

1 Sicherheit im Internet – Grundlagen und Methoden

1.1 Einführung

Online-Dienste, Cyberspace, Electronic Commerce – Schlagwörter einer »Revolution, die die Menschheit ins Informationszeitalter trägt«. So wurde sie zumindest im Schlußdokument der G-7 Konferenz in Brüssel im Februar 1995 bezeichnet – die rasante Entwicklung der Menschheit zur globalen Informationsgesellschaft, die mit vielen Hoffnungen, aber auch Risiken verbunden ist. Inzwischen haben zahlreiche Berichte über Viren, spektakuläre Einbrüche in als hochsicher geltende Computersysteme oder Wirtschaftsspionage im großen Stil zu verunsicherten Anwendern geführt. Motiviert durch das prognostizierte Wachstum der Märkte für Online-Dienste gibt es trotz der erwähnten Gefahren heute kaum noch eine Branche, in der Unternehmen nicht ihre internen Systeme und Netze mit dem Internet verbinden. Während sich viele Firmen steigende Gewinne durch höhere Umsätze und Vorteile bei der Abwicklung von Geschäftsprozessen versprechen, scheuen andere immer noch den ersten Schritt. Sie sehen im Internet eher einen Tummelplatz für Betrüger, die über die nicht mehr zu überblickenden Netzstrukturen ihr Unwesen treiben.

Die Voraussetzungen für den Datenklau im Internet scheinen ideal. Während der Geheimagent noch in früheren Zeiten Briefumschläge in filigraner Handarbeit präparieren mußte, lassen sich die elektronischen Datenströme heute in Sekunden durchforsten. Offizielle Stellungnahmen der Europäischen Union bestätigen eine lang gehegte Vermutung: Das Projekt ECHELON, ein System aus weltweit vernetzten Abhörstationen, ermöglicht internationalen Geheimdiensten, allen voran der amerikanischen National Security Agency (NSA), eine systematische Rasterfahndung in der Telefon-, E-Mail-, Internet- und Satellitenkommunikation von Regierungsstellen, Organisationen und der Wirtschaft. Bestand bei einem Banküberfall noch die begründete Hoffnung, den Dieb anhand von Videoaufzeichnungen oder Fingerabdrücken zu fassen, hinterläßt der Raubzug durch digitale Schatzkammern keine rechtskräftigen Beweise. Und was sich in den exponierten Systemen an Belastungsmaterial ansammelt, ist zu leicht manipulierbar und wird oftmals vor Gericht nicht anerkannt. Selbst wenn der Angriff entdeckt wird, schützen die vorhandenen Gesetze den Geschädigten äußerst un-

*Internet – Eldorado für
Ganoven?*

Unklare Rechtslage

zureichend. Im Zweifel muß er zuerst ein umfassendes Sicherheitskonzept vorweisen, bevor ihm die Paragraphen ein Recht auf Schadensersatz zusprechen.

Täterkreis und Motivation

Unbestritten ist, daß sich mit dem Anschluß an ein für jedermann zugängliches Netz zugleich die Wahrscheinlichkeit erhöht, gelegentlich auch ungebetene Gäste zu Besuch zu haben. Wer sich dabei nur auf Recht und Gesetz verläßt und sich nicht durch ein angemessenes Sicherheitskonzept schützt, handelt unverantwortlich. Vom Teenager, der aus sportlichem Ehrgeiz die Homepage unbemerkt nach seinen Vorstellungen verschönert, bis zum professionellen Industriespion, der im Auftrag der Konkurrenz vertrauliche Dokumente entwendet, ist im Internet alles vertreten. Wie in einem Kaufhaus werden die Ladendiebe keinen Versuch auslassen, vorhandene Sicherheitsvorkehrungen zu umgehen. Ob durch Videokamera, Detektiv oder Alarmanlage geschützt: Die offenstehende Seitentür oder das Versteck in der Warenanlieferung kann schnell zum Erfolg führen.

Informationen gelten heute als wirtschaftliches Gut mit einem oftmals großen Wert für den Besitzer

Angriffe aus dem Internet erfolgen oft auf die gleiche Weise. Im Glauben, sich durch eine Firewall ausreichend gegen Angreifer zu schützen, unterschätzen viele in vernetzten Systemen die immer wieder neu entstehenden Schlupflöcher. Sie ebnen den Weg zum kostbarsten Gut im Unternehmen, der Information, die im Zeitalter der elektronischen Kommunikation für den normalen Anwender und speziell für den kommerziellen Anbieter immer mehr an Wert gewinnt. Ein Verlust kann sich für eine Firma existenzbedrohend auswirken.

Fragen wie »Ist es für Mitbewerber möglich, an die firmeninternen Daten zu gelangen?«, »Gibt es Schwachstellen?« und »Welcher Aufwand ist nötig, um sie zu beseitigen?« werden häufig erst nach dem Anschluß der IT-Infrastruktur an das Internet gestellt. Dabei würde eine sorgfältige Planung vorab unnötige Kosten durch Schadensfälle vermeiden helfen. Der Einsatz offener, standardkonformer Systeme bietet vielversprechende Möglichkeiten für die effiziente Geschäftsabwicklung, ist aber zugleich ein sehr verletzlicher Bereich, über den ein Unternehmen nachhaltig geschädigt werden kann. Die Risiken beim Wechsel von zentralen IT-Strukturen zu verteilten Systemen müssen rechtzeitig erkannt werden, um wirkungsvolle Sicherheitsmaßnahmen einzuleiten.

Voraussetzung für die Entwicklung einer umfassenden Strategie zum Schutz der Unternehmensdaten ist zunächst ein grundlegendes Verständnis der im Internet verwendeten Techniken und den damit verbundenen Gefahren. Aus diesem Grund gibt der erste Teil des Buches eine generelle Einführung in die Sicherheitsproblematik im Internet. Es werden Grundbegriffe und Zusammenhänge erläutert sowie gängige

Methoden zur Risikoanalyse vorgestellt. Ausgangspunkt für die Diskussion über konkrete Bedrohungen ist eine Beschreibung der Architektur des weltweiten Netzverbundes. Dabei liegt der Schwerpunkt auf den verwendeten Protokollen. Eine Betrachtung der Schwachstellen und der daraus resultierenden Risiken beschließt den ersten Teil.

1.2 Sicherheit

Begriffsauffassungen zum Thema Sicherheit in der Informationstechnologie (IT) gibt es viele. Abhängig vom jeweiligen Einsatz der Computersysteme wird Sicherheit beispielsweise im militärischen Umfeld häufig unter Gesichtspunkten der Geheimhaltung zum Schutz vor Spionage sowie der ständigen Verfügbarkeit der Systeme verstanden. Als vor etwa 30 Jahren das amerikanische Department of Defense (DoD) mit der Planung des heute als Internet bekannten Netzwerks begann, konnte niemand ahnen, daß es später einmal als Transportmedium für internationale Geschäftstransaktionen eingesetzt werden würde. Die Netzwerkprotokolle mußten Leitungsausfälle erkennen und automatisch alternative Übertragungswege finden. Die Lösung besteht in einem Netzwerk ohne zentrale Vermittlungsstelle, so daß die angeschlossenen Rechner bei Ausfall eines Netzknotens trotzdem weiter kommunizieren können. Auf diese Infrastruktur aufsetzend wurde das Internet Protocol (IP) als verbindungsloses und paketvermittelndes Protokoll entwickelt. Die Notwendigkeit für weitere Sicherheitsmechanismen sah man zu diesem Zeitpunkt nicht, da nur bekannte, autorisierte Regierungsstellen Zugang zu dem damals noch geschlossenen Netzverbund erhielten.

Mit dem Anschluß von Universitäten, Bildungs- und Forschungsorganisationen in den späten 70er und den frühen 80er Jahren erfuhr der Sicherheitsbegriff im Internet erstmals eine Veränderung. Die Öffnung hatte zur Folge, daß der Zugriff auf die Daten und Kommunikationsdienste kontrolliert erfolgen und überwacht werden mußte. Die verstärkt kommerzielle Ausrichtung der im Internet angebotenen Dienste mit Beginn der 90er Jahre führte ein weiteres Mal zu einem nachhaltigen Wandel der Sicherheitsanforderungen. Nicht nur die große Teilnehmerzahl ohne explizite Identifikation, sondern auch die Inhalte der übertragenen Daten potenzieren heute die Gefahr von Mißbrauch. Im Vergleich zum mittlerweile sprichwörtlichen Kellner, der heimlich die Kreditkartennummern seiner Gäste aufschreibt, erlaubt der hohe Automatisierungsgrad bei Angriffen im Internet, sehr viel größere Datenmengen in kurzer Zeit zu sammeln und zu analysieren.

*Bedeutung der Sicherheit
in den Gründerjahren des
Internet*

*Verständnis in den 80er
Jahren*

*Heutige Begriffsdefinition
im Zeichen der
Kommerzialisierung*

1.2.1 Sicherheitsdienste

- Grundbedrohungen* Sicherheitsdienste sind Funktionen, die ein IT-System bereitstellen muß, um den Sicherheitsanforderungen seiner Benutzer zu entsprechen. Systeme, die Gebrauch von offenen und somit von jedermann zugänglichen Netzwerken machen, müssen grundsätzlich für ein gewisses Maß an Vertraulichkeit, Integrität und Verfügbarkeit sorgen. In der englischsprachigen Literatur (u. a. [PFL96], [HOL91]) werden diese Sicherheitsdienste häufig unter der Abkürzung CIA (engl. Confidentiality, Integrity, Availability) aufgeführt. Gleichzeitig werden immer wieder die unterschiedlichen Gefahren in offenen Netzen aufgrund ihrer Auswirkungen diesen drei Gesichtspunkten zugeordnet, so daß man auch von den Grundbedrohungen [BSI92] spricht.
- Vertraulichkeit* Vertraulichkeit schützt geheime Informationen beim Transport über das Internet vor unberechtigten Einblicken durch Dritte. In diese Kategorie fallen z. B. die private Korrespondenz, Paßwörter oder Zahlungsinformationen. Oftmals gehen die Anforderungen an die Vertraulichkeit sogar so weit, daß bereits die bloße Existenz der Informationen für Außenstehende nicht mehr erkennbar sein darf.
- Integrität* Unter der Erhaltung der Integrität bzw. Unversehrtheit von Daten wird die Sicherung gegen beabsichtigte oder zufällige Manipulation verstanden. Integritätsverletzungen können z. B. durch Übertragungsfehler oder bewußt herbeigeführte Attacken entstehen, indem ein Angreifer während der Übertragung Teile der Informationen modifiziert bzw. ersetzt. Dem Empfänger muß die Möglichkeit gegeben werden, die Unverfälschtheit der Daten überprüfen zu können.
- Verfügbarkeit* Verfügbarkeit trifft Vorsorge dafür, daß nutzungsberechtigte Personen auf Informationen und Kommunikationsdienste zur rechten Zeit am rechten Ort zugreifen können. Die Anforderungen eines Systems an die Verfügbarkeit sind stark von dessen Einbindung in die operativen Abläufe eines Unternehmens abhängig. Bezogen auf das Internet hat ein Teil- oder Komplettausfall eines öffentlichen Informationsservers nur geringe Auswirkungen auf die Leistungsfähigkeit und Servicebereitschaft einer Firma. Weitaus gravierender sind die Folgen, wenn mit den betroffenen Systemen, wie im Falle eines Internet-Dienstansbieters (engl. Internet Service Provider, ISP), kostenpflichtige Dienstleistungen angeboten werden. Der zahlende Kunde setzt eine ständige Erreichbarkeit und hohe Datendurchsatzraten voraus. Bei Leistungsengpässen drohen dem Betreiber schlechte Presse und eventuell sogar Schadensersatzansprüche. Wird das Internet von einem Unternehmen als Vertriebskanal genutzt, führen Betriebsunterbrechungen oder lange Antwortzeiten unweigerlich zu Umsatzeinbußen und verärgelter Kundschaft.

Betrachtet man die Entwicklung der im Internet bereitgestellten Dienste, so läßt sich ein starker Trend weg von der Nutzung als reines Informations- und Marketinginstrument, hin zu kommerziellen Angeboten feststellen. Ob Home-Banking, Internet-Einkaufszentren oder Online-Reservierungssysteme – geschäftliche Transaktionen werden zunehmend über das Kommunikationsmedium abgewickelt und stellen über die genannten Grundbedrohungen hinaus weitere Anforderungen an die Sicherheit der dahinter operierenden Systeme.

*Trendwende bei den
Internet-Diensten*

Der hohe Abstraktionsgrad der Daten in einem Netzwerk führt dazu, daß sich jeder Teilnehmer im Internet hinter einer »digitalen Maske« versteckt. Diese vorherrschende Anonymität macht es erforderlich, daß ein Benutzer vor dem Zugriff auf personenbezogene Daten und Kommunikationsdienste einen eindeutigen Beweis seiner Identität erbringen muß. Authentifikationsmechanismen prüfen die Authentizität (engl. authentication), also die Echtheit von Personen, Organisationen oder Programmen. Im Internet könnte ein solcher Dienst z. B. dafür sorgen, daß beim elektronischen Briefverkehr der Absender einer Nachricht eindeutig vom Empfänger identifiziert werden kann.

Authentifikation

Im Zusammenhang mit sicherheitsrelevanten Zwischenfällen im Internet wird immer wieder von Einbrüchen in lokale Netzwerke berichtet. Dabei gelingt es den Angreifern oftmals, auf geschützte Informationen zuzugreifen und sie zu verändern. Schutz gegen Bedrohungen dieser Art bietet die Zugriffskontrolle (engl. access control), die zumeist der Authentifikation nachgeschaltet ist und dafür zu sorgen hat, daß nur berechnete, also zuvor identifizierte und somit autorisierte Benutzer auf die ihnen zugeordneten Ressourcen zugreifen können. In Netzen mit großen Benutzerzahlen wie dem Internet ist die Verwaltung und Überprüfung von individuellen Zugriffen oftmals nicht mehr möglich. Besucher werden daher klassifiziert nach anonymen Gästen, denen lesender Zugriff auf allgemeine Informationen gewährt wird, und registrierten Benutzern, die Zugang zu erweiterten Dienstleistungen erhalten.

Zugriffskontrolle

Überall dort, wo juristische Rahmenbedingungen eine Rolle spielen, wie zum Beispiel bei der Aufgabe einer Bestellung oder Überweisung einer Rechnung, muß eine rechtsverbindliche Kommunikation sichergestellt werden. Solange man mit einem Medium wie Papier arbeitet, das den Inhalt eines Dokumentes untrennbar mit einer Unterschrift verbindet, ist die Rechtsverbindlichkeit weitestgehend sichergestellt und juristisch anerkannt. Der Unterschreibende erklärt sich mit dem Inhalt des Dokumentes einverstanden. Insbesondere im elektronischen Handel muß ein vergleichbarer Sicherheitsdienst zur Verfügung stehen, der trotz der Entkopplung zwischen digitaler Information und dem Transportmedium (Datenleitung, Satellit, Diskette etc.) aus Sicht

*Verbindliche
Kommunikation in
offenen Netzen*

*Urheber- und
Empfängernachweis*

des Käufers und des Anbieters eine verbindliche Kommunikation gewährleistet. Im Streitfall muß der Händler dem Käufer nachweisen können, daß nur er und kein anderer eine Bestellung in Auftrag gegeben hat. Andererseits darf der Händler bei Lieferschwierigkeiten auch nicht den Erhalt der Bestellung leugnen. Verbindlichkeit muß demnach Möglichkeiten zur Anerkennung der Übermittlung (Empfängernachweis) und zur Anerkennung des Ursprungs (Urhebernachweis) der Information schaffen. Daraus leitet sich die Forderung nach Verfahren ab, die einen zweifelsfreien Zusammenhang zwischen den übertragenen Daten und der Person herstellen, die diese gesendet bzw. empfangen hat.

Wahrung der Anonymität

Im Gegensatz zur Authentifikation schützt Anonymität eine Person davor, ihre Identität z. B. aus Gründen des Datenschutzes preiszugeben. Kommerzielle Dienste im Internet fordern von ihren Benutzern häufig die Angabe persönlicher Daten, die zum Teil weit über die E-Mail-Adresse oder die Lieferanschrift hinausgehen. In Verbindung mit gesammelten Zahlungsinformationen läßt sich damit z. B. leicht ein Bezug zwischen dem Kunden, seinen Interessen und seiner Kaufkraft herstellen. Es liegt in der Hand der Anbieter, wofür sie diese kritischen Informationen auswerten. Lobenswert ist der Trend, daß immer mehr Anbieter eine Datenschutzerklärung (engl. privacy statement) auf ihrer Website abgeben, die den Besucher in der Regel darüber aufklärt, welche Daten wann gesammelt werden und ob damit Auswertungen erfolgen. Fest steht, daß trotz vertrauensbildender Willensbekundigungen über den Schutz der Privatsphäre ein potentieller Mißbrauch nicht ausgeschlossen ist. Bevor es zu einem schwunghaften Handel der Kundenprofile und dem Verlust der informellen Selbstbestimmung des einzelnen kommt, sind Verfahren zu schaffen, die Identität des einzelnen bei der Teilnahme am elektronischen Handel zu schützen. Die gesetzliche Grundlage zur legalen Erhebung von personenbezogenen Daten regeln in Deutschland das Bundesdatenschutzgesetz (BDSG) und das Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz, TDDSG). Letzteres wurde speziell für Online-Dienste geschaffen und ist daher deutlich spezifischer.

Der Schutz personenbezogener Daten muß insbesondere bei der elektronischen Zahlungsabwicklung über das Internet beachtet werden, die bei Bedarf auch anonym durchführbar sein muß. Wie dies trotz des im ersten Moment augenscheinlichen Widerspruchs zur eindeutigen Identifikation und Unbestreitbarkeit von derart sensiblen Transaktionen möglich ist, wird im Zusammenhang mit Kryptographie und digitalem Bargeld (siehe 2.6.6) im zweiten Teil des Buches näher beschrieben.

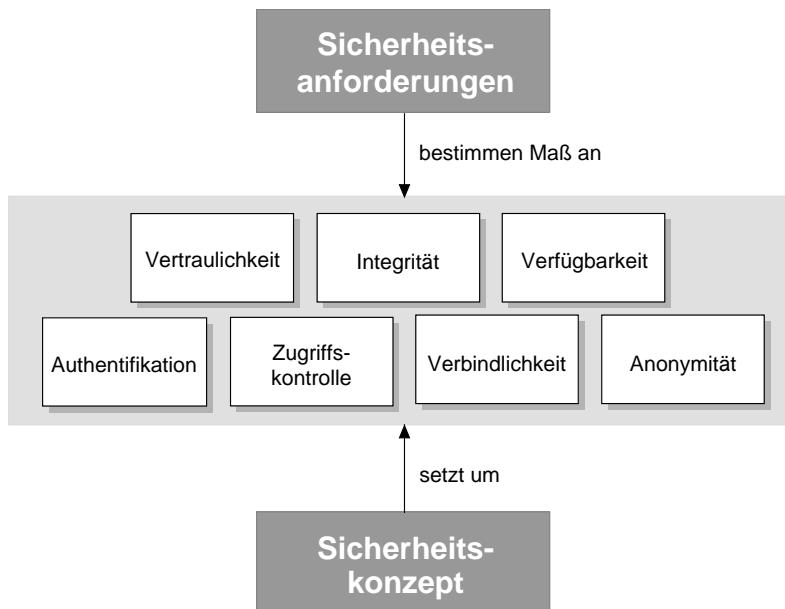


Abb. 1-1
Sicherheitsdienste
in offenen Netzen

Somit lassen sich zu den drei Grundbedrohungen Vertraulichkeit, Integrität und Verfügbarkeit unter Berücksichtigung der Anforderungen in offenen Netzen wie dem Internet vier weitere, ebenfalls fundamentale Sicherheitsdienste identifizieren: Authentifikation, Zugriffskontrolle, Verbindlichkeit und Anonymität. Wie in Abb. 1-1 dargestellt, definieren die Sicherheitsanforderungen das erforderliche Sicherheitsniveau, das durch eine Auswahl geeigneter Mechanismen im Sicherheitskonzept umgesetzt wird. Im dritten Teil des Buches werden einige Fallbeispiele auf ihre Anforderung hinsichtlich dieser sieben Sicherheitsdienste untersucht und entsprechend deren Gewichtung Konzepte vorgeschlagen, die wiederum Gebrauch von den im zweiten Teil beschriebenen Maßnahmen machen. Die Bewertung bezüglich ihrer Schutzwirkung und Einordnung möglicher Anwendungsgebiete erfolgt ebenfalls unter Berücksichtigung der Sicherheitsdienste. Damit ist ein direkter Vergleich der Lösungsansätze untereinander möglich.

1.2.2 Begriffsdefinition und Abgrenzung

Aus unternehmerischer Sicht sollte der Begriff Sicherheit als eine zentrale Eigenschaft von Geschäftsprozessen verstanden werden, die durch geeignete technische und organisatorische Maßnahmen sichergestellt, daß das Restrisiko für die Organisation auf ein tragbares Maß reduziert wird. Eine eher technische Definition, die sich an den bereits

erwähnten Sicherheitsdiensten orientiert, beschreibt Sicherheit (engl. security) als einen Zustand, in dem Informationen vor, während und nach der Verarbeitung vor Beeinträchtigung und Verlust der Vertraulichkeit, Integrität und Verfügbarkeit bewahrt werden. In offenen Netzen wie dem Internet muß darüber hinaus die Authentifikation von Benutzern, die Kontrolle von Zugriffen, die Verbindlichkeit von Kommunikationsbeziehungen und bei Bedarf auch die Anonymität des Ursprungs von Informationen sichergestellt werden.

*Daten- und
Personenschutz*

In Abgrenzung dazu hat der Datenschutz (engl. privacy) die Aufgabe, den einzelnen vor der Beeinträchtigung seines Persönlichkeitsrechts durch den sorglosen Umgang mit personenbezogenen Daten zu schützen. Der Datenschutz muß sicherstellen, daß nur bestimmte Personen im Rahmen der geltenden gesetzlichen Vorschriften (Bundesdatenschutzgesetz) und unter Beachtung einschlägiger Regelungen (z. B. Betriebsvereinbarungen) Daten erheben, verarbeiten oder nutzen dürfen. Sicherheit im Sinne von Brand- oder Personenschutz (engl. safety) ist nicht Gegenstand der weiteren Betrachtungen.

1.2.3 Effizienz und Kosten

Weder im Leben noch in der Technik kann es eine absolute Sicherheit geben. Selbst eine nahezu hundertprozentige Lösung ist mit unbegrenzten Mitteln kaum zu realisieren. Statt dessen muß das ideale Maß an Sicherheit unter Berücksichtigung der finanziellen Rahmenbedingungen angestrebt werden. Aufwand und Nutzen der Sicherheitsvorkehrungen müssen in einem ausgewogenen Verhältnis zueinander stehen. Das verbleibende Restrisiko muß durch den Einsatz entsprechender Gegenmaßnahmen auf ein tragbares oder angemessenes Maß reduziert werden. Was »angemessen« in diesem Zusammenhang bedeutet, hängt stark von der Risikobewertung im Einzelfall ab.

Ausgehend von einem exponentiellen Anstieg der Kosten für die Einführung von Abwehrmaßnahmen bei gleichzeitiger Minimierung der Risiken lassen sich die Gesamtkosten, wie in Abb. 1–2 dargestellt, aus der Summe der beiden Kurven ableiten. Am Tiefpunkt dieser parabelähnlichen Kurve ist demnach das ideale Verhältnis zwischen den Aufwendungen für die Maßnahmen und dem zu erwartenden Schaden durch das verbleibende Restrisiko erreicht. Wo sich eine Organisation oder ein Unternehmen in diesem Schaubild wiederfindet, ist maßgeblich von ihren Sicherheitsanforderungen abhängig. Auf der Parabel sollten alle Unternehmen in der Nähe des Minimums liegen. Banken sind eher auf der rechten Hälfte der Kurve einzuordnen, da für sie die Sicherheit ihrer Systeme von großer Bedeutung ist. Der kleine Shop-Be-

treiber im Internet wird nicht willens sein, hohe Summen für teure Hard- und Software auszugeben.

Als feste Größe geht bei der Kalkulation der Gesamtwert der zu schützenden Güter ein. Die Investitionen für die geplanten Maßnahmen dürfen deren Summe nicht überschreiten. Andernfalls wäre das Sicherheitskonzept unter wirtschaftlichen Gesichtspunkten nicht vertretbar.

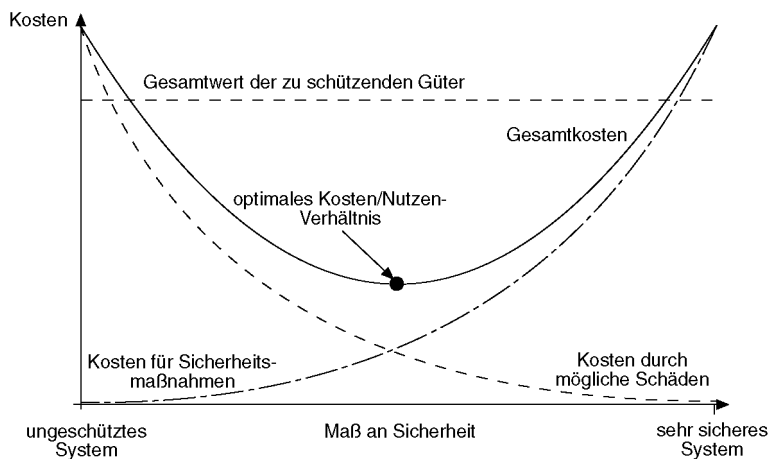


Abb. 1-2
Verhältnis zwischen Kosten
und Nutzen

1.3 Risikoanalyse

Der oftmals verfolgte Ansatz, Sicherheit durch die direkte Umsetzung von Abwehrmaßnahmen zu erreichen, führt dazu, die Auswahl einzelner Komponenten nur auf Basis ihrer Stärken und Schwächen zu treffen. Bei diesem Vorgehen besteht die Gefahr, daß

- Bedrohungen unterschätzt oder übersehen werden,
- Gefahren überbewertet werden und ein aus ökonomischer Sicht nicht akzeptabler Aufwand geleistet wird,
- Symptome und nicht Ursachen bekämpft werden.

Unter dem Begriff Risikoanalyse wird ein Verfahren beschrieben, das diese Fehler durch eine sorgfältige Planung im voraus zu vermeiden hilft. Ziel der Risikoanalyse ist es, mit den zur Verfügung stehenden Mitteln die größtmögliche Schutzwirkung zu erreichen. Damit leistet die Risikoanalyse einen entscheidenden Beitrag zur Erstellung eines Sicherheitskonzeptes, das die notwendigen Maßnahmen zur Verringerung der Risiken unter Berücksichtigung der Wirtschaftlichkeit beschreibt. Grundsätzlich existieren zwei Ansätze zur Risikoanalyse: der Grundschutz und die detaillierte Analyse.

Ziel der Risikoanalyse

1.3.1 Grundschutzansatz

Für Systeme mit geringem Schutzbedarf, wie z. B. einem von der IT-Infrastruktur entkoppelten Informationssystem im Internet, wird zur Erreichung eines angemessenen Sicherheitsniveaus, dem sogenannten Grundschutz (engl. baseline protection), ein schnell durchführbarer Soll-Ist-Abgleich zwischen den bereits vorhandenen und auf Basis anerkannter Industriestandards (engl. best practices) empfohlenen Schutzmaßnahmen vorgenommen. Die Empfehlungen sind für fast alle Bereiche im Unternehmen verfügbar, die von der IT-Sicherheit betroffen sind. In der Regel werden sie jährlich überarbeitet und auf nationaler Ebene in den sogenannten Baseline-Reports veröffentlicht.

*IT-Grundschutzhandbuch
des BSI*

In Deutschland ist das IT-Grundschutzhandbuch [BSI00] vom Bundesamt für Sicherheit in der Informationstechnik (BSI) weit verbreitet. Der Aufbau des Handbuchs gleicht einem Baukasten, mit dessen Hilfe gezielt Elemente der realen Umgebung nachgebildet werden können und je identifiziertem IT-System ein Soll-Ist-Abgleich anhand eines umfangreichen Maßnahmenkatalogs durchgeführt wird. Ergebnis des Verfahrens ist eine Aktionsliste zur Erreichung des vorgegebenen Grundschutzes. Neben IT-spezifischen Bereichen wie PC, LAN und Standard-Software werden auch organisatorische und personelle Maßnahmen wie etwa Mitarbeiterschulung und ein Notfall-Vorsorgekonzept hinterfragt (siehe Abb. 1–3). Mit dem Erscheinen der Ausgabe aus dem Jahr 1996 wurde erstmalig auch der Sicherheitsproblematik im Internet Rechnung getragen. Neben Maßnahmenempfehlungen für die Konfiguration von Firewalls werden Vorschläge zur Absicherung verbreiteter Internet-Protokolle und dem Schutz vor aktiven Inhalten (siehe 1.11.4) gegeben.

Britischer Standard 7799

Der Englische Standard (British Standard 7799, [BS99]), herausgegeben vom der British Standards Institution (<http://www.bsi-global.com>), hat eher den Charakter einer umfangreichen Checkliste. Er konzentriert sich weniger auf technische Grundschutzmaßnahmen, ist aber als Ergänzung zum IT-Grundschutzhandbuch zu empfehlen, da er den organisatorischen Bereich sehr umfassend behandelt. Eine Gegenüberstellung der Hauptthemen beider Grundschutzstandards ist in Abb. 1–3 dargestellt.

BS 7799	IT-Grundschutzhandbuch
<ul style="list-style-type: none"> ■ Sicherheitspolitik ■ Sicherheitsorganisation ■ Güterklassifikation ■ Personal ■ Kommunikations- und Betriebsmanagement ■ Zugriffskontrolle ■ Physikalische Sicherheit ■ Systementwicklung und -pflege ■ Notfallvorsorge 	<ul style="list-style-type: none"> ■ Übergeordnete Komponenten <ul style="list-style-type: none"> – Organisation, Personal etc. ■ Infrastruktur <ul style="list-style-type: none"> – Gebäude, Verkabelung etc. ■ Nicht vernetzte IT-Systeme <ul style="list-style-type: none"> – standalone PCs, Notebooks etc. ■ Vernetzte IT-Systeme <ul style="list-style-type: none"> – UNIX, NT, Novell etc. ■ Datenübertragungseinrichtung <ul style="list-style-type: none"> – Modem, Firewall etc. ■ Telekommunikation <ul style="list-style-type: none"> – TK-Anlage, Fax etc. ■ Sonstige IT-Komponenten <ul style="list-style-type: none"> – Standard-Software

Abb. 1–3
 Inhaltsübersicht
 europäischer
 Grundschutzstandards

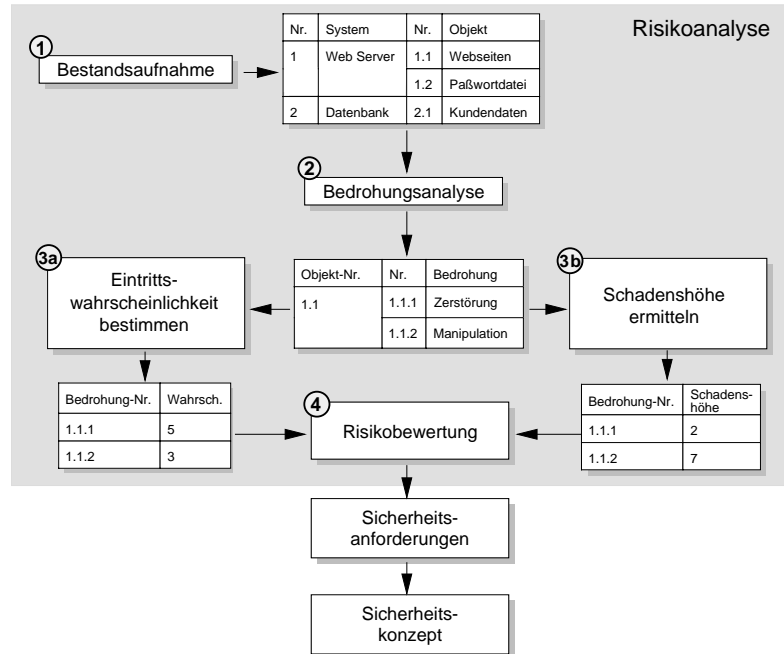
Der Grundschutzansatz geht von einer allgemeingültigen Gefährdungslage aus, die sich an den Grundbedrohungen Vertraulichkeit, Integrität und Verfügbarkeit orientiert. Dieses Vorgehen erspart bei Systemen mit geringen bis mittleren Sicherheitsanforderungen einen Teil des notwendigen Untersuchungsaufwands, der bei einer detaillierten Risikobetrachtung erforderlich ist. Wird ein höheres Maß an Sicherheit verlangt, dann sollte auf eine umfassende Analyse nicht verzichtet werden. Wie hoch der Schutzbedarf letztlich ist, hängt von den zu erwartenden Schäden bei Verletzung der Sicherheit ab. Sind sie im voraus klar absehbar und von geringem Ausmaß, dann ist der Grundschutzansatz vorzuziehen. Diese Entscheidung ist für Internet-Systeme im kommerziellen Einsatz nicht einfach zu treffen. Wie der folgende Abschnitt zeigt, fehlt es häufig noch an zuverlässigen Erfahrungswerten, um eine sichere Aussage zu machen. In der Regel weisen die Systeme aber einen hohen Schutzbedarf auf, der über die drei im Grundschutz adressierten Sicherheitsdienste hinausgeht (siehe 1.2.1).

1.3.2 Detaillierte Risikoanalyse

Die zur Verfügung stehenden Mittel (Geld, Personal, Zeit) effektiv einzusetzen bedeutet in erster Linie, alle Risiken möglichst vollständig zu erfassen und sie nach dem potentiellen Schaden, der bei Eintritt der Gefahr entstehen kann, zu priorisieren. Dazu wurden in der Vergangenheit mehrere Methoden vorgeschlagen, die aber vielfach einem ähnlichen Vorgehen folgen und sich hauptsächlich in der Darstellung der Ergebnisse unterscheiden. Qualitative Verfahren setzen die identifizierten Risiken durch eine verbale Beschreibung in Relation zueinander, quantitative Ansätze liefern eine nach dem Schadensmaß geordnete Liste aller Schwachstellen.

*Quantitative und
 qualitative Verfahren*

Abb. 1–4
Vorgehensweise der
Risikoanalyse



Trotz der gegensätzlichen Ergebnisdarstellung richten sich viele Ansätze zur Risikoanalyse nach der mathematischen Definition des Risikobegriffs:

$$\text{Risiko} = \text{Schadenshöhe (S)} * \text{Eintrittswahrscheinlichkeit (E)}$$

Risikominimierung und
Restrisiko

Demnach ist das Risiko das Produkt aus der Schadenshöhe einer bestimmten Gefährdung und der Wahrscheinlichkeit, mit der diese Bedrohung eintritt. Das Risiko wird zum Maß der Schwachstellenbewertung eines Systems. So ist die Schadenshöhe bei Absturz eines Flugzeuges auf ein Kraftwerk beispielsweise unermesslich hoch, die Wahrscheinlichkeit einer solchen Katastrophe wird allerdings als äußerst gering eingestuft. Entsprechende Sicherheitsvorkehrungen wie bauliche Maßnahmen oder Planung der Flugrouten minimieren das Risiko, können es jedoch nicht komplett ausschließen. Das verbleibende Risiko wird als Restrisiko bezeichnet und im Fall des Flugzeugabsturzes so gering eingestuft, daß der Betrieb des Kraftwerkes (zumindest von der Mehrheit der Bevölkerung) als zumutbar empfunden wird. Man spricht in diesem Zusammenhang auch von tragbaren und untragbaren Risiken.

Um beide Faktoren der Gleichung quantitativ oder qualitativ zu erfassen, sind die im folgenden aufgeführten Schritte, wie in Abb. 1–4 dargestellt, durchzuführen.

Bestandsaufnahme

Die Bestandsaufnahme (1) erfaßt alle schützenswerten Objekte des Analysebereichs. Im Rahmen einer Internet-Anwendung kommen z. B. Web-Server¹ oder Zentralrechner (Host) in Betracht, auf die aus dem öffentlichen Netz zugegriffen wird. Oft attackiert werden auch Mail Server und Verbindungsrechner zum Internet. Für jedes identifizierte System sind im Anschluß die Programme sowie die dort gespeicherten, verarbeiteten und übertragenen Daten zu identifizieren, die vor Angriffen geschützt werden müssen. Dazu zählen u. a.

- Konfigurations- und Paßwortdateien
- Datenbanken
- Kommunikationsdienste
- Logdateien²
- Sicherheitskopien (Backups)
- Überwachungsprogramme

Die Entscheidung, ob und in welchem Maß ein materielles oder immaterielles Gut geschützt werden soll, kann häufig nur in Zusammenarbeit mit dem für die Anwendungen oder das System verantwortlichen Mitarbeiter geklärt werden. Angesichts der Masse an Daten ist eine Trennung zwischen wichtigen und unwichtigen Informationen oftmals nicht einfach. Es hat sich bewährt, Daten zu klassifizieren und nach verschiedenen Prioritätsgruppen zu unterteilen. Für ein Unternehmen überlebenswichtige Informationen werden z. B. als »streng geheim« eingestuft, interne Informationen als »vertraulich«. Der Verlust dieser Daten führt in aller Regel zu einem hohen finanziellen Schaden. Allgemeine bzw. öffentliche Informationen werden nicht weiter klassifiziert. Sie sind nur von geringer oder keiner betrieblichen Bedeutung und lassen sich oftmals mit geringem Aufwand wiederherstellen.

*Klassifikation von
Informationen*

Bedrohungsanalyse

Für jedes der erfaßten Objekte muß im nächsten Schritt (2) dokumentiert werden, welche Bedrohungen bzw. Gefahren einen maßgeblichen Einfluß auf die Geschäftstätigkeit und den laufenden Betrieb des Ge-

-
1. Unter Web-Server wird eine Kombination aus Hard- und Software verstanden, die im Internet Informationen über das Standardprotokoll HTTP (siehe 1.11.2) zum Abruf bereit hält. Darüber hinaus kann der Web-Server eine Schnittstelle zu zusätzlichen Informationssystemen sein.
 2. Logdateien protokollieren lokale Aktionen auf dem jeweiligen System. Sie liefern detaillierte Informationen darüber, wer, wann wo worauf zugegriffen hat bzw. zuzugreifen versuchte.

samtsystems haben. Es wird dabei unterschieden zwischen zufälligen oder unbeabsichtigten Gefahren, wie z. B. höherer Gewalt (Feuer, Wasser, Explosion etc.), menschlichem und technischem Versagen, oder bewußt herbeigeführten Gefahren wie Manipulation, Spionage oder Sabotage. Letztere werden in bezug auf das Internet in Abschnitt 1.12 näher betrachtet.

Im Gespräch mit den Anwendern und Verantwortlichen der identifizierten Systeme muß unter der Fragestellung »Was wäre wenn ...?« der Schutzbedarf aufgrund realistischer Schadensszenarios abgeleitet werden [BSI00]. Dabei gilt es nicht nur finanzielle Schäden zu betrachten, sondern es müssen auch Auswirkungen auf das Ansehen des Unternehmens, Verstöße gegen gesetzliche Auflagen (Datenschutzgesetz) sowie maximal zulässige Ausfallzeiten berücksichtigt werden.

*Bedrohungsanalyse mit
Angriffssimulationen*

Ist bereits ein Prototyp implementiert oder ein Testsystem in Betrieb, dann ist es empfehlenswert, die theoretische Bedrohungsanalyse mit den Ergebnissen einer simulierten Attacke aus dem Internet zu untermauern. Um zu einer möglichst realistischen Einschätzung der Gefahren zu gelangen, lassen sich kommerzielle und frei verfügbare Tools wie beispielsweise SATAN (Security Administrator's Tool for Analyzing Networks) oder der Security Scanner für diesen Zweck einsetzen (siehe 1.13). Viele System- und Beratungshäuser bieten diese Dienstleistung unter dem Begriff Penetrationsanalyse im Rahmen externer Sicherheitsüberprüfungen an. Dabei werden Schwachstellen systematisch aufgedeckt, aber nicht weiter ausgenutzt.

Bestimmung der Eintrittswahrscheinlichkeit

Die Risikobewertung und alle daraus abgeleiteten Entscheidungen sind von der Abschätzung der Eintrittswahrscheinlichkeit (E) und Schadenshöhe (S) abhängig. Aus diesem Grund sollten die beiden folgenden Schritte (3a/b) mit großer Sorgfalt durchgeführt werden.

*Keine zuverlässigen
Zahlen für das Internet
verfügbar*

Die quantitative Risikobewertung definiert für die Eintrittswahrscheinlichkeit ein Maß wie etwa »Erfolgreiche Angriffe vom Typ X pro Jahr«. In diesem Fall spricht man von der sogenannten Jahresverlustquote (engl. Annual Loss Expectancy, ALE). Versicherungen ziehen dafür langjährig geführte Statistiken heran. Für die Berechnung der Prämie bei Abschluß einer Kraftfahrzeugversicherung liefern diese Daten eine nach Modell, Hersteller und Zulassungsort aufgestellte Häufigkeit typischer Gefahren wie Diebstahl oder Aufbruch. Aufgrund seiner noch relativ jungen Historie liegen vergleichbare Informationen für das Internet noch nicht vor. Die wenigen zentralen Registrierungsstellen für sicherheitsrelevante Zwischenfälle im Internet sehen sich in diesem

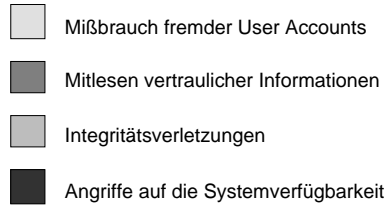
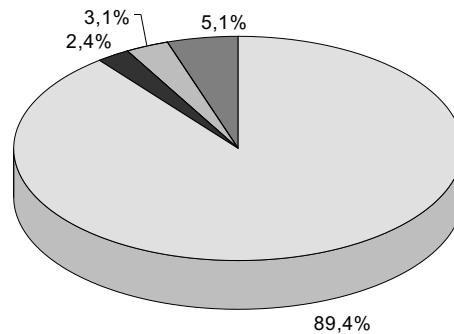


Abb. 1-5
Häufigkeit typischer
Angriffsmethoden im Internet
[HOW97]



Zusammenhang mit der schwierigen Aufgabe konfrontiert, unvorstellbare Mengen von weltweit verteilten Daten zu konsolidieren, um verlässliche Ergebnisse zu bekommen.

Im Gegensatz zu der regional unterschiedlichen Wahrscheinlichkeit von Autodiebstählen haben Gefahren im Internet immer eine globale Bedeutung. Erster und oftmals einziger Anhaltspunkt für derartige Auswertungen sind die Aufzeichnungen in den Protokolldateien exponierter Systeme. Moderne Betriebssysteme können hier jede Unregelmäßigkeit im laufenden Betrieb registrieren wie z. B. komplette oder partielle Systemausfälle sowie unerlaubte Zugriffe und Netzoperationen.

Im Auftrag des Computer Emergency Response Teams (CERT, <http://www.cert.org>) am Software Engineering Institute (SEI) der Carnegie Mellon Universität wurde eine Untersuchung [HOW97] bezüglich der Häufigkeit typischer Angriffsmethoden im Internet abgeschlossen. Das CERT fungiert als zentrale Anlaufstelle und Sprachorgan für neue Sicherheitsvorfälle im Internet, um Systemadministratoren auf dem neuesten Stand zu halten. In den sogenannten CERT-Advisories werden permanent neue Schwachstellen und entsprechende Gegenmaßnahmen publik gemacht. Auf Basis der insgesamt 4.299 Meldungen, die in den Jahren 1989 bis 1995 am CERT eingingen, wurde eine Klassifikation und Auswertung vorgenommen. Das Ergebnis ist in Abb. 1-5 dargestellt.

Die Zahlen lassen sich grob den Grundbedrohungen (siehe 1.2.1) zuordnen, wobei die Häufigkeit der Vortäuschung einer falschen Identität und der anschließende Mißbrauch von Zugriffsrechten aufgrund der engen Verbindung beider Bedrohungen nicht gesondert ausgewiesen wurde. Es läßt sich ablesen, daß dieser Kategorie gegenüber den anderen Bedrohungen ein vergleichsweise hoher Anteil (89,3%) zukommt. Auch das amerikanische Federal Computer Incident Response Capability (FedCIRC) stellt in seiner Jahresstatistik für 1999 [FED99] fest, daß der Mißbrauch der Berechtigung des Systemadministrators (bei UNIX-Systemen der Benutzer `root`) zu den häufigsten Angriffstypen zählt. Begründen läßt sich diese Tatsache damit, daß es einem Angreifer normalerweise leichter fällt, auf einem System direkt einzubrechen, als die Daten während der Übertragung durch das Internet mitzulesen. Mögliche Angriffspunkte stellen hier nur die Verbindungsrechner (engl. `router`) im Internet dar, deren Betriebssysteme allerdings sehr stark spezialisiert sind und wenig Angriffsfläche bieten. Im Gegensatz dazu sind die komplexen Server der Website-Betreiber oftmals voller Schlupflöcher und stellen den Weg des geringsten Widerstands zu den begehrten Informationen dar. Werden starke Verschlüsselungsmechanismen (siehe 2.6) zum Schutz sensibler Daten bei der Übertragung eingesetzt, stößt die zur Verfügung stehende Hardware eines durchschnittlich ausgestatteten Angreifers schnell an ihre Grenzen, um die chiffrierten Daten zu knacken (siehe Tab. 2–4). Aussagen über die Häufigkeit und Schadenshöhe von Vorfällen, bei denen Kommunikationsbeziehungen bzw. ein vollzogener Informationsaustausch von einem der Teilnehmer abgestritten wurde, sind in die Erfassung nicht eingegangen. Dies mag daran liegen, daß zum Zeitpunkt der Untersuchung das Volumen geschäftlicher Transaktionen über das Internet nur einen kleinen Anteil ausmachte.

*Nur die wenigsten
Einbrüche werden
gemeldet*

Grundsätzlich hat man bei der Erhebung statistischer Zahlen über Schadensfälle im Internet immer das Problem, daß viele Unternehmen die Zwischenfälle aus Angst vor einer Verschlechterung ihrer Reputation vertuschen. In einer breit angelegten Studie des FBI in Zusammenarbeit mit dem Computer Security Institute (CSI) wurden Firmen untersucht, die Opfer einer Computerstraftat geworden sind. Gerade einmal 17% meldeten dies auch den Strafverfolgungsbehörden.

Aus Mangel an Informationen und der Zuverlässigkeit solcher Werte schlagen viele Verfahren einen pragmatischeren Ansatz vor. Mit Checklisten und Fragebögen wird versucht, über eine Befragung der Mitarbeiter eine möglichst genaue Einschätzung der Häufigkeit für jede identifizierte Bedrohungen vorzunehmen. Sofern Erfahrungen aus dem laufenden Betrieb im Analysebereich vorliegen, könnten die Be-

fragten eine Einschätzung aufgrund einer Skala von 1 (weniger als einmal in drei Jahren) bis 10 (mehr als einmal pro Tag) [PFL96] abgeben. Andernfalls bietet sich die Ermittlung anhand bestimmter Einflußfaktoren an, die sich z. B. nach

- dem Schwierigkeitsgrad der technischen Durchführbarkeit bei vorsätzlichen Angriffen,
- vorhandenen Sicherheitsmaßnahmen und
- Art und Beschaffenheit der Zielsystems

richten. Tabelle 1-1 ordnet diese Faktoren einer Bewertungsskala für den Eintritt einer Bedrohung mit den Abstufungen »unwahrscheinlich«, »wahrscheinlich« und »hoch« zu.

Bewertung	Bedeutung	Einflußfaktor
1	unwahrscheinlich	<p>Unbeabsichtigte Bedrohungen</p> <ul style="list-style-type: none"> <input type="checkbox"/> Das Produkt ist seit mehreren Jahren auf dem Markt. <input type="checkbox"/> Es sind Schutzvorkehrungen durch vielschichtige Sicherheitsmaßnahmen getroffen. <input type="checkbox"/> Das System läuft sehr stabil, Ausfälle und Fehlfunktionen wurden nicht oder nur selten registriert. <p>Vorsätzliche Angriffe</p> <ul style="list-style-type: none"> <input type="checkbox"/> Die Durchführung des Angriffs erfordert einen sehr hohen Aufwand und steht in keinem Verhältnis zum Ergebnis. <input type="checkbox"/> Der Angriff kann frühzeitig erkannt werden. <input type="checkbox"/> Es ist ein sehr tiefes Verständnis der technischen Zusammenhänge notwendig.
2	wahrscheinlich	<p>Unbeabsichtigte Bedrohungen</p> <ul style="list-style-type: none"> <input type="checkbox"/> Das System ist erst vor kurzem in Betrieb genommen worden. <input type="checkbox"/> Es ist eine unzureichende Systemdokumentation vorhanden. <input type="checkbox"/> Es sind vereinzelt Fehlfunktionen festgestellt worden. <p>Vorsätzliche Angriffe</p> <ul style="list-style-type: none"> <input type="checkbox"/> Der Angriff kann von jedem PC-kundigen Anwender durchgeführt werden. <input type="checkbox"/> Ein grundsätzliches Verständnis über Internet-Technologien ist erforderlich. <input type="checkbox"/> Der Eintritt der Bedrohung würde einen großen Schaden bewirken. <input type="checkbox"/> Es existieren keine nachgelagerten Kontrollen.

Tab. 1-1

Bewertung der Eintrittswahrscheinlichkeit von Bedrohungen

Bewertung	Bedeutung	Einflußfaktor
3	hoch	Unbeabsichtigte Bedrohungen <ul style="list-style-type: none"> <input type="checkbox"/> Die Einsatzumgebung des Systems weist erhebliche Mängel auf. <input type="checkbox"/> Es sind noch keine Erfahrungen im laufenden Betrieb vorhanden. <input type="checkbox"/> Fehlfunktionen wurden in der Vergangenheit häufig festgestellt. Vorsätzliche Angriffe <ul style="list-style-type: none"> <input type="checkbox"/> Der Angriff kann unabhängig von bestimmten Voraussetzungen durchgeführt werden. <input type="checkbox"/> Der Angriff wurde in der Vergangenheit schon mehrfach registriert. <input type="checkbox"/> Der Angriff kann von jedem Benutzer im Internet oder Intranet durchgeführt werden. Es sind keine besonderen technischen Kenntnisse erforderlich.

Im Idealfall kann auf Basis der Befragungsergebnisse eine erste Einschätzung vorgenommen werden, die anschließend mit neutralen Zahlen verglichen und eventuell angepaßt wird, um Effekte wie z. B. Betriebsblindheit auszuschließen.

Ermittlung der Schadenshöhe

Die Schadenshöhe ist ein Maß für die finanziellen und organisatorischen Auswirkungen bei tatsächlichem Eintritt der Bedrohungen. Eine mögliche Maßeinheit für die Schadenshöhe kann der Geldbetrag sein, der aufzubringen ist, um den Zustand vor dem Zwischenfall wieder herzustellen. Dabei sind neben den direkten Schäden auch eventuelle Folgeschäden zu beachten. Eine Verunstaltung der Firmen-Homepage auf dem Web-Server durch einen Hacker erfordert nicht nur Zeit- und Personalaufwand, um die alten Seiten wiederherzustellen. Gravierender sind die mittelfristigen Folgen durch einen aus dem Vorfall resultierenden Imageverlust des Unternehmens, der allerdings schwer abschätzbar und in konkrete Zahlen zu fassen ist. Berichte über spektakuläre Hackereinbrüche stehen in der Fachpresse hoch im Kurs. Kunden können dadurch schnell das Vertrauen in die Seriosität eines Unternehmens verlieren. Umsatzeinbußen könnten die Folge sein, die unter Umständen einen negativen Einfluß auf die Börsenwerte haben.

Ein weiterer Unsicherheitsfaktor bei der Bewertung immaterieller Güter ist die Dynamik dieser Werte. Der Schaden durch Verlust einer Kundendatenbank oder Aufzeichnen von Kreditkartennummern ist zu jedem Zeitpunkt gleich hoch. Manche Informationen verlieren aber an Wert, wenn sie nicht mehr aktuell sind. Aktienkurse sind beispielsweise

immer nur so lange von Interesse, bis die Bekanntgabe aktuellerer Kursinformationen erfolgt.

Um die Ungenauigkeit bei der Nennung absoluter Beträge zu vermeiden, bieten sich wieder neutrale Bewertungsskalen an. So wie bei der Ermittlung der Eintrittswahrscheinlichkeit werden die für die Daten verantwortlichen Personen nach ihrer Einschätzung bezüglich der Auswirkungen bei Eintritt der unterschiedlichen Bedrohungen befragt. Das Verfahren vom BSI [BSI92] schlägt eine Bewertung von »Unbedeutend« bis »Existenzgefährdend« vor (siehe Tab. 1-2). Was letztlich die genaue Bedeutung der einzelnen Werte ist, muß im Einzelfall geklärt werden.

Bewertung	Bedeutung
4	Existenzgefährdend
3	Groß
2	Mittel
1	Gering
0	Unbedeutend

Tab. 1-2
Schadensbewertung nach
[BSI92]

Abhängig davon, wie detailliert die Bedrohungsanalyse durchgeführt wurde, lassen sich die möglichen Auswirkungen auch konkreter beschreiben. In diesem Fall kann mit der in [ISR96] vorgeschlagenen Bewertungsskala eine exaktere Einschätzung gemacht werden. Hier werden spezifische Gefahren des Internet adressiert und zwischen internen und externen Angreifern unterschieden. Außerdem werden Lese- und Schreiboperationen bei unberechtigten Zugriffen verschieden bewertet, und eine Klassifikation der bedrohten Systemressource vorgenommen. Je höher der Wert in der Skala, um so gravierender sind die Auswirkungen auf die Systemsicherheit und die daraus resultierenden Schäden.

Bewertung	Bedeutung
0	Denial-of-Service Attacke (siehe 1.12.1) – es erfolgt kein unberechtigter Systemzugriff.
1	Interner Eindringling kann unberechtigt Lesezugriff auf Programmdateien und Daten erlangen.
2	Interner Eindringling kann unberechtigten Schreibzugriff auf Programmdateien und Daten erlangen.
3	Interner Eindringling kann unberechtigten Schreibzugriff auf Systemdateien erlangen.

Tab. 1-3
Bewertung der
Schadenshöhe von
Internet-Angriffen

Bewertung	Bedeutung
4	Externer Eindringling aus dem lokalen Netzwerk kann Lesezugriff auf Programmdateien und Daten erlangen.
5	Externer Eindringling aus dem lokalen Netzwerk kann Schreibzugriff auf Programmdateien und Daten erlangen.
6	Externer Eindringling aus dem lokalen Netzwerk kann Schreibzugriff auf Systemdateien erlangen.
7	Externer Eindringling aus dem Internet kann Lesezugriff auf Programmdateien und Daten erlangen.
8	Externer Eindringling aus dem Internet kann Schreibzugriff auf Programmdateien und Daten erlangen.
9	Externer Eindringling aus dem Internet kann Schreibzugriff auf Systemdateien erlangen.

Risikobewertung

Abhängig von den Wertepaaren s , der Schadenshöhe, und ϵ , der Eintrittswahrscheinlichkeit, wird eine Liste der einzelnen Risikopotentiale in Hinblick auf den Schaden aus finanzieller Sicht und der Abhängigkeit des Unternehmens von der Funktionsfähigkeit der untersuchten Systeme erstellt (4). Um für jedes Wertepaar festzustellen, ob das damit verbundene Risiko tragbar ist oder nicht, ist neben einer Vergleichsrelation die Definition einer Tragbarkeitschranke erforderlich. Alle Schwachstellen, die ein untragbares Risiko aufweisen, müssen im Sicherheitskonzept durch plattformspezifische Implementierungsvorschläge und organisatorische Sicherheitsmaßnahmen adressiert werden. Den ermittelten Risiken lassen sich leicht Prioritäten zuweisen, die auch bei der Umsetzung der Maßnahmen berücksichtigt werden müssen. Hoch eingestufte Risiken (solche mit großen Wertepaaren) sollten bei der Einplanung der Mittel vorrangig behandelt werden.

Wenngleich dieses kardinale Bewertungskonzept aufgrund der prägnanten Beschreibung der Risiken durch Zahlen zu einer besseren Vergleichbarkeit der Ergebnisse führt, muß der Ansatz aus Gründen der Ungenauigkeit der Faktoren in Frage gestellt werden. Als problematisch anzumerken bleibt, daß es nicht für alle Risiken gleich gut anwendbar ist, da Größen wie »Wahrscheinlichkeit, daß ein Mitarbeiter seine Rechte mißbraucht« oder »Schadensausmaß bei Veröffentlichung falscher Unternehmensdaten« häufig nur subjektiv festgelegt werden können. Als Alternative dazu können die identifizierten Schwachstellen relativ zueinander in Beziehung gesetzt werden, um zwischen tragbaren und untragbaren Risiken zu trennen. Dazu ist allerdings Expertenwissen notwendig, um diese Bewertung intuitiv und schnell durchführen zu können.

Priorisieren der Risiken

Kritische Betrachtung der Risikoanalyse

Mit dem im Jahre 1992 vom BSI herausgegebenen IT-Sicherheitshandbuch [BSI92] wurde ein wichtiger Beitrag geleistet, eine standardisierte Vorgehensweise zur Risikoanalyse im Bereich der Behörden einzuführen. Das Verfahren ist aber genauso gut in privatwirtschaftlichen Unternehmen einsetzbar. Es gleicht in seinen Grundzügen dem hier vorgestellten Verfahren, erfordert aber bei genauer Einhaltung der insgesamt zwölf Einzelschritte einen vergleichsweise hohen Aufwand. Die vereinzelt geäußerten Bedenken, die Analyse sei aufgrund ihrer hohen Kosten nicht praktikabel, wurden mit Herausgabe des IT-Grundschutzhandbuchs (siehe 1.3.1) für Anwendungen mit geringen und mittleren Sicherheitsanforderungen aus dem Weg geräumt.

Beide Verfahren verzichten auf den Einsatz von Software-Tools, beinhalten aber eine Reihe von vorgefertigten Formularen und Checklisten für die Befragung der Mitarbeiter und die Dokumentation der Ergebnisse. Intensiven Gebrauch von Software-Unterstützung machen dagegen Tools wie Risk Check der norwegischen Firma Norman Data Defense Systems (<http://www.norman.no>) oder das von Trident Data Systems (<http://www.tds.com>) entwickelte Verfahren T-RAP (Trident Risk Assessment Process, TRAP). Auf Grundlage einer Datenbank, die u. a. typische Netzwerkkomponenten und Gefahren enthält, modelliert der Benutzer die System- und Netzinfrastruktur am PC. In der anschließenden Analysephase (Erfassung der Objekte, Bedrohungen und Schadensausmaß) wirkt sich der Software-Einsatz positiv auf die Durchführungsgeschwindigkeit aus. Alle notwendigen Daten werden von dem Tool erfaßt und verarbeitet. Als Ergebnis erhält man einen fertigen Maßnahmenkatalog, um die identifizierten Schwachstellen der analysierten IT-Umgebung zu beseitigen.

Einsatz von Software-Tools beschleunigt die Verfahrensdurchführung

Grundsätzlich andere Verfahren kritisieren das beschriebene Ursache-Wirkungs-Prinzip, dem die klassische Risikoanalyse unterliegt. Dieser Ansatz führe nur zu einer begrenzten Sichtweise auf das Problem. IT-Sicherheit muß aus Sicht dieser Verfahren als Fragestellung in einem komplexen Umfeld verstanden werden, das von sehr vielen, teilweise dynamischen Einflußfaktoren abhängt. Probleme dieser Kategorie erfordern einen ganzheitlichen, multidisziplinären Ansatz. Dazu zählt die Methodik des vernetzten Denkens, wie sie in neueren Vorschlägen zur Risikoanalyse [EGG92] zum Tragen kommt.

Alternative Verfahren

1.3.3 Sicherheitsanforderungen ableiten

Aus der Risikoanalyse leiten sich die Sicherheitsanforderungen ab (siehe Abb. 1–4), die durch das Sicherheitskonzept und den darin beschriebenen Maßnahmen abgedeckt werden müssen. Die Anforderungen dürfen

an dieser Stelle nicht auf technischer Ebene formuliert werden, sondern müssen vielmehr die allgemeinen, unternehmensstrategischen Ziele wiedergeben. Auf konkrete Implementierungsvorschläge wird erst im nächsten Schritt eingegangen, um nicht von Beginn an einen technikgetriebenen, sondern geschäftsorientierten Lösungsansatz zu verfolgen.

1.4 Sicherheitskonzept

Vordringlichste Aufgabe des Sicherheitskonzeptes ist es, die in der Risikoanalyse identifizierten Sicherheitslücken durch geeignete Maßnahmen zu schließen und somit den Anforderungen an die Sicherheit des Systems gerecht zu werden. Ist dies an einigen Stellen nicht möglich, dann müssen die Risiken zumindest vermindert werden. Die Herausforderung an das Sicherheitskonzept liegt nicht nur in der optimalen Auswahl angemessener Schutzmechanismen, sondern auch in der Gewährleistung einer beständigen, über die Lebensdauer der Systeme hinausgehenden Sicherheitsstrategie.

*Hauptkomponenten eines
Sicherheitskonzeptes*

Ein umfassendes Sicherheitskonzept (siehe Abb. 1–6) besteht aus den drei folgenden Hauptkomponenten:

- Festlegung der Internet-Sicherheitsrichtlinien (Internet-Sicherheitspolitik)
- Beschreibung technischer Maßnahmen (Sicherheitsarchitektur und Implementierungsvorschrift)
- Beschreibung organisatorischer Maßnahmen (Betriebskonzept)

1.4.1 Internet-Sicherheitspolitik

*Vorgaben für das
Sicherheitsniveau*

Die technischen und organisatorischen Maßnahmen müssen sich unternehmensspezifischen, auf die ermittelten Sicherheitsanforderungen ausgerichteten Sicherheitsvorschriften (engl. Internet Security Policy) richten. Sie sorgen dafür, daß den Schutzeinrichtungen im Sicherheitskonzept ein klar definiertes und konsistentes Maß an Sicherheit vorgegeben wird. Obgleich die Vorschriften den Charakter eines Gesetzestextes haben, so ist auf eine für jedermann im Unternehmen verständliche Formulierung zu achten. Die Internet-Sicherheitspolitik hat sich nach der allgemeinen Geschäftspolitik sowie den übergeordneten IT-Sicherheitsrichtlinien zu richten. Um Risiken durch menschliche Fehlhandlungen zu vermeiden, werden in der Internet Security Policy u. a. Grundsätze für den korrekten Umgang mit den neu eingeführten Kommunikationsdiensten definiert. Sie legt die Anforderungen an den Betrieb fest und formuliert auf technischer Ebene die Anforderungen

an die Systeme und deren IT-Sicherheitsmerkmale. Abschnitt 2.1 geht auf konkrete Inhalte einer Internet-Sicherheitspolitik ein, und Anhang A führt Beispiele für solche Richtlinien auf.

1.4.2 Auswahl geeigneter Sicherheitsmaßnahmen

Eine klar definierte Internet-Sicherheitspolitik ist die beste Basis für die Auswahl und Definition technischer und organisatorischer Maßnahmen im Rahmen des Sicherheitskonzeptes. Grundsätzlich stehen folgende Maßnahmen zur Auswahl:

- präventive Maßnahmen, die Gefahren bereits im Vorfeld zu vermeiden helfen,
- überwachende Maßnahmen, die Angriffe bei ihrem Eintritt erkennen und abzuwehren versuchen, sowie
- reaktive Maßnahmen, die nach Eintritt der Bedrohung die Schadensfolgen minimieren.

*Klassifikation von
Sicherheitsmaßnahmen*

Liegen mehrere Alternativen zur Minimierung eines Risikos vor, so ist die Entscheidung für oder gegen den Einsatz einer bestimmten Sicherheitsmaßnahme von mehreren Faktoren abhängig:

- Schutzwirkung der Maßnahme
- Kosten für die Beschaffung, Einführung und den Betrieb
- Höhe des verbleibenden Restrisikos
- Zusammenwirken mit anderen Maßnahmen
- Benutzerfreundlichkeit

Die Schutzwirkung muß immer im Verhältnis zum Wert des Objektes stehen, da mit dem Einsatz stärkerer Abwehrmechanismen gewöhnlich auch die Kosten steigen (siehe Abb. 1–2). Ist mit der Einführung der Maßnahme das verbleibende Restrisiko immer noch zu hoch, dann muß über andere oder ergänzende Alternativen beraten werden. Dabei sind die bereits vorgesehenen Sicherheitsvorkehrungen in die Planung mit einzubeziehen, da sie selbst wieder schützenswerte Objekte darstellen.

Die geplanten Maßnahmen sollten die Arbeit mit dem System weitestgehend unbeeinträchtigt lassen. Das beste Sicherheitskonzept wird von niemandem bemerkt – Angreifer natürlich ausgenommen. Sicherheit ist immer ein Kompromiß zwischen Funktionalität und Verbot. Überzogene Sicherheitsvorkehrungen lähmen das Potential des Unternehmens und wirken sich auf die Produktivität vermindern aus. Bereits eine zusätzliche An- und Abmeldeprozedur kann schon auf Ablehnung bei den Anwendern stoßen. Sie werden nach Wegen suchen, die neuen Störfaktoren zu umgehen, wie z. B. durch die Auswahl schwa-

cher, leicht merkbarer Paßwörter. Oder es werden Listen angelegt, die unsachgemäß aufbewahrt werden und somit die aufwendigsten Abwehrmaßnahmen außer Gefecht setzen. Mitarbeiter können aufgrund ihres Insiderwissens die schlimmste Gefahr für die IT-Sicherheit im Unternehmen darstellen, wie eine 1996 veröffentlichte Studie des CSI belegte: Von 563 befragten Organisationen gaben 80% frustrierte und verärgerte Mitarbeiter als Grund für sicherheitsrelevante Zwischenfälle an, 70% nannten Hacker als mögliche Ursache und 50% vermuteten Mitbewerber hinter den Angriffen, die bei 47% der Unternehmen über deren Verbindung zum Internet erfolgten.

*Auswahl technischer
Maßnahmen*

Bei der Auswahl technischer Maßnahmen ist nicht nur Wissen und Erfahrung über deren Zusammenwirken notwendig, sondern auch eine gute Kenntnis über die aktuellen Industriestandards und der am Markt erhältlichen Produkte. Stärken und Schwächen der unterschiedlichen Lösungen müssen bekannt sein, um ein ausgewogenes Sicherheitskonzept zu erstellen. Im zweiten Teil wird detailliert auf diese Fragestellungen eingegangen.

Das technische Sicherheitskonzept wird maßgeblich durch zwei Dokumente manifestiert: die Sicherheitsarchitektur und die Implementierungsvorschrift. Die Sicherheitsarchitektur definiert die technische Plattform mit einer fest umrissenen Struktur für die existierende oder geplante Systemumgebung. Sie dokumentiert

Sicherheitsarchitektur

- Aufgabe und Funktion des Systems aus Anwendersicht
- logische Komponenten des Systems
- Anforderungen an die Sicherheit des Systems
- Funktionsweise aller zulässigen Dienste und Datenflüsse zwischen den Diensten
- konkrete technische Sicherheitsmaßnahmen (siehe 2.3) und deren Beitrag zur Minimierung der identifizierten Risiken (z.B. Firewalls, Protokollierung, Datensicherung, Virenprüfung etc.)
- Testvorgaben zur Überprüfung der sicheren Funktionsweise aller Komponenten, z. B. Off- und Online-Tests, Integrationstests, Einsatz von Angriffssimulatoren (siehe 1.13)

Innerhalb der Sicherheitsarchitektur werden die Festlegungen so weit verfeinert, daß die Infrastruktur der Systemumgebung vollständig beschrieben ist. Zur Infrastruktur gehören alle Hardware- und Software-Komponenten sowie die Middleware zur Kommunikation.

*Implementierungs-
vorschrift*

Auf der Grundlage der Sicherheitsarchitektur hat die Implementierungsvorschrift die Aufgabe, die Installation und Konfiguration der zuvor festgelegten Systemumgebung zu beschreiben. Sie enthält die Details aller durchzuführender technischen Implementierungsmaßnah-

men, so daß sie als nachvollziehbare Instruktionsanleitung dient. Das Dokument richtet sich vorrangig an Mitarbeiter aus den Bereichen System- und Sicherheitsadministration, Qualitätssicherung und Revision und beinhaltet

- eine topologische Darstellung der Systemumgebung, die alle physikalischen Komponenten und Verbindungen zwischen den Systemen darstellt
- detaillierte Konfigurationseinstellungen zu jeder Komponente für das Betriebssystem und maschinenspezifische Dienste (z. B. für Web- oder Mail-Server)
- einen IP-Konfigurationsplan mit allen IP-Adressen sowie den dazugehörigen Host- und Domain-Namen (siehe 1.6.2)
- einen Testplan zur Überprüfung der korrekten Funktionsweise aller zugelassenen Dienste und Sicherheitsmaßnahmen

Die Administration der mit der Sicherheitsarchitektur eingeführten technischen Schutzeinrichtungen erfordert personelle Zuständigkeiten mit definierten Tätigkeitsprofilen und dokumentierten Prozeßabläufen. Bezugnehmend auf die erwähnten Maßnahmenkategorien beschreibt das Betriebskonzept primär Verfahrensanweisungen für überwachende und reaktive Schritte. Es dokumentiert das Verhalten bei sicherheitsrelevanten Vorfällen, wie z. B. einem Virenbefall oder einem Einbruch aus dem Internet. Weiterhin wird hier festgelegt, welche Aktionen eingeleitet werden, wenn vertrauliche Informationen wie z. B. Paßwörter oder Kundendaten in die falschen Hände geraten. In Abschnitt 2.2 wird detailliert auf die Prozesse eingegangen, die dem sicheren Betrieb einer Internet-Umgebung eingeführt werden müssen.

Neben technischen und organisatorischen Strategien zur Risikominimierung werden oftmals auch versicherungstechnische Mittel zur Abwälzung der Schadensregulierung auf Dritte eingesetzt. Allerdings wurde der Markt für Internet-Policen erst von wenigen Gesellschaften angegangen. Zu ungewiß ist vielen Versicherern noch die weitgehend ungeklärte und allenfalls auf nationaler Ebene diskutierte Rechtslage bei der Nutzung des Internet. Die nordamerikanischen Unternehmen Chubb & Son, Reliance National, die dänische Codan Insurance Group und die in London ansässige Lloyds-Versicherung haben Pionierarbeit auf diesem Gebiet geleistet. In Zusammenarbeit mit großen IT-Unternehmen wurden schon 1997 erste Produkte für den Geschäfts- und Privatkundenbereich entwickelt. Chubb bietet beispielsweise eine sogenannte Multimediaversicherung für Software-Unternehmen an, die ihre Produkte über das Internet vertreiben. Sie sichert gegen Diebstahl des Programmcodes und Verletzung des Urheberrechts ab. Insure-

*Organisatorische
Maßnahmen und Inhalt
des Betriebskonzeptes*

*Versicherungstechnische
Mittel zur
Risikominimierung*

site, so der Name eines Versicherungsproduktes der American International Group Inc., versichert Firmen mit einem Internet-Vertriebskanal gegen elektronischen Betrug und Hardware-Schäden. Außerdem wird die Haftung für Schäden übernommen, die aufgrund diffamierender Aussagen im Internet entstanden sind, wie z. B. Rufschädigung der Konkurrenz durch einen Angestellten [WWO98]. Auch in Deutschland bieten Versicherer wie die Gothaer oder die der Allianz-Gruppe zugehörige Hermes Kreditversicherungs-AG (<http://www.hermes-kredit.com>) Produkte an, die Folgeschäden von unliebsamen Homepage-Manipulationen und den Mißbrauch von Daten abdecken. Bedingung für den Vertragsabschluß ist in der Regel ein spezielles Zertifikat, das ähnlich der TÜV-Plakette ein intaktes System mit hohem Sicherheitsstandard attestiert. Regelmäßige Überprüfungen sind selbstverständlich Pflicht.

1.4.3 Umsetzung des Sicherheitskonzeptes

Im Anschluß an die Konzeption der Maßnahmen gilt es, die praktische Integration des Sicherheitskonzeptes sicherzustellen. Neben einem Projektplan zur Steuerung der Implementierung der technischen Schutzvorrichtungen müssen insbesondere die organisatorischen Abläufe rechtzeitig eingeführt werden. Dazu bietet es sich an, Workshops mit den involvierten Mitarbeitern durchzuführen, in denen das Sicherheitskonzept vorgestellt und offene Fragen diskutiert werden. In die Zeitplanung bis zur Übernahme der Systemumgebung in den Produktionsbetrieb sind auch Schulungsmaßnahmen für das Personal einzubeziehen, das später die neue Technik administrieren soll. Abhängig vom Status der Implementierung der Systemumgebung sollten Notfalltrainings an konkreten Fallbeispielen (z. B. Hackerangriff oder Ausfall eines Servers) mit Schwerpunkten in den Bereichen Alarmierung, Analyse und Wiederherstellung durchgeführt werden. Weiterhin müssen die für den Betriebsbeginn erforderlichen Arbeitsmittel zur Verfügung gestellt werden. Dazu gehören z. B.

- Benutzeranträge
- Eskalationspläne für Notfälle
- Dienstpläne mit Regelungen zur Rufbereitschaft
- Verzeichnis mit allen Ansprechpartnern

1.5 Sicherheitsprozeß

IT-Sicherheit ist keine einmalige Aktion. Mit der Auswahl und Installation von Maßnahmen müssen begleitende Prozesse angestoßen wer-

den, die eine regelmäßige Überprüfung der im Sicherheitskonzept verankerten Maßnahmen sicherstellen.

Auf eine regelmäßige Anpassung der Schutzvorkehrungen kann insbesondere in einem so dynamischen Umfeld wie dem Internet nicht verzichtet werden, in dem Entwicklungszyklen noch kürzer sind als in anderen Bereichen der Informationstechnologie. Dadurch findet geradezu ein Wettlauf zwischen neuen Angriffsmethoden und den von der Industrie entwickelten Gegenmaßnahmen statt, der sich immer weiter zuspitzt. Änderungen in der Schutzbedürftigkeit können aber auch aus neuen Betätigungsfeldern im Internet resultieren, die meist mit der Einführung zusätzlicher Anwendungen und Kommunikationsdienste verbunden sind.

Die Einbettung der in Abb. 1–6 dargestellten Verfahrensschritte in einen zyklischen Prozeßablauf ist also notwendig, um nicht nur eine effektive und sichere, sondern auch dauerhafte Lösung zu gewährleisten.

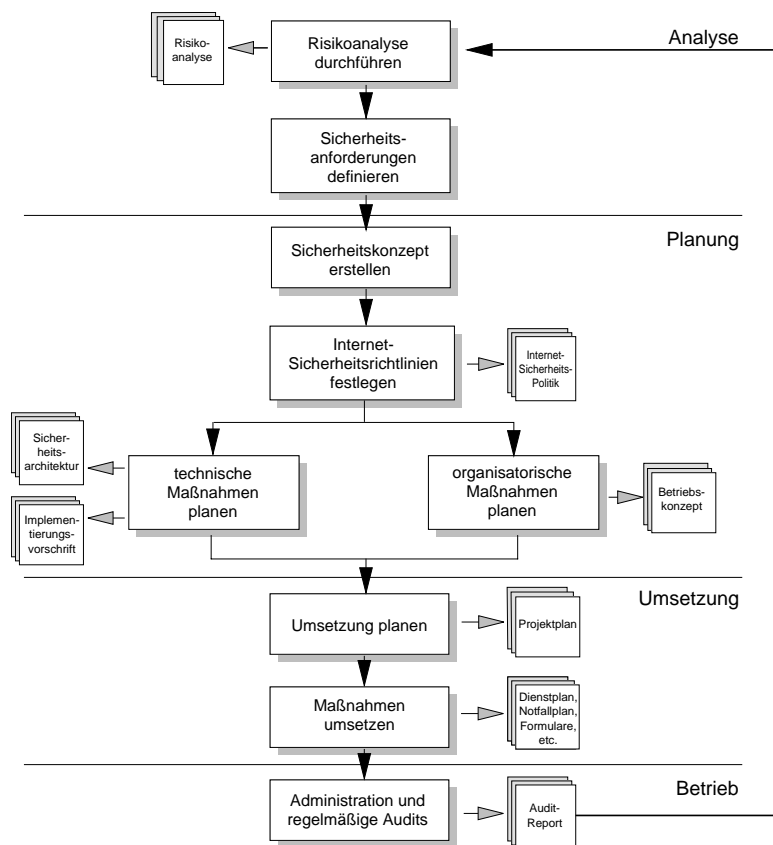


Abb. 1-6
Sicherheitsprozeß

*Kontinuierliche
Verbesserung der
Verfahren durch
regelmäßige Audits*

Den Prozeßschritten Analyse (siehe 1.3), Planung und Umsetzung (siehe 1.4) folgt der laufende Betrieb der Systeme. Um den erreichten Sicherheitsstand aufrechtzuerhalten, müssen regelmäßige Sicherheitskontrollen (engl. audits) dafür sorgen, daß die Effektivität der Schutzeinrichtungen und die Einhaltung der Vorschriften durch die Benutzer immer wieder überprüft werden. Treten bei der »elektronischen Spurensuche« Verstöße gegen die IT-Sicherheit auf, muß sofort auf die Schwachstellen reagiert und eine entsprechende Aktualisierung des Sicherheitskonzeptes veranlaßt werden.

*Kennzahlen zur
Prozeßsteuerung*

Meßkriterien für die Leistungsfähigkeit der Schutzvorkehrungen sind z. B. das Verhältnis zwischen versuchten und erfolgreichen Einbrüchen aus dem Internet oder die Anzahl von Audits ohne Mängelbericht. Ebenso sollte eine Virenstatistik geführt werden, um die Prozeßleistung zu kontrollieren. Der Anstoß für eine Änderung des aktuellen Sicherheitskonzeptes muß über die Führungsebene im Unternehmen erfolgen, die auf Grundlage der Untersuchungsergebnisse im Rahmen der Audits die neuen Maßnahmen bewilligen muß. Steigen etwa aufgrund einer Erweiterung des Internet-Angebots die Anforderungen an die Sicherheit, dann müssen neue Abwehrmaßnahmen evaluiert und mit den bereits vorhandenen abgestimmt werden. Damit ist eine Analyse der neuen Risiken verbunden, aus denen sich wiederum Anforderungen ableiten, die zu neuen Maßnahmen führen. Zusätzlich sollte das System regelmäßig durch den Gebrauch von externen Angriffssimulatoren und Auditwerkzeugen (siehe 1.13) auf neue Schwachstellen untersucht werden, um im Ernstfall besser vorbereitet zu sein.

1.6 Das Internet

Netzwerke gehören heute zu den wichtigsten Bereichen in der Informationstechnologie. Sie sind das Rückgrat der Datenkommunikation für Unternehmen, Finanzinstitute, Universitäten und Regierungen. Besonders im kommerziellen Umfeld wird zur Zeit in kommunikationsfähige Systeme und Dienstleistungen investiert, um für die stark steigende Anzahl privater Nutzer erreichbar zu sein, die Anschluß an weltweite Computernetze wie das Internet haben. Viele dieser WANs (engl. Wide Area Networks) wie z. B. das ARPANet (Advanced Research Projects Agency Network) wurden bereits Anfang der 70er Jahren installiert. Sie zählen zu den Ursprüngen des Internet. Bis heute verbinden immer schnellere Weitverkehrsnetzwerke eine ständig wachsende Anzahl lokaler Netze (engl. Local Area Network, LAN), durch die immer mehr Computer miteinander verbunden werden.