Computerspionage: Ist die Katastrophe unvermeidbar?

Hartmut Pohl und Ludger Hütte[1]

Am 2. März diesen Jahres [1989] hat das Bundeskriminalamt (BKA) aufgrund der Ermittlungen des Generalbundesanwalts eine ganze Reihe von Wohnungen in Hamburg, Hannover, Karlsruhe und Berlin durchsucht und mehrere Personen wegen des Verdachts der geheimdienstlichen Agententätigkeit für eine fremde Macht festgenommen. Noch am selben Abend berichtete das NDR-Magazin 'Panorama' ausführlich über die jahrelangen Aktivitäten von Hackern, die im Auftrag des KGB mit den modernsten Methoden Computer von Unternehmen und Behörden in der westlichen Welt über öffentliche Netze erfolgreich angegriffen, gespeicherte Daten ausspioniert und an den KGB weitergegeben hatten. Weitere Darstellungen dieses sog. KGB-Falls finden sich u.a. in [Ammann et al. 1989] und aus US-amerikanischer Sicht in [Stoll 1989].

Der Präsident des Bundesamtes für Verfassungsschutz Gerhard Boeden erklärte dazu: 'Wenn sich ... der vorliegende Verdacht bestätigt, haben wir es hier ... mit einer neuen Qualität gegnerischer Ausspähung unserer Datennetze zu tun. Das heißt mit anderen Worten, daß wir zwar mit einem solchen Versuch gerechnet haben, aber dennoch sehen müssen, daß man hier eine konsequente Ausnutzung aller technischen Möglichkeiten zum Eindringen in unsere Datennetze genutzt hat.'

Es müßte als falsch bezeichnet werden, diesen Fall als den ersten nachrichtendienstlich gesteuerten Computerspionage-Fall zu bezeichnen: Es war gewiß der erste bekannt gewordene Fall – über andere ist nichts veröffentlicht. Und es wird wohl niemand glauben, daß es der letzte Fall von Computerspionage war.

Die nachrichtendienstliche Steuerung jugendlicher Hacker hat in jüngster Zeit neben Unternehmen, Behörden insbesondere die Öffentlichkeit aufgeschreckt. Mit diesem Fall von Computerspionage ist die Problematik also nur erstmals einer breiteren Öffentlichkeit deutlich geworden. Zunehmend fragen sich insbesondere die leitenden Mitarbeiter in Unternehmen, ob ihre Daten denn überhaupt sicher sind gegen derartige Angriffe auf die Datenverarbeitung durch professionell-arbeitende Computerspione.

Die zu dem Fall von Computerspionage vom Bundesinnenministerium veröffentlichten Informationen brauchen nicht bewertet zu werden, sie sprechen für sich:

- Es ist ein international agierender Computerspionage-Ring zerschlagen worden.
- Dabei wurde eine neue Dimension der Spionage östlicher Nachrichtendienste aufgedeckt: Alle Möglichkeiten moderner Informationstechnik wurden rigoros und konsequent ausgenutzt, um in westliche Datennetze und Computersysteme einzubrechen.
- Angriffsziele (waren und) sind hunderte oder sogar tausende (!) Computer von Militär- und Forschungseinrichtungen – vornehmlich aber von Unternehmen und Wissenschaftsinstitutionen.
- Die besondere Dimension der Spionage stellt neue Anforderungen an die Abwehrmechanismen; diese Form der Spionage tritt neu zu der unverminderten Bedrohung durch die klassischen Methoden der nachrichtendienstlich gesteuerten Ausspähung.
- Die Bundesregierung hat diese Gefahren bereits vor Jahren erkannt und entsprechende Maßnahmen ergriffen.

Aber an diese Gefahr hat natürlich bisher kaum einer geglaubt – obwohl Computerspionage und Computersabotage Tag für Tag in und zwischen Unternehmen betrieben wird. Eine unangenehme Tatsache. Und: Die Spione sitzen nicht nur – aber natürlich auch – im Osten. Die 'normale' Wirtschaftsspionage ist (meist) den Unternehmensleitungen gar nicht bekannt: Konkurrenzunternehmen scheuen im Einzelfall keine Mühe und meist auch keine Kosten, frühzeitig Informationen über neue Entwicklungen der Mitbewerber zu erhalten. Bereiche, die hierunter zu leiden haben, sind in Deutschland neben den Behörden und Unternehmen, die mit der Entwicklung von Rüstungsgütern beauftragt sind (Jäger 90, Fregatte 90, intelligente Munition etc.) insbesondere der Pharmabereich inklusive der Gentechnologie, die Automobilbranche und natürlich die IT-Industrie.

Verständlicherweise werden diese Fälle von den betroffenen Unternehmen gern verschwiegen, um einen Vertrauensschaden bei Kunden und Zulieferern zu vermeiden, der weit höher als der direkte Schaden wiegen würde. Denken wir nur an Dienstleistungsunternehmen wie Geldinstitute und Versicherungen.

Wenn wir den Veröffentlichungen von Panorama und Spiegel Glauben schenken wollen, waren in diesem Fall die Forschungs- und Entwicklungsbereiche der größten deutschen Industrieunternehmen unter den Opfern des KGB.

---

[1] DV-Sicherheitsberater, Köln
Der Beitrag ist erschienen in: Journal für Wirtschaft und Gesellschaft – bonntendenz 4, III 1989

Naturgemäß dementierten fast alle in der Öffentlichkeit genannten Behörden und Unternehmen, Angriffsobjekt gewesen zu sein; und wenn doch, dann waren keinerlei zu schützende Informationen auf den Rechnern; es kann davon ausgegangen werden, daß dies in der überwiegenden Zahl der Fälle reine Schutzbehauptungen sind.

Hier soll nicht im Detail dargestellt werden, welche Folgen der Know-how-Diebstahl für ein Unternehmen hat. Hier soll aber einmal deutlich darauf hingewiesen werden, welche Folgen die Wirtschaftsspionage international operierender Mitbewerber für den Einzelnen, den Mitarbeiter hat: Aus der Spionage und dem daraus resultierenden Umsatz- und Gewinnverlust des Unternehmens folgt unmittelbar die Gefährdung von Arbeitsplätzen!

Eine ganze Reihe von Fällen, in denen insbesondere mittelständische Unternehmen durch Spionage in eine Schieflage gerieten bis hin zur Schließung von Teilbereichen der betroffenen Unternehmen sind Eingeweihten bekannt. Betrachtet man die in diesem Fall von nachrichtendienstlich-gesteuerter Computerspionage offensichtlich gestohlenen Dateninhalte, so lassen sich drei Bereiche erkennen:

- In erster Linie wurde Software wie Betriebssysteme, Datenbanksysteme und Compiler etc. kopiert und damit gestohlen.
- In zweiter Linie Programme und Daten zur Chipentwicklung und -Produktion.
- In dritter Linie personenbezogene Daten und Unternehmensdaten aus Banken.

Welcher Aspekt davon der entscheidendere ist sei dahingestellt. Der erste, Betriebssysteme, Datenbanksysteme und Compiler zu stehlen, kann noch als 'normal' bezeichnet werden; der Wert dieser Daten erscheint überschaubar.

Zum zweiten Bereich gilt folgendes: Die Entwicklung, Herstellung und der Vertrieb von Computerchips wird in den 90er Jahren weltweit ein Marktvolumen von 45 Milliarden US Dollar erreichen, den die führenden Technologieunternehmen bereits seit Jahren vorbereiten; allein die Investitionen europäischer Kooperationspartner werden etwa 7.3 Milliarden DM betragen, die übrigens überwiegend in Bayern investiert werden sollen. Der Forschungs- und Entwicklungsaufwand asiatischer (nicht nur japanischer), europäischer und US-amerikanischer Unternehmen muß insgesamt in zweistelliger Milliardenhöhe angegeben werden.

In diesem Bereich Know-how auszuspionieren, hat dem Auftraggeber der Spionage weit mehr als einige Millionen Entwicklungskosten erspart. Dabei geht es selbstverständlich nicht nur um die Ergebnisse der Grundlagenforschung, die Entwicklung von Computerchips, sondern auch um die Verfahren zur Serienherstellung. Insider wissen, daß die Silizium-Technik ausgereizt erscheint und die Zukunft im Bereich der Gallium-Arsenid-Technik liegt. Zu dieser Technologie wurden Programme zur Entwicklung und Produktionssteuerung hochintegrierter Chips, den Bauteilen von Computern, ausspioniert.

Während die ersten beiden Bereiche Wirtschaftsspionage darstellen, ist der dritte von primär nachrichtendienstlichem Wert: Personenbezogene Daten ermöglichen einem Nachrichtendienst, für ihn in der Sache relevante (Mitarbeit an bestimmten Forschungs- und Entwicklungsprojekten) und für seine Anwerbungsbemühungen (human intelligence) anfällige Personen ausfindig zu machen. Vergleichbares gilt für Unternehmensdaten; hier erfährt der Nachrichtendienst, welche Firmen finanziell nicht so gesund dastehen; in diesen Fällen wird in Abhängigkeit vom Know-how des Unternehmens geprüft, in wie weit eine – evtl. getarnte – Beteiligung für ein Staatshandelsland sinnvoll sein könnte.

Angriffe auf die Informationsverarbeitung

Neue technische Entwicklungen wecken das Interesse nicht nur von internationalen Konkurrenzunternehmen sondern insbesondere das der Staatshandelsländer des kommunistischen Machtbereichs. Einige dieser Länder habe eine ganze Bürokratie aufgebaut, um illegale Technologiebeschaffung zu planen und zu realisieren. Die Anforderungen der 'Unternehmen' werden zentral gesammelt und nach Prioritäten für die Rüstungsindustrie und Volkswirtschaft an die zentral beschaffende Organisation – dies sind die jeweiligen östlichen Nachrichtendienste – weitergeleitet. Eine besondere Bedeutung kommt hier der mehrfach-verwendbaren (dual-use) Technologie zu, die sowohl im Rüstungsbereich als auch in Unternehmen verwendet werden kann: Computerhardware und -programme.

Informationstechnik und Informationsverarbeitung spielen im Wirtschaftsleben seit fast 30 Jahren eine zunehmend stärkere Rolle. Die Innovationsgeschwindigkeit in diesem Bereich ist außerordentlich hoch. Die Speicher- und Rechenleistung, die vor 25 Jahren in Großrechenzentren installiert war, steht heute als Personal Computer auf dem Schreibtisch eines jeden Mitarbeiters.

Wir haben einen Stand der Technik erreicht, der eine weltweite Kommunikation zwischen unseren Computern ermöglicht. Am Arbeitsplatz werden Bürokommunikation und lokale Netze genutzt. Die Steuerung von Produktionsprozessen läuft rechnergestützt ab. Computer sind in der Lage, über Telefon- oder Datenleitungen – auch weltweit – miteinander zu kommunizieren; Unternehmen und Verwaltungen sind heutzutage so weltweit vernetzt. Hochintegrierte Schaltkreise und Computer werden in Waffensystemen und in intelligenten Waffen installiert.

Der Westen hat sich gegen die praktizierten Formen der Wirtschaftsspionage und des Technologiediebstahls durch die COCOM-Vereinbarungen zu schützen versucht. Allerdings mit mehr oder weniger großem Erfolg, wenn man an die Fälle illegalen Technologietransfers von Müller und Bruchhausen [CIA 1985] denkt.

In allen diesen Fällen wurde von den gegnerischen Nachrichtendiensten ein Honorar gezahlt, das den Marktwert der Lieferungen im Einzelfall um das vier- bis fünffache überstieg. Bei Materiallieferungen in der Größenordnung von 3 bis 10 Mio. DM hat der Täter als 'Honorar' einen durchaus interessanten Agentenlohn erzielt.

Dies gilt auch für den Diebstahl von Daten und Programmen aus Computern. Sicherlich ist dies ein verführerisches Angebot, für einen Täter wie einen Operateur eines DV-Systems, der zum Kopieren (und das ist der Diebstahl, die Spionage) eines Programms auf Magnetband etwa eine (unbeobachtete) Stunde benötigt.

Wie leicht zugänglich auch sehr wertvolle Informationen in Computern und Datenbanken sind, ist auch für den Experten immer wieder verblüffend. Der Know-how-Diebstahl durch Eindringen in Computer über öffentliche Netze wie Datex-P und auch Telefonleitungen, das sogenannte Hackerproblem, ist seit mehr als 10 Jahren in Fachkreisen bekannt. Zuerst wurde es in den USA praktiziert – wegen der weit stärkeren Vernetzung der Computer über öffentlich zugängliche Netze nicht verwunderlich.

Heutzutage werden Daten und Programme weltweit über Leitungen via Satelliten und Richtfunkstrecken übertragen. Unternehmen lassen Daten in Niedriglohnländern erfassen und über Satellit in ihr Stammhaus senden. Programme werden ebenfalls in Niedriglohnländern entwickelt und dem Auftraggeber über von Dritten abhörbare Leitungen zugesandt.

Modus Operandi der Computerspionage

Bereits in dem im Herbst 1987 bekannt gewordenen sog. NASA-Fall sind die Täter von ihrem Personal Computer in ihrer Wohnung über einen örtlichen Großrechner einer Universität oder einer Forschungseinrichtung in das Space Physics Analysis Network (SPAN) eingedrungen, das DV-Systeme Westeuropas mit denen der USA verbindet.

Dieser Fall muß heute in einem ganz anderen Licht gesehen werden. Die Hacker aus dem sog. KGB-Fall haben wohl von 1986 bis mindestens 1988 für den KGB gearbeitet. Eine Verbindung zwischen den damaligen Tätern des NASA-Falls und denen des KGB-Falls kann nicht ausgeschlossen werden, wenn nicht sogar von denselben Tätern ausgegangen werden kann.

Über die vielfältigen Möglichkeiten der Computerspionage anzudeuten, soll hier kurz ein technischer Angriffsverlauf auf Systeme der Informationsverarbeitung dargestellt werden.

Hacker besitzen häufig nur einen sehr kleinen Computer im Wert von etwa DM 2.000.- Auf diesem kleinen Computer wird ein Angriffsprogramm entwickelt, das über einen Akustikkoppler oder Modem und Telefonanschluß auf einen örtlichen Großrechner überspielt wird. Dies dauert nur wenige Minuten und kostet wenige Zeittakte Telefongebühren. Der örtliche Großrechner wird nun mit Hilfe des übertragenen Programms so manipuliert, daß er programmgesteuert andere an öffentliche Netze angeschlossene Computer angreift.

Von derartigen Angriffsrechnern – sie standen im KGB-Fall in Hamburg, Bremen, Hannover und Karlsruhe, aber wohl auch in England, dem nahen und fernen Osten (!) – wurden weltweit weitere Rechner angegriffen; so in Deutschland (!), aber auch in der Schweiz, Frankreich, England, Singapur, Japan und den USA.

U.a. wurden auch Kernforschungsunternehmen erfolgreich angegriffen, in denen computergesteuerte Experimente gestört wurden; was dies für eine Kernforschungsinstitution bedeutet, braucht nicht weiter ausgeführt zu werden; auch wenn keine größeren Sabotageakte veröffentlicht sind.

Hacker hinterlassen häufig keinerlei auswertbare Spuren, die Rückschlüsse auf ihre Aktivitäten oder sogar ihre Identität zulassen; dies gilt auch für die angegriffenen Computer, in denen sie die Protokollierung so manipulierten, daß der Angriff und die Spionageaktivitäten nicht mitprotokolliert oder die Protokolle wurden nachträglich gelöscht wurden.

Es liegt in der Natur der Sache, daß das Spionieren durch Kopieren von Daten und Programmen auch keine Spuren hinterläßt; dem berechtigten Anwender stehen diese Daten ja nach wie vor zur Verfügung – im Gegensatz zur klassischen Wirtschaftsspionage, bei der Dokumente oder Produkte – zumindest kurzfristig – entwendet werden. Bewußt keine Spuren zu hinterlassen kann als nachrichtendienstliches Vorgehen bezeichnet werden.

Dies gilt auch für den vorliegenden Fall: Hacker haben die auf ihren Personal Computern gespeicherten Daten verschlüsselt, so daß sie nicht mehr unmittelbar lesbar sind; weiterhin haben sie Selbstzerstörungsmechanismen eingebaut, die aktiv werden, wenn sich ein 'Unbefugter' an ihren Daten zu schaffen macht: Diese Programme bewirken ein Löschen der Daten auf der Platte und Diskette, so daß der Inhalt nicht mehr lesbar ist.

Daher ist es auch nicht verwunderlich, daß Ermittlungsverfahren noch in keinem Fall zu einer Anklageerhebung geführt haben; wie überhaupt gilt, daß nach dem vom Bundestag beschlossenen und am 15. Mai 1986 verkündeten 2. Wirtschaftskriminalitätsgesetz noch kein Hacker verurteilt worden ist; und daß die Ermittlungen des hier im Mittelpunkt stehenden Spionagefalls derzeit noch gar nicht abgeschlossen sind. Diese Verfahren dürften sich auch ausgesprochen schwierig gestalten.

Auch wenn in diesem Fall von nachrichtendienstlich gesteuerter Wirtschaftsspionage ausgegangen werden kann: Weltweit sind Konkurrenzunternehmen und die Staatshandelsländer in der Lage, sich der dargestellten Hackermethoden zu bedienen – z.B. von einem beliebigen Telefonanschluß von einem beliebigen Ort auf der Welt aus; dieser muß nicht unbedingt im Osten stehen; er kann vielmehr auch

in Tokyo stehen oder an einer deutschen Autobahn. Gegnerische Dienste werden es i. allg. vermeiden, aus ihrem Land heraus zu hacken; sie werden sich vielmehr westlicher Hacker bedienen, um derartige Angriffe zu fahren; mindestens aber können sie sich des fachlichen Wissens und der Erfahrung der Hakker bedienen.

Die für die Angriffe und die interkontinentalen Transaktionen anfallenden Leitungskosten werden von der Deutschen Bundespost nicht dem Hacker sondern der den mißbrauchten Großrechner betreibenden Institution in Rechnung gestellt.

Wenn auch auf Netzen im allgemeinen in den übertragenen Informationspaketen sowohl die Zieladresse als auch die Absenderadresse mitübertragen wird, so sind die Täter gleichwohl nicht zu identifizieren, weil ihre Spur nur bis zum örtlichen Großrechner zurückverfolgt werden kann. Der Anrufer (Hacker) kann im Normalfall im Telefonnetz bekanntlich nicht identifiziert werden – es sei denn mit einer sog. Fangschaltung. Weiterhin haben die Hacker Verfahren genutzt, die auch bei den Datennetzen der Bundespost eine Rückverfolgung nicht erlauben.

Hier soll noch auf einen weiteren Aspekt eingegangen werden: Die Hacker haben vom Betreiber unbemerkt Mailboxen in Großrechnern installiert, um sich untereinander Informationen zuzuspielen. D.h. eine direkte – und evtl. kontrollierbare – Kommunikation zwischen den Tätern fand gar nicht statt.

Neu ist bei dieser Art der Spionage allerdings nur der Einsatz des technischen Mittels Informationstechnik. Typische Spionagemethode ist auch, einen Spion (Programmierer) in einer großen Behörde zu plazieren, die personenbezogene Daten verarbeitet: Hier können Informationen über weitere noch anzuwerbende Personen gesammelt werden.

Typisierung der Täter

Wenn hier von den Hackern berichtet wird, so steht dieser Begriff sicherlich nicht für einen homogenen Kreis von KGB-Spionen. Unter Tausenden von Computerenthusiasten sind sicherlich nur ganz wenige kriminell; viele sind darunter, die Telefonnummern von Computern sammeln wie andere Briefmarken; die also auf Computern gespeicherte Daten gar nicht anschauen.

Völlig falsch wäre allerdings der Eindruck, das Risiko eines Hackerangriffs drohe nur von außen über Daten- oder Telefonleitungen. Dieselben Methoden, die von den Hackern entwickelt wurden, können auch von dem sog. Innentäter – also dem Mitarbeiter – benutzt werden zur Sabotage und Spionage.

Die technischen Angriffe können natürlich auch von Innentätern, von Mitarbeitern der Unternehmen genutzt und angewandt werden auf lokale Netze und in der Bürokommunikation. Weil viele Mitarbeiter weitgehende Zugriffsrechte auf Daten und Programme besitzen, muß dieses Innentäter-Risiko als sehr viel höher eingeschätzt werden.

Der Fall zeigt, daß die Sekretärin, die wertvolle Dokumente in die Handtasche steckt und ihrem Führungsoffizier am Bonner Rheinufer übergibt, überflüssig geworden ist. In Zukunft wird sie Datenträger wie Disketten übermitteln – oder besser noch die Informationen über Leitungen übertragen.

Die fachliche Qualifikation der Täter muß ausgesprochen hoch bewertet werden; das zeigen die hochintelligenten Angriffsverfahren. Diese gehen so weit, daß Hacker von ihrer Wohnung aus Teile des auf dem Rechner des angegriffenen Unternehmens eingesetzten Betriebssystems austauschen. Der nächste Schritt kann nur noch sein, das ganze Betriebssystem auszutauschen. Im Einzelfall bedeutet dies, daß auch eine Verschlüsselung gespeicherter Daten nicht gegen Angriffe schützen muß, weil die genutzten Programme und/oder eingestellten Parameter längst gegen andere ausgetauscht worden sind.

Werden die Täter im Bereich der gesamten Computerkriminalität betrachtet, so wird erkennbar, daß zwar eine Reihe jugendlicher Freaks aktiv sind – aber gewiss nicht die Hauptrolle spielen. Überbewertet in der Öffentlichkeit und gleichermaßen in Sicherheitskreisen wird die Szene der Hacker, die sich zum Teil in Vereinen zusammengeschlossen hat. Hier sind jugendliche Computerenthusiasten am Werk, die in der weit überwiegenden Mehrzahl nur technisch interessiert sind, nicht im geringsten kriminelle Eigenschaften haben und politisch keineswegs als extrem bezeichnet werden können.

Die persönliche Integrität der Hacker wird allerdings nicht in allen Fällen unangreifbar sein. Sie erscheinen häufig von ihren Interessen her etwas eingeengt auf Datenverarbeitung. Die finanzielle Situation der Hacker ist meist schlecht, weil im Verhältnis zum Einkommen doch hohe Kosten für Geräte und Telefongebühren anfallen.

Typisch ist der KGB-Fall insofern, als persönliche Schwächen ausgenutzt wurden – so war Rauschgiftabhängigkeit im Spiel und natürlich allgemeiner Geldbedarf oder sogar Geldgier.

DV-Sicherheitsmaßnahmen

Der Bundesbeauftragte für den Datenschutz Dr. Alfred Einwag kommentierte den Fall im Hinblick auf die notwendigen Aktivitäten der Bundesregierung: 'Die Bundesregierung muß nachdrücklich darauf hinwirken, daß sich die Betreiber und die Benutzer (von Computern) Sicherheitsanforderungen nicht als lästig und unbequem abtun. Die technischen Sicherungsmöglichkeiten, die ja vorhanden sind, müssen auch genutzt werden. Die Betreiber müssen die Datensicherheit organisieren und die Benutzer müssen entsprechend geschult werden. Ich appelliere aber auch an die Computerhersteller, die Anwender auch im Hinblick auf Sicherheitsprobleme umfassend zu beraten.' Und auf die Frage, ob die bestehenden gesetzlichen Bestimmungen zum Schutz der Daten auf Computern der Bundesregierung ausreichen: 'Was fehlt sind nicht Gesetze, sondern ein si-

cherheitsbewußtes Verhalten. Jedem Mitarbeiter, der mit Computern arbeitet, muß klar sein, welche Folgen ein zu lockerer Umgang mit Daten und Programmen haben kann.'

Einwag hat recht; neuere Untersuchungen zur Sicherheit der US-amerikanischen – im Fall betroffenen – Systeme zeigen, daß Hacker ohne größeren Aufwand bei 13% der Systeme (immer noch) Daten ausspähen können. Um Größenordnungen wird es in Deutschland nicht anders sein.

Maßnahmen gegen derartige Risiken sind also eigentlich bekannt und am Markt vielfältig verfügbar. Gleichwohl zeigt auch dieser aktuelle Fall wieder, daß diese bekannten Maßnahmen vom Anwender häufig nicht eingesetzt werden – vgl. dazu die Forderungen des Bundesdatenschutzgesetzes.

Welche Schlüsse müssen wir ziehen und welche Sicherheitsmaßnahmen sollten wir ergreifen? Hier werden nur die drei wichtigsten Grundregeln der DV-Sicherheit genannt:

- Die Computer mit den wertvollsten Daten des Unternehmens dürfen nicht für jedermann zugänglich an (öffentliche) Netze angeschlossen werden.
- Alle Aktivitäten der Benutzer und Betreiber müssen minutiös protokolliert und diese Protokolle unter Sicherheitsaspekten (Mißbrauch wie Spionage und/oder Sabotage) ausgewertet werden.
- Daten müssen verschlüsselt werden. Unberechtigte und Diebe können sie dann nicht mehr lesen.

Mit den hier im Grundsatz genannten Absicherungsmaßnahmen lassen sich Systeme der Informationstechnik und Datenverarbeitung einschließlich der Netze ausreichend absichern.

Fazit: Die Katastrophe, ungeschützt der Computerspionage ausgeliefert zu sein, ist für jedes Unternehmen und jede Behörde vermeidbar.

Frühwarnsysteme und staatliche Maßnahmen

Die Bundesregierung hat – wie der Innenminister anläßlich der Zerschlagung dieses international operierenden Computerspionage-Rings mitteilte – diese Gefahren bereits vor Jahren erkannt und auf Initiative und unter Federführung des Bundesinnenministeriums eine Reihe von Maßnahmen getroffen.

Das Bundesinnenministerium hat ein 'Rahmenkonzept zur Gewährleistung der Sicherheit bei Anwendung der Informationstechnik' erarbeitet, das auf alle grundsätzlichen Sicherheitsaspekte im Zusammenhang mit der Informationstechnik eingeht. Es soll den Handlungsrahmen für die Bundesregierung bilden [BMI 1989].

Zwischenzeitlich wurden die 'IT-Sicherheitskriterien – Kriterien zur Bewertung der Sicherheit von Systemen der Informationstechnik (IT)' veröffentlicht [ZSI 1989]. Sie sollen als 'Meßlatte' zur Beurteilung der Sicherheit informationstechnischer Systeme dienen; anhand dieser Kriterien werden Systeme der IT auf ihre Sicherheit geprüft und bewertet. Folgen wird ein 'IT-Evaluationshandbuch'.

Zur Sensibilisierung der Anwender der Informationstechnik über die bestehenden Gefahren und um diese in die Lage zu versetzen, system- und anwendungsbezogene Sicherheitskonzepte zu entwickeln und zu realisieren, wird derzeit ein 'IT-Sicherheitshandbuch' erarbeitet.

Bereits jetzt ist für technische Angriffe gegen Einrichtungen der Informationstechnik z.B. durch Hakking oder Computerviren ein spezielles Kommunikations- und Warnsystem entwickelt worden.

Die Informationen werden zentral durch das Bundeskriminalamt gesammelt, das bei Bedarf und nach Abstimmung mit Spezialisten gezielte Warnmeldungen an Unternehmen und Behörden herausgibt.

Gerade die letztgenannten Frühwarnsysteme werden – wie die Beispiele in den USA bereits zeigen – von der Zahl her und ihrer fachlichen Ausrichtung her stark zunehmen. Anwender und Hersteller schließen sich zu Vereinigungen zusammen, um sich frühzeitig und gezielt über Angriffsversuche, Angriffe und Manipulationen in der Form einer Selbsthilfeeinrichtung gegenseitig zu informieren und zu helfen.

Auswirkungen auf außen- und friedenspolitische Diskussionen

Sicherheitskreise kommentieren den Fall von Computerspionage im Zusammenhang mit der außenpolitischen und Abrüstungsdiskussion auf die Frage nach den sich ändernden Aktivitäten des KGB im Zeitalter von Gorbatschows Glasnost und Perestroika: Politische Bewegungen haben überhaupt keinen Einfluß auf die nachrichtendienstlichen Aktivitäten und erst recht nicht auf die Aktivitäten sowjetischer Geheimdienste.

Internationale Computerkriminalität

Insbesondere Computerspionage und –Sabotage ist ein international praktiziertes Delikt – zwar zuerst in den USA, aber seit Jahren in der Bundesrepublik und inzwischen längst auch in Ländern Süd-Ost-Asiens und nicht zuletzt auch in der UdSSR.

Daß diese Wirtschaftskriminalität auch in Staatshandelsländern Bedeutung erlangt hat, zeigt u.a. das 5. Strafrechtsänderungsgesetz der DDR vom 14. Dezember 1988 [Pohl et al. 1990], das den Mißbrauch, den Diebstahl, den Betrug im Rahmen der Datenverarbeitung zum Nachteil sozialistischen, persönlichen oder privaten Eigentums, Daten- und Programmveränderung und Fälschung und Vernichtung beweiserheblicher Daten bis hin zum rechtswidrigen Zugriff zu Daten und der Beihilfe dazu sanktioniert.

Techno-Terrorismus

In Zukunft dürften Bombenanschläge auf Gebäude wie Rechenzentren stark abnehmen. In einschlägigen Kreisen werden rechner- und programmgesteuerte (logische und Zeit)-Bomben diskutiert werden, die im Einzelfall wesentlich mehr Schaden anrichten können als die – zugegebenermaßen öffentlichkeitswirksameren – Sprengstoffbomben.

Selbstverständlich sind grundsätzlich Innentäter in der Lage, mit den genannten programmgesteuerten Verfahren der Hacker z.B. die Reaktor-steuernden Rechner von Kernkraftwerken zu manipulieren und zu sabotieren. Allerdings braucht die Manipulation gar nicht den größten anzunehmenden Schaden anzurichten; eine kleine – evtl. unregelmäßig wiederkehrende – Störung reicht völlig aus. In einem solchen Fall würde man auch den sicherlich hohen finanziellen Schaden gar nicht herunterspielen wollen; in jedem Fall müßte der in der deutschen Öffentlichkeit und auch in der ganzen Welt entstehende Vertrauensschaden weit höher bewertet werden. Ein solcher Vertrauensschaden kann gesellschaftliche Auswirkungen haben und die gesamte Kernindustrie vollends und endgültig diskreditieren.

Eine solche Manipulation/Sabotage mit Programmen ist durchaus realistisch. Es können auch hier zeitverzögert sich auswirkende Programme eingesetzt werden (Zeitbomben). In jüngerer Zeit mehr in das Blickfeld der Öffentlichkeit gerückt sind die Computerviren, die in der Lage sind, nicht nur den Betrieb eines Computers zu sabotieren, sondern ganze Netze – auch im internationalen Bereich – lahm zu legen. Der – hier einmal als harmlosere Form des Virus bezeichnete – Wurm des Informatik-Studenten Morris [Spafford 1989] hat im letzten Jahr einen direkten Schaden von (je nach Schätzung und Bewertung) 10 bis 100 Millionen US-Dollar verursacht.

Hier sind Sabotageaktionen nicht nur denkbar; was uns kriminelle Kreise in Amerika vorführen, wird von Kriminellen in Deutschland mit einer Zeitverzögerung von höchstens zwei Jahren nachvollzogen. Gegnerische Nachrichtendienste dürften das notwendige Know-how bereits besitzen und anwenden (können).

Auch wenn in diesem Bereich noch keine spektakulären Aktionen bekannt geworden sind, sollten sich potentiell Betroffene mit der Problematik beschäftigen.

Weiterführende Literatur

Ammann, T.; Lehnhardt, M.; Meißner, G.; Stahl, S.: Hacker für Moskau. Deutsche Computerspione im Dienst des KGB. Reinbek 1989.

Bundesministerium des Innern (BMI) (Hrsg.): Rahmenkonzept zur Gewährleistung der Sicherheit der Anwendung der Informationstechnik (IT) - IT-Sicherheitsrahmenkonzept. Beschluß des Bundeskabinetts vom 23. Nov. 1989. Datenschutz und Datensicherung 291ff., 1989

Central Intelligence Agency (CIA) (Ed.): Soviet Acquisition of Military Significant Western Technology: An Update. Washington September 1985 http://www.foia.ucia.gov/frame3.htm

Pohl, H.: DV-Sicherheit: Angriffe auf die Datenverarbeitung und Gegenmaßnahmen. Datenschutz und Datensicherung 4, 292 - 298, 1984

Pohl, H.: DP-security: Attacks against data processing and preventive measures. In: Grimson, J.B.; Kugler, H.J. (Eds.): Computer Security. IFIP/Sec 85. New York 1985

Pohl, H.: Computermißbrauch - Gefahren und taktische und strategische Gegenmaßnahmen. Handbuch der Modernen Datenverarbeitung HMD 22, 125, 9 - 18, 1985

Pohl, H.; Cremer, D.: Zur Computerkriminalität im 5. Strafrechtsänderungsgesetz (5. StÄG) der DDR und 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) der Bundesrepublik aus der Sicht der Informationstechnik. Datenschutz und Datensicherung 10, 493 - 497, 1990 und 11, 551 - 558, 1990

Spafford, E.H.: The Internet Worm Program: An Analysis. Computer Communication Review Vol. 19, Nr. 1, S. 17-57, Januar 1989

Stoll, C.: The Cuckoo's Egg. Inside the World of Computer Espionage. New York 1989

ZSI - Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheitskriterien. Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT). 1. Fassung vom 11. Januar 1989. Köln 1989.

— — o — —