Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 171 (2005)

Heft: 12

Artikel: Bedrohung und Schutz der Informationsgesellschaft

Autor: Loretan, Stephan / Dietrich, Martin

DOI: https://doi.org/10.5169/seals-69954

Bedrohung und Schutz der Informationsgesellschaft

Die beiden Autoren stellen im folgenden Artikel die Information als volks- und betriebswirtschaftliche Grösse in den Mittelpunkt. Nach einer abgrenzenden Definition erläutern die Autoren, welche Bedrohungsformen existieren und skizzieren, wie sich Unternehmen mittels einer adäquaten Sicherheitsarchitektur dagegen schützen können.

Stephan Loretan, Martin Dietrich *

Die Volkswirtschaften der Industrieländer haben sich in der Vergangenheit stark verändert. Die Liberalisierung der Telekommunikationsmärkte, das rasante Wachstum des Internets und die zunehmende Vernetzung von Wirtschaft und Gesellschaft führten allesamt zur Entstehung der Informationsgesellschaft. Unsere Gesellschaft und unser (all-) tägliches Leben stützen sich in vielfältigster Art und Weise auf Informationen. Diese sind sowohl in geschriebener, gesprochener, aber immer mehr und aktueller auch in digitaler Form unterschiedlichster Ausprägung vorhanden. Im Verlaufe der letzten Jahre wurden Informationen und deren Inhalte zu einer nicht mehr wegzudenkenden Ressource des wirtschaftlichen, sozialen und privaten Geschehens. Sowohl aus betriebs- wie auch aus volkswirtschaftlicher Sicht ist die Ressource Information längst ein Gut wie die klassischen (althergebrachten) Faktoren Arbeit, Kapital und Boden.

Information als Ressource

Für viele Gesellschaftsbereiche hat sich die Ressource «Information» mittlerweile zur strategisch wichtigsten Komponente entwickelt. Die Schweiz ist bei der Entwicklung zu einer Informationsgesellschaft weit fortgeschritten.

Gemäss dem Informatikstrategieorgan Bund (ISB) gibt sie am meisten Geld pro Kopf und Jahr für Informations- und Kommunikationstechnologien (IKT) aus. Dies zeigt sich deutlich, indem ein wesentlicher Teil des Lebens und Arbeitens darin besteht, Informationen und Wissen zu gewinnen, zu speichern, zu verarbeiten, zu vermitteln und zu nutzen. Grundlage all dieser Aktivitäten ist und bleibt der Einsatz von IKT. Exemplarisch für diese Entwicklung können die folgenden Beispiele aufgeführt werden:

- Innerhalb der IKT ist das Internet aufgrund seiner Verbreitung wohl am bedeutendsten. Sowohl im privaten als auch im unternehmerischen Bereich hat seine Nutzung stark zugenommen. Es wird über Informationsbeschaffung und Werbepräsenz hinaus zunehmend für Kommunikation und Transaktionen genutzt. Viele der neuen Internetdienste durchleben gerade die Umwandlung vom «Gratis»-Medium zum Wirtschaftsgut. Auf längere Sicht gesehen ist die weitere Ökonomisierung des Internets und die Transformation zu einer weit gehend digitalisierten Dienstleistungsgesellschaft eine zentrale Herausforderung der Zukunft.
- Die Entwicklung der Informations- und Kommunikationstechnik war Antrieb für wesentliche Neuerungen in Produktion und Dienstleistung der letzten Jahre. Die Weiterentwicklung der Technologie ist entscheidend, um auch in Zukunft international konkurrenzfähige Produkte und Dienstleistungen anbieten zu können. Mehr als die Hälfte der Industrieproduktion und ein Grossteil der Exporte hängen heute vom Einsatz moderner IKT und elektronischer Systeme ab. Sie bilden die Grundlagen der wirtschaftlichen Leistungsfähigkeit jeder Industrienation. Sie wirken zusammen mit der Produktionstechnologie, Material- und Werkstofftechnologie, den optischen Technologien und der Mikrosystemtechnik. Für den Maschinen- und Anlagenbau liefern IKT Steuerungen, Test- und Prüfeinrichtungen, in der Chemischen Industrie regeln sie Verfahrensabläufe.
- IKT sind oft und meist ausschliesslich die Schlüsseltechnologien für Innovationen. Die dabei getätigten Investitionen tragen wesentlich zum Wirtschaftswachstum bei. Die gesamtwirtschaftliche Bedeutung der IKT geht aber weit über die der IKT-Branche hinaus. Durch die Generierung von Innovationen erzeugen IKT Wachstum und schaffen zukunftssichere neue Arbeitsplätze.

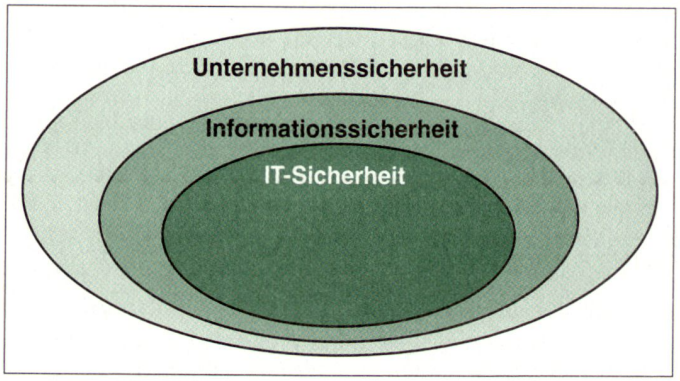
Informations- und Kommunikationstechnologien als Mittler

All diese Beispiele zeigen, dass die Nutzung und Verbreitung modernster IKT in der Informationsgesellschaft eine hohe wirtschaftliche und auch soziale Priorität haben. Im selben Umfang wie deren Bedeutung zunahm, steigerte sich jedoch auch die Abhängigkeit unserer Gesellschaft vom Vorhandensein und dem Informationsgehalt der IKT in den nachfolgend aufgeführten so genannten kritischen Infrastrukturen eines Landes:

- Energieerzeugung und -verteilung (Elektrizität, Öl, Gas)
- Transport von Gütern und Personen
- Telekommunikation
- Medien
- Finanzindustrie (Banken, Versicherungen)
- Notfall- und Rettungsdienste
- Versorgung (Gesundheitswesen, Lebensmittel, Wasser)
- Regierungsfunktionen von Bund, Kantonen und Gemeinden einschliesslich Polizei, Zoll und Armee.

In der Vergangenheit konnte man diese Schlüsselinfrastrukturen relativ gut schützen. Mit der zunehmenden Bedeutung der Ressource Information hat sich dies drastisch geändert.

Ein umfassender Schutz durch die Sicherheitsapparate eines einzelnen Staates (oder einer zuständigen Organisation) gestaltet sich aufgrund der umfassenden Vernetzung aller Bereiche, der teilweisen Privatisierung und der Globalisierung vieler Funktionen sehr schwierig. Eine Partnerschaft zwischen staatlichen Organen und der Privatwirtschaft ist ein absolutes Muss, um die Sicherheit der Infrastrukturen als nationale Aufgabe zu gewährleisten.



Sicherheitsebenen.

* Stephan Loretan, lic. oec. HSG, Berater für Projektmanagement und Organisation bei der BSG Unternehmensberatung. Ehemalige militärische Funktion: Hptm der Art in der Funktion als Nof, heute Stabschef ziviler Gemeindeführungsstab

Martin Dietrich, lic. oec. HSG, CISA, studierte Informationsmanagement. Er leitet die Entwicklung der BSG ITSEC ToolBox der BSG Unternehmensberatung, ist Sicherheitsexperte und führt Sicherheitsaudits durch.

Die Sicherheitsebenen

Mit dem Entstehen der Informationsgesellschaft muss zusätzlich zur physischen Sicherheit auch die Sicherheit der Ressource Information mitberücksichtigt werden. Diese integrale Sicht der Sicherheit beinhaltet so auch die Informationssicherheit. Sie grenzt sich von der Informatiksicherheit (IT-Sicherheit) ab, indem sich Letztere ausschliesslich mit elektronisch gespeicherten Informationen befasst, Erstere sich dagegen für den Schutz sämtlicher Informationen ungeachtet ihrer Darstellung und Speicherung verantwortlich zeichnet.

Wie durch das ISB richtig festgestellt wird, ist die Informationssicherung trotz ihrer hohen Affinität zu den IKT keine rein technische Aufgabe. Ein wirksames Informations-Sicherheits-Management-System (ISMS) hat auch die Bereiche Organisation und Prozesse, Politik und Gesetze und Ressourcen (Bsp. Personalausbildung) zu berücksichtigen.

Erforderliche IT-Sicherheit

Im Zentrum der folgenden Überlegung steht nun die IT-Sicherheit. Hierzu kann festgestellt werden, dass ohne sie kein (oder nur ein geringes) Vertrauen in die Informationssysteme vorhanden ist. Dies umso mehr, als dass der beständig zunehmende Einsatz von Informationstechniken in Produktion und Dienstleistungsgewerbe, in sozialen und öffentlichen Einrichtungen zu einer wachsenden Abhängigkeit aller Anwendungsbereiche von Informationstechnik führt. Wirtschaftliche Gründe und ein optimaler Wertschöpfungsprozess erfordern einen zuverlässigen IT-Betrieb, der ohne frühzeitige Planung, geeignete Sicherheitsmassnahmen und deren regelmässige Überprüfung nicht gewährleistet werden kann. Im Zentrum stehen dabei die verschiedenen Dimensionen der IT-Sicherheit:

- Die *Verfügbarkeit* bezieht sich auf die Funktionsfähigkeit, den eigentlichen lauffähigen Betrieb der eingesetzten Lösung und ist zukunftsorientiert; die IT soll so betrieben werden, dass die Systeme ab dem aktuellen Zeitpunkt in die Zukunft hinein verfügbar sind, und sie soll den Ausfall der Informationsverarbeitung und die Sabotage von Verarbeitungsprozessen verhindern.
- *Datenexistenz:* Die Dimension Datenexistenz ist bewusst von der Verfügbarkeit der Systeme getrennt. Grund dazu ist, dass die Ursachen und die Folgen von nicht verfügbaren Systemen oder nicht vorhandenen Daten unterschiedlich sein können. Zudem ist sie vergangenheitsorientiert, indem die IT so betrieben werden soll, dass keine Daten von heute, gestern und früher verloren gehen dürfen. Sie verhindert das bösartige Zerstören und unbeabsichtigte Löschen von Daten durch Personen und/oder Maschinen.
- *Integrität:* Die Integrität der Daten bezieht sich auf die inhaltliche Richtigkeit der Informationen. Sie stellt die Genauigkeit und Vollständigkeit der Informationen und ihrer Verarbeitungsmethoden sicher. Fehler in den Daten haben in der Regel direkte Auswirkungen auf das Vertrauen in die Informationen.
- Die Dimension *Vertraulichkeit* der Daten besteht in der Forderung, Informationen nur den berechtigten Personen zugänglich zu machen.

Wachsende Verwundbarkeit und die Gefahr massiver wirtschaftlicher Schäden in der Folge von IT-Risiken erhöhen den Handlungsdruck, durch ein aktives IT-Sicherheitsmanagement die vier Dimensionen bestmöglich zu gewährleisten und so Schäden zu verhindern und das verbleibende Restrisiko zu minimieren.

Akute Bedrohungsformen

Dieses Restrisiko geht in einem grossen Teil von der Verwundbarkeit der Informationsnetze aus. Was zu Beginn mit dem Phänomen der «Hacker» eher belustigend zur Kenntnis genommen wurde und unter sportlichen Gesichtspunkten beargwöhnt wurde, ist mittlerweile zur ernsthaften Bedrohung geworden. Inzwischen eröffnet sich ein grosses Spektrum illegaler Datenzugriffe, das von Software- oder Datenmanipulation über Betrug, Datendiebstahl und Desinformation bis hin zu organisierter Kriminalität wie Wirtschaftsspionage und Terrorismus reicht. Im Visier der Angriffe stehen dabei ohne Unterschied die Computernetze von Staat, Wirtschaft und Wissenschaft. Nach einer Untersuchung von Price Waterhouse Coopers wurden 42 Prozent der grösseren Unternehmen der Europäischen Union (EU) Opfer der so genannten Cyberkriminalität. Die Dunkelziffer der nicht erkannten oder nicht gemeldeten Angriffe dürfte noch weit höher liegen. Dabei kamen die Angreifer keineswegs immer von aussen, sondern waren zu 60 Prozent so genannte Innentäter, also Personal der eigenen Unternehmung. Neben dem Täterkreis der Innentäter wird der freie und sichere Umgang mit Daten und Informationen noch von weiteren Seiten bedroht. Das ISB geht dabei von folgenden Kreisen aus:

- Einzeltäter, wie gelangweilte oft jugendliche Script-Kiddies, Cracker oder Hacker
- Gruppierungen, die aus politischen Motiven handeln
- Unternehmen, die aus wirtschaftlichen Motiven handeln
- Nationalstaaten mit kriegerischen Absichten

Nebst all diesen als illegal einzustufenden Handlungen und Betrachtungen darf nicht vergessen werden, dass die Sicherheit zusätzlich durch unbeabsichtigtes menschliches Fehlverhalten, technisches Versagen und Naturereignisse gefährdet sein kann.

Notwendige Schutzbedarfsdiskussion

Die Dimensionen der IT-Sicherheit und die aktuellen Bedrohungsformen verlangen die Etablierung und Durchführung eines Risikodialogs. Im Zentrum steht dabei die Ermittlung des Schutzbedarfs aufgrund der prozess- bzw. anwendungsspezifischen Anforderungen in den IT-Sicherheits-Dimensionen Verfügbarkeit, Datenexistenz, Integrität und Vertraulichkeit.

Ermittelt wird der Schutzbedarf durch Beurteilung der wichtigsten Schadenszenarien und ihrer Ausprägungen, entsprechende Formeln ermöglichen ein nachvollziehbares Umrechnen (i. S. Quantifizieren?) der Szenarien in Schutzbedarfswerte. Folgende relevante Schadensaspekte werden berücksichtigt:

- Beeinträchtigung der Betriebsabläufe
- Personenschäden an Leib und Leben
- Rechtliche Folgen, Schadenersatzklagen
- Anzahl Mitarbeiter, die nicht arbeiten können
- Imageverlust
- Materieller Schaden
- Vorteil für die Konkurrenz
- Volkswirtschaftlicher Schaden

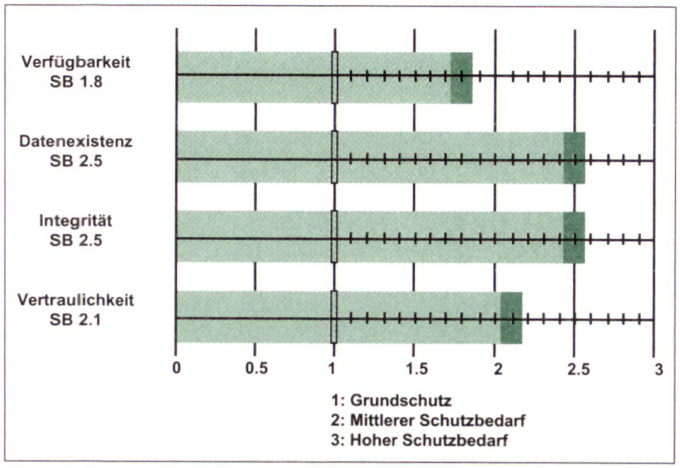
Die Ergebnisse lassen sich im Schutzbedarfsdiagramm darstellen und bilden die Anforderungen an die an der Leistungserbringung beteiligten Informatikkomponenten:

Messbarer Sicherheitszustand

Die in der Schutzbedarfsdiskussion bestimmten Sicherheitsanforderungen erlauben den Vergleich mit dem tatsächlichen Sicherheitszustand. Dazu empfiehlt sich die Gliederung in Prüfobjekte, an denen die einzelnen Prüfthemen gemessen werden:

- Rechenzentrum und seine Infrastruktur
- Server
- Operator
- Kommunikation
- Benutzer

Bewährt hat sich in diesem Vorgehen der Einsatz standardisierter Prüflisten respektive Fragestellungen, die auf internationalen Standards (Bsp. ISO), ergänzt mit praktischen Erfahrungen, beruhen und bereits mit möglichen bewerteten Antworten versehen sind. Für die Feststellung des Sicher-



Schutzbedarfsdiagramm.

heitszustandes dienen die im Voraus festgelegten Antwortmöglichkeiten. Sie enthalten die Anforderungen an einen hohen, genügenden und ungenügenden Schutz. Der mit den Prüflisten durchgeführte Soll-/Ist-Vergleich führt zu Massnahmen- und Pendenzenlisten zur Behebung der festgestellten Sicherheitslücken.

Angemessene Sicherheitsarchitektur

Sicherheitslücken lassen sich in der Regel nicht unmittelbar beseitigen. Die Etablierung einer adäquaten Sicherheitsarchitektur bedingt daher ein durchdachtes Setzen von Prioritäten unter Einbezug der Ergebnisse aus der Schutzbedarfsanalyse zur Verhinderung existenzgefährdender Schäden. Die Überlegungen umfassen Aussagen für Server, Kommunikationsinfrastrukturen und Benutzerarbeitsplätze und stellen die angestrebte Sicherheitsarchitektur und allfällige Variante mit ihren Auswirkungen auf

- minimale Ausfallzeit (Best Effort)
- maximale Ausfallzeit (garantiert)
- minimaler Datenverlust (Best Effort)
- maximaler Datenverlust (garantiert)

dar. Sie beinhalten zusätzlich Empfehlungen für grundlegende Entscheidungen, sowohl auf Seite der Informatik als auch auf Benutzerseite, z. B.

- Pikett-, Alarm- und Notfallorganisation
- Verschlüsselung von Informationen
- Ausweichlösungen
- geforderte Infrastruktur- und Hardware-Redundanzen

Bewältigte Ausnahmesituationen

Ausnahmesituationen treten meist ohne Vorwarnung und ohne Berücksichtigung einer angenommenen Wahrscheinlichkeit ein. Bei ihrer Bewältigung spielen die Umsetzung der oben dargestellten Massnahmen und Entscheidungen eine wichtige Rolle.

Je umfassender die Schutzbedarfsdiskussion geführt, je genauer der Sicherheitszustand analysiert und je adäquater die Sicherheitsarchitektur realisiert wurden, umso rascher und besser kann die Ausnahmesituation bewältigt werden, sodass der Normalzustand der Informationsgesellschaft wieder erreicht ist. ●

Network Enabled Operations – vernetzte Operationsführung; nicht nur eine technologische Herausforderung

Der Autor befasst sich im nachfolgenden Artikel mit den Grundsätzen der vernetzten Operationsführung und den der Konzeption zu Grunde liegenden technologischen, strukturellen und am Rande auch gesellschaftlichen Rahmenaspekten. Er zeigt dabei internationale Trends auf und illustriert diese an Hand konkreter Beispiele ausländischer Streitkräfte.

Andreas Moschin *

Beginn einer neuen Ära

Das neue Millennium bedeutet auch für moderne Streitkräfte eine neue Ära. Diese Ära ist geprägt durch ein sich veränderndes strategisches Umfeld und eine rasante technologische Entwicklung. Die fortschreitende Globalisierung, die Vernetzung der Gesellschaften, das Aufbrechen traditioneller Strukturen sowie die verstärkte Bedeutung der Information als Wettbewerbsvorteil. Zusammen mit dem enormen Bevölkerungswachstum und den sozialen und wirtschaftlichen Folgen sind strategische Entwicklungen, denen sich auch die Schweiz nicht verschliessen kann. Nach der vergangenen Epoche der Bipolarität bleibt die Welt zwar nach wie vor geteilt, die Grenzen bewegen sich aber ständig. Somit verändern sich auch die Konflikte. Waren früher politische Ideologien die Ursache von Konflikten, so ist im neuen Jahrtausend eine Tendenz hin zum religions- oder kulturbasierten Konflikt erkennbar. Diese Art von Auseinandersetzung zeichnet sich neben anderen Merkmalen durch eine zeitliche Synchronisation des Konfliktes und der gewaltsamen Umsetzung (Terror) aus. Diese Konfliktformen führen zu neuen und grenzüberschreitenden Risiken, Bedrohungen und Gefahren. Die neue Multipolarität ist einhergehend mit einem Verlust an Souveränität einzelner Staaten, und es besteht in verschiedenen Regionen der Welt eine Tendenz zum Zerfall der staatlichen Ordnung. Die sicherheitspolitische Antwort auf diese Herausforderungen des Informationszeitalters liegt im Erkennen der gegenseitigen Abhängigkeiten der Gesellschaften und der globalen Wirtschaft und der Notwendigkeit der gemeinsamen Vernetzung.

Die Wirtschaft hat den Nutzen der globalen Vernetzung längst erkannt. Sie setzt diese Erkenntnis auch um. Informationsmanagementsysteme ermöglichen die globale Verbreitung und Nutzung von Informationen. In multinationalen Unternehmen ist das «state of the art». In technologischer Hinsicht bringt der Übergang vom Industriezeitalter ins Informationszeitalter eine exponentielle Steigerung der Leistungsfähigkeit mit sich. Die zunehmende Verfügbarkeit und breite Anwendbarkeit der Informationstechnologie eröffnet bisher unbekannte Möglichkeiten zur Ausübung von gesellschaftlicher, industrieller, wirtschaftlicher, aber auch militärischer Macht. Im Gegensatz zu vergangenen Jahrzehnten ist heute jedoch nicht mehr der militär-industrielle Komplex die treibende Kraft bei der Entwicklung neuer Technologien, sondern die Industrie im zivilen Markt.

*Andreas Moschin, Oberstlt i Gst, Head of Sales Defense bei Siemens Schweiz AG, Civil and National Security.