

STUDIE

IT SECURITY

Methoden, Prozess-
und Vorgehensmodelle,
aktuelle Lösungsansätze,
ROI-Calculator, SWOP-
Analysen

Themen: WAF, Netzwerksicherheit, Biometrie, Toolbasierte Security Awareness,
Secure Software Development, HTML5, DLP & Endgeräte-Sicherheit, IT-Infrastruktur,
Compliance-Reifegradmodell, Innovatives Identitätsmanagement



Inklusive
CD-ROM

itresearch

IT SECURITY

Autoren:

Werner Blessing, Paul French, Dr. Ludwig Fuchs, Wolfram Funk, Kristina Javorová, Thomas Jähnel, Michael Klatte, Michael Kranawetter, Prof. Hartmut Pohl, Dr. Bruce Sams, Michael Schmidt, Andreas Schnitzer, Frank von Stetten, Thorsten Scharmatinat, , Lutz Weimann

Herausgegeben von: Ulrich Parthier, 

IT Verlag für Informationstechnik GmbH, Michael-Kometer-Ring 5

D - 85653 Aying

Tel. 08104-6494-0

Fax 08104-6494-22

E-Mail u.parthier@it-verlag.de

www.it-research.net


Text und Abbildungen wurden mit größter Sorgfalt erarbeitet. Herausgeber und Autoren übernehmen jedoch für eventuelle verbliebene fehlerhafte Angaben und deren Folgen keine Haftung.

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, der Entnahme von Abbildungen, der Funksendung, der Wiedergabe auf fotomechanischem oder ähnlichem Wege und der Speicherung in Datenverarbeitungsanlagen bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten.

Bildnachweis Cover: Yakobchuk Vasyl/shutterstock.com

Covergestaltung: Andreas Kreuz, G&K Design, www.magazinemaker.de

Layout: Florian Dausch, Sauerlach

Copyright © 2012 

1. Auflage

ISBN 3-936052-38-7

Inhaltsverzeichnis

| | | |
|-------|--|----|
| 1 | Web Application Firewalls (WAF): Zweck, Auswahl & Einsatz im Unternehmen . | 12 |
| 1.1 | Problemstellung | 12 |
| 1.2 | Lösungsansätze | 12 |
| 1.3 | Unterschied zu klassischen Firewalls | 13 |
| 1.4 | Strategien, Sicherheitsmodelle und Regelsätze | 13 |
| 1.4.1 | Negatives Sicherheitsmodell (Blacklist)..... | 14 |
| 1.4.2 | Positives Sicherheitsmodell (Whitelist) | 14 |
| 1.4.3 | Hybride Ansätze | 15 |
| 1.4.4 | Automatisierte Anomalie-Erkennung | 15 |
| 1.5 | Zusätzliche Sicherheitsmaßnahmen | 16 |
| 1.5.1 | Standardkonformität..... | 16 |
| 1.5.2 | Parameterüberprüfung..... | 17 |
| 1.5.3 | Ausgabefilter..... | 18 |
| 1.5.4 | Sichere Cookie-Verwaltung..... | 18 |
| 1.5.5 | User Session Tracking..... | 18 |
| 1.5.6 | URL Encryption | 18 |
| 1.6 | Architekturmuster zur Integration von WAFs | 19 |
| 1.6.1 | Reverse Proxy | 19 |
| 1.6.2 | Bridge | 20 |
| 1.6.3 | Eingebettetes Modul | 21 |
| 1.7 | Funktionen mit Relevanz für die Architektur | 21 |
| 1.7.1 | Auslagerung von SSL-Terminierung | 21 |
| 1.7.2 | Caching | 22 |
| 1.7.3 | Load Balancing..... | 22 |
| 1.7.4 | Auslagerung der Authentifizierung | 22 |
| 1.7.5 | Wichtig, aber meist nicht verstanden! | 22 |
| 1.8 | Konkretes Beispiel..... | 23 |
| 1.9 | WAF-Auswahlverfahren | 24 |
| 1.10 | Zusammenfassung | 25 |
| 1.11 | SWOT-Analyse..... | 28 |
| 1.12 | Ausblick..... | 29 |
| 1.13 | Über die Autoren..... | 30 |

| | | |
|---------|--|----|
| 2 | Sicherheit für Netzwerke: Auswahl von Antiviren-/Spam-Software | 31 |
| 2.1 | Status Quo: Heterogene Netzwerke benötigen mehr und flexible Sicherheit | 31 |
| 2.2 | In drei Schritten zur passenden Security-Software | 32 |
| 2.2.1 | Schritt 1: Bestandsanalyse des Netzwerks aus der Sicherheitsperspektive | 32 |
| 2.2.2 | Schritt 2: Auswahl potenzieller Produkte | 33 |
| 2.2.2.1 | Qualitätsanalyse: Informieren vor dem Installieren | 33 |
| 2.2.2.2 | Gesamtkosten sind entscheidend | 34 |
| 2.2.2.3 | Hohe Performance steigert die Leistungsfähigkeit | 36 |
| 2.2.2.4 | Flexibilität und Bedienbarkeit | 36 |
| 2.2.3 | Schritt 3: Erste Ergebnisse anhand der Entscheidungsmatrix . | 37 |
| 2.2.4 | Projektrisiken: Wenn Incidents zuschlagen | 37 |
| 2.2.5 | Unterschiede Appliances/Softwarelösungen | 38 |
| 2.3 | Praxisbeispiel: Heterogenes Netzwerk schützen | 39 |
| 2.3.1 | Was ist wichtig? | 40 |
| 2.3.2 | Stärken und Alleinstellungsmerkmale | 42 |
| 2.3.3 | Unabhängigkeit dank eigener Virenskanne | 42 |
| 2.3.4 | Proaktive Erkennung | 42 |
| 2.3.5 | Kostenreduktion durch Unilicense | 43 |
| 2.3.6 | Kostenloser Support | 43 |
| 2.4 | SWOT-Analyse | 43 |
| 2.5 | Return on Investment zur Beurteilung von Einzelinvestitionen | 44 |
| 2.5.1 | ROI-Kalkulation am konkreten Fall | 44 |
| 2.5.2 | Marktüberblick | 47 |
| 2.6 | Über den Autor | 48 |
| 3 | Biometrische Systeme: Menschliche Merkmale als Sicherheit | 49 |
| 3.1 | Fingerabdruckererkennung | 49 |
| 3.2 | Irisererkennung | 51 |
| 3.3 | Gesichtserkennung | 52 |
| 3.4 | Stimm- und Sprechererkennung | 53 |
| 3.5 | Handvenenerkennung (auch Ader-Scan genannt) | 54 |
| 3.6 | Weitere biometrische Verfahren | 54 |
| 3.7 | Ausblick und verschiedene Anwendungsszenarien | 55 |

| | | |
|---------|--|----|
| 3.8 | Ein Beispiel..... | 55 |
| 3.9 | Über den Autor | 58 |
| 4 | Toolbasierte Security Awareness | 59 |
| 4.1 | Problemstellung | 59 |
| 4.2 | Lösungsansatz: Security Awareness..... | 59 |
| 4.3 | Methoden, Prozess- und Vorgehensmodell: Die Security Awareness Kampagne | 60 |
| 4.3.1 | Phase 1 „Wach rütteln“ | 60 |
| 4.3.2 | Phase 2 „Wissen vermitteln“..... | 61 |
| 4.3.3 | Phase 3 „Nachhaltigkeit“ | 62 |
| 4.3.4 | Begleitende Kampagnenelemente | 63 |
| 4.3.5 | Überblick Security Awareness Kampagne | 64 |
| 4.3.6 | Auswahl und Umsetzung geeigneter Kampagnenelemente | 64 |
| 4.4 | Tools für Security Awareness | 65 |
| 4.4.1 | Make or Buy? | 65 |
| 4.4.2 | Tools | 66 |
| 4.4.2.1 | Phase 1: „Wachrütteln“ | 66 |
| 4.4.2.2 | Phase 2: „Wissen vermitteln“ | 66 |
| 4.4.2.3 | Phase 3: „Nachhaltigkeit schaffen“ | 68 |
| 4.5 | Zusammenfassung | 70 |
| 4.6 | Über die Autoren..... | 71 |
| 5 | Managed File Transfer..... | 72 |
| 5.1 | Herausforderungen beim Datenaustausch | 73 |
| 5.2 | Wer braucht MFT?..... | 73 |
| 5.3 | Unterschiede zu konventionellen File-Transfer-Tools | 74 |
| 5.4 | Anforderungen der Enterprise-Klasse..... | 75 |
| 5.5 | Ad-hoc- und Person-zu-Person-Datenaustausch kontrollieren und schützen..... | 76 |
| 5.6 | Die richtige MFT-Lösung auswählen..... | 78 |
| 5.7 | Anbieterübersicht | 78 |
| 5.8 | Über den Autor | 79 |
| 6 | Secure Software Development Guide..... | 80 |
| 6.1 | Einführung eines sicheren Softwareentwicklungsprozesses..... | 80 |
| 6.1.1 | Software-Entwicklungszyklus..... | 80 |
| 6.1.2 | Entwicklungsmethoden zur sicheren Softwareentwicklung | 81 |

| | | |
|-------|--|-----|
| 6.1.3 | Verfahren zur Identifizierung von Sicherheitslücken | 82 |
| 6.2 | Threat Modeling..... | 83 |
| 6.2.1 | Verfahren | 84 |
| 6.2.2 | Analyse der Datenflüsse..... | 85 |
| 6.3 | Static Source Code Analysis | 86 |
| 6.4 | Penetration Testing | 88 |
| 6.5 | Dynamic Analysis: Fuzzing | 88 |
| 6.5.1 | Verfahren | 88 |
| 6.5.2 | Herausforderungen der Identifizierung von Sicherheitslücken | 89 |
| 6.5.3 | Tool-Kombination | 89 |
| 6.5.4 | Monitor Kombination | 90 |
| 6.5.5 | Expert Advice - Manual Auditing durch IT-Sicherheitsexperten | 90 |
| 6.6 | Verfahrenskombination..... | 90 |
| 6.7 | Techniken zur sicheren Programmierung..... | 91 |
| 6.7.1 | Eingabedaten sind potentiell bösartig..... | 91 |
| 6.7.2 | Buffer Overflows | 92 |
| 6.8 | Zugriffskontrolle..... | 93 |
| 6.8.1 | Least Privilege..... | 94 |
| 6.8.2 | Speichern wertvoller Daten (Schlüssel, Passwörter,...)..... | 94 |
| 6.8.3 | Sicherheitsentscheidungen auf Grund von Namen..... | 95 |
| 6.8.4 | Websicherheit | 96 |
| 6.8.5 | Datenbanken | 96 |
| 6.9 | Ausblick..... | 97 |
| 6.9.1 | Security in Embedded Systems..... | 97 |
| 6.9.2 | Security in Smartphones | 99 |
| 6.10 | Weiterführende Literatur | 101 |
| 6.11 | Über den Autor | 102 |
| 7 | HTML5 security issues | 103 |
| 7.1 | Crosss-Origin Resource Sharing..... | 105 |
| 7.1.1 | Vulnerabilities | 106 |
| 7.1.2 | Threats and attack scenarios..... | 107 |
| 7.1.3 | Countermeasures | 111 |
| 7.2 | Web Storage..... | 112 |
| 7.2.1 | Vulnerabilities | 112 |
| 7.2.2 | Threats and attack scenarios..... | 113 |

| | | | |
|------|-------|---|-----|
| | 7.2.3 | Countermeasures | 116 |
| 7.3 | | Offline Web Application | 116 |
| | 7.3.1 | Vulnerabilities | 117 |
| | 7.3.2 | Threats and attack scenarios..... | 117 |
| | 7.3.3 | Countermeasures | 119 |
| 7.4 | | Web Messaging..... | 120 |
| | 7.4.1 | Vulnerabilities | 121 |
| | 7.4.2 | Threats and attack scenarios..... | 121 |
| | 7.4.3 | Countermeasures | 122 |
| 7.5 | | Custom scheme and content handlers | 122 |
| | 7.5.1 | Vulnerabilities | 123 |
| | 7.5.2 | Threats and attack scenarios..... | 123 |
| | 7.5.3 | Countermeasures | 125 |
| 7.6 | | The Web Sockets API | 125 |
| | 7.6.1 | Vulnerabilities | 126 |
| | 7.6.2 | Threats and attack scenarios..... | 126 |
| | 7.6.3 | Countermeasures | 129 |
| 7.7 | | Geolocation API | 129 |
| | 7.7.1 | Vulnerabilities | 130 |
| | 7.7.2 | Threats and attack scenarios..... | 130 |
| | 7.7.3 | Countermeasures | 131 |
| 7.8 | | Implicit security relevant features of HTML5..... | 131 |
| | 7.8.1 | Web Workers | 131 |
| | 7.8.2 | New elements, attributes and CSS | 132 |
| | 7.8.3 | Iframe Sandboxing | 132 |
| | 7.8.4 | Server-Sent Events..... | 133 |
| 7.9 | | Summary..... | 133 |
| 7.10 | | Outlook | 135 |
| 7.11 | | About the author..... | 137 |
| 8 | | Data Loss Prevention & Endgeräte Sicherheit: Was braucht man wirklich?..... | 138 |
| | 8.1 | Data Loss, Spionage, Compliance – alles hängt zusammen!..... | 138 |
| | 8.2 | Erster Schritt: Projekt-Erfolge – Risikominimierung | 139 |
| | 8.3 | Welche Daten sind »kritisch«? | 139 |
| | 8.4 | Import – Das Einbringen von Angriffssoftware unterbinden | 140 |
| | 8.5 | Export – die Mitnahme von Daten sauber regulieren | 140 |

| | | |
|------|--|-----|
| 8.6 | Die letzte Bastion: der Anwender | 140 |
| 8.7 | Bestimmung des Freiraumes | 141 |
| 8.8 | Im Dialog mit dem Anwender – nicht gegen ihn | 142 |
| 8.9 | Die Herausforderungen..... | 143 |
| 8.10 | Netzübergänge | 143 |
| 8.11 | Kommunikationsanwendungen..... | 143 |
| 8.12 | Kommunikationsgeräte und Kommunikationsschnittstellen | 143 |
| 8.13 | Mobile Datenträger | 144 |
| 8.14 | Endgerätesicherheit..... | 144 |
| 8.15 | Spannungsfeld der IT-Manager | 146 |
| 8.16 | Fehler in DLP Projekten vermeiden..... | 147 |
| 8.17 | Fallen vermeiden – Die häufigsten Fehler in DLP-Projekten | 147 |
| 8.18 | Best Practice, Phase 1 | 148 |
| 8.19 | Best Practice, weitere Schritte..... | 148 |
| 8.20 | Alternativen zur Klassifikation einzelner Dateien | 148 |
| 8.21 | Die Lösung »Dynamische Security« | 149 |
| 8.22 | Welches Verfahren ist nun am besten geeignet, die Sicherheitsziele des Unternehmens umzusetzen? | 149 |
| 8.23 | Compliance, Vertrauen und Wünschen..... | 150 |
| 8.24 | Security Awareness – Sicherheitsbewusstsein schaffen | 150 |
| 8.25 | Sicherheits Management..... | 151 |
| 8.26 | Application Control | 151 |
| 8.27 | VIP – selbstverantwortliche »erwachsene« Benutzer verantworten die Nutzung selbst..... | 151 |
| 8.28 | Deployment..... | 152 |
| 8.29 | Automatisierung..... | 152 |
| 8.30 | System Management..... | 153 |
| 8.31 | Kostensenkung | 154 |
| 8.32 | Controlling/Accounting | 154 |
| 8.33 | Schutz von Stand-Alone-Systemen | 154 |
| 8.34 | Verschlüsselung | 155 |
| 8.35 | Compliance..... | 156 |
| 8.36 | Fazit..... | 156 |
| 8.37 | Quellenangabe..... | 157 |
| 8.38 | Über den Autor | 158 |

| | | |
|--------|---|-----|
| 9 | IT-Infrastruktur Compliance Reifegradmodell | 159 |
| 9.1 | Executive Summary | 159 |
| 9.2 | Compliance..... | 161 |
| 9.3 | Unternehmensführung erfolgreich gestalten? Strukturiert!..... | 163 |
| 9.4 | Spielregeln einhalten? Machen Sie das Beste draus! | 165 |
| 9.5 | Worauf soll man sich konzentrieren? Kernbereiche! | 173 |
| 9.6 | Und nun die Lösung | 177 |
| 9.7 | Quo suntque quo vadis? Compliance, die Umsetzung..... | 185 |
| 9.8 | Compliance-relevante IT-Infrastruktur-Lösungen | 214 |
| 9.9 | IT-Glossar | 217 |
| 9.10 | Über die Autoren..... | 220 |
| 10 | Innovatives Identitätsmanagement | 221 |
| 10.1 | Die Herausforderung für moderne Unternehmen | 221 |
| 10.2 | Funktionen von IAM-Systemen..... | 221 |
| 10.3 | Organisatorische Aspekte von IAM | 223 |
| 10.3.1 | Die verschiedenen Reifegrade | 224 |
| 10.3.2 | Die typische Teamstruktur | 226 |
| 10.4 | Der Einstieg in unternehmensweites IAM | 227 |
| 10.5 | Erfolgsfaktor Datenqualität | 229 |
| 10.5.1 | Data Health Check – die kompakte Qualitätsprüfung..... | 230 |
| 10.5.2 | Fehler in Berechtigungsstrukturen erkennen..... | 230 |
| 10.5.3 | Datenbereinigung mit Expertenwissen | 232 |
| 10.6 | Für Profis: Rollenbasiertes IAM..... | 232 |
| 10.6.1 | Nutzen quantifizieren..... | 233 |
| 10.6.2 | Hybride Rollenmodellierung..... | 234 |
| 10.7 | Zusammenfassung | 236 |
| 10.8 | Über den Autor | 237 |
| 11 | ROI Kalkulatoren IT SECURITY | 238 |
| 11.1 | Viren-Kostenkalkulator..... | 238 |
| 11.2 | Spam-Kostenkalulator..... | 238 |
| 11.3 | Desktop-Virtualisierung..... | 238 |
| 11.4 | Web-Security | 238 |
| 11.5 | UTM..... | 238 |
| 11.6 | Application Security | 238 |
| 11.7 | Biometrie..... | 238 |

| | | |
|------|---|-----|
| 11.8 | PACS/Automatisierte Zutrittskontrolle | 238 |
| 11.9 | IAM/Identity & Access Management | 238 |