



■ Sicherheit für Systeme und Netze in Unternehmen

2. überarbeitete Auflage

Einführung in die IT-Sicherheit und Leitfaden
für erste Maßnahmen



■ Sicherheit für Systeme und Netze in Unternehmen

2. überarbeitete Auflage

Einführung in die IT-Sicherheit und Leitfaden
für erste Maßnahmen

■ Impressum

Herausgeber:

BITKOM

**Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.**

Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 – 0

Fax: 030/27 576 – 400

bitkom@bitkom.org

www.bitkom.org

Redaktion:

Hans-J. Bierschenk, BITKOM e. V., h.j.bierschenk@bitkom.org

Iris Köpke, BITKOM e.V., iris.koepke@bitkom.org

Stephan Lechner, Siemens AG, stephan.lechner@mchp.siemens.de

Rudolf Neurath, IABG mbH, neurath@iabg.de

Thomas Obert, SAP AG, thomas.obert@sap.com

Michael Otter, BGS AG, michael.otter@bgs-ag.de

Wolfgang Schäfer, Datev eG, wolfgang.schaefer@datev.de

Sandra Schulz, BITKOM e. V., s.schulz@bitkom.org

Arbeitskreis „Sicherheit für Unternehmensnetze“ im BITKOM

Vorsitzende:

Peter Kraaibeek, secunet Security Networks AG, Peter.Kraaibeek@secunet.com

Wolfgang Schäfer, Datev eG, wolfgang.schaefer@datev.de

Layout:

Proforma

■ Inhaltsverzeichnis

■	Inhaltsverzeichnis	3
■	Grußwort des Bundeswirtschafts- und Arbeitsministers Wolfgang Clement	6
■	Vorwort des BITKOM-Präsidenten Willi Berchtold	7
■	1 Sicherheit im Unternehmen	8
	1.1 Chancen und Risiken neuer Technologien	8
	1.2 Rechtliche Aspekte der IT-Sicherheit	9
	1.2.1 Haftung und Schadenersatz	9
	1.2.2 Datenschutz und Fernmeldegeheimnis	10
	1.2.3 Telekommunikationsüberwachung und Verschlüsselung	10
	1.2.4 Urheberrecht	10
	1.2.5 Gefährdende Webinhalte und Privatnutzung betrieblicher Rechner	10
	1.3 Konkrete Bedrohungen für Unternehmen	11
	1.4 Was wird von Systemen und Netzen erwartet?	12
	1.5 Sicherheitskonzept	14
	1.5.1 Inventarisierung der Unternehmenswerte	14
	1.5.2 Klassifikation nach Schutzbedarf	15
	1.5.3 Bedrohungs- und Schwachstellenanalyse	16
	1.5.4 Risikoanalyse	17
	1.5.5 Priorisierung der Schutzziele und Empfehlung von angepassten Schutzmaßnahmen	18
	1.5.6 Festlegung der Risikopolitik und Auswahl der einzusetzenden Schutzmaßnahmen	18
■	2 Bedrohung und Schutz	20
	2.1 Arbeitsplatzrechner	20
	2.1.1 Manipulation von Anwendungssoftware	20
	2.1.2 Virenbefall von Rechnern	20
	2.1.3 Präventive Maßnahmen gegen Viren	22
	2.1.4 Schwachstellen und „Features“ in Hard- und Software	23
	2.1.5 Defekte in der Hardware	23
	2.1.6 Diebstahl von Komponenten	23
	2.1.7 Fehlende Benutzertrennung	24
	2.1.8 Ausspähung von Zugangscodes/Passwörtern	24
	2.2 Server	25

2.2.1	Verhinderung von Diensten	26
2.2.2	Manipulation gespeicherter Daten	26
2.2.3	Inkonsistenz gespeicherter Daten	26
2.2.4	Informationsverlust bei erschöpftem Speichermedium	26
2.2.5	Maßnahmen zur Sicherung der Internetverbindung	27
2.3	Netzwerke und Telekommunikation	27
2.3.1	Abhören der Kommunikation	28
2.3.2	Maskerade	28
2.3.3	Wiedereinspielen alter Nachrichten	29
2.3.4	Veränderung von Nachrichten	29
2.3.5	Übertragungsfehler	29
2.3.6	Nichtanerkennung von Nachrichten	29
2.3.7	Fehlerhafte und falsche Weiterleitung von Nachrichten	30
2.3.8	Physikalische Bedrohungen der Kommunikationsbeziehungen	30
2.3.9	Systematische Planung von Kommunikationsverbindungen	30
■ 3	Sicherheitsmanagement und Organisation	32
3.1	Zugang zu Informationen und Systemen	33
3.2	Trennung von Funktionen	33
3.3	Zentrale IT-Abteilung	34
3.4	Computer Notfall Team (CERT)	34
3.5	Anforderungen an den Mitarbeiter	35
3.5.1	Verpflichtungserklärungen	36
■ 4	Sicherheitstechnologien	38
4.1	Verschlüsselungsverfahren	38
4.1.1	Symmetrische Verschlüsselungsverfahren	38
4.1.2	Asymmetrische Verschlüsselungsverfahren	39
4.1.3	Indirekte Verschlüsselungsverfahren	40
4.2	Digitale Signaturen	41
4.3	Router und Paketfilter	42
4.4	Firewalls	43
4.5	Proxy-Server	44
4.6	Intrusion Detection Systeme	44
4.7	Chipkarten	46

4.8	Biometrische Verfahren	47	
■	5	Kontrollverfahren	50
5.1	Kontrollen im täglichen Betrieb	50	
5.2	Penetrationstests	51	
5.3	Audits	52	
5.4	Passwortanalysen	52	
■	6	Standards und geprüfte IT-Sicherheit	53
6.1	Common Criteria (CC)7	53	
6.2	Das IT-Grundschutzhandbuch	54	
6.3	BS 7799 und ISO/IEC 17799	55	
6.4	Anwendung des BS 7799 oder des IT-Grundschutzhandbuchs	56	
■	7	Glossar	58
■	8	Literaturhinweise	61

■ Grußwort des Bundeswirtschafts- und Arbeitsministers Wolfgang Clement

Der schnelle Austausch digital gespeicherter Informationen in großen Netzwerken über eine wachsende Zahl von Übertragungswegen, das sind die zentralen Merkmale unserer Informationsgesellschaft, die im neuen Jahrtausend mit Wireless LAN, UMTS und anderen Breitbandkanälen auch zunehmend mobiler wird.

Die Frage der Sicherheit von Informations- und Kommunikationsbeziehungen entwickelt sich daher immer mehr zu einer Schlüsselkategorie für die Entwicklung zu neuen Ebenen des Daten- und Wissensaustauschs. Vor allem der wirtschaftliche Erfolg von Unternehmen hängt davon ab, inwieweit es gelingt, die internen Datenbestände oder die externe Kommunikation gegen Datenverlust oder Datenmissbrauch zu schützen. Umgekehrt können sich echte oder vermeintliche Sicherheitsprobleme zu einer zentralen Barriere für die wirtschaftliche Nutzung des Internet entwickeln.

Das Thema „Informationssicherheit“ hat für das Bundesministerium für Wirtschaft und Arbeit hohe politische Priorität, denn wir sind darauf angewiesen, dass Deutschland im „Electronic Business“ ganz vorne in der Weltliga mitspielt.

Dabei wollen wir insbesondere die mittelständischen Nutzergruppen mit mehr Sicherheit ins Netz bringen. Gerade unser Mittelstand, der oft keine eigenen IT-Experten beschäftigen kann, braucht Anleitung und Unterstützung in diesem so wichtigen Bereich. Das Bundesministerium für Wirtschaft und Arbeit richtet deswegen zurzeit zusammen mit dem Bundesministerium des Innern und dem Branchenverband BITKOM ein Frühwarnsystem für Gefahren aus dem Internet, speziell für mittelständische Bedürfnisse, ein. Zudem werden wir in Kürze eine breit angelegte Sensibilisierungskampagne „Sicherheit im Internet – gerade für den Mittelstand“ durchführen.

Der BITKOM als führender ITK-Branchenverband ist uns hier ein wichtiger Partner. Die vorliegende aktualisierte Auflage der Broschüre, die der BITKOM mit seinen Mitgliedsunternehmen erstellt hat, wird vielen Unternehmen, aber auch Privatpersonen helfen, ihr IT-Sicherheitsniveau zu erhöhen. Das bedeutet einen weiteren Schritt in Richtung einer sichereren und erfolgreichen Informationsgesellschaft.

Ihr
Wolfgang Clement

■ Vorwort des BITKOM-Präsidenten Willi Berchtold

Ich freue mich, Ihnen die zweite überarbeitete Auflage der Broschüre „Sicherheit für Systeme und Netze in Unternehmen“ vorstellen zu können. Die erste Ausgabe, die vor zwei Jahren erstellt wurde, hat einen sehr guten Anklang bei unseren Mitgliedern und deren Kunden gefunden.

Die Entwicklung der Informationstechnologien ist in den letzten zwei Jahren auch im Bereich der IT-Sicherheit unaufhaltsam fortgeschritten. Der Trend geht immer mehr zur Verwirklichung einer unternehmensweiten IT-Sicherheitsstrategie anstelle der Realisierung von einzelnen isolierten technischen Sicherheitslösungen. IT und ihre Sicherheit muss als ein Mittel verstanden werden, um die Unternehmensprozesse effizient, sicher und authentisch zu organisieren. Deshalb ist IT-Sicherheit ein wichtiges Instrument jeder Unternehmensführung, um ihrer Verantwortung gegenüber dem Unternehmen, den Mitarbeitern, Kunden und Shareholdern gerecht zu werden.

Diese Entwicklung spiegelt sich auch im Inhalt dieser Auflage wieder. Es wurden nicht nur alle Informationen der ersten Auflage aktualisiert. Wir haben auch die Bereiche „Rechtliche Aspekte der IT-Sicherheit“ und „Kontrollverfahren“ neu aufgenommen. Neue gesetzliche Regelungen, wie beispielsweise „Basel II“, aber auch mittlerweile eingetretene Ereignisse – wie der „Enron-Fall“ – haben bewiesen, dass die Maßnahmen zur IT-Sicherheit nicht mehr nur als technische Angelegenheit von IT-Administratoren betrachtet werden dürfen. Es hat sich gezeigt, dass Unternehmensführungen auch aufgrund von Haftungsfragen gefordert sind, entsprechende ITK-Kontrollsysteme für den ordnungsgemäßen Betrieb ihrer gesamten EDV in ihrem Unternehmen einzuführen. Dazu zählen bekannte IT-Sicherheitsmaßnahmen, wie die regelmäßige, automatische Aktualisierung des Virenschutzprogramms. Dazu zählen aber auch weniger bekannte Maßnahmen, wie beispielsweise die Funktionstrennung bei der Verarbeitung von buchhalterischen Daten, damit diese nicht unbemerkt manipuliert werden können.

Diese Broschüre soll grundlegende Fragen zur Unternehmenssicherheit beantworten und den Einstieg in einzelne IT-Sicherheitsmaßnahmen, wie z.B. Risikoanalyse oder CERT, ermöglichen. Sofern machbar, haben die Autoren auf weiterführende Information durch Links oder in den Literaturhinweisen verwiesen.

Den Autoren danke ich an dieser Stelle nochmals für ihre wertvolle Arbeit und Ihnen wünsche ich eine interessante Lektüre. Ich hoffe, dass wir Ihnen einen hilfreichen Beitrag zur Bewältigung Ihrer Herausforderungen im Bereich der IT-Sicherheit leisten können.

Ihr
Willi Berchtold

■ 1 Sicherheit im Unternehmen

Sicherheit im Unternehmen ist keine isolierte Komponente, sondern hat eine unternehmensumspannende Reichweite. Jeder Mitarbeiter und jedes eingesetzte informationsverarbeitende System im Unternehmen muss Teil einer ganzheitlichen Betrachtung sein. Die Sicherheitsaspekte gehen sogar über das eigene Unternehmen hinaus, wenn etwa global verteilte Zusammenarbeit, Outsourcing oder Application Service Provider mit betrachtet werden. Leider sehen das viele Unternehmen noch anders. Die Umfrage bei Unternehmen der ITK-Industrie in der Zeitschrift KES Nr. 3/2002 spricht eine klare Sprache: Der Stellenwert der Sicherheit der informationstechnischen Systeme (IT-Sicherheit) wird durch das Top-Management der beteiligten Unternehmen

- bei 50 Prozent als gleichrangiges Ziel der Informationsverarbeitung
- bei 29 Prozent als lästiges Übel
- und nur bei 20 Prozent als ein vorrangiges Ziel

eingestuft. Da kann es nicht wundern, dass rund einem Drittel der deutschen Unternehmen, die zwischen 100 und 500 Mitarbeiter beschäftigen, ihre Informationssicherheit (Gehälter, Hardware, Software und andere Ausgaben) im Jahresbudget 2002 nicht einmal 10.000 Euro wert war¹.

Zu ändern ist dies, wenn Geschäftführungen und Vorstände die Aufgabe „Informationssicherheit“ annehmen. Die Verantwortung für die ausreichende Sicherheit des Unternehmens kann nicht delegiert werden, sie verbleibt in den Händen der Unternehmensleitung. Sie muss den Auftrag erteilen, ein individuelles Sicherheitskonzept zu erstellen und gewährleisten, dass das Konzept mit der notwendigen Expertise durchgeführt, eingehalten und fortgeschrieben wird. Die vorliegende Broschüre soll dazu beitragen, für das Thema zu sensibilisieren, anhand konkreter Gefährdungen Bewusstsein zu wecken und zu motivieren, um die informationstechnischen Systeme in den Unternehmen angemessen zu analysieren und zu schützen.

■ 1.1 Chancen und Risiken neuer Technologien

IT-Technologie ist heute unser ständiger Begleiter. Handy und Computer sind im Beruf Alltagsgegenstände und auch privat wird häufig über E-Mail kommuniziert. In der modernen Arbeitswelt sind Unternehmen und Beschäftigte inzwischen Mitglieder von mitunter globalen Supply- und Value-Chains, deren Existenz und hohe Dynamik ausschließlich der leistungsfähigen Informations- und Kommunikationstechnik zu verdanken ist. Die zunehmende Vernetzung durch das Internet, die Dezentralisierung und Virtualisierung von Unternehmen und die damit verbundenen Möglichkeiten des elektronischen Wirtschaftens sind mittlerweile aus dem beruflichen Alltag nicht mehr wegzudenken.

Dabei dürfen aber nicht die wachsenden Risiken vergessen werden, die durch neue Technologien entstehen oder durch diese verstärkt werden. Wenn es zu massiven Bedrohungen kommt, ist die Bestürzung und Ratlosigkeit bei Internetnutzern meistens groß. Leider ist aber die nachhaltige Wirkung von solchen Ereignissen eher gering. Die Bereitschaft, eigene Schutzmaßnahmen zu ergreifen, steigt erst, wenn konkrete wirtschaftliche Verluste drohen. Dies bestätigt auch eine Umfrage der Zeitschrift „KES“ (3/2002). Danach ist der Hauptgrund für Sicherheitslücken das fehlende Sicherheits-Bewusstsein der Mitarbeiter:

¹ Quelle: Informationweek 18, Sept 2002, Studie von Price Waterhouse Coopers

- 65 Prozent Bewusstsein bei Mitarbeitern
- 61 Prozent Bewusstsein und Unterstützung im mittleren Management
- 50 Prozent Bewusstsein beim Top Management
- 46 Prozent Geld
- 38 Prozent Möglichkeit zur Durchsetzung sicherheitsrelevanter Maßnahmen
- 37 Prozent verfügbare und kompetente Mitarbeiter
- 34 Prozent Kontrolle auf Einhaltung von Sicherheitsmaßnahmen

Will ein Unternehmen sich also besser vor Angriffen schützen, muss es im eigenen Unternehmen mit Aufklärungsarbeit anfangen. Die Unternehmen müssen sich einen Überblick über die Bedrohungslage verschaffen und die Mitarbeiter entsprechend sensibilisieren. Dazu gehört, dass das Management mit gutem Beispiel vorangeht.

■ 1.2 Rechtliche Aspekte der IT-Sicherheit

Neben den technischen Eigenschaften von Systemen und Netzen sowie den organisatorischen Maßnahmen spielen rechtliche Aspekte in der IT-Sicherheit eine immer größere Rolle.

■ 1.2.1 Haftung und Schadenersatz

Unternehmen, die zum Beispiel als Service-Provider tätig sind, gewährleisten die Verfügbarkeit von Daten und Anwendungen. Bei einem Virenangriff auf den Server des Service-Providers kann es zu Ausfallzeiten kommen. Liegen diese außerhalb der vertraglichen vereinbarten Verfügbarkeit und ist der Geschäftsbetrieb des Kunden beeinträchtigt könnten Schadensersatzansprüche geltend gemacht werden.

Die Unternehmensleitung haftet gegenüber Dritten in aller Regel auch für das Verschulden einzelner Mitarbeiter (gemäß §278 BGB). Kritisch kann die Situation für die Mitglieder der Unternehmensleitung werden, wenn durch mangelnde Sicherheitsmaßnahmen massive Schäden für das Unternehmen entstehen: in zivilrechtlicher Hinsicht haften Geschäftsführer gemäß §43 GmbH-Gesetz und Vorstände gemäß §93 II Aktien-Gesetz dem Unternehmen gegenüber. Sie haben dem Unternehmen gegenüber eine Vermögensbetreuungspflicht, bei deren Verletzung sie sich gemäß §266 StGB strafbar machen. Diese Vermögensbetreuungspflicht verlangt, dass Geschäftsführer, Vorstände und Aufsichtsräte sämtliche erkennbar notwendigen Maßnahmen ergreifen, um Schäden vom Unternehmen abzuwenden. IT-Risiken sind vorhersehbare Risiken.

Die Geschäftsleitung ist daher dafür verantwortlich, dass alles Notwendige und Angemessene getan wird, um Haftungsrisiken des Unternehmens abzuwenden. IT-Sicherheit ist somit nicht nur eine Aufgabe der Fachabteilungen, sondern in erster Linie Chefsache.

■ 1.2.2 Datenschutz und Fernmeldegeheimnis

Auch wenn noch kein Schaden entstanden ist, kann die mangelnde Umsetzung von IT-Sicherheit schnell teuer werden. In Fällen, in denen personenbezogene Daten nicht ausreichend gemäß den Vorgaben des Bundesdatenschutzgesetzes (BDSG) geschützt werden, kann die Aufsichtsbehörde je nach Schwere des Verstoßes Bußgelder und sogar Freiheitsstrafen von bis zu zwei Jahren gegen die Verantwortlichen verhängen.

Erwähnenswert ist in diesem Falle, dass der Schutz der personenbezogenen Angaben durch angemessene vorgeschriebene IT-Sicherheitsmaßnahmen erfüllt werden muss (siehe Anlage zu §9 BDSG).

Ähnlich verhält es sich mit dem Fernmeldegeheimnis, welches als Grundrecht nach §10 des Grundgesetzes nicht nur in der Sprachkommunikation sondern auch bei der Datenübertragung und der Internet-Nutzung Gültigkeit besitzt. Auch der Bruch des Fernmeldegeheimnisses ist nach dem Telekommunikationsgesetz mit Geldstrafe oder Freiheitsstrafe bis zu 2 Jahren belegt.

■ 1.2.3 Telekommunikationsüberwachung und Verschlüsselung

Staatliche Interessen der inneren Sicherheit erfordern per Gesetz die Überwachung des Telekommunikationsverkehrs und damit die Aufhebung des Fernmeldegeheimnisses des Betroffenen. Telekommunikationsbetreiber sind daher verpflichtet, den Behörden die angefragten Inhalte und Begleitumstände von Telefonaten zukommen zu lassen. Schutz bietet in diesem Falle nur eine starke, durchgehende („Ende-zu-Ende“-) Verschlüsselung durch die Kommunikationspartner. In Deutschland unterliegt der Einsatz dieser Verschlüsselungsverfahren keinerlei Kryptokontrolle und ist somit legal. Das ist nicht in jedem Land der Fall. Wird Verschlüsselungssoftware bei grenzüberschreitender Telekommunikation eingesetzt, beispielsweise in Unternehmen mit Auslands-Standorten, sollte daher zunächst geprüft werden, ob die grenzüberschreitende Verschlüsselung legal ist.

■ 1.2.4 Urheberrecht

Sensibel in Unternehmen ist auch das Thema Software-Lizenzierung. Raubkopien auf Firmenrechnern sind illegal – auch wenn Mitarbeiter sie völlig unbewusst angelegt haben. Wer den legalen Ursprung seiner Software nicht einwandfrei belegen kann, läuft Gefahr, wegen Software-Piraterie und Verstößen gegen das Urheberrecht des Software-Lieferanten angezeigt zu werden.

Bei Vorsatz kann dies sogar einen Straftatbestand erfüllen. Dabei kann die Geschäftsführung eines Unternehmens strafrechtlich zur Verantwortung gezogen werden, wenn ihre Entscheidung zur Tatbegehung beigetragen hat. Ein Unterlassungsdelikt kommt in Betracht, wenn sie trotz konkreter Eingriffsmöglichkeiten keine Maßnahmen ergriffen hat.

■ 1.2.5 Gefährdende Webinhalte und Privatnutzung betrieblicher Rechner

Ähnlich brisant wie der sorglose Umgang mit nicht lizenzierte Software ist die bewusste oder unbewusste Vorhaltung von Gewalt verherrlichenden oder Jugend gefährdenden Internet-Inhalten auf Firmenrechnern. Alle gängigen Browser legen die besuchten Internetseiten im Zwischenspeicher

(„Cache“) ab und somit sind auch privat am Arbeitsplatz angesehene Seiten auf den Firmenrechnern zu finden. Obwohl das Teledienste-Gesetz (TDG) zwischen der Verantwortung für eigene und für fremde Inhalte unterscheidet, ist die rechtliche Auslegung des TDG im Einzelnen umstritten. Um die strafrechtliche Verantwortung der Unternehmensleitung zu minimieren, sind klare betriebliche Regelungen erforderlich, die sich mit der privaten Internet-Nutzung am Arbeitsplatz befassen. Wird die private Nutzung geduldet – also kein ausdrückliches Verbot erteilt – dann können sich die Mitarbeiter auf das Daten- und Fernmeldegeheimnis berufen und dadurch die Nachverfolgung der besuchten Internetseiten erschweren. BITKOM hat zu diesem Thema im August 2003 einen Leitfaden zur Nutzung von E-Mail und Internet am Arbeitsplatz vorgelegt, der kostenlos von der Website „www.bitkom.org/publikationen“ herunter geladen werden kann.

■ 1.3 Konkrete Bedrohungen für Unternehmen

Die meisten Unternehmen haben in den letzten Jahren die Vernetzung stark vorangetrieben. Ohne Internetanbindung sind Geschäftsvorgänge heute nicht mehr denkbar. Immer mehr Anwendungen, die früher auf dem eigenen Server oder im Rechenzentrum liefen, werden heute von einem Outsourcing-Partner betrieben. Mit der notwendigen Offenheit des Firmennetzes kommen aber zeitgleich neue informationstechnische Bedrohungen auf das Unternehmen zu. Die Bedrohungen lassen sich in absichtlich (passive- und aktive Angriffe) sowie unabsichtliche Bedrohungen unterteilen, für die in der folgenden Übersicht Beispiele aufgeführt werden.

Absichtlich herbeigeführte Bedrohungen		Unabsichtlich herbeigeführte Bedrohungen
Passive Angriffe	Aktive Angriffe	
<ul style="list-style-type: none"> ■ Abhören von sensitiven Daten, etwa <ul style="list-style-type: none"> ■ Teilnehmer-Identitäten ■ Authentifizierungsdaten ■ Verkehrsflussanalyse 	<ul style="list-style-type: none"> ■ Eingriff in die Datenübertragung (etwa Unterbrechung) ■ Modifikation, Zerstörung, Wiederholung und Verzögerung, Verhinderung durch Überlast-Erzeugung (Denial of Service) ■ Sabotage ■ Vortäuschen einer Identität ■ Einbringen von Schadsoftware (Viren, Würmer usw.) 	<ul style="list-style-type: none"> ■ Fehler und Ausfall aufgrund von <ul style="list-style-type: none"> ■ menschlichem Versagen (Fahrlässigkeit, Fehlbearbeitung) ■ mangelhaften Systemen ■ Umwelteinflüssen ■ Naturkatastrophen ■ Alterung von Systemen ■ Störstrahlung

Bedrohungen gehen von unterschiedlichen Quellen aus. Einige Bedrohungen entstehen unabsichtlich oder durch höhere Gewalt, beispielsweise durch Naturkatastrophen oder durch technisches Versagen. Andere Bedrohungen ergeben sich im Tagesgeschäft der elektronischen Dienstleistung, in der Geschäftsvorgänge nachweislich und verbindlich sein müssen.

Der Nutzer ist jedoch für die meisten Bedrohungen selbst verantwortlich. Schadenprogramme werden bewusst oder unbewusst verbreitet, Informationen ausgespäht, verändert oder missbraucht. Kritisch kann auch der Ausfall dringend benötigter Infrastruktur (Daten- und Kommunikationsnetze, Server und Rechenzentren) werden, falls keine entsprechenden Notfallprozesse oder Backup-Prozeduren existieren. Der Schutz unternehmenskritischer IT-Infrastrukturen gegen Bedrohungen



der Verfügbarkeit, Vertraulichkeit und Integrität muss daher im wirtschaftlichen Interesse des jeweiligen Unternehmens eine wichtige Rolle einnehmen.

Zahlreiche Branchen erbringen ferner Leistungen zur Grundversorgung der Bevölkerung, beispielsweise Telefongesellschaften, Strom- und Wasserwerke oder die Stellen zur Sicherung des Luft- und Verkehrsnetzes. Kommt es hier zu Ausfällen, stellt dies, selbst bei zeitlicher Begrenzung, ein Risiko für die Wirtschaft und dem Staat dar. In diesem Zusammenhang spricht man allgemein von kritischen Infrastrukturen, die besonders gesichert sein sollten. Die betroffenen Unternehmen müssen daher gemäß gesetzlichen Regelungen, aber auch im eigenen wirtschaftlichen Interesse weitergehende Maßnahmen zur Funktionsfähigkeit ihrer Systeme ergreifen.

Die zunehmende Vernetzung sorgt für weltweit höheren Wettbewerb und Kostendruck. Deswegen können Unternehmen es sich nicht leisten, die Sicherung des Unternehmenswissens, welches fast nur noch elektronisch aufbewahrt ist, dem Zufall zu überlassen. Jedes Unternehmen braucht ein Datensicherungskonzept, welches sich dynamisch an die sich ständig ändernden Herausforderungen anpasst. Diese Aufgabe muss auch von der Geschäftsleitung kontrolliert werden.

■ 1.4 Was wird von Systemen und Netzen erwartet?

Technische Systeme sollen so funktionieren, dass sich der Benutzer auf sie verlassen kann. Informationstechnische Systeme müssen in erster Linie hohe Vertraulichkeit, Integrität und Verfügbarkeit besitzen.

Eigenschaft	Ziel
Vertraulichkeit	Die Informationen können von Unbefugten nicht eingesehen werden. Das System ist so aufgebaut, dass nur befugte Personen Zugriff auf die Informationen haben können.
Integrität	Informationen, Systeme und Netze können nicht unbemerkt verändert werden. Das System ist so beschaffen, dass eine Veränderung offensichtlich wird.
Verfügbarkeit	Informationen, Systeme und Netze sind verfügbar. Das System muss bei einem Zugriff in einem definierten Zeitraum antworten bzw. bestimmte Aktionen auslösen.

Jedes System wird in einem Kontext verwendet, der normalerweise über die technischen Aspekte hinausgeht. Dafür sind in der Regel weitere Eigenschaften nötig, wie etwa Authentizität (ggf. gibt es auch Forderungen nach Pseudonymität oder Anonymität), Zurechenbarkeit, Revisionsfähigkeit oder Verbindlichkeit.

Eigenschaft	Ziel
Authentizität	Die Identität von Informationen, Systemen, Netzen oder Personen kann zweifelsfrei nachgewiesen werden.
Zurechenbarkeit	Aktionen und Informationen können einer auslösenden Instanz (Person oder System) zugerechnet werden. Die Zurechenbarkeit folgt mitunter aus der Authentizität.
Rechtssicherheit und Revisionsfähigkeit	Alle für den Rechtsverkehr (z.B. Haftung und Gerichtsfestigkeit) in Systemen und Netzen verwendeten Informationen und Vorgänge gegenüber Dritten sind (z.B. im Rahmen einer Wirtschaftsprüfung) nachweisbar.
Verbindlichkeit	Willenserklärungen oder Daten in digitaler Form sind verbindlich. Verbindlichkeit ergibt sich aus dem Nachweis der Authentizität, der Zurechenbarkeit und der Integrität von Daten.

IT-Sicherheit ist also keine rein technisch zu betrachtende Unternehmensangelegenheit. Vielmehr sind auch juristische, organisatorische und nicht zuletzt personelle Aspekte zu berücksichtigen. Demzufolge kann die rein technische Betrachtung von IT-Systemen auch keine abschließende Aussage über deren Sicherheit machen. Darum darf Unternehmenssicherheit nicht alleinige Aufgabe der IT-Abteilung oder gar eines einzelnen Netzwerkadministrators sein. Die Sicherheit von Systemen und Netzen ist in erster Linie in Verantwortung der Geschäftsleitung. Sie muss jedoch von Experten konzeptioniert und umgesetzt werden. In einem Spezialistenteam unter Beteiligung der relevanten Unternehmensinteressen müssen alle Aspekte aufgenommen und Konzepte entwickelt werden, die einem ganzheitlichen Ansatz folgen. Nur so lässt sich ausschließen, dass Lücken im Konzept unerkannt bleiben oder gar neue Schwachstellen entstehen. Unabdingbar für Unternehmen jeglicher Größe ist ein umfassendes Sicherheitskonzept.

■ 1.5 Sicherheitskonzept

Bei dem Einsatz neuer Technologien entstehen neue Sicherheits-Bedrohungen, denen sich der Nutzer bewusst sein muss. Diese Bedrohungen können systemimmanent sein oder durch bewusste und unbewusste Handlungen herbeigeführt werden.

Um die Bedrohung zu minimieren und das Anwendungsrisiko der neuen Technologie zu reduzieren können technische, personelle und organisatorische Maßnahmen festgelegt werden.

Für IT-Sicherheit zu sorgen, bedeutet auch eine ganzheitliche Gefährdungs- und Risikoanalyse zu erarbeiten. Das Sicherheitskonzept für ein Unternehmen muss organisatorische, personelle sowie technische Maßnahmen umfassen.

Folgendes Vorgehen ist bei der Entwicklung eines solchen Sicherheitskonzepts zu empfehlen:

1. Inventarisierung der Unternehmenswerte
2. Klassifikation nach Schutzbedarf
3. Bedrohungs- und Schwachstellenanalyse
4. Risikoanalyse
5. Priorisierung der Schutzziele und Empfehlung von angepassten Schutzmaßnahmen
6. Festlegung der Risikopolitik und Auswahl der einzusetzenden Schutzmaßnahmen

In den folgenden Abschnitten stellen wir die einzelnen methodischen Schritte vor, um ein Sicherheitskonzept zu erstellen. In der Fachliteratur sind vielfältige Beispiele zur Vorgehensweise zu finden².

■ 1.5.1 Inventarisierung der Unternehmenswerte

Das Sicherheitskonzept muss das ganze Unternehmen mit seinen Geschäftsprozessen und die Einbettung in eine Wertschöpfungskette berücksichtigen. Bevor das Konzept erstellt werden kann, muss daher zunächst ermittelt werden, welche Unternehmenswerte und welche Prozesse zu schützen sind. Dazu wird eine strukturierte Systemanalyse durchgeführt, die unter anderem folgende Bereiche einschließt:

- Infrastruktur des Unternehmens
- Eingesetzte Hard- und Software
- Informationen
- Anwendungsdaten
- Prozesse
- Kommunikationsverbindungen
- Personen

Um IT-Anwendungen zu analysieren, kann man sich an bereits vorhandene Sicherheitsrichtlinien orientieren (Beispiele: IT-Grundschutzhandbuch³, Common Criteria⁴ oder Standard BS 7799⁵/ISO 17799⁶).

2 Sven Schumann, Vorgehensweise bei der Erstellung einer unternehmensweiten Security Policy, Sven Schumann, Datenschutz und Datensicherheit DuD 26 (2002); 3 IT-Grundschutzhandbuch, ISBN 3-88784-915-9, Bundesanzeiger-Verlag, Postfach100534, 50455 Köln; 4 Common Criteria - Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik v2.1, IS 15408, Bundesamt für Sicherheit in der Informationstechnik, Referat III 2.3, Postfach 20 03 63, 53133 Bonn; 5 BS 7799, Part 1: ISBN o 580 28271 1, Part 2: ISBN o 580 28280 5, BSI Group HQ, 389 Chiswick High Road, London, W4 4AL, United Kingdom; 6 ISO 17799, Beuth Verlag GmbH, 10772 Berlin

■ 1.5.2 Klassifikation nach Schutzbedarf

Nach Abschluss der Analyse werden die Güter (Unternehmenswerte und Prozesse) in Schutzklassen gruppiert. Die Unternehmens-Informationen (unabhängig vom Aufbewahrungsmedium z.B. Papier, Festplatten) und die Systeme sind unterschiedlich sensitiv und müssen daher unterschiedlich geschützt werden. Um das Schutzniveau festzulegen, kann ein Schutzklassenkonzept eingeführt werden, das nach Geheimhaltungsgrad und Verfügbarkeitsanforderung unterscheidet. Dabei hat es sich bewährt, in wenige Klassen zu differenzieren. Hier ein Beispiel dazu:

Schutzklasse	Informationen und Systeme		Konsequenz bei Aus-spähung, Missbrauch, Ausfall oder Verlust
	Geheimhaltungsgrad	Verfügbarkeits-anforderung	
„hoch“	Streng vertraulich	Hoch verfügbar	<ul style="list-style-type: none"> ■ Schwere Schäden ■ Nicht rechtzeitig wieder beschaffbar ■ Rekonstruktion erheblich kostenintensiv
„mittel“	vertraulich	Mittlere Verfügbarkeit notwendig	<ul style="list-style-type: none"> ■ Leichtere Schäden ■ Rekonstruktion zeit- und kostenintensiv
„niedrig“	firmenvertraulich (intern frei zugänglich)	Geringe Verfügbarkeitsanforderungen	<ul style="list-style-type: none"> ■ Geringfügige Schäden
„öffentlich“	frei zugänglich	Verfügbarkeit ist unwesentlich	<ul style="list-style-type: none"> ■ Keine Nachteile oder Schäden zu befürchten

■ 1.5.3 Bedrohungs- und Schwachstellenanalyse

Nach der Einteilung in Schutzklassen schließt sich eine Bedrohungsanalyse an. Es werden alle vorstellbaren Bedrohungen, die Schäden verursachen könnten, ermittelt. Die Bedrohungen werden verschiedenen Ebenen zugeordnet: der rechtlich-wirtschaftlichen, der organisatorisch-sozialen, der logischen und der physischen Ebene.

Ebene	Bedrohungen
Rechtlich-wirtschaftlich	<ul style="list-style-type: none">■ Spionage und Diebstahl■ Verbot einer nicht-legalen Anwendung■ Vertragliche Abhängigkeit von Dritten
Organisatorisch-sozial	<ul style="list-style-type: none">■ Fahrlässige, fehlerhafte Handlungen■ Sabotage■ Fehlerhafte Programmierung und Planung
Logisch	<ul style="list-style-type: none">■ Zerstörung oder Veränderung von Informationen und Programmen■ Duplikation und Weitergabe von Informationen an Unbefugte■ Unbefugte Nutzung (Missbrauch) von Einrichtungen
Physisch	<ul style="list-style-type: none">■ Störung der Elektronik oder Stromversorgung■ Unterbindung der Übertragung■ Mechanische Alterung■ Störung und Zerstörung / Sabotage

Bei der Schwachstellenanalyse wird ein Bezug zwischen gefährdeten Objekten und möglichen Bedrohungen hergestellt. Die Schwachstellen werden dann erneut in die vorher dargestellten Ebenen integriert.

Das folgende einfache Beispiel soll diese Einordnung verdeutlichen. Die typische Schwachstellenanalyse sollte sich allerdings auf wesentlich höherem Detaillierungsgrad bewegen, um ein tatsächlich verwertbares Ergebnis hervorzubringen.

Bedrohungen / Objekte	Rechenzentrum	Netze	Desktop-PCs	Produktion
Spionage und Diebstahl	X	X	X	X
Verbot einer nicht-legalen Anwendung	–	–	–	X
Vertragliche Abhängigkeit von Dritten	X	X	–	–
Fahrlässige, fehlerhafte Handlungen	X	X	–	X
Sabotage	X	X	–	X
Fehlerhafte Programmierung und Planung	X	X	–	X
Zerstörung oder Veränderung von Informationen und Programmen	X	X	–	X
Duplikation und Weitergabe von Informationen an Unbefugte	X	X	X	–
Unbefugte Nutzung (Missbrauch) von Einrichtungen	–	X	X	–
Störung der Elektronik oder Stromversorgung	X	X	X	X
Unterbindung der Übertragung	–	X	–	X
Mechanische Alterung	–	–	–	X
Störung / Zerstörung / Sabotage	X	X	X	X

■ 1.5.4 Risikoanalyse

Als nächster Schritt muss eine Risikoanalyse für die IT-Objekte erfolgen. Hier sollen die Häufigkeit und Höhe von Schäden den jeweiligen Bedrohungen zugeordnet werden.

In der Regel kann keine genaue Schadenshöhe geschätzt werden, auch die Eintrittswahrscheinlichkeit lässt sich nur grob klassifizieren und nicht detailliert ermitteln. Um dennoch die Schadenshöhe zu bemessen, kann das Ergebnis der Schutzbedarfsanalyse helfen. Die Eintrittswahrscheinlichkeiten für bestimmte Schadensszenarien können aus der Schwachstellenanalyse abgeleitet werden.

■ 1.5.5 Priorisierung der Schutzziele und Empfehlung von angepassten Schutzmaßnahmen

Das Ergebnis der Risikoanalyse ist der Ausgangspunkt, um die Maßnahmen zum Schutz der Unternehmenswerte abschließend zu bewerten und zu priorisieren. Die Sicherheitsmaßnahmen müssen nach ihren Eigenschaften und Auswirkungen gegliedert und unter Kosten-/Nutzen-Aspekten bewertet werden. Insbesondere sind zu beachten:

Zulässigkeit	Ist die Maßnahme rechtlich umsetzbar? Stehen konkrete Gesetze oder Verordnungen dagegen? Beispiel: Überwachung der E-Mail-Kommunikation.
Ausgewogenheit und Angemessenheit	Berücksichtigt die Maßnahme alle unterschiedlichen Interessen innerhalb und außerhalb des Unternehmens?
Praktikabilität	Ist der Einsatz der Maßnahme unter den gegebenen Voraussetzungen praktikabel?
Wirksamkeit	Erreicht die Maßnahme das Ziel?
Kosten	Ist die Anwendung der Maßnahme unter ökonomischen Gesichtspunkten sinnvoll? Beispiel: Die Steigerung eines technischen Sicherheitsniveaus lässt die Kosten überproportional steigen. Die Kosten übersteigen an einem bestimmten Punkt den ökonomischen Gegenwert des zu schützenden Gutes.

Ein Hinweis: Die Kosten für Sicherheitsmaßnahmen sind letztlich gut investiert. Sie helfen dabei, mögliche finanzielle Verluste des Unternehmens zu reduzieren oder zu verhindern.

■ 1.5.6 Festlegung der Risikopolitik und Auswahl der einzusetzenden Schutzmaßnahmen

Es ist Aufgabe der Geschäftsführung, die Risikopolitik festzulegen und die jeweiligen Risikokomponenten zu berücksichtigen. Werden diese Anforderungen konsequent umgesetzt, verfügt das Unternehmen letztlich über ein Sicherheitskonzept, welches den konkreten Risiken entsprechende Maßnahmen entgegenstellt. Die Risiken werden dabei auf ein annehmbares Niveau reduziert. Einzelne Risiken können erhalten bleiben. Diese verbleibenden Risiken sollten entweder versichert oder zumindest bewusst in Kauf genommen werden.

Unternehmen, die über keine oder nur wenige hoch qualifizierte Mitarbeiter im Bereich IT-Sicherheit verfügen, sollten auf externe Unterstützung zurückgreifen, wenn sie ihr Sicherheitskonzept entwickeln.

Ist das Sicherheitskonzept erstellt und umgesetzt, so ist es noch lange nicht abgeschlossen. Die technische Infrastruktur und das Unternehmensumfeld entwickeln sich permanent weiter und deshalb ist es notwendig, das Konzept periodisch zu überprüfen und ggf. anzupassen. Nur dann ist das Unternehmen dauerhaft und wirksam geschützt.



Bei der Weiterentwicklung des Sicherheitskonzeptes sollte insbesondere beachtet werden, dass die Geschäftsführung kontinuierlich Rückmeldungen aus dem operativen Betrieb erhält. Bei der Umsetzung der Maßnahmen ergeben sich oft aktuelle Probleme. Durch den Austausch lassen sich auch auf Dauer Sinn und Akzeptanz der Maßnahmen überprüfen. So kann aus einem technisch-organisatorischen Konzept eine unternehmensweite Sicherheitskultur entstehen.

■ 2 Bedrohung und Schutz

Die folgenden Kapitel sollen exemplarisch aufzeigen, welche Elemente der Unternehmens-Infrastruktur gefährdet sind und erste Hinweise geben, wie sich die Sicherheit hier erhöhen lässt. Die Ratschläge können aber keinesfalls eine kompetente Beratung und ein von Experten erstelltes Sicherheitskonzept ersetzen.

■ 2.1 Arbeitsplatzrechner

Die meisten Arbeitsplatzrechner im Unternehmen sind PCs, die mit Microsoft-Betriebssystem und -Anwendungssoftware ausgerüstet sind. Gerade die hohe Verbreitung dieser Software begünstigt, dass Schadprogramme entwickelt werden, die die Schwachstellen der eingesetzten Software ausnutzen. Beispielsweise gibt das Werkzeug „Back-Orifice“ einem Angreifer sehr leistungsfähige Möglichkeiten, einen Rechner auszuspähen. Daher müssen Arbeitsplatzrechner in besonderer Weise geschützt werden. Folgende Gefährdungen von Arbeitsplatzrechnern sind mindestens zu beachten:

■ 2.1.1 Manipulation von Anwendungssoftware

In manchen Fällen enthalten Programme noch aus ihrer Entwicklung spezielle Testmodi, die zulassen, dass das Sicherheitssystem umgangen werden kann. Somit kann der Anwender beim Ausnutzen dieser Sicherheitslücke auf sensitive Bereiche zugreifen, die ihm ansonsten verborgen blieben. Um den PC zu warten haben manche auch Super-PINs, mit denen das Sicherheitssystem ebenfalls umgangen werden kann.

Anwendungsprogramme, die „Trojanische Pferde“ sind, enthalten neben der gewünschten Funktionalität auch nicht dokumentierte und schwer erkennbare Funktionen, mit denen beispielsweise der Rechner ausgespäht oder sogar ferngesteuert werden kann. Der Benutzer kann nicht a priori erkennen, ob es sich bei der Software, die er z.B. aus dem Internet herunter lädt, um ein trojanisches Pferd handelt. Die ausgespähten Daten können bei einer bestehenden Internetverbindung an den Hacker des „Trojanischen Pferds“ gesendet werden. Mittels eines solchen „Trojanischen Pferds“ können bei entsprechender Programmierung alle Benutzereingaben aufgezeichnet werden, so dass dem Hacker gegebenenfalls PINs und Passwörter in die Hände fallen. Mit diesen Informationen können dann weitere Angriffe nicht nur auf den Arbeitsplatzrechner selber, sondern auch auf andere Teile des Netzwerks und Server vorbereitet werden. Hierbei kann es sich beispielsweise auch um den Zugang zu einem Online-Banking-System handeln.

■ 2.1.2 Virenbefall von Rechnern

Computerviren sind eigenständig ausführbare Programmroutinen, die Daten oder Programme verfälschen oder löschen können. Sie reproduzieren sich selbst und führen für den Anwender nicht kontrollierbare Aktionen aus. Viren können jedoch nicht alleine existieren, sondern sie hängen sich an andere Daten an und vermehren sich bei deren Ausführung oder Verarbeitung. Diese Daten können Programme, Bootsektoren oder Dokumente sein.

- Bootsektor-Viren befallen den Bootsektor von Disketten oder Festplatten. Aktiviert wird der Virus durch einen Kalt- oder Warmstart. Diese Viren können sich unabhängig vom Betriebssystem auf alle Bootsektoren setzen. Sogar eine Diskette, die gar nicht bootfähig ist und nur vor dem Booten im Laufwerk vergessen wurde, kann einen Bootsektor-Virus verbreiten.
- Datei-Viren befallen ausführbare Dateien von Programmen (Wirtsprogrammen) und werden durch den Aufruf des Programms aktiviert.
- Bei Makro-Viren sind alle Dokumente gefährdet, die in der Lage sind, Informationen in Makros abzulegen. Aktiviert werden Makro-Viren durch den Aufruf der Dateien. Diese Viren sind besonders gefährlich, da sie sich schnell verbreiten, wenn infizierte Dokumente als Anlage in E-Mails verschickt werden.

Viren können sowohl unbeabsichtigt als auch bewusst eingeschleust werden. Sie können insbesondere über den Austausch von Dateien per E-Mail oder per Datenträger übertragen werden. Zum Schutz der eigenen Systeme muss daher jede fremde Datei zuerst auf Viren überprüft werden, bevor sie im eigenen System gespeichert und genutzt wird.

In letzter Zeit sind viele Falschmeldungen über Viren (so genannte Hoaxes) per E-Mail verbreitet worden. Ein Beispiel ist die Warnung vor dem angeblichen Virus „Good Times“, die einige Mailinglisten verstopfte. Falschmeldungen warnen vor nicht existierenden Bedrohungen und beinhalten Ratschläge, was zu tun ist, um sich vor diesen angeblichen Bedrohungen zu schützen. Werden diese Ratschläge ernst genommen und umgesetzt, entsteht personeller und technischer Schaden. Der Administrator führt entsprechend den Ratschlägen Sicherheitsmaßnahmen am System durch, die nicht notwendig sind und die später mit viel Aufwand wieder rückgängig gemacht werden müssen. Des Weiteren werden in der Regel Warnmeldungen über Viren an entsprechende Experten-Mailinglisten gesendet. Die Experten diskutieren über die Echtheit der Meldung. Stellt sich die Warnmeldung als eine Falschmeldung heraus, so steigt der Diskussionsbedarf in der Regel an. Aufgrund der erhöhten Kommunikation kann es auch zu einem Ausfall des Mailservers kommen.

Trojaner oder Trojanische Pferde verbergen ihren wahren Zweck, indem sie vorgeben, Spiele oder Software-Upgrades zu sein. Zum Beispiel kann ein Programm, das scheinbar ein Spiel ist, auch Dateien löschen, das System mit einem Virus infizieren oder Passwörter ausspähen (siehe Kapitel 2.1.1).

Würmer verbreiten sich über die Windows-Netzwerkfunktionen, Schnittstellen oder E-Mail-Clients wie Microsoft Outlook. Sie können eine E-Mail mit dem Wurm-Programm als Anlage erstellen oder sich selbst an ausgehende E-Mails anhängen. E-Mails, die von einem Wurm erstellt wurden, fordern häufig den Empfänger auf, die Anlage zu starten, um besondere Informationen sehen zu können. Andere Würmer nutzen die Mängel im Netzwerk-Code aus, um unbefugten Zugriff auf andere Rechner zu bekommen. Wenn sie Zugriff haben, suchen sie nach neuen Rechnern, um diese zu infizieren. Sie verbreiten sich vor allen auf Rechnern, die permanent an das Internet angeschlossen sind.

■ 2.1.3 Präventive Maßnahmen gegen Viren

Wer aktuelle Antivirus-Software (Scanner) einsetzt, kann sich vorbeugend gegen Virenbefall oder dessen Verbreitung schützen. Diese Programme durchsuchen Datenträger, Systembereiche, Ordner, Dateigruppen und einzelne Dateien auf Muster bekannter Viren, die in einer Datenbank abgelegt sind. Insbesondere die Kommunikationsknoten, über die Viren ins Unternehmensnetz gelangen können, sind zu sichern. Dazu zählen E-Mail-Server, Mail-Gateways oder Internet-Proxies. Wird eine Übereinstimmung mit einem Muster erkannt, warnt die Software vor einem möglichen Virus oder versucht, den Virus so zu entfernen, dass die ursprüngliche Funktionalität wieder hergestellt wird. Entscheidend ist jedoch, die Virenmusterdatenbank regelmäßig zu aktualisieren. Fast täglich werden neue Viren bekannt. Daher kann ein Virenprogramm, das auf einer veralteten Datenbank beruht, keine neuen Viren finden. Virens Scanner sind nur so gut wie ihre Virenmusterdatenbanken.

Der Einsatz zentral administrierbarer Produkte wird empfohlen. Diese können auf einem zentralen Server konfiguriert werden und erlauben damit auch eine automatische Verteilung der aktuellen Virenmusterdatenbank an jeden PC im Unternehmensnetz. Somit wird sichergestellt, dass jeder lokale PC über die aktuelle Virenmusterdatenbanken verfügt. Gleichzeitig werden die Mitarbeiter von administrativen Arbeiten entlastet und können sich auf ihre eigentliche Aufgabe konzentrieren.

Alle führenden Hersteller bieten residente Virenwächter, auch „On-Access-Scanner“ genannt, an. Diese Virenwächter laufen im Hintergrund und überwachen Systemkomponenten oder Betriebssystemschnittstellen. Sie suchen nach Anzeichen für Virenaktivitäten und nach bekannten Virenmustern. Werden diese gefunden, gibt der Wächter Alarm und versucht den auslösenden Prozess zu stoppen bzw. den Verursacher zu finden und den Virus zu entfernen. Unabhängig von der verwendeten Virenmusterdatenbank können Virenwächter Funktionen überwachen, die für Viren typisch sind. Dadurch können sie Viren entdecken, die noch nicht bekannt sind, diese stoppen und melden. Ein Nachteil dieser Funktion ist, dass auch schlecht programmierte Anwendungsprogramme, die z.B. versuchen fremde Dateien zu löschen, Alarm auslösen können. Manche E-Mail-Programme können so eingestellt werden, dass sie anhängende Dateien automatisch speichern, decodieren und ausführen. Diese Option sollte daher unbedingt abgeschaltet werden.

Alle eingehenden fremden Dateien sollten vor der Ausführung mit einem Virens Scanner geprüft werden.

Neben den technischen Sicherheitsvorkehrungen müssen auch organisatorische Maßnahmen durchgeführt werden. Es sollte ein „IT-Sicherheits-Verantwortlicher“ als Ansprechpartner für die Mitarbeiter benannt werden. Eine Unternehmensrichtlinie sollte Regeln zur Nutzung der Antivirensoftware festlegen und vorschreiben was zu tun ist, wenn ein Virus gefunden wurde.

Häufig werden erkannte Viren gelöscht. Für die Statistik ist es hilfreich zu dokumentieren, wie oft welche Viren auftreten. Eine Meldung an den IT-Sicherheits-Verantwortlichen sollte daher in der Richtlinie vorgeschrieben sein. Auch eine Meldung an ein Computer-Notfall-Team (CERT) ist sinnvoll.

Hier noch einige Sicherheitshinweise für die Virenprävention:

- Virensuchprogramme sollten eingesetzt werden. Empfohlen wird der Einsatz zentral administrierbarer Produkte.
- Wenn möglich, sollten auf den PCs und Servern Scanner von unterschiedlichen Herstellern eingesetzt werden.
- Die Virenmusterdatenbank sollte regelmäßig aktualisiert werden.
- Die Virensuchprogramme sollten über einen residenten Virenwächter verfügen.
- Jede externe Datei muss zuerst gescannt werden.
- Die Funktion, die in E-Mail-Programmen die anhängenden Dateien automatisch speichert, decodiert und ausführt, sollte deaktiviert werden.
- Alle Datenträger sollten in regelmäßigen Abständen gescannt werden.
- Regelmäßig sollten Backups durchgeführt werden. Sie schützen etwa vor einem eventuellen Datenverlust durch Virenbefall.
- Richtlinien, wie Mitarbeiter mit Viren und der Virensoftware umgehen sollen, müssen vorhanden sein.
- Mitarbeiter müssen sensibilisiert werden, damit sie die Organisationsanweisungen beachten.
- Ein Ausschalten des Virensuchprogrammes auf dem Arbeitsplatzrechner durch den Mitarbeiter sollte nicht möglich sein.

■ 2.1.4 Schwachstellen und „Features“ in Hard- und Software

Komplexe Hard- und Software ist nicht in jedem Fall frei von Schwachstellen. Diese Schwachstellen sind beliebte Angriffsziele von Hackern, um Zugriff auf einen Rechner zu erhalten. Manchmal sind auch so genannte Features in Hard- und Software in Wirklichkeit Schwachstellen. Obwohl sie für reguläre Zwecke vorgesehen sind, könnten sie missbraucht werden. Beispielsweise hat der „ILOVEYOU“-Virus ein Feature des Office-Pakets ausgenutzt, um sich an alle Personen im Adressbuch automatisch zu versenden. Manchmal sind sensible Funktionalitäten so praktisch, dass die Nutzer nur ungern auf sie verzichten wollen, obwohl sie ein Sicherheitsrisiko darstellen. In jedem Fall liegt die Herausforderung darin, den Missbrauch von diesen Funktionalitäten zu verhindern.

■ 2.1.5 Defekte in der Hardware

Defekte in der Hardware bedrohen die Integrität und Verfügbarkeit von Informationen. Teils durch technische Fehler, aber auch durch gezielte Angriffe verursacht, können zum Beispiel Zeitverzögerungen im Antwortverhalten einer Anwendung auftreten oder Daten verfälscht werden. Oft werden die Verfälschungen nicht unmittelbar bemerkt, was den Schaden noch vergrößert.

■ 2.1.6 Diebstahl von Komponenten

Wenn Komponenten oder ganze Rechner (Laptops und Standrechner) gestohlen werden, ist ein Unternehmen ernsthaft bedroht. Bei Laptops, die im Außendienst verwendet werden, ist der Diebstahl kritisch, wenn firmenrelevante Informationen auf dem Rechner gespeichert sind oder der Rechner den Zugriff auf das Unternehmensnetzwerk erlaubt. Je nach Authentifizierungsmethode und den Rechten des einwählenden Rechners ins Firmennetz können dabei sogar schwerwiegende Schäden angerichtet werden.

■ 2.1.7 Fehlende Benutzertrennung

Bei Rechnern, die von mehreren Personen zu unterschiedlichen Zeiten benutzt werden, besteht die Gefahr, dass die Daten auf dem Rechner nicht streng genug voneinander getrennt sind. Dies ist der Fall, wenn sich der Nutzer nur beim Einloggen in das Netzwerk oder in den Rechner authentifizieren muss, aber nicht mehr auf der Anwendungsebene.

■ 2.1.8 Ausspähung von Zugangscodes / Passwörtern

Die meisten Menschen müssen sich heute an vielen Stellen mit einer Geheimnummer oder einem Passwort identifizieren bzw. authentifizieren. Manche Personen können sich diese vielen Authentifizierungscodes nicht merken und speichern sie deshalb in einer Datei auf ihrem Arbeitsplatzrechner. Oft wird diese Datei so abgelegt, dass sie leicht ausgespäht und gelesen werden kann.

Ein weiteres Problem ist, dass die gewählten Passwörter häufig einfach zu erraten sind. Der Nutzer neigt dazu, leicht zu merkende Namen oder ein und dasselbe Passwort bei vielen unterschiedlichen Anwendungen zu wählen. Ein einmal ausgespähtes Passwort kann so schnell einen großen Schaden anrichten.

Nach wie vor kommt es vor, dass bei der Passwortabfrage im Internet dieses nicht verschlüsselt übertragen wird. So kann es im Internet leicht abgefangen und missbraucht werden.

Folgende Empfehlungen sind zum Umgang mit Passwörtern zu beachten:

Wahl von Passwörtern

- Triviale Passwörter vermeiden. Es müssen individuelle Kennungen verwendet werden.
- Passwörter sollten aus mindestens sechs Zeichen bestehen und sowohl Groß- als auch Kleinbuchstaben sowie Ziffern enthalten.

Schutz von Passwörtern außerhalb des Systems

- Passwörter müssen geheim gehalten werden. Sie dürfen nicht aufgeschrieben und keiner anderen Person – auch nicht dem Systemverwalter oder dem dienstlichen Stellvertreter – mitgeteilt werden.
- Passwörter sind regelmäßig zu ändern. Änderungen dürfen nur durch den jeweiligen Benutzer vorgenommen werden.
- Neue Passwörter müssen sich von den früher verwendeten unterscheiden.
- Passwörter müssen umgehend geändert werden, wenn der Verdacht besteht, dass sie kompromittiert wurden.

Schutz von Passwörtern innerhalb des Systems

- Passwörter sind im Computer verschlüsselt zu speichern.
- Die Passwortdatei ist gegen unberechtigtes Kopieren und Einsehen zu sichern.
- Passwörter dürfen bei der Eingabe nicht am Bildschirm angezeigt werden.
- Durch Systemverwalter eingerichtete Passwörter müssen vom Benutzer bei seiner ersten Anmeldung geändert werden.
- Alle Passwörter von System- oder Anwendungssoftware, die vom Hersteller voreingestellt wurden, sind nach der Installation des Systems umgehend zu ändern.
- Fehlgeschlagene Anmeldeversuche sind zu protokollieren. Nach mehreren fehlgeschlagenen Anmeldeversuchen unter derselben Benutzerkennung muss die Kennung für weitere Anmeldeversuche gesperrt werden.
- Speicherung der letztmalig erfolgreichen Anmeldung.

■ 2.2 Server

Die aufgeführten Bedrohungen gelten in gleicher Weise für Server. Im Unterschied zu den Arbeitsplatzrechnern können aber die Schäden erheblich schwerer ausfallen. In der Regel liegen auf den Servern sämtliche unternehmenskritischen Daten. Ein Unternehmen kann erheblich geschädigt oder sogar ruiniert werden, wenn diese Daten ausspioniert werden oder verloren gehen.

Verbreitete Betriebssysteme für Server sind derzeit Windows NT und Windows 2000 von Microsoft sowie verschiedene Unix-Varianten (z.B. Solaris, HP-UX, Linux). Grundsätzlich sind mit den verschiedenen Betriebssystemen auch unterschiedliche Gefährdungen verbunden. Es ist Aufgabe des Administrators, sich die notwendigen Informationen über Schwachstellen des Betriebssystems zu besorgen. Hier sollen im Folgenden nur allgemeine Empfehlungen für servergestützte Netze gegeben werden. Zu unterscheiden sind bei der Bedrohungsanalyse Server, die nur als Daten- oder Programmserver im Netzwerk stehen und solche, auf denen Anwendungen laufen, die direkt für den Internetzugriff bestimmt sind und bestimmte Dienste anbieten.

Maßnahmen um die Server im firmeninternen Netzwerk zu sichern:

- Server und Konsolen sollten in Räumen stehen, zu denen nur Berechtigte Zugang haben.
- Durch eine restriktive Rechtevergabe muss sichergestellt werden, dass nur Befugte den Zugang zu wichtigen Daten erhalten.
- Die Daten müssen regelmäßig gesichert werden (Backup) und die Datensicherung sollte dokumentiert werden.
- Die Backup-Medien sind an einem geeigneten und sicheren Ort (nicht neben den Servern) aufzubewahren.
- Eine sporadische Überprüfung auf Wiederherstellbarkeit der Datensicherungen ist wichtig.
- Regelmäßige, z.B. monatliche Sicherheitschecks anhand der Systemprotokolle sind durchzuführen.
- Eine aktuelle Dokumentation der Systemkonfiguration ist wichtig, um im Notfall das System wieder herstellen zu können.

Sind Server noch zusätzlich mit dem Internet verbunden, werden folgende Gefahren relevant:

■ 2.2.1 Verhinderung von Diensten

Ein so genannter „Denial-of-Service“-Angriff zielt darauf ab, bestimmte Dienste eines Servers zu sabotieren. Beispielsweise haben die „DDoS“ (Distributed Denial of Service)-Attacken des Frühjahrs 2000 bei diversen Onlinehändlern dazu geführt, dass die Webportale nicht mehr funktionsfähig waren. Allgemein werden durch diese Art der Angriff die verfügbaren Ressourcen so stark gebunden, dass entweder der Dienst für die regulären Nutzer erheblich verlangsamt ist oder sogar ganz zusammenbricht.

Das Angriff-Opfer kann technische präventive Maßnahmen nur insofern ergreifen, als er:

- nur Server mit hoher Leistungsreserve verwendet.
- redundante Internetverbindungen (zu unterschiedlichen Providern) unterhält.
- die Internetverbindungen kontinuierlich überwacht und seinen Provider bei einem akuten Angriff informiert.
- Firewalls- oder Paketfilter verwendet, die schnell umkonfigurierbar sind.
- Für alle Fälle einen Notfall- und Wiederanlaufplan ausgearbeitet hat.

Vor solchen Angriffen kann man sich am besten schützen, wenn alle Internet-Nutzer ihre Ressourcen so anlegen, dass kein Missbrauch erfolgen kann. Die von Bundesinnenminister Schily im Februar 2002 eingesetzte Task-Force „Sicheres Internet“ hat Maßnahmenkataloge erarbeitet, die für jede Nutzergruppe im Internet entsprechende Empfehlungen auflistet. Zu finden sind die Kataloge unter www.bsi.de.

■ 2.2.2 Manipulation gespeicherter Daten

Nicht immer ist das Ziel von Hackern, Daten zu zerstören. Manchmal werden Daten auch nur manipuliert. So kann es passieren, dass z.B. Server von Online-Händler angegriffen und deren Preise und Warenbeschreibungen verändert werden oder das Warenangebot unseriös erweitert wird.

■ 2.2.3 Inkonsistenz gespeicherter Daten

Häufig werden Daten redundant auf mindestens zwei Servern gehalten, um sie bei Verlust rekonstruieren zu können. Durch technische Defekte oder Angriffe können Daten so manipuliert oder verändert werden, dass sie inkonsistent werden. Ihre Rekonstruktion ist schwierig, wenn keine vertrauenswürdige Instanz vorhanden ist, aus der die Originaldaten zurück gewonnen werden können.

■ 2.2.4 Informationsverlust bei erschöpftem Speichermedium

Bestimmte Dienste sind davon abhängig, wie verfügbar die Systemressource z.B. Festplattenspeicher sind. Wird durch einen gezielten Angriff oder durch fehlerhafte Software die Kapazität des Speichermediums erschöpft, können Daten verloren gehen. Manche Angriffe bedienen sich dieser Methode, um Aufzeichnungen und Protokollierungen in Log-Dateien zu verhindern.

■ 2.2.5 Maßnahmen zur Sicherung der Internetverbindung

Es ist schwer, hier allgemeingültige Regeln aufzustellen. Wie sicher eine Internetverbindung ist, hängt wesentlich davon ab, wie die mit dem Internet verbundenen Komponenten (WWW-Server, Firewall, Router usw.) konfiguriert sind. Um Schwachstellen auszuschalten und mögliche Angriffe zu identifizieren, sollten regelmäßig Penetrationstests durchgeführt und Intrusion Detection Systeme eingesetzt werden.

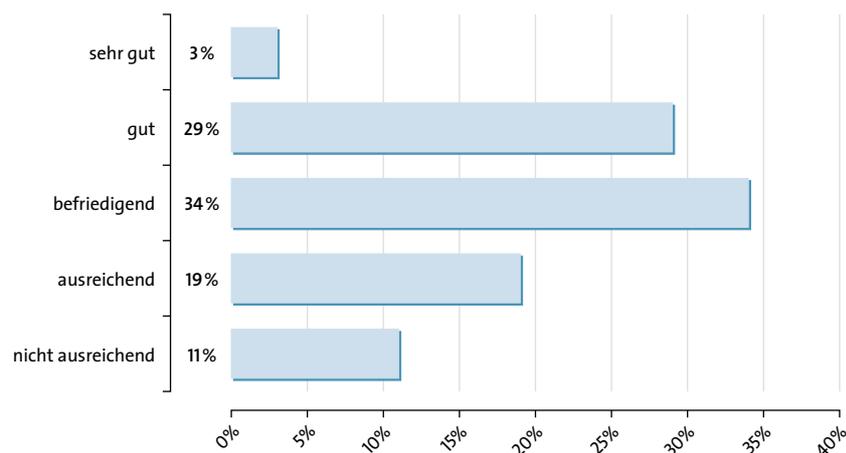
■ 2.3 Netzwerke und Telekommunikation

Damit zwei Rechner über ein Netzwerk kommunizieren können, müssen Regelungen über den formalen Aufbau der zu übertragenden Informationen festgelegt sein. Des Weiteren ist die Umsetzung der Information in elektronische Daten (Bits) zu regeln. In einem menschlichen Netzwerk sprechen wir beispielsweise die Sprache Deutsch. Im Duden ist festgelegt, wie Semantik und Grammatik der Sprache definiert sind.

Im Internet wird zur Verständigung das Protokoll TCP/IP benutzt. TCP/IP definiert zahlreiche Dienste, die dafür benötigt werden, die Kommunikation zu steuern. Wichtige und bekannte Dienste sind beispielsweise Webzugriffe über http, E-Mail über pop3 oder der Dateiaustausch über ftp.

Die Sicherheits-Zeitschrift „KES“ hat im Jahr 2000 eine Umfrage gemacht, die sich vor allem an Unternehmen aus der Informations- und Kommunikationsbranche richtete. Sie ergab folgendes Bild: Mehr als ein Drittel der Befragten schätzte die Sicherheit des Netzwerkes im eigenen Unternehmen nur als befriedigend ein. Ein weiteres Drittel beschrieb sie als ausreichend bis nicht ausreichend. Sehr wahrscheinlich ist, dass es um die Informationssicherheit in Unternehmen anderer Branchen noch schlechter bestellt ist.

■ Einschätzung der Informationssicherheit in der Telekommunikation / Datenfernübertragung



Quelle: KES 3/2000

Mit welchen Problemen müssen die Unternehmen rechnen? Worauf müssen sie sich einstellen und wogegen ihre Systeme schützen? Das folgende Kapitel soll die Gefährdungslage verdeutlichen und die wichtigsten Angriffe und Bedrohungen für die Netzwerk-Kommunikation darstellen. Gängige Schutzmaßnahmen gegen diese Angriffe sind etwa Leitungsverschlüsselungsgeräte, IPSEC-Produkte, SSL, E-Mail-Verschlüsselung (wie PGP) und digitale Signaturen.

■ 2.3.1 Abhören der Kommunikation

Um Daten zu übertragen kommen unterschiedliche Kommunikationsmedien in Betracht. In Unternehmen werden zumeist Glasfaser- und Kupferkabel verwendet, um Local Area Networks (LAN) zu realisieren. Für das Wide Area Network (WAN) wird meist zusätzlich auf drahtlose Verbindungen zurückgegriffen.

Drahtgebundene Verbindungen	Drahtlose Verbindungen		
Kabelverbindungen	Gerichtete Funkverbindungen	Ungerichtete Funkverbindungen	Infrarotverbindungen
<ul style="list-style-type: none"> ■ geschirmtes Kupferkabel ■ Koaxialkabel ■ Glasfaserkabel 	<ul style="list-style-type: none"> ■ Richtfunk 	<ul style="list-style-type: none"> ■ Mobilfunk ■ Seefunk ■ Betriebsfunk ■ BlueTooth, wireless LAN 	<ul style="list-style-type: none"> ■ PC zu PC ■ PC zu Peripheriegeräten
	Satellitenverbindung		

Grundsätzlich gilt, dass Leitungen abgehört werden können. Rein physikalisch gesehen, kann die Abstrahlung der Leitungen dazu genutzt werden, die übertragenen Signale mitzuhören. Die technischen Möglichkeiten lassen zu, dass fast alle Leitungstypen mit unterschiedlich hohem technischem Aufwand abhörbar sind, und zwar sowohl geschirmte Leitungen, koaxiale Leitungen als auch Glasfaserleitungen.

Bei Funk- und Infrarotverbindungen ist die Möglichkeit zum Abhören noch größer. Bei ungerichteten Verbindungen kann theoretisch jeder, der sich im Empfangsbereich des Senders und Empfängers befindet, die übertragenen Daten mithören. Bei gerichteten Funkverbindungen ist der Aufwand höher. Im Mobilfunkbereich wird zwar die Kommunikation zwischen der Basisstation und dem Mobilfunkgerät („Handy“) verschlüsselt, jedoch nicht die Kommunikation entlang des weiteren Übertragungsweges (Festnetzweges).

Spezielle Suchmaschinen können die übertragenen Daten mit hinterlegten Referenzdaten, wie beispielsweise die Schlüsselwörter „Angebot“ oder „Vertrag“ vergleichen. Werden solche Wörter gefunden, können sie an Lauscher oder Analyseprogramme übertragen werden.

Verhindern kann man das Abhören nur, indem ausschließlich die Daten verschlüsselt über die Kommunikationsmedien versendet werden!

Die ständig wachsende Rechnerleistung macht es möglich, verschlüsselte Daten auf allen Kommunikationsstrecken zu übertragen – erhebliche Einbußen in der Leistung sind dabei nicht festzustellen.

■ 2.3.2 Maskerade

Durch Maskerade kann erreicht werden, dass der Internetnutzer glaubt, er würde mit einem authentischen oder seriösen Partner kommunizieren.



Beispielsweise kann es Angreifern im Internet gelingen, eine Webseite als authentisch vorzugeben, um somit in Besitz von bestimmten Kundeninformationen zu gelangen. Denkbar ist auch, dass ein Kunde veranlasst wird, eine Zahlung für Waren zu initiieren, die er nur scheinbar bestellt hat. Diese Angriffe basieren auch auf der Leicht- und Gutgläubigkeit von Nutzern im Internet.

Möglich ist auch, dass nur einzelne Komponenten innerhalb eines Web-Auftritts verändert werden. Der Kunde befindet sich dann zwar beim richtigen Anbieter, die Inhalte der Anbieter-Webseite sind aber so modifiziert, dass Kundeninformationen und Geldtransaktionen umgeleitet werden können. Diese Maskerade ist aufwendiger, da sie voraussetzt, dass der Angreifer in das Websystem des Anbieters eindringen kann.

■ 2.3.3 Wiedereinspielen alter Nachrichten

Ein Angreifer kann authentische Nachrichten mithören und speichern und diese zu einem späteren Zeitpunkt erneut versenden. In Zahlungsverkehrssystemen beispielsweise kann dieser Angriff dazu dienen, eine bereits getätigte Zahlung erneut auszulösen.

■ 2.3.4 Veränderung von Nachrichten

Eine ungeschützt übertragene Nachricht kann von einem Angreifer so verändert werden, dass beispielsweise Zahlungen umgelenkt oder Verträge gefälscht werden. Um solche Angriffe zu vermeiden bzw. abzuschmettern, helfen nur kryptographische Verfahren, also Verschlüsselungsverfahren oder digitale Signaturen, mit denen die Integrität und Authentizität von Daten überprüft werden können.

■ 2.3.5 Übertragungsfehler

In einem technischen System muss stets damit gerechnet werden, dass Übertragungsfehler aus unterschiedlichen Gründen auftreten können. Solche Fehler können teilweise sehr schwer detektierbar sein, wenn nicht fehler-erkennende Codes bei der Übertragung verwendet werden. Sind Nachrichten mit einer zusätzlichen elektronischen Signatur ausgestattet, kann kontrolliert werden, ob ihr Inhalt verändert wurde. Ist dies der Fall, kann die Original-Nachricht erneut angefordert werden.

■ 2.3.6 Nichtanerkennung von Nachrichten

Werden bei der Übertragung von Informationen keine Schutzmaßnahmen getroffen, kann dies vor allem im Geschäftsverkehr zu Schäden führen. Beispielsweise kann ein Sender behaupten, er habe eine Nachricht nie gesendet oder der Empfänger kann erklären, dass er eine Nachricht nie erhalten habe. Das führt zu Problemen, wenn beispielsweise Waren von hohem Wert geliefert werden, deren Bestellung aber bestritten wird. Oder wenn eine Transaktion von Geld abgestritten wird.

■ 2.3.7 Fehlerhafte und falsche Weiterleitung von Nachrichten

Technische Defekte oder gezielte Angriffe können dazu beitragen, dass Nachrichten und Daten an Unbefugte gelangen. Im Internet werden Routing-Tabellen benutzt, damit die Netzwerkknoten den Datenfluss lenken können. Sind diese Routing-Tabellen fehlerhaft, können Personen Daten erhalten und lesen, die nicht für sie bestimmt sind. Davor können sich Nutzer nur schützen, indem sie Verschlüsselungstechnologien einsetzen.

■ 2.3.8 Physikalische Bedrohungen der Kommunikationsbeziehungen

Um ein Netzwerk aufzubauen, verwenden Unternehmen oft den Ethernet-Standard. Das birgt Probleme. Denn das Ethernet-Netzwerk besteht aus einer Anzahl von Netzknoten (Rechnern), die untereinander in einer Baumstruktur verbunden sind. Versendet ein Rechner Informationen, so werden sie grundsätzlich an alle im Netzwerk vorhandenen Rechneradressen geschickt. Nur die adressierten Empfänger sind jedoch in der Lage, sich die für sie bestimmten Informationen herauszugreifen. Der Versand im gesamte Ethernet-Netzwerk führt aber dazu, dass der Datenverkehr an jedem Netzknoten abgehört werden kann. Das gilt auch für Knoten, die zusätzlich in das Netzwerk eingebracht werden.

Begünstigt wird das Abhören dadurch, dass keine zentrale Instanz vorhanden ist, die kontrolliert, ob Netzknoten existieren. Auch passive Knoten können nicht erkannt werden. Erst wenn ein Knoten selber aktiv Daten im Netzwerk versendet, kann er im Netzwerk identifiziert werden. Problematisch ist auch, dass fremde Rechner zwar als abgeschaltete, aber zulässige Knoten des Netzwerkes getarnt werden können. Auch in diesem Fall ist es nicht möglich, sie zu erkennen.

Um diese Probleme zu mildern, lassen sich Teilnetze aufbauen, die durch Router und Switches voneinander getrennt werden. Das führt dazu, dass nicht jede Nachricht in das gesamte Netzwerk geschickt wird. In der Regel werden die Nachrichten dann nur innerhalb der Teilnetze versendet und somit wird zumindest die Datenmenge, die abgehört werden kann, kleiner. Die Grenzen des Teilnetzwerks werden nur dann verlassen, wenn sich Sender und Empfänger in unterschiedlichen Teilnetzen befinden.

Es lassen sich einfache physische Maßnahmen ergreifen, um das Abhören schwieriger zu gestalten. Beispielsweise sollten Datenleitungen in Unternehmen so verlegt werden, dass sichtbar wird, wenn Unbefugte auf sie zugreifen. Auch sollten Netzanschlussdosen, die nicht benutzt werden, versiegelt bzw. tot geschaltet werden.

■ 2.3.9 Systematische Planung von Kommunikationsverbindungen

Die Netzwerke und ihre Topologien sind in Unternehmen meist das Produkt von stetiger Migration. Das führt oft dazu, dass bei den Teilnetzen und Zugängen über LAN, Remote Access usw. „Wildwuchs“ herrscht. Eine nicht durchdachte Netzwerktopologie erschwert die effektive Absicherung und macht es Angreifern von außen und innen leicht, ins Netzwerk einzudringen. Um zu gewährleisten, dass das Netzwerk vernünftig geschützt ist, muss ein Netzwerkkonzept entwickelt und umgesetzt werden.

Sinnvoll ist dabei den Soll-Zustand zu definieren. Anschließend muss der Ist-Zustand festgestellt und mit dem Soll verglichen werden. Im Ergebnis werden Handlungsnotwendigkeiten gut sichtbar.

Besonders wichtig bei einem Sicherheitskonzept für Netzwerke ist zu definieren, welche Kommunikationsbeziehungen erlaubt, eingeschränkt erlaubt oder nicht erlaubt sind.

Art der Kommunikationsbeziehung	Bedingungen
Erlaubt	<ul style="list-style-type: none"> ■ Hohes Sicherheitsniveau beim Partner ist vorhanden. ■ Vertrauenswürdigkeit der Netze ist gegeben. ■ Kommunikation ist unumgänglich und zu jeder Zeit erforderlich.
Eingeschränkt erlaubt	<ul style="list-style-type: none"> ■ Kommunikation ist nur zu bestimmten Zeiten erforderlich. ■ Kommunikation muss von innen nach außen aufgebaut werden. ■ Nutzung nur spezieller, kontrollierbarer Ports zulässig. ■ Daten können weitestgehend kontrolliert werden.
Nicht erlaubt	<ul style="list-style-type: none"> ■ Keine Vertrauenswürdigkeit der Netze gegeben. ■ Kommunikation ist auf diesem Weg nicht erforderlich. ■ Schadwirkungen sind nicht auszuschließen. ■ Kontrolle der Daten ist kaum möglich. ■ Wahllose Nutzung von Ports. ■ Keine zeitliche Vorhersagbarkeit der Kommunikation. ■ Kommunikation von außen nach innen.

Als Grundregel für die Einteilung gilt: Es sind nur so viele Rechte zu vergeben, wie es die Anwendung unbedingt erfordert. Aufgrund sich ständig ändernder Rahmenbedingungen kann die Einteilung schon nach kurzer Zeit wieder änderungsbedürftig sein. Daher sollten die Kommunikationsbeziehungen in regelmäßigen Abständen überprüft werden.

■ 3 Sicherheitsmanagement und Organisation

Der Umgang mit Computersystemen und immateriellen Daten ist noch nicht für alle Menschen Alltag. Demzufolge ist auch ihr Bewusstsein für die Risiken und Gefahren dieser neuen Welt noch weniger ausgeprägt als bei Gütern der materiellen Welt. Darauf müssen sich insbesondere die Unternehmen einstellen. Zwar lassen sich viele Bedrohungen dadurch eingrenzen, dass technische Verfahren genutzt werden. Aber gegen menschliches Versagen der Mitarbeiter können Unternehmen häufig nicht viel ausrichten.

Angreifer wenden oft psychologische Tricks an, um an das Wissen ihrer Opfer zu gelangen. Das erbeutete Wissen lässt sich in der Regel leicht für Angriffe auf technischer Ebene nutzen. Viele Mitarbeiter sind sich nicht bewusst, welche Informationen sie weitergeben dürfen oder wie wichtig es ist, ihre Informationen und Zugänge zu schützen. Die „erfolgreichsten“ Angriffe auf Unternehmen wurden dadurch möglich, dass die Angreifer Lücken in organisatorischen Regeln ausnutzen konnten. So geben Mitarbeiter ihre Passwörter oftmals an Kollegen weiter. Auch Netzwerkadministratoren erhalten die Passwörter oft von unbedarften Kollegen. Das kann zu einem Problem werden, wenn sich der Administrator beispielsweise von der Konkurrenz abwerben lässt.

Auch die Bequemlichkeit von Nutzern lässt sich für Attacken ausnutzen. Mitarbeiter umgehen manchmal ganz bewusst Sicherheitsfunktionen, um schneller arbeiten zu können. Bequemlichkeit ist häufig auch der Grund, warum unterschiedliche Systeme nur mit einem Passwort geschützt werden. Die organisatorische Sicherheit ist eine ganz wesentliche Komponente eines Sicherheitskonzepts für Unternehmen. Einige wichtige Punkte werden hier aufgeführt:

Verantwortlichkeiten und Ansprechpartner	<ul style="list-style-type: none">■ Trennung von Funktionen■ Verantwortlichkeiten und Zuständigkeiten regeln
Erlass von Richtlinien für den Umgang mit Software und Systemen	<ul style="list-style-type: none">■ Zentrale Beschaffung■ Verbot des Einbringens privater Systeme und Software■ Versiegelung von offenen Schnittstellen und Gehäusen■ Pflege- und Wartungsintervalle■ Vernichtung von Daten und Systemen■ Festlegung von Kommunikationsbeziehungen■ Einsatz von präventiven Systemen (Virens Scanner, Firewalls und Intrusion-Detection-Systemen)■ Erstellung von EMV-Schutzkonzepten (Abstrahlung)■ Erarbeitung von Backup-, Notfall-, Katastrophenschutz- und Wiederanlauf-Konzepten
Dokumentation	<ul style="list-style-type: none">■ Vernetzungs- und Systempläne■ Zugänge■ Kennzeichnung von Datenträgern■ Bestandslisten für Hard- und Software
Revisions- und Kontrollmechanismen	<ul style="list-style-type: none">■ Einführung von Zugangs- und Zugriffsregelungen■ Regelmäßige Kontrollen des Verhaltens der Mitarbeiter■ Protokollierung sicherheitsrelevanter Ereignisse

■ 3.1 Zugang zu Informationen und Systemen

Um zu regeln, welche Personen im Unternehmen Zugang zu welchen Ressourcen erhalten, sollte folgender Grundsatz gelten: „Sowenig wie möglich, soviel wie nötig“. Es muss exakt definiert werden, welche Mitarbeiter auf welche Ressourcen Zugriff bekommen. Nicht befugte Personen müssen explizit ausgeschlossen werden. Bei besonders sensitiven Bereichen kann es auch sinnvoll sein das „Mehr-Augen-Prinzip“ einzusetzen.

Beschränkte Zugriffe können durch bauliche Maßnahmen realisiert werden. So sollte zum Beispiel ein Datenserver nur in einem speziell gesicherten Schrank oder Serverraum aufgestellt und der Zugriff nur befugten Personen ermöglicht werden.

Das Risiko, dass Unbefugte Zugang zu Räumen oder Zugriff auf Server erhalten, kann durch präventive und durch überwachende Maßnahmen verringert werden. Überwachungssysteme können sowohl Geschlossenheit und Verriegelung kontrollieren als auch den Zutritt oder Zugriff für autorisierte Benutzer freigeben. Darüber hinaus können andere physikalische Parameter überwacht werden, die ebenfalls bedrohend auf unternehmenskritische Datenverarbeitungsprozesse wirken können. Dazu zählen z.B. Übertemperaturen (vorbeugender Brandschutz), Luftfeuchte (Schutz elektronischer Geräte/Speichermedien) oder elektrische Spannung (gerade an dislozierten Knotenpunkten mit lokaler USV).

Die Melde- und Alarmierungsmöglichkeiten der Überwachungssysteme sollten sowohl die Kanäle und Verfahren der Netzwerktechnik (TCP/IP mit HTTP, SNMP) nutzen als auch unabhängig vom Netzwerk bestehen.

Durch den Wegfall großer Rechenzentren und der Verlagerung der Aufgaben auf Client-Server-Systeme ist eine bauliche Absicherung der Arbeitsplatzrechner meist nur beschränkt möglich. Deswegen sind Sicherungsmaßnahmen durch Passwörter und Chipkarten an den Arbeitsplätzen besonders bedeutsam.

Häufig stellen Faxgeräte Fundgruben für Wissen dar. Eingehende Faxe liegen solange im Ausgabe-fach, bis die zuständige Person das Dokument entnimmt. Bis dahin können sich aber auch unbefugte Personen Zugriff auf dieses Dokument verschaffen und es kopieren oder vernichten. Gleiches gilt für Dokumente, die gefaxt und am Gerät vergessen wurden. Werden unternehmensrelevante Informationen per Faxgerät übertragen, muss sichergestellt sein, dass nur ein befugter Personenkreis Zugriff auf das Faxgerät hat.

■ 3.2 Trennung von Funktionen

Im Unternehmen muss eine klare räumliche und organisatorische Funktionstrennung erfolgen. Die verschiedenen Abteilungen eines Unternehmens dürfen nicht gegenseitigen Zugriff auf Informationen und Systeme haben, wenn es nicht zwingend erforderlich ist. Nur so kann verhindert werden, dass zusammengefügte Bruchstücke von Unternehmenswissen relevante Informationen für Wettbewerber ergeben.

In diesem Sinne sollten Angestellte einer DV-Abteilung nicht auch für inhaltliche Arbeiten in der Wertschöpfungskette verantwortlich sein.

■ 3.3 Zentrale IT-Abteilung

Die Mitarbeiter der IT-Abteilung gehören zu den wichtigsten Personen im Unternehmen. Durch ihre Arbeit können sie in den Besitz von Wissen gelangen, welches für Wettbewerber interessant sein könnte. Auch könnten sie – meist ohne viel Aufwand – Systeme manipulieren oder schädigen. Daher sind die Mitarbeiter von IT-Abteilungen häufig das Ziel von Angreifern. Deshalb muss dieser Mitarbeiterkreis besonders sorgfältig ausgewählt werden. Sicherheitsrelevante Tätigkeiten dieser Mitarbeiter müssen protokolliert und kontrolliert werden. Nur so können Anhaltspunkte für ein mögliches Fehlverhalten entdeckt werden.

In vielen Fällen können „Mehr-Augen-Prinzipien“ helfen, den Missbrauch von speziellen Administrator-Rechten bereits im Ansatz zu vermeiden. Eine Möglichkeit, das Missbrauchsrisiko zu minimieren, ist beispielsweise, dass neue Benutzer nur dann Zugriffs-Rechte erhalten können, wenn zwei Mitarbeiter der IT-Abteilung den Vorgang auslösen.

Durch die Trennung von IT-Abteilung und operativen Abteilungen kann die Gefahr minimiert werden, dass bestimmte Informationen missbraucht werden. Diese Regelung muss auch durch das IT-System unterstützt werden.

Die IT-Abteilung muss sowohl baulich als auch IT-seitig gegen den Zugriff durch unbefugte Personen gesichert werden. Dazu müssen Sicherheitszonen gebildet und die Zugänge überwacht werden. Reinigungspersonal sollte nur unter Aufsicht Zugang zu den Räumen erhalten.

Baulich muss die IT-Abteilung besonders gegen Umwelteinflüsse und gegen Abhörmöglichkeiten abgesichert werden. Für sensitive Bereiche ist Redundanz zu schaffen. Selbstverständlich muss auch an eine Notstromversorgung gedacht werden, damit die Systeme auch bei einer Stromunterbrechung arbeitsfähig bleiben.

■ 3.4 Computer Notfall Team (CERT)

Zum organisatorischen Teil eines Sicherheitskonzepts gehört auch, ein Notfallteam aufzubauen. Tritt ein Sicherheitsvorfall ein, hat das Notfallteam sowohl präventive als auch reaktive Aufgaben. In der Regel verfügen nur große Unternehmen mit entsprechend großen Netzwerken über ein so genanntes Computer Notfall Team oder „Computer Emergency Response Team“ (CERT).

Ein CERT analysiert Schwachstellen der Unternehmens-Systeme und -Software und erarbeitet Maßnahmen, die die Sicherheitsrisiken minimieren sollen. Präventiv simuliert das Team Notfallsituationen, damit im Krisenfall routiniert eingegriffen werden kann. Außerdem sollte das Team die Auswirkungen neuer Software oder verdächtiger E-Mail Anhänge auf Testsystemen analysieren, bevor sie auf dem Produktivsystem installiert werden. Es erarbeitet Katastrophen- und Wiederanlaufpläne, die detaillierte Maßnahmen, Verhaltensregeln und Telefonverzeichnisse von verantwortlichen Personen enthalten, um das Unternehmen auf Notfallsituationen und Zwischenfälle vorzubereiten. Neben mehreren Unternehmens- und universitären CERTs existieren in Deutschland zwei CERTs, die einen eher öffentlichen Charakter haben: Das BSI organisiert ein CERT für die Bundesverwaltung (www.bsi.bund.de/certbund/index.htm) und der DFN-Verein unterhält ein CERT für den Wissenschaftsbetrieb (www.cert.dfn.de). Als Reaktion auf die Anschläge am 11. September 2001 und um vereint gestärkt auf mögliche Cyber-Attacks reagieren zu können, schlossen sich im August 2002 fünf der deutschen CERTs aus den Bereichen Wirtschaft und Forschung mit dem CERT der Bundesverwaltung zum „CERT Verbund“ zusammen.

Neu in der Liste der CERTs ist das von BITKOM gegründete Mcert (www.mcert.de), das speziell auf die Bedürfnisse von kleinen und mittleren Unternehmen ausgerichtet ist. Mcert unterstützt diese mit verlässlichen Sicherheitsinformationen und verständlichen Handlungsempfehlungen. In Form eines Abo-Dienstes erhalten Kunden wichtige Sicherheitsinformationen zeitnah per E-Mail. Dazu zählen u. a. Warnmeldungen zu Viren und Hinweise auf Sicherheitslücken in IT-Systemen. Aufgrund eines individuell erstellten IT-Profiles wird sichergestellt, dass die Unternehmen nur Meldungen erhalten, die ihr eigenes System betreffen.

Weltweit haben sich die CERTs schon 1992 zum „Forum of Incidence Response and Security Teams“ (FIRST; www.first.org) zusammengeschlossen, um vertraulich und international Sicherheitsinformationen und Empfehlungen unter den Mitgliedern auszutauschen. So ist es möglich, bei akuten Angriffen und Virenattacken im Internet oder bei Sicherheitslücken von Systemen und Software zeitnah Informationen, Ratschläge und Empfehlungen für Gegenmaßnahmen zu erhalten.

Relevante Informationen über Sicherheitslücken sowie konkrete Maßnahmenempfehlungen für die Absicherung von IT-Systemen werden in großem Umfang auch im Internet frei zugänglich veröffentlicht.

Informationsquellen über Sicherheitslücken im Internet:

- www.securityfocus.com
- cert.uni-stuttgart.de
- www.cert.dfn.de
- www.bsi.de
- www.securitysearch.net
- www.mcert.de

■ 3.5 Anforderungen an den Mitarbeiter

Das Personal eines Unternehmens ist immer wieder Angriffsziel für „soziale Attacken“. Dabei werden menschliche Schwächen für Angriff auf die Systeme ausgenutzt. Daher kommt der Personalauswahl eine ebenso hohe Bedeutung zu wie der Schulung und Kontrolle der Mitarbeiter. Der gewählte Ansatz sollte auf keinen Fall repressiv sein, jedoch muss sich das Unternehmen auch von der Zuverlässigkeit und Treue des Mitarbeiters überzeugen, wenn dieser Zugriff auf sensitive Informationen und Systeme hat. Gemäß dem Sicherheits- und Schutzklassenkonzept können dabei unterschiedlich hohe Anforderungen an den Mitarbeiter gestellt werden.

Bereits bei der Einstellung von Mitarbeitern für besonders sensible Bereiche sollte der Werdegang zumindest der letzten Jahre eine Rolle spielen. Ungewöhnliches Verhalten von Mitarbeitern sollte stets zur Vorsicht mahnen. Verstöße gegen Sicherheitsbestimmungen sollten protokolliert werden, um bei Wiederholungen notwendige Konsequenzen ziehen zu können. Hierbei sind die arbeits- und datenschutzrechtlichen Vorgaben zu berücksichtigen und getroffene Maßnahmen durch entsprechende Mitarbeiterinformation bzw. Betriebsvereinbarungen abzusichern.

■ 3.5.1 Verpflichtungserklärungen

Das Sicherheitsrisiko kann in vielen Bereichen minimiert werden, wenn Mitarbeiter über die Risiken ihres Handelns und deren Auswirkungen für das Unternehmen aufgeklärt und geschult sind. Hilfreich sind schlanke Handlungsanweisungen und die Verpflichtung der Mitarbeiter, diese auch einzuhalten. So können den Mitarbeitern bei Beginn ihrer Tätigkeit Verpflichtungserklärungen zum Datenzugriff auf das Unternehmensnetz vorgelegt werden, in der die Art des Zugriffs und die Pflichten für den Mitarbeiter genau geregelt sind. Auch können die Mitarbeiter verpflichtet werden, Software des Unternehmens nur in bestimmter Form zu nutzen. Schließlich können noch Regeln im Umgang mit dem Internet erlassen werden.

Vereinbarung zum Datenzugriff:

- Beschreibung des Gegenstands der Verpflichtung und des Gültigkeitsbereichs.
- Regelung der erlaubten Art des Zugriffs.
- Hinweis auf Protokollierung aller Aktionen und stichprobenartige Kontrolle.
- Vergabe bestimmter Berechtigungen (Rechte).
- Definition bestimmter Pflichten.
- Nur Nutzung der zulässigen Daten und Systeme.
- Verbot des Zugriffs auf andere Daten und Systeme.
- Verbot der eigenmächtigen Änderung von Zugriffsrechten.
- Verpflichtung zur Ergreifung aller möglichen Maßnahmen zur Vertraulichkeitssicherung.
- Verbot der Weitergabe von Daten und Zugriffsdaten an Dritte.
- Definition der Nutzung von Remote-Access-Zugängen oder VPN.
- Nutzung der Daten ausschließlich zum Zwecke der Aufgabenerfüllung.
- Verbot, Kopien von Daten und Programmen anzulegen.
- Hinweis auf Schadenersatzforderungen bei Nicht-Einhaltung der Vereinbarung.
- Hinweis auf das Bundesdatenschutzgesetz.

Software-Verpflichtungserklärung:

- Hinweis, dass Urheberrechte und gewerbliche Schutzrechte betrieblich genutzter Software einzuhalten sind (keine illegalen Kopien einer Software).
- Hinweis, dass Vergehen gegen Lizenzbestimmungen zivil- und strafprozesslich verfolgt und eventuell entstehende Regressansprüche an den Mitarbeiter weitergegeben werden.
- Hinweis, dass illegales Kopieren von Software, egal ob für private oder berufliche Zwecke, die Kündigung des Arbeitsvertrages zur Folge haben kann.
- Klare Bestimmungen zur Nutzung der eingesetzten Software.
- Verpflichtung, dass die zuständige Stelle sofort informiert werden muss, wenn der Verdacht besteht, dass im Unternehmen illegale Kopien eingesetzt werden.
- Verbot der Nutzung privat beschaffter Programme auf Systemen des Unternehmens
- Genehmigungspflicht für Upload/Download von Software/ Daten über das Internet.
- Verpflichtung zur Nutzung von Anti-Virensoftware und Mitwirkung bei der Bekämpfung von Viren und Spyware (unverzügliche Information der zuständigen Stelle bei Verdacht auf Virenbefall).

Benutzungsrichtlinien

Der Umgang mit Internet-Diensten sollte klar geregelt sein. Dazu können Benutzungsrichtlinien ausgegeben werden, die mindestens die im Folgenden aufgeführten Punkte enthalten sollten:

Allgemeines	<ul style="list-style-type: none">■ Beachtung von IT-Sicherheitsvorschriften des Unternehmens.■ Hinweise zum Umgang mit und Schutz von klassifizierten Daten.■ Hinweis auf Bundesdatenschutzgesetz.■ Verbot der Umgehung von Regeln.■ Verfolgbarkeit festlegen.■ Recht auf Überwachung durch Geschäftsführung oder zuständige Stelle.
Nutzung des Internet	<ul style="list-style-type: none">■ Private Nutzung erlauben oder verbieten.■ Erlaubte Dienste und Seiten festlegen.■ Sicherheitsvorkehrungen (Cookies, Java Applets, Javaskript).■ Downloads erlauben oder verbieten.■ Hinweis auf Urheberrechte oder gewerblichen Rechtsschutz.
Nutzung von E-Mail	<ul style="list-style-type: none">■ Private Nutzung erlauben oder verbieten.■ Format, Disclaimer und Aussehen der E-Mail festlegen.■ Regeln für Spam- und Junk-Mail.■ Hinweis auf spezielle Datenschutzregelungen.■ Regeln für Anwendung von Verschlüsselungs- und Signaturprogrammen.

Hinweis: Eine gut formulierte Benutzungsrichtlinie für den Umgang mit dem Internet findet man beim Bayerischen Landesbeauftragten für den Datenschutz unter: www.datenschutz-bayern.de/-technik/-orient/-ibenrili.pdf.

Darüber hinaus sind alle Mitarbeiter auf ihre Verpflichtungen im Umgang mit personenbezogenen Daten nach dem Bundesdatenschutzgesetz (www.datenschutz.de/-recht/-gesetze/) hinzuweisen.

■ 4 Sicherheitstechnologien

■ 4.1 Verschlüsselungsverfahren

Verschlüsselungsverfahren werden angewendet, um vertrauliche Daten vor dem unberechtigten Zugriff zu schützen. Dies kann direkt durch eine Verschlüsselung erfolgen oder durch eine andere „Manipulation“ der Daten, die den eigentlichen Inhalt unkenntlich macht, also durch indirekte Verschlüsselungsverfahren.

Schon Julius Caesar hat Nachrichten in einfacher Weise verschlüsselt, indem er alle Buchstaben um 3 Plätze im Alphabet verschoben hat. Auch typische Office-Programme können den Inhalt eines Dokumentes verschlüsseln und den Zugriff davon abhängig machen, ob das Kennwort richtig ist. Allerdings bieten beide Verfahren keinen echten Schutz. Bei Caesars Methode leuchtet das sofort ein, weil sie schnell erkennbar und zu knacken ist. Und auch für den zweiten Fall finden sich im Internet nach kurzer Recherche Programme, die es auch Laien ermöglichen, Informationen zu entschlüsseln. Hier greift man besser auf Programme zurück, die eine starke Verschlüsselung von Dateien garantieren.

In ungeschützten Netzwerken, z.B. dem Internet, kommt der Verschlüsselung eine noch wesentlich höhere Bedeutung zu – ohne sie ist nämlich die Sicherheit der Internet-Dienste nicht zu erreichen. Bei geschäftlichen Transaktionen im Internet müssen oft vertrauliche Daten ausgetauscht werden, z.B. Zahlungsinformationen. Um das Internet als kommerzielle Plattform zu nutzen, sind neben der Vertraulichkeit auch die Integrität der übermittelten Daten und die Authentizität des Geschäftspartners sicherzustellen. Alle drei Grundaspekte der Sicherheit bei Transaktionen im Internet können durch Kryptoverfahren erfüllt werden. Gesetze – wie z.B. das Signaturgesetz – juristische Regeln und kaufmännische Vereinbarungen sorgen dann dafür, dass die elektronischen Geschäfte verbindlich und rechtsgültig sind.

Verschlüsseln oder Chiffrieren bedeutet letztlich, Daten von einer lesbaren Form mit einem mathematischen Algorithmus in eine nicht lesbare Form zu bringen. Ohne den passenden Schlüssel kommt man nicht mehr an die Daten heran. Damit einfaches Ausprobieren von allen möglichen Schlüsseln – das lässt sich automatisch per Computerprogramm erledigen – nicht oder zumindest erst nach sehr langer Zeit zum Erfolg führt, ist auf eine hinreichende Schlüssellänge, gemessen in Bit, zu achten. Denn dadurch erhöht sich die Anzahl der möglichen Schlüssel und damit die Zeit, die ein Dateneinbrecher braucht, um alle Schlüssel durchzuprobieren („Brute Force Attack“). Ein 128-Bit langer Schlüssel ist derzeit der Standard für hohe Sicherheit (starke Verschlüsselung).

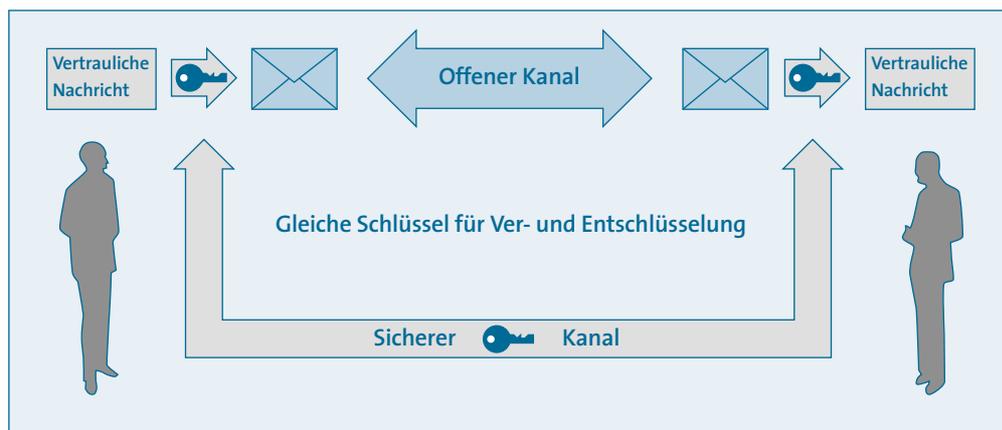
Grundsätzlich unterscheidet man zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren.

■ 4.1.1 Symmetrische Verschlüsselungsverfahren

Bei symmetrischen Verfahren wird derselbe Schlüssel zum Ver- und zum Entschlüsseln der Daten benutzt (siehe Abbildung). Daher sind diese Verschlüsselungsverfahren sehr schnell und werden meist auch in Hardware realisiert.

Bekannte Verfahren sind beispielsweise der DES (Data Encryption Standard) sowie dessen Nachfolger der AES (Advanced Encryption Standard) und der IDEA (International Data Encryption Standard). Die Kommunikationspartner müssen den Schlüssel vor Dritten geheim halten, weil nur ein Schlüssel existiert. Bei 10 Partnern, die alle miteinander kommunizieren wollen, sind daher bereits 45 verschiedene, geheime Schlüssel nötig. Wenn aber 1.000 Kommunikationsteilnehmer vertraulich miteinander kommunizieren wollen, sind schon 499.500 verschiedene Schlüssel nötig, die auf sicherem Wege ausgetauscht und sicher aufbewahrt werden müssen.

■ Symmetrische Verschlüsselungsverfahren



■ 4.1.2 Asymmetrische Verschlüsselungsverfahren

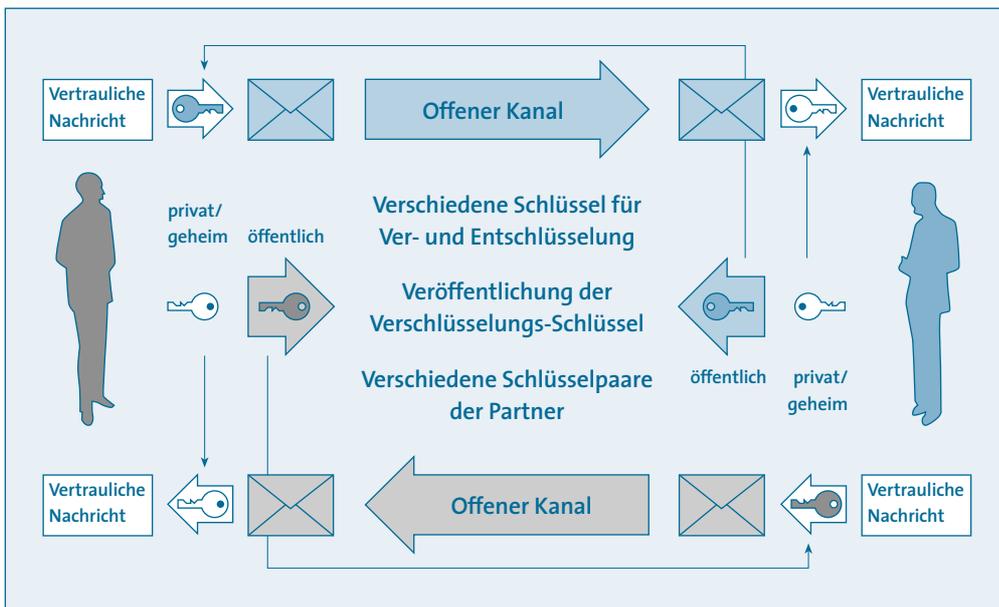
Bei asymmetrischen Verschlüsselungsverfahren wird ein Paar korrespondierender Schlüssel verwendet. Dieses Paar besteht aus einem privaten (geheimen) und einem öffentlichen Schlüssel. Aus dem einen Schlüssel lässt sich der andere Schlüssel nicht berechnen. Eine Nachricht, die mit einem Schlüssel chiffriert wird, kann nur noch mit dem korrespondierenden Schlüssel dechiffriert werden. Gelangt kein anderer in Kenntnis des geheimen Schlüssels, kann tatsächlich nur der Besitzer des geheimen Schlüssels die Nachricht im Klartext wieder darstellen.

Bei zehn Nutzern müssen bei der Verwendung von asymmetrischen Verfahren somit nur noch 20 Schlüssel generiert werden, was gegenüber symmetrischen Verfahren vorteilhafter ist.

Leider sind die asymmetrischen Verfahren deutlich langsamer als entsprechende symmetrische Verfahren. Daher werden in der Praxis oft die symmetrischen und die asymmetrischen Verfahren zu hybriden Verfahren kombiniert, um jeweils beide Vorteile der Verfahren, nämlich die hohe Verarbeitungsgeschwindigkeit von symmetrischen Verfahren und die leichte Schlüsselverteilung der asymmetrischen Verfahren, zu nutzen. So wird beim Internet-Banking meist ein geheimer 128-Bit langer IDEA-Schlüssel zunächst mit einer 1.024-Bit-RSA-Verschlüsselung übertragen und danach die Sitzung symmetrisch mit IDEA verschlüsselt.

Die nächste Abbildung beschreibt den Weg, wie mit einem asymmetrischen Verschlüsselungsverfahren eine Nachricht vertraulich über einen offenen Kanal übertragen werden kann. Dazu nimmt der Sender den öffentlichen Schlüssel des Empfängers und verschlüsselt die Daten. Danach sendet er die Daten dem Empfänger zu. Da nur der zum öffentlichen Schlüssel korrespondierende private Schlüssel die Entschlüsselung erlaubt, kann nur der Empfänger die Daten wieder entschlüsseln.

■ Asymmetrische Verschlüsselungsverfahren



■ 4.1.3 Indirekte Verschlüsselungsverfahren

Neben den direkten Verschlüsselungsverfahren, die Daten in eine nicht lesbare Form überführen, gibt es außerdem noch die so genannten indirekten Verschlüsselungsverfahren, die zwar keinen Geheimtext erzeugen, aber die Daten doch so manipulieren, dass der Klartext nicht erkannt wird. Wir wollen noch kurz auf drei derartige indirekte Chiffrierverfahren eingehen.

Steganographie

Als Steganografie wird ein Verfahren bezeichnet, bei dem die wichtigen Informationen in anderen, unwichtigen Informationen versteckt sind. Bei Texten werden z.B. wichtige Buchstaben kaum sichtbar unterpunktirt, oder Schriftzugunterbrechungen verweisen auf wichtige Buchstaben. Steganografische Verfahren erhalten im Zusammenhang mit Bildern jetzt wieder eine erhöhte Aufmerksamkeit. Man kann nämlich bestimmte Bildinformationen durch wichtige Informationen ergänzen. Dem Bild sieht man das nicht an; wer aber über den passenden Schlüssel verfügt, kann den Klartext leicht auslesen.

Frequenzsprungverfahren

Die Frequenzsprungverfahren wurden ursprünglich für den militärischen Funkverkehr zur Abwehr von Störsendern entwickelt. Die Übertragung der Information erfolgt dabei nicht über einen festen Funkkanal sondern über eine große Anzahl von Kanälen, die im Abstand von Bruchteilen von Sekunden nach einem geheim gehaltenen Schlüssel angesprungen werden. Kennt man das Vorgehen nicht, so kommt das Verfahren in seiner Wirkung einer Verschlüsselung gleich.

Chaffingverfahren

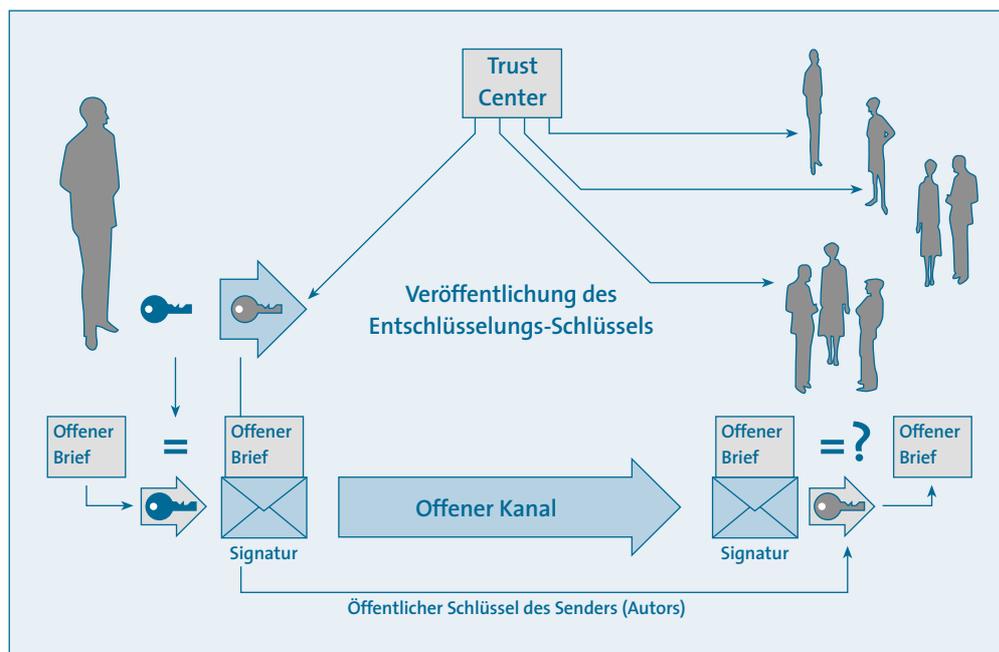
Chaffingverfahren (chaffing: englisch für häckseln) werden bei der paketweisen Übertragung von Informationen in einem Bitstrom eingesetzt. Neben den Paketen, die die wichtigen Information enthalten, wird dabei eine Vielzahl von weiteren Paketen mit Zufallsbits versendet. Nur der Eingeweihte erkennt an Hand einer Kenngruppe die echten Pakete.

■ 4.2 Digitale Signaturen

Digitale Signaturen stellen in der digitalen Welt sicher, dass Daten nicht unbefugt verändert werden können. Sie beweisen, dass die Daten authentisch und integer und somit verbindlich sind. Dies hat weitreichende Konsequenzen. Da mittlerweile auf europäischer Ebene eine Signaturrechtlinie und in Deutschland ein Signaturgesetz existieren, können Verträge, die ansonsten der Schriftform bedürfen, digital angefertigt und mit einer qualifizierten elektronischen Signatur versehen werden. Diese Verträge sind, wenn die Bedingungen des Gesetzes eingehalten werden, genauso rechtskräftig, wie der entsprechende Vertrag auf einem Blatt Papier.

Um digitale Signaturen anzuwenden, benötigt der Nutzer einen öffentlichen und einen geheimen Schlüssel eines asymmetrischen Schlüsselpaars (siehe Abbildung). Der öffentliche Schlüssel muss den potenziellen Empfängern bekannt sein. Im Besitz des geheimen Schlüssels darf allerdings nur der Benutzer selber sein.

■ Digitale Signatur



Eine digitale Signatur wird erzeugt, indem zunächst die zu schützenden Daten mit einer so genannten Hash-Funktion komprimiert werden. Diese Hash-Funktion ist eine Einweg-Funktion, d.h. sie ist nicht umkehrbar. Es kann also aus einem Funktion-Wert nicht der Eingabewert errechnet werden. Das bedeutet, dass aus einem Hash-Wert nicht die zu schützenden Daten ermittelt werden können.

Danach wird der geheime Schlüssel des Nutzers zur Verschlüsselung des Hashwertes verwendet. Das Ergebnis ist die digitale (elektronische) Signatur. Wird auf diese digitale Signatur der öffentliche Schlüssel angewendet, erhält man wiederum den vormals verschlüsselten Hashwert. Der Nutzer sendet nun dem Empfänger die Daten, also die Textdatei, und fügt die digitale Signatur hinzu. Der Empfänger kann nun mit dem öffentlich bekannten Schlüssel ebenfalls die digitale Signatur dechiffrieren und erhält den Hashwert. Wendet er nun die gleiche Hashfunktion auf die Textdatei an, erhält er einen weiteren Hashwert, der exakt der gleiche sein muss, wie der dechiffrierte. Ist dies nicht der Fall, entsprechen die gesendeten Daten nicht dem, was der Nutzer ursprünglich signiert und verschickt

hatte. Sind beide Hashwerte gleich, weiß der Empfänger, dass die Daten authentisch und integer sind. Handelt es sich bei den gesendeten Daten um einen Vertrag, wäre dieser verbindlich.

Digitale Signaturen können aber nur dann angewendet werden, wenn man sich tatsächlich sicher sein kann, dass die öffentlichen Schlüssel den betreffenden Nutzern zugeordnet sind und dass die verwendeten Schlüsselpaare immer Unikate sind. Ansonsten könnten digitale Signaturen gefälscht werden.

In Zeiten der globalen Kommunikation kann man öffentliche Schlüssel seinen wechselnden Kommunikationspartnern nur bekannt machen, indem eine dritte unabhängige Stelle dafür garantiert, dass das Schlüsselpaar einmalig und richtig zugeordnet ist. Diese Aufgabe haben Zertifizierungsstellen (Certification Authorities oder Trustcenter), die durch ein Zertifikat eine eindeutige Zuordnung zwischen einem öffentlichen Schlüssel und einer Person garantieren.

Will ein Nutzer eine digitale Signatur verwenden, so muss er sich zunächst bei einer Zertifizierungsstelle identifizieren lassen. Danach wird ein Schlüsselpaar von der Zertifizierungsstelle erzeugt, wovon der Nutzer den geheimen Schlüssel auf einem sicheren Medium verwahrt erhält und der öffentliche Schlüssel auf der Website der Zertifizierungsstelle veröffentlicht wird.

■ 4.3 Router und Paketfilter

Die anfallenden Datenströme in einem Netzwerk müssen gelenkt werden, damit sie das gewünschte Ziel erreichen. Dazu können Router (hoch spezialisierte Vermittlungsrechner) verwendet werden, die anhand der Empfängeradresse der gesendeten Daten bestimmen, in welchem Teilnetz sich der Empfänger befindet und die Daten nur an dieses weiterleiten. Dies ist die simpelste Möglichkeit, sein internes Netz nach außen hin abzuschirmen. Es ist allerdings auch die wenig effizienteste Methode. Wird auf dem Router zusätzlich noch ein Paketfilter installiert, kann mittels Vorgabe erlaubter und verbotener Ziel- und / oder Absender-Adressen der Datentransport weiter eingeschränkt werden. Ebenfalls kann auf logischer Ebene untersucht werden, ob erlaubte Protokolle benutzt werden. Der Paketfilter kontrolliert also zwischen zwei Netzen anhand der beiden Kriterien „Adresse“ und „Protokolltyp“, ob Daten von dem einen Netz in das andere gelangen dürfen und umgekehrt. Dazu werden entsprechende Regeln auf dem Paketfilter installiert.

Das Verbindungsprotokoll TCP/IP legt durch die Benutzung von Ports fest, welcher Dienst angesprochen werden soll. Soll beispielsweise E-Mail mittels des POP3-Protokolls benutzt werden, muss auf dem Paketfilter der dazu korrespondierende Port frei geschaltet sein. Für POP3 ist das der Port 110, der ungehindert über den Paketfilter gelangen darf. Tatsächlich gibt es weitere E-Mail-Dienste, die andere Ports benutzen. Hier eine kleine Auswahl der bekanntesten Protokolle:

Port Nummer	Protokoll	Abkürzung
109	Post Office Protocol - Version 2	Pop2
110	Post Office Protocol - Version 3	Pop3
995	pop3 protocol over TLS/SSL (was spop3)	Pop3s
143	Internet Message Access Protocol	imap
220	Interactive Mail Access Protocol v3	imap3
209	The Quick Mail Transfer Protocol	qmtf

Will man sicher gehen, dass z.B. ausschließlich POP3 benutzt werden kann, sind sämtliche anderen Ports zu sperren.

■ 4.4 Firewalls

In der realen Welt verhindern Brandschutzmauern (englisch: „Firewalls“) die Ausbreitung eines Feuer. Dieser Begriff wurde in der digitalen Welt für spezielle Sicherheitsrechnersysteme übernommen, da hier ähnliche Aufgaben existieren, wie die Abwehr von Angriffen (Feuer) aus einem unsicheren Netzwerk. Dabei wird eine Firewall zwischen einem unsicheren Netz, aus dem Angriffe befürchtet werden, und einem gesicherten Netz eingesetzt. Die Firewall geht in ihrer Funktionalität über die eines Paketfilters weit hinaus.

Die Hauptaufgabe der Firewall besteht darin, Zugriffsschutz (Access-Security) herzustellen. Oft rechnet man auch den zentralen Virenschutz (Bestandteil der Content-Security) zu den Leistungen eines Firewall-Systems. Access-Security bedeutet, die Zulässigkeit des Datenverkehrs von der Außenwelt (dem Internet) in das Unternehmensnetz und umgekehrt soweit wie möglich den Vorstellungen der eigenen Organisation anzupassen. Für diesen Zweck sollte zunächst eine Security Policy verabschiedet werden, die alle erlaubten Verbindungen zwischen dem Unternehmen und dem Internet festlegt. Eine Firewall wird meist so konfiguriert, dass sie zunächst alles blockiert und nur die in der Security Policy erlaubten Verbindungen zulässt. Sie bewirkt, dass die Sicherheitsmaßnahmen zentralisiert werden, denn sämtlicher Internet-Verkehr wird über sie abgewickelt.

Im Rahmen der Access-Security filtert das Firewall-System typischerweise die Internet-Pakete nach Absender- und Zieladresse sowie nach Anwendungstyp. So ist es möglich, die Nutzung besonders kritischer Internet-Anwendungen (wie z.B. Telnet) aus dem Internet heraus von vornherein zu unterbinden. Ein Firewall-Rechner kann tief in die Struktur von Datenpaketen hineinsehen und seine Entscheidungen vom Zustand vorangegangener Datenpakete abhängig machen. Im Rahmen eines

Firewall-Systeme werden oft auch noch Maßnahmen gegen das Address-Spoofing (Vortäuschen einer falschen Internet-Adresse) oder gegen den Systemausfall bei der Übermittlung übergroßer Datenpakete ergriffen.

Die Administration einer Firewall ist eine anspruchsvolle Tätigkeit. Die Regeln auf der Firewall müssen so gewählt werden, dass die benötigten Dienste und Applikationen verfügbar sind, aber andere unerwünschte Dienste gesperrt bleiben. Erschwert wird die Administration auch durch Randbedingungen der Art, dass Mitarbeiter durchaus unterschiedliche Berechtigungen haben können. Letztlich entstehen auch neue Dienste und Applikationen, die bislang unbenutzte Ports adressieren. Hier besteht also ein ständiger Überwachungs- und Änderungsbedarf. Bei der Administration der Firewall sollten kleinere Unternehmen auf jeden Fall die Hilfe eines spezialisierten Experten anfordern. Zu schnell sind sonst widersprüchliche Regeln angelegt oder Lücken nicht vollständig geschlossen. Die ständige Überwachung der Firewall ist eine Pflichtaufgabe für die IT-Abteilung. Viele Firewalls alarmieren den Administrator automatisch, wenn sich Angriffe auf die Firewall häufen oder Anfragen mit nicht erlaubten Diensten eingehen. Sodann muss der Verantwortliche zeitnah reagieren und den Angriff lokalisieren. Eventuell müssen auch weitere Gegenmaßnahmen geplant und umgesetzt werden. Solche Angriffe ereignen sich oft dann, wenn wenig Personal verfügbar ist, also am Abend oder am Wochenende. Wenig hilfreich ist, wenn die Firewall am Freitagabend meldet, dass eine Angriffsserie startet, der Administrator aber erst am Montagmorgen reagieren kann. Dann ist es übers Wochenende meistens schon zu einem erfolgreichen Angriff gekommen. Für die Überwachung der Firewall muss daher eine Rund-um-die-Uhr-Bereitschaft organisiert werden.

■ 4.5 Proxy-Server

Ein Proxy-Server ist in der Regel ein dem Unternehmensnetz vorgeschalteter Rechner, über den beispielsweise der Zugriff aus dem sicheren Netz ins Internet abgewickelt wird. Er kann aber auch als Software-Lösung realisiert sein. Jede Anfrage eines Nutzers an das Internet wird dabei an einen Proxy-Server (Stellvertreter) geleitet. Dieser sorgt dann stellvertretend für den Rechner des Nutzers, dass Daten aus dem Internet geholt und an den Empfänger im sicheren Unternehmensnetz weitergeleitet werden.

Der Einsatz eines Proxy-Servers bietet mehrere Vorteile. Bereits geholte Webseiten werden für eine gewisse Zeit aufbewahrt (im Cache) und bei erneuter Anforderung direkt aus dem Cache und nicht mehr aus dem angeschlossenen Netz (z.B. dem Internet) herunter geladen. Das entlastet erheblich den Datenverkehr. Ein richtig konfigurierter Proxy-Server nimmt nur Aufträge aus dem internen Netz entgegen und leitet nur die Antworten aus dem äußeren Netz (z.B. dem Internet) weiter. Von außen initiierte Aufträge bzw. Angriffe werden normalerweise nicht weitergeleitet. Weiterhin verbirgt der Proxy-Server auch die interne Netzstruktur, da das interne Netz nach außen nur unter der einen(!) Adresse des Proxy-Servers auftritt. Potenziellen Angreifern werden erheblich weniger Angriffspunkte geboten.

■ 4.6 Intrusion Detection Systeme

Auch die besten Firewall-Systeme bieten keinen hundertprozentigen Schutz. Sie können einmal versagen oder es können neue Lücken in diesen Systemen gefunden werden. Gelingt es einem Angreifer, in das interne Netz einzudringen, helfen so genannte „Intrusion Detection Systeme“ (IDS) dabei, ungewöhnliche Aktionen im internen Netz bzw. auf internen Rechnern festzustellen. Zwei Arten von

Systemen können unterschieden werden: Systeme, die auf einem Rechner oder einem Netzwerk basieren. Ein Rechner-basierendes IDS wirkt nur auf dem eingesetzten Rechner; es kontrolliert alle Aktivitäten dieses Rechners und kann somit die Ausführung unbekannter Programme (Viren) erkennen und verhindern. Ein Netzwerk-basierendes IDS analysiert den Datenverkehr im Netzwerk. Viele Hackerangriffe sind durch eine charakteristische Folge von Datenpaketen gekennzeichnet.

Kennzeichnend für die Arbeitsweise dieser Systeme ist ein eingebautes Expertensystem. Es lassen sich zwei wissensbasierte Systeme unterscheiden: Das AIDS-System (Anomalie Intrusion Detection System), entdeckt Anomalien im Verhalten der authentisierten Nutzer und das MIDS-System (Misuse Intrusion Detection System) entdeckt Missbrauch der Ressourcen.

Das AIDS-System speichert dazu von jedem Benutzer ein Verhaltensprofil. Beim MIDS-System werden Referenzdaten gespeichert, beispielsweise Mustern bekannter Angriffstypen, verfügbare Daten über sicherheitsrelevante Schwachstellen in den eingesetzten Betriebssystemen und Kommunikationsprotokollen oder die Ergebnisse eigener Penetrationstests.

Beide Systeme vergleichen im Betrieb die übertragenen Daten und Aktivitäten mit den gespeicherten Referenzdaten und entscheiden dann, ob Ressourcen missbräuchlich verwendet werden oder es zu Anomalien beim Verhalten des Benutzers kommt. In beiden Fällen wird die zuständige Stelle informiert, so dass Gegenmaßnahmen ergriffen werden können.

Die ständige Protokollierung der Daten erlaubt, dass sie später detailliert ausgewertet und falls notwendig die Wissensdatenbank und die eingesetzte Firewall angepasst werden können.

Wie Nutzerprofile erstellt werden und was protokolliert werden darf, sollte vorher mit einer kompetenten Stelle (Datenschutzbeauftragter des Unternehmens) diskutiert werden. Regelungen dazu bietet u. a. das Bundesdatenschutzgesetz.

Neben den wissensbasierten Systemen, die Daten und Aktivitäten beobachten, gibt es noch Simulatoren, die Angreifern authentische Netzwerkdienste vortäuschen. Diese Systeme werden auch als „honeypot“ bezeichnet. Solch ein System soll die Aufmerksamkeit eines Angreifers auf sich ziehen, damit er möglichst dieses System angreift. Es wird an den Stellen des Netzwerks installiert, an denen ein Angriff am ehesten zu erwarten ist. Für die Verteidiger bringt das den Vorteil, dass kein sensibles System beschädigt wird und man genügend Zeit bekommt, die Lücke zu finden, zu schließen und den Angreifer zurück zu verfolgen. Dadurch, dass es sich bei dem System nur um einen Simulator handelt, kann der Angreifer keinen Schaden anrichten. Solche Systeme können so aufgebaut sein, dass die Professionalität des Angreifers eingeschätzt werden kann, um Rückschlüsse auf seine Herkunft bzw. Ausbildung ziehen zu können.

Bei allen Systemen werden detaillierte Protokolle geführt, um zu einem späteren Zeitpunkt genaue Analysen durchführen zu können und um Beweismittel bei einem Strafverfolgungsverfahren gegenüber den Angreifer in der Hand zu haben.

Intrusion Detection Systeme sind heute noch Forschungs- und Entwicklungsgegenstand. Es wurden aber erhebliche Fortschritte in ihrer Effizienz erzielt. Für sicherheitsbewusste Unternehmen sind sie eine sinnvolle Erweiterung der Sicherheitsarchitektur.

■ 4.7 Chipkarten

Chipkarten oder auch Smartcards sind IT-Komponenten von der Größe einer Scheckkarte. Anfangs waren sie nur als reine Speicherchipkarten verfügbar und dienten zur Ablage von Daten. Beispiel dafür ist die Telefonkarte, die ein Guthaben enthält, das beim Telefonieren mit einem Kartentelefon reduziert wird, bis das gespeicherte Guthaben erschöpft ist und die Chipkarte unbrauchbar wird. Später kamen Prozessorchipkarten mit Mikroprozessoren und speichernden Bauteilen hinzu.

Chipkarten eignen sich als Speicher von Daten, die hinsichtlich ihrer Vertraulichkeit und/oder Integrität einen hohen Schutzbedarf aufweisen. Beispiele dafür sind die Scheck- und Kreditkarten mit Kontodaten, die Krankenversichertenkarte mit Individualdaten zur Identifizierung des Patienten sowie zur Abrechnung ärztlicher Leistungen oder Berechtigungskarten, die als elektronischer Ausweis für den Zugang zu einem Gelände oder zu Räumen dienen.

Chipkarten sind insbesondere dann verbreitet, wenn Personen authentisiert werden sollen, damit sie Zugang zu einem System oder Zugriff auf sicherheitsrelevante Daten und Funktionen erhalten. Chipkarten erzeugen Einmal-Passwörter, die im Challenge-Response-Verfahren an den Rechner übertragen werden. Damit sich Anwender nicht zahlreiche Passwörter merken müssen, gibt es auch multifunktionale Chipkarten.

Derzeit werden Chipkarten vermehrt zur Abwicklung kryptografischer Anwendungen eingesetzt, z.B. der digitalen Signatur. Die Chipkarte dient insbesondere dazu die geheimen Schlüssel der digitalen Signatur zu speichern. Chipkarten lassen sich so gestalten, dass der auf ihnen gespeicherte Schlüssel nicht auslesbar ist. Daten, die signiert werden müssen, werden in die Chipkarte als Bitstrom gesendet. Die Chipkarte antwortet darauf mit der aus den Daten berechneten Signatur. Die Signatur kann daraufhin im Rechnersystem weiterverwendet werden, beispielsweise als Signatur in einer E-Mail, ohne dass der geheime Schlüssel im Rechner verfügbar sein muss. Somit können auch keine bösartigen Schadprogramme den geheimen Schlüssel missbrauchen.

Chipkarten können auch dazu verwendet werden, sich gegenüber Systemen in beliebigen Netzen zu authentisieren. Diese Form der Authentisierung wird künftig verstärkt genutzt, um elektronische Geschäftsprozesse im Internet abzuwickeln. Vielfach genügt ein „Single-Sign-On“, um sich gegenüber allen Systemen, auf die man zugreifen darf, zu authentifizieren. Somit entfällt die Pflicht für Mitarbeiter sich unzählige PINs und Passwörter zu merken.

Die Aktivierung der Chipkarte geschieht durch eine eigene PIN. Für sie gelten die gleichen Regeln wie bei normalen Passwörtern. Die PIN ist die einzige schwerwiegende Schwachstelle des Gesamtsystems. Denn wenn die Chipkarte in falsche Hände gerät und die PIN erraten wird, ist ein Missbrauch der Karte nicht mehr zu verhindern. Außerdem kommt es immer wieder vor, dass Chipkarten durch die mehrfache Eingabe einer falschen PIN ungewollt deaktiviert und erst durch eine zentrale Service- bzw. Administrationsstelle wieder aktiviert werden müssen.

Um zusätzliche Sicherheit für die Chipkarte zu erreichen, werden moderne Karten bereits mit biometrischen Merkmalen angeboten. Beispielsweise können einige Karten den Fingerabdruck über einen Sensor einlesen und mit gespeicherten Referenzdaten vergleichen. Dann kann nur der autorisierte Nutzer der Karte die Funktionen nutzen, selbst wenn sie unberechtigten Dritten in die Hände fällt.

■ 4.8 Biometrische Verfahren

In der Kommunikation ist wichtig, dass wir uns immer sicher sind, dass unser Kommunikationspartner authentisch ist – egal, ob wir ihn persönlich treffen, telefonieren oder per Computer kommunizieren.

Im Gegensatz zu Geheimzahlen oder Passwörtern sind biometrische Authentifizierungsmerkmale an eine Person gebunden und nicht nur auf sie bezogen. Ein großer Vorteil ist, dass der Nutzer sie – anders als beispielsweise PINs – nicht vergessen kann. Dadurch sind sie komfortabel zu nutzen. Werden biometrische Verfahren eingesetzt, überprüft man die Identität von Personen, indem deren persönliche Merkmale verglichen werden. Unterschieden wird nach statischen Körpermerkmalen und aktiven Verhaltensweisen.

Übersicht von biometrischen Verfahren basierend auf Körpermerkmalen:

Ausgewertetes Merkmal des Basis-Verfahrens	Prinzip	Erfassungssystem (Beispiele)
Fingerabdruck / -bild	Muster der Papillarlinien – insbesondere Knotenpunkte eines Fingerabdrucks (Minuzien)	Optischer, kapazitiver oder thermischer Sensor
Hand	Form und Längenverhältnisse der Fingerglieder	Kamera
Gesicht	Proportionen innerhalb des Gesichtes	Kamera
Auge - Iris	Muster der Regenbogenhaut (Iris)	Kamera
Auge - Netzhaut	Blutgefäße der Netzhaut (Retina)	Infrarotlaser

Übersicht von biometrischen Verfahren basierend auf typischen Verhaltensweisen:

Biometrisches Merkmal	Ermittelte Daten	Aufnahmesystem (Beispiel)
Lippen-Bewegungen	Lippenbewegungen durch die Gesichtsmuskulatur und eines oder mehrere Kennworte	Kamera
Stimme	Individuelle Sprechweise und eines oder mehrere Kennworte	Mikrofon
Tippverhalten	Persönliches Tippverhalten (Schreibdynamik und der Tastenanschlag)	Tastatur
Unterschrift	individuelle Schreibbewegung und Schriftmuster	Schreibtablett, Spezialstift

Im alltäglichen Leben prüfen wir die Identität eines Menschen über sein Aussehen, die Stimme und /oder sein Verhalten. Dies ist uns meistens gar nicht bewusst. Insofern wäre eine Prüfung der Authentizität über biometrische Merkmale ein alltäglicher Vorgang. Computer können die notwendigen Abgleiche innerhalb kürzester Zeit vornehmen – nach eindeutig definierten und nachvollziehbaren Kriterien.

Welches Verfahren geeignet ist, richtet sich nach der Anwendungssituation. So können beispielsweise für die Zutrittskontrolle andere Verfahren eingesetzt werden als für den Schutz elektronischer Dokumente. Manchmal ist auch eine Kombination verschiedener Verfahren sinnvoll.

Biometrische Verfahren werden uns zukünftig häufig begegnen: etwa bei der Gesichtserkennung, via Webcam, um Zugang zum PC zu erhalten; beim Fingerabdruck-Leser am Türgriff, um Einlass zu besonders geschützten Arbeitsplätzen zu kriegen; bei der Iris-Erkennung am Flughafen, um in den Abflugbereich zu gelangen; bei der Unterschriftenerkennung, um elektronische Dokumente abzusichern oder bei der Spracherkennung an der Haustür, um Zutritt zu bekommen.

Die Beispiele für Anwendungsfelder biometrischer Systeme sind zahlreich: Zugangs- und Zutrittskontrolle, Raumüberwachung und Zeiterfassung, System-Log-On, Unterstützung von Geschäftsprozessen im Dokumentenmanagement, Grenz- und Einwanderungskontrolle, Strafverfolgung, Personaldokumente (wie Reisepässe), Personalisierung von Dienstleistungen und Geräten, Check-In an Flughäfen und in Hotels usw.

Das Hauptanwendungsfeld biometrischer Technologien lag im Jahre 2002 in der Zugangskontrolle mit 42 Prozent Marktanteil nach Umsätzen. Die meisten verfügbaren Verfahren basieren auf der Erkennung von Fingerbildern. Nahezu ungenutzt ist dagegen noch das Potenzial, das in der Rationalisierung papiergebundener Geschäftsprozesse im Dokumentenmanagement liegt. Hierfür eignet sich die vergleichsweise komplexe und daher auch tendenziell teurere Technologie des Unterschriftenvergleichs. Die gerade erfassten Daten eines Anwenders werden dafür mit zuvor gespeicherten Referenzwerten (Template) verglichen. Wo die Abspeicherung der Referenzdaten in einer zentralen Datenbank nicht erwünscht oder nicht möglich ist, können diese Daten auch auf einer Chipkarte



hinterlegt werden. Verbraucher- und Datenschützer sehen in dieser Speicherung auf Chipkarten die nutzerfreundlichste Lösung, da der Anwender die Hoheit über seine Daten besitzt.

Beim Einsatz biometrischer Verfahren ist zu berücksichtigen, dass nicht jede Messung exakt ist. Eine hundertprozentige Übereinstimmung kann, muss aber auch nicht vorliegen. Zur Erkennung einer Person müssen die gemessenen Daten mit den gespeicherten Daten innerhalb eines bestimmten Toleranzrahmens liegen. Einige biometrische Merkmale können sich schließlich temporär oder dauerhaft ändern (Heiserkeit, neue Frisur, Schnittwunden am Finger usw.). Die Systeme lassen sich darauf einstellen, welchen Grad der Veränderungen sie tolerieren. Die Grenze dafür ist fein, denn wenn der Toleranzrahmen zu hoch angesetzt ist, kann auch der Kollege mit einer ähnlichen Stimme den PC bzw. die Anwendung mitbenutzen und auf persönliche Daten zugreifen. Ist er zu eng gesteckt, braucht man mehrere Versuche, um einen Vorgang abzuwickeln. Eine gute Toleranzschwelle, die hinreichende Sicherheit und trotzdem genügend Bequemlichkeit bietet, kann mit Hilfe von statistischen Untersuchungen ermittelt werden.

Darüber hinaus ist die Qualität der Messtechnik zu hinterfragen. Es muss vermieden werden, dass die Sensorik überlistet wird. Je einfacher die Geräte aufgebaut sind, um so höher ist die Gefahr dazu. Fortgeschrittene Sensoren, die statische Körpermerkmale auswerten, verfügen inzwischen über eine so genannte Lebenderkennung. Sie soll verhindern, dass ein Messgerät durch ein Foto, eine Tonband- oder Videoaufnahme oder einen Fingerabdruck aus Gummi getäuscht wird. Möglich wird die Lebenderkennung, indem z.B. der Puls, die Körpertemperatur oder Augenblinzeln gemessen werden. Aktive Merkmale, wie Stimme, Unterschrift und Tastenanschlag benötigen derartige Zusatzüberprüfungen per se nicht.

Die Speicherung und Übertragung von biometrischen Daten sollte mit einer Verschlüsselung kombiniert werden, da sie andernfalls manipuliert werden können. Die Kombination von Biometrie und Verschlüsselungsverfahren gewährleistet authentische (echte) und integre (unverfälschte) Daten.

■ 5 Kontrollverfahren

Alle Sicherheitsmaßnahmen, die umgesetzt werden, können ihre volle Wirksamkeit nur entfalten, wenn sie angemessen sind. Wenn ein Sicherheitskonzept erstellt wird, sind in der Regel alle die Sicherheit betreffenden Komponenten bekannt. Da besonders die Informationstechnologie einem ständigen Wandel unterliegt, wirkt sich jede Veränderung im operativen Umfeld auf das einmal erstellte Sicherheitskonzept aus. Damit etablierte Sicherheitsmaßnahmen nicht durch permanente Veränderungen ausgehebelt werden, benötigt man Kontrollverfahren, die entsprechend einem modifizierten betroffenen Umfeld ständig überprüfen, ob sie noch angemessen sind.

■ 5.1 Kontrollen im täglichen Betrieb

Besonders im täglichen Betrieb sind Kontrollverfahren erforderlich, die die Sicherheit der zu schützenden Ressourcen dauerhaft gewährleistet. Was versteht man unter Kontrollverfahren? Hier einige Beispiele:

- Anwendungen wie auch Betriebssysteme werden in der Regel mit „Standardbenutzern“ und Standardpasswörtern ausgeliefert. In den Installationsleitfäden der Hersteller findet man meist in den ersten Kapiteln die Empfehlung, diese umgehend nach der Installation zu ändern. Dieser Rat wird oft missachtet. Diese offensichtliche Sicherheitslücke fällt vor allem deshalb nicht auf, weil die „Standardbenutzer“ im täglichen Betrieb meist nicht genutzt werden.
- Ist eine Anwendung in Betrieb genommen und mit Produktivdaten versorgt, hat natürlich immer Vorrang, dass sie reibungslos funktioniert und verfügbar ist. Kommen neue Anforderungen, z.B. aus dem Management, müssen diese schnell und effizient umgesetzt werden. Das erfolgt oft unter Umgehung der vorhandenen Sicherheitsrichtlinien – meist mit dem Vorsatz, das Versäumte bei nächster Gelegenheit nachzuholen und die Sofortmaßnahme in eine permanente, sichere Lösung umzusetzen. Leider bleibt es sehr häufig bei der guten Absicht.
- Testsysteme werden immer dann benötigt, wenn neue Anwendungen auf ihre Funktionalität überprüft werden sollen. Da in einem Testsystem meist keine sensiblen Daten enthalten sind, wird ihr Schutzbedarf als gering eingestuft. Doch Testsysteme können als Stützpunkt für Viren und Hacker dienen und für Angriffe auf die geschäftskritischen Systeme ausgenutzt werden.

Diese Beispiele verdeutlichen, dass selbst das beste Sicherheitskonzept nur dann vor Bedrohung schützt, wenn gewährleistet werden kann, dass es dauerhaft eingehalten wird.

Beispiele für Kontrollmaßnahmen im täglichen Betrieb

- Überprüfen Sie regelmäßig alle „Standardbenutzer“ und deren Passwörter. Ändern Sie Standardpasswörter in „sichere“ Passwörter, die weder zu erraten sind, noch über eine einfache Wörterbuch-Attacke schnell gefunden werden können (siehe auch Abschnitt „Passwörter“).
- Überprüfen Sie das Alter der Administratoren-Passwörter. Ändern Sie diese regelmäßig und immer sofort, wenn ein Besitzer dieses Passworts seine Position innerhalb des Unternehmens ändert oder das Unternehmen verlässt.
- Überprüfen Sie, ob jeder Mitarbeiter ausschließlich über die Rechte verfügt, die er für die Erfüllung seiner Aufgaben benötigt.
- Überprüfen Sie, ob die im Sicherheitskonzept festgelegten Maßnahmen noch funktionsfähig sind.
- Überprüfen Sie, ob neu hinzugefügte IT-Komponenten durch geeignete Sicherheitsmaßnahmen geschützt sind.
- Überprüfen Sie, ob nur die wirklich benötigten Anwendungen auf dem jeweiligen System installiert sind.
- Überprüfen Sie, ob die aktuellen Sicherheits-Updates der Hersteller installiert sind.

■ 5.2 Penetrationstests

Eine gute Methode, um zu überprüfen, ob die Sicherheitsmaßnahmen noch angemessen sind, sind die so genannten Penetrationstests. Ein Penetrationstest ermittelt die potenziellen Ziele von Hacker-Angriffen und analysiert die Schwachstellen hinsichtlich der Gefährdungen, die von ihnen für das Unternehmen ausgehen. Am Ende erhält man detaillierte Empfehlungen, wie die erkannten Schwachstellen effektiv beseitigt werden können.

Für die Durchführung eines Penetrationstests stellen sich die Ausführenden („Tiger Team“) auf die Seite eines vermeintlichen Angreifers (Hacker). Es kommen Methoden zum Einsatz, die ein Angreifer anwenden würde, um unautorisierten Zugriff auf ein System zu erhalten. Dabei ist es unerheblich, ob ein System im Internet oder im Unternehmensnetz installiert ist. Potenzielle Angreifer finden sich überall, wobei das Risiko für Systeme, die direkt im Internet stehen, erheblich größer ist.

Es gibt eine Unzahl von Dienstleistern, die die Durchführung von Penetrationstests anbieten. Selbst einige Webseiten im Internet sind frei verfügbar, mit deren Hilfe einfachste Tests, in der Regel Portscans, kostenlos ausgeführt werden können. Es empfiehlt sich, insbesondere Internet-basierte Systeme regelmäßig auf die Sicherheit zu prüfen oder überprüfen zu lassen. Um sich vor „schwarzen Schafen“ in der Branche zu schützen, sollte man auf nachvollziehbare Referenzen bestehen, bevor ein Auftrag vergeben wird. Denial-of-Service Tests sind als Referenz wenig hilfreich, da diese sehr oft erfolgreich verlaufen und somit keinen verwertbaren Hinweis auf die Qualität des möglichen Auftragnehmers bieten.

Allgemein muss gelten, dass die Penetrationstests sorgfältig geplant und abgestimmt werden müssen, um:

- das Risiko abzuwägen, dass Produktionssysteme beeinträchtigt werden
- abzuschätzen, welcher Aufwand zu treiben ist und welche Methoden eingesetzt werden (dürfen)
- sicherzustellen, dass alle Beteiligten über den Test informiert sind und dadurch unnötige Reibungsverluste vermieden werden.

Da sich die Tätigkeit eines „Tiger Teams“ in einer rechtlichen Grauzone bewegt, ist es von großer Bedeutung für Auftraggeber wie auch für Auftragnehmer, sich durch einen entsprechenden Vertrag rechtlich abzusichern.

■ 5.3 Audits

Während Penetrationstests rein auf die technische Umgebung abzielen und eine Momentaufnahme des IT-Systems darstellen, dienen Sicherheitsaudits dazu, das komplette Umfeld permanent nach Sicherheitsrisiken zu überprüfen. Bei der Durchführung von Audits werden nicht nur die aktuellen technischen Einstellungen überprüft, sondern auch die Verfahren, Dokumentationen sowie die Handlungen der Mitarbeiter genauer betrachtet.

Audits dienen dazu, das komplette Umfeld der Infrastruktur oder des Systems auf Sicherheitslücken zu untersuchen. Ergebnisse von Audits werden in der Regel mit Maßnahmenempfehlungen hinterlegt. Die Umsetzung zielt darauf ab, diese oder ähnliche Audit-Ergebnisse in Zukunft zu vermeiden. Im Gegensatz zu Penetrationstests, die konkrete technische Sicherheitslücken finden, dienen Audits dazu, strukturelle Probleme aufzudecken.

Auch für diesen Service gibt es eine Menge anerkannter Dienstleister. Hier gelten die gleichen Anforderungen wie für Penetrationstests. Ein Audit lohnt sich immer dann, wenn das zu überprüfende System kritisch, also betriebswirtschaftlich sehr wertvoll für das Unternehmen ist. Durch Audits wird die Vertrauenswürdigkeit gegenüber Kunden erhöht, etwa bei der Nutzung von E-Business-Anwendungen.

■ 5.4 Passwortanalysen

Ein Angreifer versucht in der Regel als erstes, Passwörter von Anwendungen oder Systemen zu erraten. Damit kommt er meist einfach und wirksam zum Ziel. Denn viele Passwörter sind nicht ausreichend sicher. Spezielle Programme erraten die Passwörter automatisiert. Diese so genannten Brute-Force-Attacken greifen direkt auf die Passwort-Datenbank zurück. Dort sind die Passwörter verschlüsselt abgelegt und es ist prinzipiell nicht möglich, aus dem verschlüsselten Wert das Passwort wieder herzustellen. Da jedoch die Verschlüsselungsfunktion bekannt ist, kann man für beliebige Wörter oder Buchstaben- und Ziffernfolgen den verschlüsselten Gegenwert berechnen und mit dem gespeicherten verschlüsselten Wort vergleichen. Findet man einen identischen Wert, so konnte das Passwort erraten werden.

Je nachdem, welche Komplexitätsstufe eingestellt wird, können beim automatisierten Passwort-Erraten Laufzeiten von wenigen Minuten bis zu einigen Tagen entstehen. Üblicherweise werden bereits in wenigen Stunden erstaunliche Ergebnisse erzielt.

Es ist gesetzlich verboten, Passwörter zu „knacken“. Sollte es im Notfall betrieblich unumgänglich sein ein Mitarbeiterpasswort zu „knacken“, darf dies nur nach eindeutiger Genehmigung der Geschäftsleitung sowie des Betriebsrates erfolgen. Der Mitarbeiter muss anschließend eine Meldung bekommen, dass sein Passwort nicht mehr geheim ist und er es beim nächsten Anmelden am System ändern muss. Empfohlen ist, nicht das Passwort selbst sondern die Tatsache, dass das Passwort erraten werden konnte, an den Mitarbeiter zu übermitteln, damit dieser es umgehend ändert.

■ 6 Standards und geprüfte IT-Sicherheit

Um die vielen einzelnen Sicherheitslösungen zu strukturieren gibt es standardisierte Vorgehensmodelle. Ein Vorgehensmodell in Anlehnung an das IT-Sicherheitshandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist im Kapitel 1,5 beschrieben.

Außerdem gibt es im deutschsprachigen Raum die IT-Grundsicherheitsmaßnahmen des BSI und international den britischen Standard BS 7799, der in der International Organization for Standardization (ISO) unter ISO/IEC 17799 gelistet wird.

Ein weiteres Unterstützungsinstrument bei der Einführung unternehmensweiter Sicherheit sind die Protection Profiles (Schutzprofile) der Common Criteria (CC). Dieser Standard beschreibt die Sicherheit von IT-Systemen. Die Schutzprofile stellen wiederum die Sicherheitslagen für bestimmte Anwendungen bzw. Gruppen von Anwendungen dar, die auf den involvierten Unternehmensteil übertragen werden können.

Die Standards helfen dem Anwender, sich am Stand der Technik zu orientieren und die Frage nach angemessenen Sicherheitsmaßnahmen zu beantworten.

■ 6.1 Common Criteria (CC)⁷

In Europa werden die Common Criteria (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik Version 2.0), die gemeinsam von Sicherheitsagenturen aus den USA, Kanada, Großbritannien, Frankreich, Deutschland und den Niederlanden entwickelt wurden, als Grundlage und Standard verwendet.

Die CC sind die Weiterentwicklung des vorhergehenden Standards ITSEC (Information Technology Security Evaluation Criteria – Kriterien für die Bewertung der Sicherheit von Systemen in der Informationstechnik).

Protection Profiles⁸ beschreiben eine Sicherheitslage anhand von Bedrohungen und Sicherheitszielen sowie einer Darstellung der Betriebsumgebung der IT-Systeme. Diese Sicherheitslage kann wie ein Baustein auf ähnliche Unternehmensteile übertragen werden. Die Sicherheitsziele und Maßnahmen werden entsprechend angewendet. Mögliche Abweichungen können identifiziert und gesondert analysiert werden.

Die CC stellen dazu Anforderungen an die Sicherheitsfunktionen von IT-Produkten und IT-Systemen. Die Sicherheitsfunktionen der Produkte und Systeme werden in der so genannten Evaluation anhand der gestellten Anforderungen geprüft und bewertet.

Mit diesen Anforderungen der CC ist es möglich, angemessene Produkte als Lösungen für Sicherheitsprobleme zu suchen und zu finden. Der Anwender kann einschätzen, ob das IT-Produkt oder IT-System eine ausreichende Sicherheit für die beabsichtigte Anwendung besitzt und ob die Sicherheitsrisiken bei dessen Gebrauch toleriert werden können.

⁷ Weitere Informationen sind unter den Adressen <http://www.bsi.de/cc/index.htm>, <http://www.commoncriteria.org> oder <http://www.csrc.nsl.nist.gov> erhältlich.; ⁸ <http://www.bsi.de/cc/pplist/pplist.htm>

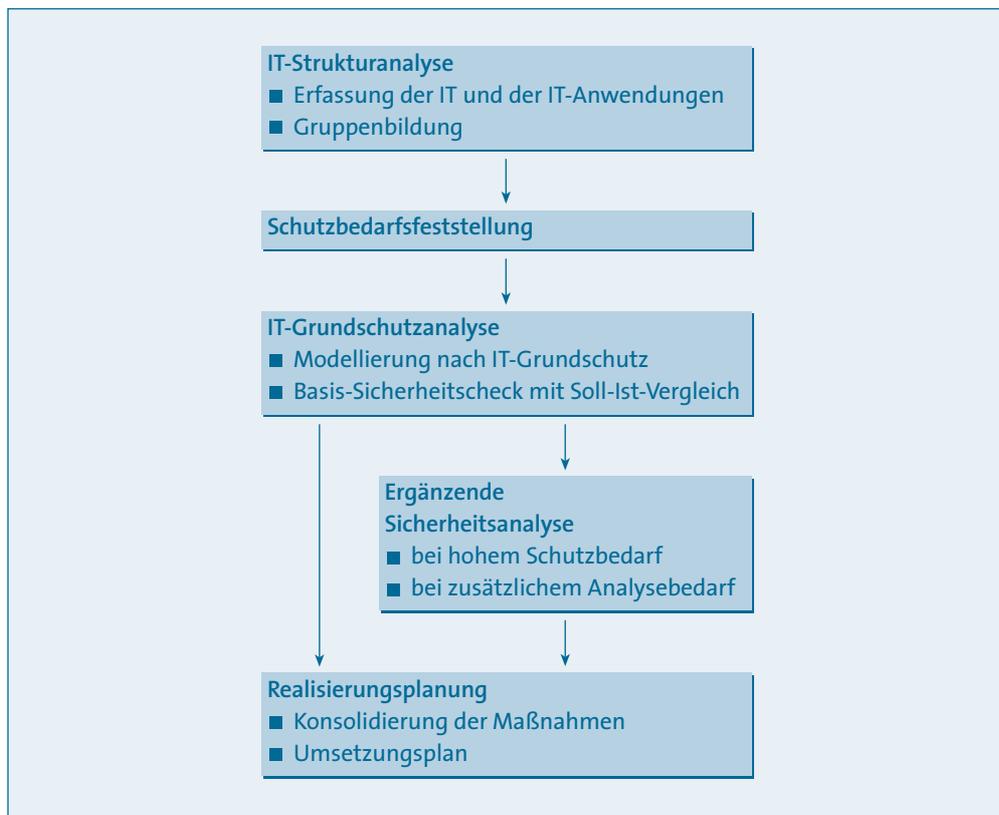
Dazu sind die Produkte in Zertifizierungsstufen eingeteilt und variieren von der niedrigsten Stufe EAL1 bis zur höchsten Stufe EAL7. Des Weiteren wird die Stärke der Sicherheitsfunktionen nach ihrer Widerstandsfähigkeit gegen Angreifer in „hoch“, „mittel“ und „niedrig“ eingeteilt.

Bei einigen Anwendungen werden solche Zertifikate per Gesetz verlangt. Beispielsweise wird für bestimmte Anwendungsfälle der digitalen Signatur gefordert, dass die Erstellungseinheit nach dem Signaturgesetz entsprechend zertifiziert ist.

■ 6.2 Das IT-Grundschutzhandbuch

Die IT-Grundschutzmaßnahmen des BSI sind in einem IT-Grundschutzhandbuch beschrieben⁹. Es handelt es sich um eine Sammlung von Ratschlägen, wie man die unterschiedlichen IT-Systeme absichern kann. Mit Hilfe des Grundschutzhandbuchs soll erreicht werden, dass man ohne komplexe Voruntersuchungen (Bedrohungs- und Risikoanalyse) und mit einfachen Bausteinen ein Mindestmaß an Sicherheit realisieren kann. Frei nach dem „Pareto-Prinzip 80/20“. Die Zielgruppen sind daher kleine bis mittelständische Unternehmen mit einfachen IT-Strukturen. Ursprünglich war der Fokus auf einen mittleren Schutzbedarf ausgerichtet. Inzwischen ist das Vorgehensmodell erweitert worden, um auch verzweigte Unternehmensstrukturen abzubilden und partiell höhere Sicherheitsanforderungen zu erfüllen. Insofern bietet das BSI-Grundschutzhandbuch heutzutage einen Rahmen, mit dem eine IT-Sicherheitsstruktur an die Unternehmensentwicklung angepasst werden kann.

■ Erstellung eines IT-Sicherheitskonzeptes



Quelle: BSI

⁹ Das Grundschutzhandbuch ist unter der Adresse www.bsi.bund.de erhältlich

Audit

Im Rahmen der Zertifizierung erfolgt in regelmäßigen Abständen ein Audit durch einen externen, zugelassenen Zertifizierer.

Die inhaltlichen Kriterien für die Zertifizierung sind im IT-Grundschutzhandbuch beschrieben. Der Maßnahmenkatalog enthält viele vorwiegend technische Empfehlungen, mit denen z.B. ein Systemadministrator seinen Bereich sichern kann. Die detaillierte Ausarbeitung empfiehlt den Maßnahmenkatalog auch als Nachschlagewerk für andere Vorgehensmodelle.

Zertifizierung

Das BSI hat für Unternehmen die Möglichkeit einer dreistufigen Zertifizierung geschaffen:

- die Selbsterklärung „IT-Grundschutz Einstiegsstufe“,
- die Selbsterklärung „IT-Grundschutz Aufbaustufe“ und
- das „IT-Grundschutz-Zertifikat“.

■ 6.3 BS 7799 und ISO/IEC 17799

Der aus Großbritannien stammende Standard BS 7799¹⁰ befasst sich mit der Sicherheit aus der Sicht des Unternehmensmanagements. Der Standard wurde im Jahr 2000 in das internationale Regelwerk aufgenommen und ist unter der Bezeichnung ISO/IEC 17799 geführt. Adressaten sind in der Regel mittlere bis große Unternehmen mit relativ komplexen Strukturen. Das Vorgehensmodell nach BS 7799 ermöglicht es dem einzelnen Unternehmen die Tiefe seiner Sicherheitsuntersuchung zu bestimmen und daraus eine eigene „maßgeschneiderte Sicherheitslösung“ abzuleiten, die jederzeit erweitert werden kann. Diese Vorgehensweise spart Mittel für Sicherheitsinvestitionen und ermöglicht es, die Kosten (besser) zu kontrollieren. Grundsätzlich ist der Standard auch für einen höheren Schutzbedarf geeignet.

Um eine Bedrohungs- und Risikoanalyse durchzuführen, ist eine Gegenüberstellung von Problembe-
reichen und entsprechenden Maßnahmen anhand einer Checkliste vorgesehen. Die Checkliste dient der Vollständigkeitskontrolle. Im Mittelpunkt steht aber, die jeweilige Lösung zu dokumentieren.

Mit dieser Vorgehensweise wird die Idee des Qualitätsstandards ISO 9000 ff. aufgegriffen und das vorhandene Fach- und Technikwissen genutzt, um angemessene Sicherheitsmaßnahmen abzuleiten.

Der Standard BS 7799 ist als ISO/IEC 17799:2000 (kurz ISO 17799) bzw. BS 7799-2 weiterentwickelt worden. Dieses Dokument umfasst die Spezifizierung eines Informationssicherheits-Managementsystems (ISMS).

Audit

Ein weiteres wichtiges Element des Vorgehensmodells ist, die Sicherheitsregelungen in regelmäßigen Audits zu überprüfen. Mit diesem Vorgehen können Unternehmen ihre Sicherheitspläne immer weiter verfeinern. In der Folge werden Sicherheitslücken sukzessive geschlossen. Das Audit als Bestandteil der Unternehmenskultur ist darauf ausgelegt, dass verschiedene Managementkonzepte zusammenwachsen, was die Integration des Standards BS 7799 vereinfacht.

¹⁰ Der Standard kann unter den Internetadressen <http://www.iso.ch> und <http://www.bsi-global.com> gekauft werden. Unter der Adresse der British Standard Institution (BSI) ist der Leitfaden auch auf Deutsch erhältlich.



Zertifizierung

Ein bestehendes Sicherheitsmanagement kann nach dem BS 7799 zertifiziert werden. Dieser Vorgang erfolgt durch einen externen und zugelassenen Zertifizierer.

■ 6.4 Anwendung des BS 7799 oder des IT-Grundschutzhandbuchs

Um die beiden Standards umzusetzen, kann man z.B. von den Herstellern erstellte Software einsetzen. Der Anwender wird Schritt für Schritt durch das Modell geleitet.

Des Weiteren bietet das Bundesamt für Sicherheit in der Informationstechnik unter dem Titel „BS 7799 Part 1 – Vergleich mit dem IT-Grundschutzhandbuch“ eine Gegenüberstellung zwischen dem internationalen ISO 17799 und dem deutschen Standard IT-Grundschutz an. In diesem Dokument werden Sicherheitsfragen themenbezogen dargestellt, so dass der Leser die Möglichkeit hat, die beiden Standards zu vergleichen.

In der folgenden Tabelle ist auf der Ebene der Hauptüberschriften ein kurzer Auszug aus dem Vergleich zwischen BS 7799 und IT-Grundschutzhandbuch des BSI dargestellt¹¹:

BS 7799 (ISO/IEC 17799)	IT-Grundschutzhandbuch
3. Sicherheitspolitik	Kap. 3.0 IT-Sicherheitsmanagement
4. Organisation von Sicherheit	Kap. 3.0 IT-Sicherheitsmanagement
5. Bewertung und Kontrolle der Unternehmenswerte	Kap. 2.1 IT-Strukturanalyse Kap. 2.2 Schutzbedarfsfeststellung
6. Mitarbeitersicherheit	Kap. 3.2 Personal Kap. 3.8 Behandlung von Sicherheitsvorfällen
7. Physische Sicherheit	Kap. 3.4 Datensicherungskonzept Kap. 4.0 Infrastruktur Kap. 4.2 Verkabelung Kap. 5.3 Tragbarer PC Kap. 9.3 Telearbeit
8. Sicherheit von Kommunikationsverbindungen und Netzen	Kap. 2.0 Anwendung des IT-Grundschutzhandbuchs Kap. 3.4 Datensicherungskonzept Kap. 3.6 Computer-Virenschutzkonzept Kap. 3.8 Behandlung von Sicherheitsvorfällen Kap. 6.1 Servergestütztes Netz Kap. 6.8 Netz- und Systemmanagement Kap. 7.1 Datenträgeraustausch Kap. 7.4 E-Mail Kap. 7.5 WWW-Server Kap. 8.0 Telekommunikation
9. Zugriffskontrolle	Kap. 5.3 Tragbarer PC Kap. 7.3 Firewall Kap. 7.6 Remote Access Kap. 8.6 Mobiltelefon Kap. 9.3 Telearbeit
10. Systementwicklung und -erhaltung	Kap. 3.7 Kryptokonzept Kap. 9.1 Standardsoftware
11. Kontinuitätsplanung	Kap. 3.3 Notfallvorsorge-Konzept Kap. 3.8 Behandlung von Sicherheitsvorfällen
12. Beachtung von Regeln und Gesetzen	Kap. 3.5 Datenschutz

¹¹ Die vollständige Gegenüberstellung kann auf der BSI-Homepage abgerufen werden: <http://www.bsi.bund.de/gshb/deutsch/aktuell/bs7799.htm>

■ 7 Glossar

Im Glossar werden einige häufig verwendete Fachbegriffe erläutert.

■ A

Angriff

Ein Angriff ist eine bewusst herbeigeführte sicherheitsgefährdende Aktion.

Asymmetrisches Kryptosystem

Kryptosystem, das zur Verschlüsselung und für digitale Signaturen verwendet werden kann. Dabei werden zwei unterschiedliche Schlüssel, ein geheimer und ein öffentlicher Schlüssel, verwendet.

■ B

Bedrohung

Eine Bedrohung ist eine gegen ein IT-System gerichtete Aktion oder ein Ereignis, das die IT-Sicherheit eines Systems gefährden kann.

■ C

CERT

Computer Emergency Response Team (Computer-Notfall-Team)

Certification Authority

Eine Certification Authority (Zertifizierungsstelle) ist eine vertrauenswürdige Institution, die öffentliche Schlüssel beglaubigt, indem sie Zertifikate ausstellt. Dazu werden die darin enthaltenen Informationen, insbesondere die Identität des Schlüsselinhabers, überprüft. Werden die Anforderungen der Zertifizierungsstelle für einen erfolgreichen Identitätsnachweis erfüllt, so versieht diese den öffentlichen Schlüssel der identifizierten Person oder des identifizierten Dienstes mit ihrer eigenen digitalen Signatur.

Chiffrierung

siehe Verschlüsselung

Cookie

Ein Cookie (engl., Kekes) ist eine Information, die ein Web-Server bei einem Clientprogramm ablegt. So wird das Surf-Verhalten eines Nutzers protokolliert und auswertbar.

CPS (Certificate Policy Statement)

Geschäftsbedingungen einer Zertifizierungsstelle, die unter anderem Aufschluss über die Voraussetzungen für die Ausstellung eines Zertifikates geben.

■ D

DEA

Data Encryption Algorithm, symmetrisches Blockchiffrierverfahren definiert im Data Encryption Standard.

DES

DES ist ein symmetrisches Verschlüsselungsverfahren. Es handelt sich um einen Blockalgorithmus, der 64-Bits-Klartext in 64-Bits-Schlüsseltext und umgekehrt überführt. Die Schlüssellänge beträgt ebenfalls 64-Bit, wobei jedoch nur 56-Bit hiervon signifikant sind. Eingesetzt wird das DES Verfahren insbesondere in Finanzanwendungen und kann als Quasi-Standard bezeichnet werden. DES ist weit verbreitet, aber aufgrund der geringen Schlüsselgröße von 56-Bit nicht mehr zeitgemäß.

Digitale Signatur

Eine digitale Signatur dient zum Unterschreiben elektronischer Daten. Eine digitale Signatur erlaubt es zu überprüfen, dass die Daten nicht verändert wurden und wirklich vom Erzeuger der Signatur stammen. Eine digitale Signatur ist mehr als eine handschriftliche Unterschrift dahingehend, dass sie sowohl den Inhalt einer Nachricht als auch die Identität des Benutzers bestätigt.

DNS

Domain Name System: Internetprotokoll, das die Zuordnung von Internet-Adressen zu Rechnernamen und umgekehrt definiert.

DNS-Spoofing

Angriff auf das DNS. Ermöglicht einem Angreifer, unter einem fremden DNS-Namen aufzutreten.

■ E

E-Commerce

Elektronische Vermarktung, Handel und Dienstleistungen auf elektronischem Wege, z.B. über das Internet.

Einwegfunktion

Berechnungsvorgang zur Erzeugung einer Zeichenfolge, der nicht oder nur mit sehr erheblichem Aufwand umkehrbar ist.

Elliptische Kurven

Elliptische Kurven sind ein asymmetrisches Kryp-

tosystem der neuesten Generation, bei dem die höchste Sicherheitsstärke pro Schlüsselbit erzielt wird.

E-Mail

Elektronische Post, einer der wichtigsten Dienste im Internet.

Ethernet

Weit verbreiteter Typ eines lokales Netzwerk mit eigenem Kommunikationsprotokoll, und einer Datenübertragungsgeschwindigkeit von 10 Mbit/s oder 100 Mbit/s (Fast Ethernet).

Extranet

Verwendung von Internet-Diensten zwischen Intranets.

■ F

Faktorisierung

Zerlegung einer ganzen Zahl in kleinere Faktoren, bei der Primfaktorzerlegung in Primfaktoren. Viele Verschlüsselungsverfahren basieren auf der Schwierigkeit, eine Zahl in ihre Primfaktoren zu zerlegen.

Fingerprint

Prüfsumme einer Datei oder eines Schlüssels.

Firewall

Eine Sicherheitseinrichtung zum Schutz eines internen Netzwerks, das an externe Netzwerke, etwa das Internet angeschlossen ist. Die Firewall soll unbefugte Zugriffe und ggf. die Übertragung von Viren verhindern.

FTP

File Transfer Protocol: Protokoll und Bezeichnung des Internet-Dienstes zur Übertragung von Dateien im Internet.

■ G

Geheimer Schlüssel

Teil des Schlüsselpaars bei der Anwendung von asymmetrischen Verschlüsselungsverfahren, der nur dem Besitzer bekannt sein darf. Mit ihm wird dechiffriert.

■ H

Hash-Funktion

Eine Hash-Funktion dient dazu, aus einem langen Text einen kurzen Text, den Hash-Text, abzuleiten. Hierbei genügt sie jedoch der Bedingung, dass es unmöglich ist, zu einem einmal abgeleiteten Hash-Text einen vom ursprüng-

lichen Langtext verschiedenen Langtext zu konstruieren. Der Hashtext dient – zusammen mit einer asymmetrischen Verschlüsselung – zur Herleitung der digitalen Unterschrift.

■ I

Identifikation

Identifikation bezeichnet die Bekanntgabe der eigenen Identität oder Ermittlung einer fremden Identität.

Identität

Eine gültige und eindeutige Kennung eines Anwenders, einer Anwendung oder einer Netzwerkkomponente.

Informationstechnik (IT)

Informationstechnik (IT) sind die technischen Mittel, die der Verarbeitung, Übertragung oder Vermittlung von Daten dienen.

Integrität

Integrität ist der Zustand, der unbefugte und unzulässige Veränderungen von Daten und an IT-Systemen oder Komponenten ausschließt.

IT-Sicherheit

siehe Sicherheit in der Informationstechnik

■ K

Krypto-Regulierung

Gesetzliche Maßnahmen, die die freie Benutzung von Kryptoverfahren zugunsten der Verbrechensbekämpfung einschränken. Die Bundesregierung hat im Juni 1999 entschieden, für die Dauer von zwei Jahren von der Kryptoregulierung. abzusehen. Danach soll erneut geprüft werden.

Kryptologie

Lehre vom Verschlüsseln (Kryptographie) und vom Brechen von Kryptosystemen (Kryptoanalyse).

Kurven, elliptische

Für die Punkte auf elliptischen Kurven sind Rechenoperationen möglich, die der Multiplikation und der Potenzierung ganzer Zahlen entsprechen. Aus diesem Grunde kann mit ihnen ein diskreter Logarithmus ($\langle \cdot \rangle$) definiert werden.

■ L

Logarithmen, diskrete

Wird eine modulo-Zahl ($\langle \cdot \rangle$ Modulo) immer wieder mit sich selbst multipliziert (in geheimgehaltener Anzahl), so hat man die diskrete Potenz. Die Rekonstruktion der geheimgehaltenen Zahl

ist der diskrete Logarithmus (DL).

Beispiel. $7 \text{ hoch } x = 2 \text{ mod } 5$; x ist der DL. Es gibt keinen Algorithmus zur Berechnung des DL.

Verschiedene asymmetrische Verschlüsselungsverfahren benutzen die Eigenschaften des DL.

■ M

Modulo (mod)

Eine Modulo-Zahl ist eine ganze Zahl, von der eine andere ganze Zahl, der Modul, so oft subtrahiert wird, bis eine Zahl gewonnen wird, die kleiner als dieser Modul ist.

Beispiel: $12 = 2 \text{ mod } 5$

Asymmetrische Schlüsselverfahren basieren auf Modulo-Zahlen.

■ O

Öffentlicher Schlüssel

Teil des Schlüsselpaars bei der Anwendung von asymmetrischen Verschlüsselungsverfahren, der öffentlich bekannt sein muss. Mit ihm wird chiffriert.

■ P

PGP

Pretty Good Privacy:

Private Key

s. geheimer Schlüssel

Public Key

s. öffentlicher Schlüssel

■ R

Risiko

Risiko ist ein Maß für die Gefährdung eines Systems oder bestimmter Systemkomponenten. Dieses Maß ist abhängig von der Anzahl eintretender Bedrohungen und den jeweiligen Schäden und Folgeschäden.

Risikomanagement

Risikomanagement ist die Gesamtheit aller Aktivitäten, die darauf ausgerichtet sind, die Risiken für ein System zu auf ein angemessenes Maß zu bringen.

■ S

Schutzbedarf

Der Schutzbedarf ist ein Maß für die Bedeutung, die Daten, Informationen oder Funktionen eines zu untersuchenden Systems für den Betreiber,

Anwender oder Nutzer des Systems haben.

Schwachstelle

Eine Schwachstelle eines Systems ist der Zustand oder die Eigenschaft des Systems oder einzelner Systemteile, die das Wirksamwerden einer Bedrohung zulässt.

Sicherheit in der Informationstechnik (IT-Sicherheit)

IT-Sicherheit ist der Zustand eines Systems, in dem die Vertraulichkeit, die Integrität, die Verbindlichkeit, und die Verfügbarkeit von Daten oder Funktionen beim Einsatz von IT-Systemen oder Komponenten entsprechend der Sicherheitsanforderungen gewährleistet sind.

Sicherheitsanforderungen

Eine Menge von Forderungen, deren Erfüllung zur Sicherheit des Systems beiträgt. Sind die Anforderungen vollständig, so wird bei ihrer Erfüllung der definierten Sicherheit des Systems erreicht.

SSL

Secure Socket Layer

Steganographie

Indirekte Verschlüsselung durch Verstecken der Information in anderen Daten.

Symmetrisches Kryptosystem

Kryptosystem, bei dem zur Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird.

■ T

Triple DES

Kryptoverfahren, bei dem der DES-Algorithmus zur Ver- und Entschlüsselung dreimal angewendet wird.

Trust Center

Vertrauenswürdige Instanz, innerhalb derer hochsensible Aktivitäten durchgeführt werden, etwa die Zuordnung von Schlüsseln zu Personen, die Ausstellung von Zertifikaten (s.a. Certification Authority) oder andere Schlüsselmanagementfunktionen.

■ V

Verbindlichkeit

Verbindlichkeit ist der Zustand, in dem geforderte oder zugesicherte Eigenschaften oder Merkmale von Dokumenten, Übermittlungen oder Übermittlungsstrecken sowohl für die Nutzer verbindlich feststellbar als auch Dritten gegenü-

ber beweisbar sind.

Verfügbarkeit

Verfügbarkeit ist der Zustand, der die erforderliche Nutzbarkeit von Daten sowie IT-Systemen und Komponenten innerhalb definierter Zeitspannen sicherstellt

Verschlüsselung

Die Verschlüsselung verändert Daten mit Hilfe eines mathematischen Verfahrens und eines Schlüssels derart, dass die Daten nicht mehr verständlich sind und nur mit Hilfe des passenden Schlüssels wieder in die ursprüngliche Form gebracht werden können.

Vertraulichkeit

Vertraulichkeit ist ein Zustand, der unbefugte Informationsgewinnung/-beschaffung ausschließt.

Virus

Computerviren sind eigenständig ausführbare Programmroutinen, die Daten oder Programme verfälschen oder löschen können. Sie reproduzieren sich selbst und führen für den Anwender nicht kontrollierbare Aktionen aus.

Virenmuster-datenbank

Datenbank mit Mustern bekannter Viren.

Virens Scanner

Antivirensoftware, die Datenträger, Systembereiche, Unterverzeichnisse, Dateigruppen und einzelne Dateien auf Viren hin durchsucht, vor einem möglichen Virus warnt und versucht, den Virus so zu entfernen, dass die ursprüngliche Funktionalität wieder hergestellt wird.

Virenschild

Virenschilde laufen im Hintergrund und überwachen Systemkomponenten oder Betriebssystemschnittstellen. Sie suchen nach Anzeichen von Virenaktivitäten und nach bekannten Virenmustern.

■ 8 Literaturhinweise

Das IT-Grundschutzhandbuch des BSI

<http://www.bsi.bund.de/gshb/index.htm>

Internet Core Protocols

<http://www.oreilly.com/catalog/coreprot/>

Gemeinsame Kampagne „Sicherheit im Internet“ des Bundeswirtschafts- und Bundesinnenministeriums sowie des BSI

<http://www.sicherheit-im-internet.de/>

Leitfaden des DFN-CERT zur Absicherung von Netzwerken

<ftp://ftp.cert.dfn.de/pub/docs/leitfaden/leitfaden.pdf>

Maßnahmen zur Abwehr von Angriffen auf Rechensysteme über Netzverbindungen. Das Sicherheitskonzept des Rechenzentrums der Universität Karlsruhe

<http://www.rz.uni-karlsruhe.de/Uni/RZ/Netze/sicherheit.pdf>

Sicherheitsinformationen der Uni Siegen

<http://www.infoserversecurity.org/>

TCP/IP Netzwerkadministration

<http://www.oreilly.com/catalog/tcp3/>

Materialsammlung zum Datenschutz

<http://www.bfd.bund.de/>

Zeitschrift „c't“

<http://www.heise.de/ct/>

Vierter Zwischenbericht der Enquête-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft zum Thema Sicherheit und Schutz im Netz“

Deutscher Bundestag, 13. Wahlperiode, Drucksache 13/11002

Computerspionage, Risiken und Prävention

Bundesministerium für Wirtschaft,

Dokumentation Nr. 444

Mit freundlicher Unterstützung von:

DATEV eG, www.datev.de; Norman Data Defense Systems GmbH, www.norman.de; Nokia Enterprise Solutions, www.nokia.com/ipsecurity/de; PSINet Germany GmbH, www.psineteurope.de; SAP AG, www.sap.com; SECARTIS AG – eSolutions by Giesecke & Devrient, www.secartis.com; secunet Security Networks AG, www.secunet.com; Siemens AG, www.siemens.com



Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) vertritt 1.300 Unternehmen, davon gut 700 als Direktmitglieder, mit ca. 120 Mrd. Euro Umsatz und etwa 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content. Mehr als 500 Direktmitglieder gehören dem Mittelstand an. BITKOM setzt sich insbesondere für eine Verbesserung der ordnungsrechtlichen Rahmenbedingungen in Deutschland, für eine Modernisierung des Bildungssystems und für die Entwicklung der Informationsgesellschaft ein.



Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 - 0
Fax: 030/27 576 - 400

bitkom@bitkom.org
www.bitkom.org