www.hessen-infoline.de

IT-Sicherheit für den Mittelstand

Leitfaden zum Thema IT-Sicherheit

Band 38

hessen »
Hier ist die Zukunft

media

hessen-media Band 38

Schriftenreihe der Landesinitiative hessen-media

Band 1 Projektdokumentation

Band 2 Online-Anbieter in Hessen

Band 3 Software-Dialog Hessen (1)

Band 4 Leitfaden zur Einführung eines Qualitätsmanagementsystems in Software-Unternehmen

Band 5 Leitfaden zum Aufbau eines Ratingsystems für Software-Unternehmen in Hessen

Band 6 Leitfaden für ein kennzahlengestütztes Finanz- und Projektcontrolling für DV-Beratungs- und Software-Unternehmen

Band 7 Leitfaden Webdesign

Band 8 Medienmanagement in Schulen

Band 9 Leitfaden „Software-Qualitätsmanagementsystem für den Maschinen- und Anlagenbau"

Band 10 Software-Dialog Hessen (2) – Software-Trends

Band 11 Analyse des softwaretechnischen Problemlösungsbedarfs der Medienwirtschaft in Hessen

Band 12 Entwicklung eines Konzeptes für die Errichtung eines Software-Kompetenz-Netzwerks für die chemisch-pharmazeutische Industrie

Band 13 Hessische Kommunen im Internet

Band 14 Strategisches kennzahlengestütztes Controlling für kleine und mittlere DV-Beratungs- und Softwareunternehmen

Band 15 Die virtuelle Universität

Band 16 Leitfaden eShop

Band 17 Software-Dialog-Hessen (3)

Band 18 Leitfaden zur Anwendung eines Ratingsystems für IT-Unternehmen in Hessen

Band 19 Hessische Handwerker entdecken das Internet

Band 20 eShop-Software

Band 21 Der Telekommunikationsmarkt in Hessen

Band 22 Leitfaden Webdesign international

Band 23 Bildung ans Netz

Band 25 Kompetenzzentren und Onlinedienste im Schulwesen – Beispiele für hessen-media Projekte

Band 26 Hessen-infoline-Netzwerk

Band 27 Entwicklung und Einsatz elektronischer Medien als Lehr- und Lernmittel an hessischen Hochschulen

Band 28 eShops in Hessen

Band 29 Kasseler Praxis-Dialog Tele@rbeit Analysen · Erfahrungen · Positionen

Band 30 TELEHAUS WETTER ein TeleServiceZentrum

Band 31 e-Learning für KMU – Neue Medien in der betrieblichen Aus- und Weiterbildung

Band 32 Gefunden werden im Internet

Band 33 Recht im Internet

Band 34 ASP: Mehr als nur Mietsoftware

Band 35 ePaymentsysteme – Bezahlen im Internet

Band 36 Wirtschaftsförderung und Standortmarketing im Internet

Band 38 IT-Sicherheit für den Mittelstand

Hessisches Ministerium für Wirtschaft,
Verkehr und Landesentwicklung
Geschäftsstelle hessen-media
www.hessen-media.de

IT-Sicherheit für den Mittelstand

Leitfaden zum Thema IT-Sicherheit
(inkl. einem Verzeichnis hessischer IT-Sicherheitsanbieter)

Olaf Jüptner
Christoph Busch
Stephan Wolthusen
Isabel Münch
Hubertus Gottschalk
Sebastian Hummel

Hessisches Ministerium für
Wirtschaft, Verkehr und
Landesentwicklung

InvestitionsBank Hessen AG (IBH)
Abraham-Lincoln-Straße 38-42
65189 Wiesbaden

Telefon 0611/774-231
Telefax 0611/774-385
eMail info@hessen-infoline.de
Internet www.hessen-infoline.de

Redaktionsteam:
Wolf-Martin Ahrend
Sebastian Hummel
Olaf Jüptner
Gabriele Medewisch (Hessisches Ministerium
für Wirtschaft, Verkehr und Landesentwicklung)

CIP-Kurztitelaufnahme der Deutschen Bibliothek

IT-Sicherheit für den Mittelstand: Leitfaden zum
Thema IT-Sicherheit / Wolf-Martin Ahrend;
Sebastian Hummel; Olaf Jüptner. … Wiesbaden:
Hessisches Ministerium für Wirtschaft,
Verkehr und Landesentwicklung,
Geschäftsstelle hessen-media, 2002
(hessen-media; Bd. 38)
ISBN 3-936598-38-X

in Zusammenarbeit mit hessen-infoline

Layout/Satz: WerbeAtelier Theißen, Lohfelden
Druck: Völker & Ritter GmbH, Marburg

Das Internet wird in immer stärkeren Maße als Medium für alle Formen des Geschäftsverkehrs genutzt. Dabei ist die Informationstechnologie mit ihren schier grenzenlosen Möglichkeiten und ihrer rasant gewachsenen Bedeutung anfällig für Ein- und Angriffe von außen geworden. Deshalb muss dem Thema IT-Sicherheit eine zentrale Rolle zugewiesen werden, doch noch immer wird vielerorts die Bedeutung der Sicherheit unterschätzt. Oftmals sind Informationen und Prozessabläufe nur unzureichend geschützt und es reichen schon kleinere Vorfälle, um ganze Wirtschaftszweige lahm zu legen.

Insbesondere kleine und mittlere Unternehmen haben sich in der Vergangenheit zu wenig mit dem Themenkomplex IT-Sicherheit auseinander gesetzt. Um diese Unternehmen zu sensibilisieren, wurde im Rahmen der hessen-media Schriftenreihe der vorliegende Wegweiser erarbeitet. Er stellt die Bausteine einer erfolgreichen IT-Sicherheitspolitik vor und beinhaltet ein Verzeichnis hessischer Anbieter auf dem IT-Sicherheitsmarkt.

Wir freuen uns, dass Hessen, einer der wichtigsten IT-Standorte der Bundesrepublik, gerade auf diesem sehr wesentlichen Sektor führend ist und „hessen » hier ist die Zukunft“ auch für zeitgemäße und innovative Sicherheitsberatung und Sicherheitsprodukte steht.

Dieter Posch, Hessischer Minister für
Wirtschaft, Verkehr und Landesentwicklung

Inhalt

Vorwort **V**

1 Warum IT-Sicherheit? **1**
Olaf Jüptner, InvestitionsBank Hessen AG

1.1 Was versteht man unter IT-Sicherheit? 2

1.2 Potenzielle Gefahren und ihre Ausprägungen 4

1.3 Auswirkungen von Sicherheitsvorfällen 7

2 IT-Sicherheit – wie geht das? **9**
Christoph Busch und Stephan Wolthusen, CAST-Forum

2.1 Die Sicherheitspolitik 10

2.2 Schützenswerte Güter / Werte 17

2.3 Vorgehensweisen 22

2.4 Firewalls und andere Sicherheitsmechanismen für Netze 27

2.5 Zusammenfassung 33

3 IT-Grundschutz nach BSI – eine gute Basis **35**
Isabel Münch, Bundesamt für Sicherheit in der Informationstechnik (BSI)

4 IT-Sicherheit – was kostet das? **43**
Hubertus Gottschalk, Leiter T-Com-Sicherheit, Deutsche Telekom AG

5 Übersicht über den IT-Sicherheitsmarkt in Hessen **48**
Sebastian Hummel, InvestitionsBank Hessen AG

6 Anbieterübersicht **52**

7 Glossar **81**

8 Stichwortverzeichnis **88**

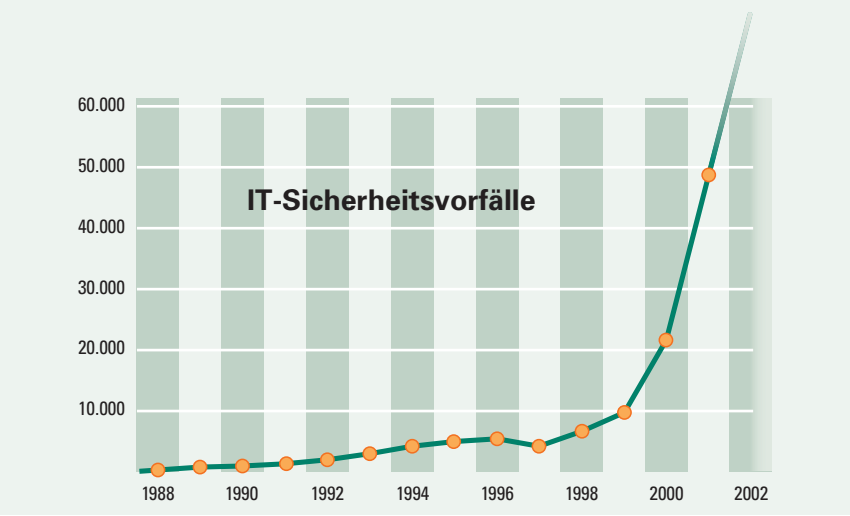
9 Die Aktionslinie hessen-infoline **90**

10 hessen-media: Eine Initiative stellt sich vor **91**

1 Warum IT-Sicherheit?

Olaf Jüptner, InvestitionsBank Hessen AG

Das Thema Sicherheit ist insbesondere seit dem 11. September 2001 in das Bewusstsein der Öffentlichkeit gerückt. Auch auf den dort eigentlich kaum berührten Aspekt der IT-Sicherheit hat diese Aufmerksamkeit ausgestrahlt. Dabei hat sich die Zahl der IT-Sicherheitsvorfälle bereits in den vergangenen Jahren exponentiell entwickelt.



Gemeldete IT-Sicherheitsvorfälle bei www.cert.org.

Zusätzlich haben sich die Rechtsvorschriften für die Unternehmensvorsorge verschärft, KonTraG lautet hier ein wichtiges Stichwort (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich). Geschäftsführern und Vorständen werden hierin neue persönliche Verantwortlichkeiten zugeschrieben.

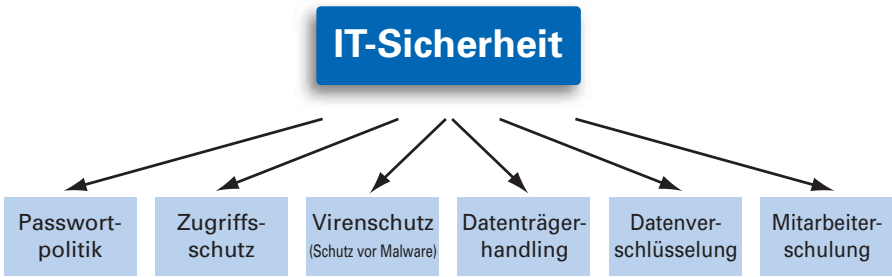
IT-Sicherheit kann immer nur ein Bestandteil der Unternehmenssicherheit sein und muss in einer vernünftigen Relation zur Wichtigkeit der unternehmenskritischen Geschäftsprozesse oder Werte stehen. Große Unternehmen haben hier sicherlich Skalenvorteile gegenüber den Mittelständlern, für die dieser Leitfaden konzipiert ist. Dennoch sind auch mittelständische Unternehmen immer wieder mit verschiedensten Sicherheitsproblemen konfrontiert, von denen sich viele Probleme bereits mit wenig Aufwand vermeiden lassen.

Nach einer Einführung zum Warum und Was soll es in dieser Broschüre um die ersten Schritte zur IT-Sicherheit im eigenen Unternehmen gehen – von der Bestandsaufnahme schützenswerter Güter, Prozesse und Werte über die Risikoanalyse zur Formulierung einer Sicherheitspolitik bis hin zu Sicherheitsmaßnahmen. Eine Methode, die des BSI-Grundschutzes, wird genauer vorgestellt und lässt sich auch bei erfolgreichem Durchlaufen zertifizieren – eine Möglichkeit, sich als solider und innovativer Geschäftspartner zu positionieren. Auch dem Thema Kosten versucht sich diese Veröffentlichung zu nähern. Ein wesentlicher Mehrwert der Broschüre besteht sicherlich auch in dem Anbieterverzeichnis hessischer IT-Sicherheitsunternehmen, das Anwendern die Kontaktaufnahme erleichtern soll. Die entsprechende Datenbank sowie weitere Informationen sind auch im Internet unter **www.hessen-infoline.de/sicherheit** verfügbar.

1.1 Was versteht man unter IT-Sicherheit?

IT-Sicherheit wird verstanden als ein Bestandteil der Unternehmenssicherheit. Hierzu gehören u.a. auch Themen wie Gebäude- und Zugangssicherheit, Personalsicherheit, Datenschutz und -sicherheit, Vertrags- und Finanzierungssicherheit, Prozesssicherheit. Alle sind dabei mehr oder weniger intensiv untereinander, also auch mit der IT-Sicherheit, gekoppelt.

Betrachten wir die IT-Sicherheit näher, kann man sie wie folgt untergliedern:



Ohne eine gute Passwortpolitik ist ein wirksamer Zugriffschutz kaum möglich. Wo immer es technisch möglich ist, eine Mindestqualität und -aktualisierungsfrequenz für Passwörter vorzuschreiben (etwa in Firmennetzwerken und Betriebssystemen von Einzelrechnern wie **Webserver** und Laptop), sollte diese Option genutzt werden. Beispielsweise können Passwörter mit mindestens acht Zeichen, darunter mindestens ein Sonderzeichen, durchgesetzt werden, die maximal einen Monat oder 100 Nutzungen lang gültig sind.

Zur Sicherung des Zugriffsschutzes werden **Firewalls**, **Intrusion Detection Systeme** und eine detaillierte Nutzerrechtevergabe eingesetzt, die in Kapitel 2.4 ausführlicher erläutert werden. Auf Virenschutz oder Schutz vor sogenannter **Malware** wird im folgenden Unterkapitel eingegangen.

Auch beim Datenträgerhandling lassen sich kurz wichtige Punkte ansprechen. Natürlich ist es essenziell, **Backups** von allen Datenträgern im Unternehmen periodisch zu erstellen, die Frequenz und das Verfahren hierfür hängen jedoch von der Aktualisierungsfrequenz der Daten und ihrer Wichtigkeit für das Unternehmen ab. Bei statischen Websites kann eine monatliche manuelle Sicherung ausreichen, bei eCommerce-Transaktionsdaten kann eine stündliche, automatische, inkrementelle Sicherung erforderlich sein. Diese letzte Sicherungsmethode würde dann nur die Veränderung der letzten Stunde im Datenbestand speichern.

Für Firmennetzwerke ohne besondere Anforderungen hat sich ein nächtliches, inkrementelles Backup bewährt – das Augenmerk sollte aber auf der Frage liegen: Wie schnell kann ich den letztmöglichen Betriebszustand wiederherstellen? Hierfür sind zusätzlich etwa die Verfügbarkeit notfallgeschulter Mitarbeiter, die Verfügbarkeit der Backups und die Gesamtkonzeption der IT-Infrastruktur zu bewerten. Ebenfalls zum Datenträgerhandling gehört die Ausfallsicherheit der Systeme, die zumeist durch unabhängige Stromversorgung (USV) und Redundanz mehrerer Komponenten (z.B. Festplatten) erreicht wird.

Datenverschlüsselung empfiehlt sich nicht nur für Festplatten von Laptops und die vertrauliche Kommunikation wichtiger Informationen per eMail oder **VPN** – auch Datensicherungsbänder oder der firmeninterne Datenverkehr über Luftschnittstellen sollte ausreichend sicher verschlüsselt werden, um von einer Basisvertraulichkeit der eigenen Daten auszugehen.

Als der Autor der Museumsdatenbank des Zentrums für Neue Norwegische Kultur starb, rief dessen Direktor die Internet-Gemeinde auf, das Passwort der Datenbank zu knacken, um wieder an wichtige Dokumente gelangen zu können. Die richtige Antwort kam am gleichen Tag.

Ganze fünf Monate hatten **Cracker** *Zugriff auf den Server einer Amazon.com-Tochter und stahlen Adressen und Kreditkartennummern von 98.000 Kunden.*

Im Februar 2000 startete der 15jährige Cracker „Mafiaboy" einen großangelegten **DDOS-Angriff** *auf Websites wie Dell, Amazon und eBay und verursachte damit einen Schaden von über 1,5 Milliarden Euro.*

Am 13.10.2001 fiel Amazon.com für mehrere Stunden aus. Bereits im Vormonat hatte Amazon technische Probleme.

In Londoner Taxis wurden im I. Halbjahr 2001 29.000 Laptops, 1.300 **PDAs** *und 63.000 Mobiltelefone vergessen.*

Alle Sicherheitsmaßnahmen können jedoch ausgehebelt werden, wenn die Mitarbeiter nicht ausreichend sensibilisiert und geschult sind. Hierzu mehr in Kapitel 1.2.2.

1.2 Potenzielle Gefahren und ihre Ausprägungen

1.2.1 Viren, Würmer und Trojaner

Immer wieder schaffen es **Computerviren** und **-würmer** aufgrund ihrer zunehmend hohen Ausbreitungsgeschwindigkeit und ihres hohen Schadenspotenzials in die allgemeinen Nachrichten – sie heißen beispielsweise Melissa, I-love-you, Nimbda oder Code Red. Sie gehören zu dem Oberbegriff Malware oder Malicious Code. Malware umfasst kleine Programme (Würmer) oder Programmteile (Viren), die schädliche Aktivitäten auf Rechnern oder in Netzen entfalten. Viren und Würmer „nisten sich in den Computer ein" und verbreiten sich dann selbst weiter – häufig auch in anderer äußerer Gestalt, etwa einer eMail mit anderem Titel und Dateianhang. **Trojaner** werden zumeist über Viren oder Würmer verbreitet, ihre Hauptaufgabe ist es jedoch häufig, Daten (Passwörter o. ä.) zu sammeln und bei Gelegenheit an einen „toten Briefkasten" zu schicken, aus dem der Angreifer dann die Informationen abholt. Trojaner enthalten also ebenfalls Programm(teil)e.

Wie kommt es nun zur Infektion des eigenen Computers oder Netzwerkes mit Malware? Früher waren es häufig von zu Hause mitgebrachte Disketten, weshalb Firmen dazu übergingen, Diskettenlaufwerke aus den Arbeitsplatzcomputern auszubauen, wenn diese nicht wirklich zwingend waren. Auch wenn dies immer noch eine sinnvolle Überlegung sein kann, liegt das Hauptproblem heute bei eMails.

Eigentlich stellt eine rein textbasierte eMail kein Sicherheitsrisiko dar, das Risiko liegt in den Anhängen (Attachments) bzw. in den in HTML-Mails eingebetteten ausführbaren Elementen. Leider sind immer noch häufig eMail-Programme so eingestellt, dass sie Anhänge direkt und ohne separate Nutzeraktivierung anzeigen und auch Elemente wie **ActiveX**, **Java** und **JavaScript/Jscript** in HTML-Mails zulassen.

Browser und eMail-Programme sollten (wenn kein besonderer Grund vorliegt) so eingestellt sein, dass sowohl ActiveX als auch Java nicht zugelassen werden. Auch JavaScript/Jscript können Sicherheitsprobleme verursachen, andererseits lässt sich dann eine Vielzahl von Websites nur noch eingeschränkt nutzen.

Typische eMail-Anhänge sind Office-Dokumente (Dateiendung etwa .doc, .xls oder .ppt), die sogenannte Makros enthalten können, also ausführbare Programmelemente. Der Melissa-Virus ist ein solches Word-Makro und verursachte 1999 einen geschätzten Schaden zwischen 93 und 395 Millionen US-$. Aber auch eine Vielzahl anderer Dateitypen (z.B. .exe, .bat, .zip, .vb, .vbs, .js) können **Viren** enthalten. So verursachte die eMail mit dem Titel „I love you" und einem .vbs-Anhang im Jahr 2000

einen geschätzten Schaden von 700 – 6700 Millionen US-$. Beeindruckend ist teilweise auch die Geschwindigkeit, mit der sich heutige Viren ausbreiten: So infizierte Nimbda allein 2,2 Millionen Rechner in den ersten 24 Stunden.

Leider gibt im Endeffekt nicht einmal die Dateiendung immer einen zuverlässigen Hinweis auf den Dateityp, so dass grundsätzlich immer gilt:

1. eMails von unbekannten Absendern und mit sehr vertraulichem, geheimnisvollem oder werblichem Titel sofort ungeöffnet löschen.
2. eMail-Programm so einstellen, dass Anhänge nur auf ausdrücklichen Wunsch des Nutzers angezeigt werden.
3. Ein ständig(!) aktualisiertes Antivirenprogramm nutzen und alle Anhänge (idealerweise automatisiert) auf Viren überprüfen, im Zweifelsfall ein zweites Programm hinzuziehen.
4. Sollte der überprüfte eMail-Anhang aus einer gepackten Datei (Endung z. B. .zip) bestehen, so sollten auch alle enthaltenen Dateien nach dem Auspacken mit dem Antivirenprogramm überprüft werden.

Eine wichtige Verwendung von **Trojanern** gilt es zusätzlich besonders zu beachten: **Hacker** nutzen häufig Zwischenstationen für ihre Angriffe. So wird im Internet automatisch nach unsicheren Rechnern gesucht, diese werden dann mit Trojanern infiziert, die entweder weitere Rechner infizieren oder direkt als Angriffsplattform der Hacker genommen werden. Hat der Hacker dann eine ausreichende Zahl von Stationen eingerichtet, kann er alle zum gleichen Zeitpunkt aktivieren und so etwa die von ihm ausgewählte Website lahmlegen (Distributed Denial of Service, DDOS) und damit einen nachhaltigen Umsatzausfall oder Imageverlust erreichen. Wird der Zielrechner nur von einem anderen Rechner angegriffen (Denial of Service, DOS), ist der Angreifer aber meist dennoch nicht einfach zu ermitteln, da er diesen Angriff meist über mehrere Zwischenrechner vorbereitet. Die Wichtigkeit dieser Trojaner-Verwendung liegt darin begründet, dass der Besitzer einer Zwischenstation für den indirekt durch seine Nachlässigkeit verursachten Schaden haftbar gemacht werden kann.

Der Webhoster Strato wurde am 25. Juli 2002 durch eine massive **DOS-Attacke** *für sieben Stunden lahmgelegt. Trotz aktiver Gegenmaßnahmen von Beginn an wechselte der Angreifer seine Strategie sehr schnell. Er konnte in den Folgetagen nicht identifiziert werden.*

1.2.2 Skript Kiddies, Hacker, Mitarbeiter

Im Internet gibt es eine Vielzahl von kostenlosen und kostenpflichtigen Skripten und Programmen zur Sicherheitsüberprüfung eigener Websites und Netzwerke. Zumeist lassen sich diese Programme aber auch von unautorisierten Personen einsetzen, die dann „erfolgreiche" Überprüfungen für ihre schädlichen Zwecke einsetzen.

„Skript Kiddies" machen genau dies; ihnen kommt es dabei auf eine möglichst hohe Zahl „geknackter" Sites an, mit der diese meist jugendlichen Angreifer (Kiddies) in ihrem Kreise prahlen können. Hierfür müssen sie ihren Erfolg irgendwie dokumentieren. Sie verändern entweder eine Seite eines **Webservers** oder legen Dateien in Netzwerken ab und verbreiten die Zugangspasswörter zu diesen Dateien.

Hacker und Cracker werden häufig ähnlich beschrieben. Zumeist werden aber unter Hackern diejenigen verstanden, die nur die Technik eines Systems kennenlernen und überprüfen wollen. Cracker dagegen wollen in den angegriffenen Systemen auch einen Schaden anrichten, etwa Daten ändern oder löschen. Hier kommt dann auch bald der Übergang zur Wirtschaftsspionage, wenn Hacker oder Cracker ihre Erkenntnisse Konkurrenzfirmen anbieten oder gar schon von diesen beauftragt wurden.

Wirtschaftsspionage ist selbstverständlich um so häufiger je größer oder innovativer ein Unternehmen ist, aber auch Mittelständler berichten von Auftragsvergaben in befreundeten Ländern, in denen sie klare Anzeichen von Wirtschaftsspionage entdecken konnten und dann auch den Auftrag gegen einheimische Konkurrenz verloren. Sowohl Russland als auch die Vereinigten Staaten verfolgen zugegebenermaßen Wirtschaftsspionage als aktives Ziel. Die USA (dort die **NSA**) betreibt zusammen mit Kanada, Großbritannien, Australien und Neuseeland das globale Kommunikationsabhörsystem Echelon, so die Feststellung des EU-Parlaments. Der dem Parlament vorgelegte Bericht beschreibt auch Berichte über den Einsatz von NSA und CIA, französischem DGSE und deutschem BND. Das von der CIA unterstützte Advocacy Center des US-Handelsministerium hat nach eigenen Angaben schon hunderten US-Unternehmen geholfen, öffentliche Aufträge im Ausland zu bekommen. Selbstverständlich wird Wirtschaftsspionage nicht nur von Geheimdiensten, sondern auch und vor allem von Wirtschaftsunternehmen betrieben.

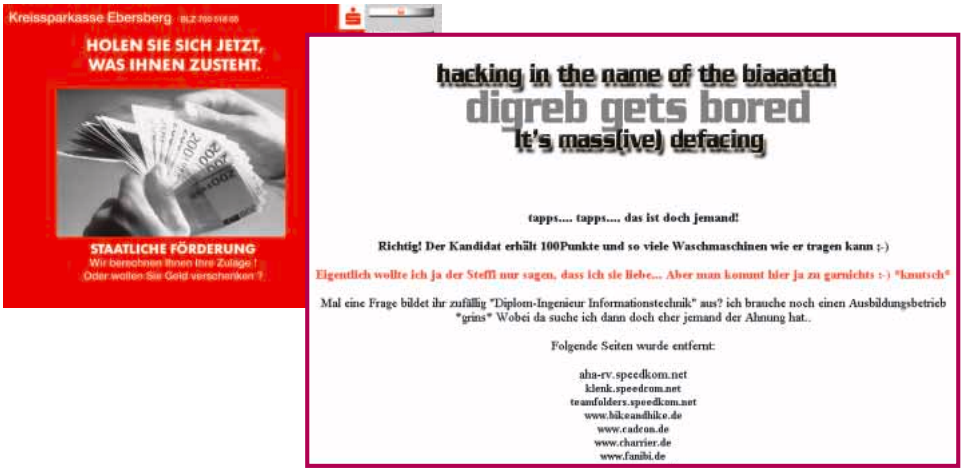
Die Mitarbeiter des eigenen Unternehmens gehören natürlich zu allermeist nicht zu den unternehmensschädigenden Personen. Dennoch geht der allergrößte Teil der Sicherheitsvorfälle auf unsachgemäße Bedienung, Vernachlässigen der Sicherheitsvorschriften, telefonische Auskunftserteilung von unautorisierten Interna u. ä. zurück. Natürlich gibt es auch die Mitarbeiter, die dem Unternehmen aufgrund von

innerer oder durch das Unternehmen ausgesprochener Kündigung schaden wollen. Allerdings sollte man die Mitarbeiter nicht durch überzogene Sicherheitsforderungen demotivieren.

Ein gut geplanter Sicherheitsprozess sensibilisiert, schult und motiviert die Mitarbeiter in Sicherheitsfragen und bezieht diese auch in den Planungsprozess ein. Wenn auch aus vielerlei Gründen nicht alle Mitarbeiter in den Prozess direkt einbezogen werden können, sollten sie doch in die Lage versetzt und aufgefordert werden, dem / den aus der Gruppe/Abteilung Beauftragten mögliche Sicherheitslücken mitzuteilen. Ein Sicherheitsbeauftragter sollte diesen Prozess moderieren und koordinieren und hierfür der direkten Unterstützung der Geschäftsführung / des Vorstandes sicher sein können. Einen besonderen Schulungsbedarf für Fragen der IT-Sicherheit sollte man in der IT-Abteilung einplanen.

1.3 Auswirkungen von Sicherheitsvorfällen

Zunächst müssen bei Sicherheitsvorfällen die Kosten der Behebung berücksichtigt werden. Das kann sich auf das Einspielen eines selektiven oder kompletten **Backups** begrenzen, über das händische Überarbeiten aller einzelnen Computer des Unternehmens bis hin zur Neuplanung und -entwicklung von durch Geheimnisverrat kompromittierten Innovationen gehen. In anderen Fällen lässt sich recht direkt ein Umsatzausfall durch das eCommerce- / eBusiness-System errechnen, darüber hinaus kann ein IT-Problem eines Zulieferers zur Auslistung beim Abnehmer führen.



Defacement einer regionalen Website am 18.7.02 – vorher, nachher

Ein schwerer quantifizierbarer Schaden entsteht möglicherweise durch einen Imageschaden, etwa im Zusammenhang mit der ungewollten Veränderung der eigenen Website-Homepage. Defacement nennt man in der Fachsprache diesen meist von **Skript Kiddies** verursachten Angriff.

Noch ernster muss man die Haftungsproblematik in mehrerlei Hinsicht nehmen: die Geschäftsführung / der Vorstand ist für die Risikovorsorge des Unternehmens gemäß **KonTraG** verantwortlich, d. h. er ist für die Einrichtung eines Prozesses für die Etablierung der Unternehmenssicherheit einschließlich der IT-Sicherheit verantwortlich und kann für das Fehlen dieses Prozesses persönlich haftbar gemacht werden. Darüber hinaus ist das Unternehmen verantwortlich, wenn seine IT-Infrastruktur für Angriffe auf andere missbraucht wird und wenn die Infrastruktur nicht revisionsfähig ist, d. h. Besteuerungsgrundlagen nicht nachvollziehbar sind. Im letzten Fall kann dies eine äußerst ungünstige Steuerschätzung zur Folge haben.

Wenn man sich den Wert der eigenen unternehmenskritischen Prozesse anschaut und diese mit wohlkalkulierten Maßnahmen absichert, lässt sich also eine sinnvolle Sicherung des Gesamtunternehmens mithilfe der IT-Sicherheit erreichen.

2 IT-Sicherheit – wie geht das?

Christoph Busch und Stephan Wolthusen, CAST-Forum

Sicherheitsaspekte bei der Informationsverarbeitung werden zumeist erst dann berücksichtigt oder wahrgenommen, wenn die betroffene Organisation bzw. das Unternehmen einen erheblichen Grad an Abhängigkeit erreicht hat, oder aber sich ein Vorfall ereignet hat, der Abhängigkeit und Verwundbarkeit vor Augen führt. Solange Geschäftsprozesse oder sonstige Vorgänge auch ohne Schutzmaßnahmen durchgeführt werden können, ist aus betriebswirtschaftlicher Sicht die Motivation, Ressourcen in IT-Sicherheit zu investieren, eher beschränkt, wenn nicht aufgrund von externen Anforderungen wie der Testierbarkeit oder aber gesetzlicher Vorschriften und Verordnungen eine solche Motivation gegeben ist.

Schützenswerte Systeme und Infrastrukturen eines Unternehmens weisen meist eine beträchtliche Komplexität auf. Erschwerend kommt hinzu, dass bei einem meist inkrementellen Aufbau die Aspekte der Überschaubarkeit, Wartbarkeit, und insbesondere Sicherheit nicht oder zumindest nicht hinreichend berücksichtigt werden. Diese Komplexität sowie die Bestrebung, möglichst geringe Einflüsse oder gar Einschränkungen etablierter Geschäftsprozesse aufgrund von Anforderungen an die Sicherheit und Zuverlässigkeit entstehen zu lassen, sorgen dafür, dass die erforderlichen Analysen und Maßnahmen meist unüberschaubar erscheinen. Zudem sind als notwendig erkannte Maßnahmen nur schwer gegenüber den Nutzern der IT-Systeme und Infrastruktur zu rechtfertigen, da die unzureichend abgesicherten Verfahrensweisen oft lange Zeit etabliert sind. Hinzu kommt, dass Sicherheitsmaßnahmen primär als Kostenfaktor wahrgenommen werden, die ihre Existenz nur schwer rechtfertigen können, da selbst bei Erfolg stets ein Negativ bewiesen werden muss, d. h. dass die Maßnahmen hinreichend waren, um Angriffe abzuwehren oder aber dass die ergriffenen Maßnahmen ein notwendiges Minimum darstellen.

Sicherheitsmaßnahmen werden primär als Kostenfaktor wahrgenommen.

Aufgrund dieser Randbedingungen ist eine strukturierte Herangehensweise zur Handhabung der Komplexität, als Instrument für die Argumentation bezüglich der Notwendigkeit und Vollständigkeit der Maßnahmen, und für die Verifikation und Validierung bei einer späteren Überarbeitung selbst in kleinen und mittleren Unternehmen oder Dienststellen erforderlich. Der tatsächliche Umfang der einzelnen Schritte innerhalb eines solchen methodischen Vorgehens kann dabei signifikant variieren; obwohl ein hoher Detailgrad sicherlich wünschenswert ist, sind hier oft pragmatische Grenzen zu ziehen.

2.1 Die Sicherheitspolitik

Eine Sicherheitspolitik legt für alle Beteiligten verbindlich die Rahmenbedingungen fest, unter denen die IT-Systeme einer Organisation betrieben werden. Damit richtet sich die Sicherheitspolitik grundsätzlich an alle mit der Informationsverarbeitung Befassten oder (auch indirekt) Verantwortlichen. Dies bedingt, dass die erforderlichen Begriffe und Konzepte in einer Art dargestellt werden, die auch für nicht in diesem Bereich spezialisierte Mitarbeiter eingängig ist. Gegenstand einer Sicherheitspolitik sind damit zumindest:

- Eine Definition des Begriffs IT-Sicherheit für das Unternehmen, der Zielsetzungen und des Umfangs der Sicherheitspolitik sowie die Bedeutung der IT-Sicherheit für die Nutzung der Datenverarbeitungs- und Kommunikationsmechanismen
- Eine Aussage bezüglich der Zielsetzung der Geschäftsführung, IT-Sicherheit durchzusetzen
- Erläuterungen der Sicherheitspolitik, der Richtlinien, Standards, und Anforderungen an Befolgung der Anforderungen, die von besonderer Bedeutung für die Organisation sind, beispielsweise
- Einhaltung vertraglicher Verpflichtungen
- Einhaltung gesetzlicher Bestimmungen
- Aus- und Fortbildung der Mitarbeiter im Bereich IT-Sicherheit
- Bestimmungen zur Zulässigkeit privater Nutzung von IT-Systemen
- Vorbeugung und Erkennung von **Computerviren** und **Trojanischen Pferden**
- Verfügbarkeitsplanung
- Konsequenzen der Verletzung der Sicherheitspolitik, insbesondere Sanktionen bei Nichteinhaltung durch Mitarbeiter
- Bestimmung der allgemeinen und spezifischen Verantwortungen für die Sicherstellung der IT-Sicherheit, z.B. Anforderungen an Berichterstattung und Meldung bei Sicherheitsverletzungen
- Verweise auf maßgebliche weiterführende Dokumente wie z.B. bereichsspezifische Sicherheitspolitiken oder Dokumente zur technischen Realisierung der allgemeinen Sicherheitspolitik

Die eigentliche Schwierigkeit bei der Erstellung einer Sicherheitspolitik ist eine Ausgewogenheit eines allgemeinen Dokumentes, das auf hinreichend hoher Abstraktionsebene die Probleme und daraus resultierenden Vorgehensweisen zur Sicherung der Werte der Organisation ableitet, gleichzeitig aber nicht derart abstrakt ist, dass eine Abbildung der Sicherheitspolitik auf die technischen Maßnahmen zur Durchsetzung dieser Politik nicht mehr offensichtlich ist.

Die eigentliche Schwierigkeit bei der Erstellung einer Sicherheitspolitik ist die Ausgewogenheit.

Gegenstand der Sicherheitspolitik ist nicht die technische Realisierung; dies hat zwei Gründe: Der erste Grund ist, dass die formulierte Sicherheitspolitik ein Dokument ist, das von nicht technisch orientierten Entscheidungsträgern vollständig unterstützt werden muss. Dieser Personenkreis ist nur bedingt dazu befähigt, eine ausgewählte technische Realisierung einer alternativen Realisierungsvariante vorzuziehen. In jedem Fall muss aber eine technische Maßnahme auf eine Zielsetzung bzw. ein Teilziel der Unternehmenspolitik bzw. des Schutzes von Werten zurückgeführt werden. Bei einer reinen Angabe technischer Maßnahmen ist dies in der Regel nicht ersichtlich.

Der zweite Grund ist die Lebenserwartung sowie der Lebenszyklus eines derartigen Dokumentes. Aufgrund des beteiligten Personenkreises wird erhebliche Zeit vom Entwurf einer detaillierten integrierten Politik und Realisierung bis zur Zustimmung aller Entscheider vergehen und damit der Realisierungsplan in der Regel vor in Kraft treten der Politik obsolet sein. Selbiges gilt für Revisionen; hier ist häufig in der technischen Realisierung auf neue, ad hoc aufgetretene Bedrohungen zu reagieren.

Die Sicherheitspolitik regelmäßig aktualisieren

Sofern nicht auch die Sicherheitspolitik Änderungen Rechnung trägt, besteht stets die Gefahr, dass sie die Bedrohungen nicht mehr abdeckt oder Maßnahmen erfordert, die nicht mehr die gewünschten Resultate produzieren. Damit wächst die Bedrohung, dass selbst die noch relevanten Teile der Politik nicht mehr hinreichend ernst genommen werden. Die Sicherheitspolitik unterliegt daher stets sowohl ereignisbezogenen als auch periodischen Überarbeitungen.

Im Rahmen der Überarbeitung sollte dann jedoch auch geprüft werden,

- ob die Politik oder eine Änderung an der Politik messbare Auswirkungen hat (z. B. dokumentiert anhand von Sicherheitsvorfällen in einem Berichtszeitraum) und
- ob die Auswirkungen in vernünftiger Relation zu den Umsetzungskosten der Politik stehen. Dies betrifft sowohl Kosten der unmittelbaren Einführung, Wartung und Pflege technischer Maßnahmen zur Umsetzung als auch mittelbare Kosten, wie die mögliche Beeinträchtigung der Effizienz von Geschäftsprozessen.

Eine Sicherheitspolitik wird immer aus einer Risikoanalyse heraus erstellt. Im Idealfall lässt sich der zunächst abstrakte Begriff „Risiko" einfach darstellen als:

Risiko = Bedrohungswahrscheinlichkeit x Folgekosten

Diese Definition erfordert jedoch eine klare Identifikation der Bedrohungen, eine realistische Einschätzung der Wahrscheinlichkeiten und eine Quantifizierung der Kosten.

Bei der initialen Erstellung der Politik sollten in der Regel nicht zu viele Interessen beteiligt werden. Effektiverweise wird die Sicherheitspolitik von einer kleinen Gruppe qualifizierter Personen erstellt werden; anderenfalls besteht die Gefahr unrealistischer Anforderungen bzw. einer nicht mehr handhabbaren Größe der Politik aufgrund der Einbeziehung von Partikularinteressen. Insbesondere bei der Abwehr von letzterem ist eine Abschätzung der Kosten von Maßnahmen, die sich nicht direkt aus der Risikoanalyse begründen lassen, hilfreich.

Sofern die Erstellung einer Sicherheitspolitik durch die Geschäftsführung gedeckt ist, muss der Entwurf lediglich mit den Mitbestimmungsgremien (so vorhanden) abgestimmt werden; anderenfalls muss eine weitere Diskussion insbesondere über Verantwortungsbereiche folgen, was nicht immer zu optimalen Ergebnissen führt.

Inhalte der Sicherheitspolitik

Eine der wichtigsten Inhalte der Sicherheitspolitik ist die Festlegung von Verantwortung und Verantwortlichen im Bereich der IT-Sicherheit. Dabei ist unter anderem festzulegen,

- welche spezifischen Rollen und Verantwortungen einzelne Stellen und Personen für die IT-Sicherheit innerhalb der Organisation übernehmen

- welche Methoden für die Realisierung der allgemeinen IT-Ziele einzusetzen sind (z.B. etwa Verfahren für Risikoanalysen, Klassifizierungsschemata für Vertraulichkeitsstufen)
- welche weiterführende Maßnahmen innerhalb der Organisation durchzuführen sind (z.B. Schulung der Mitarbeiter)
- Mechanismen für die Berücksichtigung von Sicherheitsaspekten bei der Planung und Realisierung aller neu hinzukommender IT-Vorhaben
- Mechanismen für die Bewertung von spezifischen technischen Realisierungen der Sicherheitspolitik
- Verfahren für die Umsetzung der Sicherheitspolitik in technische Maßnahmen sowie die Kontrolle der Wirksamkeit und Effektivität dieser Umsetzung
- Vorgehensweise für die Aufnahme und Analyse von Sicherheitsvorfällen

Die Zuordnung von Verantwortung für den Schutz bestimmter Werte (insbesondere auch von Geschäftsprozessen) und für die Durchführung spezifischer sicherheitsrelevanter Vorgehensweisen zu Organisationseinheiten und Personen ist eine der politisch sensibelsten Vorgänge.

Die Rolle der Sicherheitspolitik besteht zunächst darin, allgemeine Regeln für derartige Zuordnungen zu finden, die auch bei der Identifikation neuer Risiken und Werte Anwendung finden können; sofern nötig kann die Politik bereits konkrete Regelungen auf niedrigeren Abstraktionsebenen treffen. Falls die Verantwortung an eine Unterorganisation oder Organisationseinheit delegiert wird, muss auch dies klar definiert sein.

Bereits bei der Einstellung von Personal, das mit IT-Systemen, insbesondere aber deren Verwaltung in Berührung kommt, ist darauf zu achten, dass die jeweils gültige Sicherheitspolitik oder aber daraus abgeleitete Richtlinien zur IT-Sicherheit zum Bestandteil der Vertragsbedingungen werden und der Mitarbeiter auf seine Rechte, insbesondere aber auch auf die Verpflichtungen innerhalb dieser Richtlinien und Sanktionsmaßnahmen bei Zuwiderhandlung hingewiesen wird. Entsprechendes gilt für Vertraulichkeitsvereinbarungen. Neben der Bekanntmachung der Sicherheitspolitik und verwandter Dokumente sollten dabei den Mitarbeitern Gefahren sowie die zur Gefahrenabwehr notwendigen technischen und organisatorischen Maßnahmen nahegebracht werden. Dies sollte auch beinhalten, dass ein Mitarbeiter eine Verletzung der vorliegenden Sicherheitsrichtlinien jederzeit an eine benannte Stelle – notfalls auch

Organisatorische Aspekte sind von entscheidender Bedeutung.

anonymisiert – melden sollte und dies als ausdrücklich erwünscht dargestellt wird. In sicherheitskritischen Bereichen kann dies dahingehend verschärft werden, dass eine ausdrückliche Meldepflicht bei Bekanntwerden einer Verletzung eingeführt wird.

In keinem Fall darf dies jedoch dazu führen oder auch nur so verstanden werden, dass Mitarbeiter (außer dem hierfür bestellten Personal) sich auf die Suche nach Verwundbarkeiten begeben. Der Hauptgrund hierfür ist, dass anderenfalls eine Sanktionierung von die Sicherheit gefährdendem Verhalten mangels Eindeutigkeit des Vergehens nicht möglich ist.

Sofern es sich nicht um direkte Anstellungsverhältnisse, sondern um Konstruktionen unter Beteiligung von Dritten handelt, sind entsprechende Rahmenvereinbarungen zwischen den beteiligten juristischen Personen zu treffen.

Diese organisatorischen Aspekte sind zwingend notwendig, um einerseits eine Verfolgung der Verantwortlichkeiten zu ermöglichen, andererseits ist das Auftreten eines kritischen Vorfalls der vermutlich ungünstigste Zeitpunkt, um derartige Fragen zu klären.

Die IT-Sicherheit eines physisch kompromittierten Systems kann in jedem Fall prinzipiell gebrochen werden, wenn geeignete und umfangreiche Ressourcen zur Verfügung stehen. Die physische Sicherheit bildet daher die Grundlage für weitere IT-bezogene Sicherheitsmechanismen und Maßnahmen. Hierbei ergibt sich zwangsläufig eine Überlappung mit Elementen, die über die reine Sicherheitspolitik hinausgehen, wie etwa die Sicherstellung der Infrastruktur (Stromversorgung, Klimatisierung, Brandschutz, etc.). Da jedoch physische Sicherheitsmaßnahmen indirekt mit anderen Aspekten der Absicherung (z. B. Notausgänge im Brandfall) kollidieren können, muss eine Sicherheitspolitik auch diese Bereiche berücksichtigen.

Die physische Sicherheit von IT-Systemen als Grundlage.

Der Schutz sensibler und kritischer Systeme sollte in einer räumlich geschichteten Struktur erfolgen, bei der jede einzelne Schicht ein weiteres Maß an Sicherheit beiträgt. Dabei sind die einzelnen Schichten klar zu identifizieren und voneinander abzugrenzen und Übergangsregeln zwischen den Bereichen (z. B. für reguläre Mitarbeiter zugängliche Bereiche und einem designierten Rechnerraum) zu definieren. Entsprechend der Sensibilität der einzelnen Bereiche können die Absicherungen und Zugangskontrollmechanismen unterschiedlich stark ausfallen.

Von besonderer Bedeutung sind Regelungen, die den Zugang von Dritten (z.B. Wartungstechniker und Mitarbeiter von anderen Unternehmen, die mit Arbeiten an relevanten IT-Systemen beschäftigt sind) regeln. Dabei sollten bei regelmäßigem Auf-

treten derartiger Konstrukte die Räumlichkeiten für betroffene Geräte und Systeme von den verbleibenden Räumen getrennt sein und die Zugangskontrolle separat erfolgen können (oder zumindest die Möglichkeit der Überwachung durch Aufsichtspersonal berücksichtigt werden); anderenfalls ist eine ständige Überwachungs- und Zuordnungsmöglichkeit von Personen und Handlungen kaum gegeben und kosten- und arbeitsintensive Schutzmaßnahmen gegen elektronische Angriffe über Netzwerke werden fragwürdig.

Erfassung der Abläufe und Risiken

Für eine korrekte Umsetzung der Sicherheitspolitik müssen unter anderem auch Regelungen für den täglichen Betrieb gefunden werden. Dies bedingt einerseits, dass die Abläufe hinreichend genau erfasst worden sind (was im Rahmen einer Risikoanalyse der Fall sein kann, die für die Sicherheitspolitik übernommen wird), und andererseits Betriebsvorgänge, die in der Sicherheitspolitik oder in weiterführenden Dokumenten genannt oder referenziert werden, dokumentiert und bei notwendigen Änderungen über einen Revisionsmechanismus gepflegt werden. Derartige Vorgänge und Handlungsanweisungen sollten als formale Dokumente betrachtet werden und mit entsprechender Sorgfalt gepflegt werden. Analog dazu sollte eine formalisierte Vorgehensweise bei Ausfällen und Sicherheitsproblemen eingerichtet werden; dies kann mit der Notfallplanung oder auch – bei hinreichend zur Verfügung stehenden Ressourcen – mit den Betriebshandbüchern kombiniert werden.

Ein weiterer wichtiger Aspekt, dessen Regelung in der Sicherheitspolitik erfolgen muss, stellen Zugriffskontrolle und Zugriffsrechte dar. Diese sollten sich aus den operativen Anforderungen ergeben; dabei ist festzulegen, welche Nutzer (bzw. Personen mit Rollen entsprechend den zugeteilten Aufgaben der Person) zu welchen Zugriffsklassen (oder Gruppen) gehören, auf welche Systeme (die ebenfalls als funktionale Gruppen beschrieben werden können) sie in dieser Rolle Zugriff haben und welche Rechte dabei (ausdrücklich) gewährt werden. Hinzu kommt, dass unter Umständen besondere rechtliche Randbedingungen für derartige Rechte zu berücksichtigen sind. Die Einrichtung neuer Nutzerkennungen darf dabei nur mit Zustimmung (oder auf Veranlassung) des für den Bereich zuständigen Verantwortlichen erfolgen. Über jede neu angelegte Nutzerkennung, deren Sperrung oder Löschung ist Buch zu führen; vorzugsweise auf einem nicht überschreibbaren Medium oder außerhalb des IT-Systems. Entsprechend sollten Regelungen vorhanden sein, um ausscheidenden Mitarbeitern bekannte Authentisierungsdaten zu ändern und die Durchsetzung dieser Regelung zu verifizieren.

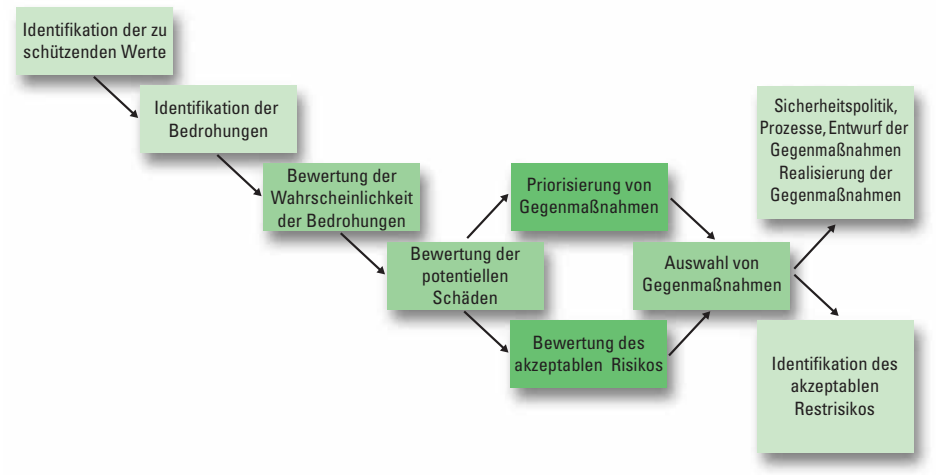
Im Rahmen einer Nutzeranmeldung muss der Nutzer explizit mit den Rechten und Verpflichtungen gemäß der Sicherheitspolitik vertraut gemacht werden. Dazu zählen insbesondere die für die Kennung spezifischen Eigenschaften und Sicherheitsrichtlinien. Die Kenntnisnahme hiervon sollte durch Abzeichnen des entsprechenden Formulars dokumentiert werden. Insbesondere fällt eine ausdrückliche Regelung über die Zulässigkeit (oder z. B. auch nur eine zeitliche Einschränkung) der Nutzung des IT-Systems für nicht eindeutig als dienstlich zu erkennende Vorgänge in diese Kategorie (z.B. private eMail, Web oder Telefon).

Von besonderer Bedeutung für die Relevanz von Revisionsdaten ist dabei eine Regelung, welche explizit die Verwendung von Nutzerkennungen durch mehrere Personen untersagt. Kennungen sollten darüber hinaus periodisch auf ihre weitere Gültigkeit hin geprüft und, sofern nicht ein expliziter Bedarf weiterhin besteht, gesperrt bzw. gelöscht werden.

Auch im Bereich der Vernetzung müssen explizite Regelungen aufgrund von operativen Anforderungen gefunden werden. Beispiele hierfür sind die explizite Anforderung von externen Netzwerk-Diensten (z. B. **File Transfer Protocol (FTP)**, Secure Shell (ssh) etc.), die Verknüpfung von Teilnetzen innerhalb einer Organisation oder auch die erforderliche Identifikation und Authentisierung bei Überschreiten von Netzwerk-Grenzen oder Inanspruchnahme von bestimmten Diensten. Eine besondere Rolle spielen hierbei mobile Geräte oder auch Heimarbeitsplätze. Bei beiden muss davon ausgegangen werden, dass sie unter die Kontrolle eines feindlichen Dritten gelangen; daher muss die Verwendung oder die Zugriffsberechtigung derartiger Systeme entsprechend eingeschränkt werden.

2.2 Schützenswerte Güter / Werte

Der Formulierung einer fundierten Sicherheitspolitik muss eine Risikoanalyse vorausgehen. Einer der entscheidenden Bestandteile der Risikoanalyse ist dabei zunächst die Bestimmung der Werte eines Unternehmens bzw. einer Organisation; erst anhand dieser Bestimmung können dann die Risiken für die einzelnen Prozesse sowie die Abhängigkeiten der Prozesse untereinander bestimmt werden. Dies ist notwendig, da nur begrenzte Ressourcen für Sicherheit zur Verfügung stehen und diese optimal eingesetzt werden müssen.



Der Begriff „Wert“ ist bewusst neutral gewählt; im Falle eines Unternehmens können dies z. B. die erforderlichen Geschäftsprozesse sein. Dabei besteht meist die erste Herausforderung darin, eine systematische Identifikation von tatsächlich erforderlichen Geschäftsprozessen vorzunehmen und sie von irrelevanten bzw. aus sekundären Gründen durchgeführten Prozessen zu trennen. Ebenfalls mit diesem Begriff bezeichnet werden können Geräte und feste Einrichtungen, die Bereitstellung eines Dienstes oder von Informationen oder auch die Reputation einer Einrichtung. Werte fallen dabei in der Regel in eine der folgenden Kategorien.

Unternehmenswerte / Kategorien

Vertrauliche Informationen: Hierunter fallen sowohl statische Daten wie z. B. Dateien oder Datenbanken als auch die Vertraulichkeit der Kommunikation von Daten. In einigen Anwendungen kann auch die Tatsache einer Kommunikation selbst vertraulich sein.

Verfügbarkeit von Ressourcen und Diensten: Hierunter fallen z.B. Dienste wie Dateisysteme, Verzeichnisdienste, aber auch mittelbar notwendige Ressourcen wie etwa die Klimatisierung eines Rechenzentrums.

Integrität von Informationen: Diese Position identifiziert die Sicherstellung der Korrektheit von Informationen sowie die Integrität der zur Verarbeitung dieser Informationen notwendigen Prozesse.

Ausrüstung: Hierunter fallen die zur Aufrechterhaltung des Betriebs notwendigen Werte:

- **Informations-Werte:** Diese Kategorie beinhaltet Datenbanken, Dateien, Dateisysteme, Dokumentation zu Systemen und Geschäftsprozessen, Anwender-Dokumentation, Aus- und Fortbildungsmaterial, Dokumentation für Katastrophenplanung, und Archivdaten.
- **Software:** Diese Kategorie beinhaltet Anwendungssoftware, Entwicklungswerkzeuge, Systemsoftware sowie sonstige Hilfsmittel.
- **Physikalische Werte:** In dieser Kategorie sind Rechnersysteme, **Periphere**, Kommunikationsgeräte (Router, Switches, Telephonanlagen, etc.), Datenträger sowie andere zum Betrieb des IT-Systems notwendige Geräte, beispielsweise Notstromaggregate oder Klimaanlagen, aufzuführen.
- **Externe Dienstleistungen:** Externe Dienstleistungen wie Kommunikationsanbindungen, Strom- und Wasserversorgung fallen in diese Kategorie.

Personal: Diese Komponente beinhaltet die Vertrauenswürdigkeit des Personals, insbesondere von Personen mit administrativer Verantwortung. Eine gewisse Doppelung gegenüber der physischen bzw. einer separaten Personal-Risikoanalyse ist dabei nicht zu vermeiden.

Dieser Schritt der Risikoanalyse stellt bereits die erheblichste Herausforderung dar, da bei der Identifikation von Abläufen, Informationen und Interaktionen häufig Abhängigkeiten von Komponenten untereinander existieren, die stillschweigend vorausgesetzt oder zum Teil auch vorab nicht bekannt sind und abgeleitet werden müssen.

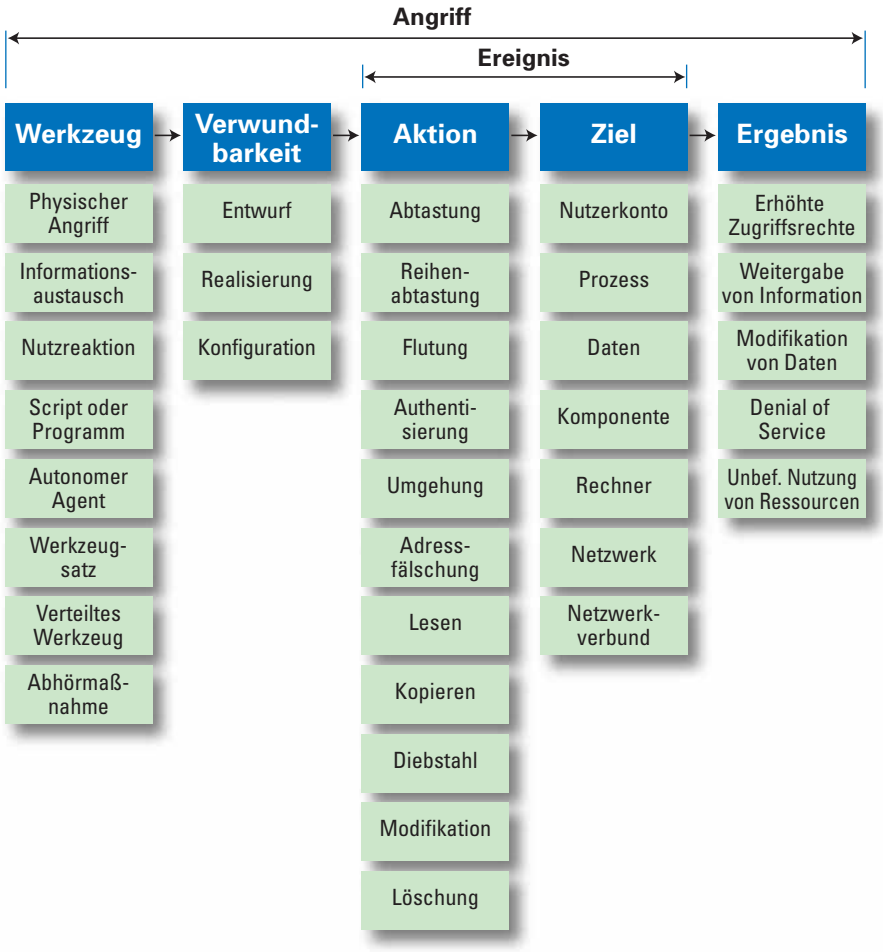
Der nächste Schritt in einer Risikoanalyse besteht darin, die Charakteristika der Bedrohungen, deren Quellen (zum Beispiel von Angriffen von beliebigen Ausgangspunkte versus Knoten aus eigenen Netzsegmenten) und Wahrscheinlichkeiten zu identifizieren. Dabei können für einen Wert mehrere Bedrohungen existieren. Die Wahrscheinlichkeiten für Bedrohungen sollten, wenn möglich, auf Basis von empirischen Daten ermittelt werden (z.B. aufgrund erfasster Statistiken); anderenfalls sind notwendigerweise stark qualitative Aussagen die Folge.

Bei der Bewertung der Bedrohungen muss ebenfalls berücksichtigt werden, dass durch die Einführung von Gegenmaßnahmen Rückkoppelungen entstehen können, welche die Wahrscheinlichkeiten für eine oder mehrere Bedrohungen sowohl positiv als auch negativ beeinflussen.

Daneben ist in vielen Fällen auch zu bewerten, welcher Quelle eine Bedrohung entspringt. Die Bedrohungswahrscheinlichkeit ist dabei ein Maß für die Wahrscheinlichkeit, dass eine Bedrohung in einen konkreten Angriff umgesetzt wird, die Quelle hingegen muss die Fähigkeiten und Motivationen der potenziellen Angreifer berücksichtigen.

Bei der Erstellung der Risikoanalyse sollte dabei selbst bei qualitativer Bewertung dokumentiert werden, welches Spektrum mit der qualitativen Aussage abgedeckt wird und wie die Einschätzung erreicht wurde, insbesondere eventuell vorgenommene Untersuchungen und Erfahrungswerte. Dies ist sowohl für eine Erstbewertung der Risikoanalyse auf Gültigkeit als auch für die zwingend notwendigen Neubewertungen erforderlich.

Angriffs-Taxonomie



Die Folgen oder Schäden, die den von einem IT-System bereitgestellten Diensten oder sonstigen Ressourcen in Folge einer eingetretenen Bedrohungssituation entstehen, sind je nach Art des betroffenen Wertes unterschiedlich. Es ist aber in jedem Fall festzuhalten, dass der Schaden nicht in Korrelation mit der Eintrittswahrscheinlichkeit einer Bedrohung zu setzen ist.

Günstiger als derartige qualitative Einschätzungen sind jedoch konkret quantifizierbare Schäden. Dies können z.B. verlorene Umsätze, Konventionalstrafen, Ausfälle

an Arbeitszeit oder die zur Wiederherstellung des Systems notwendigen Aufwendungen sein. In vielen Fällen wird es allerdings nicht gelingen, quantitative Bewertungen für Folgen wie Vertrauensverlust oder kompromittierte Informationen zu bestimmen.

Das Risiko ergibt sich – wie schon oben definiert – aus Bedrohungswahrscheinlichkeit und Folgekosten, wobei der Einsatz von quantitativen Methoden erforderlich ist.

Stehen diese Daten nicht zur Verfügung, ist insbesondere bei der Bestimmung der Bedrohungswahrscheinlichkeiten Vorsicht geboten; es besteht die Gefahr einer Konzentration von Gegenmaßnahmen auf nicht objektiv relevante Bedrohungen aufgrund subjektiver Einschätzungen. Ausgehend von den identifizierten Risiken kann so eine möglichst vollständige Liste der existierenden Risiken erstellt werden, die zur anschließenden Bestimmung des Restrisikos genutzt werden.

Restrisiken

Das Restrisiko stellt das Risiko dar, das die jeweils verantwortliche Stelle bereit ist zu tragen. Dies ist klar dann gerechtfertigt, wenn erforderliche Gegenmaßnahmen teurer sind als die kalkulierten Schäden. Selbst bei Bedrohungen mit sehr hohen Kosten als Konsequenz kann es günstiger sein, mittels einer Versicherungspolice die Folgekosten zu begrenzen. Die günstige Ausgestaltung einer derartigen Police für den Versicherungsnehmer wird maßgeblich von der Präzision und Vollständigkeit der Risikoanalyse und der Fähigkeit zur Dokumentation entsprechender Sorgfalt beim Schutz der Werte in Form einer Sicherheitspolitik beeinflusst.

Aufgrund der Entscheidung bezüglich der akzeptablen Risiken kann eine Priorisierung der möglichen Gegenmaßnahmen vorgenommen werden und aus den zur Verfügung stehenden Mechanismen zur Gegenwehr eine geeignete defensive Strategie entwickelt werden.

Für die eigentliche Erstellung der Risikoanalyse stehen eine größere Anzahl systematischer Verfahren bereit, die einerseits die Gefahr vermindern, im Laufe der Betrachtungen Elemente und Abhängigkeiten zu übersehen, andererseits auch in der Lage sind, Aussagen bezüglich Eintrittswahrscheinlichkeiten und besagten Abhängigkeiten zu treffen.

2.3 Vorgehensweisen

Für die Erstellung von Sicherheitspolitiken und den damit verbundenen Vorgängen existieren eine Reihe von Richtlinien, die zum Teil zu internationalen Standards erhoben wurden. Die Befolgung einer festen Methodik für die Durchführung von Risikoanalysen und die Erstellung von Sicherheitspolitiken ist von praktischem Vorteil. Obwohl eine Methodik nicht zwingend erforderlich ist zur Testierbarkeit des Prozesses, ermöglicht diese Vorgehensweise jedoch unter anderem einen Vergleich oder auch Abgleich mit anderen Sicherheitspolitiken. Zudem können auch neu hinzustoßende Mitarbeiter Vorgänge nachvollziehen und in den Prozess eingebunden werden.

2.3.1 ISO 17799

Mitte der 90er Jahre wurde der British Standard 7799 etabliert, der Vorgehensweisen für die Definition von Sicherheitspolitiken und deren Inhalt beschrieb; die 1999 erfolgte zweite Revision des Standards erlangte auch international Aufmerksamkeit und wurde schließlich im Dezember 2000 durch direkte Übernahme des ersten Teils von BS 7799 zu einem weltweit gültigen **ISO**-Standard (ISO 17799 – Code of Practice for Information Security Management). Der Standard befasst sich auf vergleichsweise abstrakter Ebene mit den folgenden Themenbereichen, die hier nur in Stichworten angegeben sind:

(1) Organisatorische Aspekte: Etablierung eines Arbeitskreises der Geschäftsführung zur IT-Sicherheit, Mechanismen für die Koordinierung der Durchsetzung der Sicherheitspolitik und Berücksichtigung der IT-Sicherheit bei Planung und Realisierung neuer Vorhaben, Bestimmung von Verantwortungsbereichen und Verantwortlichen, Kontakte zu Behörden, Dienststellen und Verbänden, Revision der Sicherheitspolitik durch externe Prüfer, Bestimmung von Berechtigungen für Dritte, insbesondere bei Outsourcing

(2) Erfassung von Werten und Klassifizierungsmechanismen: Bestandsaufnahme, Etablierung von Richtlinien für die Klassifizierung von Informationen und IT-Systemen, Handhabung sensibler Informationen und Datenträger

(3) Personal-Sicherheitsaspekte: Einbindung von IT-Sicherheitsaspekten in Personalverantwortung, Eignungsprüfung für Personal mit besonderen Rechten und Sorgfaltspflichten, Vertraulichkeitsvereinbarungen, Mitarbeiterschulungen und Weiterbildung, Berichtswesen bei Vorfällen, erkannten Schwachstellen in der IT-Sicherheit oder sonstigen auffälligen Problemen, Wirksamkeitsprüfung bestehender Maßnahmen, Disziplinarmaßnahmen bei Zuwiderhandlungen gegen die Sicherheitspolitik

(4) Physische Sicherheit und Umgebungsbedingungen: Absicherung des physischen Umfelds der IT-Systeme, Zugangskontrollen, Bereitstellung eines vor unbefugtem Zugriff und ungünstigen Umgebungsbedingungen geschützten Bereiches, Richtlinien für die Nutzung und den Zugang

zum geschützten Bereich, Schutzmaßnahmen gegen Umwelteinflüsse und fahrlässige Gefährdung, Schutz der Stromversorgung, Schutz von Verkabelung, Wartungs-Vorgehensweisen, Absicherung von Geräten außerhalb des Betriebsgeländes, Verhinderung der Weitergabe sensibler Informationen bei Wartung, Verkauf oder Ausmusterung von IT-Komponenten

(5) Kommunikation und laufender Betrieb: Richtlinien für die Handhabung sensibler Informationen auf physischen und elektronischen Medien sowie zur Verwendung von Zugriffskontrollen bei Verlassen des Arbeitsplatzes, für den Schutz vor Umwelteinflüssen und unbefugtem Zugriff geschützte Ablage sensibler Datenträger und Dokumente, Richtlinien für die Weitergabe oder Entfernung von Geräten und Datenträgern außerhalb des Betriebsgeländes, Verfahren für die Erfassung der Weitergabe

(6) Kontrollmechanismen: Dokumentation von Vorgehensweisen, Randbedingungen und Verantwortlichen, Verwaltung und Handhabungen von Änderungen an IT-Systemen, Verfahren für die Handhabung von Sicherheitsvorfällen, Vier-Augen-Prinzip für sensible Vorgänge, Verwaltung externer Dienstleister und Anlagen, die durch Dienstleister betrieben werden, Kapazitätsplanung und Abnahmevorgänge für neue IT-Komponenten, Schutz vor bösartiger Software, Datensicherung und Lagerung von Sicherungsmedien, Protokollierung von Fehlern und Wartungsvorgängen, Netzwerk-Überwachung und -Zugriffskontrolle, Handhabung und Vernichtung von Datenträgern, Sicherung von Informationen, die im System verarbeitet werden und des IT-Systems selbst, Vereinbarungen über Vernetzung und Austausch von Daten, Medien sowie elektronischer Geschäftsprozesse, Absicherung von eMail, Abgrenzung öffentlich zugänglicher IT-Systemkomponenten, Zugriffskontrollpolitik, Nutzerverwaltung, Rechteverwaltung, Auflagen für einzelne Nutzer zur Gewährleistung der IT-Sicherheit, Überwachung der Nutzung des IT-Systems

(7) Entwicklung und Wartung von IT-Systemen und Komponenten: Systematische Einbindung von Sicherheitsanforderungen in die Entwicklung von IT-Systemen und -Komponenten, Analyse und Spezifikation der Sicherheitsanforderungen, Sicherheitsaspekte für Anwendungsprogramme, Kryptographische Sicherheitsmechanismen, Integritätsschutz von Software in Betrieb, erforderliche Testdaten, Quellen und Entwicklungsumgebung für intern entwickelte Komponenten, Mechanismen für Änderungskontrolle an Systemen und Anwendungsprogrammen, Überwachung von Software-Entwicklung und Wartung in Outsourcing-Verhältnissen

(8) Not- und Katastrophenfallplanung: Etablierung eines Vorgehensmodells für die Verwaltung und Durchführung von Not- und Katastrophenfallplanung, Identifikation von Szenarien und Risikoanalyse, Erstellung und Pflege eines Rahmenplanes zur Koordination und Integration einzelner Not- und Katastrophenfallpläne, Verfahren für Test, Evaluierung, und Neubewertung von Not- und Katastrophenfallplänen

(9) Verifikation der Konformität: Einhaltung rechtlicher Bestimmungen, Verfolgung laufender Änderungen und Neuerungen an Gesetzen und Verordnungen, Beachtung des geistigen Eigentums Dritter sowie der notwendigen Schritte zum Schutz eigenen geistigen Eigentums, Revisionsfähigkeit und Aufbewahrungsfristen für Unterlagen und Akten, Einhaltung von Datenschutzbestimmungen, Schutz der IT-Systeme vor Mißbrauch durch Dritte

ISO 17799 zeichnet sich einerseits dadurch aus, dass es sich um einen knappen (84 Seiten) und überschaubaren Standard handelt, er andererseits durch die Verfügbarkeit von IT-gestützten Werkzeugen zur Unterstützung und Begleitung der Erstellung einer Sicherheitspolitik sowie der sich periodisch anschließenden Konformitätsprüfung als Leitfaden für die Praxis genutzt werden kann. Eine Reihe von Unternehmen bieten zudem Dienstleistungen an, um Betriebe bei der Unterstützung einer konformen Sicherheitspolitik und deren Umsetzung zu unterstützen; dies ist gerade bei kleinen und mittleren Unternehmen ohne entsprechende Kompetenzen im eigenen Haus von Interesse, da hier insbesondere aufgrund der Breite des Angebots und Referenzen der Anbieter eine vergleichende Auswahl vorgenommen werden kann; diese Transparenz ist bei ad hoc kundenspezifisch erbrachten Beratungsleistungen nicht gegeben. Zudem existiert mit dem (nicht in die ISO-Standardisierung übernommenen) BS 7799 Teil 2 eine konkrete Vorgabe, wie ein IT-Sicherheits-Managementsystem zu strukturieren ist.

Es existieren für Sicherheitspolitiken und IT-Sicherheits-Managementsysteme allerdings keine international standardisierten Zertifizierungsverfahren.

2.3.2 BSI-Grundschutz

Das Grundschutzhandbuch wurde erstmals 1994 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht und zielte gemäß des Auftrages des BSI zunächst auf Stellen der Bundesverwaltung ab. Seither wurde sowohl der Anwendungsbereich des Grundschutzhandbuches als auch der Umfang der betrachteten Sicherheitsaspekte stetig erweitert; die jüngste Auflage des Handbuches stammt vom Juli 2002. Zumindest innerhalb Deutschlands hat sich das IT-Grundschutzhandbuch als Standardwerk zur IT-Sicherheit in Deutschland etabliert.

Anders als ISO 17799 beschreibt das Grundschutzhandbuch nicht nur die Aspekte der Sicherheitspolitik und der Umsetzung in ein IT-Sicherheits-Managementsystem, sondern legt den Schwerpunkt auf die Beschreibung von spezifischen Sicherheitsmaßnahmen, die als Lösung häufig anzutreffender Einzelprobleme in vielen Fällen direkt oder mit geringen Modifikationen übernommen werden.

Dabei wird keine spezifische Erfassung der Werte und Risikoanalysen vorausgesetzt, statt dessen wird von einem pauschalierten Gefährdungsniveau ausgegangen, das einem als typisch angesehenen System sowie einer Menge von typischen Geschäftsprozessen entgegensteht. Hierfür werden detaillierte Sicherheitsmaßnahmen auf technischer Ebene dargestellt, die mit einem Katalog von Maßnahmen zur Umsetzung ergänzt werden.

Darüber hinaus bietet das Grundschutzhandbuch eine Beschreibung eines generischen Prozesses zur Erreichung und Aufrechterhaltung des als angemessen angenommenen Sicherheitsniveaus, das mit einem einfachen Soll-Ist-Vergleich überprüft werden kann.

Insofern ist das Grundschutzhandbuch nicht als Alternative zur Verwendung von ISO 17799 zu sehen; wesentliche Teile des Grundschutzhandbuches können als Grundlage für die Auswahl und korrekte technische Umsetzung der technischen Sicherheitsmaßnahmen herangezogen werden. Die alleinige Verwendung des Grundschutzhandbuches ist dahingegen nur unter der Prämisse empfehlenswert, dass entweder die als typisch angenommene Gefährdungslage und Systemstruktur hinreichend genau zutrifft oder aber die Ressourcen selbst für eine minimale Risikoanalyse mit der Möglichkeit hieraus gezielter Maßnahmen ableiten zu können aus zeitlichen oder auch Kostengründen nicht möglich ist. Dabei kennt auch das Grundschutzhandbuch die Sicherheitspolitik (unter dem Begriff IT-Sicherheitsleitlinie), wenn auch in deutlich reduziertem Umfang gegenüber ISO 17799 bzw. BS 7799 Teil 2.

2.3.3 Evaluierung von Sicherheitsprodukten

Während sich sowohl ISO 17799 als auch das BSI-Grundschutzhandbuch um den korrekten und möglichst vollständigen Einsatz von Sicherheitsmechanismen sowohl organisatorischer als auch technischer Art bemühen, bleibt dabei zunächst die Frage der Zuverlässigkeit und Vertrauenswürdigkeit der technischen Komponenten ungeklärt. Zusicherungen seitens eines Herstellers über den präzisen Funktionsumfang sind zumindest derzeit nicht üblich; statt dessen wird seitens der Hersteller in aller Regel ein weitgehender Haftungsausschluss angestrebt, der durch eine Minimierung der zugesicherten Eigenschaften des Produktes erreicht werden soll – was sich oft darin äußert, dass lediglich für die Lesbarkeit des zur Auslieferung genutzten Datenträgers Gewährleistung übernommen wird.

Funktionsklassen und Vertrauenswürdigkeit: TCSEC

Um einerseits gewährleisten zu können, dass die funktionalen Anforderungen an ein IT-System präzise und reproduzierbar festgelegt wurden, andererseits aber auch die Vertrauenswürdigkeit des Systems bewerten zu können, wurde zunächst auf Anforderung des U.S. Verteidigungsministeriums (DoD) 1983 ein Katalog mit Anforderungen an Funktion, Entwicklungsprozess und Dokumentation in Form der Trusted Computer System Evaluation Criteria (TCSEC, aufgrund der Einbandfarbe auch als Orange Book bezeichnet) sowie ein Handbuch zur Durchführung von

formalen Evaluierungen der Produkte, für die die Einhaltung der Kriterien behauptet wurde, entwickelt. Die Kriterien selbst waren in Abteilungen aufgeteilt, die ihrerseits noch einmal in Klassen untergliedert wurden. Dabei entsprach die Klasse D einem für untauglich befundenen System, wohingegen ein System der Klasse A1 ein mit formalen mathematischen Methoden entwickeltes System darstellte, das gleichzeitig die Maximalanforderungen des DoD bezüglich der Funktionalität realisiert und die Vertrauenswürdigkeit dieser Funktionalität mathematisch beweisbar darlegt.

Kernstück der Vorgehensweise sind Verfahren, mit denen einer Prüfstelle der Funktionsumfang sowie Beweise in Form von Quellen und Dokumenten bezüglich des tatsächlichen Vorhandenseins und der Vertrauenswürdigkeit der Funktionalität zur Prüfung (Evaluierung) vorgelegt werden. Gelingt dies auf dem erwünschten Niveau, so wird ein System zertifiziert.

Nationale Kriterien

Ein entsprechendes Gegenstück wurde in Deutschland mit den IT-Sicherheitskriterien (ITSK) 1989 vom jetzigen BSI entwickelt. Da die Anforderungen der TCSEC sehr stark an denen des DoD orientiert waren, wurde nach Möglichkeiten gesucht, nicht nur vollständige Systeme sondern einzelne Produkte evaluieren zu können. Dies wurde von den ITSK durch die Definition von Funktionsgruppen erreicht, die nach Bedarf zu Funktionsklassen zusammengefaßt wurden und zu denen völlig orthogonal wohldefinierte Qualitätsstufen definiert wurden.

Common Criteria

Evaluierungen, insbesondere solche auf hohen Vertrauenswürdigkeitsstufen, stellen einen erheblichen Aufwand an Ressourcen und vor allem Zeit dar. Daher kam früh der Wunsch nach einer möglichst internationalen Geltung zertifizierter Produkte auf. Im europäischen Rahmen gelang dies mit den 1991 verabschiedeten Information Technology Security Evaluation Criteria (ITSEC), bei dem sich Deutschland, das Vereinigte Königreich, die Niederlande und Frankreich dazu verpflichteten, von einem Land durchgeführte Evaluierungen ebenfalls anzuerkennen. Inhaltlich übernahmen die ITSEC weitgehend die Kerngedanken der ITSK. Um auch eine weltweite Verbreitung gewährleisten zu können, wurde schließlich in Zusammenarbeit der ITSEC-Teilnehmerländern sowie den USA und Kanada ein gemeinsamer Kriterienmechanismus entwickelt, die Common Criteria for Information Technology Security (CCITSE, oft auch nur CC), dem seither weitere Nationen beigetreten sind und die als internationaler Standard ISO 15408 kodifiziert wurden.

Die in den ITSEC begonnene Modularisierung wurde von den CC fortgesetzt; so werden die Anforderungen an Funktionalität und Vertrauenswürdigkeit nun in Form von Schutzprofilen (die ebenfalls evaluiert und zertifiziert werden müssen) festgehalten, die sich ihrerseits aus einem modularen Katalog an Anforderungen zusammensetzen lassen. Produkte lassen sich anhand derartiger Profile bzw. daraus für Produkte konkret abgeleiteten Anforderungskatalogen, den Security Targets evaluieren; die Vertrauenswürdigkeit wird dabei von EAL0 bis EAL7 auf einer klar definierten Skala bewertet.

Aussagekraft von Zertifikaten

Sofern ein Produkt mit der Aussage beworben wird, es sei nach den Common Criteria evaluiert worden, muss daher darauf geachtet werden, dass das verwendete Schutzprofil die eigenen Anforderungen abdeckt und zudem die Vertrauenswürdigkeitsstufe hinreichend ist; EAL1 entspricht beispielsweise lediglich einer einfachen Prüfung des Vorhandenseins der Funktionalität. Ähnlich kritisch sind häufig anzutreffende Formulierungen zu bewerten, wie etwa der, dass ein Produkt die Anforderungen z.B. der **TCSEC** C2-Sicherheitsstufe erfüllt (oder „C2-sicher“ ist). Derartige Aussagen sind wertlos, da insbesondere eine TCSEC-Evaluierung stets nur ein konkretes System betraf (d.h. eine zu prüfende Installation) und die letztgenannte Behauptung keinerlei Aussage über die Vertrauenswürdigkeit, sondern nur über Funktionsmerkmale beinhaltet.

Evaluierungsmechanismen stellen ein wichtiges Werkzeug bereit, um die Qualität und Vertrauenswürdigkeit technischer Umsetzungsmechanismen seitens unabhängiger Dritter bewerten zu lassen. Zumindest auf höheren Vertrauenswürdigkeitsstufen (ab EAL4 im Fall der Common Criteria) lassen sich dabei Aussagen treffen, die selbst mit sorgfältigen Funktionalitätstests nicht erreichbar sind. Hersteller müssen daher für höherwertig evaluierte Produkte deutlich mehr Sorgfalt aufwenden, als dies in der Regel, insbesondere bei Software, üblich ist.

2.4 Firewalls und andere Sicherheitsmechanismen für Netze

Obgleich in einschlägigen Studien zumeist das Risiko durch externe Angreifer (insbesondere Angriffe über Netzwerkverbindungen) überschätzt wird und Aspekte wie Innentäter oder aber auch die Absicherung der physischen Umgebung von Zugangskontrolle bis hin zu korrekter Kühlung und Brandschutz daher meist vernachlässigt werden, ist die Bedrohung durch weitreichende Vernetzung auch mit nicht vertrauenswürdigen Außenanbindungen dennoch gegeben.

Da vorhandene Sicherheitsmerkmale der eingesetzten Software meist nicht ausreichen, sind weitergehende Schutzmaßnahmen unverzichtbar.

Netzwerk-Firewalls als Werkzeug der Zugriffsbeschränkung

Ein Werkzeug zur Zugriffsbeschränkung in Netzwerken stellen Netzwerk-**Firewalls** dar, die bestimmte Datenflüsse blockieren oder zulassen können und dazu sämtliche Datenströme, die zwischen einem gesicherten Bereich und solchen geringerer Sicherheitsstufe verlaufen, über einen einzigen Übergangspunkt leiten, an dem die Überwachung und Blockierung stattfinden kann.

Dies geschieht allerdings zumeist ohne dabei Inhalt und Wirkung der Daten zu betrachten, denn leider können auch bei restriktiver Fassung der Regelwerke die eingesetzten Firewalls den Aufbau sogenannter Tunnels de facto nicht blockieren, wenn Standardkanäle (z.B. eMail, WWW) dazu für den Tunnelaufbau missbraucht werden: So können beispielsweise über das HTTP-Protokoll (etwa bei **SOAP** für die sogenannten Web Services) oder aber auch durch kryptographisch gesicherte Tunnel **(VPN)** Daten ausgetauscht werden, die von der Firewall nicht eingesehen werden können. Der dazu notwendige Schlüssel liegt nur beim Empfänger vor. Damit wird die Verwendung von Anwendungsprogrammen und Protokollen ermöglicht, die prinzipiell von der Sicherheitspolitik untersagt sind. Die Effektivität von Firewalls wird durch diese Entwicklung deutlich reduziert. Dennoch kann auf Firewalls nicht verzichtet werden, da sie einerseits den Datenverkehr kanalisieren und andererseits eine Reihe trivialer Angriffe wie etwa Netzwerk-Adressfälschungen abfangen können.

Insbesondere für kleinere und mittlere Unternehmen ist dabei jedoch problematisch, dass Firewalls keine statischen Geräte sind, die ein einziges Mal konfiguriert werden und anschließend nur minimalen Wartungsaufwand erfordern. Statt dessen ist bei korrekter Handhabung einerseits die Konfiguration ständigen Änderungen unterworfen, um etwa auf bekannt gewordene Verwundbarkeiten und Angriffe präventiv reagieren zu können, andererseits dient die Firewall zu einem großen Teil auch der Sammlung von Informationen über Datenverkehr und eventuell darin enthaltene Anomalien, die auf einen Angriff hindeuten können.

Firewalls erfordern Pflege

Insbesondere die letztere Rolle ist jedoch nicht nur mit erheblichem zeitlichem Aufwand seitens des Administrators verbunden, sondern erfordert auch, dass darüber hinaus die Administratoren über neue Entwicklungen bei Verwundbarkeiten und Angriffen ständig informiert sind.

Im elementaren Schutz wird nur auf passive Verteidigung ohne Analyse der Firewallprotokolle zurückgegriffen. Wird jedoch anhand der Protokolle der Firewalls eine aktive Analyse des internen Datenverkehrs und des auflaufenden Datenvolumens aus unsicherem (externen) Bereich durchgeführt, benötigt man ein Modell des „normalen" Verhaltens.

Zunächst ist es unerheblich, ob es sich bei dem Firewall-Produkt um ein kommerzielles System mit graphischer Benutzeroberfläche oder aber um eine aus freien Komponenten selbst zusammengestellte Lösung handelt; die Anforderungen an die Kompetenz des Administrators ergeben sich nicht aus der Benutzeroberfläche, sondern vielmehr aus den Kenntnissen der verwendeten Protokolle, Angriffe und Verteidigungstechniken.

Die Kompetenz des Systemadministrators ist entscheidend.

Derart qualifizierte Mitarbeiter sind selten und müssen in kleineren Organisationen häufig sicherheitsbezogene Aufgaben parallel zu anderen (z. B. Netzwerk- und Systemadministration) erledigen – dadurch, sowie durch Urlaubs- und Krankheitszeiten, aber auch durch die Notwendigkeit der Überwachung außerhalb der regulären Arbeitszeit, können sich im Vergleich zu einer wünschenswerten Netzwerk-Sicherheitsadministration erhebliche Differenzen ergeben. Die betriebswirtschaftliche Abwägung des daraus entstehenden Risikos ist eine der wesentlichen Bestandteile der zuvor angesprochenen Risikoanalyse.

Für die Erhöhung der Netzwerk-Sicherheit oder auch als Hilfsmittel zur Reduktion von Arbeitsaufwänden sollten parallel zu Firewalls **Intrusion Detection Systeme** (**IDS**) eingesetzt werden, die (anders als der Name vermuten läßt) nicht nur erfolgreiche Angriffe erkennen helfen, sondern auch einer Klassifizierung von Datenverkehr vornehmen in einerseits irrelevante Datenströme, bekannte (d. h. bereits von Abwehrmaßnahmen abgedeckte) und damit harmlose sowie andererseits potenziell gefährliche Angriffe sowie Anomalien, die weder regulärem Nutzerverhalten noch bekannten Angriffen zuordenbar sind. Dies kann den Sicherheits-Administrator deutlich entlasten, da ein IDS eine Voranalyse und Extraktion von Protokolldaten liefern und somit das zu bearbeitende Datenvolumen reduziert.

Intrusion Detection Systeme für zusätzliche Sicherheit

Auch bei IDS existieren sowohl kommerzielle als auch freie Implementierungen, die sich nicht notwendig in ihrer Qualität unterscheiden; signifikante Kosten entstehen wie auch bei Firewalls in jedem Fall durch Verwaltung und Betrieb des IDS.

Gerade bei IDS ist es für die Wirksamkeit extrem wichtig, bei dem Katalog bekannter Angriffe auf dem neuesten Stand zu sein, da ungeachtet der Möglichkeit zur automatischen Anomalieerkennung die zuverlässige Erkennung von Angriffen am effizientesten beim Vergleich vorgefundenen Verhaltens mit einem bekannten Muster gelingt. Auch hier ist wie bei Firewalling-Systemen neben detaillierten Kenntnissen der zugrundeliegenden Mechanismen eine ständige Arbeitsleistung zu erbringen.

Datenschutz

Ein Problem, das sich im Europäischen Rechtsraum, insbesondere jedoch aber in Deutschland ergibt, sind die Randbedingungen, unter denen eine Protokollierung bzw. die Aufbewahrung der Protokolldaten von Firewalls und IDS erfolgen dürfen. Hier sind durchaus enge Grenzen bezüglich der Zulässigkeit der Erfassung und Speicherung von personenbezogenen Daten oder auch nur von Daten, aus denen personenbezogene Daten abgeleitet werden können, gegeben. Insbesondere letzteres ist jedoch für fast alle aussagekräftige Protokolldaten der Fall, so dass eine juristische Prüfung angebracht ist, die zudem bei Vorhandensein entsprechender Gremien durch die innerbetriebliche Mitbestimmung begleitet werden sollte. Anderenfalls drohen neben rechtlichen Problemen auch erhebliche Reibungsverluste bei der Entwicklung und Umsetzung von Sicherheitsmaßnahmen.

Managed Security Provider

Aufgrund der erheblichen Ressourcen, die in Personal und die ständige Weiterentwicklung der Qualifikationen und Kompetenzen der Mitarbeiter investiert werden müssen, entstand bereits vor einigen Jahren das Geschäftskonzept der Managed Security Provider. Dieses besteht darin, analog zu anderen Outsourcing-Modellen, die Sicherheit eines Unternehmens durch eine externe Firma betreuen zu lassen.

Der Dienstleister bietet gebündelt die erforderlichen Kompetenzen und recherchiert permanent nach neuen Angriffen und Verwundbarkeiten, denen das Unternehmen dann präventiv begegnen kann. Hinzu kommt, dass bei entsprechender Fernbetreuung auch Betrieb und Überwachung rund um die Uhr gewährleistet werden kann, was anderenfalls aus Kostengründen für ein einzelnes mittleres Unternehmen kaum realisierbar ist.

Den prinzipiellen Vorteilen eines derartigen Arrangements steht jedoch auch eine Reihe gravierender Nachteile gegenüber. Dies beginnt bereits damit, dass dem Managed Security Provider ein extrem tiefer Einblick in Geschäftsprozesse (z. B. beginnend mit der oben angesprochenen Risikoanalyse) und vertrauliche Interna des Unternehmens gewährt werden muss. Damit sind direkte vertragliche Durchgriffe bei Verletzung z. B. der Verschwiegenheitspflicht nur schwer durchsetzbar, insbesondere bei Mitarbeiterfluktuationen auf Seiten des Managed Security Providers; ein Nachweis, dass vertrauliche Informationen preisgegeben wurden, wird nur schwer beweiskräftig gelingen.

Ebenfalls nicht zu vernachlässigen ist, dass dem Managed Security Provider ein meist geschäftskritischer Bereich des Gesamt-IT-Systems untersteht. Reagiert dieser nicht zeitnah auf Anforderungen, z. B. bestimmte Verbindungen an einer Netzwerk-Firewall freizuschalten, kommt es zu potenziell kostenintensiven Verzögerungen; dies kann sich bis hin zu Extremsituationen fortsetzen, in denen der Managed Security Provider durch Insolvenz oder Übernahme seine vertraglichen Verpflichtungen nicht mehr oder nicht mehr hinreichend erfüllt. Die dann notwendige Rückübernahme wird durch nicht vorhandene Mitarbeiter mit hinreichender Kompetenz auf Seiten des Kunden schwierig und durch gegebenenfalls fehlende Aufzeichnungen noch erschwert. Nicht zuletzt bleibt festzuhalten, dass die Übertragung der Sicherheits-Administration auf einen Managed Security Provider letztlich nicht von der Haftung für durch kompromittierte Systeme nach außen hin verursachte Schäden entbinden kann und zudem je nach Gesellschaftsform mit dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) der Geschäftsführung bzw. dem Vorstand eines Unternehmens die Verantwortung für ein wirksames Risikomanagement auferlegt ist.

Absicherung einzelner Rechner und Arbeitsplätze

Neben der Absicherung von Netzwerkzugängen und darüber betriebenen Anwendungen besteht ein erheblicher Bedarf bei der Absicherung einzelner Rechner und Arbeitsplätze. Insbesondere weit verbreitete Betriebssysteme und Anwendungen haben sich als signifikant verwundbar gegen Viren und **Würmer** erwiesen; der Verbreitungsgrad von **Ausbreitungsvektoren** wie etwa Microsoft Office-Produkten, Microsoft Outlook, aber auch z. B. den Apache **Webserver** des Apache-Projektes sowie der sehr hohe Grad der weltweiten Vernetzung der Netzwerke und Systeme untereinander führen dazu, dass sich binnen weniger Stunden Millionen von Systemen infizieren und als weitere Multiplikatoren für Angriffe verwenden lassen.

Antivirus-Software kann dieses Problem zum Teil reduzieren, indem bösartiger Code eliminiert bzw. vor Verarbeitung durch verwundbare Anwendungsprogamme gefiltert wird. Allerdings setzt dies immer voraus, dass die dem Antivirus-Programm zur Verfügung stehenden Profildaten, anhand derer **Viren** und **Würmer** erkannt werden, ständig aktualisiert werden. Ein Viren-Scanner, dessen Profildatenbank einige Monate alt ist, stellt bestenfalls selbst ein Risiko dar, da er ein falsches Gefühl der Sicherheit vermittelt. Problematisch ist dabei jedoch, dass die Ausbreitungsgeschwindigkeit insbesondere von Würmern Geschwindigkeiten erreicht, die den Herstellern von Antivirus-Software für die Beobachtung von Schadverhalten, der Isolierung des Verursachers, der Extraktion eines Profils für den Verursacher sowie der Verteilung an die Kunden bestenfalls nur wenige Stunden lassen. Dies gelingt nicht immer, zudem können die Viren-Scanner-Profile ihrerseits durch Fehlalarme Probleme auslösen, wenn etwa legitime Daten und Anwendungen als bösartig eingestuft werden. Insofern stellen auch Viren-Scanner eine weitere unzureichende Lösung für ein eher grundsätzliches Problem mit derzeit weit verbreiteten Anwendungsprogrammen dar; dennoch ist ihr Einsatz ebenso wie der von Firewalling- und **Intrusion Detection-Systemen** unabdingbar.

Ein Viren-Scanner, dessen Profildatenbank einige Monate alt ist, stellt bestenfalls selbst ein Risiko dar, da er ein falsches Gefühl der Sicherheit vermittelt.

2.5 Zusammenfassung

Die in Unternehmen eingesetzte Informations- und Kommunikationstechnologie (IKT) bewirkt eine zunehmende Abhängigkeit der Unternehmen von diesen IKT-Infrastrukturen. Je größer die technologische Abhängigkeit entwickelt ist, desto wichtiger wird es, Verwundbarkeiten der eingesetzten Systeme sowie der Netzwerkinfrastruktur zu betrachten und durch geeignete IT-Sicherheitsmaßnahmen zu schützen. Die wesentlichen Ziele sind dabei, die Verfügbarkeit der Infrastrukturkomponenten, die Authentizität von Dokumenten, die **Integrität** von Daten und Systemen und nicht zuletzt die Vertraulichkeit von Informationen und der Kommunikationswege zu gewährleisten.

Grundsätzlich ist bei jedem realen (Sicherheits-) System eine Kompromittierung nicht auszuschließen. Es ist daher von besonderer Bedeutung, dass Datensicherung, Katastrophenplanung sowie Maßnahmen für die Wiederherstellung des Regelbetriebes jederzeit funktional und tagesaktuell einsatzbereit sind, so dass im Falle einer Kompromittierung die Folgeschäden über unmittelbare Verluste hinaus (z. B. Verlust geistigen Eigentums, von Reputation bei Kunden und Geschäftspartnern, rechtliche Konsequenzen durch Verletzung von Sorgfaltspflichten) zumindest begrenzt werden können.

Bevor ad hoc Einzelmaßnahmen ergriffen werden, sollte im Unternehmen durch eine eigene Arbeitsgruppe unter Mitverantwortung – besser noch unter Mitwirkung – der Geschäftsführung eine Sicherheitspolitik erstellt werden. Diese Gruppe analysiert und bewertet die Sicherheitsrisiken im Unternehmen und formuliert auch geeignete Gegenmaßnahmen und deren wirtschaftliche Vertretbarkeit. Aus dieser Kosten-Nutzen Betrachtung heraus werden Maßnahmen priorisiert, die das verbleibende Restrisiko deutlich minimieren. Bei der Erstellung der Sicherheitspolitik können Konzepte und Lösungen Dritter nur als Grundlage und Anregung dienen. Eine für das Unternehmen individuelle Betrachtung ist unumgänglich. Dabei können systematische Vorgehensweisen, wie sie durch ISO 17799 oder das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik bereitgestellt werden, helfen, essenzielle Aspekte konsequent zu erfassen und zu bearbeiten.

Bei der Umsetzung der Sicherheitspolitik sollte in der Beschaffung von Komponenten darauf geachtet werden, ob die zu Einsatz kommenden Technologien hinsichtlich ihrer Qualität und Vertrauenswürdigkeit durch anerkannte Prüfstellen evaluiert und zertifiziert wurden.

Der Prozess der Erstellung, Umsetzung und regelmäßigen Verifikation der Sicherheitspolitik hat mehrseitig positive Auswirkungen. Einerseits wird durch die technischen Maßnahmen ein wirksamer Schutz vor Bedrohungen erreicht und durch die Revision kontrolliert. Andererseits kann durch die detaillierte Risikoanalyse beim Abschluss von Versicherungspolicen das abzudeckende Restrisiko weitgehend präzise quantifiziert und somit die Prämien minimiert werden. Darüber hinaus führt der Prozess zur Sensibilisierung der Mitarbeiter und in Verbindung mit entsprechenden Schulungsmaßnahmen zum konsequenten und behutsamen Vorgehen in vielen Unternehmensprozessen: IT-Sicherheit wird nicht nur durch Technologie, sondern auch durch die Mitarbeiter realisiert.

Für Konzeption und Umsetzung sowie kontinuierliche Konfiguration und Administration der eingesetzten Sicherheitsmechanismen ist eine hohe Qualifikation der zuständigen Mitarbeiter unabdingbar. Eine nachweisbare Qualifikation kann unter anderem durch Erwerb eines IT-Sicherheitszertifikats erfolgen, das von der Technischen Universität Darmstadt in Kooperation mit dem CAST-Forum vergeben wird. Darüber hinaus ist den Mitarbeitern ausreichend zeitlicher Freiraum zur Bewältigung der sicherheitsbezogenen Aufgaben einzuräumen.

Die Durchführung von technischen und organisatorischen Maßnahmen und deren Ergänzung durch Sensibilisierung und gezielte Schulung der Mitarbeiter sind die wesentlichen Schritte, die sich aus der Sicherheitspolitik ergeben. Eine regelmäßige Prüfung der Wirksamkeit und Notwendigkeit im Rahmen einer Innenrevision oder eines Unternehmens-Audits kann die Kosten für notwendige Maßnahmen in eine vergleichende Wirtschaftlichkeitsbewertung stellen und durch geeignete Bewertungsschemata aufzeigen, ob und in welchem Umfang die IT-Sicherheit im Unternehmen verbessert wurde.

3 IT-Grundschutz nach BSI – eine gute Basis

Isabel Münch, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das IT-Grundschutzhandbuch hat sich als Standardwerk zur ökonomischen Erarbeitung wirksamer IT-Sicherheitskonzepte etabliert. Belegt wird dies durch die ständig wachsende Zahl freiwillig registrierter Anwender im In- und Ausland und die intensive und aktive Nutzung der vom BSI bereitgestellten IT-Grundschutz-Hotline. In vielen Behörden und Unternehmen bildet das IT-Grundschutzhandbuch des BSI die Basis für die tägliche Arbeit des IT-Sicherheits-Managements und die kontinuierliche Umsetzung von Standard-Sicherheitsmaßnahmen.

Nach erfolgreicher Umsetzung der im IT-Grundschutzhandbuch beschriebenen Standard-Sicherheitsmaßnahmen stellt sich für viele Institutionen die Frage, wie sie ihre Bemühungen um IT-Sicherheit nach außen transparent machen können. Um diesen Bedürfnissen nachzukommen hat das BSI die Qualifizierung nach IT-Grundschutz definiert, die aufgrund der ständigen Aktualisierung und Erweiterung des Handbuchs praktisch auf der Höhe der Zeit bleibt. Nach einer erfolgreichen Qualifizierung wird dann ein IT-Grundschutz-Zertifikat vergeben, mit dem die erfolgreiche Umsetzung der Standard-Sicherheitsmaßnahmen verdeutlicht werden kann.

IT-Grundschutz-Prinzipien

Im IT-Grundschutzhandbuch werden Standardsicherheitsmaßnahmen für typische IT-Systeme empfohlen. Das Ziel dieser IT-Grundschutz-Empfehlungen ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann.

Das Baukastenprinzip

Um den sehr heterogenen Bereich der **IT** einschließlich der Einsatzumgebung besser strukturieren und aufbereiten zu können, verfolgt das IT-Grundschutzhandbuch das Baukastenprinzip. Die einzelnen Bausteine spiegeln typische Bereiche des IT-Einsatzes wider, wie beispielsweise Client-Server-Netze, bauliche Einrichtungen, Kommunikations- und Applikationskomponenten. In jedem Baustein wird zunächst die zu erwartende Gefährdungslage beschrieben, wobei sowohl die typischen Gefährdungen als auch die pauschalisierten Eintrittswahrscheinlichkeiten berücksichtigt werden. Diese Gefährdungslage

bildet die Grundlage, um ein spezifisches Maßnahmenbündel aus den Bereichen Infrastruktur, Personal, Organisation, Hard- und Software, Kommunikation und Notfallvorsorge zu generieren. Die Gefährdungslage wird zur Sensibilisierung angeführt, für die Erstellung eines Sicherheitskonzeptes nach IT-Grundschutz wird sie nicht weiter benötigt.

Um das für einen durchschnittlichen Schutzbedarf notwendige Sicherheitsniveau zu erreichen, brauchen die Anwender die vorgenannten aufwendigen Analysen nicht durchzuführen. Es ist vielmehr ausreichend, die für das relevante IT-System oder den betrachteten IT-Verbund entsprechenden Bausteine zu identifizieren und die darin empfohlenen Maßnahmen konsequent und vollständig umzusetzen.

Mit Hilfe des IT-Grundschutzhandbuchs lassen sich IT-Sicherheitskonzepte einfach und arbeitsökonomisch realisieren. Bei der traditionellen Risikoanalyse werden zunächst die Gefährdungen ermittelt und mit Eintrittswahrscheinlichkeiten bewertet, um dann die geeigneten IT-Sicherheitsmaßnahmen auszuwählen und anschließend noch das verbleibende Restrisiko bewerten zu können. Bei Anwendung des IT-Grundschutzhandbuchs wird hingegen nur ein Soll-Ist-Vergleich zwischen empfohlenen und bereits realisierten Maßnahmen durchgeführt. Dabei festgestellte fehlende und noch nicht umgesetzte Maßnahmen zeigen die Sicherheitsdefizite auf, die es durch die empfohlenen Maßnahmen zu beheben gilt. Erst bei einem signifikant höheren Schutzbedarf muss zusätzlich eine ergänzende Sicherheitsanalyse unter Beachtung von Kosten- und Wirksamkeitsaspekten durchgeführt werden. Hierbei reicht es dann aber in der Regel aus, die Maßnahmenempfehlungen des IT-Grundschutzhandbuchs durch entsprechende individuelle, qualitativ höherwertige Maßnahmen zu ergänzen.

Soll-Ist-Vergleich

Bei den im IT-Grundschutzhandbuch aufgeführten Maßnahmen handelt es sich um Standardsicherheitsmaßnahmen, also um diejenigen Maßnahmen, die für die jeweiligen Bausteine nach dem Stand der Technik umzusetzen sind, um eine angemessene Sicherheit zu erreichen. Teilweise wird mit diesen Maßnahmen auch bereits ein höherer Schutzbedarf abgedeckt, trotzdem sind sie in den jeweiligen Bereichen das Minimum dessen, was vernünftigerweise an Sicherheitsvorkehrungen umzusetzen ist.

Angesichts der Innovationsschübe und Versionswechsel im IT-Bereich ist das IT-Grundschutzhandbuch auf leichte Erweiterbarkeit und Aktualisierbarkeit ausgerichtet. Das BSI überarbeitet und aktualisiert regelmäßig das IT-Grundschutzhandbuch, um die Empfehlungen auf dem Stand der Technik zu halten.

Status Quo IT-Grundschutz

Das IT-Grundschutzhandbuch ist ein lebendes Werk, das regelmäßig aktualisiert und ergänzt wird. Dasselbe gilt für die IT-Grundschutz-Zertifizierung. Es empfiehlt sich immer, regelmäßig auf den BSI-Webseiten nachzusehen, ob es Neuigkeiten in diesem Bereich gibt oder sich auf die Mailinglisten zum IT-Grundschutz setzen zu lassen, um automatisch auf dem Laufenden gehalten zu werden.

Die aktuelle Ausgabe des IT-Grundschutzhandbuchs (Version Mai 2002) ist um die Bausteine

- Windows 2000 Client,
- Windows 2000 Server,
- Internet-PC sowie
- Novell eDirectory erweitert worden.

Neben diesen neuen Bausteinen wurden zahlreiche Ergänzungen und Aktualisierungen der vorhandenen Texte vorgenommen. So enthält der Peer-to-Peer-Baustein nun auch Sicherheitsempfehlungen für Windows 2000 und Linux.

IT-Grundschutzhandbuch als Standardwerk

Das IT-Grundschutzhandbuch hat sich inzwischen als Standardwerk zur ökonomischen Erarbeitung wirksamer IT-Sicherheitskonzepte etabliert. Belegt wird dies durch die ständig wachsende Zahl freiwillig registrierter Anwender im In- und Ausland und die intensive und aktive Nutzung der vom BSI bereitgestellten IT-Grundschutz-Hotline. In vielen Behörden und Unternehmen bildet das IT-Grundschutzhandbuch des BSI die Basis für die tägliche Arbeit des IT-Sicherheits-Managements und die kontinuierliche Umsetzung von Standard-Sicherheitsmaßnahmen.

Qualifizierung nach IT-Grundschutz

Nach erfolgreicher Umsetzung der im IT-Grundschutzhandbuch beschriebenen Standard-Sicherheitsmaßnahmen stellt sich für viele Institutionen die Frage, wie sie ihre Bemühungen um IT-Sicherheit nach außen transparent machen können. Um diesen Bedürfnissen nachzukommen, hat das BSI die Qualifizierung nach IT-Grundschutz eingeführt, die aufgrund der ständigen Aktualisierung und Erweiterung des Handbuchs praktisch auf der Höhe der Zeit bleibt. Nach Abschluss eines Qualifizierungsprozesses kann ein IT-Grundschutz-Zertifikat erteilt werden, mit dem die erfolgreiche Umsetzung der Standard-Sicherheitsmaßnahmen verdeutlicht werden kann.

Ein IT-Grundschutz-Zertifikat soll verschiedene Zielgruppen ansprechen und dabei zum Vertrauensgewinn beitragen, indem nachgewiesen wird, dass IT-Sicherheit

nach IT-Grundschutz umgesetzt ist und aufrechterhalten wird. Als Zielgruppen und Einsatzbereiche kommen in Frage:

- Wirtschaftsunternehmen oder Behörden, die mit anderen Institutionen zu kooperieren beabsichtigen und wissen wollen, welches Sicherheitsniveau dort erreicht worden ist.
- Institutionen, die durch unabhängige Dritte nachprüfen lassen wollen, dass sie IT-Grundschutz erfolgreich umgesetzt haben.
- Anbieter von eCommerce- oder eGovernment-Dienstleistungen, die den Kunden mittels eines IT-Grundschutz-Zertifikats ihre erfolgreichen Bemühungen um IT-Sicherheit nachweisen wollen.

Mindest-Sicherheitsniveau

Ziel der IT-Grundschutz-Qualifizierung ist es, einen Maßstab für die tatsächlich umgesetzten Standard-Sicherheitsmaßnahmen in informationstechnischen Einrichtungen von Behörden und Unternehmen zu etablieren und damit die Möglichkeit des Nachweises eines definierten und damit auch vergleichbaren Mindest-Sicherheitsniveaus anzubieten.

Stufen der IT-Grundschutz-Qualifizierung

Das BSI hat, unter Beteiligung registrierter IT-Grundschutzanwender und IT-Sicherheitsexperten, drei Ausprägungen der IT-Grundschutz-Qualifizierung definiert: Das „IT-Grundschutz-Zertifikat“ sowie die Selbsterklärungen „IT-Grundschutz Aufbaustufe“ und „IT-Grundschutz Einstiegsstufe“.

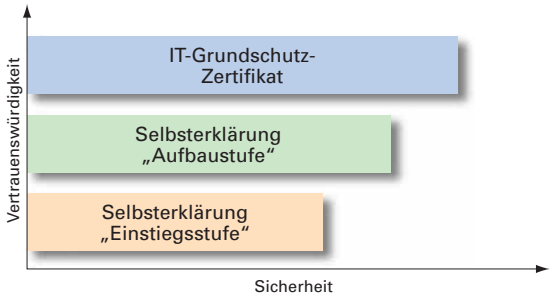
IT-Grundschutz-Zertifikat: Innerhalb der drei Ausprägungen der IT-Grundschutz-Qualifizierung stellt das IT-Grundschutz-Zertifikat den höchsten Grad an Vertrauenswürdigkeit und das höchste Sicherheitsniveau dar. Für ein IT-Grundschutz-Zertifikat muss ein lizenzierter Auditor bestätigt haben, dass die im IT-Grundschutzhandbuch beschriebenen und im vorliegenden Fall relevanten Standard-Sicherheitsmaßnahmen umgesetzt sind.

Selbsterklärung „IT-Grundschutz Aufbaustufe“: IT-Grundschutz ist eine arbeitsökonomische Vorgehensweise. Trotzdem kann die Umsetzung aller für einen vorliegenden Anwendungsfall relevanten IT-Grundschutzmaßnahmen u. U. mit erheblichem Aufwand verbunden sein. Um Behörden und Unternehmen einen Migrationspfad anbieten und wichtige Meilensteine bei der schrittweisen Umsetzung der Standard-Sicherheitsmaßnahmen transparent machen zu können, definiert das BSI daher zwei Vorstufen des eigentlichen IT-Grundschutz-Zertifikats: Die Selbsterklärungen „IT-Grundschutz Aufbaustufe“ und „IT-Grundschutz Einstiegsstufe“.
Voraussetzung für die Selbsterklärung „IT-Grundschutz Aufbaustufe“ ist, dass die Behörde oder das Unternehmen die wichtigsten Standard-Sicherheitsmaßnahmen des IT-Grundschutzhandbuchs umgesetzt hat. Die notwendigen Vorarbeiten und Erhebungen können dabei sowohl von Dritten als auch von Mitarbeitern der eigenen Institution erfolgen. Die Selbsterklärung wird darauf basierend von einem zeichnungsbefugten Vertreter der Institution abgegeben.

Selbsterklärung „IT-Grundschutz Einstiegsstufe“: Die IT-Grundschutz-Qualifizierung in der Einstiegsstufe wird erreicht, wenn die Behörde oder das Unternehmen lediglich die unabdingbaren Standard-Sicherheitsmaßnahmen des IT-Grundschutzhandbuchs umgesetzt hat. Wie bei der Aufbaustufe können die Vorarbeiten und Erhebungen sowohl durch Dritte als auch durch eigene Mitarbeiter erfolgen. Die Selbsterklärung wird wiederum von einem zeichnungsbefugten Vertreter der Institution abgegeben. Das durch die Selbsterklärung „IT-Grundschutz Einstiegsstufe“ dargestellte Sicherheitsniveau ist das geringste der drei Ausprägungen.

Interpretation: Entscheidend bei der Interpretation der drei Ausprägungen der IT-Grundschutz-Qualifizierung ist, dass die Einstiegs- und die Aufbaustufe zwar ein definiertes niedriges, jedoch noch kein ausreichendes Sicherheitsniveau gemäß IT-Grundschutzhandbuch festlegen. Sie dienen als Meilensteine bis zur Erreichung des IT-Grundschutz-Zertifikats. Nur das IT-Grundschutz-Zertifikat attestiert die Realisierung eines „umfassenden IT-Grundschutzes".

Im nachfolgenden Diagramm wird der Zusammenhang zwischen den einzelnen Ausprägungen in Bezug auf Sicherheitsniveau und Vertrauenswürdigkeit dargestellt.



Qualifizierungsschema

Der Qualifizierungsprozess nach IT-Grundschutz ist in zwei Phasen unterteilt: die Erhebungs- und die Qualifizierungsphase. Eine Beschreibung der einzelnen Schritte dieser Phasen können Sie unter **www.bsi.de/gshb/zert/eckpunkt.htm** abrufen.

- **Erhebungsphase**

  Die Erhebungsphase besteht aus den folgenden Schritten

  - Schritt 1: Definition des Untersuchungsgegenstands
  - Schritt 2: Vorarbeiten
  - Schritt 3: Basis-Sicherheitscheck
  - Schritt 4: Festlegung der weiteren Vorgehensweise

  Die Schritte 1 bis 4 stellen Vorarbeiten im Hinblick auf die Qualifizierung dar. Sie können durch die Institution selbst, aber auch mit Unterstützung externer Berater durchgeführt werden.

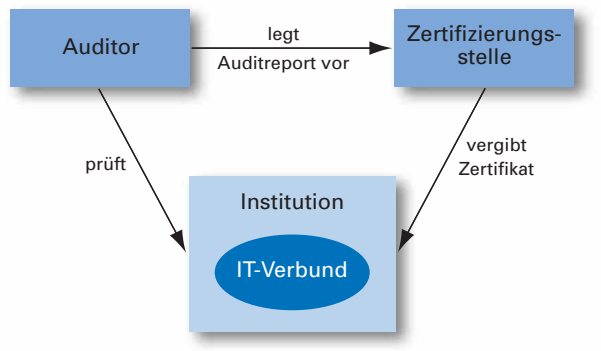
- **Qualifizierungsphase**

  Die Qualifizierungsphase besteht aus den folgenden Schritten

  - Schritt 5: Plausibilitätsprüfung (Überprüfung der Ergebnisse aus der Erhebungsphase)
  - Schritt 6: Realisierungsprüfung (Ziel der Realisierungsprüfung ist es, den im Basis-Sicherheitscheck typischerweise über Interviews ermittelten Umsetzungsstatus stichprobenartig zu überprüfen.)
  - Schritt 7: Selbsterklärung/Zertifizierung
  - Schritt 8: Re-Qualifizierung

IT-Grundschutz-Zertifikat

Eine unabhängige, akkreditierte Zertifizierungsstelle kann der Institution das IT-Grundschutz-Zertifikat verleihen, wenn die obigen Voraussetzungen erfüllt sind. Die Schritte 5, 6 und 7 müssen dann von einem für IT-Grundschutz lizenzierten Auditor durchgeführt worden sein. Die Vergabe eines Zertifikats wird dem BSI von der Zertifizierungsstelle mitgeteilt.



In vielen Fällen wird eine Institution zur Erlangung eines IT-Grundschutz-Zertifikats im Vorfeld auf externe Beratungsleistungen zurückgreifen. Audit und Zertifizierung sollten jedoch nicht durch Personen erfolgen, die an Konzeption, Beratung oder Umsetzung beteiligt waren.

Dies bedeutet für den Auditor, dass er im konkreten Umfeld mindestens zwei Jahre nicht beratend tätig gewesen sein darf; dies gilt jedoch nicht für andere Mitarbeiter des Unternehmens, dem er angehört. Für die Zertifizierungsstelle heißt das, dass kein Mitarbeiter in den zurückliegenden zwei Jahren dort beraten haben darf.

Was sagt das Zertifikat aus?

Über ein IT-Grundschutz-Zertifikat wird zunächst nachgewiesen, dass im betrachteten Verbund IT-Grundschutz erfolgreich umgesetzt worden ist. Darüber hinaus zeigt ein IT-Grundschutz-Zertifikat auch, dass in der jeweiligen Institution

- IT-Sicherheit ein anerkannter Wert ist,
- ein IT-Sicherheits-Management vorhanden ist und außerdem
- zu einem bestimmten Zeitpunkt ein definiertes IT-Sicherheitsniveau erreicht wurde.

Eine nach IT-Grundschutz qualifizierte Institution kann die Selbsterklärung oder das Zertifikat selbst veröffentlichen. Das BSI bietet aber auch an, Qualifizierungsaussagen auf dem BSI-WWW-Server zu veröffentlichen. Für das IT-Grundschutz-Zertifikat hat das BSI ein Siegel entworfen, um den Wiedererkennungswert und eine vereinfachte Online-Darstellung zu fördern. Wird das Siegel online verwendet, muss damit ein Link auf den entsprechenden **Server** des BSI bzw. der Zertifizierungsstelle verbunden sein.

Fazit

Das IT-Grundschutz-Zertifikat stellt einen ersten Schritt in Richtung „messbare" IT-Sicherheit in Behörden und Unternehmen dar. Anhand eines etablierten und praxisbewährten Katalogs von Standard-Sicherheitsmaßnahmen – dem IT-Grundschutzhandbuch des BSI – wird eine Aussage über den tatsächlich vorhandenen IT-Sicherheitszustand in dem betrachteten IT-Verbund getroffen. Das vorgestellte Qualifizierungsschema sieht neben dem eigentlichen IT-Grundschutz-Zertifikat, das eine Prüfung durch lizenzierte Auditoren umfasst, auch eine Qualifizierung in Form einer „Selbsterklärung Einstiegsstufe" und einer „Selbsterklärung Aufbaustufe" vor. Diese beiden Selbsterklärungen sind als Meilensteine auf dem Weg zum IT-Grundschutz-Zertifikat zu verstehen und dienen dazu, die Hürde beim Einstieg in den Qualifizierungsprozess zu verringern. Alle drei Ausprägungen der Qualifizierung nach IT-Grundschutz können außenwirksam dokumentiert werden. Auf diese Weise lassen sich die eigenen Bemühungen um IT-Sicherheit und die erfolgreiche Umsetzung der Standard-Sicherheitsmaßnahmen transparent machen.

Alle Informationen zum Thema Qualifizierung nach IT-Grundschutz können unter **www.bsi.de/gshb/zert** abgerufen werden.

4 IT-Sicherheit – was kostet das?

Hubertus Gottschalk, Leiter T-Com-Sicherheit, Deutsche Telekom AG

Alle zukunftsorientierten Unternehmen nutzen das Internet zur Informationsgewinnung, Kommunikation, Prozessoptimierung oder Kundengewinnung. Mit dem Internet lassen sich Produktivitätssteigerungen und Wettbewerbsvorteile erzielen. Aber: Ohne Vorsichtsmaßnahmen stellt die Schnittstelle zwischen Internet und Intranet ein Risiko dar. Nur zu leicht gelangen dann gefährliche **Viren**, **Trojanische Pferde** oder schlaue **Hacker** in Firmennetzwerke und richten enormen materiellen und immateriellen Schaden an.

Daher muss sich jedes Unternehmen der Chancen und Risiken bewusst sein, die das Internet attraktiv machen – aber auch gefährlich sein können.

Es kann jeden treffen

Bei den ursprünglichen Entwicklungen des Internets spielten Sicherheitsüberlegungen keine große Rolle. Auch den wichtigsten Internet-Diensten wie z. B. eMail fehlten effektive Schutzfunktionen. Ohne besonderen Schutz des Firmen-Internet-Anschlusses ist es aber für Profis leicht möglich, im Firmennetzwerk Geschäftsgeheimnisse, Angebote, Kontonummern oder Passwörter auszuspionieren.

Die größten Sicherheitslücken entstehen aber durch Fehler in der Administration der betroffenen Netzwerke. Ursachen hierfür sind u. a. chronische Überlastungen der IT- oder EDV-Abteilung und personelle Unterbesetzung. Die Anforderungen an den Sicherheits-Administrator von firmeninternen **TCP/IP**-Netzen sind hoch. Er muss hochqualifiziert und sicherheitssensibilisiert sein. Er soll Kenntnisse über neue Sicherheitslücken besitzen und muss sich ständig weiterbilden bzw. geschult werden. Dazu sollte er Kenntnisse über neue Angriffstechniken verfügen und über 24 Stunden verfügbar sein.

Absolute Sicherheit gibt es nicht

Absolute Sicherheit kann aber auch mit allen technologischen und organisatorischen Lösungen nicht realisiert werden. Denn dazu müssten die gefährdeten Systeme physikalisch getrennt sein und auf Kommunikation vollständig verzichtet werden. Dies widerspricht natürlich den wirtschaftlichen und strategischen Notwendigkeiten eines Unternehmens, so dass meist eine individuelle Unternehmenslösung mit einem vertretbaren Restrisiko umgesetzt wird. Dabei können auch mit geringem Sicherheitsbudget grundlegende Sicherheitsstandards eingehalten werden. Die Gesamtkosten des Sicherheitskonzepts sollten aber immer in angemessener Relation zu den möglich Kosten eines Schadensfalls stehen.

Lösungsmöglichkeit Firewall und VirusProtection

IP-Netze sollten aus Sicherheitsgründen mit einem **Firewall**-System geschützt werden. Außerdem sollte das TCP/IP-Netz über einen aktuellen Virenschutz verfügen.

Öffentlich zugängliche Serversysteme (Web- oder **FTP-Server**) sollten aus Sicherheitsgründen ausschließlich in einer sogenannten Demilitarisierten Zone (**DMZ**) platziert werden. Eine solche Anordnung garantiert eine strikte Trennung aller öffentlichen Systeme von allen internen Netzen und verhindert, das Angreifer Systeme im Intranet attackieren können. Die Firewall sollte daher über eine entsprechende Schnittstelle zur Realisierung einer Demilitarisierten Zone verfügen.

Grundsätzlich kann zwischen einer Realisierung in Eigenregie oder Vergabe an einen Dienstleister unterschieden werden.

Realisierung in Eigenregie

Zu Beginn der Realisierung in Eigenregie steht die Bestimmung der Anforderungen und des notwendigen Schutzniveaus. Dabei muss die Infrastruktur und die IT-Sicherheitsorganisation untersucht und die vorhandenen Risiken identifiziert werden. Aufbauend auf den Ergebnissen der Analyse muss die Sicherheitspolitik für den Internetzugang definiert werden. Verbindliche Regelungen über Rechte und Pflichten der Benutzer und den sicheren Betrieb des Systems müssen darin enthalten sein. Auch sollten hier die Aufgaben und Verantwortungen der beteiligten Personen benannt und festgehalten werden. Die Sicherheitspolitik muss vom Betriebsrat und den Datenschutzverantwortlichen abgestimmt und verbindlich verabschiedet werden.

Ausgehend von der Sicherheitspolitik wird ein technisches, organisatorisches und administratives Grobkonzept für die Realisierung des Systems entwickelt. Auf dieser Basis sollte eine geeignete Sicherheitsarchitektur und ein Produkt ausgewählt werden. Anschließend wird ein Detailkonzept entwickelt, das über einen Pilotbetrieb in einen Regelbetrieb überführt werden kann. Die Einhaltung der Regelungen ist durch eine IT-Revision zu überwachen.

Bevor ein Unternehmen die Realisierung einer Firewall-/VirusProtection-Lösung in Eigenregie in Angriff nimmt, sollte genau geprüft werden, ob alle notwendigen Schritte in Eigenregie durchgeführt werden können. In vielen Fällen ist zur Bestimmung der Sicherheitsanforderungen und des Schutzniveaus externe Unterstützung notwendig.

Ein selbst betreutes Firewall/VirusProtection-System benötigt mindestens 2 Systembetreuer, deren Lohnkosten zusammen ca. 120 000 € betragen. Die Einarbeitung in das Thema sowie die ständige Weiterbildung werden für 2 Mitarbeiter jährlich mit ca. 6.000 € einmalig und ca. 3.000 € jährlich geschätzt.

Realisierung durch einen Dienstleister

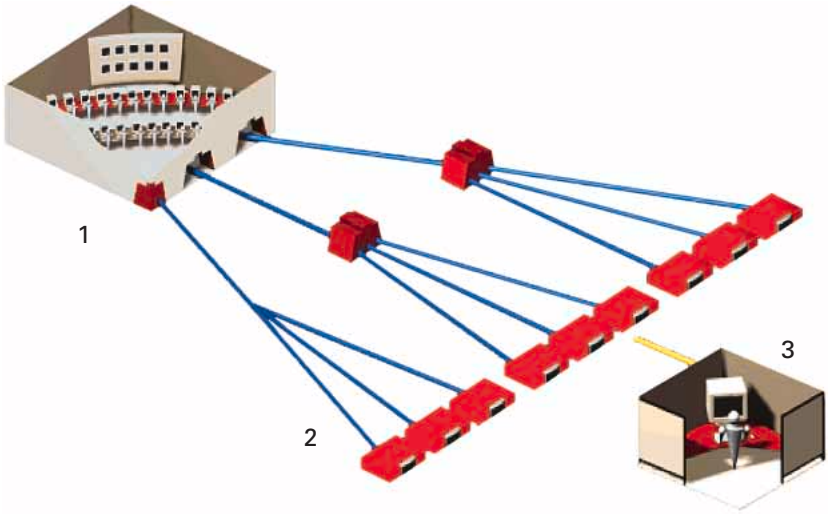
Der Betrieb eines Firewall/Virusprotection-Systems kann für ein Unternehmen einen erheblichen Aufwand bedeuten. Daher stellt sich für viele Unternehmen die Frage, ob der Betrieb des Firewall-Systems von einem Dienstleister übernommen werden kann.

Wichtige Kriterien bei der Auswahl von Lösungsanbietern sind:

1. Nachweis über ein eigenes Lösungsportfolio, das alle Anforderungen und Wünsche des Kunden abdeckt
2. Nachweis einer praktisch erprobten Gesamtkompetenz für Implementierung von integrativen Lösungen
3. Erfolgreiche Implementierung einer Internet-Sicherheitslösung für Intranet, Internet innerhalb des eigenen Unternehmens
4. Eigene Erfahrungen des Anbieters als Internet Service Provider mit Referenzkunden und Vertrauenswürdigkeit des Dienstleister
5. Flächendeckende Präsenz des Anbieters im Wirkungsgebiet des Kunden
6. Serviceleistungsangebot auf Kundenwunsch bis hin zum 24-Stunden/7-Tage-Support.

Es bestehen darüber hinaus diverse Firewall-Realisierungsmöglichkeiten über Remote-Management (Firewall im Unternehmen – vom Dienstleister von außen betrieben und gewartet) und Firewall-Housing (Firewall im Unternehmen – vom Dienstleister im Unternehmen betrieben und gewartet).

Für viele Unternehmen bietet es sich an, den Aufbau und Betrieb ihrer Firewall soweit wie möglich an externe Dienstleister zu übertragen. So können sie sich auf die Nutzung des Internets für ihr Kerngeschäft konzentrieren, ohne eigene Mitarbeiter im Bereich der Internet-Sicherheit zu binden.



Konzept eines Managed Security Providers:
1) Sicherheitszentrum, 2) Firewall beim Kunden, 3) Überwachungsoption beim Kunden

Absicherung des Firmennetzes

Ausgangspunkt dafür ist ein abgestuftes Beratungskonzept. Daraus wird eine Sicherheitsstrategie für das Firmennetz entwickelt und ein Angebot für Hardware, Software, Betriebs- und Servicekonzept erstellt. Die Installation und Administration der Firewall zwischen dem Internet und dem Firmennetz erfolgt durch Spezialisten. Danach ist das Firmennetz an das Internet angeschlossen. Angriffe von außen werden wirkungsvoll abgewehrt und die Mitarbeiter können das Internet in vollem Umfang nutzen. Die auf das Unternehmen zugeschnittene Firewall prüft intensiv den ein- und ausgehenden Datenverkehr.

Geschulte Experten überwachen die Firewall an sieben Tagen der Woche rund um die Uhr. Per Remote Control prüfen sie die Betriebsfähigkeit der Firewall und beobachten verdächtige Aktivitäten. Bei einem Einbruchsversuch leiten sie sofort Gegenmaßnahmen ein – notfalls bis hin zur Trennung des internen Netzes vom Internet. In Firewall Reports protokollieren sie kontinuierlich den Datenverkehr auf dem Internet-Anschluss – ohne kostenintensive Personalausgaben.

Kosten Firewall und VirusProtection

Firewall- und Viruswall-Produkte der Deutschen Telekom AG sind ein rund um die Uhr von der Deutschen Telekom gemanagtes Firewall/VirusProtection-System für kleine und mittelständische Unternehmen sowie Großfirmen, welches das Unternehmensnetzwerk vor unberechtigten Angriffen aus dem Internet schützt. Für kleine und mittelständische Firmen können bis zu 400 IT-Arbeitsplätze geschützt werden. Für die betriebsfähige Bereitstellung der Firewall und Viruswall für 50 IT-Arbeitsplätze inklusive 5 **IP-Sec**-Clients fallen einmalig zusammen ca. 9.200 € an. Für die Überlassung und Betrieb der Firewall/VirusProtection entstehen monatlich weitere 650 €/jährlich 7.800 € an Kosten. Die Investitionskosten der Hard- und Software fallen unabhängig der Realisierung in Eigenregie oder als Dienstleistung an.

Entscheidung

Ein Unternehmen, das eine Internet-Anbindung in Eigenregie realisieren und betreiben will, kämpft vornehmlich mit der Komplexität der eingesetzten Hard- und Software. Mangelnde Produktreife der Firewall-Software kann dann zu Defiziten in punkto Stabilität und Funktionalität führen. Das hat zur Folge, dass die Eigenrealisation und Betrieb der Firewall/VirusProtection-Lösung sehr zeit- und personalaufwändig ist.

Neben den technologischen Problemen unterschätzen viele Unternehmen die notwendigen organisatorischen Begleitmaßnahmen, die zur Aufrechterhaltung eines angemessenen Sicherheitsniveaus unerlässlich sind.

Einige Dienstleister bieten inzwischen ihren Kunden Komplettlösungen bei der Auswahl, Installation, Konfiguration und Betrieb eines Firewall/VirusProtection-Systems an. Unternehmen sollten zusätzlich auf Beratungsleistungen bestehen, die die organisatorischen Voraussetzungen für den wirksamen Betrieb einer Firewall/VirusProtection-Lösung im Unternehmen schaffen. Eine solche Outsourcing-Lösung ist mit einem seriösen Dienstleister sicher zu realisieren und sollte den Unternehmen die Anstrengung wert sein.

5 Übersicht über den IT-Sicherheitsmarkt in Hessen

Sebastian Hummel, InvestitionsBank Hessen AG

Hessen ist Deutschlands Zentrum für IT-Sicherheit. Dies ist das Ergebnis einer Untersuchung, die im ersten Halbjahr 2002 von der Aktionslinie hessen-infoline im Auftrag des Hessischen Ministeriums für Wirtschaft, Verkehr und Landesentwicklung durchgeführt wurde. Diese Aussage wird unterstützt von einer Studie der M-Result GmbH, die im Auftrag der TechnologieStiftung Hessen im ersten Quartal 2002 erstellt wurde. Diese Studie sieht Frankfurt auf Platz 2 der Rangliste deutscher IT-Standorte. Als einziges Bundesland beherbergt Hessen drei der zehn bestplatzierten IT-Standorte Deutschlands (Frankfurt Platz 1, Darmstadt Platz 4, Wiesbaden Platz 9).

Für unsere Untersuchung wurden bundesweit Fragebögen an IT-Sicherheitsanbieter verschickt mit dem Ziel, eine Übersicht über die Anbieter und deren verschiedenen Dienstleistungen und Produkte zu erhalten. Aus den Angaben der angeschriebenen Firmen wurde eine Liste der Anbieter zusammengestellt, die in Hessen entweder ihren Stammsitz haben oder aber über eine Niederlassung verfügen. Folgender Punkt sollte dabei aber beachtet werden: Die Informationen stammen von den Anbietern selbst. Es kann keine Gewähr hinsichtlich der Angaben übernommen werden, so gründlich auch versucht wurde, mit der Fragestellung die Dienstleistungen und Produkte zu qualifizieren.

Etwa 50% der in Deutschland im Bereich IT-Sicherheit aktiven Firmen haben ihren Sitz oder eine Niederlassung in Hessen. Diese hohe Konzentration von Anbietern macht Hessen zu dem Standort für IT-Sicherheit. Innerhalb Hessens ist eine sehr starke Konzentration von Anbietern im Rhein-Main-Gebiet zu verzeichnen. Über 90% der hessischen Anbieter, das entspricht circa 45% der in Deutschland tätigen IT-Sicherheitsanbieter, sind hier angesiedelt. In unsere Bestandsliste konnten wir 54 hessische Anbieter aufnehmen, die im nachfolgenden Kapitel in alphabetischer Reihenfolge aufgeführt sind (ab Seite 54). Die Liste gibt neben den Firmendaten auch einen Überblick über das angebotene Leistungsspektrum und die Zielgruppen. Eine Überblicksdarstellung ermöglicht es, schnell die Anbieter heraus zu filtern, die bestimmte Kriterien erfüllen, etwa das Anbieten eines Vor-Ort-Services oder das Durchführen von Schulungen (siehe S. 52).

Bei einer näheren Untersuchung der angebotenen Leistungen der IT-Anbieter kamen wir zu folgendem Ergebnis: Den hohen Schulungsbedarf im Bereich IT-Sicherheit haben die hessischen IT-Sicherheitsanbieter erkannt. 93% bieten Schulungen an, 94% **Auditing**, 89% implementieren oder vertreiben Sicherheitsprodukte, 85% haben eine Hotline.

Ein Vor-Ort-Service ist für 74% der Anbieter eine Selbstverständlichkeit.

Nichtkommerzielle Einrichtungen in Hessen zum Thema IT-Sicherheit

Neben der Fülle kommerzieller Anbieter ist in Hessen eine bedeutende Ansammlung nicht gewinnorientierter Einrichtungen und Institutionen tätig, die ihre Arbeit dem Thema IT-Sicherheit widmen.

An einer Reihe von Universitäten und Fachhochschulen wirken Arbeitskreise oder werden Forschungsprojekte durchgeführt, die sich mit dem Thema IT-Sicherheit beschäftigen. Sie betreiben Grundlagenforschung, auf deren Ergebnisse kommerzielle Anbieter aufbauen können. Daneben wirken eine Reihe von Instituten und Foren an der Erarbeitung und Verbreitung neuer Sicherheitskonzepte mit.

So wird im Fachbereich Mathematik/Informatik der Universität Kassel an neuen Verfahren im Bereich der **Kryptografie** gearbeitet. Die **Public-Key-Kryptografie** ist einer der Forschungsschwerpunkte der Forschungsarbeit. Laut Prof. Dr. Hans-Georg Rück können sich auch kommerzielle Entwickler kryptografischer Produkte an der Universität Kassel beraten lassen. Prof. Dr. Alexander Roßnagel, Leiter des Fachgebiets Öffentliches Recht, legt einen Schwerpunkt seiner Tätigkeit auf den Bereich Recht der (Sicherheits-)Technik.

www.uni-kassel.de

Prof. Dr. Kai Rannenberg, Inhaber der T-Mobile Stiftungsprofessur für mCommerce, forscht an der Johann Wolfgang Goethe-Universität Frankfurt am Main zu den Themen anwendungsorientierte IT-Sicherheitsevaluation und -zertifizierung, Mobile Anwendungen und Mehrseitige Sicherheit sowie Kommunikationsinfrastrukturen und -geräte (bspw. Personal Security Assistants and Services). Dr. Johann Bizer, Mitarbeiter am Lehrstuhl für Öffentliches Recht der Universität Frankfurt und Mitherausgeber der Zeitschrift „Datenschutz und Datensicherheit“, beschäftigt sich mit rechtlichen Aspekten der IT-Sicherheit.

www.uni-frankfurt.de

Als Zentrum der hessischen IT-Sicherheitsforschung ist Darmstadt anzusehen. Ein wichtiger Akteur ist die Technische Universität Darmstadt. Prof. Dr. Claudia Eckert, Inhaberin des Lehrstuhls für IT-Sicherheit, leitet das Fachgebiet Sicherheit in der Informationstechnik, das im Fachbereich Informatik angesiedelt ist. Die Arbeitsgruppe um Prof. Dr. Johannes Buchmann forscht in dem Bereich **Kryptografie** und Computeralgebra. Ein Forschungsprojekt (das FlexiPKI-Projekt) hat es sich zur Aufgabe gemacht, alternative kryptografische Verfahren zu entwickeln und in existierende Anwendungen zu integrieren.

www.tu-darmstadt.de

Um die interdisziplinären Forschungsbemühungen zu bündeln, wurde an der TU Darmstadt Ende Juli 2002 der Aufbau des „Darmstädter Zentrums für IT-Sicherheit" (DZI) beschlossen. Die Aufgaben des neuen Zentrums liegen in der Ausbildung im Bereich der IT-Sicherheit, in der Forschungsförderung, in der Öffentlichkeitsarbeit für IT-Sicherheitsaktivitäten sowie in der Funktion des Ansprechpartners für den Technologietransfer zu Wirtschaft und Verwaltung. Dem Zentrum sind 20 Professoren aus fünf Fachbereichen der TU Darmstadt zugeordnet.

In enger Kooperation mit der TU Darmstadt arbeitet das Fraunhofer Institut für sichere Telekooperation (SIT). Geleitet wird das Institut von Prof. Dr. Heinz Thielmann und Prof. Dr. Claudia Eckert. Die aktuellen Forschungsschwerpunkte des Fraunhofer SIT sind: Sichere Betriebssoftware, Betriebssysteme, Methodische Konstruktion sicherer Systeme, Sicherheitsmechanismen, Kommunikationssicherheit, sichere Anwendungen, sicheres mobiles, ubiquitäres Berechnen.

www.sit.fhg.de

Neben dem SIT gibt es in Darmstadt noch ein weiteres Fraunhofer Institut, das Institut für graphische Datenverarbeitung (IGD). Innerhalb des Fraunhofer IGD beschäftigt sich die Abteilung „Security Technology for Graphics and Communication Systems" mit der Realisierung von Sicherheitsmechanismen insbesondere im Bereich Multimedia.

www.igd.fhg.de

Ebenfalls in Darmstadt beheimatet und personell eng mit der Technischen Universität Darmstadt verbunden ist das Competence Center for Applied Security Technology (CAST-Forum). Ziel des Forums ist es, eine dem wachsenden Stellenwert der IT-Sicherheit in allen Bereichen des Wirtschaftslebens und der öffentlichen Verwaltung entsprechende Kompetenz aufzubauen und innovative Sicherheitslösungen zu fördern.

www.castforum.de

Mit dem Thema **Biometrie** beschäftigt sich das an der Fachhochschule Gießen-Friedberg beheimatete Institut für biometrische Identifikationssysteme (IBIS). Schwerpunkte der Forschung liegen unter anderem auf der Integration biometrischer Identifikationssysteme in Sicherheitskonzepte und der Evaluierung des Einsatzes unter praktischen Bedingungen.

www.biometrie-info.de

Einen regionalen Ansatz verfolgt Prof. Dr. Hans-Ulrich Bühler von der Fachhochschule Fulda. Mit Studenten aus seinem Arbeitskreis Sicherheit hilft er mittelständischen Unternehmen vor Ort mit praktischen Sicherheitstipps weiter.

www.fh-fulda.de

6 Anbieterübersicht

		Sicherheitsprodukte	Auditing	Schulung	Hotline	Vorort-Service
34123 Kassel	COBION	•	•	•	•	•
34131 Kassel	s.a.d. System Analyse und Design	•	•	•		
35305 Grünberg	OR Network	•	•	•	•	•
35315 Homberg	Soultek	•	•	•	•	•
35510 Butzbach	High-End Services	•	•	•	•	•
60052 Frankfurt	Siemens AG ICN VD CC4S	•	•	•	•	•
60313 Frankfurt	IT@work			•	•	
60313 Frankfurt	DE-CODA	•	•	•	•	
60314 Frankfurt	Cybernet	•	•	•	•	
60318 Frankfurt	STEGANOS	•		•	•	
60326 Frankfurt	Bosch Telecom	•	•	•	•	•
60326 Frankfurt	Guardian iT	•	•	•	•	•
60329 Frankfurt	Pallas it-solutions	•	•	•	•	•
60388 Frankfurt	CLASS	•	•	•	•	•
60388 Frankfurt	Neef LappCom	•	•	•	•	•
60389 Frankfurt	Frank Bernhard Informationstechnik	•	•	•	•	•
60431 Frankfurt	NCP engineering	•	•	•	•	•
60487 Frankfurt	AVINCI	•	•	•	•	•
60528 Frankfurt	ASTRUM			•	•	
60528 Frankfurt	Colt Telecom	•	•	•	•	•
60528 Frankfurt	ExperTeam		•	•		
60596 Frankfurt	DASYS	•	•	•	•	
61203 Reichelsheim	MGE USV-Systeme	•	•	•	•	•
61250 Usingen	nGENn	•	•	•		•
61352 Bad Homburg	Hewlett-Packard	•	•	•	•	•
61440 Oberursel	Utimaco Safeware	•	•	•	•	•
63150 Heusenstamm	Deteline	•	•	•	•	•

		Sicherheitsprodukte	Auditing	Schulung	Hotline	Vorort-Service
63150 Heusenstamm	Whale Communications	•	•	•	•	•
63225 Langen	EVIDIAN	•	•	•	•	•
63225 Langen	NSG Netzwerk-Service	•	•		•	•
63225 Langen	Steria GmbH	•	•	•	•	•
63263 Neu Isenburg	SECARTIS		•	•	•	
63303 Dreieich	Tiscali	•	•	•	•	•
63811 Stockstadt	Applied Security	•	•	•	•	•
64283 Darmstadt	Fraunhofer – IGD, Abt. Sicherheitstechn.	•	•	•	•	
64293 Darmstadt	Secude	•	•	•	•	
64295 Darmstadt	Fraunhofer Institut für Sich. Telekooper.	•	•			
64297 Darmstadt	FlexSecure	•	•	•		•
64331 Weiterstadt	Danet Consult	•	•	•	•	•
64347 Griesheim	DIGINET	•	•	•	•	•
64546 Mörfelden	Beta Systems Software	•	•	•	•	•
64625 Bensheim	Fahr & Partner	•	•	•	•	•
65128 Wiesbaden	CSC Ploenzke	•	•			
65189 Wiesbaden	Symax Business Software	•	•	•	•	•
65203 Wiesbaden	VISTEC Internet Service	•	•	•	•	•
65205 Wiesbaden	PECOS		•			
65451 Kelsterbach	LHSYSTEMS	•	•	•	•	•
65462 Gustavsburg	4 sale IT-Service	•	•	•	•	•
65510 Idstein	BDG	•	•	•	•	•
65760 Eschborn	SerCon GmbH	•	•	•		•
65760 Eschborn	T-Systems ISS		•	•	•	•
65779 Kelkheim	DSI	•	•	•	•	•
65824 Schwalbach	Datakey	•	•	•	•	•
65830 Kriftel	Systemberatung Axel Dunkel	•	•	•	•	•

Applied Security GmbH

63811 Stockstadt, Industriestraße 16, Telefon 060 27/406 70, www.apsec.de

Kerngeschäft	Authentifizierung; Kryptografie; Software
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 8 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K, XP; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Firewallprodukte; Managed Firewall Services; Intrusion Detection Systeme; Auditing Software
Sicherheitsprodukte - Implementierung	Antivirensoftware; Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Biometrische; Chipkarten/-leser; Firewall; Smart Cards; Token; Kryptografische Server
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur); Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service; durchschnittliche PC-Kenntnisse reichen

ASTRUM GmbH

60528 Frankfurt am Main, Lyoner Straße 14, Telefon 069/66 55 44 0, www.astrum.de

Kerngeschäft	Software
Zielgruppe	Großkonzerne
Mitarbeiter	50-250
Hotline	Ja
Vorort-Service	Nein
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	Keine Angaben
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	Gehört zum Service

AVINCI GmbH

60487 Frankfurt am Main, Insterburger Straße 7, Telefon 069 - 509 59 50, www.avinci.de

Kerngeschäft	IT-Consulting
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	> 250
Hotline	Ja
Vorort-Service	verschieden Service Level
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	BSI-IT-Grundschutzzertifikat; BSI-Auditor für ISO-15408 (Common Criteria); Überprüfung anhand ISO-17799 (information security management); automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service

BDG GmbH & Co. KG

65510 Idstein, Am Fraunwald 5, Telefon 06126 - 94 43 30, www.bdg.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datensicherung; Kryptografie; Neztwerksicherheit
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	50-250
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	Überprüfung anhand ISO-17799 (information security management); autom. Sicherheitstests von außen (z.B. IP-Scans); persönl. Sicherheitstests von außen (z.B. Black Box, Tiger Teams); autom. Sicherheitstests von innen (z.B. lokale IP-Scans); persönl. Sicherheitstests von innen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Managed Firewall; Intrusion Detection Systeme; Auditing Software
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Biometrische; Backup Systeme; Chipkarten/-leser; Firewall; Smart Cards; Token; VPN
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur); Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate; OS/X
Kenntnisse zur Implementierung	Gehört zum Service

Beta Systems Software AG

64546 Mörfelden, Waldecker Straße 6, Telefon 06105/910 80, www.betasystems.com

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datenschutz; Software
Zielgruppe	Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	Überprüfen und Härten von Betriebssystemen OS/390; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Auditing Software
Sicherheitsprodukte - Implementierung	Auditing Software
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Trifft nicht zu
Kenntnisse zur Implementierung	Administrator; IT-Systemingenieur

Bosch Telecom GmbH

60326 Frankfurt am Main, Kleyerstraße 94, Telefon 069/75 62 13 57, www.bosch.com

Kerngeschäft	Authentifizierung; Datenschutz; PKI/Trustcenter-Dienstleistungen
Zielgruppe	Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	Vertragsspezifisch
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	Persönliche Sicherheitstests von innen
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Chipkarten/-leser; Smart Cards; Token
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur); sonstiger Trustcenter-/PKI-Betreiber; sonstige Registrierungsstelle; Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	IT-Systemingenieur

CLASS AG (Systemintegrator)

60388 Frankfurt am Main, Röntgenstraße 7, Telefon 061 09 / 736 70, www.class.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datensicherung; Hardware, Kryptografie; Software; Content Security; Intrusion Detection
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 8 Stunden
Schulung	Ja
Branchenlösungen	Keine Angaben
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Apple OS/X; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Managed Firewall Services; Intrusion Detection Systeme
Sicherheitsprodukte - Implementierung	Antivirensoftware; Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Backup Systeme; Chipkarten/-leser; Firewall; Smart Cards; Token
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur); Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service

COBION AG

34123 Kassel, Miramstraße 87, Telefon 0561 / 57 08 70, www.cobion.de

Kerngeschäft	Software; Content Security
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	Überprüfen von Netzwerkkonzepten und Netzwerken; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	URL - Blocking; eMail Content-Blocking
Hardwarekomponenten	Web-/eMail Filter
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate;
Kenntnisse zur Implementierung	Gehört zum Service; Administrator; speziell geschultes Personal

COLT Telecom GmbH

60528 Frankfurt am Main, Herriotstraße 4, Telefon 069 / 959 56 06 21 80, www.colt.de

Kerngeschäft	Betriebssystemsicherheit; Datenschutz; Datensicherung; Hardware; Software; Housing; Hosting
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Managed Firewall; Intrusion Detection Systeme
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Backup Systeme; Firewall; Token
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service

CSC Ploenzke AG

65189 Wiesbaden, Abraham Lincoln Park 1, Telefon 0611 / 142 0, www.cscploenzke.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datenschutz; Datensicherung; Kryptografie; Software
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Keine Angaben
Vorort-Service	Keine Angaben
Schulung	Keine Angaben
Branchenlösungen	Nein
Sicherheitsauditing	BSI-IT-Grundschutzzertifikat; BSI-Auditor für ISO-15408 (Common Criteria); Überprüfung anhand ISO-17799 (information security management); automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Antivirensoftware; Intrusion Detection Systeme; Auditing Software
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Keine Angaben
Kenntnisse zur Implementierung	Gehört zum Service; Informatiker; Administrator; IT-Systemingenieur; speziell geschultes Personal; durchschnittliche PC-Kenntnisse reichen

Cybernet AG

60314 Frankfurt am Main, Hanauer Landstraße 320-324, Telefon 069 / 40 89 59 0, www.cybernet.de

Kerngeschäft	Betriebssystemsicherheit; Datenschutz; Datensicherung; Hardware
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	Nein
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Firewallprodukte; Managed Firewall Services
Sicherheitsprodukte - Implementierung	Antivirensoftware; Firewallprodukte
Hardwarekomponenten	Backup Systeme; Firewall; Smart Cards; Token
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	Gehört zum Service

Danet Consult GmbH

64331 Weiterstadt, Gutenbergstraße 10, Telefon 06151 / 86 84 40, www.danet-consult.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; HardwareKryptografie; Software; Beratungsleistung
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 8 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	BSI-IT-Grundschutzzertifikat; automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Managed Firewall Services; Intrusion Detection Systeme
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Firewall; Token
Kryptografische Produkte	Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service; Informatiker; Administrator; speziell geschultes Personal; durchschnittliche PC-Kenntnisse reichen;

DASYS

60596 Frankfurt am Main, Rembrandtstraße 14, Telefon 069 / 63 15 31 41, www.dasys.de

Kerngeschäft	Datenschutz
Zielgruppe	kleine Unternehmen; mittlere Unternehmen
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	Nein
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte;
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte
Hardwarekomponenten	Firewall; Smart Cards; Token
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur);
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	Gehört zum Service

Datakey

65824 Schwalbach/Ts, Am Kronberger Hang 2, Telefon 06196 / 95 04 00, www.datakey.com

Kerngeschäft	Authentifizierung
Zielgruppe	Großkonzerne
Mitarbeiter	50-250
Hotline	Ja
Vorort-Service	innerhalb 8 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	BSI-Auditor für ISO-15408 (Common Criteria)
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Chipkarten/-leser; Smart Cards; Token
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur); sonstiger Trustcenter-/PKI-Betreiber; Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	Gehört zum Service; durchschnittliche PC-Kenntnisse reichen

DE - CODA

60313 Frankfurt/Main, Börsenplatz 4, Telefon 069/21 97 15 93, www.de-coda.de

Kerngeschäft	Authentifizierung; Datenschutz; Kryptografie; Software
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	Nein
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Chipkarten/-leser
Kryptografische Produkte	Registrierungsstelle (SigG-konform); Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	Gehört zum Service; Administrator

Deteline GmbH

63150 Heusenstamm, Philipp-Reis-Straße 4-8, Telefon 061 04/40 40, www.deteline.de

Kerngeschäft	Hardware; LAN-Netzwerksicherheit
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	50-250
Hotline	Ja
Vorort-Service	innerhalb 2 Stunden
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: SUN; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Personal Firewalls; andere Firewallprodukte; Managed Firewall; Intrusion Detection Systeme
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Firewall; VPN
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Nur für Clients
Kenntnisse zur Implementierung	Wird durch Deteline erbracht

DIGINET

64347 Griesheim, Im Leuschnerpark 4, Telefon 06155/60 53 00, www.dni.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datenschutz; Datensicherung; Hardware
Zielgruppe	mittlere Unternehmen
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Keine Angaben
Sicherheitsauditing	BSI-IT-Grundschutzzertifikat; automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme; Auditing Software
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme; Auditing Software
Hardwarekomponenten	Backup Systeme; Firewall
Kryptografische Produkte	Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate; OS/X
Kenntnisse zur Implementierung	Gehört zum Service

DSI Daten Service Informationssysteme GmbH

65779 Kelkheim, Robert-Koch-Straße 106, Telefon 061 74/96 49 67, www.dsi.net

Kerngeschäft	Authentifizierung; Datenschutz; Datensicherung; Software
Zielgruppe	kleine Unternehmen; mittlere Unternehmen
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 8 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	automatisierte Sicherheitstests von außen(z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Managed Firewall; Intrusion Detection Systeme; Auditing Software
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme; Auditing Software
Hardwarekomponenten	Backup Systeme; RAID - Systeme
Kryptografische Produkte	sonstiger Trustcenter-/PKI-Betreiber; sonstige Registrierungsstelle
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Administrator

Evidian GmbH

63225 Langen, Robert-Bosch-Straße 60-66, Telefon 061 03 / 76 10, www.evidian.com

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datenschutz; Kryptografie; Software; System Management
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	>250
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Firewallprodukte; Auditing Software
Sicherheitsprodukte - Implementierung	Firewallprodukte; Auditing Software
Hardwarekomponenten	Chipkarten/-leser; Firewall; Smart Cards
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur); Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service; Informatiker; Administrator; IT-Systemingenieur

ExperTeam AG

60528 Frankfurt am Main, Hahnstraße 70, Telefon 069 / 66 40 08 0, www.experteam.de

Kerngeschäft	Betriebssystemsicherheit; Datenschutz; Risiko-Management
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	50 – 250
Hotline	Nein
Vorort-Service	Nein
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	BSI-IT-Grundschutzzertifikat; Überprüfung anhand ISO-17799 (information security management); Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate; Unixderivate; OS/X
Kenntnisse zur Implementierung	gehört zum Service

Fahr & Partner

64625 Bensheim, Robert-Bosch-Straße 35, Telefon 062 51/58 26 06 4, www.fahr.com

Kerngeschäft	Authentifizierung; Datenmanagement; Datenschutz; Datensicherung; Hardware; Kryptografie; Software; Andere
Zielgruppe	kleine Unternehmen; mittlere Unternehmen
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); Überprüfen von Netzwerkkonzepten und Netzwerken; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Firewallprodukte; Managed Firewall;
Sicherheitsprodukte - Implementierung	Antivirensoftware; Firewallprodukte;
Hardwarekomponenten	Biometrische; Chipkarten/-leser; Smart Cards
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service

FlexSecure GmbH

64297 Darmstadt, Thüringer Straße 1, Telefon 061 51/27 82 40, www.flexsecure.de

Kerngeschäft	Authentifizierung; Kryptografie; Software
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Nein
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); Überprüfen und Härten von Betriebssystemen: Unix; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Smart Cards; Token; Andere
Kryptografische Produkte	Trustcenter-/CA-Betrieb (SigG-konform); Registrierungsstelle (SigG-konform); Sonstiger Trustcenter-/PKI-Betreiber; Infrastruktur für PKI-Betreiber (Hard-, Software)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Informatiker; Administrator

Frank Bernard Informationstechnik GmbH

60389 Frankfurt am Main, Wilhelmshöher Straße 123, Telefon 069/90 47 89 80, www.fbit.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datenschutz; Datensicherung; Hardware; Kryptografie; Software; Firewall; Virenschutz
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 12 Stunden
Schulung	Ja
Branchenlösungen	Keine Angaben
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; Managed Firewalls; Intrusion Detection Systeme;
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; Intrusion Detection Systeme
Hardwarekomponenten	Firewall
Kryptografische Produkte	sonstiger Trustcenter-/PKI-Betreiber; Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service; speziell geschultes Personal

Fraunhofer Institut für Sichere Telekooperation

64295 Darmstadt, Rheinstraße 75, Telefon 061 51/86 92 85, www.sit.fraunhofer.de

Kerngeschäft	Dienstleistungen; E-Commerce; Digitale Signatur; PKI
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	50-250
Hotline	Keine Angaben
Vorort-Service	Keine Angaben
Schulung	Keine angaben
Branchenlösungen	Ja
Sicherheitsauditing	persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Intrusion Detection Systeme; Auditing Software
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Keine Angaben
Kenntnisse zur Implementierung	Keine Angaben

Fraunhofer - IGD, Abteilung Sicherheitstechnologie

64283 Darmstadt, Fraunhoferstraße 5, Telefon 06151/155 0, www.igd.fhg.de

Kerngeschäft	Betriebssystemsicherheit; Datenschutz; Datensicherung; Andere
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	Nein
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Personal Firewalls; Intrusion Detection Systeme; Auditing Software
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Informatiker; speziell geschultes Personal

Guardian iT GmbH

60326 Frankfurt am Main, Kleyerstraße 79-89, Telefon 069/70 70 88 00, www.guardianit.de

Kerngeschäft	Datenschutz; Datensicherung; Desaster Recovery; Business Continuity
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	>12 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Backup Systeme
Kryptografische Produkte	sonstiger Trustcenter-/PKI-Betreiber
Betriebssysteme	Windowsderivate; Unixderivate; OS/X
Kenntnisse zur Implementierung	Gehört zum Service; Administrator; speziell geschultes Personal

Hewlett-Packard GmbH

61352 Bad Homburg, Hewlett-Packard-Straße 1, Telefon 0180/53 26 22 2 (0.12 €/Min), www.hp.com

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datensicherung; Hardware
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	>250
Hotline	Ja
Vorort-Service	> 12 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	persönliche Sicherheitstests von innen; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Firewallprodukte; Intrusion Detection Systeme
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Backup Systeme; Firewall; Andere
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service

High-End Services GmbH

35510 Butzbach, Nussalle 13, Telefon 06033/89 09 0, www.h-e-s.de

Kerngeschäft	Software
Zielgruppe	mittlere Unternehmen
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Managed Firewall Services
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte
Hardwarekomponenten	Firewall
Kryptografische Produkte	sonstiger Trustcenter-/PKI-Betreiber; sonstige Registrierungsstelle; Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate;
Kenntnisse zur Implementierung	Gehört zum Service; Administrator

IT@work Trusted Solutions GmbH

60313 Frankfurt am Main, Kleine Hochstraße 9, Telefon 069 / 29 72 45 35, www.itatwork.com

Kerngeschäft	Betriebssystemsicherheit
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	50-250
Hotline	Ja
Vorort-Service	Nein
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	Keine Angaben
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Unixderivate
Kenntnisse zur Implementierung	Administrator

LHSYSTEMS

65451 Kelsterbach, Am Weiher 24, Telefon 069 / 69 69 02 66, www.lhsystems.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datenschutz; Datensicherung; Kryptografie
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	>250
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Antivirensoftware; andere Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur); sonstiger Trustcenter-/PKI-Betreiber; sonstige Registrierungsstelle; Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service

MGE USV - Systeme

61203 Reichelsheim, Wetteraustraße 23, Telefon 06035/96 73 16, www.mgeups.de

Kerngeschäft	Hardware
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	USV
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service

NCP engineering GmbH

60431 Frankfurt am Main, Felix-Dahn-Straße 15, Telefon 069/95 11 29 01, www.ncp.de

Kerngeschäft	Software; Andere
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	50-250
Hotline	Ja
Vorort-Service	Abhängig vom Wartungsvertrag
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	Überprüfen von Netzwerkkonzepten und Netzwerken; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Informatiker; Administrator; IT-Systemingenieur; speziell geschultes Personal

Neef LappCom GmbH

61118 Bad Vilbel, Konrad-Adenauer-Allee 8-10, Telefon 06101/80 20 0, www.neeflappcom.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datenschutz; Hardware; Software
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	50-250
Hotline	Ja
Vorort-Service	ab 6 Stunden, je nach Vereinbarung
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	Überprüfung anhand ISO-17799 (information security management); automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Managed Firewall Services; Intrusion Detection Systeme; Auditing Software
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme; Auditing Software
Hardwarekomponenten	Backup Systeme; Chipkarten/-leser; Firewall; Smart Cards; Token
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service; Administrator; IT-Systemingenieur; speziell geschultes Personal

nGENn GmbH

61250 Usingen, Schloss Kransberg, Telefon 06081/68 23 00, www.ngenn.net

Kerngeschäft	Betriebssystemsicherheit; Software
Zielgruppe	Großkonzerne
Mitarbeiter	< 50
Hotline	Nein
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; FREEBSO, Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Managed Firewall Services; Intrusion Detection Systeme; Auditing Software
Sicherheitsprodukte - Implementierung	Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Backup Systeme; Chipkarten/-leser; Firewall; Smart Cards; Token
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur); sonstiger Trustcenter-/PKI-Betreiber; Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service

NSG Netzwerk - Service GmbH

63225 Langen, Robert-Bosch-Straße 25, Telefon 06103/20 66 0, www.nsg.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datensicherung; Software
Zielgruppe	mittlere Unternehmen
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Keine Angben
Branchenlösungen	Ja
Sicherheitsauditing	Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme; Auditing Software
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme; Auditing Software
Hardwarekomponenten	Biometrische; Backup Systeme; Firewall; Smart Cards; SAN-Konzepte
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	speziell geschultes Personal

OR Network

35305 Grünberg, Eiserne Hand 11, Telefon 064 01/22 01 20, www.or-network.net

Kerngeschäft	Hardware; Software; ISP Serverhosting
Zielgruppe	mittlere Unternehmen
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 12 Stunden
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Firewallprodukte; Managed Firewall Services;
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Biometrische; Backup Systeme; Firewall
Kryptografische Produkte	sonstige Registrierungsstelle
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service; Informatiker; Administrator; IT-Systemingenieur; speziell geschultes Personal

Pallas it-solutions GmbH

60329 Frankfurt am Main, Kaiserstraße 40, Telefon 069/264 86 50, www.pallassoft.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datenschutz; Datensicherung; Hardware; Software
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 4 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Firewallprodukte; Managed Firewall Services; Intrusion Detection Systeme;
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme; Auditing Software
Hardwarekomponenten	Backup Systeme; Firewall; Smart Cards; Token
Kryptografische Produkte	sonstiger Trustcenter-/PKI-Betreiber; sonstige Registrierungsstelle; Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	Gehört zum Service; Administrator

PECOS AG

65205 Wiesbaden, Otto-von-Guericke-Ring 7, Telefon 061 22/50 45 0, www.pecos.de

Kerngeschäft	Keine Angaben
Zielgruppe	Großkonzerne
Mitarbeiter	< 50
Hotline	Keine Angaben
Vorort-Service	Keine Angaben
Schulung	Keine Angaben
Branchenlösungen	Nein
Sicherheitsauditing	BSI-IT-Grundschutzzertifikat; Überprüfung anhand ISO-17799 (information security management); automatisierte Sicherheitstests von aussen (z.B. IP-Scans); persönliche Sicherheitstests von aussen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Keine Angaben
Kenntnisse zur Implementierung	Keine Angaben

s.a.d. System Analyse und Design GmbH

34131 Kassel, Ludwig-Erhard-Straße 12, Telefon 0561/31 67 95 0, www.sad-net.de

Kerngeschäft	Betriebssystemsicherheit; Datenschutz; Datensicherung; Software
Zielgruppe	kleine Unternehmen; mittlere Unternehmen
Mitarbeiter	< 50
Hotline	Nein
Vorort-Service	Keine Angaben
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); Überprüfen von Netzwerkkonzepten und Netzwerken, Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Firewallprodukte
Sicherheitsprodukte - Implementierung	Antivirensoftware; Firewallprodukte
Hardwarekomponenten	Firewall
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service; durchschnittliche PC-Kenntnisse reichen

SECARTIS AG

63263 Neu Isenburg, Martin-Behaim-Straße 2, Telefon 06102/74 34 06, www.secartis.com

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Kryptografie; Consulting
Zielgruppe	Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	Nein
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	BSI-Auditor für ISO-15408 (Common Criteria); automatisierte Sicherheitstests von aussen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme, Auditing Software
Hardwarekomponenten	Firewall; SUN Server
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Trifft nicht zu
Kenntnisse zur Implementierung	Gehört zum Service

SECUDE Sicherheitstechnologie Informationssysteme GmbH

64293 Darmstadt, Dolivostraße 11, Telefon 06151/82 89 70, www.secude.com

Kerngeschäft	Authentifizierung; Datenschutz; Datensicherung; Kryptografie; Software
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	Nein
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	TÜV-IT
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Chipkarten
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); sonstiger Trustcenter-/PKI-Betreiber; sonstige Registrierungsstelle; Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Administrator

SerCon GmbH

65760 Eschborn, Industriestraße 30-34, Telefon 06196/49 38 0, www.sercon.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; IT-Risikomanagement; PKI
Zielgruppe	Großkonzerne
Mitarbeiter	< 50
Hotline	Nein
Vorort-Service	Ja
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	Überprüfung anhand ISO-17799 (information security management); automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IT-Scans); persönliche Sicherheitstests von innen; Social Hacking und Überprüfung von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen von Härten von Betriebssystemen (Unix, NT, Win2K); Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	keine
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; Firewalls; Auditing Software
Hardwarekomponenten	keine
Kryptografische Produkte	keine
Betriebssysteme	keine Angaben
Kenntnisse zur Implementierung	keine Angaben

Siemens AG ICN VD CC4S (Projektabwicklung)

60052 Frankfurt am Main, Rödelheimer Landstraße 5-9, Telefon 069/79 72 17 9, www.siemens.de

Kerngeschäft	Consulting und Implementation von Security-Lösungen
Zielgruppe	Keine Angaben
Mitarbeiter	50-250
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	Überprüfung anhand ISO-17799 (information security management); automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte (Vertrieb/Implem.)	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Managed Firewall Services; Intrusion Detection Systeme; Auditing Software
Hardwarekomponenten	Biometrische; Backup Systeme; Chipkarten/-leser; Firewall; Smart Cards; Token; Andere
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptogr. Zwecke (z.B. Signatur); Registrierungsstelle (SigG-konform); sonst. Trustcenter-/PKI-Betreiber; sonstige Registrierungsstelle; Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service; Administrator; speziell geschultes Personal

Soultek GbR

35315 Homberg, Frankfurter Straße 93, Telefon 06633/91 11 0, www.soultek.de

Kerngeschäft	Betriebssystemsicherheit; Kryptografie; Software
Zielgruppe	kleine Unternehmen; mittlere Unternehmen
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Keine Angaben
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme;
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Backup Systeme; Firewall
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service

STEGANOS GmbH

60318 Frankfurt am Main, Eckenheimer Landstraße 17, Telefon 069 / 970 97 10, www.steganos.com

Kerngeschäft	Datensicherung; Kryptografie; Software; Steganographie
Zielgruppe	kleine Unternehmen; mittlere Unternehmen
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	Nein
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	Keine Angaben
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls
Sicherheitsprodukte - Implementierung	Personal Firewalls
Hardwarekomponenten	Token
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	durchschnittliche PC-Kenntnisse reichen

Steria GmbH

63225 Langen, Robert-Bosch-Straße 52, Telefon 06103 / 76 14 62 8, www.steria.de

Kerngeschäft	Authentifizierung; Datenschutz; Datensicherung; Kryptografie; Betriebssystemsicherheit; Software
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Firewallprodukte
Sicherheitsprodukte - Implementierung	Antivirensoftware; Firewallprodukte
Hardwarekomponenten	Backup-Systeme; Chipkarten/-leser; Firewall; Smart Cards
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur); Registrierungsstelle (SiG-konform); Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service; IT-Systemingenieur; durchschnittliche PC-Kenntnisse reichen

SYMAX BUSINESS SOFTWARE AG

65189 Wiesbaden, Frankfurter Straße 28, Telefon 06 11/900 36 40, www.symax.de

Kerngeschäft	Betriebssystemsicherheit; Software
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	Ab 6 Stunden
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; Intrusion Detection Systeme; Auditing Software
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; Intrusion Detection Systeme; Auditing Software
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	Gehört zum Service; Administrator; speziell geschultes Personal

Systemberatung Axel Dunkel GmbH

65830 Kriftel, Gutenbergstraße 5, Telefon 06192/99 88 0, www.dunkel.de

Kerngeschäft	Security Service
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb >12 Stunden
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, NT, W2K; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Firewallprodukte; Managed Firewall Services; Intrusion Detection Systeme
Sicherheitsprodukte - Implementierung	Antivirensoftware; Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Firewall; Token
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	Gehört zum Service

T-Systems ISS GmbH

65760 Eschborn, Mergenthalerallee 38-40, Telefon 061 96/96 14 41, www.t-systems.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datenschutz; Datensicherung; Hardware, Kryptografie; Software; Andere
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	50-250
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	BSI-IT-Grundschutzzertifikat; BSI-Auditor für ISO-15408 (Common Criteria); Überprüfung anhand ISO-17799 (information security management); automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Social Hacking, Überprüfen von physischen Zutrittskontrollen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Keine Angaben
Sicherheitsprodukte - Implementierung	Keine Angaben
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	Keine Angaben
Betriebssysteme	Keine Angaben
Kenntnisse zur Implementierung	Keine Angaben

Tiscali Business GmbH

63303 Dreieich, Robert-Bosch-Straße 32, Telefon 06103/91 66 26, www.tiscali-business.de

Kerngeschäft	Betriebssystemsicherheit; Datenschutz; Datensicherung
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	>250
Hotline	Ja
Vorort-Service	innerhalb 12 Stunden
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: Unix, Linux, NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte; Managed Firewall Services
Sicherheitsprodukte - Implementierung	Antivirensoftware; Firewallprodukte
Hardwarekomponenten	Backup Systeme; Firewall; Smart Cards; Token
Kryptografische Produkte	Kein Angaben
Betriebssysteme	Windowsderivate; Unixderivate; OS/X
Kenntnisse zur Implementierung	Gehört zum Service; Administrator; IT-Systemingenieur; speziell geschultes Personal

Utimaco Safeware AG

61440 Oberursel, Hohemarkstraße 22, Telefon 06171/88 0, www.utimaco.de

Kerngeschäft	Authentifizierung; Betriebssystemsicherheit; Datenschutz; Kryptografie
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	>250
Hotline	Ja
Vorort-Service	Nach Vereinbarung
Schulung	Ja
Branchenlösungen	Keine Angaben
Sicherheitsauditing	BSI-IT-Grundschutzzertifikat; Persönliche Sicherheitstests von innen; Überprüfen von Netzwerkkonzepten und Netzwerken
Sicherheitsprodukte - Vertrieb	Personal Firewalls
Sicherheitsprodukte - Implementierung	Personal Firewalls
Hardwarekomponenten	Biometrische; Chipkarten/-leser; Smart Cards;
Kryptografische Produkte	Produktion/Vertrieb von Chipkarten für kryptografische Zwecke (z.B. Signatur); Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur); Infrastruktur für PKI-Betreiber (Hard-,Software)
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	Gehört zum Service; Administrator; IT-Systemingenieur; speziell geschultes Personal

VISTEC Internet Service GmbH

65203 Wiesbaden, Hagenauer Straße 42, Telefon 0611/22 03 9, www.vistec.net

Kerngeschäft	Internet Service
Zielgruppe	kleine Unternehmen; mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Firewallprodukte; Managed Firewall Services; Intrusion Detection Systeme
Sicherheitsprodukte - Implementierung	Antivirensoftware; Firewallprodukte; Intrusion Detection Systeme
Hardwarekomponenten	Keine Angaben
Kryptografische Produkte	sonstiger Trustcenter-/PKI-Betreiber
Betriebssysteme	Windowsderivate; Unixderivate
Kenntnisse zur Implementierung	durchschnittliche PC-Kenntnisse reichen

Whale Communications GmbH

63150 Heusenstamm, Frankfurter Straße 3, Telefon 061 04 / 669 60, www.whale-com.com

Kerngeschäft	Datenschutz; Hardware; Software
Zielgruppe	mittlere Unternehmen; Großkonzerne
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Ja
Sicherheitsauditing	automatisierte Sicherheitstests von außen (z.B. IP-Scans); persönliche Sicherheitstests von außen (z.B. Black Box, Tiger Teams); automatisierte Sicherheitstests von innen (z.B. lokale IP-Scans); persönliche Sicherheitstests von innen; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Intrusion Detection Systeme; Auditing Software
Sicherheitsprodukte - Implementierung	Intrusion Detection Systeme, Auditing Software
Hardwarekomponenten	Physikalische Trennung der Netze
Kryptografische Produkte	sonstige Registrierungsstelle
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	Gehört zum Service; Administrator

4 sale IT-Service GmbH

65462 Gustavsburg, Ginsheimer Straße 1, Telefon 06134 / 55 72 06, www.4sale-it.de

Kerngeschäft	Beratung und Implementierung
Zielgruppe	mittlere Unternehmen
Mitarbeiter	< 50
Hotline	Ja
Vorort-Service	innerhalb 6 Stunden
Schulung	Ja
Branchenlösungen	Nein
Sicherheitsauditing	Überprüfen von Netzwerkkonzepten und Netzwerken; Überprüfen und Härten von Betriebssystemen: NT, W2K; Überprüfen von Backup-Konzepten; Sicherheitsberatung der Kunden
Sicherheitsprodukte - Vertrieb	Antivirensoftware; Personal Firewalls; andere Firewallprodukte
Sicherheitsprodukte - Implementierung	Antivirensoftware; Personal Firewalls; andere Firewallprodukte
Hardwarekomponenten	Backup Systeme; Chipkarten/-leser; Firewall
Kryptografische Produkte	Produktion/Vertrieb von Chipkartenlesern für kryptografische Zwecke (z.B. Signatur)
Betriebssysteme	Windowsderivate
Kenntnisse zur Implementierung	Gehört zum Service

7 Glossar

ActiveX Eine Microsoft-Entwicklung, die plattformunabhängig Softwaremodule für andere Anwendungen zugänglich macht (etwa Webbrowser). Browser ohne ActiveX können durch ein entsprechendes ActiveX-Applet erweitert werden. → Browser

AES (Advanced Encryption Standard) Die offizielle Standardverschlüsselung der amerikanischen Normungsbehörde (NIST). Der Algorithmus, der dem AES zugrunde liegt, heißt ursprünglich Rijndael und arbeitet mit einer Schlüssellänge von bis zu 256 Bit. → Schlüssellänge

Advanced Encryption Standard → AES

Algorithmus Eine mathematische Funktion, die der Ver- und Entschlüsselung von Dateien dient.

Application Service Provider → ASP

ASP (Application Service Provider) Ein Dienstleister, der Anwendungen (Applikationen) über das Internet oder gesicherte Datenleitungen dem Anwender gegen eine Nutzungsgebühr zur Verfügung stellt.

Asymmetrische Verschlüsselung Ein Verfahren, bei dem zum Ver- und Entschlüsseln einer Nachricht unterschiedliche Schlüssel verwendet werden.
→ PKI, Public Key

Attachment (engl.) Anhang (etwa an ein eMail)

Auditing Die Beurteilung der bestehenden Sicherheitsvorrichtungen und Richtlinien einer Organisation.

Ausbreitungsvektoren Eine geometrische Beschreibung von Verbreitungswegen (z. B. dem Outlook-Prgramm).

Authentifizierung Die Echtheit einer Angabe bestätigen, etwa bei Überprüfung der Zugangsberechtigung zu einem Netzwerk.

Backbone (engl. Rückgrat) Überregionales, schnelles Netzwerk, das weitere Netzwerke verbindet.

Backup Eine Sicherheitskopie, die sicherstellt, dass auch bei einem Totalausfall eines Netzwerks/Rechners die Daten nicht vollständig verloren gehen.

Biometrie Die Identifikation eines Lebewesens anhand unverwechselbarer Körpermerkmale.

Biometrische Verfahren nutzen unverwechselbare Körpermerkmale zur Identifizierung eines Anwenders, etwa durch Überprüfung des Fingerabdrucks.

Black Box Test Überprüfung der Sicherheit eines IT-Systems ohne Insiderwissen.
→ Tiger Team, White Box Test

Breach (eng. Bresche) nennt man einen erfolgreichen Angriff auf geschützte Dateien.

Browser Software, die den Zugang zum ermöglicht. Mit Hilfe des Browsers können die Seiten im Internet aufgerufen und in ihnen geblättert werden.

Brute Force Angriffe Versuch, durch das systematische ausprobieren aller möglichen Passwörter Zugang zu einem System zu erlangen.

BSI (Bundesamt für Sicherheit in der Informationstechnik) Bundesbehörde mit Sitz in Bonn, dem Bundesminister des Innern der Bundesrepublik Deutschland unterstellt.
www.bsi.de

Business Recovery → Disaster Recovery

CC → Common Criteria

CCITSC (Common Criteria for Information Technology Security) → Common Criteria

CERT (Computer Emergency Response Team) Organisation, die über bekanntgewordene Sicherheitslücken und Bedrohungen informiert.
www.cert.org, www.bsi.bund.de/bsi-cert

CGI (Common Gateway Interface) Bezeichnung für eine Schnittstelle, über die WWW-Server Daten mit externen Programmen austauschen, bspw. zum Bearbeiten von Datenbankabfragen.

Client Computer, der von anderen Computern (den Servern) Daten abfragt, bzw. übermittelt bekommt. Auch ein Browser wird als Client bezeichnet.

Colocation Provider Stellt Räumlichkeiten inklusive unterbrechungsfreier Stromversorgung für die IT-Ausrüstung, Server etc. zur Verfügung.

Common Criteria (engl. gemeinsame Kriterien) Ursprünglich von Deutschland, Kanada, Großbritannien, Frankreich, Niederlanden und USA erarbeitete Kriterien zur Bewertung der Sicherheit von Informationstechnik. CC 2.1 ist durch die ISO unter der Nummer 15408 internationaler Standard geworden. → ISO: **www.bsi.de/cc/**

Computerviren → Viren

Cookies (oder Tokens) sind kleine Datenpakete, die von einem Webserver auf den ihn besuchenden Rechner abgelegt werden. Diese Datenpakete enthalten kleine Dossiers über den Nutzer.

Cracker Person, die unerlaubt in einen Rechner oder ein Netzwerk eindringt, um dort Schaden anzurichten (Manipulation vorhandener Dateien, Entfernen oder Kopieren geschützter Dateien). → Hacker

CUG (Closed User Group) Die amerikanische Bezeichnung für eine geschlossene Benutzergruppe; damit bezeichnet man Bereiche eines Systems, z. B. einen Dateibereich oder ein Diskussionsforum, zu denen nur bestimmte User Zugang haben.

Datenintegrität Der Zusammenhalt von Daten während einer Verarbeitung in einem Computer, z. B. bei Speichervorgängen oder Datenübertragungen.

DDOS → Distributed Denial of Service Attacken

Defacement Das Verändern einer im Web erreichbaren Seite; meist als öffentlicher Nachweis genutzt, dass ein erfolgreicher Angriff durchgeführt wurde.

Denial of Service Attacken (auch Flooding genannt) Versuch, ein System durch eine Überflutung mit Anfragen zum Zusammenbruch zu bringen.

DE-NIC Zentrale deutsche Vergabestelle des Internet für die Vergabe von Domainnamen und IP-Adressen; im Who-Is Verzeichnis von **www.denic.de** kann man überprüfen, ob der gewünschte Domainname (unter .de) schon reserviert oder gar angeschlossen ist und Informationen über die Anmelder erhalten.

DES (Data Encryption Standard). Ein von IBM entwickeltes Verschlüsselungssystem, das seit 1977 von der US-Regierung als offizielles Datenchiffriersystem eingesetzt wird. DES basiert auf dem klassischen (symmetrischen) System geheimer Schlüssel (Private Keys) zum De-/Codieren elektronischer Nachrichten. → Private Key

Disaster Recovery (auch Business Recovery), beschreibt die Maßnahmen, die für den Fall eines Notfalles zur Sicherstellung der Verfügbarkeit der EDV vorgesehen sind.

Distributed Denial of Service Attacken Ähnlich dem Denial of Service Angriff, wobei jedoch der Angriff nicht von einem System aus, sondern von einer Vielzahl von koordiniert agierenden Systemen durchgeführt wird. → Denial of Service Attacken

DMZ (Demilitarisierte Zone) Ein durch zwei Firewalls an der Schnittstelle von Inter- und Intranet errichteter Bereich, der weder von seiten des Inter- noch des Intranets zugänglich ist. → Firewall, Intranet

DNS (Domain Name System) Bezeichnung für das im Internet verwendete System von hierarchisch gegliederten Bereichsnamen. Über die auf jedem Internet-Server vorhandenen Domain-Datenbanken wird die Zuordnung der logischen DNS-Namen in numerische Server-Adressen vorgenommen. So wird bspw. aus einem logischen DNS-Namen wie www.hessen-infoline.de eine numerische Adresse wie 194.64.40.214

DoD (Department of Defense) US-amerikanisches Verteidigungsministerium

DOS → Denial of Service Attacken

Download Das Herunterladen einer Datei von einem anderen Rechner (bspw. via Internet)

EAL (Evaluation Assurance Level) Eine Skala von 0 bis 7, die die Vertrauenswürdigkeit eines Schutzprofils beschreibt.

Einmal-Passwort wir nach einmaliger Verwendung ungültig. Entschärft die Problematik bei gestohlenen oder abgehörten Passwörten.

Elektronische Wasserzeichen Verfahren, das überwiegend zum Schutz von Urheberrechten verwendet wird.

Encryption (engl. Verschlüsselung)

Ethernet Technischer Standard der Verbindungen innerhalb eines LAN. → LAN

Evaluation Assurance Level → EAL

Evaluieren bewerten, beurteilen

Extension Dateierweiterung / -endung; der Teil des Dateinamens, der nach dem letzten Punkt „.“ steht. Die Extension eines MS-Word Dokuments ist z.B. „.doc“, die einer HTML-Datei lautet „.htm“ oder „.html“.

Extranet Intranet-Datentransfer über das Internet (unter Anwendung von besonderen Sicherheitsmaßnahmen). → Intranet

File Transfer Protocol → FTP

Firewall (engl. Brandmauer) System zum Schutz vor unberechtigtem Zugriff auf Daten und Systeme eines Netzwerkes.

Flooding (engl. Überfluten) → Denial of Service Attacken

FTP (File Transfer Protocol) dient der Übertragung von Dateien zwischen Rechnern im Internet

GPG (Gnu Privacy Guard) Von der Open-Souce Gemeinde entwickeltes Verschlüsselungssystem, dessen Quellcode jedem offensteht. Als Konkurrenz zu PGP entwickelt. → PGP: **www.gnupg.org**

Hacker Person, die aus Neugier oder dem Wunsch, die Machbarkeit zu beweisen, unerlaubt in einen Rechner oder ein Netzwerk eindringt. → Cracker

Hashwert Ein mit einer Quersumme vergleichbarer Wert; durch den Vergleich der Hashwerte vor und nach der Übertragung einer Nachricht lässt sich sicherstellen, dass keine Manipulation erfolgte.

Hoax (engl. Zeitungsente) falsche Virenmeldung, die in der Regel mit der Bitte um Weiterleitung versehen versendet wird. Sollte auch nicht an den Administrator weitergeleitet werden.

Hosting bezeichnet die Bereitstellung von Servern, Webspace und Ähnlichem.

HTML (Hypertext Markup Language) ist eine von Berners-Lee entwickelte Seitenbeschreibungssprache für Seiten im World Wide Web. Mit HTML lassen sich Texte und andere Elemente wie Grafiken auf einer Internetseite formatieren; die Funktionen von HTML werden durch das „WWW Consortium“ (W3C) weiterentwickelt.

Hub (engl. Angelpunkt, Zentrum) Ein Gerät, das die Anschlussbündelung von verschiedenen Netzgeräten über einen zentralen Punkt an das Verkabelungssystem erlaubt.

IDS (Intrusion Detection System) Ein hard-/softwarebasiertes System zur Erkennung und Abwehr von internen und externen Angriffen auf das Unternehmensnetz

IKT Informations- und Kommunikationstechnologie

Integrität → Datenintegrität

Internet Protocol → IP

Internet Service Provider → ISP

Intranet Bezeichnung für ein geschlossenes Netzwerk (i.d.R. Firmennetzwerk), das jedoch Methoden und Techniken des offenen Internets verwendet.

Intrusion Detection System → IDS

IP (Internet Protocol) Die technische Grundlage des Internet.

IP-Adresse Eine für jeden an das Internet angeschlossenen Computer eindeutige Folge von vier Zahlen, bei der jede Zahl Werte von 0 bis 255 annehmen kann. Zum Beispiel 194.64.40.214. Mit Hilfe seiner IP-Adresse kann jeder ins Internet eingebundene Computer eindeutig adressiert werden.

IP-Scan Automatisierte Überprüfung eines Netzwerks auf Sicherheitslücken.

IP Spoofing Versuch, durch den Gebrauch einer gefälschten IP-Adresse Zugang zu einem fremden System zu erlangen. → IP, IP-Adresse

IPSEC → IP Security Protocol

IP Security Protocol (IPSEC) Kryptographisches Netzprotokoll zum Schutz von IP-Paketen; IPSEC wird häufig zum Aufbau von sicheren Netzverbindungen (VPN) verwendet. → VPN

ISO International Organization for Standardization. Vergleichbar mit dem europäischen CEN oder deutschem DIN, entwickelt Normen für verschiedenste Bereiche des Lebens; häufig technische Normung, z.B. ISO 17799. Qualitätsmanagement. : **www.iso.ch**

ISP (Internet Service Provider) Dienstleister, der Internetdienste wie Internetzugang und Hosting von Websites anbietet. → Hosting, Website

IT Informationstechnologie

ITSEC (Information Technology Security Evaluation Criteria) In mehreren europäischen Ländern verwendete, übereinstimmende Kriterien zur Bewertung der Sicherheit von IT-Systemen und Komponenten.

ITSK (IT-Sicherheitskriterien) 1989 von der Zentralstelle für Sicherheit in der Informationstechnik (ein Vorläufer des BSI) erstellte Kriterien zur Sicherstellung der Sicherheit in IT-Systemen. In der ITSEC aufgegangen. → BSI, ITSEC

Java Eine von der Firma Sun entwickelte Programmiersprache, die plattformunabhängig arbeitet.

Java-Applet Ein in Java geschriebenes Programm, für dessen Nutzung man einen javafähigen Browser benötigt. → Browser, Java

JavaScript Eine Scriptsprache, die als Erweiterung zu HTML gedacht war. → HTML

Java-Servlet Ein in Java geschriebenes Programm, das auf einem Server hinterlegt ist. → Java, Server

Klartext Eine unverschlüsselte Nachricht.

KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) Gemäß dieses Gesetzes ist der Vorstand/die Geschäftsführung für die Risikovorsorge des Unternehmens verantwortlich, d.h. er/sie ist für die Einrichtung eines Prozesses für die Etablierung der Unternehmenssicherheit einschließlich der IT-Sicherheit verantwortlich und kann für das Fehlen dieses Prozesses persönlich haftbar gemacht werden.

Kryptografie Die Ver- und Entschlüsselung von Informationen.

LAN (Local Area Network) Lokales, räumlich begrenztes Netzwerk, oft auf Gebäude oder Gebäudeteile beschränkt. Aufgrund ihrer geringen räumlichen Ausdehnung sind LAN gut geeignet, hohe Bandbreiten zu übertragen. → WAN

L2TP (Layer-2-Tunneling Protocol) Protokoll zum Aufbau sicherer Netzverbindungen (VPN) → VPN

Local Area Network → LAN

Login Eingabe von Name und Passwort zur Erlangung der Zugriffsberechtigung.

Makro Ein Kleinstprogramm, das innerhalb anderer Programme, wie etwa zur Textverarbeitung oder Tabellenkalkulation, häufig genutzte Aufgaben selbständig löst.

Malware (malicious software) Progamme oder Daten, die mit der Absicht erstellt wurden, Schaden anzurichten. Darunter fallen etwa → Trojaner, Viren und Würmer.

Mailbombe Ein eMail, das vorsätzlich mit einer schadenstiftenden Datei versehen wurde.

Man in the Middle Attacke Versuch eines Hackers, sich während des Kommunikation zweier Parteien unbemerkt zwischen diese zu platzieren. → Hacker

Managed Security Provider Stellt IT-Sicherheit auf Mietbasis zur Verfügung.

Managed Service Provider Stellt IT-Infrastruktur auf Mietbasis zur Verfügung.

NSA (National Security Agency) US-amerikanischer Sicherheitsdienst

Patch (engl. Flicken, Pflaster) Ein Patch dient dazu, im nachhinein aufgetauchte Fehler einer Software zu beheben.

PDA (engl. Personal Digital Assistant) Persönlicher Digitaler Assistent, elektronisches Notizbuch

Penetrationstest Ein Netzwerk, Rechner oder Programm wird durch einen Test darauf hin überprüft, ob im praktischen Betrieb bekannte Schwachstellen das Eindringen in das System ermöglichen.

Periphere An eine zentrale Recheneinheit angeschlossene Geräte.

Personal Firewall (auch Desktop Firewall) Software auf dem lokalen Rechner, der den Datenverkehr zwischen Rechner und Netzwerk/Internet überprüft. → Firewall

PGP (Pretty Good Privacy) Name eines von Phil Zimmermann entwickelten Programms, das zur elektronischen Signatur und zur Verschlüsselung benutzt wird. Vom Sicherheitsniveau den PKI-Lösungen weit unterlegen, benötigt es eine weniger aufwändige Infrastruktur, was zu einer schnellen Verbreitung beitrug. → GPG, PKI

PIN (Personal Identification Number) Die PIN hat die Aufgabe, einen Nutzer zu authentifizieren.

PKI (Public Key Infrastructure) So bezeichnet man die technische und organisatorische Infrastruktur, die zur Erstellung, Verwaltung und Verteilung von Schlüsseln benötigt wird. PKI ist ein Kernelement zur Verwirklichung der qualifizierten elektronischen Signatur.

Plaintext → Klartext

Plug-in nennt man Programme und Programmteile, die in andere Programme integriert werden, um deren Leistungsfähigkeit zu erhöhen. Häufig in Verbindung mit Browsern verwendet. → Browser

Policy Verfahrensweise, Richtlinie

PPTP (Point to Point Tunneling Protocol) Protokoll zur Realisierung von VPN & VPN

Private Key Der nur dem Besitzer bekannte Entschlüsselungsschlüssel, der ein Dechiffrieren einer mit Hilfe des komplementären Public Key verschlüsselten Nachricht ermöglicht. → Asymmetrische Verschlüsselung, PKI, Public Key

Public Key Der zur asymmetrischen Verschlüsselung bekanntgegebene Verschlüsselungsschlüssel. Nur der Private Key kann die mit diesem Schlüssel chiffrierte Nachricht dechiffrieren. → Asymmetrische Verschlüsselung, PKI, Private Key

Public Key Infrastructure → PKI

RSA Der nach seinen Entwicklern Rivest, Shamir und Adleman benannte RSA-Algorithmus ist die Grundlage der Public-Key-Verschlüsselungsverfahren.
→ Asymmetrische Verschlüsselung

Schlüssellänge gibt die Länge eines kryptografischen Schlüssels in Bit an.

Server Rechner, der Anwendungen und Daten bereitstellt, auf die von anderen Rechnern zugegriffen wird.

Serverhousing Bereitstellung von Räumlichkeiten für die Aufstellung von Servern; wird unter anderem von Colocation Providern angeboten. → Colocation Provider, Server

SET ist ein Protokoll, das maßgeblich unter der Leitung von Visa/Mastercard entwickelt wurde, um den elektronischen Zahlungsverkehr vor Eingriffen zu sichern.

Skalierbarkeit Die Möglichkeit, die Anzahl der Nutzer oder der Kapazitäten einer Softwarelösung zu erhöhen, ohne die Anwendungssoftware oder das System in größerem Stil zu modifizieren.

Skript Kiddies Zumeist jugendliche Hacker, die meist fremdentwickelte Software einsetzen, um mit diesen automatischen Tools eine möglichst hohe Anzahl von Webservern und Firmennetzwerken zu knacken. Ziel ist zumeist die Außendarstellung der eigenen Kenntnisse. Häufig vorkommend, typischerweise geringer, eher technischer Schaden. → Hacker

SmartCard Chipkarte, auf der Verschlüsselungsinformationen gespeichert sind, die nicht auslesbar sind.

SOAP (Simple Objekt Access Protocol) Ein Standard für den elektronischen Geschäftsverkehr zwischen Unternehmen.

Social Hacking (auch Social Engineering) Versuch, durch das Ausspionieren des sozialen Umfeldes einer Person an mögliche Passwörter oder wichtige Unternehmensinformationen zu gelangen. Typischerweise durch Telefonate unter falschem Vorwand bei Sekretariaten, Kollegen, Empfang, PR-, IT-Abteilung oder auch Begehungsversuche am Arbeitsplatzes (durch Kollegen oder Externe).

Softwarebombe Software, die sich bis zur Erfüllung bestimmter Bedingungen „normal" verhält; nach Erfüllung der Bedingungen wird aber ein zerstörerisches Werk in Gang gesetzt.

Spiegelserver Ein Ersatzserver, der so konfiguriert ist, dass er bei Ausfall des eigentlichen Servers dessen vollständige Funktionalität übernimmt. → Server

Spyware Software, die vom Anwender unbemerkt Daten sammelt und versendet. Häufig als Trojaner auf Rechner transportiert. → Trojaner

SSL (Secure Socket Layer) Ein Protokoll, das es ermöglicht, verschlüsselte Nachrichten über das Internet zu verschicken. SSL wendet „Public Key Encryption" an, um die Daten zwischen dem Browser und einem gegebenen Server zu versenden (z. B. Kreditkarteninformationen). Eine URL, die mit „https://" beginnt, zeigt an, dass eine SSL-Verbindung besteht. → Public Key, URL

Steganografie Verschlüsselung mit Hilfe grafischer Elemente, ähnlich einem Wasserzeichen. Besonders zum Schutz von Urheberrechten verwendet.

Symmetrische Verschlüsselung Sowohl zum Ver- als auch zum um Entschlüsseln wird der gleiche Schlüssel verwendet. → Asymmetrische Verschlüsselung

TCP / IP (Transmission Control Protocol / Internet Protocol) Ein Protokoll, das die Kommunikation verschiedener Netze untereinander ermöglicht. Am 1. Januar 1983 wurde es zum offiziellen Standard erhoben.

TCSEC (Trusted Computer System Evaluation Criteria) ein 1983 vom us-amerikanischen Verteidigungsministerium aufgestellter Katalog mit Anforderungen an Funktion, Entwicklungsprozess und Dokumentation von IT-Systemen.

Tiger Team Eine Gruppe beauftragter IT-Spezialisten, deren Aufgabe es ist zu versuchen, in die Systeme des Auftraggebers einzudringen. Dabei gelangen alle Werkzeuge echter Hacker zum Einsatz. Durch diese Versuche kann die Sicherheit der Systeme in der Praxis überprüft und Schwachstellen aufgedeckt werden. → Hacker

Thin Clients Ein Computer, der nur mit dem notwendigsten ausgestattet ist; die Daten sowie Programme werden vom Server über ein Netzwerk bereitgestellt. → Server

Trojaner oder „Trojanische Pferde“ sind Dateien, die für den Anwender nicht erkennbare Programmbestandteile beinhalten. In der Regel dienen diese Bestandteile der Spionage oder dem Manipulieren von Daten. → Spyware, Viren, Würmer

Trojanische Pferde → Trojaner

Tunnel Sichere Verbindung zwischen zwei Rechnern; wird häufig zum Aufbau eines VPN genutzt. → VPN

Update Neue Version einer Software

URL (Uniform Resource Locator). Adresse eines jeden Internet-Dokuments, bestehend aus Rechnername und Pfadangabe. Die URL der Startseite von „hessen-infoline“ lautet: http://www.hessen-infoline.de/index.cfm

USV unabhängige Stromversorgung

Viren sind Software-Fremdkörper, die Dateien angehängt werden und unterschiedlichste Reaktionen hervorrufen können. Eine wesentliche Eigenschaft eines Virus ist die Fähigkeit, sich selber zu reproduzieren und dadurch andere Rechner oder Netzwerke zu infizieren. Ein Virus kann nur in Kombination mit einem „Wirtsprogramm“ aktiv werden. → Würmer, Trojaner

Virtual Private Network → VPN

VPN (Virtual Private Network) Durch Verschlüsselung geschütztes Netzwerk innerhalb eines öffentlichen Netzes (Internet).

WAN (Wide Area Network) Netzwerk, dessen Endgeräte über große Distanzen verteilt sind. WANs verknüpfen mehrere LANs über Fernleitungen miteinander. → LAN

Webbrowser → Browser

Webserver Rechner, der Anwendungen und Dateien über das Internet bereitstellt.

White Box Test Überprüfung der Sicherheit eines IT-Systems mit Insiderwissen, eventuell in Kooperation mit Mitarbeitern oder Administratoren.
→ Black Box Test, Tiger Team

Wide Area Network → WAN

Wireless LAN Ein auf drahtlosen Verbindungen aufgebautes Local Area Network.
→ LAN

Würmer sind vollständige, ablauffähige Programme, die sich selbständig in mindestens einen Rechner kopieren. Im Gegensatz zu einem Virus benötigt ein Wurm kein „Wirtsprogramm“. → Viren, Trojaner

8 Stichwortverzeichnis

A

ActiveX, 4
Anhänge, 4, 5
Administration, 29, 31, 43, 46
Antivirus-Software, 32
Anbieterverzeichnis, 52

B

Backups, 3, 7
Biometrie, 51
BSI, 24, 26, 35
BSI-Grundschutz, 2, 24, 39

C

Common Criteria, 26
Computerviren, 4, 10
Cracker, 3, 6

D

Datenschutz, 2, 23, 30, 44
Datenträgerhandling, 2, 3
Datenverschlüsselung, 2, 3
DDOS, 3, 5
Defacement, 8
Denial of Service Attacke, 5, 20
Distributed Denial of Service Attacke, 3, 5
DOS, 5, 20
Dritte, 14, 16, 27, 33, 39
DZI, 50

E

Echelon, 6
Einstellung von Personal, 13
eMail, 3, 4, 16, 23, 28, 43
Erstellung einer Sicherheitspolitik, 11, 12, 22; 33

F

Firmennetzwerke, 3, 43, 46
Firewalls, 3, 27, 44

G

Gegenmaßnahmen, 19, 21, 33
Grundschutzhandbuch, 24, 33, 35, 42

H

Hacker, 5, 6, 43
Haftung, 8, 25, 31
HTML-Mails, 4

I

Infrastruktur, 3, 8, 9, 14, 33, 44
Integrität, 18, 23, 33
IDS, 3, 29, 32
Intrusion Detection System, 3, 29, 32
ISO 17799, 24, 33
ITSK, 26
IT-Grundschutzhandbuch, 24, 35, 39, 42
IT-Grundschutz Zertifikat, 35,
IT-Sicherheit, 1, 9, 22, 33, 43, 48
IT-Sicherheits-Managementsystem, 24, 35, 37, 42
IT-Sicherheitsleitlinie, 25
IT-Sicherheitszertifikat, 34
IT-Standorte, 48

J

Java, 4
JavaScript, 4

K

KonTraG, 1, 8, 31

M

Makros, 4
Malware, 4
Managed Security Provider, 30
Meldepflicht, 14
Mitarbeiter, 3, 6, 10, 13, 15, 18, 22, 29, 31, 34, 39, 41, 46
Mitarbeiterschulung, 2, 13, 22
Motivation, 6, 7, 9

N

Neubewertung, 3
Notfallplanung, 15
Nutzerkennung, 15, 16

P

Passwortpolitik, 2
physische Sicherheit, 14, 22
private Nutzung, 10, 16
Protokollierung, 23, 30, 46
Public-Key-Kryptografie, 49

R

Redundanz, 3
Restrisiko, 17, 21, 33, 36, 43
Risikoanalyse, 12, 17, 21, 24, 36

S

Schäden, 7, 20, 31, 33
schützenswerte Güter, 17
Sicherheitsbeauftragter, 7
Sicherheitsmaßnahmen, 9, 14, 25, 30, 35, 42
Sicherheitspolitik, 2, 10, 17, 22, 24, 33, 44
Sicherheitsprozess, 7
Sicherheitsvorfall, 1
Skript Kiddies, 6, 8
SOAP, 28
statische Websites, 3

T

TCSEC, 25
Testierbarkeit, 9, 22
Transaktionsdaten, 3
Trojaner, 4
Tunnel, 28

U

Umsetzungskosten, 12, 45
Unabhängige Stromversorgung, 3
Unternehmenssicherheit, 1, 8

V

Verantwortung, 10, 12, 18, 22, 31, 33, 44
Verfügbarkeit, 3, 10, 18, 33
Versicherungspolice, 21, 34
Vertraulichkeit, 3, 13, 18, 22, 33
Vertraulichkeitsstufen, 13
VPN, 3, 28

W

Webserver, 2, 6, 31
Wirtschaftsspionage, 6
Würmer, 4, 31

Z

Zertifikate, 27, 34, 35
Zugriffsrechte, 15, 23

9 Die Aktionslinie hessen-infoline

hessen-infoline ist die Online-Aktionslinie des Hessischen Ministeriums für Wirtschaft, Verkehr und Landesentwicklung für professionelle Anwender, d. h. für Unternehmen, Kommunen und Online-Anbieter. Die Informationsplattform stellt besonders für kleine und mittlere Unternehmen Informationen mit Fokus auf den IT-Markt und das Internet bereit.

hessen-infoline bietet u. a. eine umfangreiche Online-Datenbank, in die sich hessische Online-Anbieter kostenlos eintragen können. Diese Datenbank erleichtert somit Unternehmen die Recherche nach Anbietern und Dienstleistungen bei einem Online-Projekt.

Das hessen-infoline-netzwerk bringt Online-Initiativen wie Arbeitskreise, Forschungseinrichtungen, Institute und Vereine zusammen. Im Netzwerk werden Erfahrungen und Materialien ausgetauscht und gemeinsame Aktivitäten durchgeführt.

Kommunen werden beraten und ins Internet begleitet von hessen-infoline-kommunal.

www.hessen-kommunal.de

Handwerk online dient als Informationsplattform für **hessische Handwerksunternehmen** und stellt zusammen mit den hessischen Handwerkskammern eine Datenbank mit über 23000 Handwerksbetrieben zur Verfügung.

www.handwerker-hessen.de

hessen-commerce informiert kleine und mittlere Unternehmen über die **Einsatzmöglichkeiten von eCommerce** und unterstützt speziell die nichtkommerziellen hessischen eCommerce-Kompetenzzentren. Darüber hinaus initiiert und begleitet hessen-commerce Förderprogramme wie das Einzelhandelsprogramm „200x5000“.

www.hessen-commerce.de

Besuchen Sie unsere Web-Site unter  **www.hessen-infoline.de**

10 hessen-media: Eine Initiative stellt sich vor

Den Wandel zur Informations- und Wissensgesellschaft aktiv gestalten – mit der Initiative hessen-media fördert die Hessische Landesregierung Multimedia-Anwendungen in allen Bereichen der Gesellschaft.

hessen-media: Was steckt dahinter?

Die Initiative der Hessischen Landesregierung bündelt die Potenziale der Multimedia-Technologien und macht sie für alle Bürger und Wirtschaftsbereiche nutzbar. So stärkt sie strategisch Hessens Position als innovativer Wirtschafts- und Technologiestandort im globalen Wettbewerb und verbessert die Arbeits- und Lebensbedingungen der Bürgerinnen und Bürger. Und das heißt konkret:

Die Anwendung fördern

Reale Projekte, von hessen-media gefördert, belegen den praktischen Nutzen von Multimedia. Standortsicherung, technische Innovation und gesellschaftliche Relevanz sind die Auswahlkriterien dafür. So ist sichergestellt, dass wirklich alle Bereiche von den technischen Neuerungen profitieren – von der Schule bis zum kleinen und mittelständischen Betrieb.

Die Umsetzung unterstützen

Entwicklung, Anwendung, Ausbildung: jeder dieser Punkte wird in das Konzept einbezogen. Das erfordert die Rasanz des multimedialen Fortschritts. Dafür wurde ein Netzwerk von Kompetenz-Zentren aufgebaut. Sie bieten Beratung und Know-how für die wichtigsten Schwerpunkte:

1. **Multimedia-Kompetenz-Zentren:** Multimedia-Anwender müssen neben technischen Kenntnissen auch die Fähigkeit entwickeln, sich im Angebot zu orientieren und selbstbestimmt auszuwählen. Das Netzwerk hessischer Multimedia-Kompetenz-Zentren entwickelt dafür Ausbildungsinhalte und berät Lehrkräfte, SchülerInnen, Eltern und Medienschaffende.
2. **Multimedia-Support-Center:** Kleine und mittelständische Unternehmen benötigen passgenaue Lösungen für den Multimedia-Einsatz. Die Support-Zentren informieren, qualifizieren, beraten und vermitteln geeignete Kooperationspartner.

Den Austausch anregen

Experten aller Fachrichtungen führen ihr Know-how in Fachbeiräten zusammen. So entstehen Kooperationen zwischen Projekten, neue Konzepte und Ideen – und unnötige Parallelarbeiten werden vermieden.

Sind Sie neugierig auf hessen-media? Auf unserer Homepage

www.hessen-media.de

finden Sie vielfältige Informationen zur Landesinitiative mit Kontaktadressen und Ansprechpartnern konkreter Projekte.

In diesen Themenbereichen gibt es Telematikprojekte:

- Bildung
- Telemedizin
- Umweltschutz
- Verkehr
- Wirtschaft
- Teleworking
- Verwaltung
- Sozialnetz
- Medienwirtschaft

Kontakt:
Geschäftsstelle hessen-media
c/o InvestitionsBank Hessen AG (IBH)
Abraham-Lincoln-Straße 38-42
65189 Wiesbaden
Telefon 06 11 / 7 74 - 2 31
Telefax 06 11 / 7 74 - 3 85
eMail info@hessen-media.de
Internet www.hessen-media.de

hessen » media
Hier ist die Zukunft