Hrsg.: Prof. Dr. Dr. h. c. A.-W. Scheer

Veröffentlichungen des Instituts für Wirtschaftsinformatik (IWi), Universität des Saarlandes

Im Stadtwald, Gebäude 14.1, D - 66123 Saarbrücken,
phone: (+49) 681-302-3106, fax: (+49) 681-302-3696,
email: iwi@iwi.uni-sb.de; http://www.iwi.uni-sb.de

Heft 146

M. Luzius, M. Ewig, A.-W. Scheer

Sicherheitsmanagement bei Internet-Anbindungen – Konzepte und Anwendungen

Juni 1998

Inhaltsverzeichnis

Zusammenfassung

Das Internet wächst weiter mit enormen Raten. Mittlerweile lautet die Frage, der sich jedes Unternehmen stellen muß, nicht mehr ob, sondern wie die Nutzung des Internet aussehen soll. E-Mail ist zur schnellen Kommunikation mittlerweile für viele unentbehrlich, im WWW steht eine unüberschaubare Menge an Informationen zur Verfügung. Eine Anbindung an das Internet ist allerdings keine Einbahnstraße, mit der man für sich die Außenwelt erschließt, sondern es können auch Außenstehende auf die eigenen Daten zugreifen.

Die Frage nach wirksamen Sicherheitsmaßnahmen muß daher eine grundlegende Rolle bei der Planung einer Internet-Anbindung spielen. In diesem Beitrag wird zunächst auf unterschiedliche Angriffspunkte hingewiesen und es wird ein Konzept vorgestellt, wie die wichtigsten Gefahren in die Überlegungen einbezogen werden können. Anschließend werden die Ergebnisse einer Studie des Instituts für Wirtschaftsinformatik vorgestellt, die einen Überblick über die tatsächliche Verbreitung von Schutz- und Abwehrmechanismen in unterschiedlichen Branchen gibt.

1 Einleitung

"... Im Internet - Information Superhighway - tummelt sich eine merkwürdige Ansammlung von Fahrzeugen: Busse mit Rasenmähermotoren, Sportwagen mit Fahrradfelgen,... . Sicherheitsgurte und Airbags gibt es nur ausnahmsweise; Türschlösser, Windschutzscheiben, ja sogar Bremsen und Lenkräder gelten als entbehrliches Sonderzubehör. Zu allem Überfluß sind sämtliche Fahrzeuginsassen maskiert. ..."[1]

Das einleitende Zitat beschreibt die herrschende Situation im Internet äußerst treffend. Jeder möchte sich im Internet bewegen und die damit verbundenen Möglichkeiten nutzen. Die Zahl der Internet-Anbieter und -Nutzer steigt nach wie vor exponentiell (vgl. Abbildung 1). Dabei erkennen nach wie vor nur wenige die möglichen Sicherheitsrisiken und setzen geeignete Schutzmaßnahmen ein.

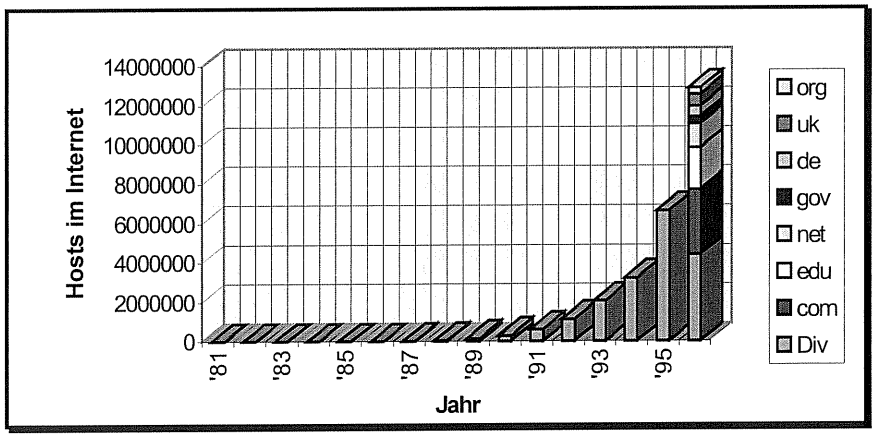


Abbildung 1: Hosts im Internet[2]

Gerade im Zuge einer Anbindung von Unternehmen an das Internet entstehen Gefahren, die – wie die vom Institut für Wirtschaftsinformatik (IWi) durchgeführte Studie zeigen wird – oftmals unterschätzt werden. Konnte das Computer Emergency Response Team (CERT) 1989 lediglich 192 gemeldete Einbrüche registrieren, so waren es 1995 schon über 3000[3].
Im Folgenden sollen nun die mit einer Internet-Anbindung verbundenen Gefahren, wie auch die möglichen organisatorischen und technischen Sicherheitskonzepte, die im Rahmen einer wirtschaftlichen Nutzung notwendig sind, kurz vorgestellt werden. Im Mittelpunkt wird die in diesem Zusammenhang durchgeführte Studie stehen.

---

1 vgl. Wallich, P. (Cracker), S.84
2 vgl. ❁ http://www.nw.com

2 Sicherheitsmanagement

Im englischen wird der Begriff der Sicherheit in zwei unterschiedliche Bereiche aufgeteilt. „*Safety*" steht dabei für die Sicherheit, keine Gefährdung Dritten gegenüber zu bewirken. „*Security*" heißt dagegen, daß ein System sicher gegenüber Beeinträchtigungen von außen ist. Im Weiteren wird Sicherheit immer im Sinne von „Security" verstanden.

Aufgabe eines Sicherheitsmanagements ist es, Risiken zu erkennen, zu bewerten und bestmöglich zu beherrschen. Dazu gehört zunächst eine Risikoanalyse, um das bestehende Gesamtrisiko ermitteln zu können. Danach ist dieses Risiko stufenweise so weit zu reduzieren, daß das verbleibende Restrisiko für das Unternehmen und die Internet-Nutzer quantifizierbar und akzeptabel ist. Eine 100%ige Sicherheit wird bei einer Internet-Anbindung allerdings niemals zu erreichen sein. Die folgende Abbildung zeigt die einzelnen Stufen zur Reduktion des Gesamtrisikos.

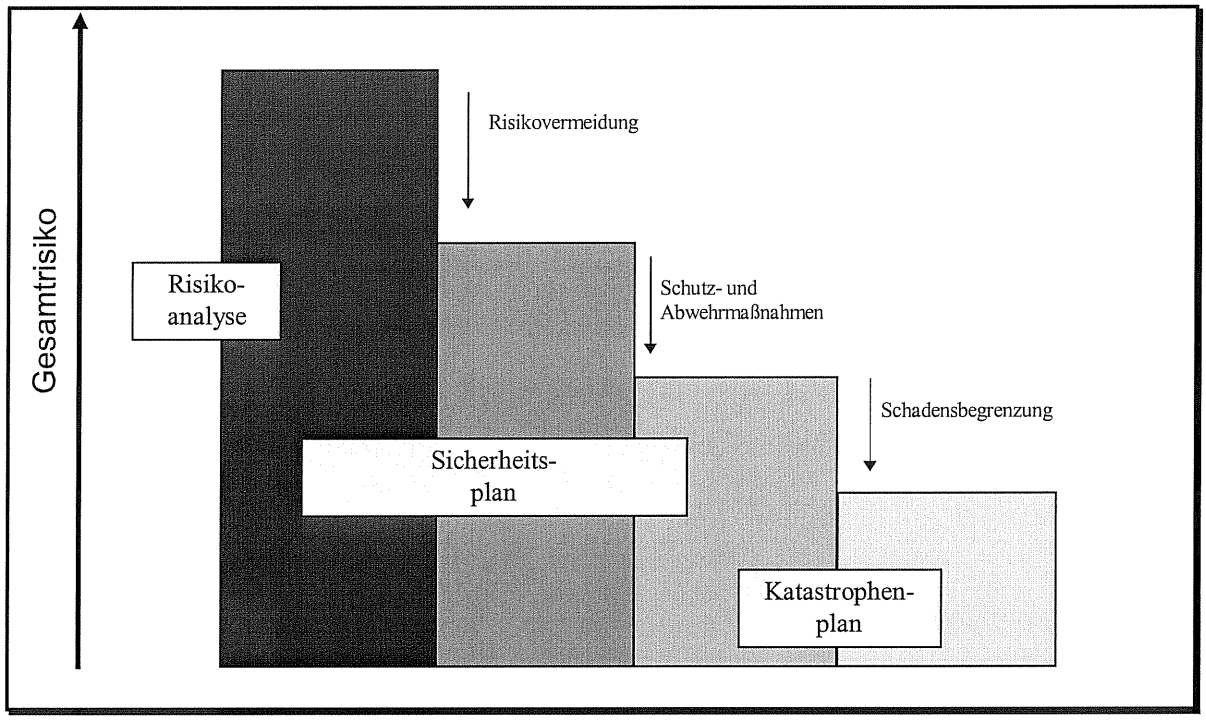


Abbildung 2: Stufenweise Reduktion des Gesamtrisikos[4]

Aufbauend auf die Risikoanalyse wird in einem nächsten Schritt ein Sicherheitsplan erstellt, der sich in verschiedene Sicherheitsstufen untergliedern läßt. Den Abschluß bildet ein Katastrophenplan zur Schadensbegrenzung.

---

[3] vgl. Chapman, B. / Zwicky, E. (Firewall), S. xi

2.1 Risikoanalyse

Aufgrund des komplexen Zusammenspiels der einzelnen IT-Komponenten einer Internet-Anbindung (Router, Gateways, Server, Protokolle, usw.) besteht ein Hauptproblem darin, die einzelnen Schwachstellen zu lokalisieren, um sie dann in einem weiteren Schritt beseitigen zu können. Deshalb unterzieht man als Erstes das gesamte LAN einschließlich der Übergänge nach Außen einer Risikoanalyse, um Sicherheitsprobleme erkennen und bewerten zu können. Das Vorgehen kann durch ein vierstufiges Sicherheitskonzept unterstützt werden.

1. **Systemabgrenzung:**

   Die Systemabgrenzung hat die Aufgabe, diejenigen Bereiche festzulegen, denen eine Gefahr durch die Internet-Anbindung droht. Im Einzelnen lassen sich diese Bereiche in Hardware, Software, Daten und Personen unterteilen.

2. **Bedrohungsanalyse:**

   Die Bedrohungsanalyse beschäftigt sich zum einen mit der Frage, welche Werte geschützt werden sollen und zum anderen, vor wem diese Werte zu schützen sind. Die nachfolgende Abbildung zeigt die Werte, die jeweils sichergestellt werden müssen[5]:

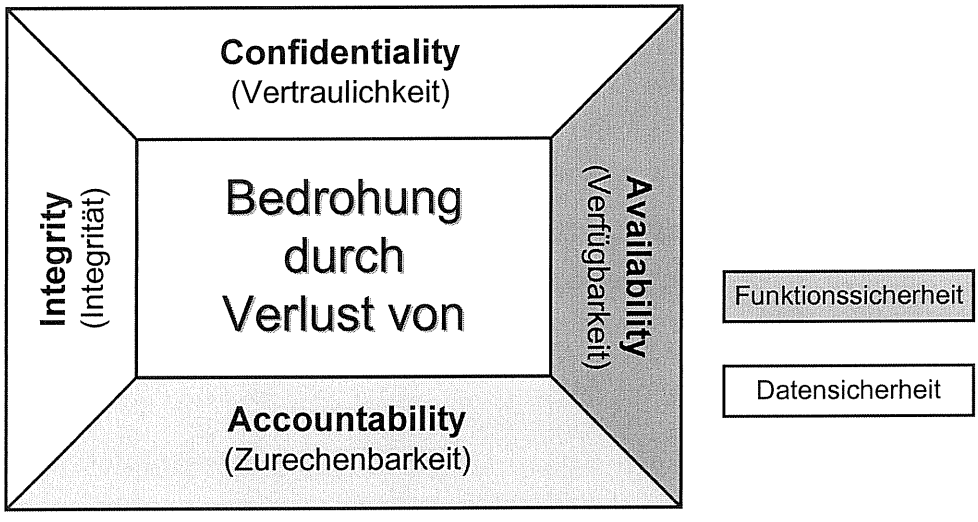


Abbildung 3: Komponenten der Sicherheit

- Ein Verlust der Vertraulichkeit (*Confidentiality*) entsteht dadurch, daß Fremde unerlaubte Einsicht in vertrauliche Daten erhalten. Der illegale Informationsgewinn

[4] vgl. Schaumüller-Bichel, I. (Sicherheitsmanagement), S.35
[5] vgl. Rannenberg, K. / Pfitzmann, A. (Sicherheit), S. 9 f.

kann beispielsweise durch das Abhören von Übertragungswegen oder durch den Zugriff auf gesperrte Dateisysteme erfolgen.

- Anstelle des Verlustes der Integrität (*Integrity*) kann man auch von einer unbefugten Modifikation, bzw. Manipulation, von vertraulichen Daten sprechen. Dies kann zum einen durch Zugriffe von Personen erfolgen wie auch durch eine Fehlfunktion des Systems.
- Der Verlust der Verfügbarkeit (*Availability*) bezieht sich auf den Ausfall einzelner IT-Systeme bzw. der damit verbundenen Daten. Eine ständige Bereitschaft aller IT-Systeme eines Unternehmens ist immer mehr von zentraler Bedeutung, da die eigentliche Leistungserbringung häufig nur noch mit Unterstützung der IT möglich ist.
- Innerhalb eines Netzwerkes muß jedes Handeln eindeutig einer Person oder Personengruppe zugeordnet werden können. Kann diese eindeutige Identität nicht gewährleistet werden, so spricht man vom Verlust der Zurechenbarkeit (*Accountability*).

Weiterhin lassen sich die Personengruppen, von denen möglicherweise eine Gefahr ausgeht, grob in interne (Mitarbeiter des eigenen Unternehmens) und externe Angreifer (außerhalb des eigenen Unternehmens) unterteilen.

3. **Schwachstellenanalyse:**

Die Schwachstellenanalyse hat zur Aufgabe, alle bekannten und für das eigene System relevanten Sicherheitslücken aufzudecken, um dann in einem nächsten Schritt effektive Schutz- und Abwehrmaßnahmen einleiten zu können.

Das gesamte Internet ist aufgrund der Komplexität innerhalb des Netzes und der Vielzahl von Hard- und Softwarekomponenten mit einer Vielzahl von Programm- und Funktionsfehlern durchsetzt, die bis heute bei weitem noch nicht alle bekannt sind. Deshalb sind Unternehmen gezwungen, sich ständig über neu bekanntgewordene Schwachstellen zu informieren. Eine wichtige Informationsquelle stellt hierbei das CERT (Computer Emergency Response Team) dar (http://www.cert.dfn.de/). Diese Institution sammelt alle bekannten Sicherheitsprobleme und liefert Lösungen, diese zu beseitigen.

Die schwerwiegendsten Sicherheitsrisiken treten in folgenden Zusammenhängen auf[6]:

- Sicherheitsrisiken bei Kommunikationsprotokollen
- Sicherheitsrisiken in Verbindung mit der Authentifikation

[6] vgl. Kyas, O. (Sicherheit), S. 45 ff.

- Risiken durch Internet-Applikationen
- Risiken durch einen unverschlüsselten Datenaustausch
- Gefahren durch Viren

Eine Analyse der Schwachstellen innerhalb eines Systems, kann stets nur eine Momentaufnahme darstellen, weil zum einen ständig neue Sicherheitslücken bekannt werden, zum anderen die Systemlandschaft eines Unternehmens ständigen Veränderungen unterworfen ist.

4. **Risikobewertung:**

   Den Abschluß der Risikoanalyse bildet die Risikobewertung. Ihr Ziel ist es, die einzelnen Risiken zu quantifizieren, indem ihnen jeweils Schadenspotential und Eintrittswahrscheinlichkeit zugeordnet werden. Die Risikobewertung liefert dabei ein Ergebnis der Gestalt, ob Risiken tragbar oder untragbar sind, bzw. ob das Eintreten dieser Risiken wahrscheinlich oder unwahrscheinlich ist. Anhand dieser Entscheidungen kann die weitere Realisierung des Sicherheitsplans ausgerichtet werden. Sicherheitsmaßnahmen für Risiken, die untragbar sind und mit einer hohen Wahrscheinlichkeit auftreten, müssen besonders schnell eingeleitet werden.

2.2 Sicherheitsplan

Nach der in der ersten Phase durchgeführten Analyse von Risiken werden in einer zweiten Phase unterschiedliche Methoden zur Beseitigung der identifizierten Schwachstellen eingesetzt. Die ergriffenen Maßnahmen müssen individuell auf das einzelne Unternehmen und die darin bestehende IT-Umgebung zugeschnitten werden. Eine Pauschallösung ist nicht möglich.

1. **Risikovermeidung:**

   Auf dem Weg zur Reduzierung des Gesamtrisikos können Risiken überall dort recht einfach vermieden werden, wo dies nahezu ohne Beeinträchtigung der Geschäftsprozesse möglich ist. In diesem Zusammenhang kann man folgende Möglichkeiten in Betracht ziehen:

   - Wegfall oder Modifikation von besonders gefährlichen Protokollen, Applikationen oder Funktionen
   - Sperrung von riskanten Diensten, sofern dies die Unternehmensrichtlinien zulassen

- Schulung der Mitarbeiter
- Überprüfung der Zugriffsrechte
- Modifikation der IT-Ressourcen

Die Übergänge zwischen Risikovermeidung auf der einen Seite und Schutz- und Abwehrmaßnahmen auf der anderen Seite sind oftmals fließend, so daß eine eindeutige Zuordnung zuweilen nur schwer möglich ist.

2. **Schutz- und Abwehrmaßnahmen:**

Aufbauend auf gefundenen Sicherheitslücken und geänderten Unternehmensrichtlinien (Sicherheitsrichtlinien) kann in dieser Phase daran gegangen werden, die eigentliche Sicherheitsinfrastruktur zu implementieren. Dies setzt im Unternehmen zunächst einen detaillierten und funktionellen Entwurf voraus, bevor die einzelnen Komponenten getestet und implementiert werden können.

Aus der Gesamtheit aller technischen Möglichkeiten sollen im Folgenden nur die Maßnahmen aufgezeigt werden, die systemunabhängig zu implementieren sind.

a) **Kryptographische Maßnahmen**

Mit Hilfe kryptographischer Maßnahmen kann neben der Vertraulichkeit auch die **Authentizität** einer Nachricht sowie die **Integrität** einer Datei sichergestellt werden. Durch digitale Signaturen ist letztlich auch eine **Zurechenbarkeit** in bezug auf einen Verfasser möglich[7]. Es zeigt sich somit, daß die in Abbildung 3 geforderten vier Bereiche der Sicherheit durch kryptographische Maßnahmen erreicht werden können.

Die modernen Verfahren der Kryptographie beruhen auf komplizierten mathematischen Algorithmen, bei denen Bitfolgen mit unterschiedlichen logischen Operatoren miteinander verknüpft werden.

Verschlüsselungsverfahren

In der Kryptographie werden zwei Verschlüsselungsverfahren unterschieden, die **symmetrische** und die **asymmetrische** Verschlüsselung.[8] Die Qualität der jeweiligen Verschlüsselung ist abhängig vom zugrundeliegenden Algorithmus und der Bit-Länge des verwendeten Schlüssels.

---

[7] vgl. Kelm, S. (PEM und PGP), S. D-5

[8] vgl. Beutelsbacher, A. et al. (Kryptographie), S.6

- Symmetrische Verschlüsselungsverfahren

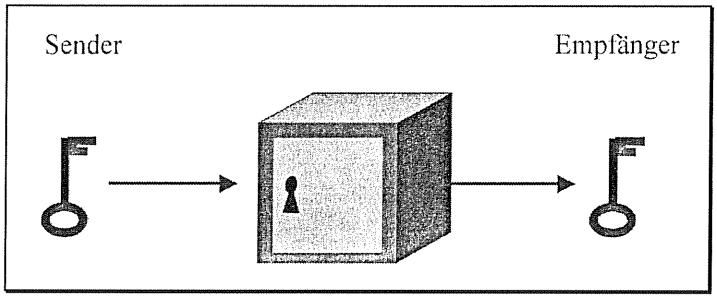


Abbildung 4: Symmetrische Verschlüsselung[9]

Charakteristisch für symmetrische Verschlüsselungssysteme ist die Verwendung des **gleichen** Schlüssels, sowohl zur Verschlüsselung als auch zur Entschlüsselung. Man spricht in diesem Zusammenhang von einem **single key** oder auch **secret key**.

Der im kommerziellen Bereich am häufigsten eingesetzte symmetrische Verschlüsselungsalgorithmus ist der Data Encryption Standard (DES).[10] DES verwendet zur Verschlüsselung einen Schlüssel mit einer Länge von 56 Bit.

Die symmetrische Verschlüsselung ist allerdings mit einigen Nachteilen behaftet. So muß beispielsweise der verwendete Schlüssel zwischen den Kommunikationspartnern ausgetauscht werden. Dies darf allerdings nicht über ein unsicheres Netz erfolgen. Des weiteren kann die Anzahl der verschiedenen Schlüssel bei großen Unternehmungen sehr schnell zu einem ernsthaften Problem werden. Ein System mit n Benutzern erfordert $\frac{n*(n-1)}{2}$ verschiedene Schlüssel.

- Asymmetrische Verschlüsselung

Im Gegensatz zu den symmetrischen Verschlüsselungssystemen werden bei asymmetrischen Verschlüsselungssystemen zwei unterschiedliche, aber mathematisch voneinander abhängige Schlüssel verwendet. Es handelt sich hierbei um einen **public key,** der veröffentlicht werden kann, und um einen **secret key,** der geheim gehalten werden muß.

[9] vgl. Beutelsbacher, A. et al. (Kryptographie), S.6
[10] vgl. Pöppe, C. (DES), S. 98-100

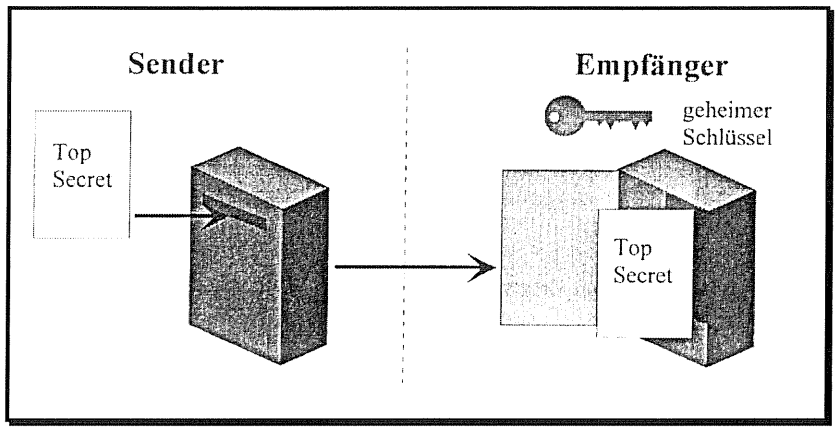


Abbildung 5: Asymmetrische Verschlüsselung[11]

Der Absender verschlüsselt seine Nachricht mit dem public key des Empfängers. Eine so verschlüsselte Nachricht kann nur durch den secret key des Empfängers wieder entschlüsselt werden.

Diese Verschlüsselungsalgorithmen finden vor allem Anwendung bei der Übertragung von electronic-mail (Pretty Good Privacy – PGP) und bei gesicherten Client-Server-Verbindungen (S-HTTP, SSL) im WWW.

- Digitale Signatur

  Neben der Verschlüsselung digitaler Informationen spielt auch die Authentizität und Integrität, d. h. die genaue Zuordnung zu einer Person und die Vollständigkeit einer Nachricht, eine wesentliche Rolle. Deshalb ist man darum bemüht, die wesentlichen Eigenschaften einer handschriftlichen Unterschrift in eine elektronische Form zu überführen. Das Ergebnis ist eine **elektronische Unterschrift** oder **digitale Signatur.** Die rechtlichen Rahmenbedingungen für den Einsatz digitaler Signaturen auch in der Kommunikation zwischen unterschiedlichen Organisationen wurden kürzlich im Rahmen des IuK-Dienste-Gesetzes geschaffen.[12] Die nachfolgende Abbildung verdeutlicht das Prinzip der digitalen Signatur:

[11] vgl. Beutelsbacher, A. et al. (Kryptographie), S.10

[12] vgl. Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste ❁ http://www.iid.de/rahmen/iukdgbt.html

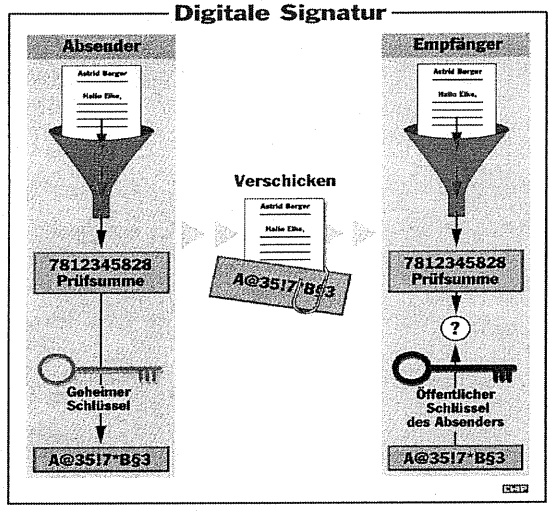


Abbildung 6: Digitale Signatur[13]

Das elektronische Dokument wird durch eine sogenannte Einweg-Hashfunktion auf eine vergleichsweise kurze Bitfolge komprimiert. Dadurch entsteht ein unmanipulierbarer Fingerabdruck (**Prüfsumme**) des Dokuments. Diese kurze Bitfolge wird mittels des geheimen Schlüssels des Absenders verschlüsselt und dem zu signierenden Dokument beigefügt. Der Empfänger ist nun in der Lage, selbst eine Hashfunktion auf das Dokument anzuwenden und diese mit dem übermittelten Hashwert zu vergleichen. Bei Übereinstimmung kann er von der Korrektheit des Dokumentes ausgehen. Durch die Anwendung einer asymmetrischen Verschlüsselung kann auch die Authentizität garantiert werden.

b) **Firewalls**

"Eine Firewall ist eine Schwelle zwischen zwei Netzen, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen."[14] Jede Kommunikation zwischen Rechnern auf unterschiedlichen Seiten der Firewall muß über die Firewall geführtwerden. Die wird durch technische und administrative Maßnahmen sichergestellt. Hierzu gehören insbesondere eine Zugriffskontrolle und ein Audit. Dabei setzt sich stets das Prinzip der geringsten Berechtigung durch. Potentielle Angriffe können somit schnell erkannt werden.

[13] vgl. Vollmuth, J. (digitale Signaturen), S.58
[14] vgl. Ellermann, U. (Firewall), S. 10

Alle Firewall-Systeme sind nach einem einheitlichen Basismuster aufgebaut:

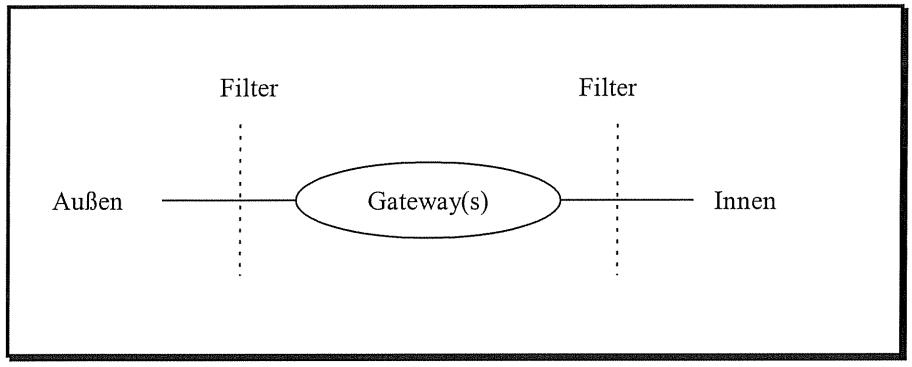


Abbildung 7: Grundprinzip einer Firewall[15]

Durch den Einsatz von Firewall-Systemen ist man in der Lage, alle Risikobereiche auf ein einzelnes System zu konzentrieren. Dadurch vereinfacht sich die Administration des Gesamtsystems und alle Verbindungen nach Außen können kontrolliert (monotoring) und protokolliert (audit) werden.

Eine Firewall wird nach einem von zwei Grundprinzipien konfiguriert:

1. *Alles, was nicht explizit erlaubt ist, ist verboten.*
2. *Alles, was nicht explizit verboten ist, ist erlaubt.*

Firewall Architekturen

Es bestehen verschiedene Möglichkeiten, eine Firewall aufzubauen. Es ist jeweils davon abhängig, welche Sicherheit im Unternehmen gefordert wird.

- Screening-Router

Firewall-Lösungen in Form von Routern mit aktivierter Paketfilterfunktion stellen die einfachste und kostengünstigste Möglichkeit einer Realisation dar, bieten aber auch die geringste Sicherheit. Von Vorteil ist bei dieser Art Firewall, daß der ohnehin vorhandene Router bei einer entsprechenden Konfiguration wiederverwendet werden kann. Die Filterung setzt direkt auf dem Network-Layer des ISO/OSI-Referenzmodells[16] auf.

[15] vgl. Cheswick, W. / Bellovin, S. (Firewall), S.62
[16] vgl. Scheer, A.-W. (Wirtschaftsinformatik), S. 373ff.

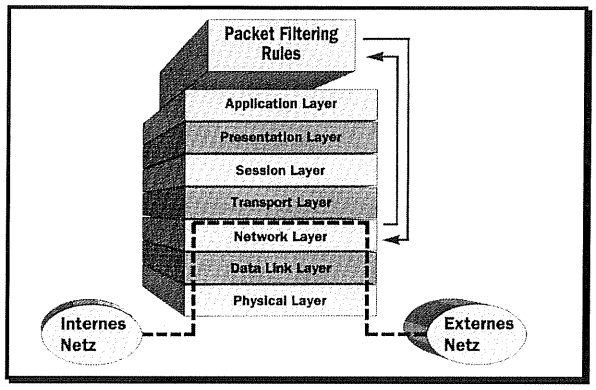


Abbildung 8: Firewall auf Basis von Routern und Paketfiltern[17]

Bei einem Screening Router werden Kommunikationsanfragen mit unerwünschten Quell- oder Zieladressen herausgefiltert.

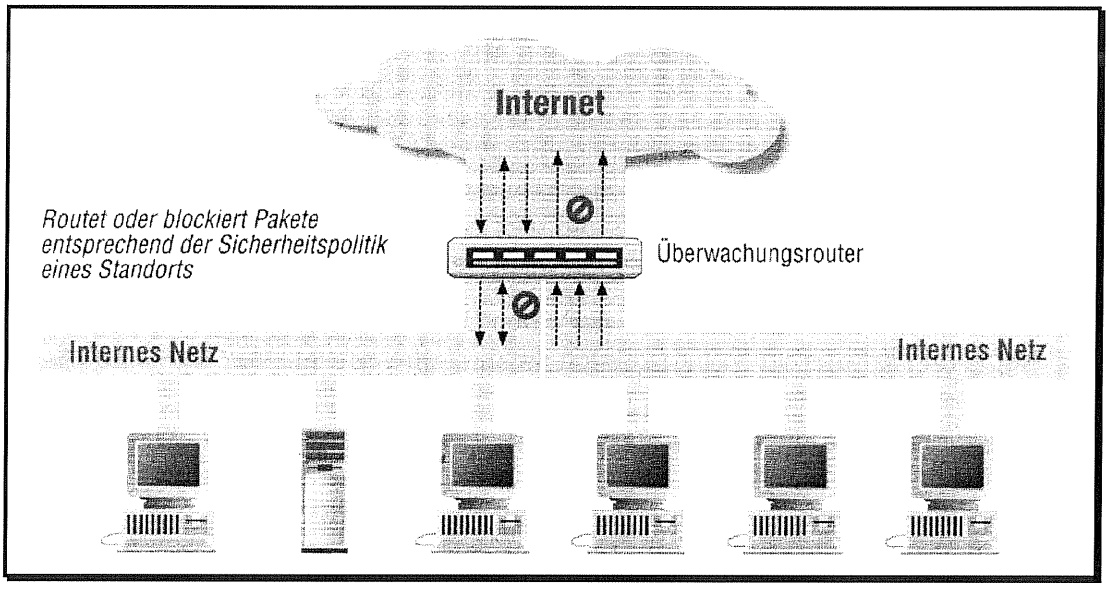


Abbildung 9: Screening-Router[18]

- Application Gateway / Dual Homed Host

"Ein Host, der Verbindung zu zwei Netzen hat, wird als Gateway bezeichnet, wenn die Verbindungen, die über diesen Rechner[19] laufen, auf Applikationsebene realisiert werden"[20].

---

17 vgl. Norman Data Defence Systems GmbH, (Informationsschrift)
18 vgl. Chapman, B. / Zwicky, E. (Firewall), S. 67
19 Der Rechner verfügt über zwei physisch voneinander getrennte Netzwerkkarten.
20 vgl. Ellermann, U. (Firewall), S. 44

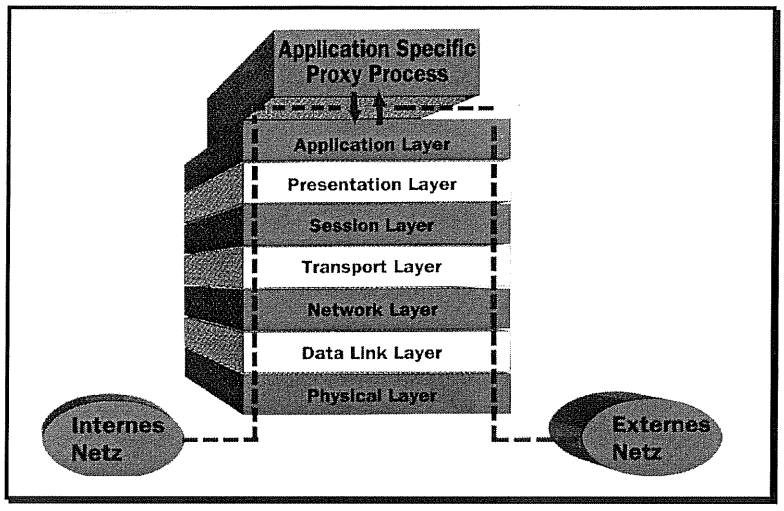


Abbildung 10: Application-Gateway[21]

Die Grundidee dieser Firewall besteht darin, das Routing von einem Netzwerk in das andere vollständig zu unterbinden. Die Netzwerke sind dadurch nicht mehr auf der Netzwerkschicht, sondern nur noch auf der Applikationsschicht miteinander verbunden.[22] Somit stellt das Gateway den einzigen vom Internet und vom LAN aus erreichbaren Host dar. Dienste, die nach dem **Store-and-Forward-Prinzip** arbeiten, wie z. B. Email oder NetNews, laufen dabei wie gewohnt ab. Bei den meisten anderen fungiert das Application-Gateway als Proxy-Server, d. h. alle Datenpakete werden dienstspezifisch einer zugehörigen Applikation auf der Firewall zugeteilt, die dann die Datenpakete protokolliert, analysiert und je nach dem Ergebnis blockiert oder weiterreicht. Es findet demnach keine direkte Kommunikation zwischen dem Internet-Client und dem realen Server statt, sondern der Proxy-Server wird als Vermittler zwischengeschaltet.
Abbildung 11 zeigt den prinzipiellen Aufbau eines Dual Home Gateways.

[21] vgl. Norman Data Defense Systems GmbH (Informationsschrift)
[22] vgl. Mütze, M. (Firewall), S. 626

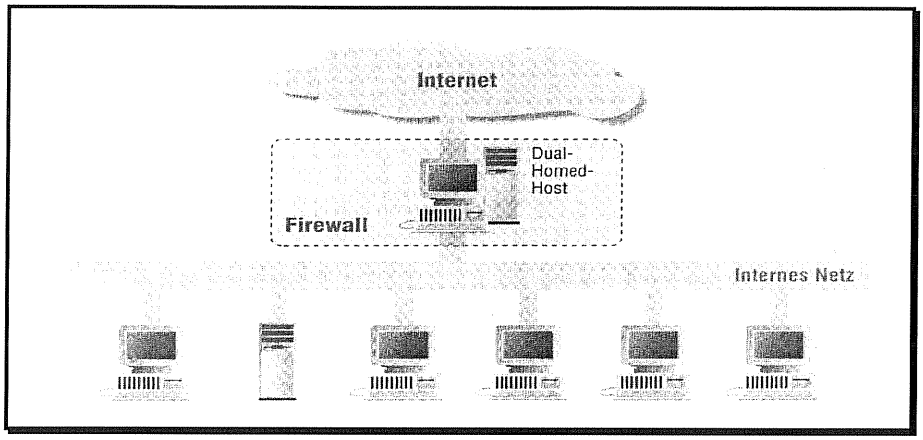


Abbildung 11: Dual Home Host[23]

Nachteilig können sich bei dieser Firewall-Architektur Performanzverluste auswirken, die dadurch entstehen, daß die Datenpakete nicht mehr auf der Netzwerkschicht geroutet werden können, sondern bis zur Applikationsschicht hochgereicht werden müssen. Insgesamt können Application-Gateway-Firewalls als sehr sicher eingestuft werden.

Wie bei allen anderen Sicherheitsmaßen, so kann es auch bei einem Firewall-Konzept keine absolute Sicherheit geben. Es verbleibt immer ein Restrisiko, bedingt durch Fehler in der Architektur, Administration oder durch momentan noch unentdeckte Sicherheitslücken. Davon sind besonders die Router oder Proxy-Server betroffen, denn eine potentielle Schwachstelle kann durch die Konzentration auf eine Stelle bzw. einen Rechner zum sofortigen und vollständigen Verlust der Sicherheit führen.

2.3 Katastrophenplan

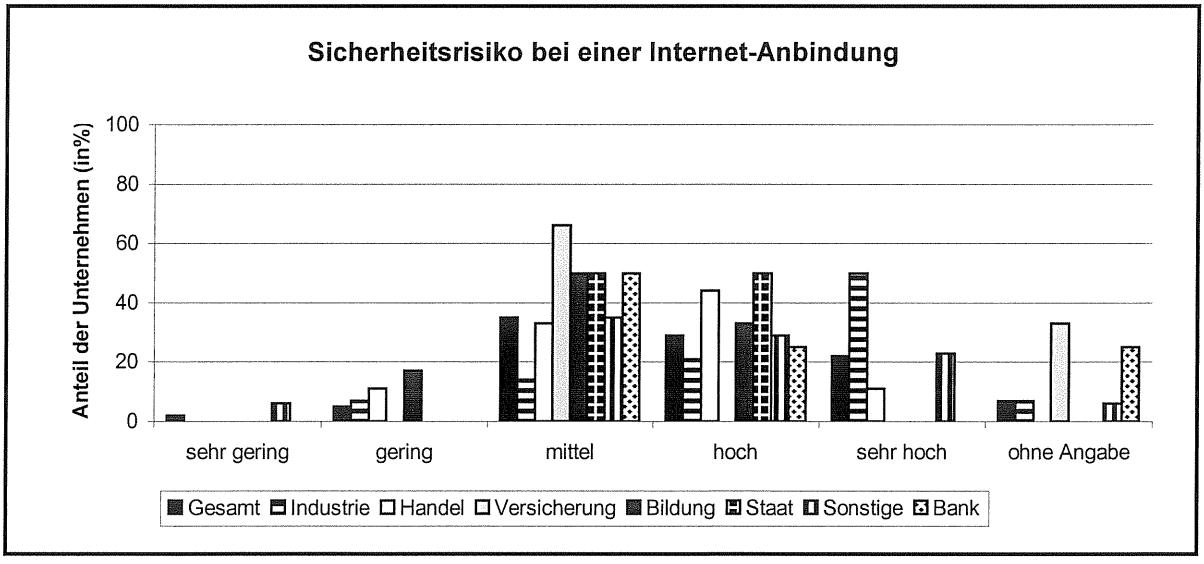
Sollte es dennoch, trotz aller eingesetzten Sicherheitsmaßnahmen, zu einem Einbruch in das eigene Netzwerk kommen, so müssen bereits im Vorfeld geeignete Maßnahmen getroffen werden, um möglichst schnell reagieren zu können. In diesem Zusammenhang haben sich Angriffsaktionspläne und Vorkehrungsmaßnahmen (Prüfsummen, Backup) als sinnvoll erwiesen. Der Katastrophenplan bildet gleichzeitig den Abschluß eines umfassenden Sicherheitsmanagements.

[23] vgl. Chapman, B. / Zwicky, E. (Firewall), S. 67

3 Sicherheitsmanagement in der Anwendung – Eine Studie

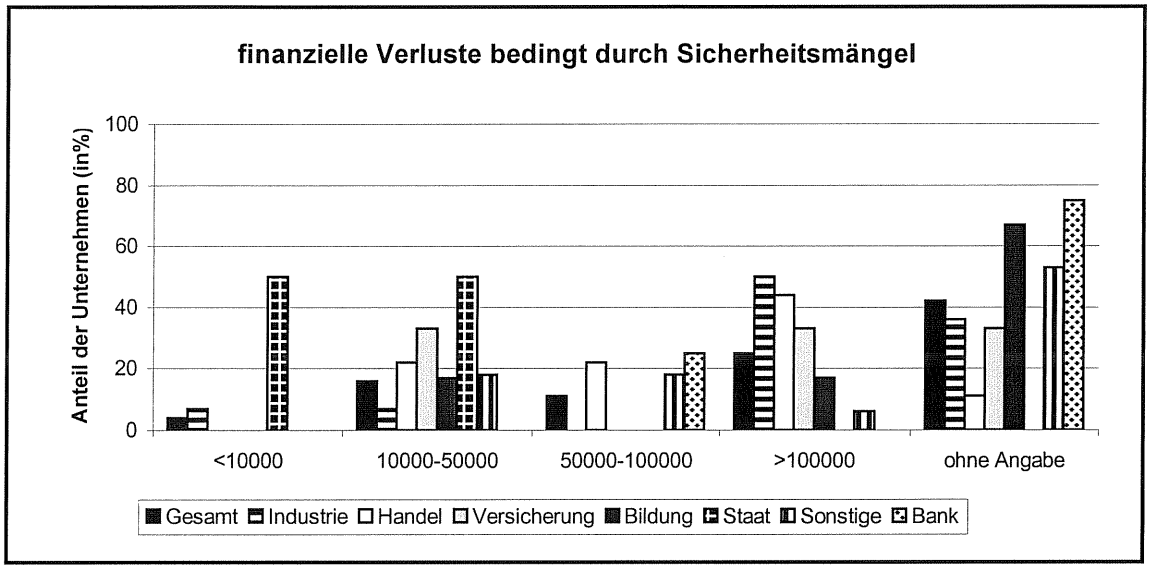
Eine vom Institut für Wirtschaftsinformatik durchgeführte Studie sollte zeigen, welche Bedeutung die verschiedenen Sicherheitsaspekte in der Praxis haben und mit welcher Grundeinstellung die Unternehmen der Sicherheitsproblematik gegenübertreten. Dazu wurden 620 Unternehmen aus den Bereichen Industrie, Handel, Banken, Versicherungen, Bildung und staatliche Stellen in die Untersuchung mit einbezogen. Die Rücklaufquote lag bei ca. 9%, was in Bezug auf die komplexe und zum Teil sehr detaillierte Fragestellung ein zufriedenstellendes Ergebnis ist. Die Befragung, die sich aus 40 Fragen zusammensetzte, wurde geschlossen über das WWW abgewickelt. Im Rahmen dieses Heftes sollen nur die wichtigsten Fragen und Ergebnisse betrachtet werden.

Die Hauptgründe für die Präsenz der Unternehmen im Internet werden von allen beteiligten Unternehmen einheitlich mit Verbesserung der Kundennähe und Werbung bzw. Selbstdarstellung beantwortet. Eine bessere Kooperation und Kommunikation, sowie Wettbewerbsvorteile gegenüber Konkurrenten, sind derzeit eher zweitrangig. Jede Branche verfolgt weiterhin noch einzelne individuelle Ziele wie z. B. Lizenzvergabe via Internet (Industrie), Schadensmeldung via Internet (Versicherungen).
Die Sicherheitsrisiken bei der Anbindung an das Internet sind den beteiligten Unternehmen durchaus bewußt. Annähernd 80% aller Befragten schätzen die Risiken als mittel bis sehr hoch ein.

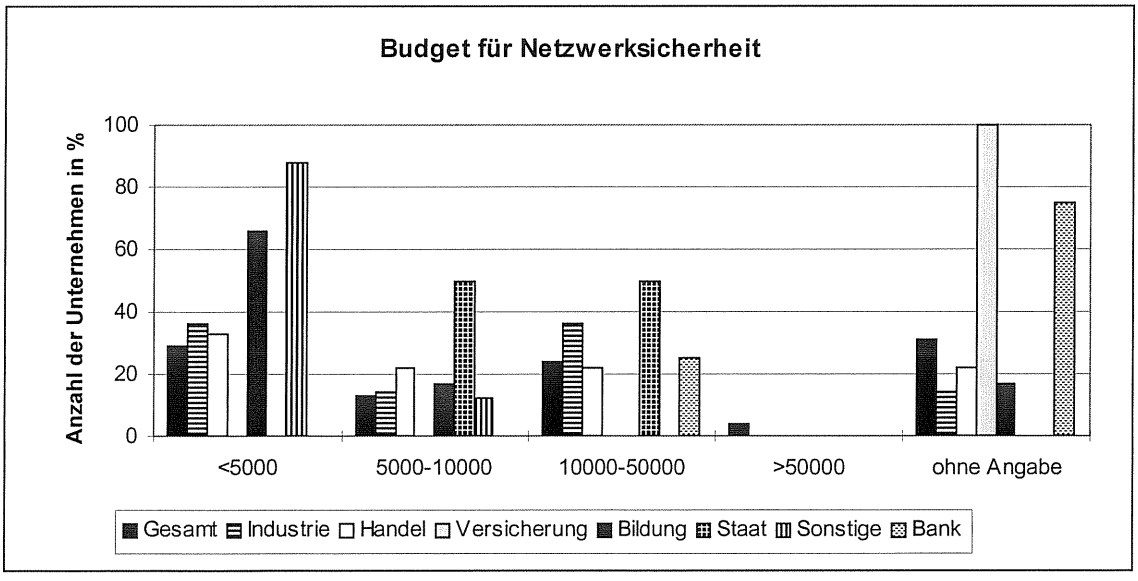


Auch die damit möglicherweise verbundenen finanziellen Verluste werden als sehr hoch eingeschätzt. Das größte Risiko sehen etwa die Hälfte aller Unternehmen durch den Ausfall ihrer Netzverfügbarkeit. Dies ist nicht weiter verwunderlich, bedenkt man, daß die

Systemausfallkosten überproportional mit der Ausfallzeit ansteigen.[24] Verluste durch eingeschleuste Viren, werden als eine weitere ernst zu nehmende Gefahr angesehen. Diese Bedenken sind durch das oftmals bedenkenlose Herunterladen von unbekannten Servern durchaus angebracht. Eine zusätzliche Gefährdung wird in geänderten oder gelöschten Daten gesehen. Die Möglichkeit des Lesens geheimer Informationen wird demgegenüber als zweitrangig beurteilt.

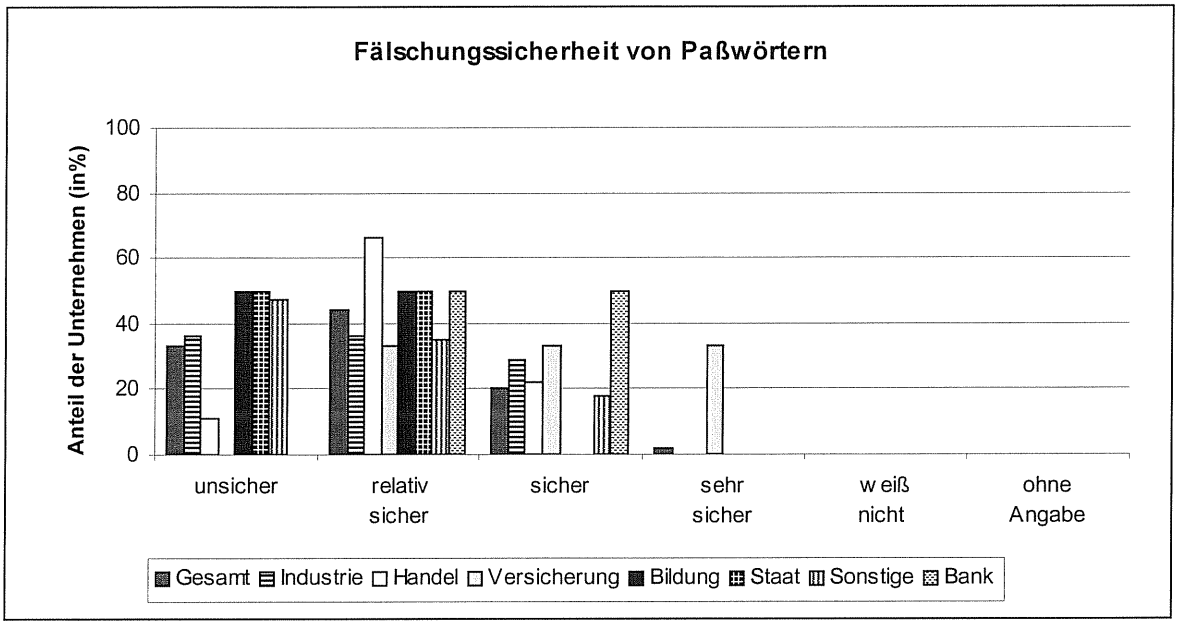


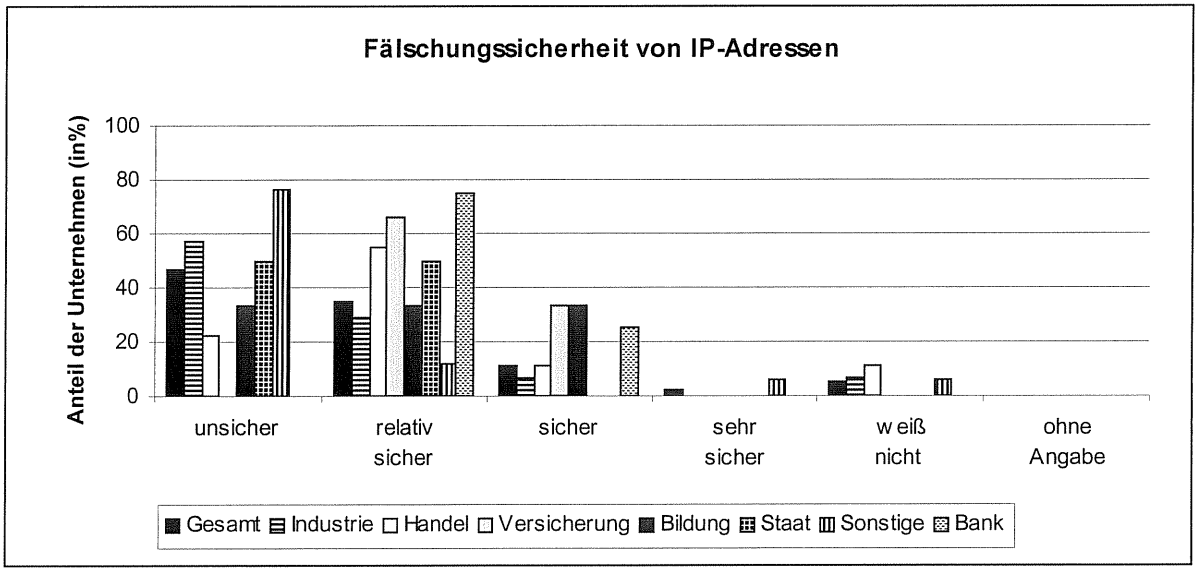
Betrachtet man in Verbindung mit den finanziellen Verlusten allerdings die Frage nach den eigenen Ausgaben für Netzwerksicherheit, so wird deutlich, daß diese wesentlich niedriger liegen. Die Mehrheit der Unternehmen gibt lediglich 5.000-10.000 DM jährlich für Netzwerksicherheit aus, obwohl die möglichen Schäden wesentlich höher eingeschätzt worden sind.



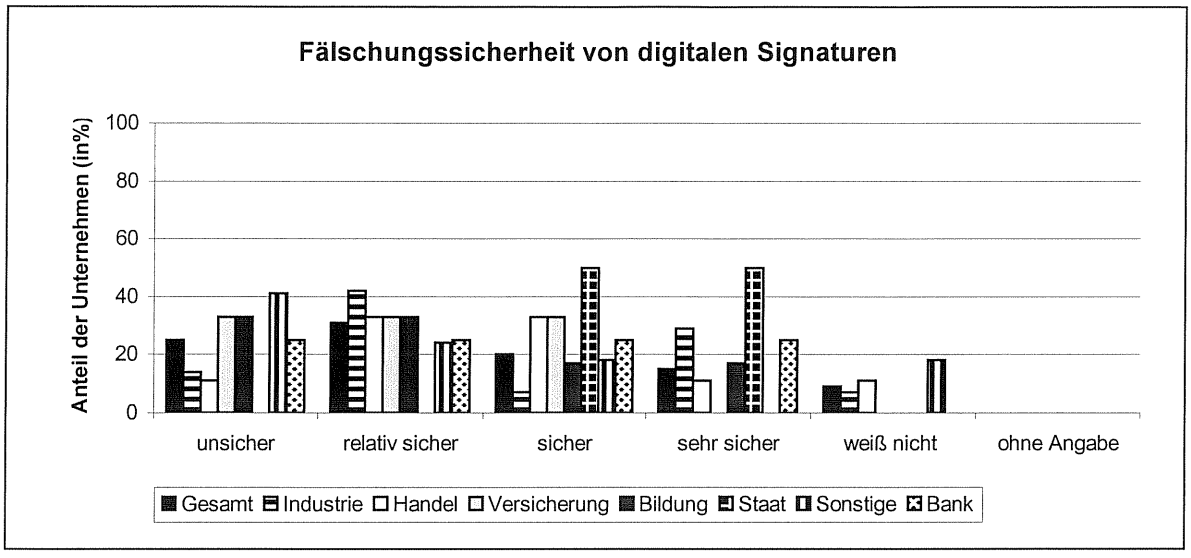
[24] vgl. Kotschenreuther, J. (Sicherheit), S. 158

Die Frage nach der Fälschungssicherheit einiger Internet-Komponenten verdeutlicht die Unkenntnis der befragten Unternehmen in Bezug auf potentielle Sicherheitsrisiken. Es wird deutlich, daß teilweise Komponenten als „sicher" oder zumindest als „relativ sicher" bewertet werden, die von der Wissenschaft nachdrücklich als unsicher ausgewiesen sind. Hierzu zählt z. B. die Fälschungssicherheit von IP-Adressen oder Paßwörtern.

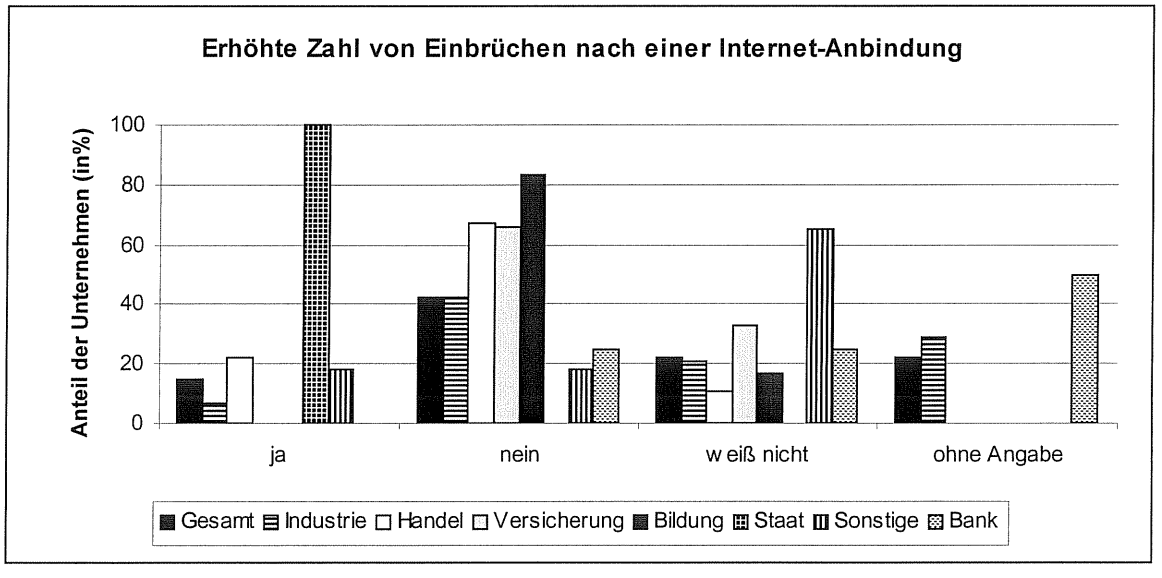




Dagegen werden Komponenten wie z. B. die digitale Signatur, die als sehr sicher einzustufen ist, häufig ebenfalls als „unsicher" beurteilt.

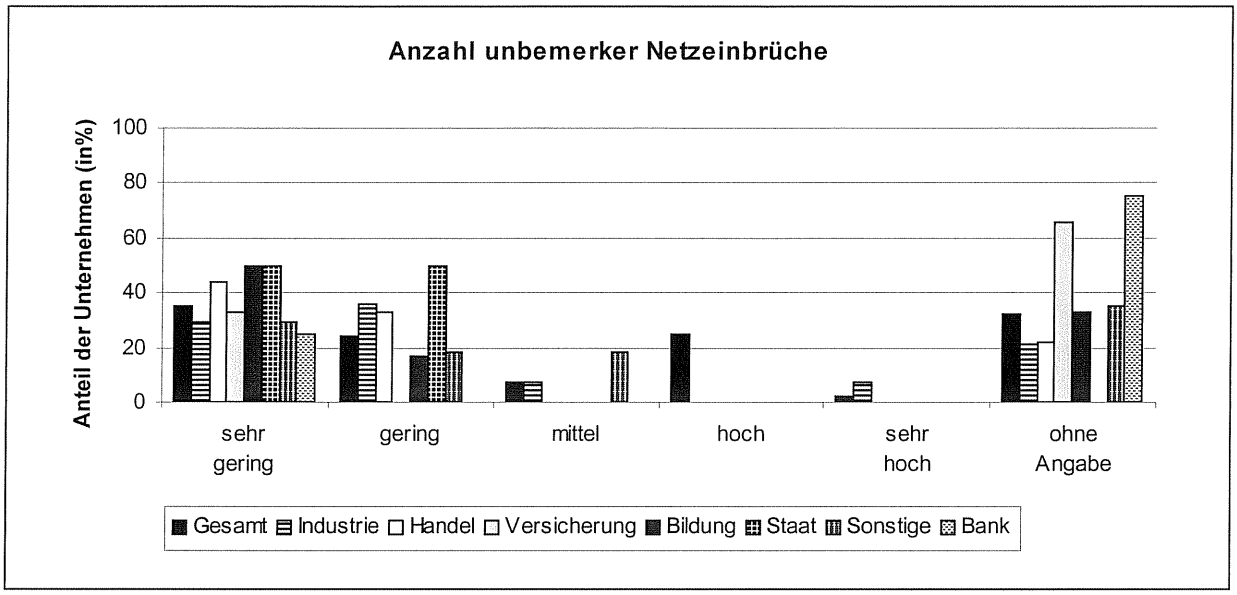


Trotz aller bestehenden Sicherheitsmängel bei der Anbindung an das Internet sind die Einbrüche, wie die Studie zeigt, durchschnittlich nur gering gestiegen. In einzelnen Branchen, z. B. bei den staatlichen Stellen, ist allerdings eine sehr deutliche Steigerung der Einbrüche zu erkennen. Diese stellen wohl aufgrund der exponierten Stellung (fehlende Konkurrenz) oder der hoheitlichen Position ein besonderes Ziel dar, das einen Angriff besonders reizvoll erscheinen läßt.

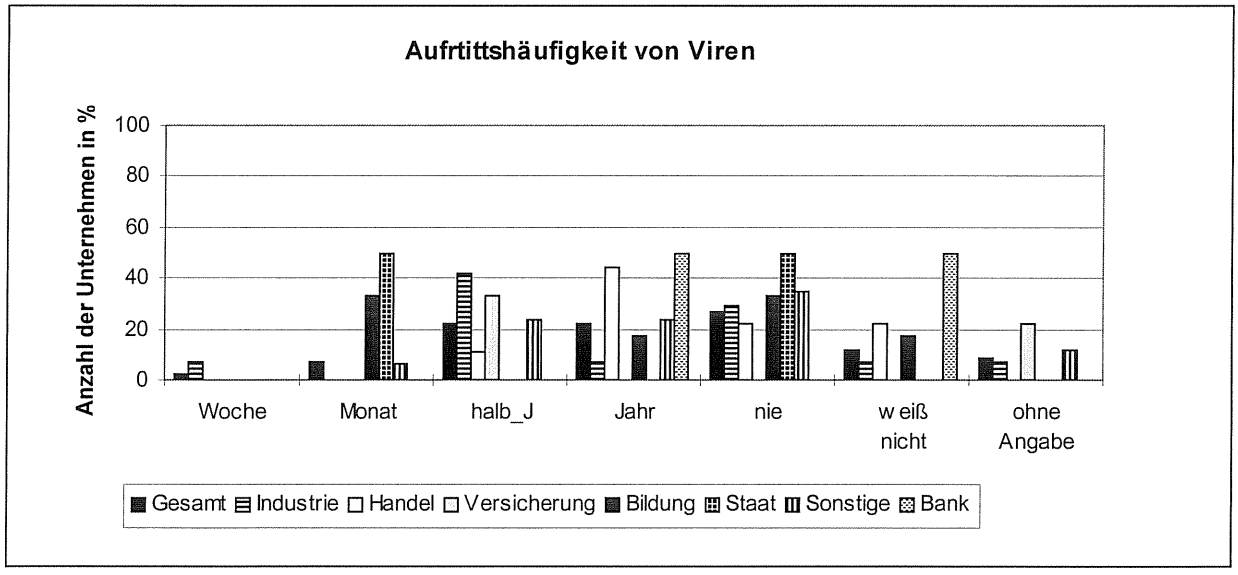


Es bleibt zu beachten, daß viele Unternehmen nicht einschätzen können, ob ihre Systeme kompromittiert wurden oder nicht. In diesem Zusammenhang schließt sich auch eine Frage nach der Zahl unbemerkter Netzeinbrüche an. Nur etwa 10% der befragten Unternehmen schätzen diese Möglichkeit als mittel, hoch oder sehr hoch ein. Zieht man allerdings die Beobachtungen von CERT heran, so wird deutlich, daß nur bei einem Bruchteil der Einbrüche

in fremde Netzwerke Spuren hinterlassen werden. Viele Einbrüche werden erst dann bemerkt, wenn der Einbrecher sein Werk an die Öffentlichkeit trägt.[25]



Um die in Verbindung mit einer vorherigen Frage bereits angesprochene Virenproblematik aufzugreifen, ist auch die Frage nach der Auftrittshäufigkeit von Viren näher betrachtet worden. Es wird dabei deutlich, daß dieser Problematik durchaus Beachtung beizumessen ist, da Viren regelmäßig in Unternehmen auftreten. Besonders die weitverbreiteten Word-Makro-Viren können eine Gefahr darstellen.

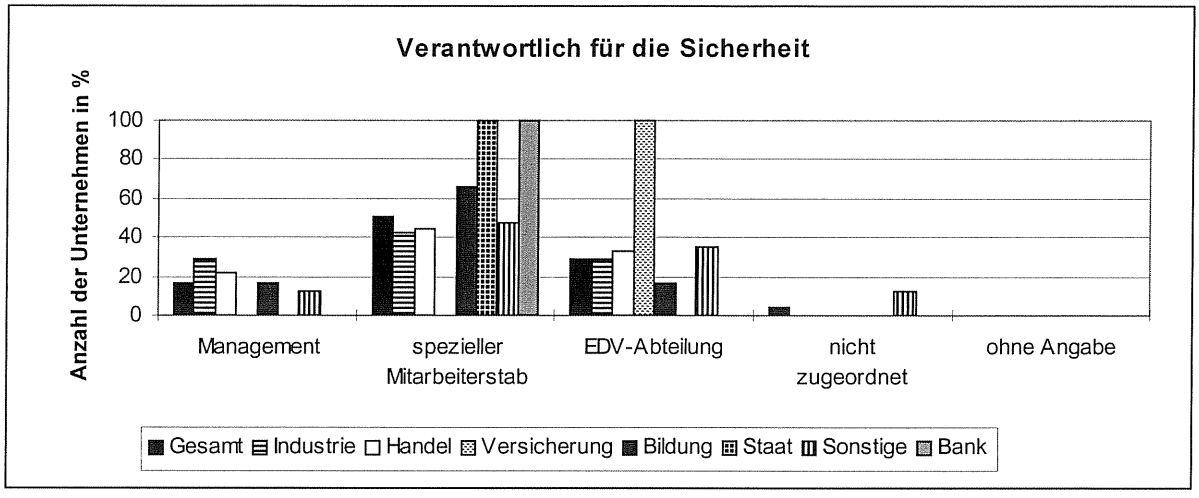


Aus den oben genannten Gründen verfügt die Hälfte aller Unternehmen über Virenaktionspläne, die die genaue Handlungsweise nach einem Virenbefall festlegen.

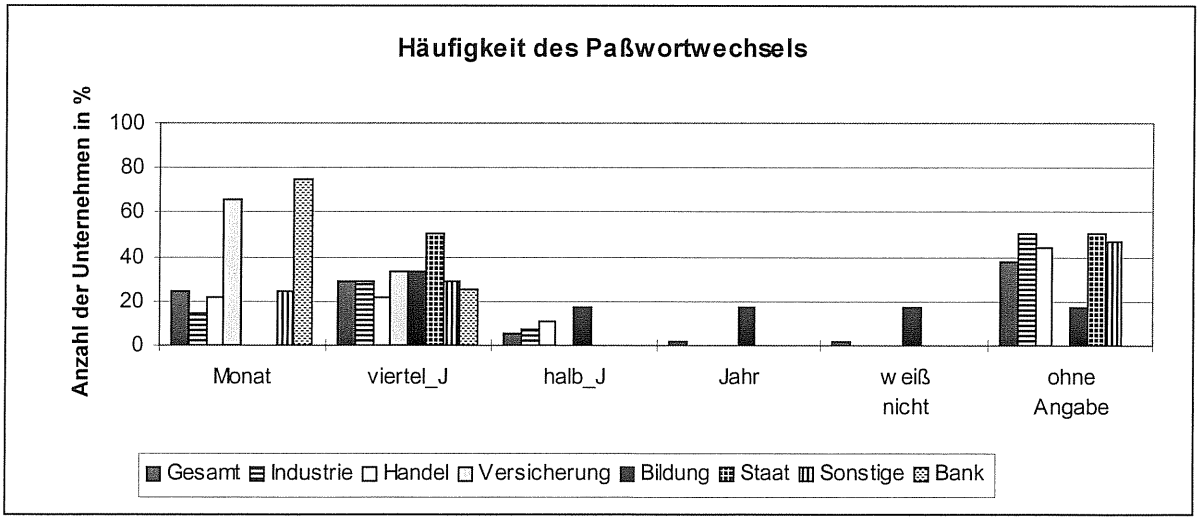
Eine weiterer Punkt der Studie befaßte sich mit der Frage, wer im Unternehmen für die Sicherheit der Netzwerke verantwortlich ist. Es zeigte sich, daß etwa 60% aller Unternehmen

[25] Hierunter fällt z. B. auch das Sicherheitsloch im Homebanking-Bereich von T-Online. Vgl. Luckhardt, N. (T-Online)

einen speziellen Mitarbeiterstab für diese Aufgaben eingerichtet haben. Auch sehen die Unternehmen von einem Outsourcing der Sicherheitsmaßnahmen weitgehend ab. Nur 1% der befragten Unternehmen ziehen eine solche Möglichkeit in Betracht.



Die Studie ergab, daß viele Unternehmen versuchen, durch administrative Maßnahmen die Sicherheit im eigenen Unternehmen zu erhöhen. Das ist ein Schritt, wie er in der eingehend beschriebenen Risikovermeidung gefordert wird. Darunter fällt vor allem die Schulung der Mitarbeiter in Bezug auf Sicherheitsfragen. Die Umfrage ergab, daß ca. 50% aller Unternehmen die eigenen Mitarbeiter über Sicherheitsrisken im Zuge der Internet-Anbindung, vor allem im Umgang mit den einzelnen Internet-Diensten, informiert haben. Des weiteren erhalten bei ca. 70% der Unternehmen die Mitarbeiter konkrete Anweisungen, wie sie die verwendeten Paßwörter zu konstruieren haben bzw. die Konstruktionsregeln werden bereits im System festgelegt. Auch müssen die Paßwörter, wie eine weitere Frage zeigte, regelmäßig geändert werden. Diese Änderung wird vielfach bereits durch die Systemkonfiguration vorgegeben.



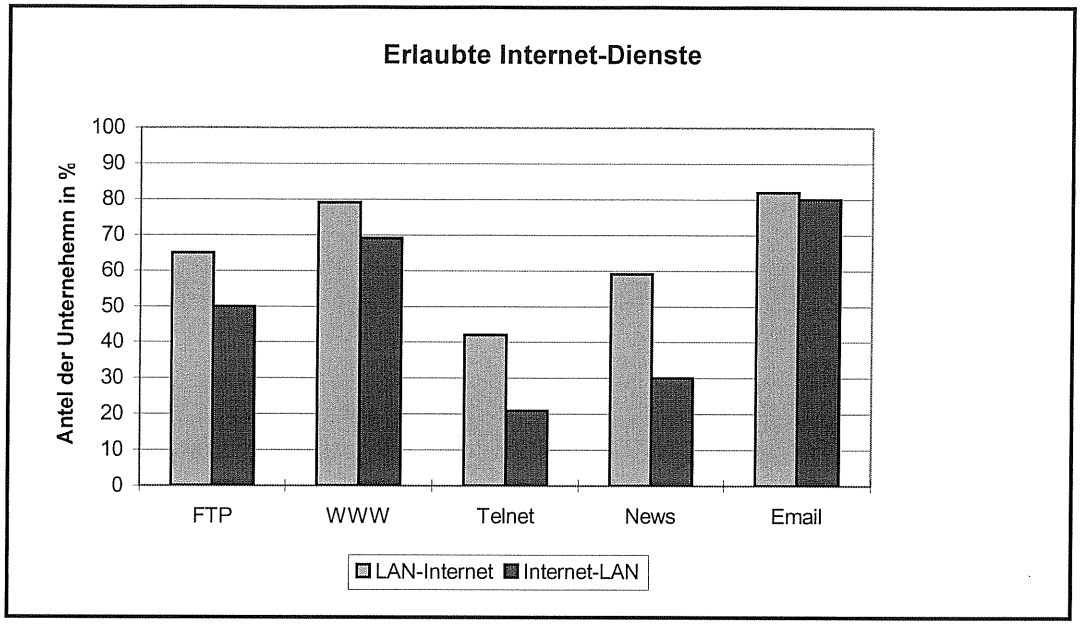
Ein bemerkenswertes Ergebnis lieferte die Frage, ob es den Mitarbeitern erlaubt sei, eigene Programme auf den Netzwerkrechnern zu installieren. Über 70% der Unternehmen machen diesbezüglich keine Einschränkungen. Betrachtet man in diesem Zusammenhang die Sicherheitslücken, die teilweise in alten Versionen der WWW-Browser bestehen, so ist dies durchaus als bedenklich anzusehen.

Viele der befragten Unternehmen sind außerdem bemüht, die festgelegten Sicherheitsmaßnahmen kategorisch durchzusetzen. So gehen etwa 35% der befragten Unternehmen streng gegen Mitarbeiter vor, die nachweislich gegen bestehende Sicherheitsbestimmungen verstoßen haben.

Neben den Fragen zu vorwiegend administrativen Aufgaben im Zusammenhang mit Mitarbeitern lag ein weiterer Schwerpunkt auf dem Einsatz technischer Möglichkeiten im Rahmen des Sicherheitsmanagements.

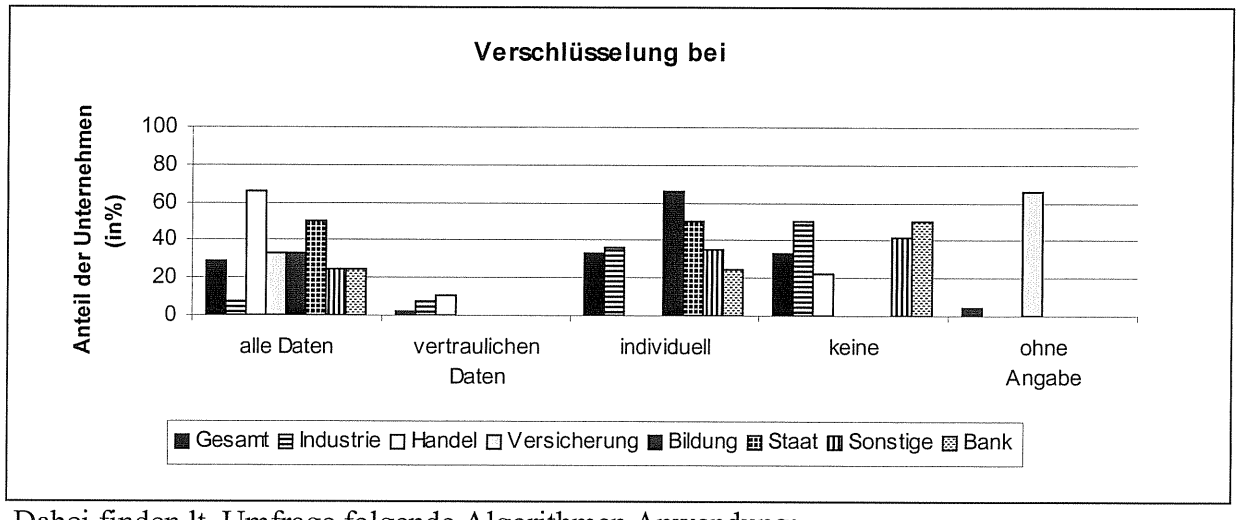
Über eine Firewall verfügen demnach schon ca. 60% aller befragten Unternehmen. Es ist allerdings als äußerst bedenklich zu bewerten, daß im Umkehrschluß etwa ein Drittel ihr LAN ohne eine solche technische Hürde an das Internet angebunden haben. Es besteht also in diesem Bereich durchaus noch ein beträchtlicher Handlungsbedarf. Die Umfrage ergab weiter, daß nur ca. 22% der befragten Unternehmen sogenannte Netzwerk-Angriffsimulatoren, wie z.B. SATAN (Security Tool for Analyzing Networks) einsetzen, obwohl diese Werkzeuge es erlauben, das eigene Netzwerk auf alle bekannten Einbruchsmöglichkeiten zu testen. Auch die Veröffentlichungen von CERT, die neueste Erkenntnisse über Sicherheitsmängel liefern, werden nur von 50% der Unternehmen verfolgt.

Da die verschiedenen Dienste im Internet mit unterschiedlichen Risiken behaftet sind, sollte untersucht werden, welche Dienste in welcher Richtung zugelassen bzw. verboten sind. Es wurde festgestellt, daß der risikoreichste Dienst Telnet nur in wenigen Fällen vom Internet ins LAN möglich ist. Dies ist damit zu begründen, daß via Telnet sehr leicht Rechner im LAN kompromittiert werden können.

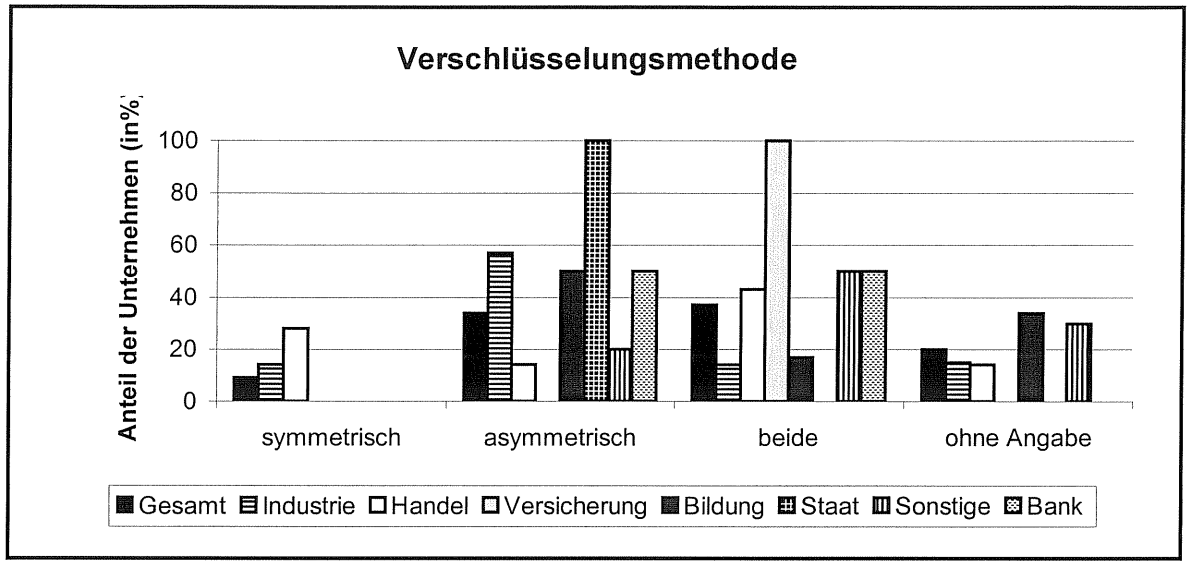


Neben den aufgeführten Diensten wurde häufig noch der Dienst IRC (Internet Relay Chat) als freigegeben genannt.

In Verbindung mit den technisch realisierbaren Sicherheitsmaßnahmen lag ein weiterer Schwerpunkt auf der Verschlüsselung von Informationen, speziell von Email-Nachrichten. Hierbei stellt sich vor allem die Frage, welche Nachrichten verschlüsselt werden.



Dabei finden lt. Umfrage folgende Algorithmen Anwendung:



4 Fazit und Ausblick

"Es ist einfach, ein Computersystem sicher zu betreiben. Sie müssen bloß alle Wählverbindungen abklemmen, ausschließlich direkt angeschlossene Terminals zulassen, diese Terminals und den Computer selbst in einen abgeschirmten Raum bringen sowie eine Wache vor die Tür stellen."[26]

Zusammenfassend wird deutlich, daß die potentiellen Risiken, die mit einer Internet-Anbindung verbunden sind, durch ein geeignetes Sicherheitsmanagements, in Form von personellen, administrativen und technischen Maßnahmen, auf ein kalkulierbares Maß reduziert werden können. Ein 100%iger Schutz wird aber niemals erreicht.
Wie die durchgeführte Studie zeigt, werden diese Risiken auch von den Unternehmen erkannt. Dennoch werden oftmals Internet-Zugänge realisiert, ohne die einfachsten Sicherheitsmaßnahmen durchzuführen.
Zukünftig werden sich Internet-Anwendungen in Qualität und Quantität ständig weiterentwickeln, die Zahl der Internet-Nutzer wird weiter steigen und das Intranet wird das Rückrad eines Unternehmens darstellen. Infolge dessen müssen auch Sicherheitsmaßnahmen an die sich veränderte Konstellation angepaßt werden. Durch den Einsatz neuer "Basis-Technologien", in Form von Applikationen und Protokollen (IPv6), kann bereits die zugrundeliegende Infrastruktur sicherer gestaltet werden.
Künftige Rechtsentwicklungen müssen die veränderten informationstechnologischen Gegeben-heiten mit einbeziehen. Es muß eine Balance zwischen der Informationsfreiheit und

[26] vgl. Cheswick, W. / Bellovin, S. (Firewall), S. xv

dem Schutz des einzelnen Anwenders im Internet gefunden werden. Dabei ist allerdings darauf zu achten, daß Informations- und Kommunikationsfreiheit entscheidend zur gesellschaftlichen und wirtschaftlichen Entwicklung beitragen. Einschränkungen dürfen deshalb nur in den Bereichen Anwendung finden, in denen dies unbedingt notwendig ist.

Literaturverzeichnis:

Beutelsbacher, A. et al. (Kryptographie): Moderne Verfahren der Kryptographie - Von RSA zu Zero-Knowledge, Braunschweig/Wiesbaden 1995

Chapman, B. / Zwicky, E. (Firewall): Einrichten von Internet Firewalls, 1. Auflage, Bonn 1996

Cheswick, W. / Bellovin, S. (Firewall): Firewalls und Sicherheit im Internet, 1. Auflage, Würzburg 1996

Ellermann, U. (Firewall): Firewalls - Isolations- und Audittechniken zum Schutz von lokalen Computer-Netzen, DFN-Bericht Nr. 76, Berlin 1994

Kelm, S. (PEM und PGP): PEM und PGP zum Schutz der elektronischen Kommunikation, in: DFN-Bericht Nr.78, Berlin 1995, Kapitel D

Kotschenreuther, J. (Sicherheit): Sicherheit und Verfügbarkeit, in: DATACOM, Heft 12/96, S. 158-159

Kyas, O. (Sicherheit): Sicherheit im Internet: Risikoanalyse - Strategie – Firewalls, Bergheim 1996

Luckhardt, N. (T-Online): Nicht ganz dicht – Jugendliche Hacker knacken T-Online, in: c't7/98, S. 62-65

Mütze, M. (Firewall): Firewalls, in: Wirtschaftsinformatik, Heft 6/96, S. 625-628

Norman Data Defense Systems GmbH (Informationsschrift): Sicher auf die Datenautobahn

Pöppe, C. (DES): Der Data Encryption Standard, in: Spektrum der Wissenschaft, Dossier: Datenautobahn 1995, S. 96-98

Rannenberg, K. / Pfitzmann, A. (Sicherheit): Sicherheit, insbesondere mehrseitige IT-Sicherheit, in: it+ti Informationstechnik und Technische Informatik, Heft 4/96, S. 7-10

Schaumüller-Bichl, I. (Sicherheitsmanagement): Sicherheitsmanagement: Risikobewältigung in informationstechnologischen Systemen, Mannheim et al. 1992

Scheer, A.-W. (Wirtschaftsinformatik): Wirtschaftsinformatik – Referenzmodelle für industrielle Geschäftsprozesse, 6. Auflage, Berlin et. al. 1995

Vollmuth, J. (digitale Signaturen): Echter geht's nicht mehr – Digitale Unterschrift, in: Chip,Heft 7/96, S.58

Wallich, P. (Cracker): Piraten im Datennetz, in: Spektrum der Wissenschaft, Dossier: Datenautobahn 1995, S. 84-90

Die Veröffentlichungen des Instituts für Wirtschaftsinformatik (IWi) im Institut für empirische Wirtschaftsforschung an der Universität des Saarlandes erscheinen in unregelmäßiger Folge.

Heft 146: M. Luzius, M. Ewig, A.-W. Scheer: Sicherheitsmanagement bei Internet-Anbindungen – Konzepte und Anwendungen, Mai 1998

Heft 145: J. Hagemeyer, R. Rolles, Y. Schmidt, A.-W. Scheer: Arbeitsverteilungsverfahren in Workflow-Management-Systemen: Anforderungen, Stand und Perspektiven, Juni 1998

Heft 144: P. Loos, Th. Allweyer: Process Orientation and Object-Orientation - An Approach for Integrating UML and Event-Driven Process Chains (EPC), März 1998

Heft 143: in Bearbeitung

Heft 142: Th. Allweyer, S. Leinenbach, A.-W. Scheer: Business Process Re-engineering in the Construction Industry, Oktober 1997

Heft 141: M. Nüttgens, V. Zimmermann, A.-W. Scheer: Objektorientierte Ereignisgesteuerte Prozeßkette (oEPK) - Methode und Anwendung -, Mai 1997

Heft 140: J. Sander, A.-W. Scheer: Offene Lernumgebungen in der Aus- und Weiterbildung am Beispiel des PPS-Trainers, März 1997

Heft 139: M. Bold, M. Hoffmann, A.-W. Scheer: Datenmodellierung für das Data Warehouse, März 1997

Heft 138: S. Stehle, A.-W. Scheer: Gestaltungsoptionen multimedialer Off- und Online- Lernsysteme aus pädagogischer Sicht, März 1997

Heft 137: M. Remme: Organisationsplanung durch konstruktivistische Modellierung, Februar 1997

Heft 136: M. Daneva, R. Heib, A.-W. Scheer: Benchmarking Business Process Models, Oktober 1996

Heft 135: M. Remme, J. Galler, M. Göbl, F. Habermann, A.-W. Scheer: IuK-Systeme für Planungsinseln, Oktober 1996

Heft 134: R. Heib, M. Daneva, A,-W.Scheer: Benchmarking as a Controlling Tool in Information Management, Oktober 1996

Heft 133: A.-W. Scheer: ARIS-House of Business Engineering, September 1996

Heft 132: J. Sander, A.-W. Scheer: Multimedia Engineering: Rahmenkonzept zum interdisziplinären Management von Multimedia-Projekten, Juli 1996

Heft 131: R. Heib, M. Daneva, A.-W. Scheer: ARIS-based Reference Model for Benchmarking, April 1996

Heft 130: R. Chen, V. Zimmermann, A.-W. Scheer: Geschäftsprozesse und integrierte Informationssysteme im Krankenhaus, April 1996

Heft 129: M. Nüttgens, V. Zimmermann, A.-W. Scheer: Business Process Reengineering in der Verwaltung, April 1996

Heft 128: P. Hirschmann, P. Lubiewski, A.-W. Scheer: Management von Konzernprozessen - Eine Fallstudie -, März 1996

Heft 127: J. Galler, M. Remme, A.-W. Scheer: Der Inseltrainer - Ein multimediales Lernsystem zur Qualifizierung in Planungsinseln, Januar 1996

Heft 126: P. Loos, O. Krier, P. Schimmel, A.-W. Scheer: WWW-gestützte überbetriebliche Logistik - Konzeption des Prototyps WODAN zur unternehmensübergreifenden Kopplung von Beschaffungs- und Vertriebssystemen, Februar 1996

Heft 125: M. Remme, A.-W. Scheer: Konstruktion von Prozeßmodellen, Februar 1996

Heft 124: M. Bold, E. Landwehr, A.-W. Scheer: Die Informations- und Kommunikationstechnologie als Enabler einer effizienten Verwaltungsorganisation, Februar 1996

Heft 123: P. Loos: Workflow und industrielle Produktionsprozesse - Ansätze zur Integration, Januar 1996

Heft 122: A.-W. Scheer: Industrialisierung der Dienstleistungen, Januar 1996

Heft 121: J. Galler: Metamodelle des Workflow-Managements, Dezember 1995

Heft 120: C. Kocian, F. Milius, M. Nüttgens, J. Sander, A.-W. Scheer: Kooperationsmodelle für vernetzte KMU-Strukturen, November 1995

Heft 119: W. Hoffmann, A.-W. Scheer, C. Hanebeck: Geschäftsprozeßmanagement in virtuellen Unternehmen, Oktober 1995

Heft 118: M. Remme, J. Galler, O. Gierhake, A.-W. Scheer: Die Erfassung der aktuellen Unternehmensprozesse als erste operative Phase für deren Re-engineering -Erfahrungsbericht-, September 1995

Heft 117: J. Galler, A.-W. Scheer, S. Peter: Workflow-Projekte: Erfahrungen aus Fallstudien und Vorgehensmodell, August 1995

Heft 116: A. Gücker, W. Hoffmann, M. Möbus, J. Moro, C. Troll: Objektorientierte Modellierung eines Qualitäts-informationssystems, Juni 1995

Heft 115: Th. Allweyer: Modellierung und Gestaltung adaptiver Geschäftsprozesse, Mai 1995

Heft 114: W. Hoffmann, A.-W. Scheer, M. Hoffmann: Überführung strukturierter Modellierungsmethoden in die Object Modeling Technique (OMT), März 1995

Heft 113: P. Hirschmann, A.-W. Scheer: Konzeption einer DV-Unterstützung für das überbetriebliche Prozeßmanagement, November 1994

Heft 112: A.-W. Scheer, M. Nüttgens, A. Graf v. d. Schulenburg: Informationsmanagement in deutschen Großunternehmen - Eine empirische Erhebung zu Entwicklungsstand und -tendenzen, November 1994

Heft 111: A.-W. Scheer: ARIS-Toolset: Die Geburt eines Softwareproduktes, Oktober 1994

Heft 110: M. Remme, A.-W. Scheer: Konzeption eines leistungsketteninduzierten Informationssystemmanagements, September 1994

Heft 109: Th. Allweyer, P. Loos, A.-W. Scheer: An Empirical Study on Scheduling in the Process Industries, July 1994

Heft 108: J. Galler, A.-W. Scheer: Workflow-Management: Die ARIS-Architektur als Basis eines multimedialen Workflow-Systems, Mai 1994

Heft 107: R. Chen, A.-W. Scheer: Modellierung von Prozeßketten mittels Petri-Netz-Theorie, Februar 1994

Heft 106: W. Hoffmann; R. Wein; A.-W. Scheer: Konzeption eines Steuerungsmodells für Informationssysteme - Basis für die Real-Time-Erweiterung der EPK (rEPK), Dezember 1993

Heft 105: A. Hars; V. Zimmermann; A.-W. Scheer: Entwicklungslinien für die computergestützte Modellierung von Aufbau- und Ablauforganisation, Dezember 1993

Heft 104: A. Traut; T. Geib; A.-W. Scheer: Sichtgeführter Montagevorgang - Planung, Realisierung, Prozeßmodell, Juni 1993

Heft 103: wird noch nicht verlegt

Heft 102: P. Loos: Konzeption einer graphischen Rezeptverwaltung und deren Integration in eine CIP-Umgebung - Teil 1, Juni 1993

Heft 101: W. Hoffmann, J. Kirsch, A.-W. Scheer: Modellierung mit Ereignisgesteuerten Prozeßketten (Methodenbuch, Stand: Dezember 1992), Januar 1993

Heft 100: P. Loos: Representation of Data Structures Using the Entity Relationship Model and the Transformation in Relational Databases, January 1993

Heft 99: H. Heß: Gestaltungsrichtlinien zur objektorientierten Modellierung, Dezember 1992

Heft 98: R. Heib: Konzeption für ein computergestütztes IS-Controlling, Dezember 1992

Heft 97: Chr. Kruse, M. Gregor: Integrierte Simulationsmodellierung in der Fertigungssteuerung am Beispiel des CIM-TTZ Saarbrücken, Dezember 1992

Heft 96: P. Loos: Die Semantik eines erweiterten Entity-Relationship-Modells und die Überführung in SQL-Datenbanken, November 1992

Heft 95: R. Backes, W. Hoffmann, A.-W. Scheer: Konzeption eines Ereignisklassifikationssystems in Prozeßketten, November 1992

Heft 94: Chr. Kruse, A.-W. Scheer: Modellierung und Analyse dynamischen Systemverhaltens, Oktober 1992

Heft 93: M. Nüttgens, A.-W. Scheer, M. Schwab: Integrierte Entsorgungssicherung als Bestandteil des betrieblichen Informations-managements, August 1992

Heft 92: A. Hars, R. Heib, Chr. Kruse, J. Michely, A.-W. Scheer: Approach to classification for information engineering - methodology and tool specification, August 1992

Heft 91: C. Berkau: Konzept eines controllingbasierten Prozeßmanagers als intelligentes Multi-Agent-System, Januar 1992

Heft 90: C. Berkau, A.-W. Scheer: VOKAL (System zur Vorgangskettendarstellung), Teil 2: VKD-Modellierung mit Vokal, Dezember 1991 (wird nicht verlegt)

Heft 89: G. Keller, M. Nüttgens, A.-W. Scheer: Semantische Prozeßmodellierung auf der Grundlage "Ereignisgesteuerter Prozeßketten (EPK)", Januar 1992

Heft 88: W. Hoffmann, B. Maldener, M. Nüttgens, A.-W. Scheer: Das Integrationskonzept am CIM-TTZ Saarbrücken (Teil 2: Produktionssteuerung), Januar 1992

Heft 87: M. Nüttgens, G. Keller, S. Stehle: Konzeption hyperbasierter Informationssysteme, Dezember 1991

Heft 86: A.-W. Scheer: Koordinierte Planungsinseln: Ein neuer Lösungsansatz für die Produktionsplanung, November 1991

Heft 85: W. Hoffmann, M. Nüttgens, A.-W. Scheer, St. Scholz: Das Integrationskonzept am CIM-TTZ Saarbrücken (Teil 1: Produktionsplanung), Oktober 1991

Heft 84: A. Hars, R. Heib, Ch. Kruse, J. Michely, A.-W. Scheer: Concepts of Current Data Modelling Methodologies - A Survey - 1991

Heft 83: A. Hars, R. Heib, Ch. Kruse, J. Michely, A.-W. Scheer: Concepts of Current Data Modelling Methodologies - Theoretical Foundations - 1991

Heft 82: C. Berkau: VOKAL (System zur Vorgangskettendarstellung und -analyse), Teil 1: Struktur der Modellierungs-methode - Dezember 1991 (wird nicht verlegt)

Heft 81: A.-W. Scheer: Papierlose Beratung - Werkzeugunterstützung bei der DV-Beratung, August 1991

Heft 80: G. Keller, J. Kirsch, M. Nüttgens, A.-W. Scheer: Informationsmodellierung in der Fertigungssteuerung, August 1991

Heft 79: A.-W. Scheer: Konsequenzen für die Betriebswirtschaftslehre aus der Entwicklung der Informations- und Kommunikationstechnologien, Mai 1991

Heft 78: H. Heß: Vergleich von Methoden zum objektorientierten Design von Softwaresystemen, August 1991

Heft 77: W. Kraemer: Ausgewählte Aspekte zum Stand der EDV-Unterstützung für das Kostenmanagement: Modellierung benutzerindividueller Auswertungssichten in einem wissensbasierten Controlling-Leitstand, Mai 1991

Heft 76: Ch. Houy, J. Klein: Die Vernetzungsstrategie des Instituts für Wirtschaftsinformatik - Migration vom PC-Netzwerk zum Wide Area Network (noch nicht veröffentlicht)

Heft 75: M. Nüttgens, St. Eichacker, A.-W. Scheer: CIM-Qualifizierungskonzept für Klein- und Mittelunternehmen (KMU), Januar 1991

Heft 74: R. Bartels, A.-W. Scheer: Ein Gruppenkonzept zur CIM-Einführung, Januar 1991

Heft 73: A.-W. Scheer, M. Bock, R. Bock: Expertensystem zur konstruktionsbegleitenden Kalkulation, November 1990

Heft 72: M. Zell: Datenmanagement simulationsgestützter Entscheidungsprozesse am Beispiel der Fertigungssteuerung, November 1990

Heft 71: D. Aue, M. Baresch, G. Keller: **URMEL**, Ein **U**nte**R**nehmens**M**od**EL**lierungsansatz, Oktober 1990

Heft 70: St. Spang, K. Ibach: Zum Entwicklungsstand von Marketing-Informationssystemen in der Bundesrepublik Deutschland, September 1990

Heft 69: A.-W. Scheer, R. Bartels, G. Keller: Konzeption zur personalorientierten CIM-Einführung, April 1990

Heft 68: W. Kraemer: Einsatzmöglichkeiten von Expertensystemen in betriebswirtschaftlichen Anwendungsgebieten, März 1990

Heft 67: A.-W. Scheer: Modellierung betriebswirtschaftlicher Informationssysteme (Teil 1: Logisches Informationsmodell), März 1990

Heft 66: W. Jost, G. Keller, A.-W. Scheer: CIMAN - Konzeption eines DV-Tools zur Gestaltung einer CIM-orientierten Unternehmensarchitektur, März 1990

Heft 65: A. Hars, A.-W. Scheer: Entwicklungsstand von Leitständen[1], Dezember 1989

Heft 64: C. Berkau, W. Kraemer, A.-W. Scheer: Strategische CIM-Konzeption durch Eigenentwicklung von CIM-Modulen und Einsatz von Standardsoftware, Dezember 1989

Heft 63: A.-W. Scheer: Unternehmens-Datenbanken - Der Weg zu bereichsübergreifenden Datenstrukturen, September 1989

Heft 62: M. Zell, A.-W. Scheer: Simulation als Entscheidungsunterstützungsinstrument in CIM, September 1989

Heft 61: A.-W. Scheer, G. Keller, R. Bartels: Organisatorische Konsequenzen des Einsatzes von Computer Aided Design (CAD) im Rahmen von CIM, Januar 1989

Heft 60: A.-W. Scheer, W. Kraemer: Konzeption und Realisierung eines Expertenunterstützungssystems im Controlling, Januar 1989

Heft 59: R. Herterich, M. Zell: Interaktive Fertigungssteuerung teilautonomer Bereiche, November 1988

Heft 58: A.-W. Scheer: CIM in den USA - Stand der Forschung, Entwicklung und Anwendung, November 1988

Heft 57: A.-W. Scheer: Present Trends of the CIM Implementation (A qualitative Survey) Juli 1988

Heft 56: A.-W. Scheer: Enterprise wide Data Model (EDM) as a Basis for Integrated Information Systems, Juli 1988

Heft 55: D. Steinmann: Expertensysteme (ES) in der Produktionsplanung und -steuerung (PPS) unter CIM-Aspekten, November 1987, Vortrag anläßlich der Fachtagung "Expertensysteme in der Produktion" am 16. und 17.11.1987 in München

Heft 54: U. Leismann, E. Sick: Konzeption eines Bildschirmtext-gestützten Warenwirtschaftssystems zur Kommunikation in verzweigten Handelsunternehmungen, August 1986

Heft 53: A.-W. Scheer: Neue Architektur für EDV-Systeme zur Produktionsplanung und -steuerung, Juli 1986

Heft 52: P. Loos, T. Ruffing: Verteilte Produktionsplanung und -steuerung unter Einsatz von Mikrocomputern, Juni 1986

Heft 51: A.-W. Scheer: Strategie zur Entwicklung eines CIM-Konzeptes - Organisatorische Entscheidungen bei der CIM-Implementierung, Mai 1986

Heft 50: A.-W. Scheer: Konstruktionsbegleitende Kalkulation in CIM-Systemen, August 1985

Heft 49: A.-W. Scheer: Wirtschaftlichkeitsfaktoren EDV-orientierter betriebswirtschaftlicher Problemlösungen, Juni 1985

Heft 48: A.-W. Scheer: Kriterien für die Aufgabenverteilung in Mikro-Mainframe Anwendungssystemen, April 1985

Heft 47: A.-W. Scheer: Integration des Personal Computers in EDV-Systeme zur Kostenrechnung, August 1984

Heft 46: H. Krcmar: Die Gestaltung von Computer am-Arbeitsplatz-Systemen - ablauforientierte Planung durch Simulation, August 1984

Heft 45: J. Ahlers, W. Emmerich, H. Krcmar, A. Pocsay, A.-W. Scheer, D. Siebert: EPSOS-D, Ein Werkzeug zur Messung der Qualität von Software-Systemen, August 1984

Heft 44: A.-W. Scheer: Schnittstellen zwischen betriebswirtschaftlicher und technische Datenverarbeitung in der Fabrik der Zukunft, Juli 1984

Heft 43: A.-W. Scheer: Einführungsstrategie für ein betriebliches Personal-Computer-Konzept, März 1984

Heft 42: A.-W. Scheer: Factory of the Future, Vorträge im Fachausschuß "Informatik in Produktion und Materialwirtschaft" der Gesellschaft für Informatik e. V., Dezember 1983

Heft 41: H. Krcmar: Schnittstellenprobleme EDV-gestützter Systeme des Rechnungswesens, August 1983, Vortrag anläßlich der 4. Saarbrücker Arbeitstagung "Rechnungswesen und EDV" in Saarbrücken vom 26. - 28.09.1983

Heft 40: A.-W. Scheer: Strategische Entscheidungen bei der Gestaltung EDV-gestützter Systeme des Rechnungswesens, August 1983, Vortrag anläßlich der 4. Saarbrücker Arbeitstagung "Rechnungswesen und EDV" in Saarbrücken vom 26. - 28.09.1983

Heft 39: A.-W. Scheer: Personal Computing - EDV-Einsatz in Fachabteilungen, Juni 1983

Heft 38: A.-W. Scheer: Interaktive Methodenbanken: Benutzerfreundliche Datenanalyse in der Marktforschung, Mai 1983

Heft 37: A.-W. Scheer: DV-gestützte Planungs- und Informationssysteme im Produktionsbereich, September 1982

Heft 36: A.-W. Scheer: Rationalisierungserfolge durch Einsatz der EDV - Ziel und Wirklichkeit, August 1982, Vortrag anläßlich der 3. Saarbrücker Arbeitstagung "Rationalisierung" in Saarbrücken vom 04. - 06. 10.1982

Heft 35: J. Ahlers, W. Emmerich, H. Krcmar, A. Pocsay, A.-W. Scheer, D. Siebert: EPSOS-D, Konzept einer computergestützten Prüfungsumgebung, Juli 1982

Heft 34: J. Ahlers, W. Emmerich, H. Krcmar, A. Pocsay, A.-W. Scheer, D. Siebert: EPSOS - Ein Ansatz zur Entwicklung prüfungsgerechter Software-Systeme, Mai 1982

Heft 33: A.-W. Scheer: Disposition- und Bestellwesen als Baustein zu integrierten Warenwirtschaftssystemen, März 1982, Vortrag anläßlich des gdi-Seminars "Integrierte Warenwirtschafts-Systeme" in Zürich vom 10. - 12. Dezember 1981

Heft 32: A.-W. Scheer: Einfluß neuer Informationstechnologien auf Methoden und Konzepte der Unternehmensplanung, März 1982, Vortrag anläßlich des Anwendergespräches "Unternehmensplanung und Steuerung in den 80er Jahren in Hamburg vom 24. - 25.11.1981

Die Hefte 1 - 31 werden nicht mehr verlegt.