

Business Information Warfare

– Einige vorläufige Bemerkungen –

Hartmut Pohl¹

1. Einleitung

Jede Technik hat ihre eigenen Kriminalitätsformen mit steigenden Schadenssummen hervorgebracht – so auch in jüngerer Zeit sehr stark ansteigend die ubiquitäre und zunehmend pervasive elektronische/digitale Kommunikation im – auf zahlenmäßig zunehmenden und schnelleren Breitband-Verbindungen aufbauenden – Internet.

Der seit Anfang der 90er Jahre – insbesondere in den USA – benutzte Begriff Business Information Warfare sowie die Begriffe CyberWar, CyberWarfare, Cybotage, Economic Information Warfare, Information Warfare, InfoWar, NetWar etc.. sollen ein neues Paradigma der Informationssicherheit transportieren, das mit Schadenspotentialen von 1 Mio. bis derzeit hin zu zehn Milliarden Dollar weit über den klassischen Begriff des 'Computermisbrauchs' hinausgeht. In Deutschland wurde frühzeitig der umfassendere Begriff der Verletzlichkeit geprägt [Roßnagel et al., 1989]

Auf Aspekte der internationalen Sicherheit (Geiger, 1997) sowie auf militärische Aspekte [Weizsäcker, 2000] soll hier nicht weiter eingegangen werden.

Im folgenden werden einige aktuelle Aspekte dieser bedeutender werdenden Angriffe mit Hilfe der Informationsverarbeitung auf Systeme der Informationsverarbeitung beschrieben.

2. Stand der Technik

2.1. Begriffsbeschreibung

Unter Business Information Warfare werden hier Angriffe auf wesentliche Teile des Kerngeschäfts von Unternehmen oder Behörden verstanden. Das Ziel der Angriffe ist, das Kerngeschäft eines Unternehmens oder einer ganzen Branche zu übernehmen oder zu verhindern: Nutzung der Informationsverarbeitung gegen Informationssysteme. Auch andere Definitionen und insbesondere die militärischen Aspekte berücksichtigende sind gebräuchlich [Pohl, 2000].

2.2. Problembeschreibung

Sicherheitsprobleme mit Schwachstellen, Risiken, Angriffszielen, einfache Angriffsmodelle, Angriffsverfahren, Beschreibung der Täter und Motive sowie historische und aktuelle Angriffsabläufe sind genauso beschrieben wie einige aktuelle Fälle des Business Information Warfare [Pohl, 2000].

Angriffe auf die Informationsverarbeitung werden durch die Ubiquität der Informationsverarbeitung und durch zunehmende Pervasivität der Anwendungen einerseits gezielter andererseits werden breite Bevölkerungskreise und Unternehmen und Branchen angegriffen.

¹ Prof. Dr. Hartmut Pohl, Fachhochschule Bonn-Rhein-Sieg, St. Augustin und
ISIS Institut für Informationssicherheit, Köln
Max-Pechstein-Str. 4. 50858 Köln. Tel.: 0221 – 4847 – 526. Fax.: – 529. Hartmut.Pohl@sang.net

Nicht nur PC, Notebooks, Handhelds, Mobiltelefone, Organizer wählen sich programmgesteuert ins Netz ein, um Informationen abzurufen, sondern auch Haushaltsgeräte wie der per Wetterbericht gesteuerte Rasensprenger, Web-Fernseher oder Web-Telefone; Waschmaschinen mit Internet-Anschluss und Internet-Steuerung sind erhältlich.

Angriffe wie SMS-Bomben werden praktiziert. Andere neue Angriffe sind grundsätzlich bekannt – allerdings noch nicht verbreitet. In Zukunft dürften die technischen Möglichkeiten einer zunehmenden Zahl von potentiellen Tätern bekannt werden und tatsächlich ausgenutzt werden.

2.3. Umfrageergebnisse und Schadenssummen

Angriffsart	Geschätzte jährliche Schadenssumme in Mrd. US \$
Denial of service (d.o.s.) attacks	4.0
AT&T toll frauds	4.0
Summe	8.0

Abb. 1: Geschätzte und erfasste Schadenssummen umfangreicher Angriffe. [Nach: Cohen 1995]

In nationalen und internationalen Umfragen [Pohl, 1998] wird z.T. eine zehnfach höhere Anzahl von Fällen und eine zehnfach höhere Schadenssumme im Vergleich zu behördlichen Veröffentlichungen genannt – vgl. auch die Abbildung 1 'Geschätzte und erfasste Schadenssummen umfangreicher Angriffe'.

Korrekte und die Lage vollständig beschreibende Zahlen zur Häufigkeit und zu den jeweils bewirkten Schäden liegen weltweit nicht vor. Umfrageergebnisse und Schadensbewertungen beruhen vielmehr auf kaum nachvollziehbaren Schätzungen weniger (nicht systematisch ausgewählter) Unternehmen. Nur in wenigen Unternehmen werden nachvollziehbare Verfahren zur Schadensbewertung eingesetzt.

Die Ursachen liegen in Folgendem.

- Es existieren keinerlei gesetzliche Meldepflichten – auch nicht an die Strafverfolgungsbehörden. Unternehmen melden Fälle nicht, weil sie bei Veröffentlichung einen Vertrauensschaden befürchten – auch durch die bekannt gewordenen Schwachstellen.
- Darüber hinaus werden für den gesamten Bereich Dunkelziffern genannt, deren Berechnungsgrundlage nicht offen gelegt wird. Um so wichtiger ist daher die Analyse und Bewertung veröffentlichter oder anderweitig bekannt gewordener Einzelfälle.

Tatsächlich kann festgestellt werden, dass es mit der Programmierung eines Virus/Wurms wie 'I love you' Informationsverarbeitung erstmals möglich war, mit geringem Aufwand weltweit einen (geschätzten) Gesamtschaden von 10 Mrd. US \$ zu verursachen. [Der Spiegel, 2000]

Das zur Erstellung und Verteilung eines Virus notwendige Wissen ist vielfältig im Internet für jedermann verfügbar und sehr leicht nachvollziehbar: Auf frei zugreifbaren Websites werden derzeit mehr als 60 Bausätze zur Erstellung von Viren angeboten.

3. Maßnahmen gegen Information Warfare

3.1. Potentielle Maßnahmen

Es hat eine Reihe politische Versuche und solche von Verbänden gegeben, die gesamte Internet-Kommunikation zu filtern – so der des Bundesverbands der Phonographischen Wirtschaft e.V., für das Internet sogenannte Grenzkontrollen für musikalische Inhalte durchzusetzen. Das Modell dieses sog. Rights Protection Systems sieht vor, mit einem Web-Cachingsystem gezielt den Zugriff auf einzelne Dateien im Internet mit als illegal oder gesetzeswidrig bewerteten Inhalten zu verhindern [TCP/IP, 2000].

Auf US-Behörden-Initiative ist Bilderkennungs-Software entwickelt worden als Basis entspre-

chender Filterprogramme (z.B. der sog. Kinderbrowser "Safari" [Heartsoft, 1999]), deren pflichtgemäßer Einsatz wiederholt diskutiert wurde. Von deutschen Strafverfolgungsbehörden wird zur Erkennung von Kinderpornographie o.ä. das Produkt 'perkeo filescan' eingesetzt [Heise, 1999].

3.2. Supranationale Aktivitäten

Die Verfolgung transnationaler Kriminalität erscheint geboten und wird auch gefordert [Fiedler, 2000] – allerdings waren die Versuche – insbesondere 'malicious programming code', Kinderpornographie und Kriminalität in Infrastrukturen wie dem Finanz- und Bankensystem – bis heute nicht erfolgreich [G 8, 1999].

3.3. Aktive und passive Maßnahmen

In der Vergangenheit wurden allein passive Sicherheitsmaßnahmen gegen Computermisbrauch realisiert: Mit Zugriffskontrollsystemen, die auf Tabellen-gespeicherten Zugriffsrechten oder Firewalls basieren, wurde wie mit einem Filter versucht, Zugriffe Unberechtigter zu erschweren oder zu verhindern – mindestens aber zu erkennen.

Aktive Maßnahmen gehen weiter, in dem sie kontrollierend in die Kommunikation eingreifen: Sie verifizieren z.B. die von Nachrichten mitgeführten digitalen Signaturen. Weiterhin können mit Tools der Kontrolle und Beobachtung [Lessing, 1998] die sicherheitsrelevanten Parameter von Programmen wie Betriebssystemen, Datenbanksystemen und Anwendungssoftware überwacht werden; bei Veränderungen wird ein Alarm ausgelöst und dieser eskaliert.

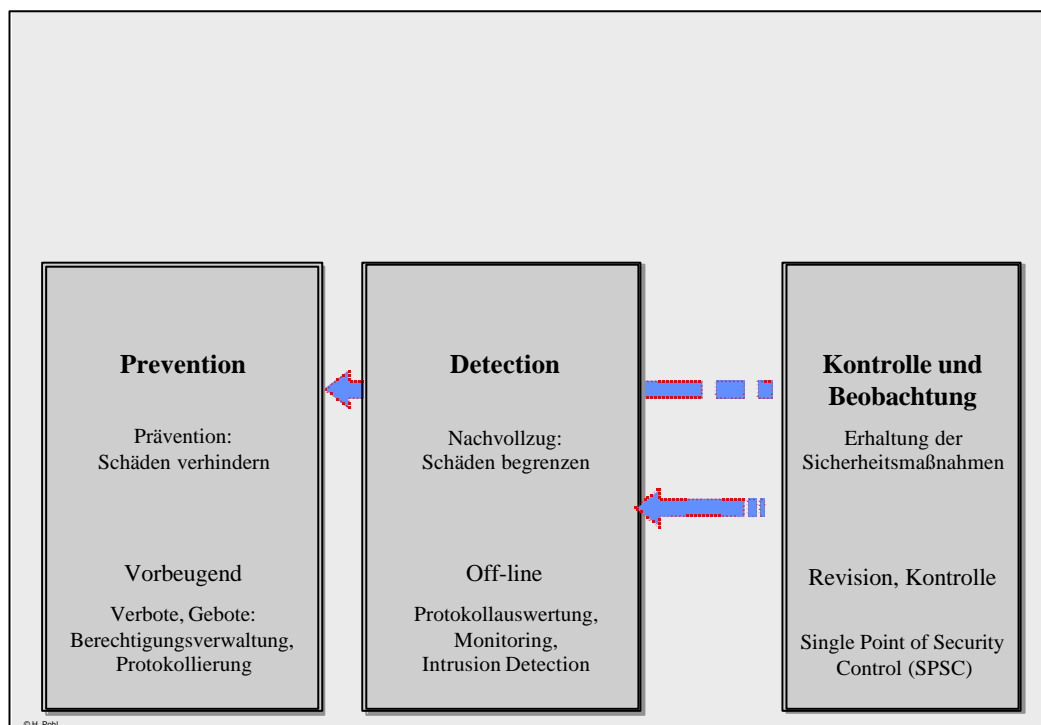


Abb. 2: Wirkungsweise von Sicherheitsmaßnahmen

3.3.1. Passive Maßnahmen

Das sind Zugriffskontrollmaßnahmen auf den Clients gegen unberechtigte Nutzung (Passwort, Token, biometrische Merkmale) mit Berechtigungsverwaltung, Protokollierungsmöglichkeit aller Aktivitäten und Sicherheitsauswertung der Protokolldaten; weiterhin Maßnahmen am Netzanschluss in der Funktion eines Filtersystems (Security Guards) mit Angriffserkennung zur Erkennung oder Verhinderung unberechtigter Nachrichten, Files und Zugriffe.

Weiterhin sind das Nutzungsbeschränkungen im Internet wie.

- Ausschließlicher Einsatz und Anschluss geprüfter und zugelassener Systeme (Hardware und Software).

- Nutzungsmöglichkeit des Internet nur durch geprüfte und zugelassene (wie ein 'Computer-Führerschein') Benutzer.

3.3.2. Aktive Maßnahmen

Kontrolle der Hardware, Software und Anwender.

- Überprüfung aller angeschlossenen Systeme (Hardware/Software) und Endanwender durch bei Providern zu installierende Kontroll-Hard- und -Software. Dies ist möglich durch die Überprüfung biometrischer Merkmale zugelassener Benutzer sowie durch Überprüfung der installierten Hardware und Software.
- Überwachung (Protokollierung und Protokollauswertung) aller Netzaktivitäten. So kann durch eine Überprüfung der digitalen Signatur des Senders eine Überwachungen jeglicher Kommunikation vorgenommen werden.
- Inhaltsüberwachung auf (bekannten) bösartigen Code wie Viren und auch Code in Scripts, Applets, Servlets etc. Ansätze hierzu liegen u.a. durch die Filtersoftware vor [Heartsoft, 1999].

Kontrolle & Beobachtung

- Eine wesentliche Maßnahme ist der – häufig vernachlässigte – Selbstschutz der IV-technischen Maßnahmen; die Kontrolle der sicherheitsrelevanten Parameter aller eingesetzten Hardware und Software wird als überzogen angesehen. Tatsächlich gehen nämlich viele Anwender (völlig zu unrecht) davon aus, dass Sicherheitsmaßnahmen selbst keine Sicherheitslücken enthalten – das Gegenteil scheint der Fall zu sein [Hartmann, 2000 a und b].

Sicherheitsmaßnahme	Sachziel - Funktion	Wirkungsort	Wirkungsart	Alarm- eskalation
Kontrolle & Beobachtung	Integrität von Programmen. Parameter-Überwachung	Clients, Server	aktiv	ja
Intrusion Detection	Authentizität. Auswertung, Vergleich, Mustererkennung	Netzabschluss, Clients, Server	aktiv/passiv	ja
Virensuchprogramme	Integrität von Programmen. Mustererkennung, Löschung	Clients, Server	aktiv	nein
Firewalls	Authentizität. Filterung (Ports, Adressen)	Netzabschluss	passiv	nein
Verschlüsselung	Vertraulichkeit (Zugriffskontrolle)	Clients, Server	passiv	nein
Zugriffskontrollsysteme	Authentizität. Filterung: Zugriffsberechtigungen, Protokollierung, Auswertung	Clients, Server	passiv	nein

Abb. 3: Sicherheitsmaßnahmen und Funktionen

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. Zugriffskontrollsysteme, 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, 1998] – vgl. Abb. 2 'Wirkungsweise von Sicherheitsmaßnahmen'. In jedem Fall spielen sie eine zunehmende Rolle bei Cascaded Infrastructure Security Systems (CISS) als Intranet-Absicherung (so mit Public Key Infrastructures) und als Intranet-Abschluss gegenüber dem Internet – vgl. die Abb. 3 'Sicherheitsmaßnahmen und Funktionen'.

- Da Systeme nur mit großem Aufwand vollständig abgesichert werden können, wird in Abhängigkeit vom Informationswert und dem daraus resultierenden Sicherheitsniveau differenziert in

benötigte Schutzzonen [Lessing, 1999; Naumann, 2000].

Die Auswirkungen von Angriffen sowie die hier skizzierten Abwehrmaßnahmen werden an der Fachhochschule Bonn-Rhein-Sieg in Zusammenarbeit mit Unternehmen und Behörden im Rahmen des Projekts 'Business Information Warfare' untersucht [vgl. Geiger, 2000 c].

4. Literatur

- Abegglen, C. M. V. : Information Warfare - Ein strategisches Mittel der Zukunft. Darstellung der Mittel, Möglichkeiten und Einsatzarten. Diplomarbeit Abteilung für Militärwissenschaften, Militärische Führungsschule, ETH Zürich 1996
- Arquilla, J. und Ronfeldt, D.: Cyberwar is Coming. Comparative Strategy, 12, 141-165, 1993
- Arquilla, J. und Ronfeldt, D.: The Advent of Netwar. Santa Monica. 1996
- Bortloff, N.; Henderson, J.: Notice and take-down agreements in practice in Europe. Views from the Internet Service Provider and Telecommunications industries and the recording industry. WIPO Document OSP/LIA/3. December 1, 1999
http://www.wipo.int/eng/meetings/1999/osp/doc/osp_lia3.doc
- Bundesamt für Sicherheit in der Informationstechnik - BSI (Hrsg.): Informationstechnische Bedrohung für Kritische Infrastrukturen in Deutschland. Kurzbericht der Ressortarbeitsgruppe KRITIS. Entwurfsversion 7.95. Bonn 1999
<http://userpage.fu-berlin.de/~bendrath/kritis-12-1999.html>.
- Cerny, D.: Schutz kritischer Infrastrukturen in Wirtschaft und Verwaltung. In: Geiger, G. (Hrsg.): Sicherheit der Informationsgesellschaft. Baden-Baden 2000
- Cohen, F. B.: Protection and Security on the Information Superhighway. New York 1995
- CSI (Ed.): Ninety percent of survey respondents detect cyber attacks, 273 organizations report \$265,589,940 in financial losses. Los Angeles 2000
http://www.gocsi.com/prelea_000321.htm
- Denning, D. E.: Information Warfare and Security. Reading 1999
- Der Spiegel: Killerprogramme bedrohen die Computerwelt. 15. Mai 2000 a
- Der Spiegel: Das Web im Fadenkreuz. 9. Februar 2000 b
- Der Spiegel: Norddeutscher Hacker legte Kölner Telefongesellschaft lahm. 21. Februar 2000 c
- Fiedler, H.: Der Staat im Cyberspace - Electronic Law Enforcement. Verwaltung und Management 6, 1, 4 - 6, 2000
- Geiger, G.: 'Cyberwar' und neue Strukturen der internationalen Sicherheit – Informationsdominanz als Faktor der internationalen Stabilität. Unveröffentlichter Arbeitsbericht der Stiftung Wissenschaft und Politik. Ebenhausen 1997
- Geiger, G. (Hrsg.): Sicherheit der Informationsgesellschaft. Baden-Baden 2000 a
- Geiger, G.: Information Warfare. Bedrohung und Schutz IT-abhängiger gesellschaftlicher Infrastrukturen. Datenschutz und Datensicherheit 24, 3, 129 - 135, 2000 b
- Geiger, G.: Information und Infrstruktursicherheit. Grundzüge eines sicherheits- und technologiepolitischen Forschungs- und Entwicklungsprogramms. SWP - AP 3130. Ebenhausen 2000 c
- 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)
- G 8 (Ed.): Communique Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime. Moscow, October 19-20, 1999.
<http://www.dfait-maeci.gc.ca/foreignp/g7/1999/moscow1-e.htm>
- Hartmann, J.; Pohl, H.: IPsec - der Standard für Virtual Private Networks (VPN). To be published. 2000a
- Hartmann, J.; Pohl, H.; Schlichting, J.: Evaluierung IPsec-basierter Virtual Private Network Produkte. To be published. 2000b
- Heartsoft (Ed.): Safari. http://www.heartsoft.com/press_releases/1999/pr-6-17-99.html
- Heise (Hrsg.): Programm zur Erkennung relevanter kinderpornografischer eindeutiger Objekte. 1999 <http://www.heise.de/tp/deutsch/inhalt/te/1363/1.html>
- Lessing, G.: Parameterspezifische Schwachstellenanalyse – Basisfunktionalität in ge-

- schotteten Produktionsstätten. In: Bauknecht, K.; Büllsbach, A.; Pohl, H.; Teufel, S. (Hrsg.): Sicherheit in Informationssystemen. Zürich 1998
- Lessing, G.: Festlegung von Sicherheitsniveaus. Arbeitsbericht. Berlin 1999
- Libicki, M. C.: Defending the National Information Infrastructure. Oktober 1996 <http://www.ndu.edu/ndu/inss/actpubs/niitemp.html>
- Libicki, M. C.: What is Information Warfare. Oktober 1996 <http://www.ndu.edu/ndu/inss/actpubs/act003/a003ch00.html>
- Naumann, M.: Bestimmung von Sicherheitsniveaus in Cascaded Infrastructure Security Systems (CISS) auf der Basis des Schutzzonenmodells. To be published.
- 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.: Nationale und internationale Umfragen zur Informationssicherheit. Arbeitsbericht. Frankfurt 1998
- Pohl, H.: Business Information Warfare - Elektronische Kriegführung zwischen Unternehmen. In: Geiger, G. (Hrsg.): Sicherheit der Informationsgesellschaft. Baden-Baden 2000
- Pohl, H.; Cerny, D.: Information Warfare: Der Krieg im Frieden. In: Bauknecht, K.; Büllsbach, A.; Pohl, H.; Teufel, S. (Hrsg.): Sicherheit in Informationssystemen SIS '98. Zürich 1998
- Roßnagel, A.; Wedde, P.; Hammer, V.; Pordesch, U.: Die Verletzlichkeit der 'Informationsgesellschaft'. Opladen 1989
- Hartmann, J.; Pohl, H.: IPsec - der Standard für Virtual Private Networks (VPN). To be published. 2000a
- Hartmann, J.; Pohl, H.; Schlichting, J.: Evaluierung IPsec-basierter Virtual Private Network Produkte. To be published. 2000b
- TCP/IP GmbH (Hrsg.): Stellungnahme zum Rights Protection System des Phonoverbandes. 17. März 2000
- Weizsäcker, R.: Gemeinsame Sicherheit und Zukunft der Bundeswehr. Bericht der Kommission an die Bundesregierung. Berlin 2000

- - - o o o - - -