Information Warfare
Der Krieg im Frieden

Hartmut Pohl[1] und Dietrich Cerny

0 Einleitung

Seit einiger Zeit werden – insbesondere in den USA – zunehmend Begriffe wie Business Information Warfare oder Information Warfare, InfoWar, CyberWar, Cybotage etc. benutzt. Diese Begriffe sollen ein neues Paradigma der Informationssicherheit transportieren, das mit einem Schadenspotential in zweistelliger Millionen Dollar Höhe bis hin zu Schäden von zehn Milliarden Dollar weit über den klassischen Begriff des 'Computermißbrauch' hinausgeht.

Unter Business Information Warfare sollen hier Angriffe auf wesentliche Teile des Kerngeschäfts von Unternehmen oder Behörden verstanden werden mit dem Ziel, das Kerngeschäft dieser oder der ganzen Branche zu übernehmen oder zu verhindern: Totaler Krieg mit Mitteln der Informationsverarbeitung gegen Informationssysteme. Auch andere Definitionen und insbesondere die militärischen Aspekte berücksichtigende sind gebräuchlich [Geiger et al. 1998].

Im folgenden werden die möglichen Täter und ihre Motive, die Angriffsverfahren und die Ziele von Business Information Warfare sowie Fälle dargestellt.

1 Sicherheitsprobleme der Informationsverarbeitung

Sicherheitsprobleme der Informationsverarbeitung wie Wirtschaftsspionage, Computerkriminalität, Computer-Mißbrauch, Hacker, Viren und Würmer sind für viele Unternehmen nur scheinbar Schlagworte ohne Bedeutung. Die Zahl der Fälle von schadensträchtigem Computer-Mißbrauch (Computerspionage und Computersabotage) ist ausgesprochen hoch und allein der im jeweiligen Fall entstandene direkte Schaden ist erheblich.

Der Einsatz neuer Technologien hatte in der Vergangenheit auch immer Mißbrauchsmöglichkeiten zur Folge. Mit zunehmendem Einsatz von Informationsverarbeitungssystemen und Kommunikationssystemen hat der Computer-Mißbrauch zugenommen. Insbesondere durch den Einsatz von Arbeitsplatzcomputern, Workstations und Servern sowie dem Betrieb von Netzwerken sowie der Kopplung von Netzwerken und durch die Integration von Daten-, Text-, Sprach- und Bildverarbeitung (Multimedia) werden weitere Mißbrauchsmöglichkeiten geschaffen.

Im folgenden sollen die Aspekte des Information Warfare dargestellt werden.

Eine vollständige bundesweite oder gar weltweite Übersicht der Schäden durch Information Warfare ist bisher nicht vorhanden. Allerdings existieren offenbar realistische Umfragen zum Computermißbrauch – so z.B. InformationWeek 1998, KES/Utimaco Sicherheits–Studie 1997/98 sowie Marschdorf et al. 1997.

1.1 Grundlegende Risiken

Konventionelle Bedrohungen

Zu den konventionellen Bedrohungen wie Naturkatastrophen sind auch die Störungen der Betriebssicherheit durch Feuer, Wasser, Strom und Blitz zu zählen sowie Störungen durch Erschütterungen und – in Deutschland im allgemeinen vernachlässigbar – durch Erdbeben. Weiterhin ist technisches Versagen von Komponenten durch Verschleiß und Alterung zu berücksichtigen sowie Einflüsse durch Temperatur und Temperaturwechsel, Feuchtigkeit, Gase, Staub sowie Strahlung. Diese Aspekte werden unter dem Begriff "Höhere Gewalt" zusammengefaßt. Zu diesem Bereich sind auch Vandalismus, Explosionen und klassische kriegerische Handlungen zu zählen. Diese sollen hier nicht weiter behandelt werden, weil

[1] Prof. Dr. Hartmut Pohl, Fachhochschule Rhein–Sieg, St. Augustin (Bonn) und
ISIS InStitut für InformationsSicherheit, Köln
Max–Pechstein–Str. 4. 50858 Köln. Tel.: 0221 – 4847 – 526. Fax.: – 529. Hartmut.Pohl@sang.net

sie eher konventioneller Natur sind und damit nicht spezifisch für Information Warfare.

Fahrlässiges Verhalten

Fahrlässiges Verhalten und auf Fahrlässigkeit beruhende Handlungen können meist auf Unwissenheit und damit auf eine unzureichende Ausbildung zurückgeführt werden – zumindest aber auf fehlende Sensibilisierung für die genutzte Technik und insbesondere auf eine fehlende Sensibilisierung für die Sicherheitsrisiken der Informationsverarbeitung.

Angriffsziele

Information Warfare kann in die beiden folgenden Kategorien gegliedert werden:

Spionage

Spionage oder unberechtigte Kenntnisnahme ist der einfache Tatbestand der Einsichtnahme (Lesen). Dazu sind Tatbestände zu zählen wie Kopieren sowie der weitergehende des Diebstahls; dabei ist es unerheblich, daß z.B. der Kopierende evtl. die Daten selbst gar nicht anschaut, sondern sofort an einen interessierten Dritten weitergibt.

Sabotage und Manipulation

Damit ist nicht der klassische Fall der Belegfälschung des unzuverlässigen Buchhalters gemeint, sondern die unberechtigte Manipulation von Eingabe- und Ausgabedaten sowie von gespeicherten oder verarbeiteten Daten. Dies kann mit direktem Zugriff geschehen (Ändern, Zerstören, Löschen), aber auch durch programmgesteuertes Erzeugen falscher Daten. Weiterhin ist hierzu die Dienstleistungsverhinderung zu zählen.

1.2 Ein einfaches funktionales Angriffsmodell

Unter Angriff im Rahmen des Information Warfare soll hier ein nicht-dokumentiertes Vorgehen mit dem Ziel der unberechtigten Nutzung von Informationssystemen (Mißbrauch) verstanden werden.

Ein Angriff wird also durch die folgenden Eigenschaften gekennzeichnet:

- Absichtliches Vorgehen.
- Nicht-dokumentiertes Vorgehen (Trojanisches Pferd).
- Unberechtigte Nutzung.

Programmgesteuerte Angriffe bestehen aus einem Transportmechanismus und einer Schadensfunktion. Bei festinstallierten ('stationären') Angriffen fehlt die Transportfunktion. Im Einzelfall kann auch die Schadensfunktion fehlen; dann besteht der Angriff nur aus der Transportfunktion – ggf. mit einer oder mehreren Schnittstellen.

Die Diskussion der Aspekte von Information Warfare wird häufig allein auf den militärischen Bereich beschränkt. Dies ist eine unvollständige Betrachtung. Im folgenden soll nur auf den nicht–militärischen Aspekt eingegangen werden – den Business Information Warfare.

Während sich Computermißbrauch gegen die beiden unteren Ebenen 'Informationssystem' und 'Information Management System' richtet, zielt Information Warfare insbesondere auf die oberste Ebene der Decision Process Systems.

Damit sind zwei Unterscheidungskriterien des Information Warfare vom Computermißbrauch erkennbar:

- Eklatante Schadenshöhen.
- Angriffe auf der Ebene der Decision Process Systems.

1.3 Angriffsverfahren

Angriffsverfahren lassen sich in sog. statische an einer Stelle im Informationssystem fest implementierte programmgesteuerte Angriffe gliedern und in sog. dynamische, die ihren Ort

verändern können und z.B. sich in andere Informationssysteme kopieren wie z.B. Würmer[2] und Viren[3]. Ein Beispiel für nicht-mutierende Angriffe ist der Wurm, der seine Befehlsfolge und sein Bit-Muster nicht verändert. Mutierende Angriffsverfahren können ihr Erscheinungsbild ändern (z.B. die Befehlsfolge abändern oder sich selbst verschlüsseln) oder ihre Funktion ändern; d.h. ihre Schadensfunktion ändern.

Asynchronous attack

Ein Beispiel für die fehlende Nachweisbarkeit von Angriffen ist das Ausnutzen sog. undefinierter Systemzustände zu Spionage- oder Sabotagezwecken. Derartige undefinierte Systemzustände treten nach unbeabsichtigtem Fehlverhalten von Hardware oder Software auf.

Eine Folge derartigen Fehlverhaltens ist der Zusammenbruch oder Absturz des Betriebssystems; danach steht das System bis zum Neustart ungeschützt einem potentiellen Täter zur Verfügung.

Ein Zusammenbruch des Betriebssystems kann auch gezielt herbeigeführt werden, wenn der Täter die Ereignisse kennt und ausnutzt, die zusammentreffen müssen, um den Absturz herbeizuführen.

Viren

Unter Viren werden (unselbständige) Befehlsfolgen verstanden, die zur Ausführung ein Wirtsprogramm benötigen – also kein selbständig ablauffähiges Programm darstellen. Ein Virus kann daher erst aktiv werden, wenn er in ein Programm hineinkopiert wurde; diese Aufgabe übernimmt der Virus selbst: Viren kopieren also die Befehlsfolge, aus der sie bestehen, in (andere) Programme.

Dieser Vorgang wird als Infektion bezeichnet. In der Befehlsfolge ist außer dieser Kopierfunktion meist ein störender Wirkmechanismus enthalten: Eine Schadensfunktion zur unberechtigten Veränderung von Daten (Manipulation). Beispiele sind das Löschen von Datenträgern wie Magnetplatten oder Disketten, das Spielen einer Melodie, Anzeige eines Textes auf dem Bildschirm oder die Zeichen auf dem Bildschirm 'trudeln' in die unterste Zeile etc. Ein Virus hat also meist eine sabotierende Wirkung.

Viele Viren prüfen vor der Infektion, das neue Wirtsprogramm, ob es nicht schon infiziert wurde. Damit vermeiden sie ein unnötiges 'Aufblähen' des Wirtsprogramms mit mehreren Kopien ein und desselben Virus.

Viren werden programmiert und weitergegeben über Netze oder auf Datenträgern. Wirtsprogramme können Spiele und raubkopierte Programme wie Betriebssysteme, Anwendungsprogramme etc. sein. Träger des Virus können grundsätzlich nur Programme sein, weil die Befehlsfolge des Virus ausgeführt werden muß. Nutzdaten werden nicht ausgeführt; sie können daher auch nicht Träger eines Virus sein. Zwar könnte man einen Virus auch in Datenbereiche hineinkopieren, er könnte aber dort nie aktiv werden, da Datenbereiche i. allg. nicht als Befehle ausgeführt werden. Die häufigste Infektionsquelle ist neben der Weitergabe auf Disketten insbesondere die e–mail–Kommunikation und die Übertragung von Dokumenten. Viele Viren sind für das verbreitete Betriebssystem DOS geschrieben worden; Viren kommen aber auch auf anderen Betriebssystemen vor und auch Großrechnerbetriebssysteme sind nicht grundsätzlich vor Viren gefeit. Allerdings können sich Viren in sicheren Systemen mit guten Zugriffskontrollsystemen nur unter großem Aufwand ausbreiten.

Es sind weltweit eine ganze Reihe von Viren-Suchprogramme auf dem Markt. Kritisch sollte die Qualität sog. geprüfter oder zertifizierter Viren-Suchprogramme bewertet werden;

---

[2] Unter Wurm (oder auch Blob, Vampir) wird hier ein ablauffähiges Programm verstanden, das sich selbst reproduzieren und die Ergebnisse seines ausgeführten Wirkmechanismus zusammenführen kann.

[3] Unter Virus wird hier eine Menge von Instruktionen verstanden, die in der Lage ist, sich selbst in ein anderes Programm zu kopieren; ein Virus ist nicht selbständig ablauffähig, sondern benötigt ein sog. Wirtsprogramm.

sie werden gegen eine beim realen Einsatz meist schon veraltete Viren-Referenzdatenbank getestet.

Wegen ihrer eklatanten Wirkungen werden Viren zu den sog. harten Angriffen gezählt. Es wird erwartet, daß Viren in Zukunft auch auf Netzen und Großrechnern verstärkt agieren. Es werden mutierende Viren mit tool-box-gespeicherten Schadensfunktionen in Umlauf gesetzt werden, die von Scanner-Programmen nur schwer erkannt werden können.

Weiche Angriffe

Anders als bei Viren entstehen viel mehr und größere Schäden durch Programme, die sich nicht durch offensichtliche und eklatante Schäden auszeichnen. Bei diesen Programmen werden bei Eintritt der Schadenswirkung z.B. nur sehr wenige Bits geändert, so daß die Manipulation kaum auffällt; die Schadenswirkungen sind wegen ihrer Punktualität (ein oder wenige Bits) auch nur schwer erkennbar.

So kann z.B. das Gehalts- oder Zinsprogramm verändert werden, das pro Vorgang nur einige wenige Pfennige zu Gunsten des Täterkontos umbucht. Das Programm zur Lagerverwaltung kann durch z.B. zufallsgesteuerte Manipulation weniger Daten falsche Mengenangaben zu gelagerten Teilen ausweisen oder auch Teile an "falschen" Stellen lagern. Parameter des Netzwerk-Betriebssystems können sporadisch derart verändert werden, daß der Durchsatz an übertragenen Daten zunehmend zurückgeht. Daten können so verändert werden oder auch völlig zerstört werden, daß Produktionsabläufe gestört werden.

Diese sog. weichen (nur sehr schwer erkennbaren) Angriffe werden gar nicht – oder erst nach Jahren – häufig erst durch ein Geständnis der Täter – bekannt. Die vorgenommenen Änderungen an Datenbeständen können ungeplant (Vandalismus) und zielgerichtet (Sabotage) vorgenommen werden. Es ist deutlich, daß sich derartige Angriffe vergleichsweise verheerend auswirken können, weil sie nicht – oder zumindest nicht so schnell und klar (wie die vergleichsweise eklatanten Viren) erkannt werden können.

Zu diesen weichen Angriffen sind die meisten schadensträchtigen Computermißbrauchsfälle zu zählen.

Dual use

Häufig werden vorhandene Programme zu unberechtigten Zwecken mißbraucht.

Dynamische Angriffe

Dynamische Angriffe sind gekennzeichnet durch die Fähigkeit sich zu vermehren (zu kopieren) sowie zusätzlich durch die Fähigkeit, sich zu verändern, d.h. ihr Erscheinungsbild zu ändern. Zu dieser Klasse sind insbesondere die erwähnten Viren zu zählen.

Statische Angriffe

Zu den statischen Verfahren zählen die logischen Bomben, die erst nach Eintreten eines inneren oder äußeren Ereignisses (trigger) in Aktion treten.

Aktivierendes (inneres) Ereignis kann das Erreichen eines Datums oder einer Uhrzeit sein oder das Überschreiten einer festgelegten Anzahl von Plattenzugriffen – dies sind Ereignisse, die vom Betriebssystem oder zugeordneten Routinen generiert werden.

Als äußeres Ereignis wird eine Eingabe in das IV-System bezeichnet wie die Eingabe eines Kennworts, Erreichen oder Überschreiten einer Temperatur und generell die Signalisierung eines Prozesses etc.

Trojanisches Pferd (trojan horse)

Unter Trojanischem Pferd wird eine nicht-dokumentierte – also heimliche – Implementierung einer Instruktionsmenge in ein Programm ohne (notwendige) Änderung der dokumentierten Aufgaben des Programms verstanden oder auch die heimliche Installation eines vollständigen Programms in einem IV-System.

Weitergehend können transitive Trojanische Pferde (ihre spezifische Funktion weitergebend

– kopierend) unterschieden werden von universellen Trojanischen Pferde, die lediglich eine Schnittstelle aufweisen, an die vom Angreifer (universell) beliebige und auch austauschbare Schadensfunktionen angeschlossen werden können.

Wurm

Ein Wurm ist ein selbständig ablaufendes Programm mit der Fähigkeit, sich selbst zu reproduzieren.

Simulation

Ein Unberechtigter gibt sich durch die Nutzung des Paßworts etc. eines anderen als Berechtigter aus – er simuliert den Berechtigten.

Object re-use

Die Wiederverwendung von Speicherbereichen im Hauptspeicher und auf anderen Datenträgern wie Disketten, Magnetplatten oder Bändern etc. stellt in vielen Betriebssystemen ein erhebliches Sicherheitsrisiko dar. Genutzte Speicherbereiche, die von dem laufenden Prozeß nicht weiter benötigt werden, werden zwar freigegeben – die Bereiche werden allerdings häufig nicht gelöscht. Dadurch können andere Prozesse die (immer noch) gespeicherten Daten lesen.

Verdeckte Kanäle

Gemeint sind nicht-dokumentierte Datenübertragungen. Auf diesen nicht immer offenkundigen Informationskanälen können unberechtigt – und meist unerkannt – Daten zwischen Kommunikationspartnern übertragen werden.

Ein "Sender" belegt z.B. im Morserhythmus eine Ressource wie die Magnetplatte. Der "Empfänger" versucht auf die Platte zuzugreifen und kann eine sporadische Belegung feststellen: Interpretiert er den Belegungsrhythmus, kann er die ihm vom Sender zugedachte Nachricht lesen: Verdeckter Zeitkanal.

Neben verdeckten Zeitkanälen spielen insbesondere die verdeckten Speicherkanäle eine Rolle: Ein Kommunikationspartner hinterlegt an einer vereinbarten Stelle – z.B. auf der Magnetplatte – geheime Daten. Der Empfänger liest die Daten aus dem vereinbarten Bereich aus. Ein derartiges Vorgehen ist aus den Protokollen und Audits nur mit großer Mühe zu erkennen.

Abstrahlung

Elektrische Geräte senden häufig elektromagnetische Wellen aus. Computer – und dies gilt insbesondere für Sichtgeräte aber auch für Drucker und andere periphere Geräte und Komponenten – senden die verarbeiteten Daten. Diese Tatsache wird als Abstrahlung bezeichnet. Die Abstrahlung kann z.B. mit Richtantennen und modifizierten Fernseh–Recordern auch aus größerer Entfernung gezielt aufgenommen werden.

Abhören

Auf Leitungen kann der Datenverkehr mit einfachen Geräten abgehört werden. In Vermittlungsrechnern (Router, Bridges, Hubs etc.) sowie allen Netzsteuerungsrechnern werden die übertragenen Daten zwischengespeichert; diese Phase kann von Unberechtigten dazu genutzt werden, die Daten zu kopieren. Dies gilt sowohl für die unternehmensinternen Geräte als auch beim Anschluß an öffentliche Netze für dessen Vermittlungsrechner.

Mithören

Gelegentlich kann es zwischen Leitungen zu unbeabsichtigten Einkopplungen und sog. Übersprechen kommen; in diesen Fällen, ist die übertragene Information nicht nur auf der (dazu vorgesehenen) Übertragungsleitung vorhanden, sondern auch auf anderen ggf. parallel laufenden Leitungen.

Solange die Effekte nicht gezielt erreicht werden können, muß von Zufallsereignissen ausgegangen werden. Diese werden meist als nicht so bedrohlich empfunden. Allerdings sind

eine Reihe von Fällen bekannt geworden, in denen auf diese Weise wertvolle Informationen an unberechtigte Dritte gelangt sind.

Replay

Auf Datenträgern und Datenübertragungsleitungen werden Nachrichten – ggf. modifiziert – wieder eingespielt.

Trigger

Angriffe werden meist in Abhängigkeit vom Eintreten bestimmter Ereignisse eingeleitet. Derartige Ereignisse können außerhalb des angegriffenen Systems generiert werden (Eingabe eines Codeworts) oder innerhalb des angegriffenen Systems eintreten wie Erreichen einer voreingestellten Uhrzeit (timer) oder anderer voreingestellter Werte wie das Erreichen einer voreingestellten Plattenspeicherbelegung.

1.4 Täter und Motive

1.4.1 Täter

Außenstehende Angreifer wie sog. Hacker, Cracker, Freaker u.a. spielen eine geringe Rolle deswegen, weil sich sicherheitsbewußte Unternehmen gegen diese Tätergruppe hinreichend schützen können; vielmehr kommen in den meisten untersuchten Fällen sog. Innentäter in Betracht, die Zugang zum Unternehmen haben. Deutlich zeigt dies eine aktuelle weltweite Untersuchung von etwa 1200 größeren Unternehmen [InformationWeek 1998] mit Mehrfach–Nennungen.

Innentäter

Bei der Analyse klassischer und aktueller Fälle von Computerkriminalität in Netzwerken wird deutlich, daß die von Hackern entwickelten DV-technischen Angriffsmethoden von den Innentätern – Mitarbeitern der geschädigten Unternehmen – übernommen und weiterentwickelt wurden – und zwar mit dem entscheidenden Vorteil der Innentäter: Sie besitzen bereits – wenn auch möglicherweise nur eingeschränkte – Zugriffsrechte.

Täter	Prozent
Berechtigte Mitarbeiter	58
Unbekannte	36
Unberechtigte Mitarbeiter	24
Hacker	14
Ausgeschiedene Mitarbeiter	13
Vertragspartner, Kontraktoren	9
Hersteller, Lieferanten	8
Kunden	4
Mitbewerber	3
Umweltgruppen	2
Ausländische Behörden	1

Abbildung 1: Erfaßte Täter

Die größte Gefahr geht von (unzuverlässigen) eigenen Mitarbeitern (Innentätern) aus, die berechtigt sind, auf Daten zuzugreifen. Mitarbeiter besitzen häufig die notwendigen Zugriffsrechte um sich vollständige Kopien von wichtigen und wertvollen Daten und Dateien erstellen und auch Daten und Programme manipulieren (Struktur) und Daten inhaltlich verändern zu können. Zu diesem Personenkreis sind alle Anwender, Teamleiter und Projektleiter zu zählen sowie Operateure, Systemprogrammierer, Anwendungsprogrammierer, Organisatoren etc. Auf diesen Kreis sind daher auch die meisten Angriffe zurückzuführen.

Eine Gefahr kann weiterhin von Personen ausgehen, die bzgl. der Zugriffsrechte den eigenen Mitarbeitern (oftmals unbegründet) gleichgestellt werden: Das sind insbesondere Un-

ternehmensberater (!) und alle Hardware- und Softwaretechniker von Herstellern oder Softwareunternehmen.

Dazu kommen fremde Mitarbeiter, die vergleichbare Kenntnisse und Zugriffsrechte besitzen wie das Wartungspersonal der Infrastruktur (Klima, Strom, Netzwerk- und andere Datenübertragungsleitungen etc.) und das Reinigungspersonal (!).

Außentäter

Nur von nachrangiger Bedeutung sind außenstehende Dritte wie die viel zitierten Hacker, Cracker etc. Sie führen den geringeren Teil der Angriffe durch. Mit den vielfältigen und spektakulär formulierten Publikationen wird allerdings versucht, einen anderen Eindruck zu erwecken.

1.4.2 Motive

Bei Angriffen lassen sich die Täter von den folgenden Motiven leiten.

Spieltrieb

Dieses Motiv muß sicherlich an erster Stelle genannt werden. Durch Ausprobieren von dokumentierten oder nicht dokumentierten Funktionen gelingt es Tätern, Computermißbrauch zu treiben.

Unzufriedenheit

Aus sehr unterschiedlichen Gründen unzufriedene Mitarbeiter durchstöbern Datenbestände und ändern Strukturen und Inhalte. Die Gründe können in Fehleinschätzungen, Erwartungen und Erfahrungen im beruflichen und privaten Bereich liegen; weiterhin in mangelhafter Motivation. Sie liegen häufig auch darin, daß Vorgesetzte der Informationsverarbeitung inklusive der Mitarbeiter in diesem Bereich zu wenig Aufmerksamkeit widmen.

Geltungsbedürfnis

Übersteigertes oder fehlgeleitetes Bedürfnis nach Anerkennung kann zu Computermißbrauch führen. Dies äußert sich u.a. darin, daß Mißbrauchsfälle unberechtigt den Medien mitgeteilt werden.

Geldgier

Mitbewerber zahlen recht großzügige Honorare für Computerspionage und –sabotage. Anwerbungsversuche werden bei sehr unterschiedlichen Gelegenheiten und von unterschiedlichen Personenkreisen unternommen. So bieten sich immer wieder Verkäufer von Sicherheitshardware und Software und auch sog. Berater in publizierten Mißbrauchsfällen zur Abwehr von Angriffen an. In einigen Fällen wurden die Angebote bereits vor der Publikation der Fälle gemacht, so daß der Eindruck der Kooperation zwischen Tätern, Beratern und Verkäufern entstand. Auch die Täter selbst bieten sich als Sicherheitsberater an – in Verkennung der Tatsache, daß derjenige, der in ein IV-System eindringen kann, das System auch nachhaltig gegen Angriffe absichern kann.

Offensichtlich wird auch Computermißbrauch getrieben, um den Tathergang und den Erfolg an die Medien gegen Entgelt zu verkaufen.

Die genannten Motive sind meist nicht allein ursächlich sondern werden in Kombination angetroffen. In jedem Fall geht es bei den Tätern um das Grundmotiv der Machtausübung.

1.5 Schwachstellen

Während früher in Unternehmen sehr wenige Großrechner vorhanden waren – häufig auch nur ein einziger – wird Informationsverarbeitung heute nicht nur dezentral sondern weitgehend netzorientiert betrieben – und zwar in lokalen Netzen, in Intranets und im Internet. Die Informationsverarbeitung entwickelte sich auf der Basis starker physischer Zugangskontrollen (klassisch-materielle Sicherheit) des closed shop Betriebs von Rechenzentren hin zu weltweit völlig offenen Systemen.

Allerdings haben die Entwicklungen im Sicherheitsbereich mit der Entwicklung vernetzter Systeme nicht mithalten können, so daß erhebliche Sicherheitslücken klaffen. Die flächendeckend vernetzten, offenen Client/Server Architekturen mit verteilten Datenbanken und verteilten Anwendungen in allen Unternehmensbereichen sind vergleichsweise völlig unsicher.

Der heute häufig anzutreffende Anschluß von Personal Computer, Terminals oder Workstations an offene und öffentlich zugängliche und zugreifbare internationale Netze (Internet) mit Nutzung von Hypermedia und Multimedia verstärkt die Unsicherheit deswegen, weil die eingesetzten Produkte meist nicht unter Sicherheitsaspekten entwickelt wurden und daher eine ganze Reihe sicherheitsrelevanter Schwachstellen enthalten. Darüberhinaus werden von Unternehmen häufig von Servern des Internets kostenlos kopierte Tools ohne weitere Prüfung eingesetzt. Dies obwohl diese Programme ohne jegliche Gewährleistung oder zugesicherte Eigenschaften lediglich bereitgestellt werden und der Autor nicht weiter bekannt ist.

Die Informationsverarbeitung wird absehbar in den mobilen (z.B. Verkehr) und privaten Bereich (Gesundheitswesen) weiter vordringen und dabei auch die Gebäudetechnik einbeziehen. Die Entwicklung dürfte in Zukunft zu einer stärkeren Integration der Informationsverarbeitung in allen Bereiche führen: Pervasive Computing. Dementsprechend werden sich die Schwachstellen auch auf alle diese Bereiche auswirken!

In Netzen werden unterschiedliche Typen von Geräten und Systemen verschiedener Hersteller mit unterschiedlichen Betriebssystemen, Datenbanksystemen und Anwendungssoftware wie Standardsoftware gekoppelt. Das sichere Zusammenwirken dieser Komponenten ist meist nicht gewährleistet.

Mit der Nutzung von Hypermediasystemen sind in diesem Bereich auch die ersten Mißbrauchsfälle aufgetaucht. Dazu sind von Tätern systematisch diese neuen Standardprogramme hinsichtlich möglicher Schwachstellen untersucht worden; die erkannten Schwachstellen wurden unmittelbar genutzt, um in IV-Systeme einzudringen und auf Daten unberechtigt zuzugreifen und sie zu kopieren oder sie zu manipulieren.

Sicherheit von Betriebssystemen

Entscheidend für die Sicherheit eines IV-Systems sind in erster Linie die im Betriebssystem vorhandenen und vom Betreiber eingesetzten Sicherheitsfunktionen. Häufig nutzen allerdings die Systemverwalter die vom Hersteller in das Betriebssystem eingebauten Sicherheitsfunktionen nicht – oder nicht so intensiv, daß die verarbeiteten Daten angemessen abgesichert wären. Dann bleibt dem Systemverwalter weitgehend verborgen, was auf den Systemen (Clients und Servern) geschieht. Was auf dem Netzwerk geschieht, bleibt dem Systemverwalter ebenfalls verborgen.

Erst in zweiter Linie ist daher die Qualität des benutzten Betriebssystems relevant. Die Betriebssysteme müssen Sicherheitsfunktionen enthalten, um unberechtigte Zugriffe mit dem Ziel der Sabotage oder Spionage zu verhindern.

Diese Aussagen gelten sinngemäß auch für die Netzwerk-Betriebssysteme in verteilten Systemen: Anwender sollten die implementierten Sicherheitsmaßnahmen der Netzwerk-Betriebssysteme einsetzen; auch hier ist erst in zweiter Linie die Qualität des Netzwerk-Betriebssystems entscheidend.

Die zur Verfügung stehenden Betriebssysteme (insbesondere DOS – aber auch viele Unix-Systeme) sind unsicherer als Mainframe-Betriebssysteme. Diese Betriebssysteme für kleinere Rechner wie PC und Workstations bieten aus den folgenden Gründen meist sehr wenig Schutz:

- Die Systeme wurden für einzelne Benutzer entwickelt. Eine Nutzung durch Dritte war nicht vorgesehen. Daher wurden Sicherheitsmaßnahmen auch als überflüssig angesehen.
- Die meisten der heute implementierten Sicherheitsmaßnahmen in Betriebssystemen sind

meist nur auf vorhandene (alte) Systeme aufgesetzt.

- Derartige Betriebssysteme für kleine Systeme sind in großer Zahl verbreitet, so daß weite Kreise von Benutzern Schwachstellen der Systeme durch Ausprobieren herausfinden und nutzen können. Tatsächlich kennt eine Vielzahl von Benutzern daher auch Schwachstellen. Die speziellen Schwachstellen eingesetzter Programmsysteme sind in Fachkreisen bekannt.

Auf den verteilten Systemkomponenten von Client/Server-Umgebungen wird eine insgesamt sehr große Menge an Daten gespeichert. Über immer schnellere Netzwerke sind die Daten weiterer DV-Systeme verfügbar; damit steigen die Mißbrauchsmöglichkeiten weiter an. Sind Maßnahmen erst einmal in einem Netz auch nur teilweise außer Kraft gesetzt, ist es bald insgesamt unsicher.

Die lokalen Netze und Intranets sind an öffentliche und damit offene Netze angeschlossen, auf denen jeder für seine Sicherheit selbst verantwortlich ist, von denen aber auch jeder von jedem Ort der Welt auf das Client/Server-System zugreifen kann. Wegen der Vernetzung kann an unterschiedlichen Stellen des Client/Server-Systems parallel oder sogar gleichzeitig mit ähnlichen Verfahren zugegriffen werden: Die Zahl der möglichen Angriffspunkte vervielfacht sich damit.

Client/Server-Systeme werden – im Gegensatz zum früher üblichen closed shop Betrieb von Großrechnern – häufig in Umgebungen eingesetzt, die nicht überwacht werden (können).

Heterogenität schafft Unsicherheit

Beim Einsatz unterschiedlicher Hardware und Software treten die folgenden vier sicherheitsrelevanten Probleme auf:

- Verschiedene Prozessoren und Geräte (Hardware) reagieren völlig unterschiedlich auf gleichartige Ereignisse. Der Sicherheitsbeauftragte müßte diese unterschiedlichen Reaktionen 'richtig' deuten. Dies setzt voraus, daß er die verschiedenen Hardwarekomponenten insoweit vollständig kennt.

  Hardwareplattformen: In betrieblichen Umgebungen werden häufig Hardwarearchitekturen (z.B. Workstations, PC, Server) eingesetzt, die Sicherheitsmaßnahmen aufwendig machen.

  Stand-alone Systeme – ohne Anschlüsse an lokale oder andere Netzwerke – lassen sich relativ einfach absichern.

  Dies gilt insbesondere für Mainframes. Diese Großrechner sind Hardwareplattformen mit einer für sicherheitsrelevante Aufgaben nutzbaren Hardwarearchitektur mit u.a. unterschiedlichen Zuständen – und mit unter Sicherheitsaspekten guten Betriebssystemen.

  In Client/Server Konfigurationen werden häufig sehr unterschiedliche Zentraleinheiten eingesetzt. Dies ist unter dem Aspekt Herstellerunabhängigkeit ein Vorteil, zumal in Abhängigkeit von der Aufgabenstellung spezielle Geräte eingesetzt werden können.
- Unter Sicherheitsaspekten sehen dies eine Reihe von Unternehmen kritisch, da auf den verschiedenen Zentraleinheiten unterschiedliche Betriebssysteme laufen, die unterschiedlich sicher sind. Verschiedene Betriebssysteme enthalten unterschiedliche Sicherheitskomponenten. Die Sicherheitsarchitekturen sind unterschiedlich.
- Inkompatibilität der Protokolldaten: Sofern eine Protokollierung (Audit) vorgenommen wird, werden von unterschiedlichen Betriebssystemen andere sicherheitsrelevante Ereignisse mit unterschiedlichen Protokolleinträgen festgehalten. Sollen die Protokolleinträge zusammengeführt werden, müssen sie vereinheitlicht und interpretiert werden. Bei der Vereinheitlichung gehen viele Informationen verloren, so daß die Aussagekraft der Audits erheblich nachläßt.

Auf einem Client erkannte Sicherheitsereignisse müssen mit Ereignissen auf anderen Clients und Servern korreliert werden. Der Sicherheitsbeauftragte muß sich einen Überblick über die Sicherheitslage auf dem Netz oder auf einzelnen Servern verschaffen. Dies können die unter Kapitel 3.2 Handlungsvorschläge erwähnten Tools zur Kontrolle und Beobachtung

leisten.

Allerdings muß daraufhingewiesen werden, daß diese (notwendigerweise) komplexen Tools die Heterogenität des Gesamtsystems verstärken. Weiterhin müssen diese Tools selbst gegen Mißbrauch durch Unberechtigte geschützt werden (Selbstschutz).

Nutzungsweisen

Durch die Netzorientierung haben sich die Nutzungsweisen der IV-Systeme in Richtung Client/Server-Architekturen verändert mit der Folge, daß wertvolle Daten auf Servern konzentriert werden, die von vielen Benutzern zugreifbar sind. Bei PC muß von dem unpersönlichen Personal Computer gesprochen werden, weil Hard- und Software der Geräte eine Nutzung durch mehrere Anwender ermöglichen. Die Vielzahl der berechtigten Nutzer erschwert eine Überwachung der Systeme hinsichtlich unberechtigter Nutzungsversuche.

Unsicherheit von Anwendungen und Verfahren

Die in Unternehmen und Behörden genutzten Individualprogramme weisen in einer ganzen Reihe von Fällen ein 'Alter' von mehreren Jahren auf. Manchmal gehen sie auch nur auf Entwicklungen diesen Alters zurück und sind dann fortgeschrieben worden. Diese Programme sind im Laufe der Zeit mit anderen kombiniert worden zu komplexeren Anwendungen. Auf diese Weise ist es gelungen, Verfahrensabläufe vollständig programmgesteuert abzubilden. Sicherheitsaspekte blieben bei der Entwicklung der Programme unberücksichtigt.

Eigenerstellte Anwendungsprogramme enthalten daher häufig keinerlei Sicherheitsmaßnahmen oder auch nur Zugriffskontrollen. Erst in jüngerer Zeit wird auch bei der Entwicklung und Programmierung von Anwendungsprogrammen auf Sicherheitsaspekte geachtet.

In Datenbanksystemen abgespeicherte Abfrage-Prozeduren stellen ein erhebliches Sicherheitsrisiko dar, weil sie auch von Unberechtigten ohne aufwendige und auffällige Neuprogrammierung schnell genutzt werden können.

Die entscheidenden organisatorischen und DV-technischen Sicherheitsprobleme in der Informationsverarbeitung lassen sich wie folgt zusammenfassen:

- Hardware: Sicherheitsarchitekturen sind nur bei Großrechnern realisiert.
- Client/Server-Architekturen: Hoher Vernetzungsgrad im Unternehmen, Anschlüsse an offene, öffentliche Weitverkehrsnetze (Internet). Verteilte Datenbanken und Anwendungen.
- Die Portabilität der Geräte und IV-Systeme ermöglicht unkontrollierte 'Heimarbeit' und Kundendialoge vor Ort.
- Betriebssysteme, Datenbanksysteme und Netzwerksysteme: Die Systeme enthalten viele bekannte Schwachstellen.
- Organisatorische Aspekte: Eine Vielzahl von Nutzern muß unter Sicherheitsaspekten administriert und kontrolliert werden. Lean Management bedeutet häufig die Konzentration von operativen und von Kontroll–Aufgaben bei einem Mitarbeiter.
- Neue Medien: Die Inhalte der per Fax, e-mail, ftp, gopher, World Wide Web etc. eingehenden und versandten Daten werden nicht kontrolliert.

1.6 Historischer und aktueller Angriffsablauf

Historischer Angriffsablauf

Angriffe werden rechnergestützt – programmgesteuert – vom Angreifer durchgeführt; Ergebnisse werden in einem speziellen log-file vollständig protokolliert. Angreifer erhalten mit diesen Angriffsprogrammen recht schnell die ihnen wichtigen Ergebnisse, die auf dem geschilderten Weg (Abfragen, Ausprobieren etc.) beschafft werden:

- Typ und Version des eingesetzten Betriebssystems,
- Anzahl und Art der installierten Anschlüsse eines IV-Systems (Kanäle, Leitungen,

Schnittstellen) und angeschlossene Geräte.

- Art und Version der installierten Anwendungsprogramme,
- Art, Anzahl und Größe der gespeicherten Dateien (Inhaltsverzeichnis) zusammen mit Beispiel-Ausdrucken,
- Quantität und Qualität weiterer – insbesondere in Anwendungsprogrammen – installierter Sicherheitsmaßnahmen,
- Anzahl und Art weiterer angeschlossener IV-Systeme oder Netzwerke ...

Dieses Vorgehen ist nachweislich vor allem deswegen von erheblichen 'Erfolgen' gekrönt, weil die Opfer des Computermißbrauchs meistens nicht mit einer derartigen Akribie bei der Absicherung der Informationsverarbeitungssysteme vorgehen, die auch nur annähernd mit der der Täter vergleichbar ist.

Aktuelles Vorgehen bei Angriffen

Es gibt eine Reihe von Hinweisen, daß das Vorgehen im Bereich des Computermißbrauchs sehr stark arbeitsteilig organisiert ist. Die Akteure kennen sich meist nicht oder wissen zumindest gegenseitig nicht von ihren konkreten Aufgaben.

Alle Jahre wieder lancieren Freaks der Computerszene eklatante Fälle von Computermißbrauch in die Medien; dabei werden auch Namen von sog. Hackern genannt. Diese verkaufen den Medien die jeweilige Story und sind gewiß nicht immer die tatsächlichen Täter. Andere stehen als Galionsfigur im Blickpunkt einer bestimmten Szene oder auch der Öffentlichkeit, ohne selbst je kriminell gewesen zu sein.

Entscheidender für die Mißbrauchsfälle sind die im Hintergrund agierenden Personen. Dabei müssen in erster Linie diejenigen Fachleute genannt werden, die – ohne es zu merken – ausgenutzt werden und z.B. bestimmte Angriffsprogramme im Auftrag schreiben. Gegebenenfalls wollen sie es auch angesichts des Entgelts gar nicht merken. Wichtiger noch sind sog. Schweiger, die als Fachleute keinerlei Kontakte zu Clubs, Vereinen o.ä. der Szene pflegen.

Dazu kommt das notwendige Fußvolk, das Adressen ausbaldowert, Dateien kopiert etc.

2 Aktuelle Fälle von Business Information Warfare

Im folgenden werden drei Fälle von Business Information Warfare kurz geschildert.

Zwei große Finanzberatungsunternehmen entwickelten mit unterschiedlichem Erfolg eine Beratungsunterstützungssoftware. Weltweit wanderten Kunden zu dem erfolgreicheren Unternehmen ab. Der unterlegene Mitbewerber beauftragte daher einen sog. Information Broker mit der Beschaffung des Quellcodes der relevanten Software, verbesserte damit sein eigenes Produkt und bremste den Kundenschwund. Der entstandene Schaden wird in der noch andauernden Untersuchung von den Strafverfolgungsbehörden auf 10 Milliarden US $ geschätzt.

Aus einem supranationalen Informationssystem lieferte ein Mitarbeiter den darin gespeicherten und zur Festnahme und auch zur überwachenden Fahndung ausgeschriebenen Mitgliedern organisierter Kriminalität über sie gespeicherte Information.

Ein Fluggesellschaft ließ mit eigenen Mitarbeitern die Vielflieger–Datei eines Mitbewerbers hacken und kopieren und bewarb die erhaltenen Adressaten. Die Gesellschaft wurde zu 1 Million englische Pfund Strafe verurteilt.

3 Maßnahmen gegen Information Warfare

3.1 Aktive und passive Maßnahmen

In der Vergangenheit wurden allein passive Sicherheitsmaßnahmen gegen Computermißbrauch realisiert: Mit Zugriffskontrollsystemen mit Tabellen–gespeicherten Zugriffsrechten oder Firewalls versuchte man wie mit einem Filter Eindringlinge abzuweisen und Unberech-

tigten einen Zugriff zu verweigern.

Aktive Maßnahmen gehen weiter, in dem sie selbst kontrollieren: So z.B. die von Nachrichten mitgeführten digitalen Signaturen verifizieren. Weiterhin können mit Tools der Kontrolle und Beobachtung [Lessing 1998a] die sicherheitsrelevanten Parameter wichtiger Programme wie Betriebssysteme, Datenbanksysteme und wichtiger Anwendungssoftware überwacht werden und kann bei Veränderungen Alarm ausgelöst und eskaliert werden.

Zu den aktiven Maßnahmen sind auch die Penetration Tests zu zählen. Hierbei werden von vertrauenswürdigen Personen systematische Test–Angriffe gegen Server, Clients und lokale Netze und Intranets gefahren mit dem Ziel, Schwachstellen der Konfiguration, der Betriebs– und Netzwerksysteme etc. zu erkennen [Lessing 1998].

3.2 Handlungsvorschläge

Alle Maßnahmen der Informationssicherheit setzen eine vollständige Sensibilisierung der Mitarbeiter und der Unternehmensleitung voraus. Im Einzelfall mangelt es daran – und insbesondere am Verständnis der Unternehmensleitung für die Risiken der Informationsverarbeitung. Hier läßt das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) hoffen, das die Möglichkeit eröffnet, den Vorstand persönlich in Haftung zu nehmen und Schadensersatzansprüchen auszusetzen [Deutscher Bundestag 1998 sowie Becker 1998].

Für einen Schutz gegen Angriffe des Information Warfare kommt als umfassende Maßnahme nur die unternehmensweite Realisierung einer Sicherheitsarchitektur [Pohl, 1995] in Betracht, die dem Wert der verarbeiteten Informationen angemessene technische, organisatorische und personelle Maßnahmen beinhaltet und auf Vollständigkeit und Überdekkungfreiheit der Detailmaßnahmen überprüft ist.

Eine wesentliche Detailmaßnahme ist der – bis heute häufig vernachlässigte – Selbstschutz der technischen Maßnahmen. Für ausgewählte Betriebssysteme, Firewalls und generell Zugriffskontrollsysteme sowie Intrusion Detection Systeme etc. müssen die jeweils für ein eingesetztes Produkt spezifischen sicherheitsrelevanten Parameter bestimmt und im laufenden Betrieb überwacht werden, um Sicherheitsverstöße wie Angriffe erkennen oder sogar verhindern zu können. Diese Überwachung muß beim Start– und Bootvorgang beginnen und bis hin zu Pflege und Wartung reichen. Überwacht werden müssen also die Parameter der Software einer jeden Ebene wie BIOS und Betriebssystem, die add–on Sicherheitstools wie z.B. RACF, Firewalls und Intrusion Detection Systeme sowie die Datenbank– und Anwendungssysteme. Derartige Verfahren sind als Tools zur Kontrolle und Beobachtung in Ansätzen bereits vorhanden und in der Entwicklung [Lessing 1998a].

Literatur

Becker, C.: Haftungsprobleme für Vorstände und Geschäftsführungen von Unternehmen bei Verletzung der IT–Sicherheit. Persönliche Mitteilung. Köln 1998

Cerny, D.: Schutz kritischer Infrastrukturen in Wirtschaft und Verwaltung. In: Geiger, G. (Hrsg.): Information War – Informationskrieg. Baden Baden 1998

Deutscher Bundestag: Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) vom 27. April 1998. Bundesgesetzblatt Jahrgang 1998 Teil I Nr. 24, S. 786 – 794. Bonn 1998

Geiger, G.; Huck, B. J.; Ziß, D.: Information War / Informationskrieg. Gefährdung und Schutz kritischer Infrastrukturen. Bd. 1: Analyse und Materialien. Bd. 2: Literaturverzeichnis und Volltexte. Aktuelle SWP–Dokumentation, Nr. 18 (August 1998)

InformationWeek (Hrsg.): Security Survey. New York 1998

KES (Hrsg.): KES/Utimaco Sicherheits–Studie. Sicherheit in der Datenverarbeitung. Ingelheim 1998

Lessing, G.: Parameterspezifische Schwachstellenanalyse – Basisfunktionalität in geschotteten Produktionsstätten. In: Bauknecht, K.; Büllesbach, A.; Pohl, H.; Teufel, S. (Hrsg.): Sicherheit in Informationssystemen. Zürich 1998 a

Lessing, G.: Penetrationstests in der Praxis. Ihre konstruktiven und destruktiven Wirkungen auf ein Sicherheitskonzept. Workshop im Rahmen der Euroforum Fachkonferenz. In: Pohl, H. (Hrsg.): IT–Sicherheit '98. Management und Lösungen für die Sicherheit in der Informationstechnologie. Frankfurt 1998 b

Marschdorf, H. J.; Müller, C. (Hrsg.): Wirtschaftskriminalität. Die Lage. Revisuisse Price Waterhouse. Zürich 1997

Pohl, H.: Taschenlexikon Sicherheit der Informationstechnik (information security). Köln 1989

Pohl, H.: Entwicklung und Realisierung unternehmensübergreifender Sicherheitsarchitekturen. In: Hammer, K. et al. (Hrsg.): Synergie durch Netze. Fachtagung der Otto-von-Guericke-Universität. Magdeburg 1995

Pohl, H.: Informationssicherheit der Global Information Infrastructure (GII) - Einige Bemerkungen zu Problemen und Entwicklungen. In: Tauss, J. et al. (Hrsg.): Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik. S. 358 - 390. Baden Baden 1996

Pohl, H.; Cerny, D.: Information Warfare: Der Krieg im Frieden. In: Bauknecht, K.; Büllesbach, A.; Pohl, H.; Teufel, S. (Hrsg.): Sicherheit in Informationssystemen SIS '98. Zürich 1998