Einführung in die Informationssicherheit

Eine Projektarbeit von Christian Brandt über das Thema von Definitionen und Abgrenzungen der Begriffe:

Informationssicherheit
Sachziele Information Warfare
Informationskrieg
Cyber Terrorism
Computer Espionage
Computer Sabotage
Computer Terrorism
Waffe
Angriff
Computermissbrauch
Krieg
Frieden
Terrorismus
Infrastruktur

Die Projektleitung untersteht Herrn Prof. Dr. Hartmut Pohl

Inhaltsverzeichnis

1. Einführung in die Informationssicherheit
1.1. Sachziele Informationssicherheit

2. Infrastruktur
2.1. Kritische Infrastruktur

3. Sachziele Information Warefare
3.1. Informationskrieg
3.2. Terrorismus
3.3. Cyber Terrorism
3.4. Computer Terrorism
3.5. Computer Espionage
3.6. Computer Sabotage

4. Einsatz von Waffen in der Informationsverarbeitung und deren Wirkweise
4.1. Angriff
4.2. Krieg
4.3. Kriegsschauplatz Internet

5. Missbrauch in der Informationsverarbeitung
5.1. Computermissbrauch
5.2. Computerkriminalität
5.3. Internetkriminalität

6. Zusammenfassung

7. Literaturverzeichnis

1. Einführung in die Informationssicherheit

Die Informationssicherheit, eine Zusammensetzung aus den Substantiven Information und Sicherheit, beschreibt, aus dem Lateinischen abgeleitet, die Zuverlässigkeit bzw. den Anspruch auf Unversehrtheit von Auskunft und Begriffsbelehrung.

Heute soll damit der Anspruch auf die Unversehrtheit von Auskünften, Handlungen, Übermittlungen, Steuerungen, Archivierungen und genutzter Anlagen gewährleistet werden. Zu den Auskünften, Handlungen, Übermittlungen und Steuerungen gehört der unversehrte Transport von Daten, zum Bereich Archivierung, das Ablegen von Daten auf Systemspeichern zum Bereich der Anlagen gehört der gesamte Komplex der Hardware, die bei der elektronischen Informationsverarbeitung angewendet wird.

Informationen stellen im Informationszeitalter die wertvollste Ressource dar. Ohne den schnellen und ungehinderten Austausch von Informationen wäre eine stabile Infrastruktur in den Industrieländern und eine Globalisierung der Wirtschaft nicht möglich. Ebenso wäre das effiziente Arbeiten, bei dem man auf schnellen und unbürokratischen Zugriff auf Wissens- oder Datenbanken setzt, undenkbar. Das Steuern von Maschinen, die ohne physische Anwesenheit des Menschen ihre Aufgaben verrichten sollen, ist dann eine Illusion.
Durch diese Voraussetzung ist das Existieren von Politik, Wirtschaft und das Wohlergehen der Zivilbevölkerung in den 1.Welt Ländern erst möglich. Ebenso bieten sich den Schwellenländern und auch einigen 3.Welt Ländern die Möglichkeit, auch ohne Bodenschätzen den wirtschaftlichen Anschluss an das Informationszeitalter zu erreichen. Hier kommt es auf Wissen und Know-How an, das man über die informationsverarbeitenden Schnittstellen, wie das Internet, frei beziehen kann.

Beim Thema Know-How aus wirtschaftlichen Gründen ist die angesammelte Information die Basis der Existenz eines Unternehmens. Hier sollte dieses Gut durch Kontrollen bei Zugang und Zugriff optimal geschützt sein. Ebenso gehört die Aufklärung und Sensibilisierung der Mitarbeiter zu diesem Thema.
Hier liegt durch absichtlich Zerstörung der Hauptschwerpunkt möglicher Schäden durch Fehlbenutzung oder Manipulation von Daten oder Infrastrukturen. Dabei kommt es nicht darauf an, ob die Schädigung von außen oder betriebsintern ausgeführt wird.
Die Schädigung von außen geschieht durch das Freisetzen von Viren, Würmern und Trojanern im weltweiten Netz, die sich, durch den Programmierer geführt, den Weg zum Ziel suchen. Dabei werden Schäden an unbeteiligten Dritten in Kauf genommen.
Eine andere Formen von Schädigung von außen ist das Eindringen über das Netz in fremde Rechner. Ist der Einbruch gelungen, stehen dem Eindringling alle Daten zum Missbrauch zur Verfügung. Auf die einsetzbaren Werkzeuge und Waffen wird in einem späteren Kapitel eingegangen.
Für Unternehmen und Institutionen heißt das, dass ein Höchstmaß an Datensicherheit durch räumliche, personelle und technische Maßnahmen gewährleistet werden muss. Hierzu ebenso später mehr.

Auf politischer Ebene ist die USA soweit, dass sie im Dokument 130010 festgelegt hat, welche Einrichtungen den unbedingten Schutz vor informationsverarbeitendem Missbrauch zu erfahren hat. Sie werden als kritische Infrastruktur definiert, bei dessen Ausfall die innere Sicherheit gefährdet ist. Dazu mehr im Kapitel Infrastruktur.

Auf der anderen Seite gibt es die Überlegung, ob jede Information, die in einem informationsverarbeitenden Medium zur Verfügung steht, auch der Realität entspricht und wer diese Information bestätigen kann.
Diese Situation taucht regelmäßig dann auf, wenn eine Differenz oder eine Auseinandersetzung zwischen großen Elementen wie Staaten oder Firmen im Gange sind. Bei solchen Auseinandersetzungen werden gezielte Falschinformationen in Umlauf gebracht, um einen Informationsvorsprung zu erlangen oder seine Taktik nicht zu veröffentlichen.
Es ist festzustellen, dass durch die zunehmende Vernetzung der Wirtschaft und der Infrastruktur und dem Zugang eines Jeden, der in der Lage ist, sich mit einer entsprechenden Hardware ins Internet einzuwählen, die Frage nach der Informationssicherheit geworfen wird. Dabei stellt sich die Frage, wie man auftretenden Gefahren begegnen kann und soll. In wie weit soll das Netz reglementiert werden, welche Sicherheitseinrichtungen sollen eingeführt werden.
Ist vielleicht eine Registrierung eines jeden Nutzer notwendig.
Eine Auseinandersetzung mit den Maßnahmen wird im folgenden erörtert.

1.1. Sachziele Informationssicherheit

Zu den grundlegenden Punkten der Sachziele der Informationssicherheit gehören:

- Confidentiality – Vertraulichkeit

Unbefugten darf keine Zugangsmöglichkeiten zu vertraulichen Informationen gegeben werden. Streng vertrauliche Information darf Dritten nicht zugänglich gemacht werden.

- Integrity – Integrität

Informationen müssen sich in absolutem Integerzustand befinden und somit eine Unverletzlichkeit der Daten gewährleisten. Unverletzlichkeit der Information an Außenstehende bzw. das Vertrauen in integere Personen ist sicherzustellen.

- Availability – Verfügbarkeit

Uneingeschränkte Zugriffsmöglichkeit auf vorhandene Information von berechtigten Personen. Keinerlei Beschränkungen oder Reduzierungen an Information dürfen vorgenommen werden. Dazu gehört auch der Zugang zu Räumlichkeiten und Hardware.

Weitere Punkte, die noch nicht vollkommen anerkannte Sachziele sind:

- Authenticity – Authentifizierung

Die Festlegung auf Korrektheit von Informationen und Personen. Insbesondere im E-Commerce sowie in der Übermittlung sicherheitsrelevanter Information muss die Authentifizierung gewährleistet sein. Der Nachweis über die an der Übermittlung von Information Beteiligten ist hier das Ziel.

- Liability – Verbindlichkeit

Die Verbindlichkeit ist eine Schnittmenge der oben aufgeführten Einzelpunkte. Aus der Kombination verschiedener Sachziele der Informationssicherheit entsteht automatisch eine feste Definition von Information mit festgelegten Eigenschaften und einer verbindlichen Aussage.

Punkte, die oft mit zu den Sachzielen der Informationssicherheit zählen:

- Reliability – Verläßlichkeit

Zusicherung auf Absicherung von Information und Datenbestand sowie deren zugriffsberechtigten Personen.

- Non-Propagation – Nicht-Vermehrbarkeit

Kontrolle von Vervielfältigung oder andersartiger Verbreitung von Information durch Speichermedien oder Personen.

- Anonymity – Anonymität

Nicht-Identifizierung, um die Gefahr eines Datenmissbrauchs nicht aufkommen zu lassen oder den getarnten Zugriff auf entsprechende Hardware oder auch Personen sicherzustellen.

- Pseudonymity – Pseudonymität

Ein weiterer Schutz gegen die Identifizierung mit den Mitteln der Tarnung im Gegensatz zur „Unsichtbarkeit“ - Anonymität.

- Non-Observability – Unbeobachtbarkeit

Nicht-Identifizierung

[Thomas Hungenberg, 2000]

Hier ist zu erkennen, welche Kosten bei der Durchsetzung der drei anerkannten Ziele auftreten. Diese ist aber in keinem Verhältnis zu setzen zur Relevanz der Informationen. Die Gefahr bei einem Angriff ist der gesamte Verlust an Information und damit die Gefährdung des Unternehmens in seiner Existenz.

Um diese Ziele zu erreichen sind bauliche Maßnahmen zunächst von großer Wichtigkeit, wie das Unterbringen von informationsverarbeitender Hard- und Software in zentralgelegenen und nicht allgemein zugänglichen und kontrollierten Räumen. Das Ausstellen von Sicherheitsausweisen mit regelmäßiger Kontrolle der Inhaber sowohl am Unternehmensein- und Ausgang und stichprobenartig innerbetrieblich. Zugriffsmöglichkeiten auf nur der Person entsprechenden Daten durch Login für diese Bereiche.

Die Schwachstelle ist immer der Mensch.

Einige der oben aufgeführten Punkte sind in der Theorie nicht durchsetzbar. Man kann im Internet nicht anonym arbeiten, da jede IP nachvollziehbar ist.
Anonymität und Nicht-Identifizierung haben dasselbe Ziel und stehen im Gegensatz zur Authentifizierung und zu der Tatsache, dass die IP, wie oben schon ausgeführt, immer nachvollziehbar ist.

2. Infrastruktur

Definition von Infrastruktur

Eine Infrastruktur ist die Gesamtheit der Einrichtungen, die in einem organisatorischen oder geografischen Bereich an unterschiedlichen Standorten gleichartige Dienstleistungen für eine Vielzahl von Kunden bereitstellt.

2.1. Kritische Infrastruktur

Definition kritische Infrastruktur

Eine Infrastruktur ist dann kritisch, wenn ihr Ausfall oder eine Einschränkung ihrer Funktionsfähigkeit dazu führt, dass sie Dienstleistungen nicht mehr bereitstellen kann auf die Staat, Wirtschaft oder Bürger angewiesen sind.

Dies ist vom PCCIP, einer Institution vom amerikanischen Präsidenten ins Leben gerufen, definiert worden, an die sich auch andere Institutionen weltweit anlehnen:

Telekommunikation und Informationseinrichtung
Transport- und Verkehrswesen
Energieversorgung (Elektrizität, Öl, Gas)
Gesundheitswesen
Lebensmittel- und Trinkwasserversorgung
Notfall- und Rettungsdienste
Regierung und öffentliche Verwaltung (einschließlich Polizei, Zoll und Bundeswehr)
Bank-, Finanz- und Versicherungswesen

Fällt eine dieser Strukturelemente nachhaltig oder für lange Zeit komplett aus, ist die innere Sicherheit und wirtschaftliche Stabilität nicht mehr gewährleistet.
Bei der Definition wird unterschieden zwischen öffentlich verwalteter und privat unterstellter Infrastruktur. Es wird auf eine Zusammenarbeit beider Verwaltungssektoren wert gelegt, um eine optimale Sicherheit zu garantieren.

Wie deutlich die amerikanische Definition der kritischen Infrastruktur und deren Maßnahmenkatalog ist, stellt die Beschreibung der kanadischen Definition der kritischen Infrastruktur und deren Sicherung dar. Die Erneuerung nach dem Anschlag vom 11. September ist mit Verweis auf das FBI angelegt.
Aus deutschen Regierungskreisen ist nichts derartig Aufwendiges zu erfahren. Bei den großen deutschen Unternehmen sieht man die Wertigkeit der amerikanischen Festlegung. Viele übernehmen den Maßnahmenkatalog an Sicherung im Bezug auf ihr Unternehmen.

Schutzmechanismen für kritische Infrastruktur in Institutionen, Unternehmen und privaten Haushalten.

- Bauliche Maßnahmen durch das Aufstellen der informationsverarbeitenden Hardware in separate, nicht frei zugängliche Räume.
- Technische Maßnahmen durch Sicherheits- und Kontrolleinrichtungen wie Zugangskarten oder Monitorüberwachung
- IT - technische Maßnahmen durch Passwortvergabe und Netzanbindung nur für bestimmte Mitarbeiter

- Organisatorische Maßnahmen durch Festlegung von Ablaufprogramme für das Ergreifen von Maßnahmen
- Personelle Maßnahmen durch Kompetenz- und Zugangsverteilung auf die informationsverarbeitenden Einrichtungen

Fünf Standbeine für die Sicherheit von kritischer Infrastruktur sind definiert:

- Feststellung von kritischer Infrastruktur
- Beschreibung der gesamten Infrastruktur
- Festlegung von Schutzpolicy, -informationen und –aufgaben
- Regelung von Organisation, Zuständigkeit und Zusammenarbeit der Beteiligten
- Erstellung der Rahmenbedingungen der Schutzmaßnahmen

[Cerny, 2000].

3. Sachziele Information Warefare

Information Warfare ist der englische Begriff für die moderne Kriegsführung im Informationszeitalter. Der Gedanke, der sich hinter Information Warfare verbirgt, ist der Einsatz der Informationstechnik zur unerkannten Bekämpfung oder zum Ausschalten von gegnerischen Stellungen oder Informationsveröffentlichungen sowie der Verteidigung der eigenen Stellung. Die Kurzbezeichnung lautet C4I: Command, Control, Communcations, Computers and Intelligence.
Das amerikanische Verteidigungsministerium stellte als erste Institution eine Definition des Information Warfare fest:

- Volle Unterstützung der militärischen Infrastruktur durch Einsatz von informationsverarbeitenden Maschinen und Werkzeuge, wie Hardware und Software.
- Absolute Kontrolle der zur Verfügung stehenden Informationsnetze, um Informationen zu bestimmen und Zugänge zur Information zu reglementieren.
- Einsatz von informationsverarbeitenden Werkzeugen zum Schaden von gegnerischer Infrastruktur, Informationsfluss und informationsbasierter Strategien und Waffen.
- Entwicklung der Soldaten zu intelligenten Kämpfern durch Einsatz von Informationsverarbeitenden Werkzeugen.

Grundlage zur Überlegung des Einsatzes von Information Warfare ist die Reduktion von physischen Elementen wie Mensch und Waffen. Durch den Einsatz von elektronischen Waffen kann gezielt operiert werden, ohne direkt Menschenleben zu gefährden und mit dem Vorteil, dass sich die Kommandostruktur nicht auf dem Schlachtfeld verteilt befindet. Von elektronmagnetischen Bomben über Laser und lasergestützte Lenkwaffen bis hin zum verkabelten Soldaten und bis zum Arbeiten mit Viren und Würmern erstreckt sich der Einsatz von Informationsverarbeitung im militärischen Bereich.
Soldaten werden soweit mit Information ausgestattet, dass ein Zugriff in REALTIME und mit Sichtkontakt zur Kommandostruktur erfolgen kann. Heutige ist der Einsatz von Spezialeingreiftruppen, die mit GPS-Satellitennavigationssystemen, kompletten Mobilfunkanlagen und Videokameras inklusive Monitor ausgerüstet sind, Standard. Somit kann der Soldat auch in für ihn unübersichtlichem oder unbekanntem Gelände agieren.. Die U.S. Army verfolgt das Land Warrior Program für die Entwicklung eines "Soldier's Computers", der jedem Soldaten hohe Computerleistung zur Verfügung stellt . Der Soldat erhält, wie oben angerissen, Befehle und Daten und liefert - zum Teil automatisch - seinen Befehlshabern Videobilder, Positions- und Telemetriedaten über seinen physischen Zustand und den seiner Waffensysteme. Die dafür notwendige Kommunikations-Infrastruktur wird derzeit ausgebaut.
Zur Steuerung gehören auch Lenkwaffensysteme, die während der Flugphase navigiert werden können. Zudem kann man die Flugbahn auch über Satelliten verfolgen. Hierzu gehören auch die aktuelle Diskussion um die Raketenabwehr im Weltraum.

Gezielte Freisetzungen von Falschinformationen erzielen in der Regel einen psychologischen Vorteil, mit dem die Gegenseite in die Irre geführt wird. Die Propaganda ist immer ein wichtiges Mittel in der allgemeinen Kriegsführung. Mit den Mitteln der Informationsverarbeitung kann man schnell und gezielt Informationen streuen oder Informationen zurückhalten oder reglementieren.
Die bekanntesten Beispiele zum Einsatz der Information Warfare war sowohl im Golf- als auch im Balkankrieg das Ausschalten der Informationszentralen der gegnerischen Seite durch das Zerstören der Einrichtungen.

Mit der wichtigste Gedanke hinter Information Warfare ist die eigene Infrastruktur und Informationsverarbeitung zu sichern und zu schützen. Hierfür werden genau die Maßnahmen ergriffen, die zur Bekämpfung des Gegners angewandt werden.

Das Problem bei Information Warfare ist eine unabhängige Kontrolle der Aufrüstung von informationsverarbeitenden Waffen und Handlungen. Wie im klassischen Rüstungsbereich wird keine Institution sein Know-How darlegen. Jedoch sollte eine Reglementierung des eingesetzten Waffenumfangs und der entsprechenden Einrichtungen durchgeführt werden. Nach dem Muster der Rüstungsabkommen im konventionellen Rüstungsbereich sollte auch in der Informationsverarbeitung eine Überwachung der Entwicklung und des Einsatzes festgeschrieben werden.
Auch stellt sich die Frage, wie weit sich die Macht und Kontrolle mit Hilfe der Information Warfare ausbreitet und welche Folgen das hat. Es besteht die Gefahr, wenn eine politische Institution den alleinigen Zugriff auf die Informationsverarbeitung gewinnt, sie somit die weltweite Kontrolle übernimmt. Hier besteht noch Nachholbedarf und es ist zu hoffen, dass zügig eine Kooperation von Staaten entsteht, die sich mit der Thematik auseinandersetzt und eine Basis zur Nutzung und Reglementierung der Information Warfare findet.

Es ist die Frage zu stellen, ob Information Warfare wirklich der unblutige Krieg mit minimalem Verlust ist. Jede Waffe, die freigesetzt wird, ist eine Bedrohung der Zivilbevölkerung. Die Technik ist nur so sicher, wie der Bediener, der sie führt. Jede fehlgeleitete Waffe und jede veröffentlichte Falschinformation, kann Unbeteiligten körperlichen und ökonomisch Schaden zufügen.

Wie groß ist der Wirtschaftsfaktor hinter Information Warfare. Zu beachten sind nicht nur die Unternehmen, die auf die Abwehr von Angriffen spezialisiert sind, sondern auch die Unternehmen, die zu den Waffenherstellern gehören.

3.1. Informationskrieg

Mit Hilfe der Informationsverarbeitung ist eine neue Art von Kommunikations- und Informationspolitik möglich. Wie bei jeder neuen Technologie ist das Militär die erster Institution, die diese in Gebrauch nimmt und einsetzt, sowie modifiziert und Weiterentwicklungen unter Verschluss hält.
Da die Informationsverarbeitung die Infrastruktur bis hin zum Menschen erreicht hat, muss sich als Folge mit den Gefahren, die von der Technologie ausgeht, auf politischer Ebene auseinandergesetzt.
Die Auswirkung einer Bedrohung des informationsverarbeitenden Bereichs ist groß, da sich in unserer Gesellschaft die gesamte Infrastruktur in der Informationsverarbeitung eingebunden ist. Somit ist durch ein gezieltes Lahmlegen der Infrastruktur ein großer ökonomischer und politischer Schaden zu erreichen.

In gleicher Weise greifen Falschinformationen in das gesellschaftliche Leben ein. Um militärische Interventionen zu legitimieren, wird über die Medien eine Propaganda der Verharmlosung offeriert oder im Sinne einer Institution argumentiert (NATO, UNO, Befriedung,...).
Es werden Bild- und Tondokumente auf allen Medien verbreitet, ohne das die Quelle nachvollzogen werden kann. Ebenso ist eine neutrale Berichterstattung unmöglich, da der Zugang zu Kriegsschauplätzen verwehrt oder behindert wird.
Für das Ziel zum Durchsetzen von Interessen werden keine Mittel gescheut.

Mit Fotos und Schriftstücken werden Begründungen für einen Eingriff in eine Situation hervorgerufen, ohne die Möglichkeit einer Verifikation.

Beispiele bekannter Desinformation:

- Beginn der zweiten Weltkriegs durch eine Lüge der Propaganda der Nationalsozialisten über den polnischen Überfall auf Deutschland.
- Das wirtschaftliche Interesse der USA an billigem Öl ist so wichtig, dass bis heute Truppen in den V.A.Emiraten stationiert sind. Die offizielle Begründung hierfür ist die angebliche Befriedung eines Schurkenstaates, der im Besitzt von B- und C-Waffen sein soll.
- Beginn der amerikanischen Invasion in Afghanistan zum Zweck der Ergreifung einer einzelnen Person.

Aus aktuellem Anlass, dem Anschlag vom 11. September und dessen Auswirkungen, sind einige amerikanische Quellen über Sicherheitsaspekte und Informationspolitik aus sicherheitspolitischen Gesichtspunkten von den Servern genommen wurden, da diese Seiten strategische Informationen über Informationssicherheit enthielten und damit einen Zugriff für potentielle Angreifer auf die Informationsverarbeitung gaben.

3.2. Terrorismus

Terrorismus ist ein Angriff jedweder Art, die in voller Absicht, heimtückisch und versteckt ausgeführt wird. Dabei kommt es zu erheblichem Sach- und/oder Personenschaden. Auf die Schädigung Unbeteiligter wird keine Rücksicht genommen. Ziel solcher Anschläge ist die Einschüchterung und die Verbreitung von Angst mit dem Gedanken, politische, ökonomische oder religiöse Vorstellungen gegen alle Vernunft durchzusetzen.
Gefahren bestehen in der Ausschaltung der Infrastruktur, im Datenmissbrauch im öffentlichen, wie im privaten Sektor. Allem gemeinsam ist ein hoher materieller Schaden.

Terroristen werde innerhalb eines Staates der Justiz übergeben und ein rechtskräftiges Urteil gefällt.
Was aber, wenn der Terrorismus nicht nur Grenzen überschreitet, sondern auch die Grenzen jener Staaten, die aufgrund gemeinsamer Rechtsüberzeugungen und effektiver Rechtsschutzabkommen in der Strafverfolgung zusammenarbeiten - und die unter terroristischen Verbrechen ungefähr dasselbe verstehen?
Was, wenn ein bestimmter Terrorismus nur funktioniert, weil bestimmte Staaten aktiv mit eigenen Mitteln (oder passiv durch die Duldung anderer) diesen Terror stützen und schützen?
Was, wenn diese Mittel nicht ausreichen, einen Förderstaat des Terrorismus zur rechtlichen Raison zu bringen? Und zwar in jenem Zeitraum, der ausreicht, die Fortsetzung des Terrors und die Vermehrung der Opfer zu vermeiden?
Überlegungen hierzu sind heute aus aktuellem Anlass angebracht und Aktionen, die zur Vergeltung aufrufen sind weder Lösung der Problems noch eine alternative Reaktion.

3.3. Cyber Terrorism

Cyber Terrorism ist die englische Definition für Terrorismus mit Hilfe der Informationsverarbeitung. Dabei kommt als Waffe Software zum Einsatz, die zur Zerstörung, zum Ausfall oder Datenmissbrauch eingesetzt wird. Als Einsatz- und Transportgebiet wird das Internet genutzt.

In den USA ist Informationsmissbrauch in der Strafgesetzliste weit oben angesetzt und gleichgesetzt mit der Handlungsweise von Terrorismus.
Auf Informationsmissbrauch steht hohe Haftstrafe.

Bei der Auswertung von 100.000 Angriffen weltweit wird jedoch deutlich, dass die Mehrzahl der Angriffe von „Amateuren“ ausgeht, also von Personen, die ohne definiertem politischen, ökonomischen oder religiösen Ziel gehandelt haben.
90% Der Angriffe waren von nicht terrormotivierten Angreifern ausgeführt.
9,9% der Angriffe gingen auf das Konto von professionellen Angreifern, die auf Gehaltslisten von politisch, ökonomisch oder religiös motivierten Auftraggebern standen. Nur 0,1% der Angriffe stammten von „world-class-Cyberterrorism“.
Zudem wurde bei 3000 Systemangriffen festgestellt, dass bei 88% ein einfach angelegter Angriff schon erfolgreich war. Bei 96% wurde der Angriff nicht registriert und bei den 4% registrierten Angriffen nur 5% nachvollzogen und Gegenmaßnahmen ergriffen wurden [Sproles, Byars 1998].

Es gibt in den USA Quellen, die behaupten, dass die Panikmache um Cyberterror, der Statistik entsprechend, nicht gerechtfertig sei [Lee, 2001].

Dies hat drei Gesichtspunkte:

- die Anzahl der nach Terrordefinition motivierten Angriffe
- die Anzahl der unentdeckten Angriffe
- die Schäden der Gesamtheit von Angriffen

Auf der anderen Seite gibt es diejenigen, die vor einem „digital Pearl Harbor“ warnen und mit nationalpolitischem Gedankengut auf das Gefahrenpotential aufmerksam machen.
Eine Sensibilisierung ist nötig und richtig, um die Schadensmöglichkeiten einzuschränken. Der Ausbruch von Hysterie bezüglich Cyberterror ist nicht gerechtfertigt, wenn man die Motivation der Angreifer auswertet.

Die Entwicklung der Hard- und Software und der Zugriff auf Tools im Netz, die einen Zugriff auf Fremdrechner zulassen oder die den Bau von informationsverarbeitenden Waffen anbieten, lässt die Gefahr größer werden, Opfer eines Hackerangriffs zu werden. Heute ist es möglich, über den Zugriff auf Fremdrechner einen Angriff auf andere Rechner auszuführen. Das heißt, dass jeder, ohne es zu wissen, als Basis eines Angriffs genutzt werden, der über heimlich aufgespielte Software ausgeführt wird. Man kann als Angreifer registriert werden ohne eigenes Verschulden.
Aus diesem Grund, durch den hohen Grag an Vernetzung und durch die hohe Anzahl an sicherheitstechnisch unwissenden Usern, ist die Aufklärung im Bezug auf Cyberterrorismus erforderlich.

3.4. Computer Terrorism

Computer Terrorism ist nach allgemeiner Definition das Handeln durch Nutzen und mit Ziel der Informationsverarbeitung.
Der Begriff wird als Überschrift für Handlungen benutzt, die die Sicherheit von Infrastruktur, Politik, Wirtschaft und Bevölkerung durch Mittel der Informationsverarbeitung gefährdet.
Im Gegensatz zum Cyber Terrorism wird beim Computer Terrorism die Informationsverarbeitung als Ganzes eingesetzt. Die inhaltliche Auseinandersetzung ist in beiden Fällen die selbe.

Auf internationaler Ebene wird durch den Austausch von Experten versucht, mit der Entwicklung der programmierten Waffen Schritt halten zu können, da sich die Angreifer ebenfalls der internationalen Entwicklung bedienen. Als Beispiel sei hier der Loveletter-Virus „I Love You“ genannt, der zahlreiche Nachahmer hat und eine neue Entwicklungsstufe der Viren darstellt, auf die die neue Generation aufbaut.

3.5. Computer Espionage

Die Computer Espionage ist heute die am häufigsten eingesetzte Spionagetätigkeit. Ziel des elektronischen Auskundschaftens ist es, mit Hilfe von informationsverarbeitenden Medien wie Hard- und Software, an Informationen zu gelangen oder sich einen Wissensvorsprung zu verschaffen.
Das bevorzugte Einsatzgebiet hierbei sind die Wirtschaft-, der Rüstungs- und Strategiebereich des Militärs.
Kontrolliert wird das Telekommunikationsnetz, das Internet und Großrechneranlagen. Über ein „Monitoring“, ein Überwachen der Medien durch Schlüsselwörter wird versucht, an nutzungsrelevante Information zu gelangen.
Der frühe Einsatz der elektronischen Auskundschaftung beschränkte sich in der Zeit des kalten Krieges auf die politischen und militärischen Ziele, während es sich heute in der Zeit der Globalisierung auf den Know-How - Vorteil und den technischen und wirtschaftlichen Fortschritt richtet. Hierbei bedient man sich der technischen Anlagen, die in der Zeit des kalten Krieges genutzt worden sind. Das bekannteste Beispiel in Deutschland ist das ECHELON - System, dass zum Abhören der Funkaktivitäten tief in den territorialen Bereich des Warschauer Paktes hineinhorchte. Heute wird das System zum Aushorchen der deutschen Kommunikationsaktivität eingesetzt mit dem Ziel der wirtschaftlichen Spionage.

USA, Frankreich, Israel und Japan sind die Staaten, die am häufigsten bei der Industriespionage angeführt werden, da es nach den Gesetzen dieser Länder legitim ist, die heimischen Wirtschaft durch Beschaffen von fremder Know-How zu unterstützen.
Im Gegensatz dazu wird die ökonomische Sicherheit in den USA als integraler Bestandteil der inneren Sicherheit angesehen und die Industriespionage gegen die USA gerichtet, mit harten Strafen belegt.
Aktuelle Fälle von Espionage im Consumerbereich sind sogenannte Spy-Programme (Trojanern). Softwareproduzenten spionieren die User mit versteckt eingesetzten Programmen aus, um das Userprofil zu ermitteln. Dies geschieht, wenn der User sich ins Internet einwählt. Dann aktivieren sich die versteckten Programme und übertragen Cache- und Cookydateien.

3.6. Computer Sabotage

Computer Sabotage ist das absichtliche Beschädigen von informationsverarbeitenden Werkzeugen wie Hard- und Software bzw. der Störversuch an informationsverarbeitenden Werkzeugen.
Zum Einsatz kommen ebenfalls informationsverarbeitende Werkzeuge wie Hard- und Software.
Das Lahmlegen oder Ausschalten von Telekommunikationsanlagen und informationsverarbeitender Hardware ist in erster Linie das Ziel solcher Anschläge. Dadurch wird die Kommunikation unterbrochen, was in kurzer Zeit zum Gesamtausfall der Unternehmensstruktur führt.

Zu Beschreiben sind die Faktoren:

Ausführende Organe

Bei der Beschreibung der ausführenden Organe wird Bezug auf Unternehmen und Institutionen genommen. Diese sind Ziele von Störversuchen oder Sachbeschädigungen.

Der Mitarbeiter als ausführendes Organ kommt als Quelle für Diebstahl und physikalische Zerstörung von Hardware, Software und Know-How sowie für interne Netzangriffe durch das Einspielen von Viren, Würmern und Trojanern in Betracht.
Dabei ist zu differenzieren, ob die Handlungsweise absichtlich durch Unzufriedenheit und Stress am Arbeitsplatz bzw. aus persönlichen Gründen wie finanzielle Schwierigkeiten erfolgt oder ob Beschädigungen unabsichtlich durch Unwissenheit und Nichteinweisung geschieht.
Im zuletzt beschriebenen Fall muss geprüft werden, ob eine Autorisation zur Ausführung der Tätigkeit bestand.
Schon diese Darlegung zeigt, wie ausführlich eine Analyse von Sabotageakten allein innerhalb eines Unternehmens geführt werden muss und wie viele Faktoren auf das ausführende Organ einwirken.
Bei Sabotageakten von Unternehmensfremden, die sich im Unternehmen selber aufhalten, gelten die selben Faktor wie beim Mitarbeiter.

Als Maßnahmen gelten die im Abschnitt Informationssicherheit beschriebenen grundlegenden Sachziele der Informationssicherheit und der Maßnahmen zur Sicherung der innerbetrieblichen kritischen Infrastruktur.

Bei Sabotageakten außerhalb eines Unternehmens gilt der Netzanbindung die ganze Aufmerksamkeit. Hier besteht immer die Möglichkeit für Außenstehende, Zugang zu Unternehmen oder zu Rechneranlagen zu erlangen. Im Bereich der klein- und mittelständischen Unternehmen besteht noch ein Nachholbedarf, da die Sicherheitsaspekte in der Netzanbindung auf Grund der ökonomischen Belastung nicht auf dem Stand der Technik oder gar nicht vorhanden ist.

Der Einsatz von Werkzeugen beschränkt sich auf den Hard- und Softwarebereich. Unter Hardware ist der Einsatz von klassischen Werkzeugen wie Schraubenziehern oder von vor Ort befindlichem Büromaterial zu nennen wie Kugelschreibern, Brieföffnern etc. Diese Werkzeuge dienen zur Oberflächenzerstörung und/oder zum Ausbau von Hardware aus Rechnersystemen.
Beim Einsatz von Software werden Kontroll- und Schnüffelsoftware sowie Viren und Würmer eingesetzt.

Wie schon in oben angegebenen Quellen ist die Motivation von Außenstehenden der „sportliche Antrieb“ und nicht die politisch, ökonomisch oder religiös motivierte Grundlage [Göttinger Tageblatt, 1999].

Es zeigt sich jedoch am Beispiel des Lufthansaboykotts, welche Möglichkeiten motivierten Saboteuren zur Verfügung stehen und welche Propagandamittel eingesetzt werden, um Rechtsbruch zu begehen und dazu anzustiften [Mazassek, 2001].
Es treten Motivationsgruppen auf, mit denen man nicht unbedingt rechnet. Daher ist die Einschätzung von Gefahren um so schwerer. Es wird offen erklärt, mit welchen Mitteln Server zu sabotieren sind und es werden Werkzeuge für die Sabotage veröffentlich, so dass jeder User ein potentieller Saboteur sein könnten.

4. Einsatz von Waffen in der Informationsverarbeitung und deren Wirkweise

Eine Waffe ist ein Werkzeug oder Gerät welches von vornherein zum Angriff und zur Verteidigung bei einem Kampf erdacht und hergestellt wurde. Dabei ist der primäre Zweck einer Waffe, den Gegner außer Gefecht zu setzen. Eine Tötung kann eine unvermeidliche Folge sein.

Die Waffen, die in der Informationsverarbeitung eingesetzt werden, bestehen aus Softwareprogrammen und Werkzeugen, die zur Zerstörung von informationsverarbeitender Hard- und Software eingesetzt werden.

Als Waffe aus dem Softwarebereich kommen zum Einsatz:

- Virus:

Eine Menge von Instruktionen mit der Eigenschaft, genau diese Instruktionsmenge mit Hilfe eines (Wirts-)programms in mindestens ein anderes Programm (evtl. modifiziert) implantieren zu können (Infektion) evtl. auch durch Überschreiben von Daten. Wesentliche Eigenschaft eines Virus ist also die Fähigkeiten, sich zu kopieren. Die Folge von Instruktionen enthält meist eine Schadensfunktion.
Die Schadensfunktion kann zu Datenverlusten führen. Auslöser der Schadensfunktion können Datum, Uhrzeit oder bestimmte Systemzustände sein. Viren werden verbreitet durch Austausch von infizierten Dateien (auf Datenträgern oder durch Datenübertragung). Makro-Viren können auch Dokumente für Textverarbeitungen infizieren. Ein Virus ist kein ausführbares Programm[Pohl, 2001]

- Dateiviren sind die bekannteste und häufigste Art der Computerviren. Sie infizieren ausführbare Programme (COM-, EXE-, OVL-, OBJ-, SYS-, BAT-, DRV-, DLL - Dateien) und können bei deren Abarbeitung aktiviert werden.
- Bootsektorviren (Bootviren) verstecken sich im Bootsektor von Festplatten und Disketten sowie im Master Boot Record (MBR) von Festplatten, können sich nach dem Booten von eben diesem Datenträger resident in den Hauptspeicher verlagern und permanent Schaden anrichten.
- Makroviren sind in Makros (d.h. in automatischen Programmabläufen) von Dokumenten, Tabellen, Grafiken, Datenbanken u.a. enthalten. Sie können bei Weiterverarbeitung dieser Dateien mit den entsprechenden Anwendungsprogrammen (z.B. Word für Windows) aktiv werden.
- Hybridviren sind Kombinationen von mehreren Virenarten, insbesondere von Datei- und Bootsektorviren. Damit machen sie sich verschiedene Ausbreitungsmethoden gleichzeitig nutzbar und sind somit schwerer aus dem System zu entfernen.
- Eine ganz neue Generation von Viren sind neben den schädlichen JAVA - Applets vor allem die auf Visual Basic Script basierenden Script Viren. Diese können in VBS-Dateien und sogar in HTML-Code versteckt sein.
- Link-Viren (auch: Directory-Viren) manipulieren die Datenträger-Einträge so, dass vor dem Aufruf von bestimmten Programmen zuerst andere Teile des Datenträgers angesprungen werden, welche den eigentlichen Virencode enthalten.
- Stealth - Viren sind Viren mit speziellen Mechanismen, sich vor Virensuchprogrammen zu verstecken. Sie können z.B. eine infizierte Datei vor der Überprüfung restaurieren und somit die Verseuchung unkenntlich machen. Vergleiche zum Stealth - Bomber sind hier angebracht.

- Polymorphe Viren verändern in einem bestimmten Rhythmus ihr Aussehen, so dass sie für Virenscanner, die nach Erkennungsmustern arbeiten, nicht oder schwer entdeckt werden können.
- Slow - Viren sind Viren, die lange Zeit unentdeckt bleiben, weil sie die Daten nur geringfügig manipulieren. Damit wird es wahrscheinlich, dass sie auch auf Sicherungsdatenträger übertragen werden, so dass der Benutzer keine virenfreien Duplikate oder älteren Versionen mehr zur Verfügung hat.
- Direct – Action - Viren infizieren bei der Ausführung des infizierten Programms sofort weitere Programmdateien und führen eine eventuell vorhandene Schadensroutine sofort aus. Anschließend übergibt der Virus die Kontrolle an das ursprüngliche Programm und entfernt sich aus dem Hauptspeicher.
- ANSI Viren sind im eigentlichen Sinne keine Viren, sondern nur besonders „reizende“ Manipulationen der Funktionstasten mit ANSI - Zeichenketten. Sie können nur dann Schaden anrichten, wenn der Treiber ANSI.SYS geladen wurde.
- Experimentelle Viren treten, wenn überhaupt, nur im Bereich der LISP-Programmierung auf und infizieren dabei den Quellcode. Sie sind allerdings sehr schwer zu programmieren und finden in der Informationsverarbeitung kaum Beachtung.
- E-Mail-Viren sind Viren, die sich im Attachment von Mails verstecken und die sich bei deren Benutzung auf den lokalen Rechner übertragen.
- Beim E – Mail - Bombing überhäuft ein Angreifer ein Zielsystem mit Mails, so dass im Extremfall die normale Nutzung von Mail nicht mehr möglich ist.

- Wurm:

Eine Menge von Prozessen, welche sich in Netzwerken replizieren und durch Prozessgabelung Rechenzeit abzweigt. Die Prozesse sind nicht auf (Wirts-)programme angewiesen.

- Trojanisches Pferd:

Trojanische Pferde (Trojaner*)* können sich im Gegensatz zu Viren und Würmern nicht replizieren. Es sind Prozesse, die undokumentierte Handlungen im Hintergrund von laufenden Programmen ausführen. Dies sind Formatieren der HD, Veränderung der FAT, Ausspionieren der Dateien, Datentransfer im Hintergrund.

- Sendmail Bugs sind trojanische Pferde, die in das zum Verschicken von E-Mails wichtige Sendmail-Programm eingeschmuggelt werden und Passwörter ausspionieren.

- Logische Bomben sind eine spezielle Art von Trojanischen Pferden.

Logische Bomben sind Prozesse, die beim Eintreten bestimmter Umstände (Erreichen eines Datums, Löschen eines speziellen Datensatzes einer Datenbank, Erzeugen einer Datei mit einem speziellen Namen) einen Prozess auslösen, die Schäden anrichten.

Weitere Angriffswerkzeuge:

- DNS

Bei einem DNS-Angriff erfolgt eine Umleitung einer Internet-Anfrage eines Nutzers an einen Rechner auf einen dritten Rechner. Auf diese Weise können z.B. Passwörter ausspioniert werden. Denial of Service

- RIP

Die gesamte Kommunikation zwischen zwei Rechnern wird zu einem externen Angreifer umgeleitet und ausspioniert. Danach werden die Daten dem richtigen Adressaten zugestellt.

- Backdoors

Backdoors (Hintertüren) lassen z.B. eine Fernsteuerung des Rechners zu. Damit kann ein Angreifer von außen über das Netzwerk Daten manipulieren oder ausspionieren.

- Keystroke Reader

Jeder Tastendruck eines Benutzers wird durch ein in den Rechner eingeschmuggeltes Programm heimlich mitgelesen und aufgezeichnet. Dadurch lassen sich Passwörter ausspionieren.

- Packet Sniffer

Packet Sniffer sind Programme, die von Benutzern ausgesendete Daten lesen und Passwörter erkennen und sammeln können.

- IP Spoofing

Ein Angreifer erzeugt Datenpakete mit gefälschter Absenderadresse; der Empfänger-Computer nimmt an, einen internen Nutzer vor sich zu haben, und gibt Zugangsrechte frei.

- ICMP - Angriff

ICMP - Protokolle dienen der Fehlermeldung und automatischen Reparatur bei Netzwerkproblemen. Gefälschte ICMP - Protokolle können die Funktionsfähigkeit von Netzwerken beeinträchtigen.
[Konzen, 1998]

- E-Bombe

Die elektronische Bombe ist eine Waffe, bei deren Aktivierung elektromagnetischen Wellen einer bestimmten Frequenz freisetzt werden. Diese freigesetzten Strahlen haben die Fähigkeit, die Wirkung eines Blitzeinschlages zu erzeugen. Dadurch kann innerhalb kurzer Zeit sowohl das Telekommunikationsnetz, wie auch die Stromversorgung lahmgelegt werden [Güow, 2001].

Das Wachstum der Waffentypen und die Intelligenz der Waffen entwickelt sich so schnell, dass Gegenmaßnahmen nicht sofort eingeleitet werden können. Die Zeit, die zur Entwicklung von Gegenmaßnahmen bereitsteht, zwischen erster Erkenntnis der Existenz des neuen Virus, der Analyse des Virus und der Bereitstellung von Gegenmaßnahmen, dauert zwischen einer und drei Stunden. In der Zeit und bei der Intelligenz der Waffen, hat sich der Virus schon im Netz verbreitet und Rechneranlagen befallen. Analysen haben gezeigt, dass die Entwicklung von Viren und Würmern soweit fortgeschritten ist, dass innerhalb von 24 Stunden das gesamte Internet befallen ist [Zuo, 2001].
Angriffe auf Rechner und Rechnersysteme sind heute schnell, einfach und in der Wirkung folgenschwer, da über 90% der Rechner mit Betriebssystem und Applikationen eines Anbieters bestückt sind [Inceon, 2001].
Hinzu kommt die Unwissenheit der User im Umgang mit infizierten Dateien.

4.1. Angriff

Eigenschaften eines Angriffes sind

- unberechtigte Tätigkeit
- Absicht
- Schäden
- undokumentiert Ausführungen

Eine Handlung kann als Angriff definieren werden, wenn mindestens eine der angeführten Bedingungen vorherrscht oder nachvollzogen werden kann.
Mit der Definition ist ein Programm oder eine Handlung beschrieben, das unvorhergesehene Ausführungen auf informationsverarbeitenden Anlagen hervorruft. Wenn eine der Bedingungen zutrifft, kann die Tätigkeit des Programms oder Handlung als ein Angriff angesehen und damit als strafbare Handlung gewertet werden.

Eine unberechtigte Tätigkeit ist ein Prozess, der nicht beschrieben ist und in Unkenntnis des Benutzers vollzogen wird. Hier hat der Urheber mit Absicht eine Ausführung hervorgerufen.

Mit Absicht wird eine Prozess ausgeführt, wenn es ein festes Ziel des Verfassers und damit Bestandteil des Programms ist, den Prozess ausführen zu lassen und damit einen Schaden zu verursachen.

Schäden werden unterschieden als passive und aktive Schäden.
Zu den passiven Schäden gehören Prozesse, die ausgeführt werden, ohne im Programm dokumentiert zu sein oder zu kurzzeitige Funktionsuntüchtigkeit der Hardware führen. Ökonomische Schäden sind gering, bringen jedoch Schrecken und Ärgernis.
Aktive Schäden sind Zerstörung von Hard- und Software, sowie langzeitiges Außerbetriebsetzen von Betriebsmitteln, wie Servern, Netzwerken oder Arbeitsplätzen. Schäden sind hier nicht zu differenzieren zwischen Privatusern, Unternehmen und Institutionen.

Als Programmfehler kann ein Prozess dann nicht beschrieben werden, wenn der Prozess undokumentiert ist.
Darunter versteht man das Verheimlichen von Prozessen in einem Programm. Da in einem Programm zum besseren Verständnis der Quellcode mit Beschreibungen über Ausführbarkeit versehen wird, kann eine undokumentierte, nicht beschriebene Quelle lokalisiert werden und bei Fehlfunktion der Ausführung als Angriff beschrieben werden, wenn die Funktion völlig von der Programmbeschreibung abweicht.
Angriffe können von außen über eine Netzanbindung oder von innen innerhalb eines informationsverarbeitenden Systems erfolgen. Dies ist wichtig, um entsprechende Gegenmaßnahmen einzuleiten oder Vorsorge zu treffen.
Als Gegenmaßnahme von Netzwerkeinbrüchen stehen IDS - Intrusion Detection Systems oder ein IRS - Intrusion Response Systems zu Verfügung. Bei IRS werden bei Angriffen alle Informationen über den Zustand des Systems gesammelt und dem Administrator zugespielt. Bei IDS kontrolliert ein System den gesamten Datenfluss im gesamten Netzwerk. Bei Angriffen, die registriert werden, werden Sofortmaßnahmen zur Sicherheit des Netzes ergriffen und der Administrator informiert. Bekanntes Beispiel für ein solches System ist der „honeypot“, eine Einrichtung, welche Angreifer vom eigentlichen Netzwerk ablenken soll.

Im administrativen Bereich kommt CERT, Computer Emergency Response Team zum Einsatz. Hier wird ein Frühwarnsystem aufgebaut, dass sofort auf Angriffe reagiert und dem Administrator mit Informationen versorgt.

Für den Bereich der Software gibt es heutzutage eine Vielzahl von Schutzprogrammen. Virenscanner und Firewalls sind dabei die Standardprogramme zum ersten Schutz für jeden Rechner. Effektiv wirkt der Schutz nur, wenn regelmäßige Sicherheitsupdates und Patches für Betriebssystem und das Schutzprogramm gefahren werden. Das Wissen über Angriffsart und -weisen muss protokolliert sein, um eine weitere Verbreitung zu verhindern. Der beste Schutz wertvoller Informationen ist das Separieren dieser Daten. Hierfür ist es ausreichend, die Daten nach einem Sicherheitsscan auf einen Rechner zu spielen, der nicht mit dem Netz verbunden ist und nur authentifizierte Zugriffsrechte hat.

Statistiken zeigen auf, welche Arten von Viren und Würmern sich „etabliert“ haben. Es sind sehr intelligente Angreifer, die sich durch Automatismen sehr schnell verbreiten. Ebenfalls wird aufgezeigt, mit welchen Mitteln sich die Angreifer einnisten und weiterverbreiten. Das Problem ist, wie bereits oben beschrieben, das Angriffe nicht festgestellt werden und wenn, dann nur zu einem geringen Teil nachverfolgt werden. Im Bereich der Homeuser besteht immer noch zu 30% überhaupt keine Schutzeinrichtung [BSI Virenstatistik, 1999].

4.2. Krieg

„Klassisch" ist der völkerrechtlich definiert Krieg als Auseinandersetzung zwischen Nationalstaaten unter der Geltung exakter Unterscheidungen zwischen Krieg und Frieden, Zivilisten und Kombattanten, Schlachtfeld und zivilem Raum.
Waffe und Ziel der Waffen des Anderen ist die Informationsverarbeitung (s. o.). Ein Krieg dank besserer Informationen soll gewonnen werden. Spionage und Nachrichtendienste, Verschlüsselung und Täuschung spielen eine wachsende, auch zunehmend von Techniken abhängige Rolle.
Spionage, Nachrichtentechnik sind in einem globalen Computernetz verschmolzen. Die Manipulation von Information ist nicht mehr ein Mittel im Krieg, sondern der Krieg selbst. Der Kriegsschauplatz ist kein Schlachtfeld an einem bestimmten Ort zu einer bestimmten Zeit, sondern das Internet. Statt Soldaten kämpfen zunächst einmal Programmierer und Hacker.
Die Angriffe auf Rechner und Datenbanken der Infrastruktur kann sauber und unblutig mit dem Computer geschehen, stellt aber einen gewaltsamen und folgenschweren Angriff auf die Zivilbevölkerung dar.
Aktuelles Beispiel ist die Auseinandersetzung zwischen dem FBI und der amerikanischen Hackerszene, nachdem das FBI mit Razzien gegen die Hackerszene startete.

4.3. Kriegsschauplatz Internet

Nach der Entwicklung des Internets in den sechziger Jahren nutzt das Militär das Internet für seine Operationen.
Der hohe Entwicklungsstand der Informationstechnik macht sie heute zum Zentrum militärischer Konzepte und Aktivitäten. Information Warfare, die militärische Seite der Informationsgesellschaft, ist bisheriger Höhepunkt militarisierter Informatik. Sie macht das Militär gleichzeitig zum größten Einzelrisiko der Informations-Infrastruktur und damit einer darauf fußenden Gesellschaft.

Information Warfare ist der vorläufige Höhepunkt des seit über 50 Jahren ungebrochenen Verlangens von Militärs, Computer für kriegerische Zwecke einzusetzen. Angriffsziele in den Kriegen einer Informationsgesellschaft werden die Knotenpunkte ihrer elektronischen Infrastruktur. Die zivile Informations-Infrastruktur wird schon in Friedenszeiten zum Gegenstand der Führung von kriegerischen Auseinandersetzungen.

Zu Bedenken ist allerdings, dass das Militär für seine Infrastruktur eigene Satelliten und Netze benutzt. Dadurch ist die Sicherheit gewährleistet, wenn dass Internet oder dem Internet nahe Infrastruktur zerstört wird.

Es ist als mutig zu bezeichnen, die risikoreiche Computertechnologie noch stärker als bisher zum Kern militärischen Handelns zu machen. Bei genauerer Betrachtung stellt sich jedoch zweierlei heraus: Erstens lässt sich eine Steigerung militärischer Erfolge vor allem durch Computertechnologie erreichen und zweitens haben die USA auf dem Gebiet der IT-Sicherheit einen ausgeprägten Wissensvorsprung, der Risiken bis zu einem gewissen Grad handhabbar macht. Beides konsequent integriert, gibt kriegerischen Auseinandersetzungen eine völlig neue qualitative Dimension. Zum neuen Mittel beim Austragen von Konflikten wird die per Computer bearbeitete Information im Information Warfare [Bernhardt und Ruhmann, 1998].

5. Missbrauch in der Informationsverarbeitung

5.1. Computermissbrauch

Computermissbrauch ist jede Art von unberechtigter Computerbenutzung. Das schließt sowohl den ordnungsgemäßen aber unbefugten als auch den nicht ordnungsgemäßen unbefugten Gebrauch mit Schadensfolge ein.

5.2. Computerkriminalität

Alle deliktischen Handlungen, bei deren Ausübung die Informationsverarbeitungstechnik genutzt wird, sind Handlungen des Computermissbrauchs und der Computerkriminalität.

Zu unterscheiden sind

- der personenbezogene Missbrauch
- der vermögensbezogene Missbrauch

Verstöße sind unter anderem

- Softwarepiraterie -> Urheberrecht
- Verrat von Betriebs- und Geschäftsgeheimnissen -> Wettbewerbsgesetz

Vorstufen zum Missbrauch sind

- Zeitdiebstahl in Form von Begrenzung einer Zeit durch unbefugte Nutzer
- Eindringen in ein System, ohne etwas zu verändern oder zu zerstören

Diese beiden Handlungen sind nach deutschen Gesetz nicht strafbar. In den USA fallen diese jedoch unter das Strafgesetz und werden mit Haftstrafe geahndet.

- Computerbetrug

Manipulation von Programmen oder Daten, wodurch eine Person oder Institution eine finanzielle Schädigung erleidet und gleichzeitig jemand einen finanziellen Nutzen zieht.

- Computerbezogene Urkundenfälschung

- Computersabotage

Beeinträchtigung der Funktionalität der Anlage, deren Zerstörung oder Datenbeeinflussung

- Computerspionage

Tatbestand von Ausspähen von Daten und Programmen

- Unerlaubter Zugang

Das sich unerlaubte Zugangverschaffen zu Systemen und Informationen

- Unerlaubte Nutzung

- Unerlaubte Verwertung

- Illegale Kopien, Vervielfältigung und verwerten von urheberrechtlich geschützten Daten
- Softwarepiraterie
- Chippiraterie
- Illegaler Technologietransfer
- Unerlaubte Weitergabe von Software und Hardware entgegen nationaler und internationaler Bestimmungen

5.3. Internetkriminalität

Austausch oder Angebot von gesetzeswidriger Ware.

Der scheinbare grenzenlose Handel mit Waren aller Art im Internet öffnet dem Missbrauch im Netz Tür und Tor. Aus Mangel an Kontrollmöglichkeiten blüht der Handel mit gesetzeswidriger Ware. Es handelt sich um Waffen, Medikamente, Daten und Menschen. Sowohl derjenige, der die Ware anbietet, als auch derjenige, der die Ware bestellt ist nach den Gesetzen in Deutschland und den USA ein Straftäter.
Das Problem bei der Durchsetzung der Verfolgung von Internetkriminalität ist das Verabschieden von einheitlichen Gesetzen für die Kontrolle und die Reglementierung von Warenangeboten.

Das Veröffentlichen von Inhalten im Netz ist ein weiteres großes Problem, das eng mit der Gesetzeslage im jeweiligen Staat verbunden ist. In einigen Staaten ist die Rechtslage so frei, dass rechtsradikale Inhalte oder kinderpornografische Bilder auf den Servern liegen. Hier muß auf politischer Ebene ein Eingreifen gefordert werden.

6. Zusammenfassung

Es ist aus den Definitionen zu erkennen, dass die Informationssicherheit einen wichtigen Stellenwert in Politik, Wirtschaft und beim Enduser in Zukunft einnimmt.

Aufgrund der starken Vernetzung der Rechner untereinander und durch die Nutzung der selben Software ergeben sich hohe Anfälligkeiten gegenüber Missbräuchen, die mit Hilfe der Informationsverarbeitung stattfindet. Dieser Missbrauch erfolgt grundsätzlich mit voller Absicht, entweder aus militärischen, ökonomischen oder persönlichen Gründen.
Die wirtschaftlichen Schäden, de heute dadurch entstehen und die Gefahren, die sich daraus für die Bevölkerung ergeben, sind so hoch, dass sich die Gesellschaft mit der Thematik der Informationssicherheit unbedingt auseinandersetzen muss.
Ebenso steigt die Qualität der Werkzeuge, die zum Missbrauch eingesetzt werden und somit binnen kurzer Zeit ein hohes Maß an Zerstörungskraft freisetzen können.
Die Sensibilisierung der Benutzer erfolgt aber bis heute nicht in dem gleichen Maße ausweitet, wie die Vernetzung und Ausweitung des Einsatzes der Informationsverarbeitung.
Aufgrund der derzeitigen Preise der Hard- und Software kann sich theoretisch jeder Haushalt in den Industrieländern ein PC leisten und sich damit in das weltweite Netz einklinken.

In der Darlegung von Gefahrenquellen für die Nutzer stehen die USA an der Spitze derjenigen, die durch die Offenlegung von Schwachstellen in Systemen und durch die Sicherstellung von Angriffen eine Transparenz zu erreichen versuchen.
Dadurch , dass die USA das Land mit der engsten Vernetzung und der technisch am weitest entwickelten Informationsanbindung sind, ergibt sich zwangsläufig auch eine hohe Anfälligkeit an Angriffen über das Netz, insbesondere für Großunternehmen. Die hierdurch gewonnenen Erfahrungen haben im Hinblick auf Cyberterrorismus Einblicke in Angriffsstrategien und Vorgehensweise gegeben.
Die USA entwickeln Informationsverarbeitende Werkzeuge, um ihrerseits einen Informationsverarbeitungsschaden bei anderen Nutzern hervorzurufen, z.B. im Bereich der Spionage, auf militärischem und wirtschaftlichem Gebiet oder in der Freisetzung unrichtiger Informationen.
Vergleicht man die Sicherheitsstandard der USA mit denen anderer Staaten in der hochentwickelten Informationsverarbeitung, dann stellt man fest, dass sich die Sicherheitsbestimmungen stark an die der USA anlehne oder noch gar nicht so weit entwickelt sind. Innerhalb der Institutionen und der Wirtschaft sind die Informationssicherheitsgedanken hierarchisch gegliedert, wobei die großen Einrichtungen und Unternehmen am weitesten in der Entwicklung sind, während kleine Unternehmen und der Endverbraucher die geringsten Sicherheitsmaßnahmen aufgrund hoher Kosten und zur Zeit noch geringer Informationsanstrengung aufweisen.

In Deutschland steckt die Informationssicherheit noch in den Kinderschuhen im Gegensatz zu den USA, wo der Präsident einen eigenen Mitarbeiterstab mit der Entwicklung von Standards beauftrage hat.

Maßnahmen und Gedanken für die Zukunft, die zu diskutieren sind, sind die Rechtslage und deren Auslegung auf die Informationssicherheit. Als Beispiel ist hier auch die USA anzuführen, die einen Angriff auf oder mit Informationsverarbeitung klar als Straftatbestand auslegt. Das Problem ist allerdings die fehlenden globalen Rechtsstandards zur Durchsetzung netz- und weltübergreifender Sicherheitsbestimmungen.

Als Maßnahmen zur Ausweitung des Wissens über Informationssicherheit ist vorzuschlagen, dass dem User beim Kauf bzw. vor Gebrauch einer informationsverarbeitenden Hardware eine Einweisung oder Schulung über die Gefahren und Fehlerquellen im Internet angeboten wird. Überlegungen zu einer Pflichtveranstaltung nach dem Vorbild einer Führerscheinprüfung ist zu überlegen, da dann definiert werden muss, wann man den Führerschein machen darf und wie man mit den jungen Usern umgeht. Ebenso kann der Verbraucherschutz erweitert werden, so dass eine gewisse Verpflichtung der verkaufenden Unternehmen dem Kunden gegenüber entsteht und diese überwacht wird.
Ein Weg zu mehr Sicherheit ist auch die Überlegung zum Einsatz von Internetüberwachungen in Form einer Polizei oder Agentenprogrammen. Hierzu ist aber erforderlich, dass ein einheitliches Rechtssystem global und ein spezielles für das Netz erlassen wird. Reglementierung und Zertifizierung muss bei den Möglichkeiten des Missbrauchs der Informationsverarbeitung überlegt werden. Dem Gegenüber steht allerdings die Meinungs- und Handlungsfreiheit, eines der wichtigsten Menschenrechte. Wer hat dann was zu beschneiden und zu welchen Lasten geht die Einschränkung.
Beispiele in der VR China zeigen, wie eine Reglementierung aussieht. Jeder User wird registriert und darf nur von der politischen Führung freigegebene Informationen abrufen. Abruf nicht freigegebener Informationen aus dem Netz ist ein Straftatbestand und wird mit Haftstrafe geahndet.

7. Literaturverzeichnis

Schönwälder, J.: Sicherheit in vernetzten Systemen http://www.vorlesungen.uni-osnabrueck.de/informatik/sec01/sec.pdf Osnabrück 2001

Monse, R. : Informationssicherheit http://www.suicidal.de/Berufsschule/doc/referate/monse/informationssicherheit.pdf o. J.

PCCIC: Executive Order http://www.info-sec.com/pccip/web/eo13010.html White House 1996

InfoSurance: Leitfaden zur Informationssicherheit http://www.infosurance.ch/de/pdf/leitfaden.pdf Zürich 2000

Minkwitz, O.; Schöfbänker, G.: Die neue Herausforderung für die Rüstungskontrolle, http://www.heise.de/tp/deutsch/special/info/6817/1.html Hannover 2000

Cert : Statistic 188-2001, http://www.cert.org/stats/cert_stats.html 2001

http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm Hrsg.: SANS Institute, Bethesda 2000

UNO: UNO-Abkommen gegen internationalen Terrorismus, http://www.uno.de/frieden/terrorismus/publ.htm Bonn 2001

Hirschmann, K.: Veränderung des weltweiten Terrorismus, http://www.gfw-sicherheitspolitik.de/ES00-05HirschmannTerrorismus.htm Bonn 2000

Dreyfuss, R.: Company Spies, http://www.mojones.com/mother_jones/MJ94/dreyfuss2.html Washington 1994

NSI: Economic Security Act, http://nsi.org/Library/Legis/bill1557.html Washington 1996

BFV: Computerespionage and Security Protection, http://www.verfassungsschutz.de/publikationen/gesamt/page05.html Köln 2000

Klingelschmitt, K.-P.: Mehr Spione in der Wirtschaft als im Militär, http://gib.squat.net/echelon/wirtschaft-militaer.html Stuttgart 1999

Dammann, M. - O.: Computerkriminalität aus Sicht der Ermittlungsbehörden, http://www.cert.dfn.de/dfn/berichte/db087/lka52.html Hamburg 2000

Virus Statistic, http://vx.netlux.org/virstat.shtml Hrsg.: VX Heavens 2001

http://www.avp.ch/avpve/entry/entry3.htm Hrsg.: Metropolitan Network BBS Inc. 1999

Wolf, S.; Häger, D.; Schorn, R.: Erkennung und Behandlung von Angriffen aus dem Internet, http://www.bsi.de/taskforce/literatur/angriff.htm Bonn 2001

Mell, P.: Computer Attacks, http://csrc.nist.gov/staff/mell/compattack.pdf Gaithersburg 1999

Einbruchserkennung: Intrusion Detection, http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=75&tdid=572 Hrsg.: BMWI, Berlin 2001

Blech, M.: Insider als Sicherheitsrisiko, http://zeus.fh-brandenburg.de/infoalt/fhbi_labore/sicherheit/ss2001/society/insider_risiko/ Brandenburg an der Havel 2000

Schetsche, M.: Internetkriminalität: Daten und Diskurse, Strukturen und Konsequenzen, http://www-user.uni-bremen.de/~mschet/interkrim.html Bremen 2001

Groebel, J.; Metze-Mangold, V.; Ward, D.: Cybercrime-Report, http://www.eim.org/Events/Downloads/CYBERCRIME-German1.pdf Hrsg: The European Institute of the Media 2001