

# TEC CHANNEL

## COMPACT

IT EXPERTS INSIDE

Ratgeber

# IT-SICHERHEIT

- Auf neue Bedrohungen vorbereiten
- Managed Security Services einsetzen
- Richtige Sicherheitslösung finden

## Benutzerverwaltung

- Rechte unter Windows & Linux
- Fehler beim Identity Management
- Sicherheitseinstellungen für den IE

## Admin-Praxis

- Log-Dateien bequem auswerten
- Datenrettungs-Tools im Überblick
- Notfall-USB-Stick selbst gemacht



Windows & Linux  
absichern

# Editorial

## Keine Angst vor Cyber-Kriminalität!

Laut den Analysten von IDC und Gartner werden die Angriffe auf IT-Systeme in Unternehmen weiter zunehmen und eine neue Qualität erreichen. Die Attacken werden sich künftig konkret gegen einzelne Firmen, Abteilungen oder Personen richten und nicht mehr flächendeckend erfolgen. Doch Panik ist nicht angesagt, wie unser TecChannel-Sicherheits-Compact zeigt.



Wer die aktuellen und künftigen Bedrohungen kennt, kann diese zielgerichtet abwehren oder sich zumindest darauf vorbereiten. Wir gehen auf diese Thematik ausführlich ein und stellen wirkungsvolle Hardware- und Software-Sicherheitslösungen in Form von Tools und Appliances vor. Zusätzlich beleuchten wir den zentralen Aspekt der IT-Sicherheit, die Benutzerverwaltung. Darüber hinaus erhalten Sie in vielen Praxisbeiträgen Lösungswege unter Windows und Linux aufgezeigt, wie Sie Ihre IT-Systeme effektiv vor Angriffen von innen und von außen schützen oder die Sicherheit der Geräte erhöhen können.

Viel Spaß beim Lesen der spannenden Lektüre – und bleiben Sie stets wachsam, denn Cyber-Kriminelle schlafen nie!

**Bernhard Haluschak**  
Redakteur Hardware



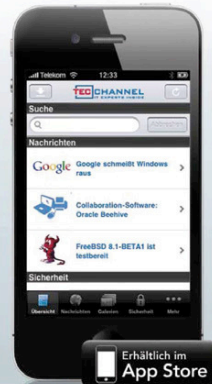
## Die neue TecChannel App

Alles drin. Immer dabei. Jetzt fürs iPhone.

News, Infos,  
Tipps & Tricks  
für unterwegs!

- ▶ topaktuelle News
- ▶ Hintergründe
- ▶ Analysen
- ▶ Tests und Bilderstrecken

[www.tecchannel.de/iphoneapp](http://www.tecchannel.de/iphoneapp)



Voraussetzungen: Kompatibel mit iPhone, iPod touch und iPad. Erfordert iOS 3.0 oder neuer.

# 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](http://www.TecChannel.de),  
E-Mail: [feedback@TecChannel.de](mailto:feedback@TecChannel.de)

**Autoren dieser Ausgabe werden bei den Fachbeiträgen genannt**

**Verlagsleitung:** Michael Beilfuß

**Copyright:** Das Urheberrecht für angenehme 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), Twentyfirst Communications (Bernd Maier-Leppla)

**Titel:** Clemens Strimmer, Jokatoons/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 Eckebrecht (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](http://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 572 72 52-276, Fax: -377, für Österreich 1/21 95 560, für Schweiz, 0 71/3 14 06-15, E-Mail: [shop@TecChannel.de](mailto:shop@TecChannel.de)

# Inhalt

	<b>Editorial</b>	<b>3</b>
<b>1</b>	<b>Trends</b>	<b>9</b>
<b>1.1</b>	<b>IT-Sicherheit 2011: Risiken in Unternehmen minimieren</b>	<b>9</b>
1.1.1	Malware und Cyber-Attacks	9
1.1.2	IT-Sicherheit – ständige Vorbereitung auf neue und alte Bedrohungen	12
1.1.3	Gefahren rechtzeitig erkennen und bekämpfen	14
1.1.4	Sicherheitsbedrohungen effektiv und wirksam abwehren	16
1.1.5	Security in Verbindung mit Cloud und Virtualisierung	18
<b>1.2</b>	<b>IT-Sicherheit 2011: Das kommt auf Admins zu</b>	<b>21</b>
1.2.1	IT-Consumerization: wenn die Nutzer eigene Hardware mitbringen	21
1.2.2	Unified Communication: Angriff auf die Kommunikation	21
1.2.3	Die sieben Todsünden beim Umgang mit der Cloud	22
1.2.4	Fazit: bekannte Probleme in neuem Umfeld	23
<b>1.3</b>	<b>Darauf müssen Sie achten – Die neuen IT-Bedrohungen</b>	<b>24</b>
1.3.1	Spear Phishing schleust Trojaner ein	24
1.3.2	Hacker-Teams organisieren Angriffe	25
1.3.3	Mobile Malware im Kommen – auch Smartphones sind bedroht	26
1.3.4	Facebook, Twitter und Co. im Visier	27
1.3.5	Next Generation Firewalls bieten mehr Schutz	28
1.3.6	Fazit: Security-Weiterbildung ist ein Muss	29
<b>2</b>	<b>Ratgeber</b>	<b>30</b>
<b>2.1</b>	<b>Lückenhafte Benutzerverwaltung ist ein Sicherheitsrisiko</b>	<b>30</b>
2.1.1	Provisorien außerhalb der Richtlinien	31
2.1.2	Eine kritische Rechtekombination	32
2.1.3	Die Prozesse sind nicht ausgereift	33
2.1.4	An den Produkten liegt es nicht	33
2.1.5	Die häufigsten Fehler beim IdM	34
2.1.6	Liste: Das sind die häufigsten Fehler	35
<b>2.2</b>	<b>Wie Benutzerrechte die Verwaltungskosten senken</b>	<b>36</b>
2.2.1	Das Benutzerobjekt und seine Rechte	37
2.2.2	Mehrfache Verwaltung führt zu hohen Verwaltungskosten	37
2.2.3	Single-Sign-on: der Universalschlüssel	38
2.2.4	Fazit	38
<b>2.3</b>	<b>Managed Security Services – Sicherheit auslagern</b>	<b>39</b>
2.3.1	Sicherheit aus dem Baukasten	39
2.3.2	Gängige Preis-Leistungs-Modelle	40
2.3.3	Unterschiedliche Ansätze, gleiches Ziel	41
2.3.4	Auch die rechtliche Sicherheit gewinnt	42
2.3.5	Backups sind Vorschrift	43

2.3.6	Hybrider Backup-Ansatz	44
2.3.7	Rechtlich sichere Partnerwahl	44
2.3.8	Fazit	45
<b>2.4</b>	<b>Rettung für Vergessliche</b>	<b>46</b>
2.4.1	Der sichere Transport	46
2.4.2	Komfort beim Management	47
2.4.3	Kollaborativ einsetzbar	47
2.4.4	Verschlüsselungssysteme	48
<b>3</b>	<b>Windows-Praxis</b>	<b>49</b>
<b>3.1</b>	<b>NTFS-Berechtigungen richtig einrichten</b>	<b>49</b>
3.1.1	Gruppen im Active Directory anlegen	50
3.1.2	Aufbau einer Beispielstruktur mit zwei Standorten	51
3.1.3	NTFS-Berechtigungen vergeben	52
3.1.4	Berechtigungen vererben	53
3.1.5	DFS-Namespace einrichten	55
3.1.6	Daten und Berechtigungen mit Robocopy umziehen	56
<b>3.2</b>	<b>Datenleck USB richtig absichern</b>	<b>57</b>
3.2.1	USB als Sicherheits-Albtraum	57
3.2.2	Daten verlassen ungewollt oder gewollt die Firma	58
3.2.3	Spezielle Lösungen und Suites sollen die Endpunkte sichern	58
3.2.4	Einsatz in Netzwerken	62
3.2.5	Kontrolle der USB-Geräte: Schnelle Hilfe durch Freeware	64
3.2.6	Auch Windows kann schützen	65
3.2.7	Gruppenrichtlinien können helfen	66
3.2.8	Das Problem existiert überall – die Lösung muss sich anpassen	67
<b>3.3</b>	<b>USB-Nutzung per Gruppenrichtlinie reglementieren</b>	<b>69</b>
3.3.1	Geräte-Identifikations-String und Gerätesetupklasse	69
3.3.2	Geräteklassen	70
3.3.3	Geräteinstallation per Gruppenrichtlinien	71
3.3.4	Gruppenrichtlinien einsetzen	72
3.3.5	Konfiguration von Gruppenrichtlinien für den	
3.3.6	Neue Gruppenrichtlinie erstellen	73
3.3.7	Richtlinien anwenden	74
<b>3.4</b>	<b>Workshop – Log-Dateien auf Windows-Systemen auswerten</b>	<b>76</b>
3.4.1	Das Problem unterschiedlicher Formate	76
3.4.2	Werkzeuge für den Weg zur richtigen Information	78
3.4.3	Der Schlüssel: Die Ereignis-ID führt zum Ziel	79
3.4.4	Übersicht wichtiger Ereignis-IDs	79
3.4.5	Nützliches Werkzeug: Filtern und eigene Sichten	80
3.4.6	Benutzerdefinierte Ansichten – Suche eingrenzen	81
3.4.7	Zugriff von der Kommandozeile und mit Hilfe der PowerShell	83
3.4.8	Log-Dateien untersuchen	83
3.4.9	Beispiele	84

4.3.3	Trinity Rescue Kit	124
4.3.4	Virenjagd mit TRK	125
	Windows-Rechner aufräumen und Passwort wiederherstellen	126
	Konsolen-Tools und weiterführende Links	126
4.3.5	SystemRescueCd	127
	Enthaltene Programme	127
	SystemRescueCd Tipps und weiterführende Informationen	128
4.3.6	Fazit	128
<b>4.4</b>	<b>Kostenlose Datenrettungs-Tools</b>	<b>129</b>
4.4.1	Reparieren mit TestDisk	129
4.4.2	Daten wiederherstellen mit photorec	130
4.4.3	Jagd auf Schadcode	131
4.4.4	Partitionen mit partimage oder FSArchiver sichern	132
4.4.5	Eine eigene Rettungsdistribution erstellen	133
4.4.6	Flexible Möglichkeiten	134
4.4.7	Fazit	135
<b>5</b>	<b>Produkte</b>	<b>136</b>
<b>5.1</b>	<b>Ratgeber UTM: Die richtige Sicherheitslösung finden</b>	<b>136</b>
5.1.1	Unified Threat Management	136
5.1.2	Viel Schutz, wenig Mühe	137
5.1.3	Sicher auch gegen Verstöße von innen	138
5.1.4	Praxisbeispiel	138
5.1.5	Auch UTM ist nicht perfekt	139
5.1.6	Dynamisches Duo	140
5.1.7	Preis/Leistung: Kaum zu schlagen	141
<b>5.2</b>	<b>Die beliebtesten UTM-Appliances</b>	<b>142</b>
<b>5.3</b>	<b>Die beliebtesten Sicherheits-Tools</b>	<b>146</b>
<b>5.4</b>	<b>Die beliebtesten Security-Suiten</b>	<b>150</b>
<b>5.5</b>	<b>Test – Blue Coat ProxyOne Security Appliance</b>	<b>154</b>
5.5.1	Details der ProxyOne Security Appliance	154
5.5.2	Erste Konfiguration der ProxyOne	156
5.5.3	Konfiguration und Analyse über die Weboberfläche	157
5.5.4	URL-Filter und Malware-Filter	158
5.5.5	Auswertung über Dashboard und Reports	160
5.5.6	Fazit	162