Kapitel 1

Einleitung: Gesellschaftlicher Wandel und IT-Sicherheit

Dieses Buch beschäftigt sich mit Sicherheitslösungen, die vor Bedrohungen in unsicheren Netzen wie dem Internet schützen. IT-Sicherheit ist dabei nicht allein eine technisch-organisatorische Aufgabe, sondern steht im gesellschaftspolitischen Zusammenhang. Deshalb beginnt dieses Kapitel mit einem kurzen historischen Überblick.

1.1 Entwicklung von Informationstechnologie und IT-Sicherheit

Schon immer hatte der technologische Fortschritt Einfluss auf alle Bereiche der Gesellschaft. Wasserleitungen machten einerseits Wasserträger brotlos, ermöglichten andererseits erst die Siedlungsform Großstadt. Der Traktor verdrängte das Pferd, die elektrische Schreibmaschine die mechanische und so fort. Die Agrargesellschaft wurde in Europa durch die Industriegesellschaft abgelöst, Triebfedern waren Stahl, Kohle und Dampfkraft, später Erdöl und Elektrizität.

Mit Energie, Maschinen, menschlicher Arbeitskraft und Intelligenz wurde zunehmend mehr Materie formbar. Mit hoher Eigendynamik bildeten sich neue Lebensumgebungen; Mobilität für Güter und Menschen beschleunigte die Entwicklung, Handwerk und Wissenschaften organisierten sich.

Durch den Buchdruck wurde Wissen verteilbar, durch die Nachrichtentechnik körperlos (elektronisch) übermittelbar und schließlich – nun »Information« genannt – durch die Informationstechnik »prozessierbar«.

Gegenwärtig erleben wir den *Wandel zur Informations- und Kommunikationsgesellschaft*. Die dazu gehörenden Technologien sind die Schlüsseltechnologien für unsere Arbeits- und Lebenswelt von heute und morgen.

Meilensteine der Kryptographie bis zum II. Weltkrieg

1900 v. Chr.	Ägyptische Schreiber benutzten spezielle Hieroglyphen zur Verschlüsselung von Nachrichten; später wurde in Palästina ein »umgekehrtes Alphabet« zur Kodierung verwendet.
50-60 v. Chr.	Julius Caesar verwendete eine einfache Verschiebesubstitution von Buchstaben für vertrauliche Regierungskommunikation. Er ersetzte jedes A durch ein D, jedes B durch ein E usw. Nur wer die einfache Regel »Verschiebung um drei Buchstaben« kannte, konnte die Nachrichten entziffern.
1518	Johannes Trithemius schrieb das erste Buch zur Kryptographie.
1586	Maria Stuart wurde das prominente Opfer einer unzureichend verschlüsselten Nachricht
1660	Leon Batista Alberti konstruierte die erste Verschlüsselungsmaschine.
1917	Gilbert S. Vernam erfand bei AT&T in den USA eine praxistaugliche polyalphabetische Chiffriermaschine, die einen absolut zufälligen und niemals wiederholten Schlüssel verwendete. Dies war die erste beweisbar sichere Verschlüsselungsmaschine.
1918	Der deutsche Ingenieur Arthur Scherbius meldete das Rotorprinzip für Chiffriermaschinen zum Patent an und gründete 1923 die »Chiffriermaschinen Aktiengesellschaft« für Herstellung und Verkauf seiner ENIGMA. Die nach dem griechischen Wort für »Rätsel« benannte Maschine war für die vertrauliche Übertragung von geschäftlichen Mitteilungen und Telegrammen vorgesehen, war aber zunächst kein kommerzieller Erfolg. Später wurde sie in verbesserter Form zu Zehntausenden als Standard-Verschlüsselungsautomat bei Militär und diplomatischem Dienst eingesetzt.

Leser, die sich für die detaillierte Geschichte der Kryptographie interessieren, finden in David Kahns 1200-seitigen Standardwerk »The Code-Breakers« ausführliche Informationen /Kahn97/.

Die effiziente Verbindung von Kodierung und Prozessierbarkeit belegt ein schreckliches Beispiel: Datenbanksysteme mit IBM-Hollerith-Lochkarten lieferten dem Nazi-Regime die Informationsstruktur für Völkermord, von der Volkszählung 1939 über DV-gestützte Selektion nach »Rassemerkmalen« bis zur »Verwaltung« des Holocaust /Black2001/.

Entwicklung der Informationstechnik und -sicherheit seit 1938:

- Konrad Zuse entwickelte 1938 den ersten mechanischen Ziffernrechner »Z1«. Im II. Weltkrieg konnten die Briten mit einem Röhrenrechner die bis dahin als sicher geltende Verschlüsselung der deutschen mechanischen ENIGMA-Apparate brechen und gewannen den passiven Zugang zu dem weltweiten Funknetz. 1948 legte Claude E. Shannon mit dem »Bit« (Kürzel aus binary digit) als kleinste Dateneinheit den Grundstein für die Informationstheorie.
- Nach 1950 begann der Siegeszug des Transistors, der die langsame, anfällige, voluminöse und energiefressende Röhrentechnik ablöste. »Silicon, the new steel« lautete schließlich das Credo, als lochkartengespeiste Großrechneranlagen seinerzeit unglaubliche Datenmengen verarbeiteten. Als sich damals die Frage der Sicherheit stellte, wurde sie räumlich (Zugangsregelungen zum Rechenzentrum) und administrativ (Aufgabenteilung: Systemadministrator, Anwender, Daten-Eingabekraft) geregelt.
- Seit den 60er Jahren wurden, ausgehend von den USA, Terminals an Großrechner angeschlossen und der Siegeszug der Vernetzung begann. Die IT-Sicherheit hatte endgültig ihre räumliche Abgeschlossenheit verloren. Das ISO-Referenzmodell, TCP/IP-Technologie und Ethernet-Topologie wurden entwickelt; bald gab es dezentrale militärische Netze und Firmennetze wie SNA, DEC-Net und das globale IBM-Netz. 1973 entstand das Arpanet als Vorläufer des Internet, dieses wurde 1991 »öffentlich«, und mit dem World Wide Web begann das Online-Zeitalter.
- Parallel zur Entwicklung der Informationstechnologie entwickelte sich die Kryptographie. Wichtige Algorithmen entstanden, unter anderem 1976 der US Data Encryption Standard (DES), 1977 RSA, 1990 IDEA und 1991 Phil Zimmermanns Verschlüsslungssoftware PGP.
- Ein Technologiesprung aus dem Silicon Valley brachte den (Home-)PC mit eigenem Betriebssystem und schnellem Prozessorboard, immer größeren Festplatten, Floppy-Disk- und später ZIP-, CD- und DVD-Laufwerken zum Datenaustausch. Die Datenträger waren mobil, durch Miniaturisierung wurden es dann auch die Computer selbst (Laptops und Palmtops). Immer preiswertere und leistungsfähigere PCs ermöglichten die Integration von Audio und Video. Inzwischen besitzt in den Industrienationen ein erheblicher Teil der Bevölkerung einen eigenen Multimedia-PC, oft mit zahlreichen Peripheriegeräten (Scanner, Drucker etc.). Firmen wie Privatleute rüsteten ihre PCs mit Modems für den Zugang zu Mailboxen und später zu Online-Diensten über das Telefonnetz aus.
- Die Frage der IT-Sicherheit wurde zunächst viel zu einseitig auf den Bereich »Computerviren« bezogen. Dabei gedieh im Verborgenen längst der Datenmissbrauch. In Deutschland wird seit 1987 der Bereich Computerkriminalität von der Polizei eigenständig erfasst (siehe Anhang A).

1.2 Siegeszug des Internet

In den letzten Jahren hat sich das Internet als universales, bidirektionales und globales Kommunikationsmedium etabliert. Das »Netz der Netze« ist unabhängig von den räumlichen und zeitlichen Begrenzungen, die den Informationsfluss über die klassischen Print- und Rundfunkmedien einengen.

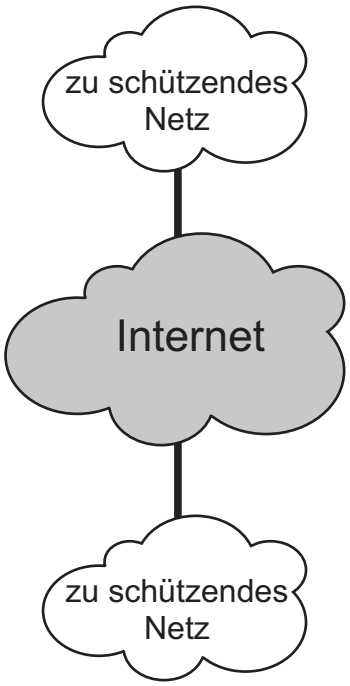

Abb. 1.1: Kommunikation über das Internet

Merkmale des Internet als das globale Datennetz:

- Einfacher und kostengünstiger Zugang
  Vom Notebook über PCs und Workstations bis zum Großrechner kann jeder Computer einfach und kostengünstig angeschlossen werden .
- Einheitlicher Standard
  Es gibt keine länderspezifischen Besonderheiten wie bei X.25-Netzen oder ISDN, denn die TCP/IP-Technologie ist netzunabhängig und für alle Betriebssysteme verfügbar.
- Weltweites Netz, shared infrastructure
  Hunderttausende Netzwerke verbinden über 100 Millionen angeschlossene Rechnersysteme in mehr als 240 Ländern. In praktisch allen Ländern der Welt

kann man über das Telefonnetz Zugangsrechner von Online-Diensten wie AOL, CompuServe und T-Online anwählen oder sich über Internet-Provider wie EUnet, MAZ und DFN direkt an das Internet anschließen.

- Steigende Akzeptanz
  Ende 2001 nutzten schätzungsweise 500 Millionen Menschen weltweit das Internet. Die Zuwachsrate ist weiterhin hoch, denn selbst in den Vereinigten Staaten haben lediglich knapp über 50 % der Haushalte einen Internet-Anschluss, in Deutschland sogar erst knapp über 25 %. Daraus kann man jedoch nicht ohne weiteres auf die Anzahl der Internetnutzer schließen, da zum einen eine erhebliche Zahl von Personen einen Internetzugang am Arbeits- oder Ausbildungsplatz hat und zum anderen die Nutzung eines Internet-Anschlusses durch mehrere Personen nur schwer abzuschätzen ist.

  Es ist zu erwarten, dass die Internetnutzung in diesem Jahrzehnt genauso alltäglich wird wie die Nutzung des Telefons und neuerdings des Mobiltelefons. Das Karlsruher Fraunhofer Institut für Systemtechnik und Innovationsforschung (ISI) berichtete im August 1998, dass nur 7 % der Internetnutzer in Deutschland aus der Arbeiterschicht kommen, was zeigt, dass starke gesellschaftliche Ungleichgewichte bestehen. Andererseits zeigt dies auch, dass das Potenzial hoch ist, denn in den nächsten Jahren werden sich die Unterschiede weiter angleichen. So berichtet die Gesellschaft für Konsumforschung (GfK) in Nürnberg, dass zwischen Ende 1997 und März 2001 der Anteil von Frauen unter den deutschen Internetnutzern von 29 % auf 42 % gestiegen ist.

  Ein neues gesellschaftliches Phänomen ist übrigens die Internetsucht, siehe »Münchener Ambulanz für Internet-Abhängige«:
  `www.psychiater.org/Internetsucht/ambulanz2.htm`.

- Extranet, Intranet
  Unternehmensweite *Intranets* können über das Internet zu einem *Extranet* verbunden werden. Das Extranet ist damit Teil des globalen Kommunikationssystems.

- Günstig für internationale Geschäftsbeziehungen
  Mitarbeiter eines Unternehmens, zum Beispiel im Vertrieb, greifen aus allen Ländern der Welt über das Internet auf die Rechnersysteme der Zentrale zu. Die Vorteile liegen auf der Hand: Preise, Lieferzeiten, neue Informationen können schnell abgerufen und Bestellungen sofort übermittelt und bearbeitet werden. Es gibt keinen Medienbruch, die Informationen müssen nur einmal eingegeben werden. Dies ermöglicht die effiziente Abwicklung immer komplexer werdender Aufgaben.

1.3 Allgemeine Bedrohungen aus dem Internet

In den letzten Jahren hat sich die Moral der Hacker gewandelt: Früher waren Hacker Tüftler, die aus Spaß an der Sache oder um ihr Können unter Beweis zu stellen, in fremde Datenbanken einbrachen und sich einen Jux erlaubten, der dem Betroffenen allenfalls einen Schreck einjagte oder ihn ärgerlicherweise teure Arbeitszeit kostete.

Heute agieren sie professionell und organisiert als Cracker – was nicht weiter verwunderlich ist, wenn man bedenkt, wie viel Gewinn sich mit den Daten und Informationen erzielen lässt, die in Netzen kursieren. Dabei haben die meisten Cracker kein Unrechtsbewusstsein und keine Moralvorstellung.

Obwohl viele Fälle von Computerkriminalität und Spionage bekannt geworden sind und die dadurch entstehenden Schäden in Milliardenbeträgen gerechnet werden (siehe Anhang A), wurde das Thema Sicherheit lange unterschätzt und sorglos übergangen. Die Schnelligkeit und die Informationsvorteile der Kommunikationsnetze werden genutzt, ohne dass man sich – bildlich gesprochen – um Sicherheitsgurte, Knautschzone und Airbag kümmert.

Der Missbrauch von Kommunikationsnetzen ist bereits heute ein großes Problem. Hinter mancher Hackergeschichte in der Presse verbirgt sich vielleicht eine Legende – das darf aber nicht darüber hinwegtäuschen, dass die Frage der Sicherheit vermutlich noch brisanter ist, als die bisher bekannt gewordenen Fälle von Einbrüchen und Missbrauch nahe legen.

Cracker und ihre Methoden werden immer erfindungsreicher, zumal die Beute, um die es geht, immer lohnender wird. Anders als bei einem Bankraub in der realen Welt ist das Risiko für Cracker nicht allzu groß, denn sie sind nur schwer zu verfolgen. Sind die Einbrecher erst einmal im System, ist es fast unmöglich, sich an ihre Fersen zu heften. Noch leichter ist es, Daten während der ungeschützten Übertragung durch das Internet »abzufangen« – die Möglichkeit besteht an fast jedem beliebigen Netzknoten, und die Wahrscheinlichkeit, dass ein solcher Angriff auf die Kommunikationsbeziehung überhaupt bemerkt wird, ist gering.

1.4 Notwendigkeit von IT-Sicherheit

Wozu brauchen wir Sicherheit in der Informationstechnik?

Ein moderner Arbeitsplatzrechner hat heute die gleiche Leistungsfähigkeit wie ein klassisches Rechenzentrum vor einigen Jahren. Bei diesen Rechenzentren genügten noch Sicherheitsmaßnahmen, die mit Hilfe von organisatorischen und personellen Regelungen durchgeführt wurden. Dazu gehörten unter anderem

- Zugangskontrolle zu den Gebäuden und Räumen der Rechenzentren
- kontrollierte und definierte Arbeitsabläufe und eine dementsprechende Auftragsabwicklung
- Trennung zwischen dem Personal der Fachabteilung (den Anwendern) und den DV-Mitarbeitern (Programmierern, Operateuren usw.)

Die EDV stand abgeschottet in einem Gebäude, wodurch die externen Bedrohungen überschaubar waren, und das Betriebssystem des Hosts war für den Schutz der Ressourcen vor unerlaubtem Zugriff zuständig.

Durch moderne informationstechnische Konzepte wie Client-Server-Verbindungen, Down-Sizing, Out-Sourcing, Internet, Intranet usw., in denen Informationen über ein angreifbares Netz ausgetauscht werden, verlassen Daten die »geschützte Umgebung« und sind damit neuen Gefahren ausgesetzt.

Die heutigen verteilten Rechnersysteme mit ihren »offenen« Verbindungen lassen sich nicht mehr allein durch organisatorische Maßnahmen schützen. Es müssen zusätzliche *technische Sicherheitsmechanismen* bereitgestellt werden, die eine sichere und kontrollierbare Informationsübertragung und -verarbeitung ermöglichen. Dazu sind strategische Sicherheitskonzepte notwendig, die *Vertraulichkeit und Integrität* der per Netzwerk übermittelten Daten gewährleisten. Außerdem müssen Verbindlichkeit und Zurechenbarkeit der Vorgänge und Veranlassungen – wo immer notwendig – garantiert werden.

Welche Rolle spielt IT-Sicherheit in der Informationsgesellschaft?

In den letzten Jahren hat sich der Wert der Informationen und damit der Schutzbedarf beträchtlich vergrößert.

Der steigende Wert von Informationen ist ein wichtiger, wenn nicht der wichtigste Wirtschaftsfaktor geworden. Beispiele sind:

- Vollständige Entwicklungs- und Fertigungsunterlagen: Manche Organisationen besitzen Hardware im Wert von 5000 EUR, auf der Informationen im Millionenwert gespeichert sind.
- Geschäfts- und Betriebsergebnisse, Strategiepläne: Wenn solche Ergebnisse oder Pläne der Öffentlichkeit bekannt werden, können damit beispielsweise Börsen-Aktivitäten in Bewegung gebracht werden, die wiederum hohe Verluste verursachen können.
- Logistikinformationen: Falls Daten nicht mehr verfügbar oder nicht mehr verlässlich sind, weiß kein Mitarbeiter mehr, wie groß der Lagerbestand ist, welche Kunden welche Produkte bestellt haben und wann an wen geliefert werden soll.
- Kundendaten: Diese stellen einen erheblichen Wert dar, den es zu schützen gilt.

Netzwerkstrukturen ermöglichen eine effiziente Abwicklung von Aufgaben, die in vielen Bereichen anders kaum noch zu erfüllen sind. Wir sind in solchem Ausmaß von Kommunikationssystemen abhängig, dass unsere wirtschaftliche Leistungsfähigkeit gefährdet ist, wenn die Funktionsfähigkeit der Systeme nicht in angemessener Weise gewährleistet werden kann.

Globale Ausdehnung und Veränderung der Geschäftsprozesse

Die meisten Geschäftsprozesse (Angebotserstellung, Auftragsannahme, Bestellung, Liefereingang) wurden in der Vergangenheit auf dem Papier oder persönlich bei Kundenbesuchen abgewickelt. Diese Abläufe können weitaus rationeller gestaltet werden, indem der personelle und materielle Aufwand durch elektronische Verfahren verringert wird. Geschäftsunterlagen können per Rechnersystem erstellt und elektronisch übertragen werden, so dass kein Medienbruch mehr auftritt.

Unsere Rechnersysteme und insbesondere die darauf verarbeiteten Informationen werden dadurch immer attraktiver für potenzielle Angreifer. Gleichzeitig kommt heute keine Behörde und kein Unternehmen mehr ohne die Verlagerung von Geschäftsprozessen und die Vernetzung von Rechnersystemen aus.

Einerseits möchte man leicht handhabbare und immer verfügbare Verbindungen nach außen haben. Andererseits müssen geschäftsinterne Daten und Beziehungen zu Geschäftspartnern vor Diebstahl, Manipulation und mutwilliger Zerstörung geschützt werden.

In Kaufhäusern sind Wachpersonal und Detektive, Videoüberwachung und stählerne Rollläden selbstverständlich. Aber erst in jüngster Zeit machen sich Organisationen Gedanken darüber, dass auch Daten vor unbefugtem Zugriff geschützt werden sollten, weil sie einen erheblichen Wert darstellen – oft sogar den Hauptanteil ihres Vermögens.

Die Informationstechnologie hat Möglichkeiten geschaffen, Wirtschaftsspionage bequem mit Rechnersystemen zu betreiben. Für diese neue Form der Spionage, bei der keine Wände eingerissen oder Tresore geknackt werden müssen, fehlt häufig jegliches Unrechtsbewusstsein der Täter, die ihre Arbeit vom Wohnzimmer aus erledigen. Die Tools für solche Aktivitäten sind auf dem Softwaremarkt oder im Internet frei erhältlich, ausführliche Informationen dazu gibt es in der Literatur und im Web.

Experten schätzen die wirtschaftlichen Schäden, die durch Computerkriminalität entstehen, bereits heute auf Milliardenbeträge – mit steigender Tendenz.

Staatliche Industrie- und Wirtschaftsspionage

IT-Kriminalität wächst mit dem Kommunikationsmöglichkeiten: Wirtschaftsspionage ist ein Hauptproblem im heutigen Business und hat seit Beendigung des Kalten Kriegs die militärische Spionage abgelöst. Dabei werden die wesentlichen Gefahren nicht mehr geographisch-politisch (westliche und östliche Staaten), sondern nach der Konkurrenzfähigkeit der Staaten eingeschätzt.

US-Präsident Bill Clinton erklärte »ökonomische Aufklärung« zum Staatsziel und stattete den »Supergeheimdienst« National Security Agency (NSA) mit entsprechenden Mitteln aus.

Die USA unterhalten mit einigen befreundeten Staaten das globale Echelon-System, um Kommunikation (per Telefon, Fax, DFÜ, Internet, ...) abzuhören und automatisiert auszuwerten. Bürgerrechtler verfolgen dies mit Sorge. Ein Zitat von `www.echelonwatch.org`:

> *»Echelon is perhaps the most powerful intelligence gathering organization in the world. Reports suggest that this network is being used to spy on private citizens everywhere, including on the Internet.«*

Aufschlussreich ist auch der STOA-Report des Europäischen Parlaments »An Appraisal of the Technologies to Political Control« (Download und aktuelle Ergänzungen unter `www.europarl.eu.int/dg4/stoa/en` oder `http://cryptome.org/stoa-atpc.htm`).

Schließlich meldete die Berliner Tageszeitung »taz« am 10. Januar 2000 unter der Schlagzeile

> *»Präsident Clinton legt Zwei-Milliarden-Dollar-Programm auf: Gegen Internet-Terroristen und für die Ausbildung des Spionage-Nachwuchses«,*

in dem Drei-Jahres-Plan seien – so die »taz« – allein 150 Millionen Dollar »Stipendien« enthalten, um Wissenschaftler und Studenten in »IT-Sicherheitsfragen auszubilden«.

1.5 IT-Sicherheit als Wirkungs- und Handlungszusammenhang

IT-Sicherheit beschäftigt sich mit dem Schutz von Werten gegen Angriffe, wobei Angreifer das Ziel haben, die Werte für eigene Zwecke zu nutzen oder den Eigentümer zu schädigen /Comm98/:

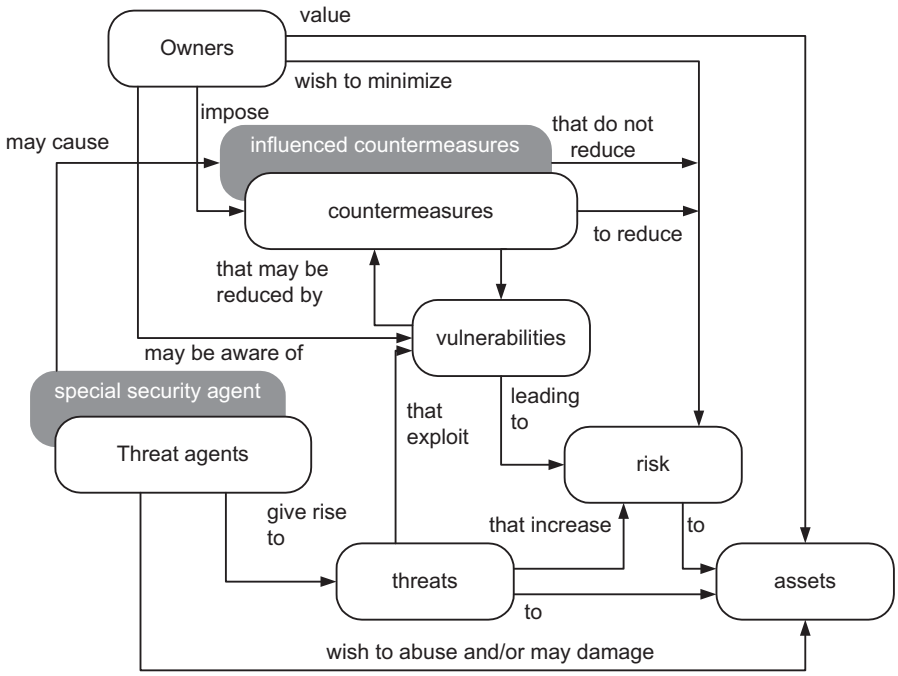

Abb. 1.2: IT-Sicherheit als Wirkungs- und Handlungszusammenhang

Die Sicherung der Werte (Assets) liegt in der Verantwortung ihres Eigentümers (Owner). Die Angreifer (Threat Agents) wollen mit einem Angriff (Threat) auf die Werte deren Vorteile ausnutzen und handeln somit gegen den Eigentümer der Werte. Der Eigentümer nimmt den Angriff – sofern er ihn bemerkt – als Reduzierung seiner Werte wahr. Spezielle Angreifer (zum Beispiel Geheimdienste) sind in der Lage, die Hersteller von Gegenmaßnahmen so zu beeinflussen, dass diese Möglichkeiten einbauen, die es diesen Angreifern erlauben, trotz der Gegenmaßnahmen auf die Werte zuzugreifen.

Für den Eigentümer bedeutet dies wiederum eine Reduzierung seiner Werte und ist als »trügerische Sicherheit« in Wirklichkeit nur eine scheinbare Reduzierung seines Risikos.

Die Angriffe auf IT-Werte beziehen sich in der Regel – aber nicht ausschließlich – auf:

- Verlust der Vertraulichkeit:
  Angreifer kommen unberechtigt in den Besitz der Werte (Informationen).
- Verlust der Integrität:
  Angreifer sind in der Lage, unautorisiert Werte (Informationen) zu manipulieren.

- Verlust der Verfügbarkeit:
  Angreifer enthalten dem Eigentümer den berechtigten Zugriff auf Werte (Informationen, Betriebsmittel etc.) vor.
- Verlust der Verbindlichkeit:
  Die Verbindlichkeit der Transaktion ist nicht gewährleistet. Das Senden und Empfangen von Werten/Information kann geleugnet werden.
- Verlust der Authentizität:
  Die Echtheit des Kommunikationspartners wird gefälscht, der Ursprung der Information (Daten) ist nicht gesichert.

1.6 Chancen und Risiken der Informationstechnik

Jeder Eigentümer von (Informations-) Werten sollte eine Analyse durchführen, welche Angriffe für ihn relevant sind und welche er vernachlässigen kann. Diese Analyse der möglichen Angriffe hilft ihm, geeignete Gegenmaßnahmen auszuwählen, die sein Risiko der Verwundbarkeit auf ein akzeptables Maß reduzieren.

Die Verwundbarkeit und damit der eigene Schutzbedarf ist in der Regel für verschiedene Anwendungen sehr unterschiedlich /Bans96/.

Die eingeführten Gegenmaßnahmen reduzieren die Verwundbarkeit und müssen mit der jeweiligen Sicherheitspolitik übereinstimmen. Auch nach der Einführung der Gegenmaßnahmen bleibt eine Rest-Verwundbarkeit bestehen, die mit anderen Maßnahmen weiter eingeschränkt werden kann /Zurf99/.

Die folgende Grafik symbolisiert den durch »best practice« maximierten Geschäftserfolg:

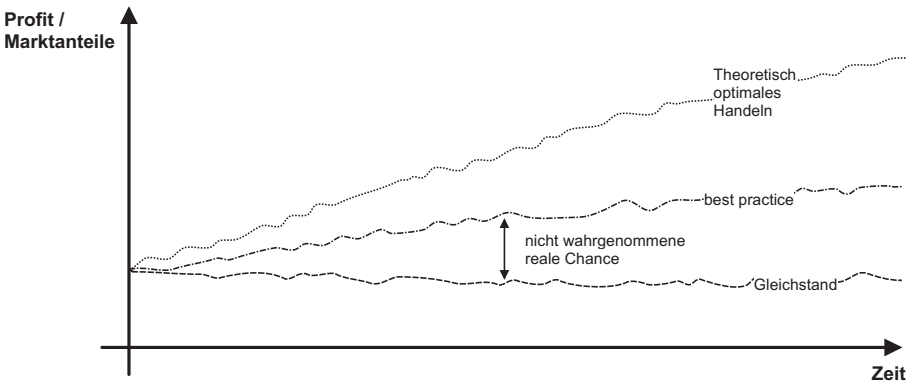

Abb. 1.3: Chancenoptimiertes geschäftliches Handeln

Es besteht weitgehend Einigkeit darüber, dass zum einen die Ungewissheit über das Kommende und zum anderen die negative Valenz des möglichen Ereignisausgangs die zentralen Bestimmungsstücke des Risikos darstellen.

Die Nutzung von Informationstechnik ist immer Chance und Risiko zugleich: Chance, ein angestrebtes Ziel zu erreichen, beispielsweise die Vorteile des Internet zu nutzen und dadurch etwas zu gewinnen (Profit, Marktanteile etc.), und Risiko, dass man etwas Existierendes (Werte) durch das eigene Handeln – zum Beispiel durch die Nutzung des Internet – zur Disposition stellt und dass dadurch Informationswerte beeinträchtigt werden oder man diese sogar verliert /Birn96/ (siehe Abb. 1.4).

Unternehmen und Organisationen sollten die Chancen nutzen, die die Informationstechnik eröffnet – zum Beispiel durch Nutzung des Internets – aber zugleich durch Investitionen in die geeigneten Gegenmaßnahmen (Firewall-Systeme, VPNs, Intrusion-Detection-Systeme, Anti-Virus-Systeme, ...) dafür sorgen, dass das Risiko einer Verwundbarkeit reduziert wird. Hierdurch ist verantwortungsvolles Handeln möglich und die Leistungsfähigkeit beziehungsweise Profit und Marktanteil wird gesteigert – zur betriebswirtschaftlichen und in summa schließlich auch zur volkswirtschaftlichen Blüte /Mcke95/.

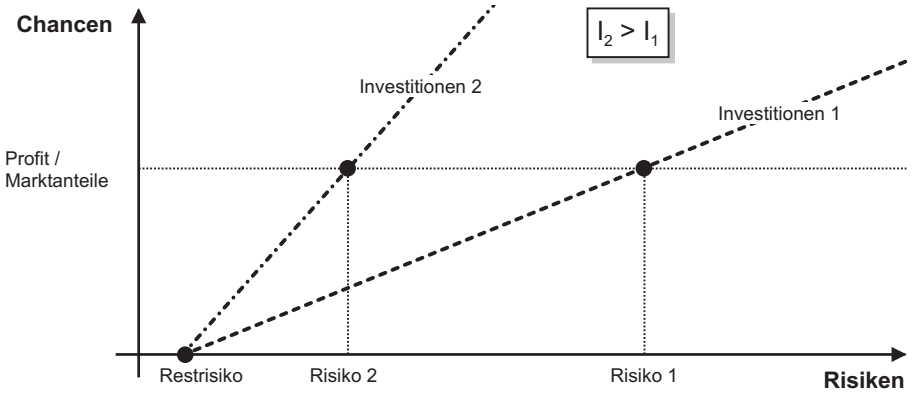

Abb. 1.4: Angemessene Investitionen

In diesem Zusammenhang sei auf zwei Bücher von Tim Cole hingewiesen: »Erfolgsfaktor Internet – Warum kein Unternehmen ohne Vernetzung überleben wird« /Cole99a/ sowie: »Managementaufgabe Sicherheit« /Cole99b/.

1.7 Der VPN-Markt

Das Thema VPN ist so sehr in Bewegung, weil es vor allem durch die Anwender vorangetrieben wird und erst in zweiter Linie durch die Hersteller von Geräten und Software.

Im Rahmen von E-Commerce, E-Business und Remote-Access-Projekten ist die Ausdehnung der Unternehmensnetze gegenwärtig ein zentraler Aspekt in der IT-Welt. Daran wird sich auch in den kommenden Jahren wenig ändern. Soll eine vertrauenswürdige Kommunikation über öffentliche Netzwerke erfolgen, liegt die Erwägung nahe, ein VPN einzurichten.

Was den Einstieg in das Thema VPN interessant macht, ist zum einen die Verfügbarkeit des IPSec-Standards in einer Vielzahl marktreifer Produkte. Denn mit dem IPSec-Standard ist auch ein Haupthemmnis im Bereich der Netzwerksicherheit beseitigt: Anwender erhalten die notwendige Gewährleistung der Investitionssicherheit bei der Anschaffung neuer Produkte, weil sie auch herstellerübergreifend weitgehend interoperabel sind. Zum anderen bewirkt der durch Innovationen angeregte Wettbewerb, dass den Anwendern neue und auf ihre Anforderungen zugeschnittene Lösungen bereitgestellt werden.

Ein weiterer Trend, der zu beobachten ist, ist das Auslagern von Dienstleistungen rund um das Thema Sicherheit: In Organisationen mit geringem Netzwerk-Know-How können in Zukunft externe Dienstleister mit »managed VPNs« die Inhouse-Lösung ersetzen.

Von geringerer Relevanz ist der Wunsch der Organisationen, Kosten zu sparen. Dennoch ist dieses Motiv nicht von der Hand zu weisen, wenn Niederlassungen oder Telearbeitsplätze günstig mittels eines VPN über das öffentliche Telefonnetz anstatt über teuer gemietete Standleitungen angebunden werden können.

Natürlich ist auch der Einsatz von VPNs mit Kosten verbunden, doch kann sich dieser Aufwand auf zweierlei Arten amortisieren:

1. Wie bereits beschrieben, können Niederlassungen, Telearbeitsplätze und mobile Mitarbeiter über günstige lokale Wählverbindungen an das Unternehmensnetz gekoppelt werden und es müssen keine teuren »Leased Lines« verwendet werden.
2. Durch Investitionen in Sicherheitstechnologie kann eine Organisation sich bei Ihren Kunden einen Vertrauensvorsprung vor möglichen Wettbewerbern erarbeiten. Das erhöhte Sicherheitsniveau wird von den Kunden registriert und mit dauerhaften Geschäftsbeziehungen honoriert werden. Schließlich gehen Schreckensnachrichten über Angriffe auf E-Commerce- und E-Business Webseiten beinahe regelmäßig durch die Medien. Und so werden sich die sicherheitsbewussten Kunden bei den Unternehmen wiederfinden, die ein angemessen hohes Sicherheitsniveau bieten. Die Ausgaben, die für ein VPN

entstehen, können daher als vertrauensstiftende Maßnahmen angesehen werden. Damit können möglicherweise auch Investitionen in E-Commerce-Projekte gerettet werden, deren Akzeptanz aufgrund mangelnden Vertrauens niedrig ist.

Als Bremsen für den Einsatz von VPNs haben sich bisher die Investitionskosten und die möglicherweise übertriebenen Versprechungen der Hersteller erwiesen. Gerade hier setzt sich auf dem Markt jedoch eine rationellere Sichtweise über die Möglichkeiten und Grenzen von VPNs durch. Die renommierten Anbieter haben nun schon einige – auch große – Installationen bewältigt und können diese Erfahrungen auf neue Projekte übertragen. Somit verkürzen sich derzeit die Einkaufs- und Einführungsprozesse, und ein VPN ist ein »must-have« für die Mehrzahl von Unternehmen.

Auch Service Provider haben sich mit dem Thema VPN noch nicht ausreichend auseinandergesetzt. Bisher haben nur wenige erkannt, dass sie den Kunden mit einer erhöhten und in Service Level Agreements (SLAs) garantierten Sicherheit einen Mehrwert bieten können. Insbesondere kleineren und mittleren Organisationen können die Service Provider die Sorgen um die ungesicherte Kommunikation nehmen, wenn sie in diesem Bereich Produkte und Servicepakete anbieten. Diese Entwicklung wird zusätzlich durch die – vermutlich anhaltende – Knappheit an qualifizierten Sicherheits-Mitarbeitern forciert. Auch aus diesem Grund werden Fachleute von außerhalb herangezogen und Sicherheitsdienstleistungen ausgelagert.

Bisher galten »Dedicated Line Networks« als die sicherste Form einer Kommunikationsinfrastruktur. Mit der Erkenntnis beziehungsweise dem Nachweis, dass dies nicht der Fall ist, investieren nun viele Organisationen in den Aufbau sicherer VPNs. Weil der Anschluss an das Internet wesentlich günstiger ist als »Dedicated Line Networks«, können nun auch einzelne Rechner beziehungsweise Arbeitsplätze und weltweit verteilte Büros kostengünstig angebunden werden. Selbst für kleinere Organisationen, Mittelständler und in einem Projektnetz arbeitende Freiberufler ist dies möglich. Weil die öffentlichen Leitungen in diesem Fall von Beginn an für geschäftskritische Anwendungen und Informationen genutzt werden, steht die Frage nach Sicherheit in Form von Vertraulichkeit, Manipulationsschutz und Verfügbarkeit sofort im Raum.

Die Nachfrage auf dem europäischen VPN-Markt wird von Unternehmen und Organisationen verschiedenster Art und Größe bestimmt. Service Provider haben nun das Potential dieser Technologie erkannt; sie entwickeln und bieten Lösungen für die verschiedenen Einsatzgebiete an. Viele der großen multinationalen Konzerne planen, ihre Netzwerke über IP-VPNs zu erweitern und werden ihre ATM- und Frame-Relay-Netzwerke nach und nach ersetzen.

VPN-Marktzahlen nach einer Studie von Frost & Sullivan

Dem VPN-Markt in Europa wird – auch zukünftig – ein kräftiges Wachstum bescheinigt: Für 1999 wurde eine Marktgröße von ca. 85 Millionen US-$ festgestellt; das jährliche Marktwachstum soll zwischen 1996 und 2006 bei durchschnittlichen 45,1% liegen. Markt- und Technologieanalysten unterscheiden den VPN-Markt nach Hardware- und Softwarelösungen.

Millionen $	1996	1997	1998	1999	2000	2001	2002	2004	2006
Hardware	10.6	22.4	44.7	84.9	148.6	237.8	368.6	799.9	1149.9
Software	7.5	15.9	31.7	60.2	102.4	176.1	308.2	644.9	890.0
Gesamt	18.2	38.2	76.4	145.2	251.0	413.9	676.8	1445	2040

Tabelle 1.1: VPN Markt 1996-2006
(aus: European Internet Communications Security Market, Frost&Sullivan, 11/2000)

1.8 Fazit

Die internationale wirtschaftliche Ausdehnung vieler Organisationen – man denke an die Mega-Fusionen von Daimler-Benz und Chrysler, Vodafone und Mannesmann oder die größte Fusion der bisherigen Wirtschaftsgeschichte zwischen AOL und Time Warner – braucht vernetzte IT-Strukturen und eine Kommunikationsplattform wie das Internet. Das Internet dringt in viele öffentliche und private Lebensbereiche vor und eröffnet gleichzeitig neue rechtliche, soziale und ethische Probleme, denen wir uns stellen müssen. Politische und juristische Instrumente stehen noch nicht zur Verfügung, um einem Missbrauch wirksam begegnen zu können.

Informationstechnologie kann nur sinnvoll eingesetzt werden, wenn sie sicher und beherrschbar ist. Die Bedrohungen, die aus der neuen Technik resultieren, können wir nicht beeinflussen, sehr wohl aber unsere Verletzbarkeit.

Voraussetzung dafür ist jedoch, dass für bewährte klassische Sicherheitsmechanismen wie Pförtner, Briefumschlag, Siegel, handgeschriebene Unterschrift, Rohrpost und Sicherheitstransporter elektronische Äquivalente eingesetzt werden.