

Alexander Pfeffer

Konzepte zur Absicherung von Unternehmensnetzwerken

Dargestellt an einem konkreten Fallbeispiel

Bachelorarbeit

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 2003 Diplom.de
ISBN: 9783832466114

Alexander Pfeffer

Konzepte zur Absicherung von Unternehmensnetzwerken

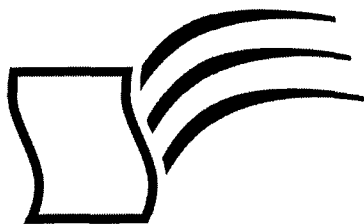
Dargestellt an einem konkreten Fallbeispiel

Alexander Pfeffer

Konzepte zur Absicherung von Unternehmensnetzwerken

Dargestellt an einem konkreten Fallbeispiel

**BA-Arbeit / Bachelor
an der Fachhochschule Darmstadt
Januar 2003 Abgabe**



Diplom.de

Diplomica GmbH _____
Hermannstal 119k _____
22119 Hamburg _____

Fon: 040 / 655 99 20 _____
Fax: 040 / 655 99 222 _____

agentur@diplom.de _____
www.diplom.de _____

ID 6611

Pfeffer, Alexander: Konzepte zur Absicherung von Unternehmensnetzwerken - Dargestellt an einem konkreten Fallbeispiel

Hamburg: Diplomica GmbH, 2003

Zugl.: Darmstadt, Fachhochschule, BA-Arbeit / Bachelor, 2003

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden, und die Diplomarbeiten Agentur, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Diplomica GmbH

<http://www.diplom.de>, Hamburg 2003

Printed in Germany

Danksagung

Besonderer Dank gilt meinen Kollegen und Freunden, die die vorliegende Arbeit einer kritischen Korrekturlektüre unterzogen haben, darunter David Krause, Andreas Körner, Jens Simon und Matthias Engler. Danken möchte ich auch den Betreuern meiner Arbeit, Claudia Parton und Thomas Müller, und meinen Kollegen Kai Steuernagel und Christian Bolk für alle wertvollen Tipps, Anregungen und Kritikpunkte bei der Konzeptionierung der Studie.

Inhaltsverzeichnis

Ehrenwörtliche Erklärung	i
Danksagung	ii
1 Einleitung	1
1.1 Motivation – Warum IT-Sicherheit?	1
1.2 Ziele der Arbeit	2
1.3 Zielgruppe und Voraussetzung	2
1.4 Aufbau der Arbeit	3
2 Problem- und Aufgabenstellung	4
2.1 Ist-Zustand	4
2.2 Aufgabenstellung	4
2.3 Anforderungen	5
2.3.1 Fragebogen zur Bewertung der IT-Sicherheitsstruktur	5
2.3.2 Analyse der Aufgabenstellung	5
3 Grundlagen der IT-Sicherheit	7
3.1 Zentrale Sicherheitsanforderungen	7
3.2 Gefahren	8
3.2.1 Aktive Angriffe	9
3.2.2 Passive Angriffe	10
3.2.3 Zufällige Gefährdungen	11
3.3 Sicherheitstechnologien	11
3.3.1 Kryptographie	11
3.3.1.1 Warum Kryptographie?	11
3.3.1.2 Kryptographische Verfahren	11
3.3.2 Firewalls	17
3.3.2.1 Firewall-Prinzipien	18
3.3.2.2 Zugriffskontrolle	19
3.3.3 Virtual Private Network	19
3.3.3.1 Funktionsweise eines VPN	20
3.3.3.2 VPN auf Basis von IPSec	20
3.3.4 Virenschutz	22

3.3.5	Content Security	25
3.3.6	Virtual Local Area Network	25
3.3.7	Sichere Client-Server-Kommunikation	25
3.3.7.1	Secure Socket Layer	26
3.3.7.2	Transport Layer Security	27
3.3.7.3	Secure HTTP	27
3.3.8	Notwendigkeit von E-Mail-Verschlüsselung	28
3.3.9	Public Key Infrastruktur	29
3.3.9.1	Vertrauensmodelle	29
3.3.9.2	Komponenten einer PKI	31
3.3.9.3	Digitale Zertifikate	33
4	Umsetzung der Anforderungen in ein Sicherheitskonzept	34
4.1	Sicherheitsrichtlinie	34
4.2	Absicherung des Netzübergangs	35
4.2.1	Auswahl des Firewallkonzepts	36
4.2.2	Hochverfügbarkeit	36
4.2.3	Perimetersicherheit vs. Sicherheitszonen	37
4.2.4	Fazit	39
4.3	Anbindung der Außenstellen und Remote-User	40
4.3.1	Wählleitung vs. IPSec - VPN	40
4.3.2	Sicherheitsphilosophie	41
4.3.3	VPN-Konzept	42
4.4	Schutz vor Viren	44
4.4.1	Zentraler Virenschutz	45
4.4.2	Virenschutz auf Servern und Einzelpatzrechnern	45
4.4.3	Virenschutz-Updates	45
4.4.4	Fazit	46
4.5	Gesicherter Zugriff auf Server	46
4.5.1	Lösung mit Benutzerauthentifizierung	46
4.5.2	Lösung ohne Benutzerauthentifizierung	47
4.5.3	Fazit	48
4.6	Sichere E-Mail-Kommunikation	48
4.6.1	Programme und Erweiterungen zur Realisierung von E-Mail Sicherheit	49
4.6.2	Einzelplatzlösung	49
4.6.3	Zentrales Gateway zur Ver- und Entschlüsselung von E-Mails	50
4.6.4	Fazit	51
4.7	Filtern einzelner Internetseiten	51
4.8	Weiterführende Themen	52

5 Aktuelle Technologien und Produkte	59
5.1 Firewall und VPN-Gateway	59
5.2 Virenschutz	62
5.3 URL-Filter	62
5.4 Gesicherte Client/Server-Kommunikation	63
6 Zusammenfassung und Ausblick	65
Literaturverzeichnis	I
Abbildungsverzeichnis	VII
Tabellenverzeichnis	VIII
A Abkürzungsverzeichnis	IX
B Fragebogen zur Bewertung der IT-Sicherheitsstruktur	XI
B.1 Basisanalyse der IT-Sicherheit	XI
B.1.1 Beantwortung der Fragen	XI
B.1.2 Abhängigkeit von IT-Daten	XI
B.1.2.1 Verfügbarkeit	XI
B.1.2.2 Vertraulichkeit	XI
B.1.2.3 Integrität	XI
B.1.3 Festlegen des Sicherheitsniveaus	XIII
B.2 Ermittlung des bestehenden IT-Sicherheitszustandes	XIV
B.2.1 Virenschutz	XIV
B.2.2 Organisation / Datensicherung	XIV
B.2.3 Datenaustausch	XIV