IT-Sicherheit als Managementaufgabe

Udo Helmbrecht, Carina Gneuß

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
D-53175 Bonn
udo.helmbrecht@bsi.bund.de

Abstract: Mit der zunehmenden Digitalisierung des wirtschaftlichen und gesellschaftlichen Lebens steigt die Abhängigkeit von der Informationstechnik. Die Sicherheit und Zuverlässigkeit der IT-Systeme ist demnach existenziell. Entwicklungen ohne die adäquate Berücksichtigung der IT-Sicherheit sind kaum noch denkbar. Aufgrund der übergreifenden Bedeutung des Themas ist eine interdisziplinäre Zusammenarbeit zwischen allen Beteiligten notwendig: IT-Sicherheit ist ein Querschnittsthema und muss als Managementaufgabe aktiv aufgegriffen werden.

1 Einleitung

Wie viel Sicherheit braucht die Informatik? Keine leichte Frage. Fest steht: Am Thema Sicherheit kommt niemand mehr vorbei. Denn Arbeits- und Geschäftsprozesse basieren immer stärker auf IT-Lösungen - das wirtschaftliche und gesellschaftliche Leben ist zunehmend digitalisiert. Die Vernetzung hat inzwischen zu große Ausmaße angenommen, als dass die Sicherheit der IT-Systeme vernachlässigt werden dürfte. Schließlich entscheidet die Sicherheit und Zuverlässigkeit der Informationstechnik darüber, ob zentrale gesellschaftliche Bereiche überhaupt funktionieren können. Zwar birgt die dynamische Entwicklung der Informationstechnik viele Chancen, doch es entstehen auch Risiken. Vor allem die Komplexität der heutigen IT-Systeme wird zur Herausforderung für die IT-Sicherheit. Jeden Tag gibt es neue Sicherheitslücken in den IT-Systemen. Um die damit verbundenen Risiken zu minimieren, müssen Sicherheitsfunktionen integraler Bestandteil moderner Informationstechnik sein. IT-Sicherheit ist dabei kein Selbstzweck. Die Vermeidung aller möglichen Risiken ist aussichtslos und nicht effektiv. Vielmehr soll den Risiken beim IT-Einsatz mit einem verlässlichen Risikomanagement begegnet werden. Doch sind sichere Informationssysteme unter diesen Voraussetzungen überhaupt möglich?

2 IT-Sicherheit: Ziele, Bedrohungen, Angreifer

Um diese Frage zu beantworten, gilt es ganz vorn anzufangen: mit der Definition von IT-Sicherheit. Der traditionelle Sicherheitsbegriff aus den Anfängen des BSI definierte 1992 den „Ausschluss bzw. die Verminderung von Gefahren“ und „die Betrachtung von technischen Gefährdungen wie Bedienungsfehler, technisches Versagen, katastrophenbedingte Ausfälle und absichtliche Manipulationsversuche“ [BS92] als IT-Sicherheit. Die Norm ISO 17799 bzw. BS 7799 liefert folgende Definition: „Die Implementierung zu begründender Schutzmaßnahmen zwecks Sicherstellung fortgesetzter IT-Services innerhalb sicherer Parameter, als da sind: Vertraulichkeit, Integrität und Verfügbarkeit.“

Die drei Hauptziele der IT-Sicherheit erklären sich wie folgt:

- Vertraulichkeit: Schutz sensibler Informationen (Daten) vor nicht autorisiertem Zugriff
- Integrität: Schutz sensibler Informationen (Daten) vor ungewollter Veränderung
- Verfügbarkeit: Sicherstellen, dass Informationen (Daten) und unerlässliche IT-Services verfügbar sind, wenn sie gefordert werden.

Hinzu kommen die Aspekte Authentizität und Verbindlichkeit: Der Informationsempfänger muss einerseits erkennen können, ob eine Nachricht gefälscht ist. Andererseits muss nachweisbar sein, dass er die Nachricht überhaupt erhalten hat. Darüber hinaus gibt es neben der Perspektive der Systembetreiber die der Nutzer. Zusätzlich zu den klassischen Sicherheitszielen müssen deshalb die Aspekte Anonymität, Transparenz und Nutzerselbstbestimmung berücksichtigt werden. [FKP01]

Die Verwirklichung dieser Ziele ist keine leichte Aufgabe. Denn die Liste der möglichen Attacken ist lang: Angriffe auf die Zugriffskontrolle, Integrität und Verfügbarkeit der Daten, Authentizität, Vertraulichkeit, Anonymität, Bedrohungen durch Computer-Viren, Würmer, Trojanische Pferde, IP-Spoofing, DNS-Spoofing, E-Mail-Spoofing, Password-Cracking, Ausspähen. Die Verletzung des Datenschutzes, Sniffing, Social Engineering, Man in the Middle-Attacken, Denial of Service, E-Mail-Bombing und noch viel mehr ließe sich aufzählen. Zusammengefasst sind Angriffe auf die Hard- und Software einer Organisation möglich - sowie auf die Daten bzw. Informationen selbst. [GS02]

Doch wer hat Interesse daran, die IT-Sicherheit zu gefährden? Und welche Motivation haben die Angreifer? Grundsätzlich kommen infrage:

- *interne Angreifer:* Rund ein Viertel aller Sicherheitslücken wird von den eigenen Mitarbeitern eines Unternehmens verursacht. Falscher Umgang mit den Computersystemen, mangelndes Sicherheitsbewusstsein für die IT-

Systeme sowie mutwillige Angriffe von frustrierten Mitarbeitern sind die Gründe. [Mu03]

- *externe Angreifer:* Hier kommen Hacker und Script Kiddies in Betracht. Ziele sind das Einsehen von vertraulichen Unternehmensdaten, Verändern/Fälschen von Daten, das Einschleusen schädlicher Programme in die Netzwerke sowie die Absicht den Ruf des angegriffenen Unternehmens zu schädigen. Die Motivation: Rache gekündigter Mitarbeiter, monetäre Anreize sowie das Ausloten der eigenen Grenzen und Fähigkeiten. Dabei nutzen die Täter zumeist bekannte Schwachstellen – wie z.B. nicht eingespielte Patches oder schwache Passwörter – um in die Netzwerke einzudringen.

- *Schadsoftware:* Diese wird auch als Malware bezeichnet und umfasst Computerviren, Würmer und Trojanische Pferde. Sie dient vor allem externen Angreifern als Hilfsmittel.

3 Auswirkungen

Seit 1998 hat sich die Anzahl der strafbaren IT-Delikte auf 80.000 im Jahr 2002 verdoppelt. Damit sind fast 60 Prozent der deutschen Unternehmen bereits Opfer eines IT-Angriffes geworden. In 85 Prozent der Fälle gehen finanzielle Verluste mit den Angriffen einher. Die geschätzten Schäden summieren sich in Deutschland mindestens auf einen dreistelligen Millionenbetrag pro Jahr. Weltweit gehen Experten von einem zweistelligen Milliardenbetrag aus. Inzwischen rechnen vier von fünf Unternehmen mit einem weiteren Anstieg der IT-Attacken. Wobei in jedem dritten Fall bereits bekannte Schwachstellen innerhalb der Betriebssysteme ausgenutzt werden. [Mu03]

Dabei hat die Sicherheit für rund 75 Prozent der deutschen Unternehmen hohe oder höchste Priorität. Doch den Worten folgen nur selten Taten: Es wird kaum in IT-Sicherheit investiert. Nur jedes vierte Unternehmen ist bereit, die notwendigen Schritte für die Verbesserung der Informationssicherheit einzuleiten. Noch schlimmer: Bei rund der Hälfte der Unternehmen stagnieren die Budgets für IT-Sicherheit und bei zehn Prozent sind sie sogar rückläufig. Besonders kleine und mittlere Unternehmen (KMU) schneiden schlecht ab. [Mu02]

Anders ausgedrückt heißt das: Im letzten Jahr haben deutsche Unternehmen mit mehr als hundert Mitarbeitern etwa 7,3 Milliarden Euro für die Sicherheit ihrer IT-Landschaft ausgegeben. Das sind durchschnittlich rund zehn Prozent des IT-Budgets oder 410 Euro pro Mitarbeiter. [Mu02]

Doch Viren- und Hackerangriffe richten sich längst nicht mehr nur gegen Großunternehmen. Inzwischen ist jedes Unternehmen ein potenzielles Angriffsziel für Attacken aus dem Internet – unabhängig von der Größe oder Branchenzugehörigkeit. Umso wichtiger ist deshalb auch der Schutz der KMU. Und nicht nur Hacker, Spione oder Saboteure bedrohen die Unternehmen:

Systemausfälle, technisches Versagen und die Fehlbedienung gefährden ebenfalls die Verfügbarkeit von Informationen.

4 Die Lösung: Systematisches IT-Sicherheitsmanagement

Effektiver Schutz der IT-Sicherheit ist nicht unmöglich. Damit ein Unternehmen die Sicherheitsrisiken steuern, kontrollieren und auf Vorfälle geeignet reagieren kann, bedarf es eines methodischen IT-Sicherheitsmanagements. Denn einzelne Sicherheitsmaßnahmen - wie die Verschlüsselung von Informationen oder der Einsatz einer Firewall - sind nicht ausreichend, sondern nur integraler Bestandteil eines modernen IT-Sicherheitskonzepts.

Ziel des IT-Sicherheitsmanagements ist es, durch einen systematischen und koordinierten Einsatz von organisatorischen, technischen und physischen Sicherheitsmaßnahmen einen angemessenen Schutz aller informationellen Ressourcen zu gewährleisten und sicherzustellen. Dabei ist IT-Sicherheitsmanagement ein kontinuierlicher Prozess, der Sicherheitsstrategien und -konzepte festlegt, diese auf ihre Wirksamkeit und Leistungsfähigkeit überprüft und bei Bedarf fortschreibt. Die Maßnahmen sind Bestandteil des Risikomanagements und damit Sache des Vorstandes bzw. der Geschäftsführung, die per Gesetz zur Einrichtung eines unternehmenseigenen Risikomanagement-Systems verpflichtet ist. Liegen solche Kontrollmechanismen nicht vor, drohen erhebliche persönliche Haftungsrisiken. [Ko98]

Das IT-Grundschutzhandbuch des BSI [GSHB] beinhaltet alle wesentlichen Schritte, die für einen kontinuierlichen IT-Sicherheitsprozess notwendig sind:

- Entwicklung einer IT-Sicherheitspolitik
- Auswahl und Etablierung einer geeigneten Organisationsstruktur für das IT-Sicherheitsmanagement
- Erstellung eines IT-Sicherheitskonzeptes
- Realisierung der IT-Sicherheitsmaßnahmen
- Schulung und Sensibilisierung
- Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb

Ein funktionierendes IT-Sicherheitsmanagement muss in die existierenden Managementstrukturen einer jeden Organisation eingebettet werden. Daher ist es praktisch nicht möglich, *eine* IT-Sicherheitsmanagement-Struktur anzugeben, die für jede Organisation unmittelbar anwendbar ist. Vielmehr sind häufig Anpassungen an organisationsspezifische Gegebenheiten erforderlich.

Die Hemmnisse für die Realisierung von IT-Sicherheitsmaßnahmen sind vielfältig: knappe Budgets, intransparente Kosten-Nutzen-Relationen, mangelhaftes technisches Know-how und zu viele „Insellösungen“, die einer integrierten Sicherheitsarchitektur widersprechen. Und besonders die

Komplexität der IT-Systeme stellt bei der Umsetzung des Gesamtprozesses eine große Hürde dar. [TD02]

Das Problem der Komplexität betrifft besonders die KMU. Ihnen versucht das BSI gezielt Hilfestellung zu geben: So wird derzeit mit dem "Leitfaden Sicherheit - IT-Grundschutz kompakt" eine Ergänzung zum IT-Grundschutzhandbuch erstellt. Dieser Leitfaden bietet auf 60 Seiten einen Überblick über die wichtigsten Fakten zum IT-Grundschutz. Außerdem wird aufgezeigt, was die wesentlichen Sicherheitsmaßnahmen für KMU sind und wo dringlicher Handlungsbedarf für Sicherheitsvorkehrungen besteht.

Darüber hinaus bietet sich gerade für KMU, die sich keine IT-Sicherheitsexperten leisten können, auch das Auslagern von Sicherheitsdienstleistungen an (Information Security Management - ISM). [NP03] Dabei übernehmen IT-Profis die Beratung, die Installation, den Betrieb und kümmern sich rund um die Uhr um die Sicherheit des Netzwerkes. Ein externes Sicherheitsmanagement spart interne Ressourcen und ist besonders für KMU eine verhältnismäßig günstige Alternative. Es senkt die Kosten und setzt gleichzeitig IT-Ressourcen frei. Für diesen Schritt bedarf es jedoch einer grundlegenden Einstellungsänderung: Wenn es um den Schutz von physischem Eigentum geht, zögert man nicht, professionellen Schutz - z.B. Wachmänner - in Anspruch zu nehmen. In der virtuellen Welt muss sich diese Überzeugung erst noch durchsetzen.

Laut den Prognosen der Marktforschungsinstitute hat dieses Umdenken bereits begonnen: Demnach werden die Ausgaben für IT-Sicherheit steigen. IDC geht für das Jahr 2006 von einem weltweiten Marktvolumen von 45 Mrd. US-Dollar aus. Im Jahr 2001 waren es nur rund 17 Mrd. US-Dollar. [ID02] Nach Beobachtung von Experten ist vor allem die Auslagerung der Netzwerksicherheit ein wachsender Geschäftszweig.

5 Fazit

Klar ist: Absolute Sicherheit wird es nie geben. Es ist unmöglich, sich gegen alle eventuellen Bedrohungen zu schützen. Doch wenn es um die IT-Sicherheit eines Unternehmens geht, ist man gut beraten, sich nicht auf technische Einzellösungen zu verlassen und diese als umfassenden Schutz zu begreifen. Denn: Die Betriebsfähigkeit der IT-Infrastruktur ist nicht nur ein wirtschaftliches Interesse, sondern existenzielle Notwendigkeit für ein Unternehmen! Schließlich ist Information ein wichtiger Produktionsfaktor. Wer im Wettbewerb vorn liegt, darüber entscheiden oft scheinbar wettbewerbsfremde Faktoren wie die Datensicherheit. Datenverluste können hohe finanzielle Einbußen verursachen, wenn es zu Produktionsausfallzeiten kommt, wertvolle Arbeitszeit verloren geht und Finanzgeheimnisse ausgespäht werden. Auch bei sehr gravierenden Störungen im IT-Bereich müssen Prozesse und Transaktionen ohne Unterbrechung fortgeführt und ausgefallene IT-Systeme in kürzester Zeit wiederhergestellt werden können.

Deshalb ist ein allumfassendes, organisationsweites IT-Sicherheitsmanagement von entscheidender Bedeutung. Dabei darf nicht vergessen werden, dass es sich um einen Prozess handelt, der kontinuierlich weiterentwickelt werden muss, um mit dem technologischen Wandel Schritt halten zu können.

Literaturverzeichnis

[BS92] BSI 7105: IT – Sicherheitshandbuch - Handbuch für die sichere Anwendung der Informationstechnik, Version 1.0, März 1992, http://www.bsi.bund.de/literat/kriterie.htm

[FKP01] Fox, D.; Köhntopp, M.; Pfitzmann, A.: Verlässliche IT-Systeme 2001, Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, 2001

[GSHB] BSI: „IT-Grundschutzhandbuch, Standardsicherheitsmaßnahmen", Loseblattsammlung, Schriftenreihe Band 3, Bundesanzeiger-Verlag, jährlich neu, http://www.bsi.bund.de/gshb

[ID02] The Big Picture: IT Security Software, Hardware and Services Forecast and Analysis, 2002-2006 (IDC #28604), Dezember 2002, http://www.idc.com

[Ko98] KonTraG: Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, 5. März 1998

[Mu02] Studie „IT-Security“: Informationsweek/Mummert+Partner Unternehmensberatung AG, 2. September 2002, http://www.mummert.de/deutsch/press/a_press_info/020209.html

[Mu03] Studie: Mummert+Partner Unternehmensberatung/Bundesamt für Sicherheit in der Informationstechnik (BSI), 6. März 2003, http://www.mummert.de

[NP03] Neundorf, Dörte; Petersen, Holger: Information Security Management – Vom Prozess zur Umsetzung, in: DuD – Datenschutz und Datensicherheit 27 (2003), S. 200-206

[TD02] Wie viel Sicherheit braucht ein Unternehmen? – Branchenspezifische Entscheiderbefragung im Rahmen der Kampagne „TrustD@y-IT-Sicherheit ist Chefsache!“ Oktober/November 2002, http://www.trustday.de