

TEC CHANNEL **COMPACT**

IT EXPERTS INSIDE

Alles sicher!

- **Web-Anwendungen vor Angriffen schützen**
- **Netzwerk abschotten**
- **Ausfallsicherheit erhöhen**
- **Schutzschild für Smartphones**
- **Tools & Tipps für mehr IT-Sicherheit**
- **Rundumschutz für Windows-Server & PCs**



Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)

Stellv. Chefredakteur / CvD: Albert Lauchner
Redaktion TecChannel:

Lyonel-Feininger-Straße 26, 80807 München,
Tel.: 0 89/3 60 86-897, Fax: -878

Homepage: www.TecChannel.de,

E-Mail: feedback@TecChannel.de

Autoren dieser Ausgabe: Wolfgang Aigner, Johann Baumeister, Manfred Bremmer, Hans-Christian Dirscherl, Jürgen Donauer, Matthias Fraunhofer, Katharina Friedmann, Bernhard Haluschak, Wolfgang Herrmann, Peter Höpfl, Thomas Hruby, Moritz Jäger, Magnus Kalkuhl, Albert Lauchner, Stefan Marx, Walter Mehl, Harald Philipp, Ramon Schwenk, Christian Vilsbeck, Christoph Wolfert, Sebastian Wolfgarten, Max Ziegler

Verlagsleitung: Michael Beilfuß

Copyright: Das Urheberrecht für angenommene und veröffentlichte Manuskripte liegt bei der IDG Business Media GmbH. Eine Verwertung der urheberrechtlich geschützten Beiträge und Abbildungen, vor allem durch Vervielfältigung und/oder Verbreitung, ist ohne vorherige schriftliche Zustimmung des Verlags unzulässig und strafbar, soweit sich aus dem Urheberrechtsgesetz nichts anderes ergibt. Eine Einspeicherung und/oder Verarbeitung der auch in elektronischer Form vertriebenen Beiträge in Datensysteme ist ohne Zustimmung des Verlags nicht zulässig.

Grafik und Layout:

stroemung GmbH (Michael Oliver Rupp, Oliver Eismann), Multimedia Schmiede, Twentyfirst Communications: B. Maier-Leppla

Titelbild: iStockphoto

Anzeigen: Anzeigenleitung: Sebastian Woerle
Tel.: 0 89/3 60 86-628

Ad-Management: Edmund Heider (Ltg.) (-127)
Anzeigenannahme: Martin Behringer (-554)

Druck: Sachsendruck GmbH, Paul-Schneider-Strasse 12, 08525 Plauen

Gesamtvertrieb: Josef Kreitmair

Produktion: Heinz Zimmermann (Ltg.) (-157)

Jahresbezugspreise:

Inland: 49,20 EUR, Studenten: 43,80 EUR Aus-

land: 52,20 EUR, Studenten: 46,80 EUR

Haftung:

Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Veröffentlichungen in TecChannel-Compact erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt. Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleinigere Gesellschafter der IDG Business Media GmbH ist die IDG Communications Media AG, München, eine 100-prozentige Tochter der IDG Inc., Boston, Mass., USA.

Verlag:

IDG Business Media GmbH, Lyonel-Feininger-Straße 26, 80807 München

Tel.: 0 89/3 60 86-0, Fax: -118

Website: www.idgmedia.de

Handelsregisternummer: HR 99187

Umsatzidentifikationsnummer: DE 811257800

Geschäftsführer: York von Heimbürg

Mitglied der Geschäftsführung: Michael Beilfuß

Vorstand: York von Heimbürg, Keith Arnot,

Bob Carrigan

Aufsichtsratsvorsitzender: Patrick J. McGovern

TecChannel ist Mitglied der IDG Business Media GmbH und somit ein Teil der IDG-Verlagsgruppe. Darin erscheinen unter anderem auch folgende Zeitschriften:

COMPUTERWOCHE
Macwelt

ChannelPartner
GameStar

PC WELT
CIO

DigitalWorld
gamepro

Abonnement, Einzel- und Nachbestellung, Umtausch defekter Datenträger:

TecChannel Kundenservice, Postfach 81 05 80, 70522 Stuttgart, Tel: (+49) 07 11/72 52-276, für Österreich 1/21 95 560, für Schweiz, 0 71/3 14 06-15, Fax: (+49) 07 11/72 52-377, E-Mail: shop@TecChannel.de

Inhalt

	Editorial	3
	Impressum	4
1	Schutz von Webservern	10
1.1	Grundschutz für Web-Applikationen	10
1.1.1	Proaktiver Schutz mit WAFs	11
1.1.2	Links überprüfen	12
1.1.3	Best-of-Breed statt All-in-one	12
1.2	Die größten Schwachstellen in Web-Anwendungen	14
1.2.1	Cross Site Scripting (XSS)	14
1.2.2	Injection Flaws	15
1.2.3	Malicious File Execution	15
1.2.4	Insecure Direct Object Reference	16
1.2.5	Cross Site Request Forgery (CSRF)	16
1.2.6	Information Leakage and Improper Error Handling	16
1.2.7	Broken Authentication and Session-Management	17
1.2.8	Insecure Cryptographic Storage	17
1.2.9	Insecure Communications	17
1.2.10	Failure to Restrict URL Access	18
1.3	Den Lücken in Web-Anwendungen auf der Spur	19
1.3.1	Das Web-Audit	19
1.3.2	Wie Scanner arbeiten	19
1.3.3	Manuelle Aufgaben	20
1.3.4	Der Markt	21
1.3.5	Weitere Vorteile von Scannern	21
1.3.6	Qualitätsmerkmale und Hürden	22
1.3.7	Tücken bei der Anmeldung	23
1.3.8	Die Grenzen der Scanner	23
1.4	Web Application Firewalls in der Praxis	25
1.4.1	Aber die Firewall?	25
1.4.2	Die Integration	25
1.4.3	Die Grundfunktionen einer WAF	26
1.4.4	Wie eine WAF Angriffe erkennt	26
1.4.5	Schutz vor Manipulation	27
1.4.6	Authentisierung via WAF	28
1.4.7	SSL-verschlüsselte Anfragen	28
1.4.8	Das WAF-Regelwerk	28
1.4.9	Black- und Whitelists	28
1.4.10	False Positives	29
1.4.11	Marktübersicht	29
1.4.12	Die Stolpersteine	31

1.5	Web-Anwendungen sicher entwickeln	32
1.5.1	Sicherheit im Entwicklungsprozess	32
1.5.2	Anforderungsanalyse	32
1.5.3	Architektur und Design	33
1.5.4	Implementierung	34
1.5.5	Test	35
1.5.6	Integration in Produktion	35
1.6	Schutz von Webshops und E-Commerce-Lösungen	37
1.6.1	Phishing	37
1.6.2	Was ist Cross Site Scripting (XSS)?	37
1.6.3	Was hilft gegen XSS-Attacken?	38
1.6.4	Wie lassen sich Session-Hijacking und SQL-Injection verhindern?	38
1.6.5	Welche grundsätzlichen Schutzmaßnahmen gibt es?	39
1.6.6	Wie Web-Bedrohungen nachhaltig abwehren?	39
1.6.7	Was ist bei der Absicherung der Server-Plattform zu beachten?	40
1.6.8	Inwieweit sind die eigenen Mitarbeiter gefordert?	40
1.7	Apache-Sicherheitsoptimierung	41
1.7.1	Tipp 1: Listen-Anweisungen	41
1.7.2	Tipp 2: User nobody	42
1.7.3	Tipp 3: Optionen für das Wurzelverzeichnis	42
1.7.4	Tipp 4: Optionen für htdocs anpassen	43
1.7.5	Tipp 5: Die ServerTokens-Anweisung	44
1.7.6	Tipp 6: Fehlermeldungen	45
1.7.7	Tipp 7: /icons/ löschen	46
1.7.8	Tipp 8: /manual/ löschen	46
1.7.9	Tipp 9: Test-Skripte löschen	46
1.7.10	Tipp 10: Hilfsprogramme löschen	46
2	Netzwerksicherheit	48
2.1	Sourcefire: Intrusion Detection in der Praxis	48
2.1.1	Test-Szenario und Aufbau	49
2.1.2	In der Praxis	50
2.1.3	Reports: Übersichtlich und anpassbar	52
2.2	Network Access Control für mehr Netzwerksicherheit	54
2.2.1	Viel Nutzen, viel Aufwand	54
2.2.2	Transparenz ist der Schlüssel	55
2.2.3	Audit und Compliance	56
2.2.4	Anforderungen an eine NAC-Lösung	56
2.3	Ports scannen mit Nmap & Co.	58
2.3.1	Sockets sind die Adressen von PC und Servern	58
2.3.2	Well known und registrierte Ports	59
2.3.3	Ports schließen oder absichern	60
2.3.4	So spüren Sie offene Ports auf	61
2.3.5	Mit Nmap offene Ports erkennen und analysieren	62
2.3.6	Fingerprinting: Betriebssysteme identifizieren	63

2.4	Millionen DSL-Router hochgradig gefährdet	67
2.4.1	Angriffsvektor CSRF (XSRF oder Session Riding)	67
2.4.2	CSRF-Logout-Button-Attacke	68
2.4.3	Cookie-Manipulation mit CSRF	70
2.4.4	CSRF-Angriff auf das interne Netz	73
2.4.5	Sicherheitsrisiko DSL-Router	74
2.4.6	AVM bestätigt Angriff	75
2.4.7	Das Passwort allein schützt nicht	75
2.4.8	Potenzielle und reale Gefahren für DSL-Router	77
2.4.9	Schutzmaßnahmen	78
3	Schutz für Server	80
3.1	Serverräume wirkungsvoll vor unbefugtem Zutritt schützen	80
3.1.1	Authentifizierung, Identifizierung und Verifizierung	81
3.1.2	Traditionelle Absicherung und Überwachung von Serverräumen	81
3.1.3	Raumüberwachung per Videokameras	82
3.1.4	Intelligente Videoüberwachung	82
3.1.5	Praxisnaher Einsatz biometrischer Zutrittssysteme	84
3.1.6	Personenvereinzelung und 3D-Gesichts-Scan	85
3.2	Server-Fernwartung effizient einsetzen	89
3.2.1	Grundlagen des Remote-Managements	89
3.2.2	Remote-Management- und Client-Software	90
3.2.3	Sichere Konsolen-Server (SCS)	91
3.2.4	KVM-over-IP-Switch	92
3.2.5	Baseboard Management Controller (BMC)	93
3.3	Test – Hochverfügbarkeit mit Server-Cluster	95
3.3.1	Testsystem: 2x Dell PowerEdge 1950	95
3.3.2	Funktionsweise des Avance-HA-Cluster	96
3.3.3	Installation der Avance-Cluster-Software	97
3.3.4	Installation und Verwaltung von virtuellen Maschinen	100
3.4	Intel: Nehalem EX greift RISC-CPUs an	103
3.4.1	Hohe Skalierfähigkeit	103
3.4.2	RAS-Features auf RISC-Niveau	105
3.4.3	Performance-Angaben	105
3.5	Standard-x86-Server vs. RISC-Unix-Systeme	107
3.5.1	Warum Unternehmen Standard-Server nutzen	108
3.5.2	Technische Gründe für x86-Server	109
3.5.3	Virtualisierung beflügelt x86-Serversysteme	109
3.5.4	Blade-System sparen Energie	110
3.5.5	Sieben Aspekte, die für x86-Server sprechen	111
3.5.6	Zukunftsperspektiven von RISC-Unix-Systemen	111
3.6	Datenaustausch zwischen Linux, Windows 7 und Server 2008 R2	112
3.6.1	Mit Linux auf Windows-7-Partitionen zugreifen	112
3.6.2	Umkehrschwung: Windows 7 und Linux-Partitionen	113

5	Praxis und Know-how	151
5.1	Verhaltensweise nach IT-Angriffen	151
5.1.1	Hinter den Kulissen	151
5.1.2	Verhalten im Verdachtsfall	152
5.1.3	Rechnen Sie mit unglaublichen Datenmengen	153
5.1.4	Die Analyse	153
5.1.5	IT-Forensik fordert Vertrauen	154
5.2	Von Fingerprint bis Gesichtserkennung	156
5.2.1	Optische und kapazitive Fingerprint-Systeme	157
5.2.2	Thermo- und Ultraschall-Fingerprint-Systeme	158
5.2.3	Analyseverfahren von Fingerabdrücken	159
5.2.4	Handgeometrie	160
5.2.5	2D-Gesichtserkennung	160
5.2.6	3D-Gesichtserkennung	161
5.2.7	Iriserkennung	162
5.2.8	Retina-Scan	163
5.2.9	Stimmidentifikation	164
5.2.10	Unterschriftenerkennung	165
5.2.11	Venen- oder Aderscan	166
5.2.12	Tastentippdynamik-Verfahren	167
5.2.13	Personenerkennung durch Herzschlaganalyse	168
5.2.14	Biometrische Systeme im Vergleich	170
5.2.15	Fazit und Ausblick	171
5.3	Certgate Protector: Smartphones sicher betreiben	173
5.3.1	Setup mit vielen Einstellungsmöglichkeiten	173
5.3.2	Sperren von Funktionen	175
5.3.3	Beschreiben der MicroSD-Card	176
5.4	Zehn IE-Einstellungen für sicheres Surfen	178
5.4.1	Deaktivieren Sie XPS-Dokumente	178
5.4.2	Deaktivieren Sie den Schriftart-Download	179
5.4.3	Schließen Sie beim Datei-Upload den lokalen Verzeichnispfad aus	179
5.4.4	Deaktivieren Sie die automatische Eingabeaufforderung	180
5.4.5	Geben Sie stets Nutzernamen und Passwort ein	180
5.4.6	Deaktivieren Sie SSL-2.0-Unterstützung	180
5.4.7	Aktivieren Sie TLS-Unterstützung	181
5.4.8	Deaktivieren Sie die Suche in der Adressleiste	181
5.4.9	Deaktivieren Sie unnötige Add-ons	181
5.4.10	Deinstallieren Sie alte Java-Installationen	182
5.5	Die besten Check- und Sicherheits-Tools	183
5.5.1	Stick Security: USB-Stick-Zugriffsschutz für den PC	183
5.5.2	1st Backup: Tool für die einfache Datensicherung	184
5.5.3	Autoruns: Zeigt alle Programme im Autostart	184
5.5.4	Dvdisaster und weitere Tools	185
	Index	191