Information Warfare
Der Krieg im Frieden

Thesen für eine Podiumsdiskussion

H. Pohl und D. Cerny

Die gezielte Ausnutzung der Verletzlichkeit der Informationsgesellschaft zur Durchsetzung von wirtschaftlichen und politischen Interessen durch Einzelne, Gruppen, Organisationen, Institutionen oder Nationen wird im amerikanischen Sprachgebrauch als Information Warfare - als Kriegführung mit Mitteln der Informationstechnik gegen Informationssysteme und gegen Informationsinfrastrukturen - bezeichnet. Die folgenden Thesen sollen Grundlage der Diskussion sein.

1 Die heutige Gesellschaft ist weitgehend auf die Informationsverarbeitung angewiesen, diese Entwicklung ist nicht umkehrbar.

Die Informationsverarbeitung mit Informations- und Kommunikationstechnik (Informationsinfrastrukturen) bestimmt zunehmend das wirtschaftliche Zusammenwirken und das soziale Zusammenleben in unserer Gesellschaft. Die moderne Informationsgesellschaft von Unternehmen, Behörden und Privaten mit Produktions-, Verwaltungs- und Distributionsprozessen ist nur handlungsfähig, wenn Informationsverarbeitung in breitem Maße zur Verfügung steht und ist damit darauf angewiesen, daß Informationen korrekt, zeitgerecht und zuverlässig, weitgehend ungestört und ausfallsicher dort zur Verfügung stehen, wo sie gebraucht werden.

Ohne verfügbare Informationsverarbeitung muß ein Unternehmen binnen weniger Tage seinen Betrieb einstellen und die Mitarbeiter entlassen. Betrifft der Ausfall von Informationssystemen die gesamte Bundesrepublik oder wesentliche Teile, so muß binnen 3 Tagen mit Versorgungsengpässen und als Folge davon mit Plünderungen und Unruhen gerechnet werden sowie weiterhin mit Toten wegen fehlender Lebensmittel, Energieversorgung etc.

Als konkretes Beispiel soll hier nur die Manipulation von Rechensystemen zur Steuerung der Stromversorgung in Europa genannt werden. Derartige Angriffsszenarien gehen deutlich über die klassische Sabotage, die Wirtschaftsspionage und auch die politische Spionage hinaus.

2 Trotz der Verbesserung der Sicherheitseigenschaften der IuK-Systeme hat die Verwundbarkeit nur geringfügig abgenommen, die Sicherheitsmaßnahmen sind unzureichend.

Verwundbarkeit

Die vorhandene Verwundbarkeit der Informationsverarbeitung in Unternehmen und Behörden sowie der benutzten Kommunikationsinfrastruktur mit für Unberechtigte öffentlich zugänglichen Netzen stellt ein Gefährdungspotential dar, dessen gezielte Ausnutzung zur Durchsetzung von wirtschaftlichen und politischen Interessen durch Einzelne, Gruppen, Organisationen, Institutionen oder Staaten technisch und personell bereits seit Jahren möglich ist (heutzutage zwar noch sehr punktuell aber schon praktiziert wird) und für

Erschienen in:
Bauknecht, K.; Büllesbach, A.; Pohl, H.; Teufel, S. (Hrsg.): Sicherheit in Informationssystemen. Zürich 1998

die Zukunft als weltumgreifendes Vorgehen allgemein als wahrscheinlich angesehen wird.

Informationssicherheit bei Unternehmen und Behörden unzureichend

Unternehmen und Behörden werden zunehmend ein Ziel IT-gestützt geführter Auseinandersetzungen. Die unterstützenden IT-Systeme werden damit bei einem Information Warfare Ziele hoher Priorität. Die Bedeutung, die die IT dadurch erlangt und die Bedrohung, der sie dadurch ausgesetzt ist, erfordern eine neue Qualität des Umgang mit den Schutzmechanismen. Die Art und Weise, wie bisher IT-Sicherheit betrieben wurde, reicht nicht mehr aus.

Passive Maßnahmen wie die klassische Zugriffskontrolle mit Berechtigungstabellen, Paßwörtern und Firewalls (Filterrechner, die den ein- und ausgehenden Datenstrom hinsichtlich bestimmter Parameter wie Adressen des Absenders und Empfängers, verwendetes Protokoll etc. auf Berechtigung filtern) sind nur ein allererster Schritt – gegen Information Warfare aber völlig unzureichend.

Aktive Maßnahmen wie der Einsatz der digitalen Signatur und der Überprüfungsmöglichkeit durch Zertifizierungsstellen und einer Sicherungsinfrastruktur sind Voraussetzung aller Überlegungen zur Informationssicherheit.

Kommunikationsnetze sind verwundbar

Das derzeit genutzte Adress-System des Internet kann (erfahrungsgemäß) leicht lahmgelegt werden. Generell sind die genutzten Protokolle unter Sicherheitsaspekten nicht nachweisbar sicher und gegen Angriffe nicht resistent.

Diese Verwundbarkeit gilt im Grunde auch für die "klassischen" Medien wie Telex, Telefon, Fax, Rundfunk und Fernsehen.

3 Das Ziel zukünftiger Angriffe ist der Zugriff auf die Information des Gegners und nicht die Vernichtung seiner Infrastruktur

Angriffsweisen

Angriffe mit Mitteln der Informationstechnik sind verhältnismäßig einfach durchzuführen. Diese Mittel, wie z.B. PCs, sind billig und stehen global zur Verfügung. Aufgrund der zunehmenden weltweiten Vernetzung der Informationsinfrastrukturen sind damit programmgesteuerte Angriffe möglich, die für den Angreifer gefahrlos weit entfernt vom eigentlichen Ziel eingeleitet werden können. Mit geringem Risiko läßt sich also ein hoher Schaden erreichen.

Die Angriffsweise im Rahmen eines Informationskrieges kann wie folgt charakterisiert werden: An die Stelle früher isoliert geführter Angriffe auf einzelne Komponenten einer Informationsinfrastruktur bedroht nun der strategisch geplante Einsatz von Mitteln der Informationstechnik die Informationsversorgung eines gesamten Unternehmens, eines Staates oder Staatenbundes.

Angriffsziele

Es ist gar nicht erforderlich, Informationsverarbeitung zu blockieren oder Informationen zu zerstören. Viel kritischer für den Angegriffenen und wirkungsvoller für den Angreifer (auch weil vom Angegriffenen schwerer zu erkennen) ist es, Informationen (unbemerkt) zu modifizieren oder ihre Verfügbarkeit graduell einzuschränken.

Beides führt - neben dem direkten Schaden - zu einem nachhaltigen Verlust von Vertrauen in die Integrität der informationellen Ressourcen des Angegriffenen und behindert damit seine jeweiligen Steuerungs- und Entscheidungsprozesse – und zwar unabhängig davon, ob der jeweilige Angriff tatsächlich erkannt oder nur vermutet wird.

Angriffsverfahren

Es wird zunehmend mit intelligenten (programmgesteuerten) Angriffen zu rechnen sein: Z.B. sog. Würmer oder Agenten (ausführbare Programme) mit einer Reihe von Schadensfunktionen, die heute einzeln bei Viren vorhanden sind, aus der je nach Situation eine Schadensfunktion (Manipulation, Löschen) ausgewählt wird. Oder auch Implementierung undokumentierter Schadensfunktionen in kommerzielle Produkte.

4 Die Verantwortlichen für die Innere (Zivilschutz) und Äußere Sicherheit (Landesverteidigung) müssen umdenken

Militärische Maßnahmen, wie Überschreitung von Landesgrenzen oder Einsatz von Waffensystemen, sind nicht mehr zwingend notwendig. Vor dem Hintergrund dieser Möglichkeiten erweitert sich auch das Spektrum der potentiellen Angreifer: Neben Staaten kommen nun auch Organisationen, Industriekonzerne und sogar einzelne Interessengruppen als Angreifer in Frage, wobei die Gründe für einen Angriff eben politischer, wirtschaftlicher oder weltanschaulicher Art sein können.

Selbst kleinere (z.B. sog. substate groups wie die IRA oder islamische Gruppen) oder sehr kleine Gruppen können sich solche Angriffe „leisten“ oder zumindest damit drohen (Erpressung), wenn sie in der Lage sind, das zugehörige technische Know-How aufzubauen.

Bei zukünftigen Auseinandersetzungen zwischen Staaten bieten sich Angriffe auf die Informationsinfrastruktur also deswegen an, weil sie kostengünstig, risikoarm und erfolgversprechend sind. Jedoch wird ein reiner Information Warfare zwischen Staaten gegenwärtig (unbegründet!) noch nicht für wahrscheinlich gehalten.

Die Bundesregierung hat mit diesem Umdenkungsprozeß begonnen, das Bundesministerium des Innern hat bereits eine interministerielle Arbeitsgruppe eingerichtet.

5 Die Unternehmen sind sich der Bedrohung durch einen Angriff auf ihre Informationsinfrastruktur bisher nicht bewußt

Bei zukünftigen Auseinandersetzungen zwischen Unternehmen und zwischen Organisationen bietet sich ein Angriff auf die Informationsinfrastruktur der Unternehmen an, weil derartige Angriffe kostengünstig, risikoarm und wirkungsvoll durchgeführt werden können. Jedoch wird dies von Unternehmen gegenwärtig noch nicht für wahrscheinlich gehalten – jedenfalls von deren Mitarbeitern nicht fürs eigene Unternehmen – jedoch durchaus für andere Unternehmen und Mitbewerber: 'So schlimm wird’s schon nicht kommen. Und wenn, wird es wohl die anderen treffen.'

Tatsächlich haben sich Unternehmen und Verbände mit dem Thema Information Warfare überhaupt noch nicht beschäftigt.

6 Unsere Informationsgesellschaft ist auf einen Informationskrieg und seine Folgen nicht vorbereitet

Neben einer allgemeinen Aufklärung breiter Bevölkerungskreise über die Gefahren durch einen Informationskrieg muß insbesondere der Aus- und Weiterbildung der Endanwender und der Administratoren besondere Aufmerksamkeit geschenkt werden.

7 Das rechtliche Instrumentarium zur Behandlung konventioneller Auseinandersetzungen reicht für die Behandlung von Informationskriegen nicht mehr aus

Sowohl die gängigen Festlegungen des Völkerrechts als auch des Kriegsvölkerrechts reichen nicht mehr aus. Alle derartigen Vereinbarungen und Regelungen müssen daher dringend aktualisiert werden.

8 Zur Bewältigung der Probleme ist ein Bündel von Maßnahmen notwendig, die in enger Zusammenarbeit zwischen allen Beteiligten eingeleitet und durchgeführt werden müssen

Die Kenntnis der Verletzlichkeit heutiger Informationsinfrastrukturen und der möglichen Bedrohungen, denen sie ausgesetzt sein können, erfordert neben der Erkennung sowie einer objektiven Bewertung der Gefährdung auch umfangreiche Überlegungen zum Schutz- und entsprechende Gegenmaßnahmen, die über das lückenhafte Maß gegenwärtiger IT-Sicherheitsmaßnahmen weit hinausgehen.

Informationswertanalyse, Schwachstellen, Sicherheitsarchitektur

Zum Schutz gegen die Angriffe und Folgen eines Informationskrieges muß zunächst festgelegt werden, welche Teile einer nationalen Informationsinfrastruktur „lebenswichtig“ und damit besonders schützenswert sind. Die gegenwärtigen Schwachstellen müssen ermittelt und eine angemessene die Bundesrepublik vollständig (!) abdeckende Sicherheitsarchitektur (integrierte Maßnahmen) muß erarbeitet und implementiert werden.

Das gilt gleichermaßen für die Informationsstruktur von Unternehmen insbesondere dann, wenn sie Dienste oder Produkte zur Verfügung stellen, die für die Gesellschaft lebenswichtig sind.

Indikatoren

Für die Erkennung eines Informationskrieges (Beginn, Durchführung, Ende) fehlen bisher geeignete Indikatoren. Eine besondere Bedeutung gewinnt deshalb die Sammlung und Auswertung über erkannte Angriffe auf Informationsinfrastrukturen und Einbrüche in Systeme. Derartige Erkenntnisse könnten wesentlich dazu beitragen, ein Gesamtlagebild zu gewinnen. Ohne ein solches Lagebild werden Schutzmaßnahmen für eine Informationsinfrastruktur (sowohl auf Unternehmensebene als auch auf staatlicher Ebene) weitgehend wirkungslos bleiben.

Kontrolle und Beobachtung

Im technischen Bereich müssen Überlegungen dahingehend angestellt werden, auf welche Weise und in welchem Umfang Angriffe - nach Möglichkeit automatisiert und programmgesteuert – erkannt und abgewehrt werden können.

Intrusion Detection Systeme sind hier nur ein erster Ansatz, der allerdings – zwar nicht nur IT-System-bezogen sondern netzweit und insbesondere in der Globalen InformationsInfrastruktur (GII) - weiterverfolgt werden muß.

Internet und GII

Die derzeitige Abhängigkeit von dem Internet muß unverzüglich weltweit überprüft werden. Jegliche zentrale Abhängigkeit ist zu vermeiden. Nationale Monopole durch Reglementierung und Sicherheitsstrategien und Hersteller- und Anbietermonopole sind zu vermeiden. Standards und Normen sind hinsichtlich ihres Sicherheitsniveaus zu überprüfen.

Kooperation und Aufgabenteilung

Eine enge Zusammenarbeit zwischen den gesellschaftlichen Gruppen und Wissenschaft, Wirtschaft und Regierung bei all diesen Fragen ist unbedingt erforderlich, eine internationale Abstimmung ist unumgänglich.

Die gegenwärtige Aufteilung der Aufgaben zwischen Staat und Wirtschaft zum Schutz der Gesellschaft muß vor dem Hintergrund eines Information Warfare überprüft werden.

Produkte und politische Einflußnahme

Die hier nur beispielhaft genannten technischen Sicherheitsmaßnahmen bekommen ein neues Gewicht insbesondere vor dem Hintergrund des zunehmenden Einsatzes kommerzieller Produkte (commercial off the shelf). Da die US-Regierung mit massiven Entwicklungsforderungen und auch der notwendigen Unterstützung handelt, dürften in spätestens 3 Jahren Produkte auf dem Markt sein, die das Informationssicherheitsniveau massiv anheben.

Allerdings werden es US-amerikanische Produkte sein. Damit wird in Deutschland und Europa die bereits in der Vergangenheit mehrfach bemängelte wirtschaftliche Abhängigkeit vom Ausland und die generelle Abhängigkeit im Sicherheitsbereich noch stärker.

Die Frage der Sicherheit einer Informationsinfrastruktur muß daher insbesondere vor dem Hintergrund des Einsatzes von Komponenten (Soft- und Hardware) bewertet werden, die von ausländischen Herstellern geliefert werden.

Ganzheitlicher Ansatz der Informationssicherheit

Informationstechnik muß inhärent sicher erstellt werden und nicht erst im nachhinein sicher 'gemacht' werden. Das bedeutet notwendig Grundlagenforschung und -Entwicklung sicherer Systeme i.S. verifizierbarer Systeme – angefangen vom Design bis hin zur Implementierung und Installation in einer Umgebung mit weiterer Hard- und Software und in Netzen eines Unternehmens. Dies muß vorrangig für Systeme realisiert werden, die Leib und Leben von Menschen tangieren.

Situation in den USA

In den USA hat Präsident Clinton bereits 1995 die Einsetzung einer Kommission "Critical Infrastructure Protection" angeordnet, die binnen eines Jahres einen „National Information Warfare Defense Plan“ ausgearbeitet hat, der die Grundlage für den Schutz der amerikanischen nationalen Informationsinfrastruktur gegen Angriffe von Terroristen und gegen Angriffe von außerhalb bilden soll. Die Mittel für Forschungs- und Entwicklungsarbeiten zur Sicherung und Verbesserung der Überlebensfähigkeit der Informations- und Kommunikationssysteme sollen bis zum Jahr 2004 auf insgesamt 1 Mrd. US$ aufgestockt werden.

Zusammenfassung

Wir sind in Deutschland und Europa auf die skizzierte Situation des Information Warfare nicht vorbereitet, weder politisch noch technisch oder organisatorisch noch im Bereich des Rechts. Es bereitet sich auch keiner vor. Wir wissen überhaupt nicht wie wir uns vorbereiten könnten und wir wissen erst recht nicht, wie wir reagieren könnten oder sollten.

Angesichts der in Deutschland und Europa vorhandenen Kompetenz in Fragen der Informationssicherheit erscheint es äußerst dringend, Verfahren und Produkte zur Erkennung, Beobachtung und Abwehr in gesellschaftlichem Konsens zwischen Politik, Unternehmen und Wissenschaft zu entwickeln und zu testen, die national und in der Europäischen Union genutzt werden können.

Allerdings wird in Deutschland wahrscheinlich erst dann etwas konstruktives geschehen, wenn einschlägige Produkte aus anderen Ländern – insbesondere den USA – sich dort auf dem nationalen Markt durchgesetzt haben und in Deutschland angeboten werden [so wie bei Firewalls, Recovery Center etc.]. Die EU-Kommission wird dann den Import reglementieren.