



TEC CHANNEL COMPACT

IT EXPERTS INSIDE

Sicherheit

Windows 7

- Client-Virtualisierung
- AppLocker & BitLocker
- Gruppenrichtlinien

Netzwerk

- **Pflicht: Log-Management**
- **Risiken beim Patch-Rollout**

Virtualisierung

- **Virtuelle Maschinen absichern**
- Backup für virtuelle Server



Die besten
Security-
Tools

Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)

Stellv. Chefredakteur / CvD: Albert Lauchner

Redaktion TecChannel:

Lyonel-Feiningerg-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 angemessene 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)

Titelbild: Andres Rodriguez – 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

Gesamtvertrieb: Josef Kreitmair

Vertrieb: Stefan Rörig

Produktion: Jutta Eckebrecht (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: 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-Feiningerg-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

Zusätzlich erschienen im tredition-Verlag

Printed in Germany

ISBN: 978-3-86850-489-7

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliothek; detaillierte bibliografische Dateien sind im Internet über <http://dnb.ddb.de> abrufbar.

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	Virtualisierung	9
1.1	Backup und Restore in virtuellen Umgebungen	9
1.1.1	Virtualisierung verknüpft Daten und Prozesse als eine Einheit	10
1.1.2	Der traditionelle Weg der agentenbasierten Sicherung	10
1.1.3	Besonderheiten bei virtuellen Systemen	11
1.1.4	Continuous Date Protection befreit vom Backup-Zeitfenster	12
1.1.5	Das Problem der Daten- und Applikations-Konsistenz	13
1.1.6	Applikationsintegration für Backup-Läufe	14
1.1.7	Sicherung durch den Host	14
1.1.8	Snapshots vereinfachen die Wartung?	15
1.1.9	VMware Consolidated Backup entlastet den ESX-Host	15
1.1.10	Backup-Software sorgt für Applikationskonsistenz	16
1.1.11	Zero Downtime Backup	17
1.1.12	Datenreduktion durch Deduplizierung	18
1.1.13	Fazit	19
1.2	Virtuelle Server gegen Ausfall absichern	20
1.2.1	Imaging von virtuellen Maschinen	20
1.2.2	Failover und Lastverteilung	21
1.2.3	Sicherung von Daten im Kontext der Prozesse	22
1.2.4	Dynamische Lastverteilung in virtuellen Umgebungen	23
1.2.5	Windows Server und Clustered Shared Volumes	24
1.2.6	Absicherung des Hyper-V durch Live-Migration	25
1.2.7	Replikation des Hyper-V in Beispielen	26
1.2.8	Sicherungsmöglichkeiten der Storage-Systeme	27
1.2.9	Absicherung des Data Centers	27
1.2.10	Fazit	28
1.3	Test: Double-Take für Hyper-V	29
1.3.1	Double-Take repliziert Server und Datenbereiche	29
1.3.2	Verschiedene Verfahren der Replikation	30
1.3.3	Zentrale Verwaltung durch die Double-Take-Konsole	31
1.3.4	Initialer Abgleich der Daten	33
1.3.5	Failover und Failback in der Praxis	34
1.3.6	Überwachungsfunktionen des aktiven Servers	35
1.3.7	Fazit	37
2	Windows	38
2.1	Gruppenrichtlinien in Windows Server 2008 R2	38
2.1.1	Neuerungen in Windows Server 2008 R2 & Windows 7	38
2.1.2	Richtlinien mit der PowerShell verwalten	39
2.1.3	Gruppenrichtlinien-Preferences effizient einsetzen	40

2.1.4	Gruppenrichtlinien verwalten	43
2.1.5	Gruppenrichtlinien konfigurieren und anwenden	44
2.1.6	Gruppenrichtlinien erzwingen und Priorität erhöhen	46
2.1.7	Vererbung für Gruppenrichtlinien deaktivieren	47
2.1.8	Anbindung von USB-Sticks steuern	48
2.1.9	Fehlerbehebung und Tools für den Einsatz von Gruppenrichtlinien	49
2.2	Neue Sicherheitsfunktionen von Windows 7	51
2.2.1	Differenzierte UAC	51
2.2.2	BitLocker Festplatten-Verschlüsselung	52
2.2.3	BitLocker to Go für portable Speicher	54
2.2.4	AppLocker sperrt unerwünschte Programme	55
2.3	Windows 7: Zusatzfunktionen und Virtualisierung	58
2.3.1	App-V virtualisiert und streamt Programme	58
2.3.2	Med-V – XP-Mode für Unternehmen	60
2.3.3	Desktop Optimization Pack (MDOP) – Zusatzfunktionen per Aufpreis	62
2.3.4	Remote-Zugriff RDP wird deutlich überarbeitet	62
2.3.5	Fazit	64
3	Netzwerk	65
3.1	Netzwerkschutz ab Layer 2	65
3.1.1	Intelligent auf Layer 2 verschlüsseln	66
3.1.2	Offensive Abwehr	67
3.1.3	Sicherheit managen	68
3.2	Praxistipps zur NAC-Einführung	69
3.2.1	Typische Probleme bei der Planung	69
3.2.2	NAC und die Geräteerkennung	70
3.2.3	Fazit NAC-Konzeption	71
3.2.4	NAC-Leitfaden	71
3.3	WLAN-Management – eine Herausforderung	72
3.3.1	Grundlagen	72
3.3.2	Herausforderungen des WLAN-Managements	73
3.3.3	Problem: Heterogene WLAN-Infrastrukturen	73
3.3.4	Hilfe durch Visualisierung und einheitliches Monitoring	74
3.3.5	Fehleranalyse im WLAN	75
3.3.6	Große Installationen im Griff	76
4	Management	77
4.1	Log-Management: Wichtige gesetzliche Pflicht für Unternehmen	77
4.1.1	Herausforderungen eines zentralen Log-Managements	77
4.1.2	Sammeln von Log-Dateien allein reicht nicht aus	79
4.1.3	Vertraulichkeit und Integrität von Log-Informationen	79
4.1.4	Sichere Ablage der Log-Dateien ist Pflicht	80
4.1.5	Log-Datei-Management als Chance	81
4.1.6	Wegsehen hilft nicht	82
4.2	Neues Datenschutzgesetz zwingt Unternehmen zum Handeln	83
4.2.1	Arbeitnehmer besser geschützt	83

4.2.2	Stärkung des Datenschutzbeauftragten	84
4.2.3	Zehn Punkte für die Auftragsdatenverarbeitung	85
4.2.4	Adresshandel wird erschwert	85
4.2.5	Fazit und Ausblick	86
4.3	Sicherheitsmeldungen: Panikmache oder fundierte Warnung?	87
4.3.1	So entsteht eine Sicherheitsmeldung	87
4.3.2	So informieren Sie sich als Nutzer	88
4.3.3	Kommunikation ist kritisch – Tipps für Hersteller	89
4.3.4	Fazit	89
4.4	Risikofaktor Patch-Management	90
4.4.1	Rollouts stets prüfen	90
4.4.2	Fehleinschätzungen durch „blindes Vertrauen“	91
4.4.3	IT-Security-Controlling – Aufgabe des Managements	92
5	Praxis	93
5.1	Notebooks sicher einsetzen	93
5.1.1	Security-Richtlinien definieren	93
5.1.2	Mitarbeiter sensibilisieren	94
5.1.3	Trau, schau, wem auf der Reise	94
5.1.4	Sichere Passwörter verwenden	94
5.1.5	Passwort vor dem Booten abfragen	95
5.1.6	Schutz über das Passwort hinaus	95
5.1.7	Ruhemodus absichern	95
5.1.8	Schnittstellen absichern	95
5.1.9	Daten verschlüsseln	96
5.1.10	Sicherheit in Gefahr	97
5.2	Notebooks: Integrierte Sicherheit ab Werk	98
5.2.1	Biometrische Verfahren	98
5.2.2	Sichere Authentifizierung	99
5.2.3	Datentresor Festplatte	100
5.2.4	Diebstahlsicherung	101
5.2.5	Die größte Gefahr sitzt vor dem Rechner	102
5.3	Notebooks und Netbooks: Zubehör und Tools für mehr Sicherheit	103
5.3.1	RFID-Chip sichert externe Festplatte	103
5.3.2	Daten-Safe mit Selbstzerstörungsmechanismus	104
5.3.3	Notebook-Tasche macht es Dieben schwer	105
5.3.4	Notebook hinter Schloss und Riegel	106
5.3.5	Seitenblicke gehen ins Leere	107
5.3.6	Tools suchen gestohlene Notebooks	107
5.3.7	Alarmsirene für das Notebook	108
5.3.8	Zeitbombe auf dem gestohlenen Notebook	109
5.3.9	Sicherheit am USB-Port	110
5.3.10	TrueCrypt versteckt sensible Daten	111
5.3.11	USB-Stick wird zum Security-Schlüssel	112
5.3.12	Funkschloss regelt Notebook ab	112
5.3.13	Daten-Crashes verhindern	113

1 Virtualisierung

Bei der Server-Virtualisierung sinkt der Wartungs- und Administrationsaufwand insbesondere für die Hardware, jedoch stellen virtuelle Umgebungen deutlich höhere Anforderungen an die Security-Strategien, denn bereits der temporäre oder dauerhafte Ausfall eines einzigen Systems kann erheblichen Ärger oder Schaden verursachen. Mit dem richtigen Ansatz, guten Werkzeugen und langfristigen Sicherheitskonzepten lassen sich virtuelle Umgebungen effektiv absichern. Praktische Tipps dazu liefert dieses Kapitel.

1.1 Backup und Restore in virtuellen Umgebungen

Vom Backup- und Restore-Techniken bis zur Sicherung der Datenbestände durch das Speichersubsystem reichen die Storage-Konzepte, wenn es darum geht, die Daten auf Abruf bereit zu halten. Auch in virtuellen Umgebungen ändern sich die Konzepte nicht. Allerdings ist die Umsetzung oftmals anders gelöst.

Das oberste Ziel für den Einsatz von IT liegt in der Bereitstellung der Daten und der Applikationen zu deren Bearbeitung. Durch unterschiedliche Konzepte zur Absicherung soll dabei eine möglichst hohe Verfügbarkeit von beiden, Daten und Programmen, erreicht werden. Um diese zu gewährleisten, werden allerdings unterschiedliche Techniken angewandt.

Damit die Daten stets verfügbar sind, greift man heute noch meist auf die traditionellen Backup-Verfahren zurück. Doch die Vorkehrungen zur Datensicherung sind weitaus vielfältiger. Sie beginnen beim Aufbau eines RAID-Plattenverbund (Webcode **401665**), ziehen sich fort über die unterschiedlichen Sicherungstechniken und enden heute bei den hierarchischen Speichersystemen und der Spiegelung der Daten mittels geeigneter Storage-Subsysteme.

Die Verfügbarkeit der Applikationen wird durch eine eigene Gruppe an Storage-Techniken erreicht. Der traditionelle Weg ist dabei, im Fehlerfall als ersten Schritt einen neuen Server aufzusetzen, um im zweiten Schritt die Datenbestände zu synchronisieren. Dieser Weg ist in jedem Fall mit einem Ausfall des entsprechenden Dienstes verbunden. Will man einen Ausfall der Dienste vermeiden, werden häufig Cluster (Webcode **456463**) als probates Mittel eingesetzt. Hinzu kommen Techniken, die die Server-Last bei einem Fehlerfall auf andere Systeme transferieren.

Das Absichern der Daten und Programme in virtuellen Umgebungen kann der Anwender durch völlig unterschiedliche Techniken erreichen. Gleiches gilt auch für die Frequenz der Datensicherung. Da sich die Daten beständig ändern, muss deren Sicherung weitaus öfter erfolgen. Programme und Rechnerprozesse hingegen sind relativ statisch. Eine laufende Sicherung erscheint daher überflüssig.