroutinen oder den Kommandointerpreter. (unter MS-DOS COMMAND COM, der für die Interpretation eingegebener Betriebssystemkommandos wie DIR, CD, EDLIN, RENAME oder Copy verantwortlich ist.)

[60]vgl. Solomon, PC viruses, S56/57
[61]Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.67
[62]vgl. Solomon, PC viruses, S59/60

Wird ein DOS-Kommando ausgeführt, so kommt es zur Aktivierung des Virus und er kann seine Schadensfunktion ausführen.[63]
Ist ein System z.B. mit dem Vienna Virus infiziert, wirkt sich das folgendermaßen aus; Bei jedem Aufruf eines infizierten Files sucht der Virus auf dem aktuellen Pfad nach dem nächsten File, das noch nicht befallen ist. Der Austrian[64] wird kopiert, sofern es sich bei dem File um kein EXE. File handelt. Ist zum Beispiel der Kommandointerpreter COMMAND.COM befallen, so wird der Computer bei jedem Hochfahren des Systems nicht aufhören, sich immer wieder zu "booten". Bei der "Eingabevariante" des Virus ist es für den Benutzer unmöglich, weitere Befehle an den Rechner zu geben. Das System "hängt". [65]

4.2.2 Trojanische Pferde

Trojanische Pferde sind ein Teil der Virenproblematik, obwohl es falsch wäre, sie als Viren zu definieren. Der Grund dafür ist offensichtlich. Genau wie ein Virus hinterläßt das trojanische Pferd seinen Code auf jeder infizierten Festplatte bzw. Diskette. Unterschiede bestehen jedoch hinsichtlich der Funktionsweise sowie den Auswirkungen.
Ist ein Programm mit einem trojanischen Pferd infiziert führt es nicht nur erwünschte Dienste aus, sondern auch Funktionen für denjenigen, der es implementiert hat. Um zu verhindern, daß ein trojanisches Pferd zum Beispiel durch Code-Inspektion entdeckt wird, versteckt es der Erzeuger im Maschinencode[66]. Hier wird es in der Regel nicht bemerkt, da Programmierer zur Überprüfung eines Programms meistens nur den Quellcode inspizieren. [67]
Die Vorgehensweise[68] des Erzeugers könnte folgendermaßen aussehen:

1. Er wählt ein geeignetes Programm P aus, dessen Quellcode SP ihm zur Verfügung steht.
2. Er fügt das trojanische Pferd H hinzu: SP + H = SPH

[63]vgl. Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.67
[64]anderer Name für den Vienna Virus
[65]vgl. Solomon, PC viruses, S70/71
[66]Maschinencode macht das eigentliche Programm aus
[67]vgl.Gleissner, Manipulation in Rechnern und Netzen, S.18

3. Er compiliert SPH: Compiler (SPH) = PH.
4. Er löscht den neuen Quellcode SPH und das alte Programm P.
5. Er benennt das Programm PH in P um.

Für einen Außenstehenden existiert nun der alte Quellcode SP, an dem keine Veränderung feststellbar ist. Das mit dem trojanischen Pferd behaftete Programm P (=PH) verhält sich wie gewohnt, da die Infizierung nicht direkt ersichtlich ist. Theoretisch könnte nun durch eine erneute Compilation des Quellcodes SP das trojanische Pferd H im Programm P zerstört werden. Dies kann der Erzeuger einfach verhindern, indem er ein zweites trojanisches Pferd innerhalb des Compilers setzt. Er geht nach obigem Schema vor und fügt in den Compiler eine Sequenz ein, die, wenn sie die Quelle SP des Programms P erkennt, automatisch bei der Compilation das trojanische Pferd H hinzufügt. Dadurch wird das Programm T = TH erzeugt. Jede Compilation des Programms ST führt aufgrund dieser Sequenz wieder auf TH zurück. Das trojanische Pferd ist nun durch die zweite Sequenz auch vor Recompilation geschützt, ohne das verdächtige Eintragungen im Quellcode erscheinen.[69]
Die Auswirkungen von trojanischen Pferden sind von der Intention des Erzeugers abhängig. Er kann sich zum Beispiel Zugriff zu Daten ermöglichen, indem er ein trojanisches Pferd innerhalb einer Datenbanksoftware installiert. Ebenso sind Betriebssysteme, Editoren, Datenübertragungsprogrammme, Textverarbeitung, Compiler, Buchhaltungsprogramme wie auch Spiele vor einer Implementierung nicht sicher.[70]

4.2.3 Würmer

Wie bei trojanischen Pferden ist es auch bei Würmern falsch, sie als Viren zu bezeichnen, obwohl sie durch die Virenproblematik erfaßt werden. Der Unterschied zwischen Würmern und Viren besteht darin, das Computerviren keine eigenständig existierenden Programme sind. Ein Wurm im Gegensatz dazu ist als eine Ansamm-

[68]Gleissner, Manipulation in Rechnern und Netzen, S.18
[69]vgl.Gleissner, Manipulation in Rechnern und Netzen, S.18
[70]vgl.Gleissner, Manipulation in Rechnern und Netzen, S.21

lung vollständiger Programme charakterisiert.[71] Charakteristika bzgl. Funktionsweise und Weiterverbreitung sollen nun ein Beispiel veranschaulichen.

Am 2. November 1988 kam es zu einer der schlimmsten Attacken auf das Internet. Der sogenannte Internet - Wurm, ein sich selbst replizierendes Programm, verbreitete sich innerhalb von Stunden auf eine Vielzahl von Computern die am Internet angeschlossen waren. Innerhalb des Netzwerks wurden nur Rechner befallen, die als Betriebsystem die Berkeley 4.3 Version von UNIX oder das SunOS - Betriebssystem benutzten. [72] Der Wurm, den Morris, ein Student der Cornell - Universität (USA) programmierte, startete unter Ausnutzung einiger Fehler im Betriebssystem drei verschiedene Attacken auf das Netz.

1. Sendmail - Attacke

"Der damalige UNIX - Editor gestattete es, Programme auf dem Zielrechner zu kompilieren und auszuführen, ohne daß die Login-Prozedur des Zielrechners durchlaufen werden mußte. Ein Wurmsegment im Ausgangsrechner eröffnete also eine Verbindung zu einem Sendmail-Programm im Zielrechner und sendete im Debug-Modus des Editors den Quellcode mehrerer Dateien an den Zielrechner. Dort wurde zunächst das Steuerprogramm compiliert, daß dann Dateien des Ausgangsrechners herüberspielte und compilierte. Dadurch konnte der Wurm ein neues Wurmsegment erzeugen."[73]

2. Fingered - Attacke

"Durch das im Hintergrund laufende Dienstprogramm fingered kann man sich Informationen über einen anderen Benutzer verschaffen, wie zum Beispiel den Login - Namen und die Telefonnummer. Da Dienstprogramme unter UNIX keinem festem Benutzer zugewiesen werden, konnte sich auch Morris dieses Hintergrundprozesses bedienen." [74] Dazu wurde über eine aufgebaute Verbindung der Puffer des fingered-Hintergrundprozesses so weit geladen, daß er überlief. Dies hatte zur Folge, daß an

[71]vgl.Gleissner, Manipulation in Rechnern und Netzen, S.23
[72]vgl. Denning, Computers under Attack, S.194/195
[73]Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.53
[74]Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.53

einer bestimmten Stelle ein Befehl geladen wurde, der dann durch fingered ausgeführt die Implementierung eines neuen Wurmsegments veranlaßte.[75]

3. Remote - Shell - Attacke

“Bei dieser Attacke wurde der Umstand ausgenutzt, daß im UNIX-System eine Datei existierte, welche die verschlüsselten Paßwörter enthält. Da diese Datei von allen Benutzer gelesen werden kann und der Verschlüsselungsalgorithmus bekannt ist, konnte der Wurm eine Liste von Paßwörtern verschlüsseln und mit den gespeicherten vergleichen. Wurde ein passendes Paßwort gefunden, so konnte in dem damit erreichbarem Rechner über einen Remote-Shell-Befehl ein neues Wurmsegment erzeugt werden.“[76]

Diese drei Attacken ermöglichten es dem Wurm innerhalb weniger Stunden einen “denial of service“ hervorzurufen, wobei er mehr als 6000 Rechner lahmlegte. Grund dafür war, daß aufgrund der zahlreichen Kopien der Wurmsegmente der Plattenplatz der Computer nicht mehr ausreichte.[77]

4.3 Vorsichts- und Gegenmaßnahmen

Bezüglich der Virenproblematik ist es wichtig, den Umgang mit Soft- und Hardwaresystemen so zu regeln, daß ein Auftreten von Viren weitgehend verhindert wird. Unumgänglich ist dabei der Einsatz von Antivirensoftware

4.3.1 Antivirensoftware

Eine Vielzahl von Unternehmen vertreibt unterschiedliche Virenschutzprogramme.[78] Es gibt kein “bestes“ Softwarepaket und auch keines der Programme kann vor allen Viren Schutz garantieren. Zu schnell werden neue Viren in Systeme eingeschleust,

[75]vgl. Brobeil, Softwareangriffe auf PC´s und Netzwerk S.53
[76]Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.53
[77]vgl. Brobeil, Softwareangriffe auf PC´s und Netzwerke, S.53
[78]siehe Anhang

die erst erkannt werden müssen. Im wesentlichen benutzen aber alle Programme drei Techniken, um den Befall durch Viren zu verhindern bzw. Viren vom System zu entfernen: [79]

1. Signatur-Suche (→Activity Monitors)[80]

Durch Activity Monitors werden alle Dateien auf das Auftreten von für die jeweiligen Viren charakteristische Programmsequenzen hin untersucht. [81]

2. Aktivitätsfilter (→Scanner)[82]

Scanner versuchen im Computersystem Verhaltensweisen, die für einen Virenbefall typisch sind, festzustellen. Sie können dadurch indirekt auf die Aktivität eines Virus schließen.[83] Einige Aktivitätsfilter benutzen Techniken der künstlichen Intelligenz um Virencodierungen zu erkennen.[84]

3. Veränderungsüberwachung (→Change Detectors)[85]

Wichtige Systemdateien werden durch Change Detectors überwacht. Die unterschiedlichen Algorithmen zur Veränderungsüberwachung sind auch in der Lage, verdächtige Modifikationen zu erkennen und so indirekt auf Virenbefall zu schließen.[86]

Die verschiedenen Softwareprodukte beschränken sich entweder auf eine Technik der Virenerkennung, oder sind eine Kombination aus den verschiedenen Techniken. Im Normalfall reicht ein Virenscanner aus, um Viren zu identifizieren. Um ihn wirksam einzusetzen sollte er beim Erwerb von neuen Programmen und Disketten gestartet werden. Auf diese weise können Viren schon erkannt werden, bevor sie das System attackieren. Sehr wichtig ist ein regelmäßiges Update des Antivirenprogramms, da

[79]vgl. Slade, Guide to Computer Viruses, S.191
[80]vgl. Slade, Guide to Computer Viruses, S.191
[81]vgl. Kyas, Sicherheit im Internet, S.119
[82]vgl. Slade, Guide to Computer Viruses, S.191
[83]vgl. Kyas, Sicherheit im Internet, S.120
[84]vgl. Slade, Guide to Computer Viruses, S.191
[85]vgl. Slade, Guide to Computer Viruses, S.191

ansonsten der Schutz vor neueren Viren entfällt.[87] In der Regel sind diese Updates kostenlos im Internet erhältlich. Die Internet-Adressen einiger Hersteller sind im Anhang zu finden. Auf den Homepages findet man nicht nur Software, sondern auch Beschreibungen der einzelnen Viren sowie Tips zur Vorgehensweise bei einem Befall.[88]

4.3.2 Vorsichtsmaßnahmen

Das System kann noch effizienter vor Viren geschützt werden, wenn neben der Verwendung von Antivirensoftware einige Vorsichtsmaßnahmen[89] beachtet werden.

- niemals den Computer starten, wenn sich noch eine Diskette im Laufwerk befindet
- regelmäßig Datensicherung auf Streamern oder Disketten durchführen
- virenfreie Startdiskette erstellen und mit Schreibschutz versehen
- fremde Disketten mit Antivirenprogramm auf Viren überprüfen
- E-Mail-Attachments vor dem öffnen auf Viren checken
- Im Browser die Option “Java/Java Script“ deaktivieren

4.3.3 Reaktionsplan

Wann immer Verdacht besteht, daß Viren im System sind, muß sofort reagiert werden. Man sollte sich so schnell wie möglich einen aktuellen Virenscanner besorgen bzw. seine Version updaten. Wird kein Virus gefunden, kann es hilfreich sein, Programme auszuprobieren, die eine andere Technik[90] zur Erkennung anwenden. Können die Zweifel selber nicht behoben werden, müssen die “eventuell“ infizierten Files einem Experten[91] zugeschickt werden.[92] Wird ein Virus zu spät entdeckt, müssen folgende “Erste-Hilfe-Maßnahmen“ [93] eingeleitet werden:

---

[86]vgl. Kyas, Sicherheit im Internet, S.120
[87]vgl. Slade, Guide to Computer Viruses, S.190/191
[88]siehe Anhang
[89]Enskat, Hochschulanzeiger/Nr.40, S.21
[90]vgl. Gliederungspunkt 4.2.1
[91]siehe Anhang

- gegebenenfalls Disketten entfernen, den Rechner vom Netzwerk trennen und ausschalten
- von einer virenfreien, schreibgeschützten Startdiskette aus den Rechner wieder hochfahren (Virus ist dann noch vorhanden, aber nicht aktiviert)
- ein Antivirenprogramm von einer sauberen Diskette starten
- das Virus und dessen Quelle (E-Mail, Diskette, Programm) mittels Virenprogramm lokalisieren und exterminieren
- alle Disketten und Back-Ups überprüfen und gegebenenfalls säubern

Konnte der Virus nach der Durchführung der Maßnahmen nicht entfernt werden, muß eine infizierte Datei an eine Anti-Virus-Software-Firma[94] geschickt werden.
Ist der Virus gefunden und entfernt, besteht der nächste Schritt in der Ursachenanalyse. Dies ist genauso wichtig, wie das Entfernen der Viren, da 90% der Systeme innerhalb von drei Monaten über die selben oder ähnliche Wege erneut infiziert werden.[95] Bestandteil der Ursachenbehebung ist Gefahrenquellen innerhalb des Unternehmens abzubauen und den Umgang mit der Hardware zu regeln.

5 Sicherheitslücken innerhalb des Unternehmens und Richtlinien zur Bekämpfung

Nicht nur im Rahmen der Virenproblematik, sondern auch bezüglich aller anderen Sicherheitsrisiken ist es wichtig, Gefahrenquellen im Unternehmen entgegenzuwirken.
Größte Gefahr für das Unternehmen sind die eigenen Mitarbeiter. In der Regel wird bezüglich der Sicherheit zu leichtfertig mit Hard- und Software umgegangen. Sehr hilfreich sind entsprechende Schulungen der Mitarbeiter, da laut Untersuchungen des

[92]vgl. Slade, Guide to Computer Viruses, S.190
[93]Enskat, Hochschulanzeiger/Nr.40, S.21
[94]siehe Anhang

wissenschaftlichen Instituts für Kommunikationsdienste fehlendes Wissen über die Gefahren die entscheidende Ursache dafür ist, daß Sicherheitsrisiken nicht abgebaut werden.[96] Ebenso gilt es für die gesamte EDV-Infrastruktur des Unternehmens inklusive Datenverbindungen, Softwarequellen sowie Gastzugängen für Besucher und Geschäftspartner systematische Maßnahmen der Prävention zu erstellen. Allgemeine Nutzungsbestimmungen für EDV-Systeme und Datennetze müssen eingeführt werden. Vor allem bezüglich der Internetnutzung ist zu klären, wer berechtigt ist welche Systeme bzw. Dienste zu nutzen. Eine Blockierung aller Internetdienste die nicht zugelassen sind, ist erforderlich. Das Zugriffsmanagement erfolgt über ein dediziertes Firewallsystem. Eine direkte Verbindung des internen Unternehmensnetzwerkes mit dem Internet ist zu unterbinden. Jede Internetverbindung hat über das unternehmensinterne Firewallsystem zu erfolgen, auf dem Überwachungssysteme zur Erkennung von Verletzungen gegen die Sicherheitsrichtlinien installiert werden müssen.
Technische Schutzvorkehrungen sind jedoch nutzlos, wenn die Hardwarekomponenten, aus denen sie bestehen nicht ausreichend geschützt sind. Physikalische Abschirmung von kritischen Elementen der EDV-Infrastruktur wie Programm Server , Daten Server, Router, Brücken, etc. in einem klimatisiertem Computerraum ist unumgänglich. Zu den Schutzmaßnahmen von Hardwarekomponenten gehört auch das Anlegen von Sicherheitskopien der Daten von Festplatten. [97]
Unter Verwendung dieser Sicherheitsrichtlinien kombiniert mit einem effizienten Risikomanagement lassen sich die Sicherheitsrisiken des Internet auf ein Minimum reduzieren.

[95]vgl. Kyas, Sicherheit im Internet, S.118
[96]Hillebrand, Sicherheit im Internet zwischen Selbstorganisation und Regulierung, S40ff.
[97]vgl. Kyas, Sicherheit im Internet, S.124ff

6 Literaturverzeichnis

Ahuja, Vijay: Network and Internet Security, New York 1996

Brobeil, Hedwig: Software Angriffe auf PC´s und Netzwerke, Band 4, Oldenburg Verlag, München 1992

Buhl, Hans Ulrich: Skript Wirtschaftsinformatik II, WS1998/99

Denning, Peter J.: Computers under attack, USA 1990

Enskat, Robert: Hochschulanzeiger/Nr.40, Computerviren: Keiner ist immun, WS1998/99

Gleissner, Winfried: Manipulation in Rechnern und Netzen, Bonn 1989

Hillebrand, Anette: Sicherheit im Internet zwischen Selbstorganisation und Regulierung, Wissenschaftliches Instiut für Kommunikationsdieste, Diskussionsbeitrag 182, Bad Honnef 1997

Kyas, Othmar: Sicherheit im Internet, Datacom Buchverlag, Bergheim 1996

Lobel, Jerome: Foiling the System Breakers, 1.Auflage, USA 1986

Mertens, Peter: Wirtschaftsinformatik, 4.Auflage, Springer Verlag, Berlin 1996

Scholles, Frank Die Präferenzmatrix, http://www.laum.uni-hannover.de

Slade, Robert: Slade´s Guide to Computer Viruses, Springer Verlag, New York 1994

Solomon, Alan: PC viruses, 1.Auflage, Springer Verlag, London 1991

Wojcicki, Marek: Sichere Netze, Carl Hanser Verlag, München 1991

7 Anhang

Antiviren-Software

McAfee Hersteller von VirusScan
http://www.mcafee.com

S§S Hersteller von Dr.Solomons AV Toolkit

http://www.drsolomon.com

Safetynet Hersteller von VirusNet
http://w3.gti.net:80/safety

Hersteller von Sweep
http://www.sophos.com

SMYNTEC Hersteller von Norton AV-Utilities
http://www.symantech.com

TCT-ThunderBYTE Hersteller der Thunderbyte AV-Utilities
http://www.thunderbyte.com

Internet-Sicherheit: Organisationen

FIRST-Team (Forum of Incident Response and Security Teams
http://www.first.org/first

AUSCERT-Australian Computer Emergency Response
http://www.auscert.org.au

CERT Koordinatioszentrum
http://www.sei.cmu.edu/SEI/programs/cert.html

Internet Society
http://www.isoc.org

FBI computer crime information
http://www.fbi.gov/compcrim.htm

National Security Agency
http://www.nsa.gov:8080