

TEC CHANNEL COMPACT

IT EXPERTS INSIDE

Netzwerk-Praxis

- **WLAN-Security für Unternehmen**
- **Sicherheitslücke Multifunktionsgeräte**
- **NAC- und Snort-Workshops**
- **Fehler im LAN finden**
- **Frühzeitig planen: 100 GbE Netzwerk**

Windows 7 & Server 2008 R2

- **Windows 7: Die neuen Funktionen für Unternehmen**
- **Active Directory mit Windows Server 2008 R2**
- **Softwareverteilung mit dem ESB**

**Die besten Tools
fürs Netzwerk**

Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)

Stellv. Chefredakteur / CxD: Albert Lauchner
Redaktion TecChannel:

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

Homepage: www.TecChannel.de,

E-Mail: feedback@TecChannel.de

Autoren dieser Ausgabe: Martin Bayer, Hans-Christian Dirscherl, Jürgen Hill, Georg von der Howen, Malte Jeschke, Thomas Joos, Andreas Kroschel, Gabi Lutz, Daniel Prokop, Uli Ries, Marko Rogge, Elmar Török

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 (Bernd Maier-Leppa)

Titelbild: iStockphoto

Anzeigen: Anzeigenleitung: Sebastian Woerle

Tel.: 0 89/3 60 86-628

Ad-Management: Edmund Heider (Ltg.) (-127)

Anzeigenannahme: Martin Behringer (-554)

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

Gesamtvertrieb: Josef Kreitmair

Vertrieb: Stefan Rörig

Produktion: Jutta Eckbrecht (Ltg.) (-256)

Bezugspreise je Exemplar im Abonnement:

Inland: 12,30 Euro, Studenten: 10,95 Euro,

Ausland: 13,05 Euro, Studenten: 11,70 Euro

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: Alleiniger 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

Homepage: www.idg.de

Handelsregisternummer: HR 99187

Umsatzidentifikationsnummer: DE 811257800

Geschäftsführer: York von Heimburg

Mitglied der Geschäftsführung: Michael Beilfuß

Vorstand: York von Heimburg, 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:



Abonnement, Einzel- und Nachbestellung, Umtausch defekter Datenträger:

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

Inhalt

	Editorial	3
	Impressum	4
1	Netzwerk-Sicherheit und -Praxis	9
1.1	Open-Source und kostenlose NAC-Lösungen	9
1.1.1	Auswahl am Markt	10
1.1.2	Testkriterien	10
1.1.3	Test Stillsecure SafeAccess Lite	11
1.1.4	Gerätemanagement	12
1.1.5	Jede Menge Tests	14
1.1.6	Fazit SafeAccess Lite	15
1.1.7	Test FreeNAC	15
1.1.8	Konfiguration von FreeNAC	16
1.1.9	Kommandozeilenmodus	18
1.1.10	Management mit GUI und Browser	19
1.1.11	Fazit FreeNAC	20
1.2	Workshop: Intrusion Detection und Intrusion Prevention mit Snort	21
1.2.1	Aufgaben eines IDS	21
1.2.2	Vor- und Nachteile eines IDS	22
1.2.3	Snort installieren und konfigurieren	23
1.2.4	Konfiguration und Regeln von Snort	26
1.2.5	Preprocessors	27
1.2.6	Fazit	29
1.3	Workshop: Snort konfigurieren und IDS-Regeln erstellen	30
1.3.1	Rule Header und Rule Options	30
1.3.2	Output-Module	32
1.3.3	Snort starten	32
1.3.4	Zusatz-Tools	33
1.3.5	Fazit	33
1.4	Sicherheitslücke Drucker und Multifunktionsgeräte	34
1.4.1	Risiken im Betrieb	35
1.4.2	Spam aus dem Drucker	35
1.4.3	Protokolle deaktivieren	36
1.4.4	Verschlüsselt verwalten	37
1.4.5	Kontrollierter Zugang	38
1.4.6	Sicher drucken	39
1.4.7	Druckdaten verschlüsseln	41

1.4.8	Multifunktion im Alltag	42
1.4.9	Fazit	43
1.5	Sicherheitslücke WLAN: Risikofaktor trotz Verschlüsselung	44
1.5.1	WPA2 und feste Passwörter	45
1.5.2	Neue Angriffe, größere Gefahr	46
1.5.3	Die größte Gefahr: WLAN verbieten	47
1.5.4	WLAN muss sein – aber sicher	48
1.5.5	Erziehung tut not	48
1.5.6	Konferenz mit dem Datendieb	50
1.5.7	Teuer, aber nützlich: Wireless-IDS	50
1.6	Die besten Netzwerk-Tools	52
1.6.1	Angry IP Scanner – Geräte im Netzwerk suchen	52
1.6.2	Netdrive – FTP und WebDAV als Laufwerk einbinden	53
1.6.3	HP Web Jetadmin – Drucker im Netz verwalten	55
1.6.4	TeamViewer – Remote-Steuerung & Fernwartung von Servern und PCs	56
1.6.5	LAN Search Pro – Versteckte Dateien im Netzwerk finden	58
1.6.6	TCPView – TCP- und UDP-Verbindungen analysieren	59
1.6.7	Network Scanner – IP, NetBIOS und SNMP im Netzwerk analysieren	60
1.7	Praxis: Fehler im LAN entdecken	62
1.7.1	Tückische Ethernet-Kabel	62
1.7.2	Netzdesign	63
1.7.3	Fehlende Segmentierung	64
1.7.4	Ungenutztes Trunking-Potenzial	65
1.7.5	Performance-Falle Priorisierung	66
1.7.6	TCP/IP-Bremse	67
1.7.7	Fazit – Vorbeugen statt heilen	68
2	Netzwerk-Infrastruktur	69
2.1	Die wichtigsten Verfahren zur WAN-Optimierung	69
2.1.1	Wichtige Aspekte der WAN-Optimierung	70
2.1.2	Erst Datenverkehr analysieren, dann optimieren	70
2.1.3	Komprimierung – die wichtigsten Stellschrauben	71
2.1.4	Caching und Protokoll-Optimierung	72
2.1.5	Traffic Shaping, Bandbreiten-Management und Multimedia-Optimierung	73
2.1.6	Neun Fragen zur WAN-Optimierung	74
2.1.7	Das Bandbreiten-Paradoxon beachten	74
2.2	Intelligentes Energie-Management mit Switches	76
2.2.1	Energiesparen beginnt bei der Switch-Wahl	77
2.2.2	Energiehunger der Switches in der Praxis	77
2.2.3	Wie intelligente Switches Strom sparen	78

2.2.4	Switch-Betriebssystem und Schnittstellen	78
2.2.5	Fazit und Ausblick	79
2.3	100 Gbit/s – die neue Dimension der Netzwerke	80
2.3.1	Der Weg zu 100G-Standards	80
2.3.2	Netzwerkanforderungen für 100-Gbit/s-Transport	82
2.3.3	100-Gbit/s-Transport-Technologie	84
2.3.4	100 Gbit/s durch fortschrittliche Modulationsformate	85
2.3.5	Fazit	87
2.4	Mehr Performance durch Netzwerk-Management	88
2.4.1	Die wichtigsten Management-Komponenten	88
2.4.2	Leistungsmessung mit Application Performance Monitoring	89
2.4.3	Anwendungen simulieren statt Probleme im Live-Betrieb	89
2.4.4	Testmethoden der Netzwerk-Performance	90
2.4.5	Künftige Herausforderungen	91
3	Windows im Netz	92
3.1	Windows Server 2008 R2: PowerShell 2.0, Hyper-V und VDI	92
3.1.1	Virtualisierung mit Hyper-V 2.0	93
3.1.2	Virtuelle Desktop Infrastructure (VDI) und Terminal Services	94
3.1.3	Hyper-V und schnelles Deployment	96
3.1.4	PowerShell 2.0	97
3.1.5	Active Directory mit Windows Server 2008 R2	99
3.1.6	Fazit	100
3.2	Active Directory mit Windows Server 2008 R2	101
3.2.1	Active Directory Administration Center	101
3.2.2	Best Practices Analyzer – Überprüfung von Active Directory	103
3.2.3	Papierkorb für Active Directory	105
3.2.4	Objekte vor dem versehentlichen Löschen schützen	107
3.2.5	Offline-Domänenaufnahme	107
3.2.6	Neue Version der PowerShell	108
3.2.7	Wichtige PowerShell-Befehle	111
3.3	Software automatisch verteilen mit dem Essential Business Server	113
3.3.1	Softwareverteilung mit SCE 2007	113
3.3.2	Erstellen von Paketen	115
3.3.3	Grundlagen zur automatisierten Installation	116
3.3.4	Gruppenrichtlinien für Office 2007	117
3.3.5	Die Setup-Optionen von Office 2007	118
3.3.6	Service-Packs in den Installationsordner von Office integrieren	121
3.3.7	Softwarepaket für System Center Essentials konfigurieren	122
3.3.8	Softwareanbindung ohne Updates	123

1 Netzwerk-Sicherheit und -Praxis

Netzwerke bilden die zentrale Kommunikationsader im Unternehmen und sind damit ein lohnendes Ziel für Angriffe. Insbesondere WLANs erfordern eine praxistaugliche Komplettabsicherung. Dieses Kapitel zeigt, wie eine moderne Einbruchserkennung funktioniert und welche Werkzeuge dabei zum Einsatz kommen.

1.1 Open-Source und kostenlose NAC-Lösungen

Auch wenn Network Access Control (NAC) schon seit einigen Jahren mit Konzept und entsprechenden Produkten Einzug in die Unternehmenswelt gefunden hat, breitet sich das Schutzsystem nur langsam in den Firmen aus. Schließlich präsentierte der Netzwerk-Riese Cisco schon 2003 das Konzept der Network Access Control, abgekürzt NAC. Die simple Idee dahinter: Sobald das Netzwerk ein neues Gerät erkennt, das Zugriff auf die Ressourcen haben möchte, muss es erst einen Check auf Unbedenklichkeit durchlaufen, bevor es logisch mit dem LAN verbunden wird. Mehr zu den Grundlagen von NAC lesen Sie in unseren beiden Artikeln „Sicheres Netzwerk durch Network Access Control“ (Webcode **2020365**) und „Die Technik hinter Network Access Control“ (Webcode **2020870**).

Wenn man Faktoren wie mangelnde Standardisierung und die Marketing-schlachten der Hersteller außer Acht lässt, bleibt ein Hauptgrund gegen die Einführung von NAC übrig: Weil NAC Auswirkungen auf fast alle Komponenten der Netzwerkinfrastruktur hat, ist die Umsetzung aufwendig und damit sehr teuer. „Nur mal ausprobieren“ kommt nicht in Frage. NAC-Projekte müssen mit hohen Ressourcenbudgets vorbereitet und durchgezogen werden.

Das mag in großen Unternehmen der richtige Weg und durchaus machbar sein. Kleine und mittlere Firmen hingegen stehen dem NAC-Prinzip eher skeptisch gegenüber und wollen erst abklären, ob die Nutzeffekte in ihrer spezifischen Umgebung den Aufwand rechtfertigen. Die Angebote der großen Hersteller wie Enterasys, Cisco oder Symantec sind auf die Belange großer Unternehmen mit der entsprechenden Finanzkraft zugeschnitten. Weit günstiger, zumindest was das NAC-System selbst angeht, lässt sich die Sicherheitslösung mit einem Open-Source-Angebot angehen. Das mag in einigen Firmen nicht der offiziellen Policy entsprechen, aber für den Test und erste Erfahrungen mit NAC genügen die kostenlosen Angebote auf alle Fälle.

Eigentlich wollte auch Cisco, einer der wichtigsten Hersteller im NAC-Markt, seinen NAC-Client der Open-Source-Community übergeben. Doch nach einer Weile ruderte der Hersteller zurück und gab an, die Offenheit „über den Ansatz der Standards“ weiterführen zu wollen.