

TEC CHANNEL COMPACT

IT EXPERTS INSIDE

Firmen-IT absichern

- **Komplettschutz mit Forefront**
- **Backup für SharePoint, Exchange**
- **Daten & Identitäten schützen**

Windows 7

- **Neue Sicherheitsfunktionen nutzen**
- **Systemdienste sinnvoll aufräumen**
- **Rettungsfunktionen richtig einsetzen**

Praxis

- **Windows-7-Tricks für Admins**
- **OpenVPN optimal einsetzen**
- **Zabbix: Client & Server überwachen**



UTM
Lösungen

Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)

Redaktion TecChannel:

Lyonel-Feiningger-Straße 26, 80807 München,

Tel.: 0 89/3 60 86-897

Homepage: www.TecChannel.de,

E-Mail: feedback@TecChannel.de

Autoren dieser Ausgabe werden bei den

Fachbeiträgen genannt

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-Leppla)

Titelgestaltung: Clemens Strimmer

Titelbildquelle: Kiki – Fotolia.com

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

Gesamtvertriebsleitung IDG Deutschland:

Josef Kreitmair

Produktion: Jutta Eckbrecht (Ltg.)

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-Feiningger-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) 0180 5 72 7252-276*, Fax: -377*, für Österreich 1/21 95 560, für Schweiz, 0 71/3 14 06-15, E-Mail: shop@TecChannel.de

(* aus dem dt. Festnetz nur 0,14 Euro pro Minute, Mobilfunkpreise max. 0,42 Euro pro Minute)

Inhalt

	Editorial	3
	Impressum	4
1	Microsoft Sicherheitslösungen	9
1.1	Microsoft Forefront – Sicherheitsprodukte im Überblick	9
1.1.1	Forefront Threat Management Gateway 2010	10
1.1.2	Forefront Unified Access Gateway 2010	11
1.1.3	Forefront Server Protection	12
1.1.4	Forefront Client Security	12
1.1.5	Forefront Endpoint Protection 2010	13
1.1.6	Forefront Protection Suite	14
1.1.7	Forefront Identity Manager	14
1.1.8	Fazit	15
1.2	Microsoft Forefront – Das Threat Management Gateway 2010	16
1.2.1	Die Neuerungen des Threat Management Gateway 2010	17
1.2.2	Sicherheitsfunktionen des TMG auf dem Prüfstand	19
1.2.3	Die Architektur des TMG	19
1.2.4	Forefront-TMG-Assistenten im Dienste des Administrators	20
1.2.5	Fazit	20
1.3	Microsoft Forefront – Threat Management Gateway 2010 in der Praxis	21
1.3.1	Die Testumgebung	21
1.3.2	Netztopologie des TMG definieren	22
1.3.3	TMG im Praxiseinsatz	23
1.3.4	Server für den Webzugriff vorbereiten	24
1.3.5	Fazit	26
1.4	Microsoft Forefront – Das Unified Access Gateway 2010	27
1.4.1	Bereitstellung von Anwendungen durch Trunks	28
1.4.2	Applikationspublizierungen durch das UAG	29
1.4.3	Rundumschutz durch mehrfache Absicherung	30
1.4.4	Fazit	31
1.5	Microsoft Forefront – Unified Access Gateway 2010 in der Praxis	32
1.5.1	Die Torwächterfunktion des UAG	32
1.5.2	Der Trunk – ein konfigurierbares Zugangsportal	33
1.5.3	Sicherheit und Integration von Applikationen	34
1.5.4	Dedizierte Rechtezuordnung für den Benutzer	35
1.5.5	Fazit	36
1.6	Microsoft Forefront – Endpoint Protection 2010 im Detail	37
1.6.1	Endgeräte mit Client-Security-Tools schützen	37
1.6.2	Fazit	38

1.7	Microsoft Forefront – Identity Manager 2010	39
1.7.1	Der Benutzer und seine Arbeitsmittel im Sinne von FIM	40
1.7.2	Konnektoren integrieren Fremdsysteme	41
1.7.3	Self Service Passwort Reset	42
1.7.4	Dynamische Gruppen vermeiden Gruppen-Leichen	42
1.7.5	Fazit	43
1.8	Microsoft Forefront – Integration in Windows-Betriebssysteme	44
1.8.1	Die Sicherheitsbausteine des Windows-Betriebssystem	44
1.8.2	Sicherheit der SQL-Datenbank	46
1.8.3	Network Access Protection	46
1.8.4	Rights Management System	47
1.8.5	Fazit	48
1.9	Microsoft Forefront – Server Protection 2010	49
1.9.1	Gebündelte Sicherheit in Forefront Server Protection	49
1.9.2	Fünf parallele Scanner erhöhen die Sicherheit	50
1.9.3	Größte Sicherheit versus Effizienz bei Abwehr der Angreifer	51
1.9.4	Online- oder Offline-Untersuchung der Dokumente	52
1.9.5	Spyware und Spam-Abwehr durch Forefront Server Protection	52
1.9.6	Fazit	53
1.10	Microsoft System Center Data Protection Manager 2010	54
1.10.1	Optimale Datensicherung in Microsoft-Netzwerken	54
1.10.2	Exchange- und SQL-Server effizient sichern	55
1.10.3	Datensicherung in Niederlassungen über WAN-Leitungen	57
1.10.4	Schnelle und einfache Wiederherstellung	58
1.10.5	Jobs neu starten und Volumes selbst verwalten	59
1.10.6	Zusammenarbeit mit anderen Produkten	60
1.10.7	Virtuelle Systeme und Arbeitsstationen	62
1.10.8	Lizenzen	63
2	Systemüberwachung und sichere Einwahl	64
2.1	Komplette Server- und Client-Überwachung mit Zabbix 1.8.1	64
2.1.1	Installation	65
2.1.2	Apache-Webserver	68
	MySQL-Datenbank-Server	68
2.1.3	Zabbix-Frontend	69
2.1.4	Vorbereitende Schritte zum Starten der Zabbix-Daemons	69
2.1.5	Konfiguration des Server-Daemon	70
	zabbix_sender und zabbix_get	70
2.1.6	Konfiguration des Agenten	71
2.1.7	Letzte Schritte und Starten des Zabbix-Daemons	71
2.1.8	Zabbix-Agent unter Windows einrichten	73
2.2	Workshop – Clients und Server mit Zabbix überwachen	75
2.2.1	Administration und Konfiguration	76
2.2.2	Hinzufügen von Clients	77
	Zu überwachende Elemente konfigurieren	78

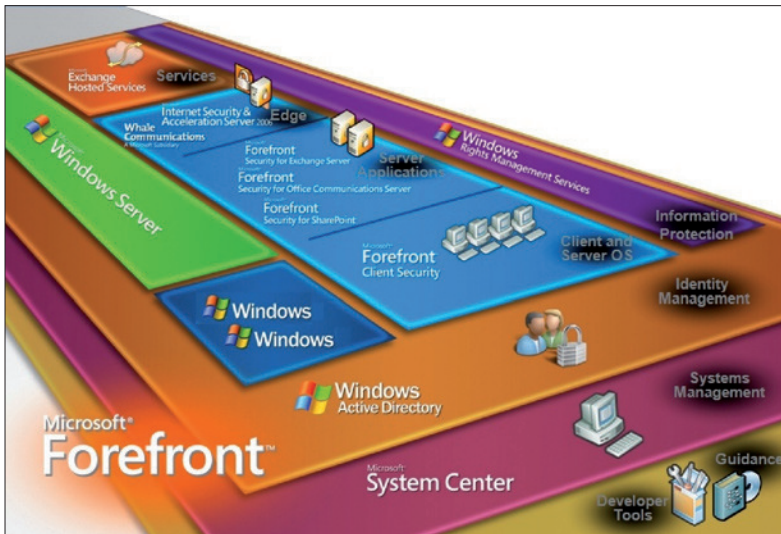
2.2.3	Konfiguration der Auslöser und der Aktionen	79
2.2.4	Pläne, Graphen und Übersichtstafeln	81
2.2.5	Import- und Export-Funktion	82
2.2.6	Eigene Elemente erstellen	82
2.2.7	Neuerungen in Zabbix 1.8.x	83
2.2.8	Dokumentation	84
2.2.9	Fazit	84
2.3	Workshop – Sichere Einwahlverbindungen mit OpenVPN auf einem Windows-Server	86
2.3.1	Kurze Beschreibung der verschiedenen VPN-Lösungen	87
2.3.2	Installation des Servers unter Windows	87
2.3.3	Community-Version der OpenVPN-Software auf einem Windows-Rechner	88
	Erzeugung der Schlüssel	88
2.3.4	Schlüssel für die Clients erzeugen	89
2.3.5	Die Datei server.ovpn	90
2.3.6	Die Datei client.ovpn	92
2.3.7	Einwahl unter Windows und Linux	93
2.3.8	Schwarze Liste für Einwahlzertifikate	94
2.3.9	Fazit	96
2.4	Sichere Einwahl: professionelle und fertige OpenVPN-Lösungen	97
2.4.1	Kurze Beschreibung der verschiedenen VPN-Lösungen	97
2.4.2	OpenVPN Access Server	97
2.4.3	Astaro Security Gateway	100
2.4.4	Linux Small Business Server eBox	101
2.4.5	IPCop	103
2.4.6	Fazit	104
2.5	UTM – H3C SecPath U200-A im ersten Test	105
2.5.1	Konfiguration per Command Line	107
2.5.2	Das Web-Interface	108
2.5.3	Trick beim Arbeiten mit dem Web-Interface	109
2.5.4	Fazit	110
3	Sicheres Windows 7	111
3.1	Windows 7 – Die neuen Sicherheitsfunktionen nutzen	111
3.1.1	Differenzierte UAC	111
3.1.2	BitLocker Festplatten-Verschlüsselung	112
3.1.3	BitLocker to Go für portable Speicher	114
3.1.4	AppLocker sperrt unerwünschte Programme	115
3.2	Windows 7 – Tipps & Tricks für Admins	118
3.2.1	Godmode – Vollzugriff auf nützliche Systemfunktionen	118
	Godmode – Neue Verknüpfungen hinzufügen	120
	Godmode in das Kontextmenü des Desktops integrieren	120
3.2.2	Explorer für Profis	122
3.2.3	Netzwerkpfade in Bibliotheken aufnehmen	122

1 Microsoft Sicherheitslösungen

Forefront ist der Gattungsname für Microsofts umfangreiche Palette unternehmensbezogener Sicherheitsprodukte. Unter dieser Bezeichnung bündelt der Softwarehersteller aus Redmond seit einigen Jahren den Großteil seiner Enterprise-Sicherheitswerkzeuge. In diesem Kapitel geben wir einen Überblick über die einzelnen Module der Forefront-Familie.

1.1 Microsoft Forefront – Sicherheitsprodukte im Überblick

Forefront ist der Sammelbegriff für Sicherheitsprodukte von Microsoft (www.microsoft.com/germany/Forefront/). Diese Palette baut der Softwarehersteller aus Redmond seit einigen Jahren beständig aus. Aus den Anfängen des Microsoft Proxy Server, der später zum ISA Server wurde, ist mittlerweile ein ganzes Set an Sicherheits-Tools geworden. Diese Sicherheitswerkzeuge stehen im Mittelpunkt dieses Beitrags. Dabei gehen wir auf die Konzepte, die Architektur und auf wissenswerte Details der Tools ein.



Im Überblick: Die Forefront-Produkte umfassen ein ganzes Set an Werkzeugen zum Schutz der Betriebssysteme, von Anwendungsservern und des Perimeters. (Quelle: Microsoft)