universität mainz

LEHRSTUHL FÜR
ALLG. BWL UND WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. HERBERT KARGL

Schwickert, Axel C.; Häusler, Oliver

Web Site Security

ARBEITSPAPIERE WI
Nr. 5/1999

Schriftleitung:
Dr. rer. pol. Axel C. Schwickert

Information

Reihe: Arbeitspapiere WI

Herausgeber: Univ.-Prof. Dr. Axel C. Schwickert
Professur für BWL und Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Bis Ende des Jahres 2000 lag die Herausgeberschaft bei:

Lehrstuhl für Allg. BWL und Wirtschaftsinformatik
Johannes Gutenberg-Universität Mainz
Fachbereich Rechts- und Wirtschaftswissenschaften
Welderweg 9
D - 55099 Mainz

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IuK-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstanden aus Forschungsarbeiten, Diplom-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr- und Vortragsveranstaltungen des Lehrstuhls für Allg. Betriebswirtschaftslehre und Wirtschaftsinformatik Univ. Prof. Dr. Herbert Kargl an der Johannes Gutenberg-Universität Mainz.

Hinweise: Wir nehmen Ihre Anregungen und Kritik zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.
Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit dem Herausgeber (Gießen) unter obiger Adresse Kontakt auf.
Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe und deren Bezug erhalten Sie auf dem Schlußblatt eines jeden Arbeitspapiers und auf der Web Site des Lehrstuhls unter der Adresse http://wi.uni-giessen.de

Arbeitspapiere WI Nr. 5/1999

Autoren: Schwickert, Axel C.; Häusler, Oliver

Titel: Web Site Security

Zitation: Schwickert, Axel C.; Häusler, Oliver: Web Site Security, in: Arbeitspapiere WI, Nr. 5/1999, Hrsg.: Lehrstuhl für Allg. BWL und Wirtschaftsinformatik, Johannes Gutenberg-Universität: Mainz 1999.

Kurzfassung: Der Untersuchungsbereich der vorliegenden Arbeit erstreckt sich über die Sicherheit aller mit der Web Site eines Unternehmens verbundenen IT-Komponenten vor unbefugter Benutzung, Verlust, Beschädigung, Diebstahl und Manipulation. Dieser Untersuchungsbereich wird hier als „Web Site Security“ (WSS) bezeichnet. Ziel ist es, über die grundlegende Aufarbeitung des Themas „Web Site Security“ zu einem Konzeptvorschlag zu gelangen, der alle wichtigen sicherheitsrelevanten Aspekte bei der Implementierung und dem Betrieb einer Web Site zusammenfügt. Dazu werden in Kapitel 2 zunächst die Grundlagen eines Sicherheitsmanagements von Internet-Systemen in Unternehmen skizziert. Die spezielle Positionierung des IT-Systems „Web Site“ mit den zugehörigen Sicherheitsaktivitäten erfolgt anhand eines Modells, das das Umfeld und die Zusammenhänge eines unternehmerischen eBusiness abbildet. Kapitel 3 gibt einen Überblick über Sicherheitslücken und Gefahrenquellen für eine Web Site. Die Schilderung von unterschiedlichen Angriffsmöglichkeiten auf Internet-, Extranet- und Intranet-Ebene dient dazu, das Bewußtsein für die typischen Schwachstellen zu schärfen. Auf technische Details wird nicht tiefer als zum allgemeinen Verständnis notwendig eingegangen; wegen der sich schnell verändernden Techniken und Instrumente sind diesbezügliche Aussagen häufig schon veraltet, wenn sie zu Papier gebracht werden. In Kapitel 4 wird dann aus den vorhergehenden Ausführungen ein Konzeptvorschlag für eine umfassende Web Site Security abgeleitet. Eine Risikoanalyse führt zu organisatorischen und technischen Sicherheitsmaßnahmen, die anhand von Checklisten operationalisiert werden. Ein Ausblick auf Tendenzen im Bereich von Web Site Security schließt die Arbeit ab.

Schlüsselwörter: Sicherheit, Sicherheitskonzept, Web Site, Security, Risikoanalyse, Firewall, Intrusion Detection, Virtuelle Private Netzwerke, Viren, Protokolle, Web-Sprachen, WWW, Internet

Inhaltsverzeichnis

1 Ziel und Aufbau

Seit Anfang der 90er Jahre sind vermehrt Schlagzeilen in der Fachpresse zu finden, die die Sicherheit von Computersystemen betreffen:

- „Millionenschäden durch CIH-Virus. (...) Allein in China sollen bis zu 200 000 Computer von CIH betroffen sein, in Südkorea bis zu eine Million. Andere Quellen nennen mindestens 7600 geschädigte Rechner in China. 30 000 in Indien, 10 000 in Bangladesch und in Südkorea sogar bis zu 240 000."[1]
- „Sicherheitsbedenken halten viele Anbieter und Konsumenten noch vom elektronischen Handel ab."[2]
- „Bedrohte IT: Überall lauern Gefahren, (...)"[3]
- „Nach Berichten in der Sicherheits-Mailing-Liste Bugtraq sind in Hunderten Online-Shops die Kunden- und Bestelldaten für alle Welt per WWW lesbar."[4]

Besonders in puncto Internet und eBusiness rückt das Thema „IT-Sicherheit" in den Mittelpunkt des Interesses. Ein Unternehmen zeigt seine eBusiness-Präsenz anhand einer unternehmenseigenen Web Site, über die die eBusiness-Aktivitäten des Unternehmens abgewickelt werden. Unter dem Begriff „Web Site" wird alles zusammengefaßt, was die Präsenz des Unternehmens im Web betrifft: neben der normalerweise aufgeführten, öffentlichen „Home Page" des Unternehmens (mit weiterführendem öffentlichem Page-Unterbau) gehören dazu die Strukturen des unternehmenseigenen Intranets sowie die Schnittstellen und Verfahren zur (längerfristigen) Kooperation mit Geschäftspartnern (Extranet).

Der Untersuchungsbereich der vorliegenden Arbeit erstreckt sich über die Sicherheit aller mit der Web Site eines Unternehmens verbundenen IT-Komponenten vor unbefugter Benutzung, Verlust, Beschädigung, Diebstahl und Manipulation. Die Darstellung von Risiken und Bedrohungen für ein eBusiness und die Beschreibung geeigneter und angemessener Gegenmaßnahmen ist ein daraus resultierender Hauptbestandteil der vorliegenden Arbeit. Dieser Untersuchungsbereich wird hier als „Web Site Security" (WSS) bezeichnet.

In den folgenden Ausführungen wird davon ausgegangen, daß sich ein Unternehmen für eBusiness-Aktivitäten über eine Web Site entschieden hat und demzufolge die involvierte unternehmenseigene IT-Infrastruktur an das öffentliche Internet anzubinden ist. Ziel der vorliegenden Arbeit ist es, über die grundlegende Aufarbeitung des Themas „Web Site Security" zu einem Konzeptvorschlag zu gelangen, der alle wichtigen sicherheitsrelevanten Aspekte bei der Implementierung und dem Betrieb einer Web Site zusammenfügt. Dazu werden in Kapitel 2 zunächst die Grundlagen eines Sicherheitsmanagements von Internet-Systemen in Unternehmen skizziert. Die spezielle Positionierung des IT-Systems „Web Site" mit den zugehörigen Sicherheitsaktivitäten erfolgt anhand eines Modells, das das Umfeld und die Zusammenhänge eines unternehmerischen eBusiness abbildet. Hierbei lassen sich organisatorische und technische Maßnahmen unterscheiden.

---

1 Luckhardt, N.: Millionenschäden durch CIH-Virus, in: c´t Magazin für Computertechnik, 10/1999, S. 22.

2 Vgl. Afif, Noelani Maria: Sichere Abrechnung im Internet-Handel, in: Information Week 19/1998, S. 12.

3 Weck, Gerhard; Gerbisch, Sandra Ines: Gefahren lauern überall: IT-Sicherheitskonzepte helfen Risiken mindern, in: IT-Management, 03/1999, S. 48.

4 Luckhardt, N.: Hunderte Online-Shops verraten Kundendaten, in: c´t Magazin für Computertechnik, 10/1999, S. 22.

Kapitel 3 gibt einen Überblick über Sicherheitslücken und Gefahrenquellen für eine Web Site. Die Schilderung von unterschiedlichen Angriffsmöglichkeiten auf Internet-, Extranet- und Intranet-Ebene dient dazu, das Bewußtsein für die typischen Schwachstellen zu schärfen. Auf technische Details wird nicht tiefer als zum allgemeinen Verständnis notwendig eingegangen; wegen der sich schnell verändernden Techniken und Instrumente sind diesbezügliche Aussagen häufig schon veraltet, wenn sie zu Papier gebracht werden.

In Kapitel 4 wird dann aus den vorhergehenden Ausführungen ein Konzeptvorschlag für eine umfassende Web Site Security abgeleitet. Eine Risikoanalyse führt zu organisatorischen und technischen Sicherheitsmaßnahmen, die anhand von Checklisten operationalisiert werden. Ein Ausblick auf Tendenzen im Bereich von Web Site Security schließt die Arbeit ab.

2 IT-Sicherheit und Web Site Security

2.1 Grundlagen eines Sicherheitsmanagements von Internet-Systemen

Grundsätzlich bestehen für jedes IT-System erhebliche Risiken. Einem Teil dieser Risiken sind IT-Systeme auch schon ohne den Anschluß an externe Kommunikationsnetze ausgesetzt. Oftmals verursacht nicht die Informationstechnik finanzielle Verluste und Probleme mit der Sicherheit, sondern Mitarbeiter des eigenen Unternehmens.[5] Viele Probleme werden zudem unbeabsichtigt verursacht, z. B. durch die Experimentierfreudigkeit von Mitarbeitern. Aus dieser Betrachtung ergibt sich eine organisatorische Ebene von Sicherheit, während die technischen Belange auf der Hand liegen.

Durch die Anbindung an das öffentliche Internet erhöht sich das Risiko erheblich, Ziel von Attacken zu werden. Achtzig Prozent aller Angriffe auf unternehmensinterne Datennetze erfolgen nach einer Studie des amerikanischen Verteidigungsministeriums über das Internet als Zugangsmedium.[6] Seit der Entstehung des Internets befinden sich die Sicherheitsanforderungen an dieses Medium in einem stetigen Wandel. Weil sich das heutige Internet aus dem militärischen DARPA-Projekt entwickelte, standen zu Anfang die Interessen des Militärs im Vordergrund. Geheimhaltung, Schutz vor Spionage und Verfügbarkeit der Systeme waren die Anforderungen, die das Militär an die Internet-Technologien (Protokolle) stellte. Das verbindungslose, paketvermittelnde Internet-Protokoll wurde deshalb so konzipiert, daß beim Ausfall eines Teilnetzes die restlichen Netzsegmente weiterhin kommunizieren konnten. Die einzigen Kommunikationsteilnehmer waren damals nur bekannte und vertrauenswürdige Militäreinrichtungen. Zu diesem Zeitpunkt war noch nicht vorhersehbar, daß sich das Internet zum Transportmedium für internationale Geschäftstransaktionen entwickeln würde.[7] Dies geschah erst allmählich durch die sukzessive, weltweite Öffnung des Internets für Universitäten und Bildungs- und Forschungseinrichtungen in den siebziger und achtziger Jahren. Ein breites Massenpublikum fand seinen Weg ins Internet erst zu Beginn der neunziger Jahre mit der Einführung des HTT-Protokolls (HTTP), das die Nutzung von Internet-Diensten und -Angeboten stark vereinfachte.

5 Vgl. Kyas, Othmar: Sicherheit im Internet, 2. Aufl., Bonn: Internat. Thomson Publishing 1998, S. 16.

6 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 17.

7 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, Heidelberg: dpunkt-Verlag 1998, S. 3.

Heute hat sich die offene Internet-Technologie als Kommunikationsstandard auch im Intra- und Extranet von Unternehmen etabliert und verdrängt immer schneller andere, ältere und oftmals proprietäre Kommunikationsplattformen. Das Internet hat sich von einem Medium für Militärs und Intellektuelle zu einem Massenmedium entwickelt.

Die vermehrt kommerzielle Ausrichtung des Internets (siehe Kapitel 2.3), die große Menge an übertragenen Daten und die unüberschaubare Anzahl von anonymen Benutzern haben die Anforderungen an Sicherheit im Internet grundlegend verändert. Internet-Systeme im unternehmerischen Einsatz und vor allem im eBusiness müssen ein grundlegendes Maß an Vertraulichkeit, Integrität und Verfügbarkeit[8] bieten. Diese Anforderungen werden als Grundanforderungen an IT-Sicherheit angesehen. Funktionalitäten von IT-Systemen, die dies gewährleisten, sind Sicherheitsdienste.[9] Zusätzlich zu den vorgenannten Grundanforderungen gilt es, weitere Aspekte zu berücksichtigen: Die Sicherheitsdienste müssen gewährleisten, daß nur explizit bekannte Personen durch „Authentifikation“ auf definierte Bereiche einer Web-Präsenz Zugriff erhalten. Die Sicherheitsdienste müssen den Zugriff auf bestimmte kritische Bereiche, wie z. B. Personalstammdaten, über „Zugriffskontrollen“ beschränken. Schließlich ist es wünschenswert, daß z. B. bei der elektronischen Zahlungsabwicklung im Internet ein definiertes Maß an Anonymität gewahrt bleibt.

Im allgemeinen werden sieben Sicherheitsdienste benannt, deren konkrete Leistungen durch die individuellen Sicherheitsanforderungen eines Unternehmens bestimmt werden:[10]

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentifikation
- Zugriffskontrolle
- Verbindlichkeit
- Anonymität

Ein Sicherheitskonzept setzt mit Hilfe der Sicherheitsdienste diese Anforderungen um. Die Durchsetzung von Sicherheitsanforderungen und -konzepten erfordert ein individuelles Sicherheitsmanagement besonders für jene Unternehmen, die im eBusiness tätig werden. Im folgenden wird unter Sicherheitsmanagement von IT-Systemen die Summe aller organisatorischen und technischen Maßnahmen zur Gewährleistung der sieben Sicherheitsdienste für unternehmerische Daten und IT-Infrastrukturen verstanden.

Grundlegend für den Erfolg organisatorischer und technischer Maßnahmen eines Sicherheitsmanagements ist die systematische Integration der Maßnahmen in den gesamten Lebenszyklus von Internet-Systemen, also in Planung, Entwicklung und Betrieb. In bezug auf das IT-System „Web Site“ erfolgt diese Integration über das nachfolgend vorgestellte WSE-Komponentenmodell.[11]

8 Vgl. Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, Bonn: O´Reilley, Internat. Thomson-Verl., 1996, S. 4.

9 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 4 f.

10 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 7.

11 Eine Gesamtdarstellung dieses Modells findet sich in Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, in: Arbeitspapiere WI, Nr. 12/1998, Hrsg.: Lehrstuhl für Allg. BWL und Wirtschaftsinformatik, Johannes Gutenberg-Universität: Mainz 1998.

2.2 Web Site Security im Web-Site-Engineering-Komponentenmodell

Das Web-Site-Engineering-Komponentenmodell lehnt sich an das bekannte Software Engineering an und besteht aus einem Struktur- und Vorgehensmodell; letzteres beschreibt die dynamische Aktivitätenabfolge bei der (Weiter-)Entwicklung einer Web Site, womit auch die Maßnahmen eines Sicherheitsmanagements erfaßt werden.[12]

Unter „Web Site Engineering“ (WSE) wird dabei die ingenieurwissenschaftliche Planung und Entwicklung einer Web Site verstanden. Dazu gehören die Festlegung strategischer Zielvorgaben, eine Situationsanalyse, die systematische Erarbeitung von Anforderungen an das System Web Site, die Modellierung und Realisierung des Systems Web Site sowie die permanente Pflege und Weiterentwicklung. Weiterhin beinhaltet das WSE-Komponentenmodell eine zeitliche und inhaltliche Strukturierung der Ressourcen, Methoden, Techniken und Werkzeuge, die auf den Entwicklungsgegenstand Web Site abgestimmt sind. Das Gesamtmodell setzt sich aus drei Komponenten zusammen: der strategischen Unternehmensführung, den Zielfeldern des WSE und dem WSE-Vorgehensmodell.

WSE-Komponente 1: Strategische Unternehmensführung[13]

Die WSE-Komponente der strategischen Unternehmensführung teilt die Realisierung von eBusiness-Vorhaben in strategische, taktische und operative Ebenen auf. Dies geschieht analog zur organisatorischen Aufteilung von lang-, mittel- und kurzfristigen Unternehmensentscheidungen nach Hinterhuber.[14] Die Komponente der strategischen Unternehmensführung spiegelt außerdem das aus der Aufbauorganisation abgeleitete Leitungssystem wider.[15] Oberes, unteres und mittleres Management stehen hier im Hinblick auf Weisungsbefugnisse in Verbindung. Die erste Modell-Komponente gibt auf strategischer Ebene Ziele, auf taktischer Ebene Programme und Konzepte und auf operativer Ebene konkrete Pläne für eBusiness-Maßnahmen vor. Die strategische Unternehmensführung stellt damit die Aktivitäten bei der Implementation und beim Betrieb einer unternehmerischen Web Site in einen allgemeingültigen betriebswirtschaftlichen Zusammenhang, indem sie sich auf klassische Vorgaben bei der Unternehmensplanung bezieht. Innerhalb der strategischen Planung werden die zu besetzenden eBusiness-Segmente sowie die Wettbewerbs- und Erfolgsziele eines unternehmerischen Web Site festgelegt. Die taktische Planung einer Web-Präsenz im Rahmen des WSE-Komponentenmodells enthält die zielorientierte Bereitstellung von Ressourcen (Personal, Finanzen, Betriebsmittel) und die Festlegung mittelfristiger Ziele für die Ausgestaltung und Strukturierung einer Web Site.[16] Bei der operativen Planung einer Web Site müssen die strategischen und taktischen Vorgaben als Rahmenbedingungen berücksichtigt werden. Es wird über den konkreten Einsatz der Ressourcen entschieden. Um die Zielvorgaben zu operationalisieren, werden konkrete Finanz-, Personal- und Terminpläne erstellt. Die operative Planung innerhalb

12 Vgl. Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, a. a. O., S. 7 ff.

13 Vgl. Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, a. a. O., S. 8.

14 Vgl. Hinterhuber, Hans H.: Strategische Unternehmensführung, Band 1: Strategisches Denken – Visionen, Unternehmenspolitik, Strategie, 5., neubearb. und erw. Auflage, Berlin, New York, De Gruyter 1992.

15 Vgl. Wöhe, Günter: Einführung in die allgemeine Betriebswirtschaftslehre, 19., überarb. und erw. Aufl., München: Vahlen 1996, S. 189.

16 Vgl. Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, a. a. O., S. 10.

des WSE-Komponentenmodells bezieht sich auf die substantielle Ausgestaltung und Strukturierung der Zielvorgaben aus der strategischen und taktischen Planung für eine Web Site (siehe Abb. 1[17]).

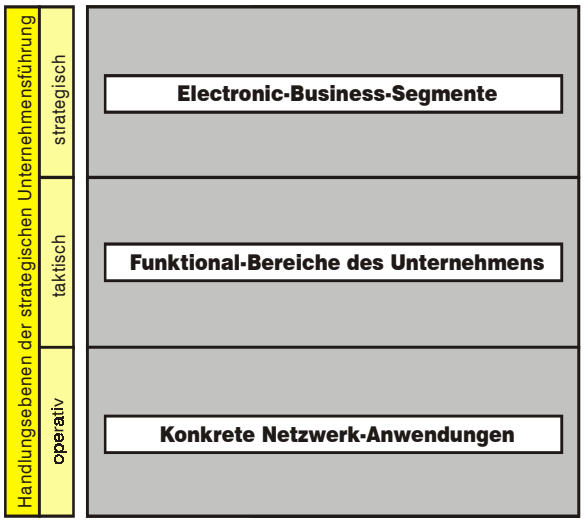

Abb. 1: Strategische Unternehmensführung

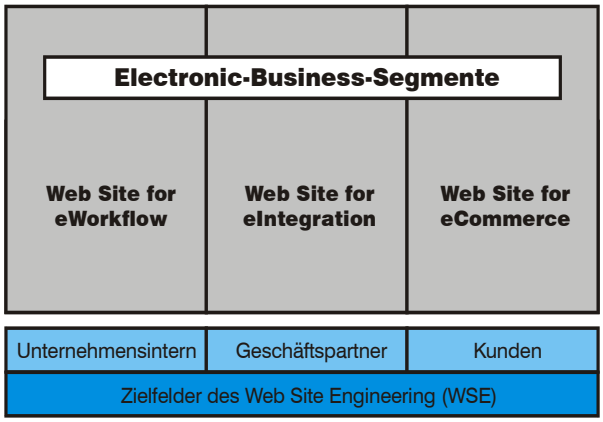

Abb. 2: Zielfelder des WSE

WSE-Komponente 2: Zielfelder des WSE[18]

Über Komponente 2 wird die klare inhaltliche und funktionale Ausrichtung einer Web Site gefordert.[19] Die über die Web Site realisierten eBusiness-Aktivitäten sind auf den elektronischen Markt gerichtet. Dieser wird analog zur kundengruppenorientierten Marktsegmentierung im Marketing in unterschiedliche Zielfelder aufgeteilt. Diese Aufteilung wird an den spezifischen Bedürfnissen der einzelnen Kundengruppen festgemacht. Als Nutzer von Angeboten einer unternehmerischen Web Site können Mitarbeiter, Geschäftspartner und Kunden identifiziert werden. Die Ausrichtung einer Web Site wird dementsprechend auf die spezifischen Bedürfnisse von Mitarbeitern, Geschäftspartnern und Kunden zur Realisierung der eBusiness-Segmente „eWorkflow“, „eIntegration“ und „eCommerce“ abgestimmt (Abb. 2[20]).

Führt man die WSE-Komponenten 1 und 2 zusammen, erhält man eine zweidimensionale Matrix, welche die strategischen Unternehmensentscheidungen auf die Zielfelder des WSE-Komponentenmodells abbildet (Abb. 3[21]). Die strategische Ebene bezieht sich damit auf die langfristig angestrebten eBusiness-Segmente. Auf die zugehörigen Funktionalbereiche (Organisation, Logistik, Absatz) eines Unternehmens zielt die mittelfristige/taktische Handlungse-

17 Vgl. Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, a. a. O., Abb. 2: Handlungsebenen der strategischen Unternehmensführung, S. 9.

18 Vgl. Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, a. a. O., S. 11 f.

19 Vgl. Stahlknecht, Peter; Hasenkamp, Ulrich: Einführung in die Wirtschaftsinformatik, 8., vollst. überarb. und erw. Aufl., Berlin et al.: Springer 1997, S. 323.

20 Vgl. Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, a. a. O., Abb. 3: Zielfelder des Web Site Engineering, S. 9.

21 Vgl. Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, a. a. O., Abb. 4: Handlungsebenen-Zielfeldmatrix, S. 15.

bene ab. Konkrete Netzwerkanwendungen auf Basis von Internet-Technologie stellen die operative Handlungsebene dar. Sie teilt sich analog zur Zielfeldaufteilung mit Mitarbeitern, Geschäftspartnern und Kunden in die Bereiche Intranet, Extranet und Internet auf. Die konkreten Anwendungen für das Intranet können Workflow-Management-Systeme (WFMS), Workgroup Computing System (WGC-Systeme) oder individuelle IT-Systeme sein. Bei den Extranet-Anwendungen kann es sich z. B. um Web-to-Host-Anwendungen, Internet EDI und XML EDI (Extensible Markup Language) zur Anbindung von Geschäftspartnern handeln. Im Rahmen von Internet-Anwendungen im eCommerce-Segment sind auf der operativen Ebene z. B. Angebote wie „eShops“, „eStores“, „Electronic-Payment-Systeme“ (EPS) sowie „eServices“ zu nennen.

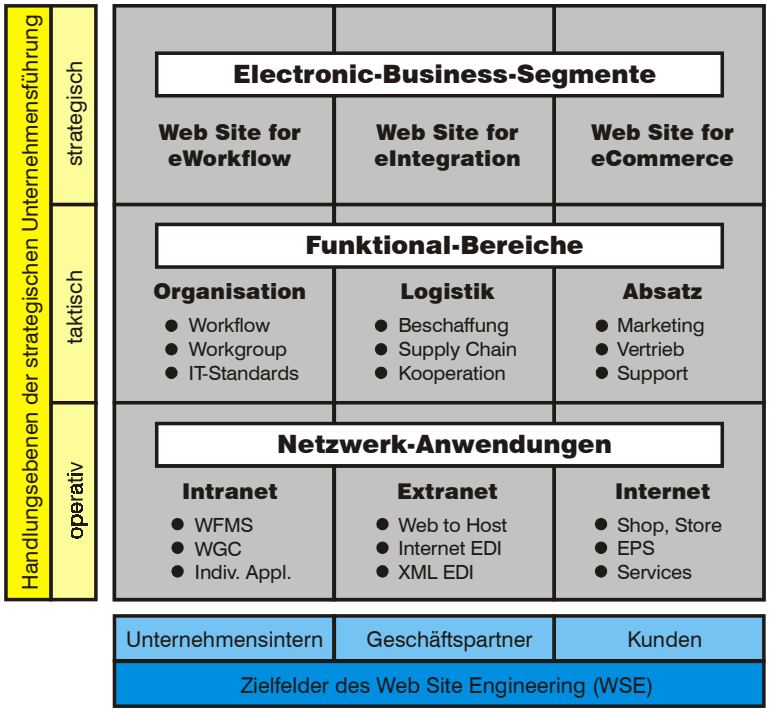

Abb. 3: Handlungsebenen-Zielfeldmatrix

WSE-Komponente 3: Das WSE-Vorgehensmodell[22]

Das WSE-Vorgehensmodell als dritte Komponente des WSE-Komponentenmodells integriert Erfahrungen aus ingenieurwissenschaftlichen Systementwicklungsprozessen in den Bereich der Entwicklung von Anwendungssystemen und stellt ein auf den Einsatz in der Web-Site-Entwicklung abgestimmtes Modell dar. Bei der Entwicklung einer unternehmerischen Web Site wird damit vorrangig die Realisierung eines effizienten Projektmanagements angestrebt. Um dieses Ziel zu erreichen, wird eine Einteilung in typische Phasen bei der Entwicklung einer Web Site vorgenommen. Diese Phasen sind „Web Site Requirements Engineering“ (WSR), „Web Site Design“ (WSD) und „Web Site Online“ (WSO). Den einzelnen Phasen werden Aufgaben und Aktivitäten zugeordnet (siehe Abb. 4[23]).

22 Vgl. Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, a. a. O., S. 16 ff.

23 Vgl. Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, a. a. O., Abb. 5: Das WSE-Vorgehensmodell, S. 20 f.

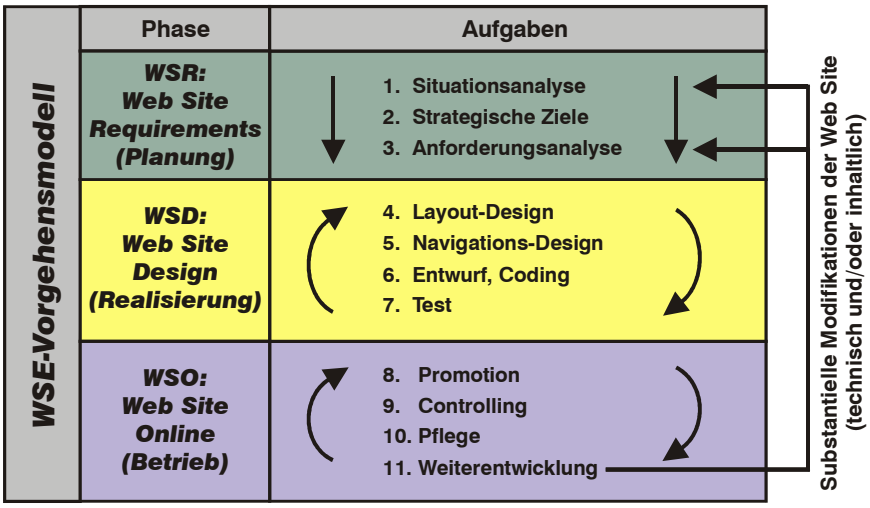

Abb. 4: Aufgaben und Aktivitäten im WSE-Vorgehensmodell

Das WSE-Vorgehensmodell setzt einen kontinuierlichen Durchlauf der einzelnen Phasen voraus, wobei auch Rücksprünge erlaubt sind. Damit wird der Möglichkeit von Veränderungen in den fachlichen und technischen Anforderungen Rechnung getragen. Werden die drei WSE-Komponenten zusammengeführt, ergibt sich ein Würfel, der das komplette WSE-Komponentenmodell graphisch veranschaulicht (Abb. 5[24]). Die 3. Dimension ergibt sich aus dem WSE-Vorgehensmodell. Das WSE-Komponentenmodell liefert damit einen Vorschlag zum systematischen Vorgehen bei der Entwicklung von unternehmerischen Web Sites für eBusiness.

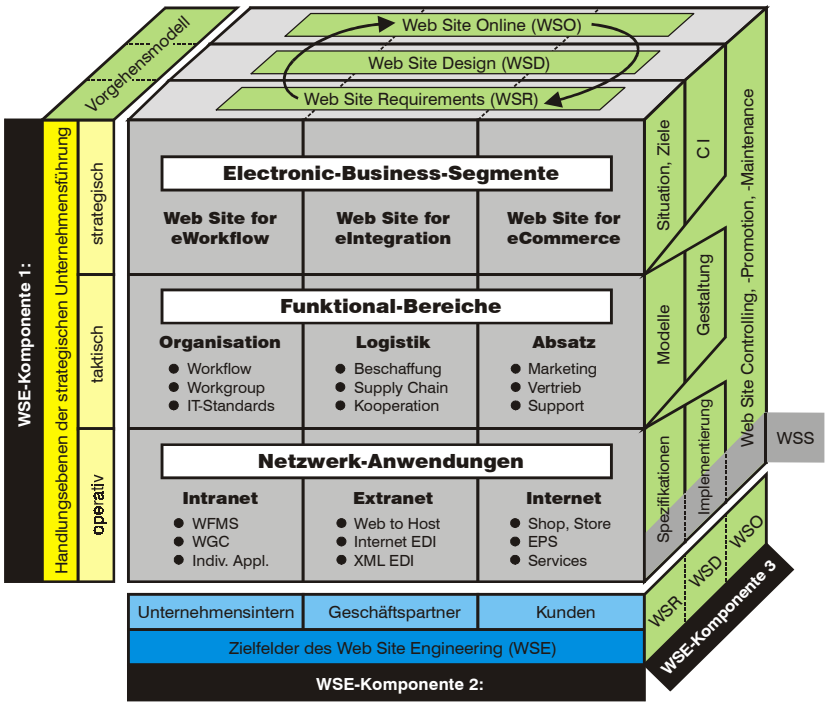

Abb. 5: Das WSE-Komponentenmodell

24 Vgl. Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, a. a. O., Abb. 7: Das WSE-Komponentenmodell, S. 23.

Web Site Security positioniert sich dabei auf der operativen Handlungsebene des WSE-Komponentenmodells. WSS betrifft alle drei Zielfelder des WSE-Komponentenmodells. Hinsichtlich der in Kapitel 2.1 eingeführten Grundbedrohungen müssen für alle Anwendungen auf Intra-, Extra- und Internet-Ebene Sicherheitsdienste zur Verfügung gestellt werden. Im Rahmen des WSE-Vorgehensmodells laufen die Aktivitäten zur WSS zunächst in der Phase WSR ab. Dort wird geplant und entworfen. Des weiteren werden Sicherheitsspezifikationen festgelegt. Diese Pläne und Spezifikationen werden dann auf der WSD-Ebene implementiert und in konkrete Systeme umgesetzt. Diese Systeme „laufen" dann in der Phase WSO. Genauso wie die Inhalte einer Web Site einem stetigen Wandel unterworfen sind (Aktualität), müssen sich auch die Maßnahmen zur Sicherheit den Sicherheitsanforderungen anpassen und sich mit ihnen verändern. Der für Kapitel 4 der vorliegenden Arbeit angekündigte Konzeptvorschlag bündelt die Aktivitäten zur WSS über die drei Phasen WSR, WSD und WSO.

3 Web Sites – Sicherheitslücken und Gefahrenquellen

3.1 Kategorien von Bedrohungen

Um zu einem Konzept mit abgestimmten Sicherheitsmaßnahmen für Web Sites zu gelangen, ist es erforderlich, die Bedrohungen von Web Sites zu systematisieren. Für eine unternehmerische Web Site bestehen organisatorisch und technisch begründete Kategorien von Bedrohungen auf den Ebenen Internet, Extranet und Intranet. Da sich diese Ebenen auf kritische Erfolgsfaktoren eines Unternehmens beziehen (die Kunden-, Partner- und Mitarbeiterbeziehungen), wirken sich Angriffe auf die Web Site direkt auf den Erfolg und die Ziele eines Unternehmens aus.

Beispiele für direkte technische Angriffe auf Web Sites und die ihnen zugrunde liegenden Kommunikationsstrukturen sind seit 1998 verstärkt zu diagnostizieren. Siemens verlor einen milliardenschweren Auftrag aus Südkorea für einen Hochgeschwindigkeitszug, ähnlich dem ICE, an GEC-Alsthom aus Frankreich[25], weil der französische Geheimdienst die unverschlüsselte Kommunikation über Faxe von Siemens abgehört hatte und GEC-Alsthom deshalb den Preis von Siemens unterbieten konnte. Ein weiteres Beispiel ist eine Aktion von IBM, bei der es „gutwilligen Hackern" im Auftrag der IBM gelang, in neun von zehn Online Shops einzudringen und dabei Zugang zu Kreditkarteninformationen zu erlangen, die auf den Servern gespeichert waren.[26]

Vorfälle wie diese verursachen meßbare finanzielle Schäden. Nicht direkt monetär quantifizierbar sind hingegen Imageverluste durch die unbefugte Veränderung von Web Sites[27], der

25 Vgl. Krempel, Stefan; Schmidt, Michael; Kuri, Jürgen: Lange Ohren, in: c´t Magazin für Computertechnik, 4/99, S. 175 und Schmeh, Klaus: Safer net: Kryptografie im Internet und Intranet, Heidelberg: dpunkt-Verlag 1998, S. 17.

26 Vgl. Kuri, Jürgen: IBMs Hackertruppe knackte neun von zehn Online-Shops, Online im Internet: http://www.heise.de/newsticker/data/jk-11.02.99-000/, 11.02.1999.

27 Belege für solche imageschädigenden Eingriffe sind auf einschlägigen Hacker Sites im Internet zu finden, z. B. o. V.: Homepage 2600, Online im Internet: http://www.2600.com/hacked_pages, 28.05.1999.

in der Öffentlichkeit großes Interesse entgegengebracht wird.[28] Publikumswirksame Beispiele derartiger technischer Manipulationen lassen sich der Presse entnehmen:

- Web Site der New York Times gehackt,[29]
- Web Site des FBI gehackt,[30]
- Web Server von ARD Online und RTL geknackt,[31]
- BMW-Hompage gehackt,[32]
- Web Site des Weißen Hauses gecrackt.[33]

Die technisch begründeten Bedrohungen erwachsen vorrangig aus Schwächen in Netzwerkbetriebssystemen, der Ausnutzung besonderer technischer Details von Kommunikationsprotokollen und Web-Sprachen (z. B. Active-X und Java) sowie Viren, Würmern und Trojanischen Pferden. Kapitel 3.3 geht detaillierter auf die technisch begründeten Bedrohungen ein.

Spezifische Bedrohungen für eine Web Site resultieren auch aus ihrem oganisatorischen Umfeld. Private Disketten von Mitarbeitern, die mit Viren verseucht sind, können ganze IT-Systeme lahmlegen. Einige amerikanische Atomwaffenlabors haben z. B. im Frühjahr 1999 vorübergehend die Arbeit eingestellt, weil ihre Rechner zwar nicht mit dem Internet verbunden, aber mit Diskettenlaufwerken ausgestattet waren.[34] Weiterhin legte zur selben Zeit ein Microsoft-Word-Makrovirus namens „Melissa“ wenige Tage nach seiner Entdeckung die eMail-Server vieler Unternehmen lahm.[35]

Oftmals wird auch die Datensicherung vernachlässigt, so daß es nach einem „Crash“ nicht möglich ist, den ursprünglichen Zustand einer Web Site wiederherzustellen.[36] Beispiele für solche Vorfälle sind in der Literatur zwar nicht zu finden, aber es liegt auf der Hand, daß Unternehmen sie nicht publik machen. Der nachlässige Umgang mit Paßworten führt dazu, daß Unbefugte Zugriff auf geschützte Daten erhalten oder Daten verfälscht werden. Es ist beispielsweise nicht erwünscht, aus Bequemlichkeit Paßworte für eMail-Accounts oder den Internet-Zugang lokal auf dem Arbeitsplatzrechner abzuspeichern, weil Angreifer sich Fehler in der entsprechenden Client-Software zunutze machen können, um an diese Paßworte zu gelan-

28 Vgl. Ghosh, Anup K.: E-Commerce Security: Weak Links, Best Defenses, New York et al**.:** Wiley Computer Publishing 1998, S. 11.

29 Vgl. Medosch, Armin: NYTIMES gehackt, Online im Internet: http://www.heise.de/tp/deutsch/inhalt/te/1549/1.html, 14.09.1998.

30 Vgl. Diedrich, Oliver: Der Krieg zwischen FBI und Hackern eskaliert, Online im Internet: http://www.heise.de/newsticker/data/odi-28.05.99-000/, 28.05.1999.

31 Vgl. Luckhardt, Norbert: Weitere Web-Hacks in Deutschland, Online im Internet: http://www.heise.de/newsticker/data/nl-08.10.98-000/, 08.10.1998.

32 Vgl. Ebeling, Adolf: BMW-Homepage gehackt, Online im Internet: http://www.heise.de/newsticker/data/ae-02.01.98-000/, 02.05.1998.

33 Vgl. Rötzer, Florian: Website des Weißen Hauses wurde gecrackt – Update: Online im Internet: http://www.heise.de/tp/deutsch/inhalt/te/2834/1.html, 11.05.1999.

34 Vgl. Meyer, Egbert: Sicherheitsrisiko Diskettenlaufwerk, Online im Internet: http://www.heise.de/newsticker/data/em-08.04.99-000/, 08.04.1999.

35 Vgl. Luckhardt, Norbert: Virus-Alarm: Melissa verbreitet sich wie ein Buschfeuer, Online im Internet: http://www.heise.de/newsticker/data/nl-28.03.99-000/, 28.03.1999 und vgl. Luckhardt, Norbert: Büchse der Pandora, in: c´t Magazin für Computertechnik, 8/99, S. 17.

36 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 216 f.

gen.[37] Das Fehlen sicherheitsrelevanter organisatorischer Vorgaben, z. B. Zutrittsbeschränkungen und Berechtigungskonzepte, lückenhafte Schulung von Mitarbeitern, menschliches Versagen, mangelndes Sicherheitsbewußtsein, Unkenntnis über die potentiellen Angreifer, aus Zeitdruck nicht ausreichend getestete Software- und Hardware-Komponenten etc. produzieren weitere Sicherheitslücken im organisatorischen Umfeld einer Web Site, auf die in Kapitel 3.2 näher eingegangen wird.

Der Vollständigkeit halber muß neben den o. g. Bedrohungen für eine Web Site auch die Kategorie zufälliger Gefahren wie Feuer, Wasser, Blitzschlag etc. („höhere Gewalt“) erwähnt werden, die sich auf den Betrieb einer Web Site negativ auswirken können. Im weiteren Verlauf der vorliegenden Arbeit werden diese Gefahren außen vorgelassen, da sie für IT-Systeme im allgemeinen bestehen und keine spezifische Bedrohung für eine unternehmerische Web Site darstellen.

3.2 Organisatorisch begründete Bedrohungen

3.2.1 Potentielle Angreifer

Informationen über die möglichen Angreifer auf eine Web Site können wichtige Anhaltspunkte für die Dimensionierung eines Sicherheitssystems liefern. Unter „Hackern“ und „Crackern“ werden allgemein alle Personen zusammengefaßt, die versuchen, sich unrechtmäßig Zugang zu fremden Computersystemen zu verschaffen. Dabei bestand die „Hacker-Gemeinde“ zu Anfang der achtziger Jahre hauptsächlich aus Jugendlichen und Studenten, die in ihrer Freizeit die Netzzugänge und Computer von Schulen und Universitäten nutzten. Ihre Motivation ist oftmals reine Neugier, Spieltrieb oder der Drang nach Selbstbestätigung. Für sie stellt das Einbrechen in fremde Computersysteme lediglich eine spielerische Herausforderung dar, und sie richten oft nur geringen Schaden an. Zu dieser Art von Hackern gehören auch diejenigen aus der Computer-Untergrundszene, die ihre Ursprünge in der „Phone-Phreak“-Bewegung der sechziger und siebziger Jahre in den USA haben.[38] Sie sind organisiert, tauschen ihre Erfahrungen über „Hacker-Bulletin-Board-Systeme“ aus und rechtfertigen ihre Taten mit einer sogenannten „Hacker-Ethik“. Eines der bekanntesten Beispiele für eine solche organisierte Hacker-Gemeinschaft ist der Chaos Computer Club (CCC).[39]

Zu den soeben beschriebenen traditionellen Hackern gesellen sich zunehmend Personen aus dem Bereich der organisierten Kriminalität. Neben der Abwicklung von verdeckter Kommunikation über das Internet stehen für diese Personen alle Arten von Transaktionen mit finanziellen Auswirkungen im Mittelpunkt des Interesses.

Seit dem Zusammenbruch des Ostblocks und dem (vermeintlichen) Ende des kalten Krieges Anfang der neunziger Jahre treten auch staatliche Geheimdienste verstärkt als potentielle Angreifer auf. Viele Geheimdienste haben ihr Betätigungsfeld in die Industriespionage verlegt,

37 Vgl. Persson, Christian: Datendiebstahl mit Internet Explorer 4, Online im Internet: http://www.heise.de/newsticker/data/cp-16.10.97-000/, 16.10.1997 und vgl. Kossel, Axel: Ein waches Auge, in: c´t Magazin für Computertechnik, 3/99, S. 142.

38 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 37 f.

39 Vgl. o. V.: Chaos Computer Club, Online im Internet: http://www.ccc.de/, 29.05.1999.

weil sie ihren ursprünglichen Tätigkeitsbereich verloren haben.[40] Ein Beispiel für einen ebensolchen zweckentfremdeten Einsatz ist das ECHELON-System der USA[41] und Rußlands SORM 2.[42]

Die größte Bedrohung für eine Web Site und die IT-Sicherheit eines Unternehmens sind aber nicht Hacker oder Spione, sondern die Mitarbeiter der Unternehmen selbst.[43] Sei es nun unbeabsichtigt, aus Frustration oder aus Rache am Unternehmen, können Mitarbeiter einen erheblichen Schaden verursachen. Hier seien nur das Einschleusen von Viren und das Stehlen von Daten oder auch das „Social Engineering“ (siehe dazu Kapitel 3.2.2) erwähnt. Zu den o. g. Aspekten kommen weitere Sicherheitsprobleme bei der Tele- und Heimarbeit hinzu, wie z. B. die Absicherung der Einwahlverbindungen oder die physikalischen und technischen Sicherheitsvorkehrungen, die in einem Privathaushalt nur bedingt zu gewährleisten sind.

3.2.2 Mangelndes Sicherheitsbewußtsein

Für die meisten sicherheitsrelevanten Vorfälle in Zusammenhang mit einer Web Site sind die Mitarbeiter des Unternehmens selbst verantwortlich. Dies ist oftmals auf ein mangelndes Sicherheitsbewußtsein unter den Mitarbeitern und in den Unternehmen allgemein zurückzuführen.[44] Dem mangelnden Sicherheitsbewußtsein liegt eine Reihe von Ursachen zugrunde. Es entstehen z. B. Wissenslücken und menschliches Versagen durch die schnellen und immer kürzeren Technolgiezyklen. Es ist für Mitarbeiter einer DV-Abteilung und Systemverwalter u. a. aus Zeitgründen nicht mehr möglich, mit allen Details von Betriebssystemen und Protokollen vertraut zu sein. So befinden sich Installationen häufig noch in einem „unsicheren“ initialen Zustand, wobei z. B. noch Standardbenutzerkonten ohne Paßwörter aktiv sind.[45]

Das Fehlen von Sicherheitsbeauftragten sowie mangelnde Fortbildungsaktivitäten zeigen Fehler in der Unternehmensorganisation auf, die in Kapitel 3.2.3 näher erläutert werden. Es ist oft ohne technische Mittel sehr einfach für Hacker, sich unberechtigt Zugang zu Computersystemen zu verschaffen. Eine manipulierte eMail oder ein Zettel mit Paßworten an einem Monitor oder einer Tastatur können für einen Hacker schon ausreichen, um Zugang zu einem System zu bekommen, das auf technischer Seite mit den raffiniertesten Sicherheitsmechanismen ausgestattet ist.[46] Es werden auch oft von Personen, die sich als „Techniker“ oder „Mitarbeiter der DV-Abteilung“ ausgeben, telefonisch Paßworte in Erfahrung gebracht. Diese Methode ist weiter verbreitet und wesentlich gefährlicher als allgemein angenommen wird. Sie wird in der Fachliteratur als „Social Engineering“ oder auch „Social Hacking“ bezeich-

40 Vgl. Krempel, Stefan; Schmidt, Michael; Kuri, Jürgen: Lange Ohren, a. a. O., S. 175 f.

41 Vgl. Ruhman, Ingo; Schulzki-Haddouti, Christinae: Abhördschungel, in: c´t Magazin für Computertechnik, 24/98, S. 90.

42 Vgl. Rötzer, Florian: SORM 2, Online im Internet: http://www.heise.de/tp/deutsch/inhalt/te/1923/1..html, 21.02.1999.

43 Vgl. Fill, Christian: IT-Security; Zwischen Panik und Perfektion, in: Information Week,. 19/1998, S. 39 f.

44 Vgl. Görtz, Horst; Stolp, Jutta: Informationssicherheit in Unternehmen, 1. Aufl., Bonn, Reading , Mass.: Addison-Wesley-Longman, 1999, S. 23.

45 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 118.

46 Vgl. Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet, a. a. O., S. 193.

net.[47] Social Engineering bedeutet, daß eine unbekannte Person unter Angabe einer falschen und in der Regel vertrauenswürdigen Identität sowie unter Angabe von sehr wichtig erscheinenden Gründen Auskünfte verlangt, die eigentlich nicht gegeben werden dürften. Im Falle von Netzwerken können dies Zugangsnummern, Accountnummern, User-IDs und Paßwörter sein. Es sollte den Anwendern verständlich gemacht werden, daß solche Informationen nur an Personen gegeben werden dürfen, deren Berechtigung zum Empfang vorher eindeutig nachgeprüft wurde.

Fehlerhafte und nicht ausreichend getestete Software stellt ein weiteres Problem von WSS dar. Es ist oft schon allein aus wirtschaftlichen Gründen und im Hinblick auf die Dynamik des Marktes nicht möglich, Software solange zu testen, bis ein fehlerfreies Funktionieren in jedem Betriebszustand gewährleistet werden kann. Erst seit Mitte der neunziger Jahre wächst das Bewußtsein für Sicherheitsmechanismen in Internet-Protokollen und Applikationen aufgrund der immer stärkeren Kommerzialisierung des Internets.

Was das Hardware-Design angeht, werden in vielen, vor allem kleinen und mittleren Betrieben immer noch grobe Fehler gemacht. So sind physikalische Netzwerkkomponenten, wie Router, Hubs und Verkabelung, für jedermann frei zugänglich und ermöglichen damit auf einfachstem Weg Sabotage und Spionage.

Eine Forderung, die aus den o. g. Aspekten entsteht, ist, daß Sicherheitsmaßnahmen in übergeordnete Prozesse integriert werden müssen.[48] Das bedeutet, daß es genaue Richtlinien geben muß, wie bei einem sicherheitsrelevanten Vorfall vorgegangen werden soll und wer zu informieren ist.

3.2.3 Organisatorische Insuffizienz

Der in den Kapiteln 3.2.1 und 3.2.2 dargestellte Problemhintergrund konkretisiert sich in fehlenden oder mangelhaften organisatorischen Vorgaben für die tägliche Praxis zur Planung, Steuerung, Durchführung und Kontrolle erforderlicher Sicherheitsmaßnahmen. Folgende offene Liste umreißt ein weites Feld unternehmensindividueller, typischer organisatorischer Fehlleistungen:[49]

1. Fehlende oder unzureichende „Alarmpläne“
2. Unzureichende Verbreitung und Kenntnis von „Alarmplänen“
3. Fehlende, ungeeignete, inkompatible Betriebsmittel
4. Fehlende oder unzureichende „Wartungspläne“
5. Unbefugter Zutritt zu schutzbedürftigen Räumen
6. Unzureichende und inkonsistente Berechtigungskonzepte
7. Unkontrollierter Einsatz von Betriebsmitteln
8. Mangelhafte Anpassung an Veränderungen der IT-Infrastruktur
9. Konzeptionslose Aufbewahrung von Datenträgern

47 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 81 f. und vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 37, 199, 299.

48 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 119.

49 Vgl. o. V.: Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch 98, CD-ROM, Bonn, 1998, Teil 1, Kapitel 3.1, S. 1.

Um diese vorgenannten Mängel in den Griff zu bekommen, ist es notwendig, ein kompetentes und konsistentes „Sicherheitsmanagement“ im Unternehmen zu etablieren. Der Begriff „Management“ ist dabei „personell“ und „funktionell“ zu verstehen: Wer tut was und in welcher Reihenfolge? Dieses Sicherheitsmanagement stellt primär auf die organisatorischen Maßnahmen (siehe Kapitel 4.4) ab, die dann durch technische Maßnahmen (siehe Kapitel 4.5) ausgekleidet werden müssen. Die vorliegende Arbeit soll hier durch einen Konzeptvorschlag Abhilfe schaffen, indem organisatorische und technische Maßnahmen konsistent im Sinne eines Sicherheitsmanagements für eine Web Site gebündelt werden.

3.3 Technisch begründete Bedrohungen

3.3.1 Viren, Würmer und Trojanische Pferde

Durch die weltweite Vernetzung von Computern mit der Internet-Technologie haben sich Computerviren wieder zu einer großen Bedrohung für die Sicherheit in unternehmensinternen Netzwerken entwickelt. In den achtziger Jahren verbreiteten sich Viren hauptsächlich durch den Austausch von Datenträgern. Mit der weltweiten Vernetzung stehen ihnen jedoch erheblich erweiterte Möglichkeiten zur Verbreitung offen. Gerade im eBusiness stellen Viren eine große Gefährdung dar. Durch ihr Angebot von Waren und Dienstleistungen über das WWW handeln sich Unternehmen 15 Prozent mehr Viren ein als Mitbewerber, die noch nicht mit einer Web Site auf dem elektronischen Marktplatz präsent sind.[50]

Folgende Formen von Viren sind zu unterscheiden:

- Boot-Viren
- Programm-Viren
- Stealth-Viren
- Daten-Viren
- Würmer
- System- (Cluster-)Viren
- Polymorphe Viren
- Retro-Viren
- Trojanische Pferde

Bis auf die letzten beiden Formen ist das Ziel der Viren, sich über möglichst viele Systeme zu verbreiten; sie werden entweder zu einem bestimmten Zeitpunkt aktiv, um Daten zu löschen und zu beschädigen oder sie machen einfach nur in Form eines „Scherzes“ auf sich selbst aufmerksam. Unter einem Scherz ist dabei z. B. das Anzeigen eines veränderten Bildschirmhintergrundes auf dem infizierten System zu verstehen.

Würmer traten zum erstenmal im November 1988 in Erscheinung. Robert Tappan Morris jr., Student der Cornell University, legte schätzungsweise 2000 bis 6000 Internet-Systeme lahm; der dabei entstandene Schaden wurde auf $ 97 Millionen geschätzt. Der tatsächlich entstandene Schaden liegt möglicherweise sehr viel höher, da viele betroffene Firmen keine Angaben machen wollten. Robert Tappan Morris jr. hatte ein Programm geschrieben, welches automatisiert in Computersysteme einbrach, indem es bekannte Schwachstellen in Netzwerksoftware und Vertrauensbeziehungen zwischen Rechnern ausnutzte.[51] Vertrauensbeziehungen zwi-

50 Vgl. Afif, Noelani Maria; Fill, Christian: Sicherheit zahlt sich aus, in: Informationweek, 11/99, S. 18.

51 Vgl. Freiss, Martin: SATAN: Sicherheitsmängel erkennen und beheben, 1. Aufl., Bonn: O´Reilley, Internat. Thomson-Verl., 1996, S. ix.

schen Rechnern autorisieren den Zugriff anhand von Rechnernamen. Dieser Vorfall ist als der „Internet Wurm“[52] bekannt geworden und schärfte das Bewußtsein für Sicherheit im Internet nachhaltig. Im Dezember 1988 wurde das Computer-Emergency-Response-Team/Coordination-Center (CERT/CC) durch die DARPA ins Leben gerufen und setzt sich seitdem mit Sicherheitsproblemen wie dem „Internet Wurm“ auseinander.[53]

Trojanische Pferde, oder auch einfach nur „Trojaner“ genannt, sind eine Virensonderform, die sich auf den infizierten Systemen nicht vervielfältigen, sondern dort einer bestimmten Aufgabe nachgehen. Trojaner können per eMail-Attachement, CD-ROM, per Download oder auf Disketten verbreitet werden und aktivieren/installieren sich allein schon durch „Anklic??ken“. Die meisten Trojaner haben z. B. die Aufgabe, Tastatureingaben zu protokollieren, sie an einen bestimmten Empfänger über das Internet zu senden und so z. B. Paßwörter auszuspionieren, auch wenn diese nicht lokal gespeichert wurden.[54] Trojaner können durch den Benutzer in den meisten Fällen nicht erkannt werden, weil sich in der Regel keine Symptome der Infizierung zeitigen. Viele Trojaner sind sogar in der Lage, sich selbst zu löschen, nachdem sie ihre Aufgabe erfüllt haben und das befallene System damit wieder in den Zustand vor der Infizierung zurück zu versetzen. Populäre Beispiele für solche Trojaner sind z. B. „BackOrifice“ und „Netbus“. Sie ermöglichen das komplette Fernsteuern eines fremden PCs.[55] Die Trojaner stellen den gefährlichsten Virentyp dar, da sie Systeme nicht „nur“ beschädigen oder lahmlegen, sondern sicherheitsrelevante Informationen ausspähen. Sie können evtl. sogar die Signatur und Verschlüsselung von Daten aushebeln.[56]

3.3.2 Kommunikationsprotokolle

Das Internet-Protokoll TCP/IP (Transport Control Protocol/Internet Protocol) hat sich seit den neunziger Jahren als Quasi-Industriestandard für lokale Netze durchgesetzt und verdrängt ältere, häufig proprietäre Protokolle, wie z. B. SNA, IPX, DECnet oder Appletalk.[57] Da bei der Entwicklung des TCP/IP-Protokolls in den siebziger Jahren seine spätere kommerzielle Nutzung nicht vorhersehbar war, sind wegen seiner systemimmanenten Mängel, wie z. B. zu kleiner Adreßraum, fehlende Möglichkeiten zur Priorisierung von Echtzeitdaten und fehlende Mechanismen zu Verschlüsselung und Authentifikation, immer wieder Angriffe gegen Web Sites auf Basis der Internet-Protokolle bekannt geworden.[58] Die meisten Attacken gegen eine Web Site und die darunter liegende IT-Infrastruktur setzen beim Angreifer ein fundiertes

52 Vgl. Kossakowski, Klaus-Peter: Der Intenet-Wurm, Klassifikation und Abwehr von Computer-Würmern in Netzwerken, DFN-CERT Online-Tutorial, Online im Internet http://www.cert.dfn.de/tutorial/wuermer/kap222.html, 06.06.1999.

53 Vgl. Siyan, Karanjit; Hare, Chris: Internet Firewalls & Netzwerksicherheit, 1. Aufl., Haar bei München: SAMS, 1995, S. 165 und vgl. o. V.: DFN-CERT Hompage, Online im Internet: http://www.cert.dfn.de/, 06.06.1999.

54 Vgl. Luckhardt, Norbert: Trojaner sendet nach China, in: c´t Magazin für Computertechnik, 3/99, S. 21.

55 Vgl. Kossel, Axel: Ein waches Auge, a. a. O., S. 144.

56 Vgl. Kossel, Axel: Ein waches Auge, a. a. O., S. 144.

57 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 175.

58 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 175.

technisches Verständnis der Kommunikationsprotokolle voraus.[59] Nachfolgend werden nur einige Möglichkeiten aufgezählt, wie Angriffe auf Basis von Transport- und Anwendungsprotokollen erfolgen können.

ICMP-Angriffe
Das Internet Control Message Protocol (ICMP) ermöglicht es, störungsfreie Routen zwischen Kommunikationspartnern zu ermitteln oder Verbindungen schlechter Qualität zu beenden. Es kann dazu benutzt werden, alle bestehenden Verbindungen zwischen zwei Rechnern zu unterbrechen oder Pakete umzuleiten.[60]

Internet-Routing-Angriffe
Über das Routing Information Protocol (RIP) besteht die Möglichkeit, auf das Routing von TCP/IP-Paketen Einfluß zu nehmen. Es können ebenfalls TCP/IP-Pakete abgefangen oder umgeleitet werden.[61]

Mail-Spoofing
Das Simple Mail Transport Protocol (SMTP) ist so einfach gehalten, daß Hacker die Befehle für die Protokolldateneinheit (PDU) selbst eingeben können.[62] Diese interpretiert die SMTP-Befehle innerhalb eines üblichen eMail-Headers und kann so manipuliert werden, daß der eMail-Daemon[63] einem Hacker z. B. die Paßwortdatei des Systems schickt.

Name- und Adress-Spoofing
Durch die Fälschung von Quelladreßauthentifikationen (Name- und Adress-Spoofing[64]) können übliche Sicherheitsvorkehrungen, wie z. B. die Anmeldung am Netzwerk (Login), umgangen werden. Viele TCP/IP-Verbindungen zwischen Rechnern kommen dadurch zustande, daß den Hosts Namen oder IP-Adressen von anderen vertrauenswürdigen Hosts durch Vorgaben vom Systemverwalter bekannt sind (Vertrauensbeziehungen). Hosts sind allgemein Rechner im Netz, die anderen Rechnern Dienste zur Verfügung stellen. Wenn es einem Hacker gelingt, die TCP-Pakete, die zwischen zwei über das Internet verbundene Hosts gesendet werden, zu überwachen, kann er diese Pakete entschlüsseln. Die Verbindung zu einem der Kommunikationspartner kann daraufhin unterbrochen werden, und der Rechner des Hackers kann sich als der vertrauenswürdige Host ausgeben. Für den „neuen“ vertrauenswürdigen Host ist dann keine erneute Authentifikation über ein Login mehr nötig. Es werden damit auch alle Rechte vererbt, die der ursprüngliche Client auf dem entfernten Host hatte. Es gibt verschiedene Arten, dies zu bewerkstelligen. Beim Adress-Spoofing wird dem angegriffenen System eine andere Absenderadresse als die eigentlich richtige Absenderadresse vorgetäuscht. Der Hacker hat über die TCP-Pakete die Absenderadresse eines vertrauenswürdigen Hosts ermittelt und gibt sich selbst als der eigentliche Absender aus. Das Name-Spoofing verwendet im

59 Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 59.

60 Vgl. Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet, a. a. O., S. 29.

61 Vgl. Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet, a. a. O., S. 30.

62 Vgl. Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet, a. a. O., S. 35.

63 Ein Daemon ist ein Programm, welches unter Unix immer wiederkehrende Aufgaben (Drucken, Datensicherung, Netzwerkdienste) im Hintergrund abarbeitet.

64 Engl. für Parodieren, Verballhornen.

Gegensatz zum Adress-Spoofing den vertrauenswürdigen Namen eines Rechners, um Zugang zum angegriffenen System zu erlangen. Der TCP-Sequenznummernangriff ist eine Technik, bei der die Sequenznummern, die zu jedem TCP-Paket gehören, vorhergesagt werden, um einem auf Antwort wartenden Server vorzutäuschen, der eigentliche Client zu sein, mit dem die Verbindung ursprünglich aufgebaut wurde.

DNS-Angriffe
Das Domain Name System (DNS) dient der Zuordnung von Rechnernamen zu den entsprechenden IP-Adressen. Es versendet an jeden Rechner im Netz eine Liste mit den Namen von Systemen, welche für Hacker wiederum nützlich sein können, um interessante Angriffsziele auszuspähen. An den Netzwerknamen von Computern kann ihre Funktionalität innerhalb eines Netzwerkes erkennbar sein.[65] Eine weitere Möglichkeit, den DNS-Dienst für Angriffe zu benutzen, ist das DNS-Spoofing, welches ähnlich abläuft wie das Name- und Adress-Spoofing.[66] Der Angreifer versucht dabei, seinen eigenen Rechner als vertrauenswürdigen Host in die DNS-Tabellen des DNS-Servers einzutragen.

3.3.3 Schwächen in Netzwerkbetriebssystemen

Weitere Angriffspunkte sind Fehler in Konfiguration und Software von Betriebssystemen. Diese Fehler können sich Angreifer zunutze machen.

Paßwörter stellen die übliche Zugangskontrolle zu einem Computersystem dar. Deshalb liegt es für einen Hacker nahe, sich ein gültiges Paßwort zu beschaffen. Die meisten Rechner im Internet werden mit dem Betriebssystem Unix betrieben. Paßworte werden auf Unix-Systemen in einer Paßwortdatei abgelegt. Diese ist somit das primäre Ziel eines Hackers. In der Vergangenheit waren Paßworte häufig nicht durch Verschlüsselung geschützt, sondern wurden unverschlüsselt übertragen oder im Klartext in einer Paßwortdatei abgelegt.[67] Auf Unix-Systemen liegt die Paßwortdatei im Verzeichnis „/etc“ und heißt „passwd“. Auf vielen FTP-Servern ist sie frei zugänglich. Sobald ein Angreifer im Besitz einer Paßwortdatei ist, kann er sie auf seinem eigenen System verwenden, um über Paßwortlisten (Dictionary Attack) gültige Paßworte zu ermitteln. Auf einem System mit lediglich 16 Benutzern ist mit einer Wahrscheinlichkeit von 99 Prozent ein schwaches Paßwort vorhanden.[68] Schwache Paßworte kommen aus verschiedenen Gründen zustande. Zum einen beträgt die übliche Länge von Paßworten sechs bis acht Zeichen. Zum anderen sind für die in Paßworten vorkommenden Zeichen die Wahrscheinlichkeiten nicht alle gleich hoch. Kontrollzeichen, Zahlen und Großbuchstaben werden häufig vermieden. Diese Einschränkungen erleichtern das Ermitteln von Paßworten für ausgereifte Entschlüsselungsalgorithmen erheblich.

65 Vgl. Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet, a. a. O., S. 198.

66 Vgl. Mraz, Viktor; Weidner, Klaus: Falsch verbunden – Gefahr durch DNS-Spoofing, in: c´t – Magazin für Computertechnik, 10/1997, S. 286 ff.

67 Vgl. Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet, a. a. O., S. 191 und vgl. Siyan, Karanjit; Hare, Chris: Internet Firewalls & Netzwerksicherheit, a. a. O., S. 86 ff. und vgl. Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, a. a. O., S. 10.

68 Vgl. Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet, a. a. O., S. 13.

Die Qualität eines Paßwortes läßt sich leicht verbessern, in dem man z. B. als Paßwort die Anfangsbuchstaben von ganzen, leicht einprägsamen Sätzen in Kombination mit Groß-, Kleinschreibung und Zahlen verwendet. Ein solches Paßwort ist wesentlich schwieriger zu knacken als beispielsweise die Vornamen oder Geburtsdaten von Familienangehörigen. Benutzer sollten zusätzlich in regelmäßigen Intervallen ihre Paßwörter freiwillig ändern oder durch entsprechende Einstellungen vom Systemverwalter dazu gezwungen werden.[69] Viele Benutzer wählen auf verschiedenen Systemen dasselbe Paßwort, durch das sich ein Hacker gleichzeitig zu mehreren Rechnern Zugang verschaffen kann, wenn er an einem Rechner an das Paßwort gelangen konnte.

Einen weiteren Aspekt stellen Dienstprogramme von Betriebssystemen dar, die dem Angreifer das Ausspionieren von Informationen für ein späteres Social Engineering ermöglichen. Durch den Anschluß eines Netzwerkes an das Internet werden Informationen für Außenstehende zugänglich gemacht, die es einem Angreifer ermöglichen, sich Hintergrundwissen über Strukturen innerhalb eines Netzwerkes anzueignen. Ein Beispiel hierfür ist der Finger-Befehl auf Unix-Systemen. Steht auf einem Host der Finger-Befehl zur Verfügung, kann ein Angreifer je nach der Konfiguration des Finger-Daemons, detaillierte Informationen über Namen, Adressen und Telefonnummern von Mitarbeitern abrufen.

Denial-of-Service-Angriffe zielen auf Fehler in Betriebssystemsoftware und Betriebssystemdiensten ab. Dabei steht nicht das Ausspähen oder der Zugriff auf fremde Rechner im Vordergrund, sondern einzig und allein das Lahmlegen derselben. Mail-Server können mit Mail überflutet und FTP-Server durch Uploads überlastet werden. Diese Vorgänge werden als „Flooding“ bezeichnet. Auf einem FTP-Server ohne Beschränkungen des Incomming-Bereiches kann die Kapazität der lokalen Festplatte überschritten werden, so daß andere auf der Festplatte befindliche Daten, z. B. das Verzeichnis mit dem Betriebssystem, überschrieben werden und damit das ganze System unbrauchbar wird. Ebenso ist es durch sich ständig wiederholende eMails möglich, einen Mail-Server über seine Kapazitätsgrenze hinaus zu belasten. Durch diese ständige Belastung des Servers während eines Denial-of-Service-Angriffs werden auch andere Dienste, wie Client-Applikationen, die der Server zur Verfügung stellt, in Mitleidenschaft gezogen. Für diese steht nicht mehr genügend Rechenzeit zur Verfügung. Ein Angreifer muß sich also nicht unbedingt direkten Zugriff zum System verschaffen, um Schaden anzurichten.

3.3.4 World Wide Web, Active-X und Java

Wenn es um Sicherheit von WWW-Anwendungen geht, können drei Problemkreise ausgemacht werden: Web-Browser-Sicherheit, Transaktionssicherheit und Web-Server-Sicherheit.[70]

Zum Thema Web-Browser-Sicherheit verdeutlichen die in der Fachpresse diskutierten Nachrichten von neuen Sicherheitslücken in Web-Browsern, wie z. B. dem „Netscape Communicator“ und dem „Internet Explorer“ von Microsoft und die daraufhin immer wieder erschei-

69 Vgl. Siyan, Karanjit; Hare, Chris: Internet Firewalls & Netzwerksicherheit, a. a. O., S. 86 f.

70 Vgl. Ghosh, Anup K.: E-Commerce Security: Weak Links, Best Defenses, a. a. O., S. 21.

nenden Updates für diese Produkte, die Problematik von Web-Browser-Sicherheit.[71] Dabei werden in diesem Zusammenhang häufig Fehler in der Browser-Software und aktive Web-Inhalte, wie Active-X, Java und Cookies genannt.[72] Bietet ein Unternehmen seinen Mitarbeitern die Möglichkeit, mit Web-Browsern auf die Informationen des WWW zuzugreifen, setzt es sich einer Vielzahl von obskuren, aber sehr realen Gefahren aus.[73] Nachdem Active-X-Elemente oder JavaScript-Komponenten über das WWW geladen wurden, können sie auf dem betroffenen Rechner ausgeführt werden und evtl. Programme und Systemroutinen aufrufen, die z. B. die lokale Festplatte löschen.[74] Zusätzlich dazu geben die modernen Browser Angreifern aus dem WWW einfache Möglichkeiten für Social Engineering an die Hand. So ist es mit einem sehr einfachen JavaScript-Programm möglich, den Anwender z. B. zur Eingabe seines Paßwortes aufzufordern (siehe Abb. 6).

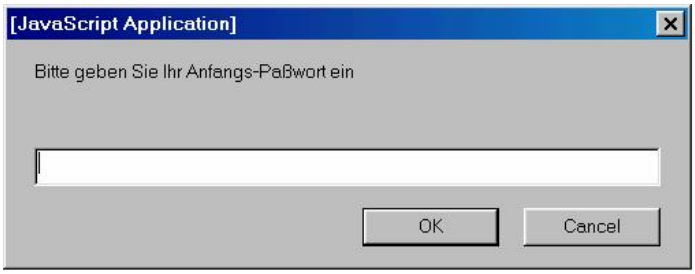

Abb. 6: Einfache JavaScript-Eingabeaufforderung

Das „offiziell“ aussehende Eingabefenster aus Abbildung 6 wurde nur mit den folgenden drei Zeilen JavaScript erzeugt[75]:

```
<script>
password = prompt ("Bitte geben Sie Ihr Anfangs-Paßwort ein","");
</script>
```

Um der Ausnutzung solcher Möglichkeiten vorzubeugen, hat der Internet Service Provider (ISP) America Online (AOL) die Benutzerschnittstelle seiner eMail-Software mit dem ständigen Hinweis versehen, daß der Kunde niemals von AOL-Mitarbeitern wegen Paßwortinformationen belästigt wird.[76] Andere Fehler in Browsern ermöglichen Angreifern, den Zwischenspeicher (Cache) oder die History-Datei des WWW-Browsers nach Inhalten, die von Interesse sein könnten, zu durchsuchen.[77]

71 Vgl. Luckhardt, Norbert: Frame-Fälscher im WWW, Online im Internet: http://www.heise.de/newsticker/data/nl-18.11.98-005, 04.06.1999 und Bager, Jo: IE-Sicherheitsloch ermöglicht Datenklau, Online im Internet: http://www.heise.de/newsticker/data/jo-12.10.98/, 04.06.1999.

72 Vgl. Ghosh, Anup K.: E-Commerce Security: Weak Links, Best Defenses, a. a. O., S. 31 f.

73 Vgl. Ghosh, Anup K.: E-Commerce Security: Weak Links, Best Defenses, a. a. O., S. 22.

74 Vgl. Schwickert, Axel C.; Dandl, Jörg: HTML, Java, ActiveX – Strukturen und Zusammenhänge, in: Arbeitspapiere WI, Nr. 6/1997, Hrsg.: Lehrstuhl für Allg. BWL und Wirtschaftsinformatik, Johannes Gutenberg-Universität: Mainz 1997, S. 10, 18 f.

75 Vgl. Garfinkel, Simon; Spafford, Gene: Web Security & Commerce, Köln et al.: O´Reilley & Associates, Inc. 1997, S. 35.

76 Vgl. Garfinkel, Simon; Spafford, Gene: Web Security & Commerce,a. a. O., S. 35.

77 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 200 f.

Transaktionssicherheit stellt besonders für eBusiness im Internet einen sehr wichtigen Punkt dar. In diesem Bereich bestehen wiederum Lücken, die sich Angreifer zunutze machen können. Der HTTP-Standard, als Grundlage für das WWW, bietet nur unzureichende Schutzmechanismen zur Authentifikation von Kunden und Partnern für geschäftliche Transaktionen.[78] Ohne Verschlüsselung und Authentifikation ist es Dritten mit geringem Aufwand möglich, auf der Ebene der in Kapitel 3.3.2 beschriebenen Kommunikationsprotokolle Informationen abzufangen, zu kopieren oder umzulenken. Zu diesen Informationen gehören vorrangig z. B. Kreditkartennummern und persönliche Kundendaten. Als Schutz gegen ebensolche Manipulationen wurden Erweiterungen und Ergänzungen wie Secure Socket Layer (SSL) und Secure HTTP (S-HTTP) für den HTTP-Standard entwickelt, die Verschlüsselung und Authentifikation von Transaktionen ermöglichen.[79]

Web-Server-Sicherheit stellt einen integralen Bestandteil von WSS dar, da die Web Server aus technischer Sicht die Zentren einer unternehmerischen Web Site bilden. Sie halten die unternehmerischen WWW-Seiten für die Benutzer vor und geben über bestimmte Programmschnittstellen, wie z. B. das Common Gateway Interface (CGI), Informationen an Datenbanken, Groupware-Anwendungen oder eCommerce-Systeme weiter.[80] Zwei bekannte Angriffsmethoden gegen Web Server sind URL- und CGI-Angriffe. Das CGI wird von einem Benutzer durch den Aufruf einer URL auf dem Web Server gestartet. Dort gibt das CGI die Daten, die über bestimmte Felder in einem Hypertext-Markup-Language-Dokument (HTML-Dokument) eingegeben werden, weiter an z. B. eine Datenbank. Die Ergebnisse der Datenbankabfrage werden vom Web Server zurück auf den Web Client des Anwenders geschickt.[81] Eine Gefahr besteht darin, daß jede Anfrage lokal auf dem Server abgearbeitet wird und damit bei einer sehr großen Anzahl von Anfragen die Ressourcen des Servers überlasten kann.[82] Weiterhin besteht bei vielen Implementationen von CGI die Möglichkeit, Betriebssystembefehle in HTML-Formulare einzugeben, die abgearbeitet werden, ohne vorher überprüft und herausgefiltert zu werden.[83] Eine weitere Form des Angriffs auf einen Web Server ist der HTML-Angriff. Dabei begibt sich der Angreifer ganz normal per Web Browser auf eine WWW-Seite. Er versucht anschließend, durch das Verändern des letzten Teils der angezeigten URL z. B. Skripte auszuführen, die sich in einem Unterverzeichnis des Web Servers befinden können. Solche Skripte liegen oftmals auf Web Servern bereit, um beispielsweise eMail an Kunden automatisiert zu verschicken. Ein Angreifer könnte die Skripte nun dahingehend manipulieren, daß der Web Server dazu veranlaßt wird, ihm die Datenbank mit den Benutzerkonten als eMail-Attachement zuzusenden.

78 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 73.

79 Vgl. Görtz, Horst; Stolp, Jutta: Informationssicherheit in Unternehmen, a. a. O., S. 74.

80 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 203 f.

81 Pohlmann, Norbert: Firewall-Systeme, Bonn et al.: Internat. Thomson Publishing 1997, S. 331.

82 Pohlmann, Norbert: Firewall-Systeme, a. a. O., S. 332.

83 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 206 f und Garfinkel, Simon; Spafford, Gene: Web Security & Commerce,a. a. O., S. 294.

4 Web Site Security – Ein Konzeptvorschlag

4.1 Organisatorische Maßnahmen

4.1.1 Risikoanalyse

Die Höhe des Risikos durch den Einsatz einer Web Site läßt sich nur unternehmensindividuell einschätzen. Durch systematische Risikoanalysen kann die Wahrscheinlichkeit des Eintritts von Sicherheitsvorfällen ermittelt werden. Unter relevanten Sicherheitsvorfällen wird eine Anzahl von Angriffen auf eine Web Site verstanden, bei denen im Gegensatz zu einem einzelnen Angriff ein Zusammenhang festgestellt werden kann. Diese Unterscheidung ist sinnvoll, wenn nicht jede falsche Paßworteingabe eines Mitarbeiters schon als Sicherheitsvorfall behandelt werden soll. Als Risiko wird laut DIN, VDE Norm 31000, das „Schadensausmaß bei Schadenseintritt“ (DIN 85) und die „erwartete Ereignishäufigkeit“ definiert.[84] Beide Faktoren sind in den letzten Jahren im gleichen Ausmaß angestiegen wie der verbreitete Einsatz von Internet-Technologien. In der Fachliteratur werden Risikoanalysen allgemein in vier Phasen aufgeteilt:[85]

1. Beschreibung des Analysebereichs
2. Erfassung des Risikos (Bedrohungsanalyse)
3. Bewertung des Risikos
4. Auswertung der Ergebnisse

Die Beschreibung des Analysebereichs wird wegen der Komplexität von EDV-Infrastrukturen nur für einen bestimmten Teilbereich vorgenommen. Im vorliegenden Fall für eine unternehmerische Web Site.

Die Erfassung des Risikos (Bedrohungsanalyse)[86] erfolgt durch die detaillierte Beschreibung aller bestehenden Risiken und deren Auswirkungen (siehe Kapitel 3). Dies kann durch Szenarioanalysen oder Simulationen geschehen. Bei Szenarioanalysen konstruiert eine Arbeitsgruppe mit Hilfe von Fallbeispielen hypothetische Sicherheitsvorfälle, während in Simulationsstudien der Analysebereich detailgetreu nachgebildet und die Einwirkungen von Gefahrenquellen simuliert werden. Im Gegensatz zu den Szenarioanalysen haben Simulationsstudien den Nachteil, daß sie sehr aufwendig sind und spezielle Software benötigen, z. B. ASIS von Siemens Nixdorf (SNI).[87]

Die Bewertung des Risikos kann sowohl qualitativ als auch quantitativ erfolgen.[88] Innerhalb einer quantitativen Risikobewertung werden den ermittelten Ereignissen kardinale Werte zu-

84 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 19.

85 Für eine detailliertere Darstellung von Risikoanalysen vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O. und o. V.: Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch 98, a. a. O.

86 Vgl. Weck, Gerhard; Gerbisch, Sandra Ines: Gefahren lauern überall: IT-Sicherheitskonzepte helfen Risiken mindern, a. a. O., S. 49.

87 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 20.

88 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 11.

geordnet. Es werden die Eintrittswahrscheinlichkeiten eines Sicherheitsvorfalls pro Jahr mit der zu erwartenden Schadenshöhe in Geldeinheiten multipliziert. So erhält man einen Wert für das Risiko eines bestimmten Sicherheitsvorfalls in Geldeinheiten pro Jahr. Als Beispiel soll der Einbruch in eine Web Site zum eCommerce mit anschließender Löschung der Kundendaten dienen: Es wird davon ausgegangen, daß ein solcher Einbruch wegen der Schwierigkeit der Durchführung nur einmal in zehn Jahren zu erwarten ist. Seine Eintrittswahrscheinlichkeit wird deshalb mit 10 Prozent bewertet. Der finanzielle Folgeschaden durch die Löschung der Kundendaten zusammen mit den Kosten für die Wiederherstellung derselben und die Behebung der Sicherheitslüc??ken wird mit 500 000 DM bewertet. Das ergibt zusammen ein Risiko von 50 000 DM/Jahr für diesen einen Sicherheitsvorfall (Risiko = 500 000 x 0,1 = 50 000 DM/Jahr).[89] Die bei der Erfassung des Risikos in Phase zwei ermittelten Sicherheitsvorfälle können jetzt anhand ihres Risikos in eine Reihenfolge gebracht werden. Bei der qualitativen Risikobewertung werden den Sicherheitsvorfällen im Gegensatz zur quantitativen Risikobewertung ordinale Werte zugeordnet. Die Web Site wird in Objekte zerlegt, denen mit Hilfe von Listen und Matrizen Risiken der Form „tragbar/untragbar“ und „wahrscheinlich/unwahrscheinlich“ zugeordnet werden.[90]

Die Auswertung der Ergebnisse ist der letzte Schritt der Risikoanalyse, bei dem einige weitere Probleme zu lösen sind. Die Eintrittswahrscheinlichkeiten von Sicherheitsvorfällen werden in der Praxis aus statistischen Tabellen abgeleitet, die jedoch Exaktheit oftmals nur vortäuschen. Eintrittswahrscheinlichkeiten können für ein spezielles Unternehmen durchaus verschieden sein. Als Faktoren, die Eintrittswahrscheinlichkeiten von Sicherheitsvorfällen im Umfeld von unternehmerischen Web Sites zum eCommerce beeinflussen, sollten berücksichtigt werden:[91]

- die eingesetzten Computer- und Netzwerksysteme,
- das Vorhandensein von Einwahlleitungen,
- bereits bestehende Sicherheitssysteme (Firewalls etc.),
- die Attraktivität des Unternehmens als Angriffsziel (Produkte, Wettbewerber etc.),
- geographische Lage,
- Unternehmensgröße und Anzahl der Mitarbeiter (Anonymität).

Zusätzliche Probleme bei einer Risikoanalyse ergeben sich daraus, daß Bedrohungen überschätzt oder übersehen werden könnten. Es ist weiterhin möglich, daß das Risiko überbewertet wird und daß deshalb, aus ökonomischer Sicht, ein zu hoher Aufwand zur WSS betrieben wird. Außerdem besteht immer die Gefahr, daß nur Symptome und nicht Ursachen von Sicherheitsvorfällen bekämpft werden.[92] Die Risikoanalyse stellt einen entscheidenden Beitrag zur Erstellung eines Sicherheitskonzeptes dar, das die Verringerung der Risiken für eine Web Site unter Berücksichtigung der Wirtschaftlichkeit beschreibt.

89 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 21.

90 Vgl. o. V.: Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch 98, a. a. O., Teil 1, Kapitel 2.2, S. 3 f.

91 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 26.

92 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 9.

Sicherheitsmaßnahmen werden in der Regel Kosten verursachen. Da eine annähernd hundertprozentige Lösung selbst mit unbegrenzten Mitteln nicht realisierbar ist, muß ein optimales Kosten-/Nutzenverhältnis von Sicherheitsmaßnahmen zur WSS angestrebt werden. Aufwand und Nutzen von Sicherheitsmaßnahmen müssen in einer ausgeglichenen Relation zueinander stehen und dabei das Restrisiko minimieren. Das jeweilige Kostenniveau der Schutzmaßnahmen ist aber branchenspezifisch unterschiedlich. Banken, Versicherungen und Finanzdienstleister haben typischerweise einen höheren Sicherheitsbedarf als der Betreiber eines Online Shops und werden deshalb bereit sein, mehr Aufwand zum Schutz ihrer Web Site zu betreiben. Wichtig ist bei der Dimensionierung der Sicherheitsmaßnahmen der Gesamtwert der zu schützenden Güter.

4.1.2 Sicherheitskonzept

Das Sicherheitskonzept für eine Web Site definiert die notwendigen Maßnahmen hinsichtlich Datensicherheit und Datenschutz. Das Sicherheitskonzept wird selbst als organisatorische Maßnahme verstanden; es muß speziell für eine Web Site systematisch erzeugt, dokumentiert und realisiert werden. Grundlage hierfür ist die (Ist-)Analyse der bestehenden organisatorischen und technischen Regelungen sowie der Computer- und Netzwerksysteme zusammen mit den Ergebnissen der Risikoanalyse. Die primäre Aufgabe des Sicherheitskonzepts ist es, die in der Risikoanalyse identifizierten Sicherheitslücken zu schließen.[93] Die unternehmensindividuellen Maßnahmen zur WSS können dabei aus allgemeinen Maßnahmenkatalogen zur IT-Sicherheit abgeleitet werden. Ein Beispiel dafür ist das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI).[94] Ein Sicherheitskonzept für eine WSS muß analog zu den allgemeinen Maßnahmen zur IT-Sicherheit mindestens Regelungen für folgende Punkte enthalten: [95]

- Infrastruktur
  - Physikalische Zutrittskontrolle und Überwachung
  - Schutz gegen physikalische Schäden
  - Stromversorgung/Klimatisierung
  - Aufstellung von Geräten
- Organisation
  - Organisatorische Regelungen, z. B. Stellen für Datenschutzbeauftragte schaffen
  - Planung und Systemauswahl
  - Überwachung/Kontrolle der Maßnahmendurchführung
  - Permanente Anpassung und Aktualisierung des Sicherheitskonzepts
- Personal
  - Maßnahmen bei Einstellung/Ausscheiden
  - Schulung/Bereitstellung geeigneten Personals

93 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 21.

94 Vgl. o. V.: Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch 98, Online im Internet: http://www.bsi.de/gshb/deutsch/menue.htm, 06.06.1999.

95 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 235.

- Hardware/Software
  - Hardware-Struktur/Betriebssystemfunktionen
  - Sicherheitsgrundfunktionen
  - Anwendungsspezifische Funktionen
- Kommunikation
  - Sicherung der Netzanbindung
  - Übertragungssicherung
  - Nutzung von Sicherheitsfunktionen der Systeme/Protokolle
- Notfallvorsorge
  - Datensicherungskonzept
  - Einsatz von Redundanz zur Erhöhung der Verfügbarkeit
  - Notfallplanung

Zusätzlich zu den organisatorischen und technischen Sicherheitsmaßnahmen ist auch eine Absicherung des Risikos über eine Versicherungsgesellschaft als Teil eines Sicherheitskonzepts zu prüfen.[96]

4.2 Technische Maßnahmen

4.2.1 Firewall-Systeme

Als eine technische Maßnahme zur Absicherung einer Web Site bieten sich Firewall-Systeme an. Ein Firewall ist die einzige Verbindung des lokalen Netzes zum weltweiten Internet. Es handelt sich dabei immer um eine Kombination aus Hard- und Software. Alle Datenpakete, die die Firewall passieren, werden von ihr nach bestimmten Regeln überprüft. Firewalls kontrollieren so den Datenverkehr zwischen dem Internet und dem angeschlossenen lokalen Netz (siehe Abb. 7).

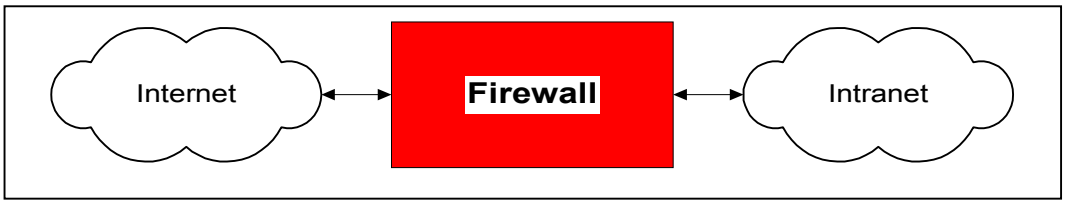

Abb. 7: Firewall

Firewall-Systeme finden seit Anfang der neunziger Jahre einen weit verbreiteten Einsatz in der unternehmerischen Praxis. Bei der Auswahl der geeigneten Firewall-Lösung muß beachtet werden, daß eine Firewall mehrere Anforderungen erfüllen soll. Sie muß zum einen die vorhandenen Netzzu- und -übergänge kontrollieren. Des weiteren muß eine Selektion der zuge-

96 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 21.

lassenen Netzwerkprotokolle möglich sein. Das Ausmaß der Protokollfunktionen (Audit) von Benutzeraktivitäten ist zusammen mit automatischen Alarmfunktionen ein dritter zu berücksichtigender Punkt. Diese Funktionen setzen bei bestimmten Ereignissen, wie z. B. dem unberechtigten Zugriffsversuch auf bestimmte Daten, eine eMail mit einer Vorfallsbeschreibung an den Administrator ab. Zusätzliche Funktionen wie Verschlüsselung und Virenerkennung sind ebenso zu beachten. Letztlich sind auch die Administrierbarkeit, die Flexibilität und der Preis der Firewall-Lösung zu prüfen.[97]

Als klassische Firewall-Komponenten werden in der Fachliteratur Paketfilter und Application-Level-Filter unterschieden. Eine neuere Form wird als Stateful-Inspection-Technik bezeichnet. Nachfolgend werden diese Firewall-Komponenten erläutert; eine Beschreibung der möglichen Positionierung der Firewall-Komponenten schließt sich daran an.

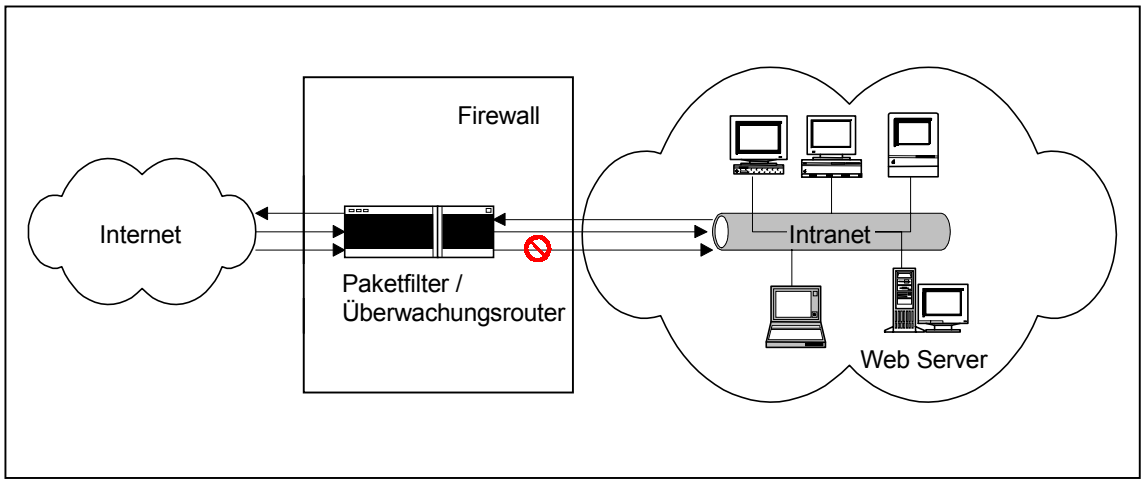

Abb. 8: Paketfilter

Paketfilter sind Programme, die entweder auf einer speziellen Hardware, einem Router, oder auf einem Computer, der als Router dient, installiert werden (siehe Abb. 8). Ein solcher Router mit Paketfilterung wird als Überwachungsrouter bezeichnet. Paketfilter kontollieren Datenpakete auf der Netzwerkschicht des OSI-Referenz-Modells. Sie analysieren die Header der ein- und/oder ausgehenden Datenpakete hinsichtlich ihrer Absender-/Empfängeradressen, der IP-Adressen und der Portnummern. Die Inhalte von IP-Paketen werden von Paketfiltern nicht analysiert.[98] Protokolle wie SMTP, FTP, UDP (User Datagram Protocol) und TCP/IP benutzen standardmäßig bestimmte Portnummern. SMTP (eMail) benutzt z. B. den Port 25.[99] Wenn man für eine Web Site die Benutzung von eMail erlauben will, müssen Pakete an den Port 25 des eMail-Servers der Web Site zugelassen werden. Ein Paketfilter muß so konfiguriert werden, daß er bestimmte Pakete anhand von Positiv-/Negativlisten durchläßt bzw. andere ablehnt. Zum Beispiel darf jeder Rechner auf die öffentliche Web Site eines Unternehmens

97 Vgl. Richter-Maierhofer, E.: Firewalls – Sicherheitsschleusen für das LAN, in: NT Journal, 5/1997, S. 88.

98 Vgl. Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, a. a. O., S. 152.

99 Vgl. Kuppinger, Martin; Bauer, Markus: Netzwerk & Intranet – Firewalls für Windows NT, Firewall-Konzepte, in: PC Professional, 8/1997, S. N 21 und vgl. Richter-Maierhofer, Ellen: Firewalls – Sicherheitsschleusen für das LAN, a. a. O., S. 88.

zugreifen, aber auf die Homepage des unternehmensinternen Intranets nur Rechner von innerhalb des Unternehmens. Ein solches Regelwerk kann genau festlegen, welche Protokolle für eine Web Site erlaubt sind und welche nicht.

Vorteile von Paketfiltern sind:

- Hoher Datendurchsatz[100]
- Ein Überwachungsrouter kann ein hinter ihm liegendes Netz vollständig schützen.
- Der Zugriff auf die Clients im Netz ist durch den Paketfilter einmal und eindeutig geregelt und muß nicht für jeden Client einzeln konfiguriert werden.
- Paketfilter sind auf den meisten handelsüblichen Routern schon werksseitig installiert und müssen deshalb nicht gesondert beschafft werden.[101]

Nachteile von Paketfiltern sind:

- Schwer bedienbare, inkonsistente Filterwerkzeuge, die eine manuelle Eingabe von Routingtabellen in Konfigurationsdateien erfordern, stehen der einfachen Formulierung von Filterregeln im Wege, z. B. in nichtkommerziellen Linux-Firewall-Systemen.
- Einige Betriebssystembefehle, wie die r-Befehle von Unix und die auf Remote Procedure Calls (RPC) basierenden Dienste (Network File System – NFS, Network Information System/Yellow Pages – NIS/YP), eignen sich aufgrund ihrer Konzeption nicht für Paketfilterung.
- Es ist nicht möglich, über Paketfilterung bestimmten Benutzern den Netzzugriff zu verwehren. Die IP-Pakete enthalten nur Informationen über den sendenden Host aber nicht über den Benutzer.[102]

Unter den Application-Level-Filtern werden Proxy-Dienste und Circuit-Level-Filter zusammengefaßt.[103] Application-Level-Filter arbeiten auf der Anwendungsschicht des OSI-Referenz-Modells.[104] Application-Level-Filter selektieren den Datenverkehr zwischen Internet-Client und Internet-Server anhand einer bestimmten Anwendung, z. B. Telnet. Sie sind in der Lage, den Zugriff eines Telnet-Programms auf einen SMTP-Server zu unterbinden.[105] Bei den Application-Level-Filtern steht demnach nicht das Protokoll im Vordergrund, sondern die Applikation, von der die Pakete erzeugt werden. Zu den Application-Level-Filtern gehören die Proxy-Dienste. Bei Proxy-Diensten (Stellvertreterdienste) handelt es sich um Programme, welche die Anfragen von internen Internet-Clients, z. B. Telnet-, eMail oder WWW-Brow-

100 Vgl. Richter-Maierhofer, Ellen: Firewalls – Sicherheitsschleusen für das LAN, a. a. O., S. 88.

101 Vgl. Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, a. a. O., S. 154 f.

102 Vgl. Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, a. a. O., S. 156.

103 Die Firewall-Terminologie ist in der Literatur hinsichtlich der Unterscheidung der Application-Level-Filter nicht einheitlich. Im weiteren werden die Begriffe Application-Level-Filter, Proxy-Dienste, Circuit-Level-Filter, Circuit-Level-Gateways und Application-Level-Gateways synonym verwendet vgl. Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, a. a. O., S. 69.

104 Weitere Informationen zum OSI-Refernz-Modell finden sich u. a. bei Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, a. a. O., S. 527 ff.

105 Vgl. Richter-Maierhofer, Ellen: Firewalls – Sicherheitsschleusen für das LAN, a. a.. O., S. 88.

sern, stellvertretend an netzwerkexterne Rechner weiterleiten. Die Verbindung zwischen zwei Rechnern kommt somit nicht direkt zustande, sondern wird vom Proxy-Dienst vermittelt. Dieser kann so überprüfen, ob die Programme wie z. B. FTP oder Telnet der Sicherheitspolitik des Web-Site-Betreibers entsprechend zugelassen sind oder nicht. Proxy-Dienste wurden entwickelt, um den Zugriff interner Benutzer auf das Internet zu beschränken. Ursprünglich waren sie nicht für den umgekehrten Weg konzipiert (siehe Abb. 9).

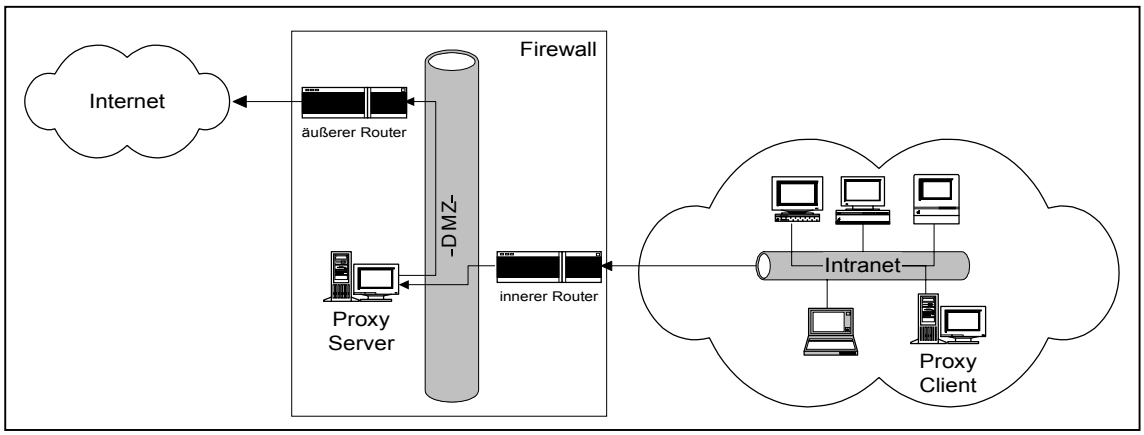

Abb. 9: Proxy-Dienste

Ein Proxy-Dienst besteht immer aus mindestens zwei Komponenten: dem Proxy-Server und dem Proxy Client.[106] Proxy Clients sind spezielle Versionen von normalen Client-Programmen, wie WWW-, Telnet- oder FTP Clients. Es können aber auch Standardversionen von Clients zum Einsatz kommen, die entsprechend dem eingesetzten Proxy-Dienst konfiguriert werden müssen. Der Proxy-Client schickt eine Anfrage, die an einen externen Server gerichtet ist, an den Proxy-Server. Dieser wertet die Anfrage aus und entscheidet über ihre Weiterleitung an den externen Server. Die Antwort des externen Servers läuft wiederum über den Proxy-Server. Auch auf diesem Weg entscheidet der Proxy-Server, ob die Antwort an den Client weitergeleitet wird.

Der Einsatz von Proxy-Diensten ist nur in einem Netzwerk mit einer einzigen Verbindung zum Internet über einen Dual-Homed-Host sinnvoll.[107] Bei einem Dual-Homed-Host handelt es sich um einen Gateway-Rechner mit zwei Netzwerkkarten (siehe Abb. 10). Eine der beiden Netzwerkkarten ist mit dem Internet verbunden, die andere mit dem internen Netzwerk. So ist gewährleistet, daß jedweder Verkehr durch den Gateway laufen muß. Auf dem Gateway werden Proxy-Dienste installiert. Sobald jedoch eine Verbindung mit externen Maschinen auch auf einem anderen Weg hergestellt werden kann, kann der Proxy-Dienst umgangen werden. Dies wird bei der Einrichtung von Internet-Firewalls häufig übersehen.[108]

106 Vgl. Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, a. a. O., S. 70.

107 Vgl. Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, a. a. O., S. 66.

108 Vgl. Strobel, Stefan: Nebeneingang – Firewalls nicht nur für den Internet-Anschluß, in: iX 10/98, S. 132.

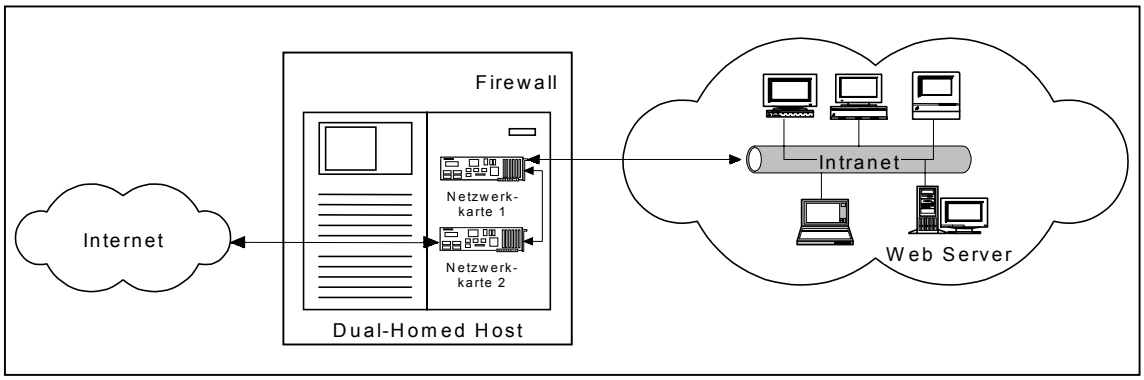

Abb. 10: Dual-Homed-Host

Ein Circuit-Level-Filter integriert Funktionalitäten von Paketfiltern und Proxy-Diensten. Datenpakete werden bei Circuit-Level-Filtern sowohl anhand der Serviceart als auch der Sender-/Empfängeradressen gefiltert.[109] Ein Vorzug der Application-Level-Filter ist ihre einfache Konfigurierbarkeit; sie haben jedoch gegenüber Paketfiltern den Nachteil, daß sie langsamer[110] arbeiten und in ihrer Protokollunterstützung weniger flexibel sind als Paketfilter.[111]

Eine neuere Firewall-Technologie stellt die Stateful-Inspection-Technik dar. Diese Technik wurde von der Firma Checkpoint für ihre Firewall-Produkte entwickelt. Die Stateful-Inspection-Technik stellt eine dynamische Paketfilterung zur Verfügung. Hierbei werden die Datenpakete zunächst mit der o. g. Paketfilterung untersucht. Der Inhalt der Datenpakete wird dann zur weiteren Analyse an die sogenannte „Inspect-Engine“ weitergegeben. Diese ist ein Teil der Firewall-Software und kann die Inhalte der Datenpakete nach verschiedenen potentiellen Gefahrenquellen wie Viren, falschen Authentifizierungen oder Tags für Java-Applets untersuchen und diese unerwünschten Inhalte gegebenenfalls entfernen. Zusätzlich zur Filterung der Pakete werden bei der Stateful-Inspection-Technik bestehende Verbindungen protokolliert und nach dem tatsächlichen Verbindungsende getrennt, so daß kein Name- oder Adress-Spoofing mehr möglich ist.[112]

Bei der Auswahl eines Firewall-Produktes zur WSS gilt es, die eingesetzten Betriebssysteme (Unix, Windows NT, Novell) und die Netzwerk-Hardware zu berücksichtigen. Ursprünglich war Firewall-Software eine Domäne von Unix-Systemen. Mit der zunehmenden Verbreitung von Windows NT im professionellen Netzwerkmanagement wurden vermehrt Produkte aus dem Unix-Bereich auf Windows NT portiert. Beispielhaft werden nachfolgend einige kommerzielle Produkte von bekannten Herstellern aufgeführt:[113]

- Cisco-Systems (Überwachungsrouter in Hardware)
- Altavista (Firewall mit Application-Level-Filter)

109 Vgl. Richter-Maierhofer, Ellen: Firewalls – Sicherheitsschleusen für das LAN, a. a.. O., S. 88.

110 Vgl. Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet, a. a. O., S. 135.

111 Vgl. Richter-Maierhofer, Ellen: Firewalls – Sicherheitsschleusen für das LAN, a. a.. O., S. 88.

112 Vgl. Richter-Maierhofer, Ellen: Firewalls – Sicherheitsschleusen für das LAN, a. a.. O., S. 88 und vgl. Kuppinger, Martin; Bauer, Markus: Netzwerk & Intranet – Firewalls für Windows NT, Firewall-Konzepte, a. a.. O., S. N 21.

113 Vgl. Kuppinger, Martin; Bauer, Markus: Netzwerk & Intranet – Firewalls für Windows NT, in: PC Professional, 8/1997, S. N 21 ff.

- Checkpoint (Firewall-1 mit Stateful-Inspection-Technik)
- Sun Microsystems (Solistice Firewall-1 mit Stateful-Inspection-Technik)
- Linux („kostenloses“ Betriebssystem mit diversen Firewall-Lösungen)

Für die Plazierung von Firewalls zum Schutz einer Web Site und eines betrieblichen Netzwerkes gibt es verschiedene Ansätze. Grundsätzlich gilt, daß Firewalls immer zwischen dem zu schützenden Objekt (Web Site, internes Netzwerk) und dem aus Sicht des Betreibers unsicheren Internet plaziert werden müssen. Ein Einsatz von mehreren Firewalls innerhalb eines Intranets zur Abschirmung unterschiedlicher Sicherheitsbereiche[114] ist ebenso denkbar. Innerhalb eines Unternehmens haben eben nicht alle Mitarbeiter Zugriff auf alle Daten. Es ist auch sinnvoll, besondere Teilbereiche, wie z. B. den Zugriff auf die Datenbank mit Kreditkarteninformationen bei einem Online Shop, nur dem Verwalter des Shops zu ermöglichen.

Weil unter einer Firewall nicht nur ein einzelnes Programm verstanden wird, sondern der Einsatz von einer oder mehreren mehrstufigen Firewall-Komponenten, gibt es die unterschiedlichsten Möglichkeiten für den Aufbau eines konsistenten Firewall-Konzepts. Im einfachsten Fall besteht eine Firewall lediglich aus einem Überwachungsrouter. Bringt man Paketfilter zusammen mit Application-Level-Filtern innerhalb eines Subnetzes zum Einsatz, spricht man von einem Dual-Screened-Subnet.[115] Unter einem Subnet wird ein Netzwerk innerhalb eines größeren Netzwerkes verstanden. Ein Maximum an Sicherheit ist aus der Kombination eines Dual-Screened-Subnet mit der Stateful-Inspection-Technik zu erreichen.[116]

Ein exponiertes Gateway mit Firewall-Komponenten bezeichnet man auch als Bastion Host.[117] Ein Bastion Host (siehe Abb. 11) verdient besondere Aufmerksamkeit, weil er die wichtigste Schnittstelle zwischen dem Unternehmensnetzwerk und dem Internet darstellt. Die Firewall-Komponenten auf dem Bastion Host entscheiden, welche Protokolle und Dienste zum internen Netzwerk durchgelassen und welche blockiert werden.[118]

Eine häufig verwendete Architektur zur Erhöhung der Sicherheit ist ein Grenznetz, welches zwischen zwei Routern liegt. Ein Grenznetz ist ein dem zu schützenden Unternehmensnetzwerk vorgelagertes Netz. Es wird auch als „Demilitarisierte Zone“ (DMZ) bezeichnet.[119] Gelingt einem Angreifer das Überwinden des ersten Filters (äußerer Router in Abb. 11), hat er nur Zugriff auf den Verkehr innerhalb des Grenznetzes und nicht auf das hinter dem zweiten Router (innerer Router in Abb. 11) liegende Netzwerk. In der Regel wird der Angreifer dann innerhalb der DMZ versuchen, die Sicherheitsmechanismen des Bastion Host[120] zu umgehen.

114 Vgl. Siyan, Karanjit; Hare, Chris: Internet Firewalls & Netzwerksicherheit, a. a. O., S. 76–79.

115 Vgl. Kuppinger, Martin; Bauer, Markus: Netzwerk & Intranet – Firewalls für Windows NT, Firewall-Konzepte, a. a.. O., S. N 21.

116 Vgl. Kuppinger, Martin; Bauer, Markus: Netzwerk & Intranet – Firewalls für Windows NT, Firewall-Konzepte, a. a.. O., S. N 21.

117 Vgl. Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet, a. a. O., S. 61 und vgl. auch Siyan, Karanjit; Hare, Chris: Internet Firewalls & Netzwerksicherheit, a. a. O., S. 309.

118 Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, a. a. O., S. 105.

119 Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, a. a. O., S. 66.

120 Amorroso, Edward; Sharp, Ronald: Intranet and Internet Firewall Strategies, in: PCWEEK, Emeryville California: Ziff-Davies Press 1996, S. 53.

Er ist damit innerhalb des Grenznetzes „gefangen“. Seine Aktivitäten dort können relativ einfach bemerkt werden.

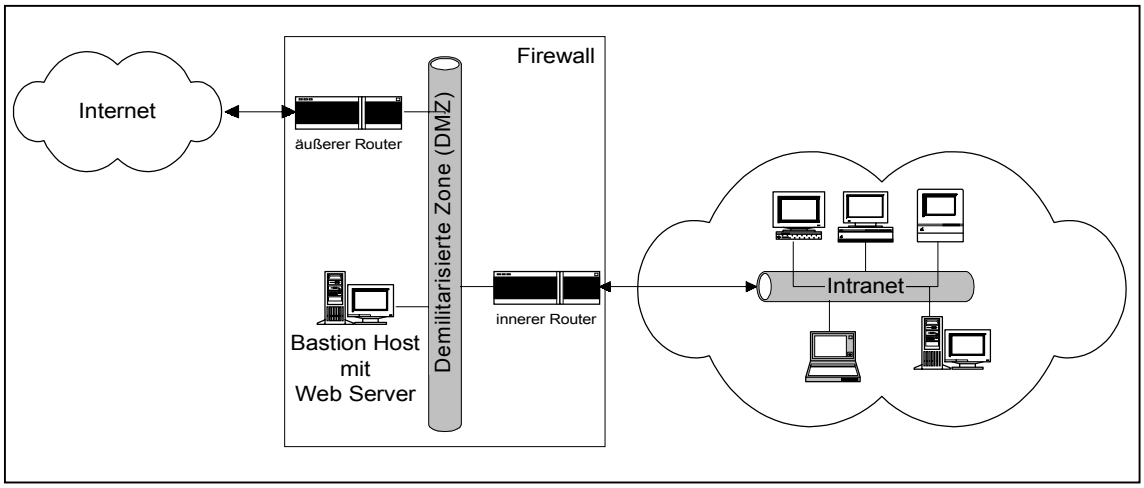

Abb. 11: Bastion Host

4.2.2 Intrusion-Detection-Systeme (IDS)

Betrachtet man eine Firewall als einen Wächter, der das Tor zu einer Web Site bewacht, ist ein Intrusion-Detection-System der Sicherheitsdienst, der den Netzwerkverkehr auf Auffälligkeiten hin untersucht.[121] Gerade weil davon ausgegangen wird, daß die eigenen Mitarbeiter für die meisten sicherheitsrelevanten Vorfälle in einem Netzwerk verantwortlich sind, erscheint es dabei sinnvoll, nicht nur die Schnittstellen zwischen Intra-, Extra- und Internet abzusichern, z. B. mit Firewalls, sondern auch die Aktivitäten innerhalb von Intra- und Extranet zu analysieren. Wenn man sich realiter damit abfinden muß, daß es trotz starker Firewalls immer wieder zu sicherheitsrelevanten Vorfällen kommt, ist es sinnvoll, sich mit ihrer schnellen Erkennung zu beschäftigen.[122]

IDS sind Initiatoren für die im Sicherheitskonzept festgelegten „Alarmpläne“. Sie können bei einem sicherheitsrelevanten Vorfall z. B. über Pager oder eMail Warnungen an den Sicherheitsbeauftragten verschicken.[123] IDS sind als zwei verschiedene Lösungen auf dem Markt, die sich gegenseitig ergänzen:

1. Netzwerk- oder signaturbasierte IDS
2. Host- oder expertensystembasierte IDS

Ein signaturbasiertes IDS untersucht die Datenströme innerhalb eines Netzwerkes nach Signaturen von bekannten Angriffsmethoden[124] ähnlich der Arbeitsweise eines Virenscanners.

121 Vgl. Hillmeister, Bernd: Intrusion Detection – Software-Tools spüren Einbrecher im Netz auf, in: Computer Zeitung, 18/99, S. 35.

122 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 299.

123 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 92.

124 Hillmeister, Bernd: Intrusion Detection – Software-Tools spüren Einbrecher im Netz auf, a. a. O., S. 35.

Dadurch lassen sich z. B. Lücken einem bestehenden Firewall-System aufdecken. Host-basierte IDS analysieren ebenso Datenströme, jedoch suchen sie nach auffälligen Abweichungen vom „normalen“ Netzwerkverkehr. Dies geschieht entweder regelbasiert oder über heuristische Analysen unter Zuhilfenahme von Expertensystemen. Regelbasiert bedeutet, daß dem IDS durch Regeln „beigebracht“ wird, was es als Angriff interpretieren und wann es Alarm auslösen soll. Eine Regel könnte z. B. lauten, daß immer Alarm ausgelöst wird, wenn jemand mehr als dreimal sein Paßwort falsch eingibt oder wenn ein Portscan über alle Ports eines Web-Servers stattfindet.[125] Der Nachteil ist, daß die Regeln immer manuell auf einen aktuellen Stand gebracht werden müssen. Dieses Manko kann ein expertensystembasiertes IDS (zum Teil) beseitigen. Das expertensystembasierte IDS muß vor seiner Aktivierung den Netzwerkverkehr analysieren und aus den ermittelten Informationen einen „Normalzustand erlernen“. Mit diesem Normalzustand als Grundlage können daraufhin Schwellenwerte definiert werden, bei deren Überschreitung das IDS Alarm auslöst.[126] Eine solche Überschreitung kann z. B. ein plötzliches Ansteigen der Aktivität des Web-Servers zu einer außergewöhnlichen Zeit sein. Oftmals werden gehackte Web Sites als illegale Lager für raubkopierte Software mißbraucht. Das führt naturgemäß zu ungewöhnlich hohem „Kundenverkehr“. Problematisch ist bei expertensystembasierten IDS jedoch die Ermittlung des Normalzustandes. Es muß selbstverständlich sichergestellt sein, daß bei der Analyse des Netzwerks noch alles „normal“ ist und nicht schon sicherheitsrelvante Aktivitäten im Gange sind.[127] IDS stellen eine optimale Ergänzung zu Firewalls bei der Implementation von WSS dar.

4.2.3 Virtuelle Private Netzwerke (VPN)

In den letzten Jahren hat sich in den Unternehmen die Erkenntnis durchgesetzt, daß die Internet-Protokoll-Familie zu weitaus mehr gut ist als nur zur Präsentation einer öffentlichen Web Site.[128] Damit Unternehmen das öffentliche Internet auch als sichere Kommunikationsplattform für ihre Kunden- und Partnerbeziehungen nutzen können, ist es notwendig, die technischen Designschwächen des Internets zu umgehen.[129] VPNs sollen die internen Kommunikationsprozesse nicht nur beschleunigen, sondern auch die Beziehungen zu Kunden und Lieferanten transparent machen.[130] Die Technik, Daten überall da zu verschlüsseln wo sie das Firmennetz verlassen und wieder zu entschlüsseln, wenn sie ihr Ziel erreicht haben, wird als Virtuelles Privates Netzwerk (VPN) bezeichnet.[131] VPNs stellen im Grunde nichts anderes dar, als die verschlüsselte und authentifizierte Kommunikation über öffentliche Netze (siehe Abb. 12).[132]

125 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 300.

126 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 300.

127 Vgl. Kyas, Othmar: Sicherheit im Internet, a. a. O., S. 300.

128 Vgl. o. V.: Internet-Technik ist kein Sicherheitsrisiko mehr, in: Computer Zeitung, 18/1999, S. 29.

129 Vgl. Amorroso, Edward; Sharp, Ronald: Intranet and Internet Firewall Strategies, a. a. O., S. 113.

130 Vgl. o. V.: Internet-Technik ist kein Sicherheitsrisiko mehr, a. a. O., S. 29.

131 Vgl. Schmeh, Klaus: Safer net: Kryptografie im Internet und Intranet, a. a. O., S. 17.

132 Vgl. Kuri, Jürgen: Privatissimo, in: c´t Magazin für Computertechnik, 4/1999, S. 190.

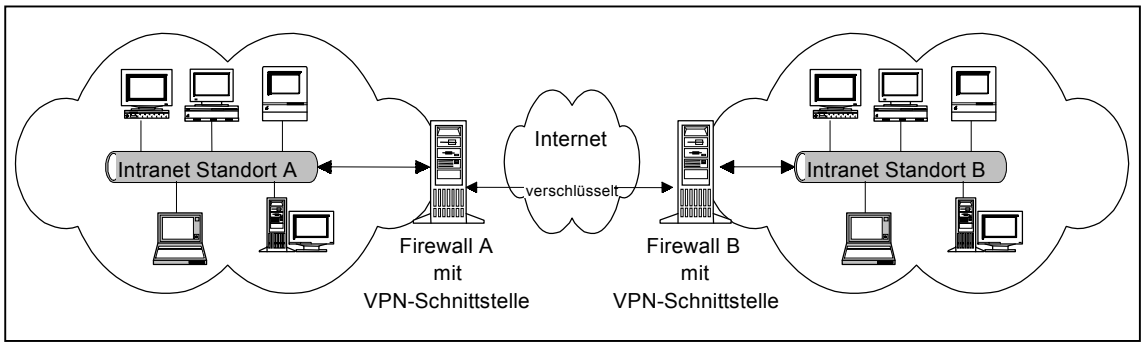

Abb. 12: VPN

Bei VPNs besteht zwar immer noch die Gefahr, abgehört zu werden, aber ein Spion kann wegen der Verschlüsselung der Daten lediglich noch feststellen, daß Daten verschickt wurden. Die Verschlüsselung bringt jedoch auch mit sich, daß nur gegenseitig abgestimmte Firewalls feststellen können, ob Datenpakete sicherheitsgefährdende Inhalte transportieren.

Als Problematisch für die Implementation eines VPNs stellt sich die Vielfalt der konkurrierenden Lösungen heraus. VPNs können auf der Anwendungs-, der Netzwerkprotokoll- oder der Netzwerkverbindungschicht des OSI-Refernez-Modells realisiert werden.[133]

Auf der Anwendungsebene sind die Programme selbst für die Verschlüsselung zuständig. Beispiele dafür sind eMail-Verschlüsselung mit PGP (Pretty Good Privacy), PEM (Privacy Enhanced Mail) und S/MIME (Secure Multipurpose Mail Extensions). Auch Web Browser unterstützen anwendungsbasierte Verschlüsselung mittels SSL.[134] Bei VPNs auf Basis der Verschlüsselung von Netzwerkprotokollen hat sich das IP-Security-Verfahren (IPSec) durchgesetzt. Bei diesem Verfahren werden die IP-Pakete gekapselt verschlüsselt und mit der Adresse der Ziel-Firewall versehen. In der Ziel-Firewall werden die Pakete dann entschlüsselt und an den „richtigen“ Empfänger innerhalb des Intranets weitergeleitet.[135] Diese Form des VPN wird bisher nur von einigen wenigen Firewall-Produkten unterstützt, z. B. Firewall-1 von Checkpoint[136] und von der NetGuard Firebox[137]. Als „Tunneling“ wird die Methode zum Aufbau von VPNs auf der Ebene der Netzwerkverbindung bezeichnet. Auf diesem Gebiet hat sich Microsoft hervorgetan. Hier wird eine Erweiterung des Point-To-Point-Protokolls (PPP) genutzt, mit dem überlicherweise Einwahlverbindungen zu ISPs aufgebaut werden, um über diese Verbindung die Daten zu verschlüsseln. Das benutzte Protokoll nennt sich Point-To-Point-Tunneling-Protokoll (PPTP) und ist unabhängig vom eingesetzten Netzwerkprotokoll, wie z. B. TCP/IP oder IPX.[138]

133 Vgl. Kuri, Jürgen: Privatissimo, a. a. O., S. 191.

134 Vgl. Kuri, Jürgen: Privatissimo, a. a. O., S. 191.

135 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 176.

136 Vgl. Online im Internet: http://www.checkpoint.com/, 28.05.1999.

137 Vgl. Online im Internet: http://www.ntguard.com/, 28.05.1999.

138 Vgl. Kuri, Jürgen: Privatissimo, a. a. O., S. 192.

4.3 Checklisten zu Web Site Security

Die nachfolgenden Checklisten zur WSS operationalisieren die in der vorliegenden Arbeit beschriebenen Maßnahmen auf organisatorischer und technischer Ebene. Sie dienen als Leitfaden, um zu gewährleisten, daß bei der Implementation einer unternehmerischen Web Site alle relevanten Sicherheitsaspekte berücksichtigt werden. Für die Anwendung der Checklisten wird vorgeschlagen, der sequentiell/parallelen Systematik aus Abb. 13 zu folgen.

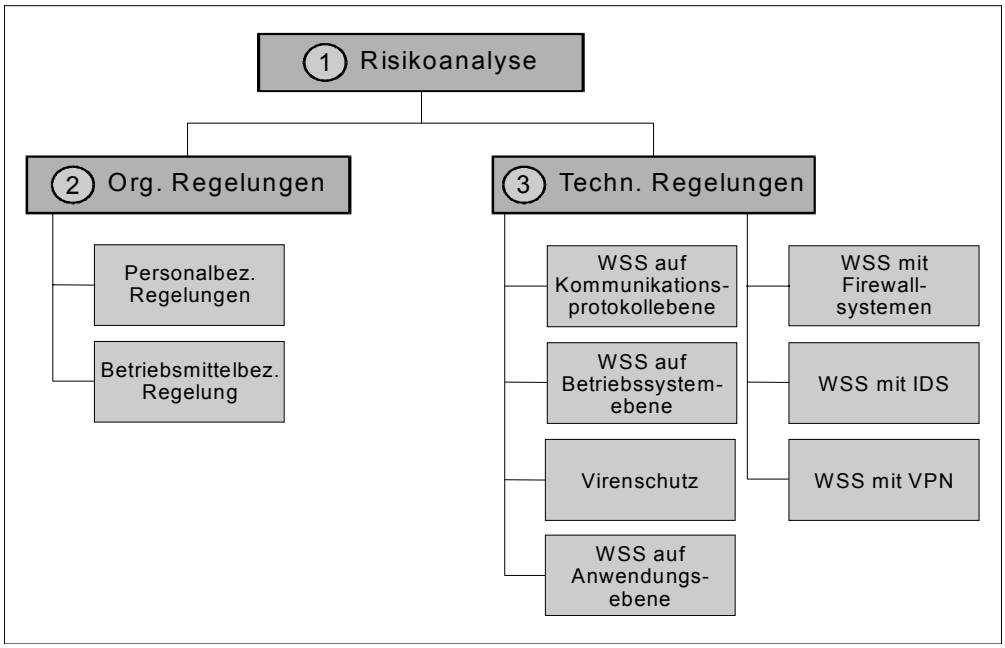

Abb. 13: Checklistenübersicht

Für die unternehmensindividuelle organisatorische und technische Ausdetaillierung der Checklisten bieten sich besonders die Maßnahmenkataloge für vernetzte Internet-Systeme aus dem IT-Grundschutzhandbuch 1998 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an.

Organisatorische Maßnahmen zur WSS		
Risikoanalyse		
Maßnahme	Erläuterung	☑
Analysebereich	Web Site in einzelne Bereiche unterteilen, wie z. B. Betriebssysteme, Web Server, eMail-Server, Netzwerk etc.	☐
Bedrohungsanalyse	Arbeitsgruppen zur detaillierten Szenarioanalyse/Simulation von Sicherheitsrisiken einrichten	☐
Risikobewertung	Ermitteltes Risiko und Eintrittswahrscheinlichkeiten qualitativ oder quantitativ bewerten	☐
Ergebnisauswertung	Risiken richtig bewertet, d. h. nicht über- oder unterschätzt, keinen Analysebereich übersehen	☐

Tab. 1: Checkliste Risikoanalyse

Organisatorische Maßnahmen zur WSS		
Organisatorische Regelungen		
Maßnahmen	Erläuterungen	☑
Alarmpläne	Sind Regelungen für das Vorgehen bei einem Sicherheitsvorfall vorhanden? (Wer macht was wann?)	☐
Alarmpläne bekannt	Sind alle Mitarbeiter über die Regelungen zum Verhalten bei einem Sicherheitsvorfall informiert?	☐
Wartungspläne	Sind Regelungen für die Kontrolle der technischen Sicherheitsmaßnahmen vorhanden?	☐
Zugangsregelungen für kritische Bereiche	Sind personelle Regelungen für den Zugang zu den Server-Räumen und Netzwerkkomponenten vorhanden? (Wer darf an die Maschinen?)	☐
Berechtigungskonzept	Sind Regelungen über die Rechte auf den Datenzugriff vorhanden? (Wer darf schreiben, lesen, Vollzugriff?)	☐
Überwachung und Kontrolle	Wird die Maßnahmendurchführung überwacht und kontrolliert?	☐
Dokumentation	Sind alle organisatorischen Maßnahmen dokumentiert?	☐
Personalbezogene Regelungen		
Maßnahmen	Erläuterungen	☑
Einstellung und Ausscheiden von Mitarbeitern	Sind Maßnahmen für Aktivitäten bei Einstellung und Ausscheiden von Mitarbeitern implementiert, z. B. Löschung von Accounts beim Ausscheiden?	☐
Mitarbeiterausbildung und -schulung	Sind Schulung und Bereitstellung von geeignetem Personl sichergestellt?	☐
Betriebsmittelbezogene Regelungen		
Maßnahmen	Erläuterungen	☑
Betriebsmitteleignung	Sind die vorhandenen Betriebsmittel für die Durchsetzung von WSS geeignet?	☐
Betriebsmitteleinsatz	Werden die Betriebsmittel zielorientiert eingesetzt?	☐
Systemplanung und Auswahl	Werden regelmäßig neue Betriebsmittel ausgewählt und beschafft?	☐
Beauftragter für Betriebsmittelbeschaffung	Gibt es Mitarbeiter, die für die Beschaffung und Auswahl von Betriebsmitteln zuständig sind?	☐
Datensicherungskonzept	Gibt es ein Konzept zum Vorgehen und Ablauf von Datensicherungen?	☐

Tab. 2: Checkliste orgainsatorische, personalbezogene, betriebsmittelbezogene Regelungen

Technische Maßnahmen zur WSS		
WSS auf Kommunikationsprotokollebene		
Maßnahmen	Erläuterungen	☑
Protokollauswahl	Sind nur die benötigten und geeigneten Protokolle installiert?	☐
Protokollversion	Sind die Protokolle in einer aktuellen, fehlerbereinigten Version installiert?	☐
Protokolltest	Angriffssimulatoren auf Protokollebene laufen lassen, z. B. SATAN.	☐

Tab. 3: Checkliste WSS auf Kommunikationsprotokollebene

Technische Maßnahmen zur WSS		
WSS auf Betriebssystemebene		
Maßnahmen	Erläuterungen	☑
Diensteauswahl	Sind nur die benötigten und geeigneten Dienste installiert, z. B. Sendmail, Finger etc.?	☐
Betriebssystemversion	Sind die eingesetzten Betriebssysteme in einer aktuellen, fehlerbereinigten Version installiert?	☐
„Sichere“ Paßwörter	Sind auf Betriebssystemebene die Voraussetzungen geschaffen worden, um Benutzer zur Auswahl „sicherer“ Paßwörter und zur regelmäßigen Änderung der Paßwörter zu veranlassen?	☐
Betriebssysteme testen	Angriffssimulationen auf Betriebssystemebene durchführen	☐

Tab. 4: Checkliste WSS auf Betriebssystemebene

Technische Maßnahmen zur WSS		
Virenschutz		
Maßnahmen	Erläuterungen	☑
Viren-Signaturen	Ist das regelmäßige Aktualisieren von Viren-Signaturen der Antivirensoftware gewährleistet?	☐
Antivirensoftware aktualisieren	Ist die Antivirensoftware immer auf dem neuesten Stand?	☐
Antivirensoftware verteilen	Ist die Antivirensoftware lückenlos auf allen Systemen installiert?	☐

Tab. 5: Checkliste Virenschutz

Technische Maßnahmen zur WSS		
WSS auf Anwendungsebene		
Maßnahmen	Erläuterungen	☑
„Sichere“ Anwendungen	Sind nur „sichere“ Anwendungen im Einsatz (z. B. fehlerhafte Client Software)?	☐
Anwendungsversionen	Sind die Anwendungen in einer aktuellen, fehlerbereinigten Version installiert?	☐
Filterung unerwünschter Benutzung	Werden unerwünschte Eingaben, wie z. B. Betriebssystembefehle in CGI-Abfragen, von den Anwendungen gefiltert?	☐
Schließung von Sicherheitslücken	Sind alle Sicherheitslücken bei der Interaktion von Anwendungen geschlossen, z. B. unerwünschte Paßwortübermittlung bei Web Browsern?	☐
Datensicherung	Ist geeignete Software zur systemweiten Datensicherung nach einem Datensicherungskonzept vorhanden?	☐
Angriffssimulation	Angriffe auf Anwendungsebene simulieren	☐

Tab. 6: Checkliste WSS auf Anwendungsebene

Technische Maßnahmen zur WSS		
WSS mit Firewall-Systemen		
Maßnahmen	Erläuterungen	☑
Paketfilter installieren	Unerwünschte Protokolle filtern	☐
Dual-Homed-Host	Intranet für Angreifer unsichtbar machen	☐
Application-Level-Filter installieren	Unerwünschte Anwendungen, z. B. Telnet, filtern	☐
Statefull-Inspection-Technik implementieren	IP-Pakete anhand von Protokollen und Inhalt (z. B. Viren) filtern.	☐
Dual-Screened-Subnet (→DMZ) einrichten	Paketfilterung vor und hinter einer DMZ, um einen potentiellen Angreifer aus dem sicheren inneren Netz heraus zu halten	☐
Proxy-Server und/oder Bastion-Host einrichten	z. B. Web Server auf Bastion-Host einrichten, um Datenbanken und Infrastrukturen hinter zweitem Paketfilter besser zu schützen	☐
Mehrstufiges Firewall-Konzept implemetieren	Mehre verschiedene Firewalls analog der Unternehmensorganisation auf Abteilungsebene einrichten	☐

Tab. 7: Checkliste WSS mit Firewall-Systemen

Technische Maßnahmen zur WSS		
WSS mit IDS		
Maßnahmen	Erläuterungen	☑
Signaturbasiertes IDS installieren	Einrichtung eines signaturbasierten IDS zur Angriffserkennung	☐
Expertensystembasiertes IDS installieren	Einrichtung eines expertensystembasierten IDS zur Angriffserkennung	☐
Kombination beider IDS-Varianten	Alarmkonzept mit Kombination beider IDS-Varianten erarbeiten	☐

Tab. 8: Checkliste WSS mit IDS

Technische Maßnahmen zur WSS		
WSS mit VPN		
Maßnahmen	Erläuterungen	☑
VPN für Kunden-Partnerbeziehungen einrichten	VPN zur Absicherung der Kommunikation zwischen Kunden und Partnern	☐
VPN für Mitarbeiterkommunikation einrichten	VPN für unternehmensinterne Kommunikation einrichten	☐

Tab. 9: Checkliste WSS mit VPN

5 Abschließende Betrachtung und Ausblick

Im Rahmen eines immer weiter verbreiteten Einsatzes von Web Sites zum eCommerce und der stetig anwachsenden Anzahl von Transaktionen im Internet kommt der Sicherheit von Daten und Transaktionen eine entscheidende Bedeutung zu. Nur die Betreiber von Web Sites, die gewährleisten können, daß Daten und Transaktionen vertrauenswürdig, verläßlich und konsistent sind, werden das Vertrauen von Kunden und Partnern gewinnen und den damit verbundenen strategischen Geschäftsvorteil für sich ausnutzen können. Besonders bei der konsistenten Entwicklung einer Web Site unter Zuhilfenahme eines Web-Site-Engineering-Komponentenmodells[139] darf Web Site Security nicht hinter anderen wichtigen Aspekten, wie Web Site Requirements Engineering, Web Server Engineering, Web Site Design oder Web Site Promotion anstehen, weil sich die Aktivitäten von WSS auf die Mitarbeiter-, Kunden- und Partnerbeziehungen direkt auswirken. Sowohl die lokal gespeicherten Daten einer Web Site als auch die Kommunikationswege müssen „sicher“ sein.

Ein aktueller Trend ist der kombinierte Einsatz mehrerer technischer Lösungen zur WSS. Viele Firewall-Anbieter kombinieren Firewall-Funktionen mit VPN-Verschlüsselung und IDS-Funktionalitäten in ihren Produkten. Neue Tendenzen in der Sicherheit gehen auch weg vom rein technisch orientierten Ansatz hin zur Integration von Sicherheitsprozessen in Unternehmensprozesse. Dies berücksichtigt die Erkenntnis, daß die meisten Sicherheitsvorfälle immer noch durch die eigenen Mitarbeiter ausgelöst werden. Eine solide technische Basis stellt damit nur das „Rückgrat“ von WSS dar, die Unternehmensorganisation hingegen das „Gehirn“.

Zunehmend wird auch die Notwendigkeit erkannt, Sicherheit stiftende Funktionen in Anwendungen, Betriebssysteme und Kommunikationsprotokolle zu integrieren. Dazu soll die Zertifizierung von Software-Produkten mit sicherheitsrelevanten Funktionen dienen, um aus dem derzeitigen Teufelskreis von „penetrate and patch“ herauszukommen. Zur Zeit ist es leider immer noch gängige Praxis, daß erst wenn eine Sicherheitslücke in einem Produkt entdeckt/ausgenutzt wurde, die entsprechende Fehlerkorrektur vom Hersteller oder Dritten nachgeliefert wird. Derartige punktuelle und unsystematische Maßnahmen verschaffen nur einen gewissen Zeitvorsprung bis zu ihrer Ausschaltung oder Umgehung.[140]

Auf Kommunikationsprotokollebene soll der IPv6-Standard mittelfristig das zur Zeit noch gebräuchliche IPv4 ablösen. Mit IPv6 werden die Schwächen des derzeitigen Internet-Protokolls weitgehend beseitigt; so sind z. B. außer einem größeren Adreßraum und Authentifikation dabei auch garantierte Verbindungen zwischen Rechnern im Internet möglich. Die beiden letztgenannten Neuerungen stellen einen entscheidenden Schritt für den eCommerce im Internet dar. Der schnellen Migration auf IPv6 steht noch die Notwendigkeit im Wege, alle Endsysteme anzupassen sowie die Neukonfiguration des Routernetzwerks im Internet.[141] Innerhalb von Unternehmen stehen einer schnellen Adaption des neuen Standards wegen seiner Abwärtskompatibilität zu IPv4 weitaus weniger Probleme im Weg.

---

139 Eine Gesamtdarstellung dieses Modells findet sich in Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, a. a. O.

140 Vgl. Ghosh, Anup K.: E-Commerce Security: Weak Links, Best Defenses, a. a. O., S. 261.

141 Vgl. Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, a. a. O., S. 24.

Literaturverzeichnis

Afif, Noelani Maria: Sichere Abrechnung im Internet-Handel, in: Information Week, 19/1998, S. 12.

Afif, Noelani Maria; Fill, Christian: Sicherheit zahlt sich aus, in: Information Week, 11/99, S. 18-19.

Amorroso, Edward; Sharp, Ronald: Intranet and Internet Firewall Strategies, in: : PCWEEK, Emeryville California: Ziff-Davies Press 1996.

Bager, Jo: IE-Sicherheitsloch ermöglicht Datenklau, Online im Internet: http://www.heise.de/newsticker/data/jo-12.10.98/, 04.06.1999.

Bauer, Markus: Netzwerk & Intranet – Firewalls für Windows NT, in: PC Professional, 8/1997, S. N 21-26.

Chapman, D. Brent; Zwicky, Elizabeth D.: Einrichten von Internet Firewalls: Sicherheit im Internet gewährleisten, Bonn: O´Reilley, Internat. Thomson-Verl., 1996.

Cheswick, William R.; Bellovin, Steven M.: Firewalls und Sicherheit im Internet: Schutz vernetzter Systeme vor cleveren Hackern, Bonn et al.: Addison-Wesley 1996.

Diedrich, Oliver: Der Krieg zwischen FBI und Hackern eskaliert, Online im Internet: http://www.heise.de/newsticker/data/odi-28.05.99-000/, 28.05.1999.

Ebeling, Adolf: BMW-Homepage gehackt, Online im Internet: http://www.heise.de/newsticker/data/ae-02.01.98-000/, 02.05.1998.

Fill, Christian: IT-Security; Zwischen Panik und Perfektion, in: Informationweek,. 19/1998, S. 38-45.

Freiss, Martin: SATAN: Sicherheitsmängel erkennen und beheben, 1. Aufl., Bonn: O´Reilly, Internat. Thomson-Verl., 1996.

Garfinkel, Simon; Spafford, Gene: Web Security & Commerce, Köln et al.: O´Reilley & Associates, Inc. 1997.

Ghosh, Anup K.: E-Commerce Security: Weak Links, Best Defenses, New York et al.: Wiley Computer Publishing 1998.

Görtz, Horst; Stolp, Jutta: Informationssicherheit in Unternehmen, 1. Aufl., Bonn, Reading , Mass.: Addison-Wesley-Longman, 1999.

Hillmeister, Bernd: Intrusion Detection – Software-Tools spüren Einbrecher im Netz auf, in: Computer Zeitung, 18/99, S. 35.

Hinterhuber, Hans H.: Strategische Unternehmensführung, Band 1: Strategisches Denken – Visionen, Unternehmenspolitik, Strategie, 5., neubearb. und erw. Auflage, Berlin, New York. De Gruyter 1992.

Kossakowski, Klaus-Peter: Der Intenet-Wurm, Klassifikation und Abwehr von Computer-Würmern in Netzwerken, DFN-CERT Online-Tutorial, Online im Internet: http://www.cert.dfn.de/tutorial/wuermer/kap222.html, 06.06.1999.

Kossel, Axel: Ein waches Auge, in: c´t Magazin für Computertechnik, 3/99, S. 142-145.

Krempel, Stefan; Schmidt, Michael; Kuri, Jürgen: Lange Ohren, in: c´t Magazin für Computertechnik, 4/99, S. 174-181.

Kuppinger, Martin; Bauer, Markus: Netzwerk & Intranet – Firewalls für Windows NT, Firewall-Konzepte, in: PC Professional, 8/1997, S. N 21.

Kuri, Jürgen: IBMs Hackertruppe knackte neun von zehn Online-Shops, Online im Internet: http://www.heise.de/newsticker/data/jk-11.02.99-000/, 11.02.1999.

Kuri, Jürgen: Privatissimo, in: c´t Magazin für Computertechnik, 4/1999, S. 190-194.

Kyas, Othmar: Sicherheit im Internet, 2. Aufl., Bonn: Internat. Thomson Publishing 1998.

Luckhardt, Norbert: Büchse der Pandora, in: c´t Magazin für Computertechnik, 8/99, S. 17.

Luckhardt, Norbert: Frame-Fälscher im WWW, Online im Internet: http://www.heise.de/newsticker/data/nl-18.11.98-005, 04.06.1999.

Luckhardt, Norbert: Hunderte Online-Shops verraten Kundendaten, in: c´t Magazin für Computertechnik, 10/1999, S. 22.

Luckhardt, Norbert: Millionenschäden durch CIH-Virus, in: c´t Magazin für Computertechnik 10/1999, S. 22.

Luckhardt, Norbert: Trojaner sendet nach China, in: c´t Magazin für Computertechnik, 3/99, S. 21.

Luckhardt, Norbert: Virus-Alarm: Melissa verbreitet sich wie ein Buschfeuer, Online im Internet: http://www.heise.de/newsticker/data/nl-28.03.99-000/, 28.03.1999.

Luckhardt, Norbert: Weitere Web-Hacks in Deutschland, Online im Internet: http://www.heise.de/newsticker/ data/nl-08.10.98-000/, 08.10.1998.

Medosch, Armin: NYTIMES gehackt, Online im Internet: http://www.heise.de/tp/deutsch/inhalt/te/1549/1.html/, 14.09.1998.

Meyer, Egbert: Sicherheitsrisiko Diskettenlaufwerk, Online im Internet: http://www.heise.de/newsticker/data/em-08.04.99-000/, 08.04.1999.

Mraz, Viktor; Weidner, Klaus: Falsch verbunden – Gefahr durch DNS-Spoofing, in: c´t – Magazin für Computertechnik, 10/1997, S. 286.

o. V.: Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch 98, ‚CD-ROM, Bonn, 1998.

o. V.: Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutzhandbuch 98, Online im Internet: http://www.bsi.de/gshb/deutsch/menue.htm, 06.06.1999.

o. V.: Chaos Computer Club, Online im Internet: http://www.ccc.de/, 29.05.1999.

o. V.: DFN-CERT Hompage, Online im Internet: http: // www.cert.dfn.de/, 06.06.1999.

o. V.: Homepage 2600, Online im Internet: http://www.2600.com/hacked_pages, 28.05.1999.

o. V.: Internet-Technik ist kein Sicherheitsrisiko mehr, in: Computer Zeitung, 18/1999, S. 29.

Persson, Christian: Datendiebstahl mit Internet Explorer 4, Online im Internet: http://www.heise.de/newsticker/ data/cp-16.10.97-000/, 16.10.1997.

Pohlmann, Norbert: Datenschutz – Sicherheit in öffentlichen Netzen, Heidelberg: Hüthig 1996.

Pohlmann, Norbert: Firewall-Systeme, Bonn et al.: Internat. Thomson Publishing 1997.

Raepple, Martin: Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung, Heidelberg: dpunkt-Verlag 1998.

Richter-Maierhofer, Ellen: Firewalls – Sicherheitsschleusen für das LAN, in: NT Journal, 5/1997, S. 88.

Rötzer, Florian: SORM 2, Online im Internet: http://www.heise.de/tp/deutsch/inhalt/te/1923/1.html, 21.02.1999.

Rötzer, Florian: Website des Weißen Hauses wurde gecrackt – Update: Online im Internet: http://www.heise.de/ tp/deutsch/inhalt/te/2834/1.html, 11.05.1999.

Ruhman, Ingo; Schulzki-Haddouti, Christinae: Abhördschungel, in: c´t Magazin für Computertechnik, 24/98, S. 90.

Schmeh, Klaus: Safer net: Kryptografie im Internet und Intranet, Heidelberg: dpunkt-Verlag 1998.

Schwickert, Axel C.; Dandl, Jörg: HTML, Java, ActiveX – Strukturen und Zusammenhänge, in: Arbeitspapiere WI, Nr. 6/1997, Hrsg.: Lehrstuhl für Allg. BWL und Wirtschaftsinformatik, Johannes Gutenberg-Universität: Mainz 1997.

Schwickert, Axel: Web Site Engineering – Ein Komponentenmodell, in: Arbeitspapiere WI, Nr. 12/1998, Hrsg.: Lehrstuhl für Allg. BWL und Wirtschaftsinformatik, Johannes Gutenberg-Universität: Mainz 1998.

Siyan, Karanjit; Hare, Chris: Internet Firewalls & Netzwerksicherheit, 1. Aufl., Haar bei München: SAMS 1995, S. 86 ff., 165, 175.

Stahlknecht, Peter; Hasenkamp, Ulrich: Einführung in die Wirtschaftsinformatik, 8., vollst. überarb. und erw. Aufl., Berlin et al.: Springer 1997, S. 323.

Strobel, Stefan: Nebeneingang – Firewalls nicht nur für den Internet-Anschluß, in: iX, 10/98, S. 132-137.

Weck, Gerhard; Gerbisch, Sandra Ines: Gefahren lauern überall: IT-Sicherheits-konzepte helfen Risiken mindern, in: IT-Management, 03/1999, S. 48-53.

Wöhe, Günter: Einführung in die allgemeine Betriebswirtschaftslehre, 19., überarb. und erw. Aufl., München: Vahlen 1996.

Bisher erschienen

Stand: Dezember 2000 – Den aktuellen Stand der Reihe erfahren Sie über unsere Web Site unter http//wi.uni-giessen.de

Nr. 1/1996	Grundlagen des Client/Server-Konzepts	Schwickert/Grimbs
Nr. 2/1996	Wettbewerbs- und Organisationsrelevanz des Client/Server-Konzepts	Schwickert/Grimbs
Nr. 3/1996	Realisierungsaspekte des Client/Server-Konzepts	Schwickert/Grimbs
Nr. 4/1996	Der Geschäftsprozeß als formaler Prozeß - Definition, Eigenschaften, Arten	Schwickert/Fischer
Nr. 5/1996	Manuelle und elektronische Vorgangssteuerung	Schwickert/Rey
Nr. 6/1996	Das Internet im Unternehmen - Neue Chancen und Risiken	Schwickert/Ramp
Nr. 7/1996	HTML und Java im World Wide Web	Gröning/Schwickert
Nr. 8/1996	Electronic-Payment-Systeme im Internet	Schwickert/Franke
Nr. 9/1996	Von der Prozeßorientierung zum Workflow-Management - Teil 1: Grundgedanken, Kernelemente, Kritik	Maurer
Nr. 10/1996	Von der Prozeßorientierung zum Workflow- Management - Teil 2: Prozeßmanagement und Workfflow	Maurer
Nr. 11/1996	Informationelle Unhygiene im Internet	Schwickert/Dietrich/Klein
Nr. 12/1996	Towards the theory of Virtual Organisations: A description of their formation and figure	Appel/Behr
Nr. 1/1997	Der Wandel von der DV-Abteilung zum IT-Profitcenter: Mehr als eine Umorganisation	Kargl
Nr. 2/1997	Der Online-Markt - Abgrenzung, Bestandteile, Kenngrößen	Schwickert/Pörtner
Nr. 3/1997	Netzwerkmanagement, OSI Framework und Internet SNMP	Klein/Schwickert
Nr. 4/1997	Künstliche Neuronale Netze - Einordnung, Klassifikation und Abgrenzung aus betriebswirtschaftlicher Sicht	Strecker/Schwickert
Nr. 5/1997	Sachzielintegration bei Prozeßgestaltungsmaßnahmen	Delnef
Nr. 6/1997	HTML, Java, ActiveX - Strukturen und Zusammenhänge	Schwickert/Dandl
Nr. 7/1997	Lotus Notes als Plattform für die Informationsversorgung von Beratungsunternehmen	Appel/Schwaab
Nr. 8/1997	Web Site Engineering - Modelltheoretische und methodische Erfahrungen aus der Praxis	Schwickert
Nr. 9/1997	Kritische Anmerkungen zur Prozeßorientierung	Maurer/Schwickert
Nr. 10/1997	Künstliche Neuronale Netze - Aufbau und Funktionsweise	Strecker
Nr. 11/1997	Workflow-Management-Systeme in virtuellen Unternehmen	Maurer/Schramke
Nr. 12/1997	CORBA-basierte Workflow-Architekturen - Die objektorientierte Kernanwendung der Bausparkasse Mainz AG	Maurer
Nr. 1/1998	Ökonomische Analyse Elektronischer Märkte	Steyer
Nr. 2/1998	Demokratiepolitische Potentiale des Internet in Deutschland	Muzic/Schwickert
Nr. 3/1998	Geschäftsprozeß- und Funktionsorientierung - Ein Vergleich (Teil 1)	Delnef
Nr. 4/1998	Geschäftsprozeß- und Funktionsorientierung - Ein Vergleich (Teil 2)	Delnef
Nr. 5/1998	Betriebswirtschaftlich-organisatorische Aspekte der Telearbeit	Polak
Nr. 6/1998	Das Controlling des Outsourcings von IV-Leistungen	Jäger-Goy
Nr. 7/1998	Eine kritische Beurteilung des Outsourcings von IV-Leistungen	Jäger-Goy
Nr. 8/1998	Online-Monitoring - Gewinnung und Verwertung von Online-Daten	Guba/Gebert
Nr. 9/1998	GUI - Graphical User Interface	Maul
Nr. 10/1998	Institutionenökonomische Grundlagen und Implikationen für Electronic Business	Schwickert
Nr. 11/1998	Zur Charakterisierung des Konstrukts “Web Site”	Schwickert
Nr. 12/1998	Web Site Engineering - Ein Komponentenmodell	Schwickert
Nr. 1/1999	Requirements Engineering im Web Site Engineering – Einordnung und Grundlagen	Schwickert/Wild
Nr. 2/1999	Electronic Commerce auf lokalen Märkten	Schwickert/Lüders
Nr. 3/1999	Intranet-basiertes Workgroup Computing	Kunow/Schwickert
Nr. 4/1999	Web-Portale: Stand und Entwicklungstendenzen	Schumacher/Schwickert
Nr. 5/1999	Web Site Security	Schwickert/Häusler
Nr. 6/1999	Wissensmanagement - Grundlagen und IT-Instrumentarium	Gaßen
Nr. 7/1999	Web Site Controlling	Schwickert/Beiser
Nr. 8/1999	Web Site Promotion	Schwickert/Arnold
Nr. 9/1999	Dokumenten-Management-Systeme – Eine Einführung	Dandl
Nr. 10/1999	Sicherheit von eBusiness-Anwendungen – Eine Fallstudie	Harper/Schwickert
Nr. 11/1999	Innovative Führungsinstrumente für die Informationsverarbeitung	Jäger-Goy
Nr. 12/1999	Objektorientierte Prozeßmodellierung mit der UML und EPK	Dandl
Nr. 1/2000	Total Cost of Ownership (TCO) – Ein Überblick	Wild/Herges
Nr. 2/2000	Implikationen des Einsatzes der eXtensible Markup Language – Teil 1: XML-Grundlagen	Franke/Sulzbach
Nr. 3/2000	Implikationen des Einsatzes der eXtensible Markup Language – Teil 2: Der Einsatz im Unternehmen	Franke/Sulzbach
Nr. 4/2000	Web-Site-spezifisches Requirements Engineering – Ein Formalisierungsansatz	Wild/Schwickert
Nr. 5/2000	Elektronische Marktplätze – Formen, Beteiligte, Zutrittsbarrieren	Schwickert/Pfeiffer
Nr. 6/2000	Web Site Monitoring – Teil 1: Einordnung, Handlungsebenen, Adressaten	Schwickert/Wendt
Nr. 7/2000	Web Site Monitoring – Teil 2: Datenquellen, Web-Logfile-Analyse, Logfile-Analyzer	Schwickert/Wendt
Nr. 8/2000	Controlling-Kennzahlen für Web Sites	Schwickert/Wendt
Nr. 9/2000	eUniversity – Web-Site-Generierung und Content Management für Hochschuleinrichtungen	Schwickert/Ostheimer/Franke

Bestellung (bitte kopieren, ausfüllen, zusenden/zufaxen)

Adressat:

Professur für BWL und Wirtschaftsinformatik
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefax: (0 641) 99-22619

Hiermit bestelle ich gegen Rechnung die angegebenen Arbeitspapiere zu einem Kostenbeitrag von DM 10,- pro Exemplar (MwSt. entfällt) zzgl. DM 5,- Versandkosten pro Sendung.

Nr.	An
1/1996	
2/1996	
3/1996	
4/1996	
5/1996	
6/1996	
7/1996	
8/1996	
9/1996	
10/1996	
11/1996	
12/1996	

Nr.	An
1/1997	
2/1997	
3/1997	
4/1997	
5/1997	
6/1997	
7/1997	
8/1997	
9/1997	
10/1997	
11/1997	
12/1997	

Nr.	Anz
1/1998	
2/1998	
3/1998	
4/1998	
5/1998	
6/1998	
7/1998	
8/1998	
9/1998	
10/1998	
11/1998	
12/1998	

Nr.	Anz
1/1999	
2/1999	
3/1999	
4/1999	
5/1999	
6/1999	
7/1999	
8/1999	
9/1999	
10/1999	
11/1999	
12/1999	

Nr.	Anz
1/2000	
2/2000	
3/2000	
4/2000	
5/2000	
6/2000	
7/2000	
8/2000	
9/2000	

Absender:

Organisation

Abteilung

Nachname, Vorname

Straße

Plz/Ort

Telefon Telefax eMail

Ort, Datum Unterschrift