Februar 2012 Deutschland € 14,90 Österreich € 16,40 Schweiz SFR 29,80
www.TecChannel.de

TECCHANNEL COMPACT

IT Experts Inside

Gefahren abwehren

Der große IT-Sicherheits-Ratgeber

Die Top-Sicherheits-Tools

Windows & Office absichern

IT außer Kontrolle: Cloud & Virtualisierung

ISBN 419-5-9149-1490-4

Editorial

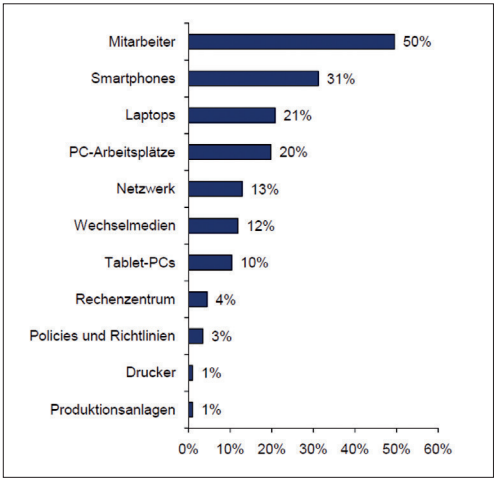
Jeder kann der Nächste sein …

Ob im Büro, daheim oder unterwegs: Es kann Sie plötzlich und unerwartet treffen. Wenn Sie es bemerken, dann ist es meistens schon zu spät, und eine Katastrophe droht. Der Grund: Ihre sensiblen, privaten und womöglich auch noch Firmendaten wurden auf Ihrem Notebook oder Smartphone durch Angreifer ausgespäht. Das ist kein seltener Fall und die Frage nach dem "Wie?" oder "Was habe ich falsch gemacht?" ist dann durchaus berechtigt.

In einer aktuellen Studie zu IT-Security in Deutschland 2011 haben die Marktforscher von IDC herausgefunden, dass der Mensch mit 50 Prozent die größte Schwachstelle für die IT-Sicherheit in einem Unternehmen darstellt. Bei der Studie wurde besonderes Augenmerk auf die Auswirkungen von steigender Mobilität und der Nutzung von Cloud-Computing-Services und Social-Media-Angeboten auf die IT-Sicherheit gelegt. Mit 31 Prozent stellen Smartphones ebenfalls ein großes Gefahrenpotenzial für die IT dar, gefolgt von Notebooks und Desktop-Arbeitsplätzen. Auch Netzwerke werden als eine signifikante Gefahr angesehen. Wie aber kann man das Security-Risiko solcher "Schwachstellen" minimieren? Dabei hilft Ihnen unsere Compact-Ausgabe.

Nur wer die möglichen Schwachstellen seiner IT-Sicherheit kennt, kann diesen wirkungsvoll begegnen. Diesem Themenkomplex haben wir ein ganzes Kapitel gewidmet und dabei auch namhafte Security-Experten befragt. Darüber hinaus stellen wir eine Fülle von Lösungen und Tools vor, die Ihre IT-Sicherheit sofort deutlich verbessern. Besonders empfehlenswert ist unser Praxisteil: Er unterstützt Sie mit vielen Schritt-für-Schritt-Beiträgen dabei, Ihre IT zu „härten" und Angreifern das Leben schwer zu machen. Ich wünsche Ihnen viel Erfolg dabei – und viele neue Erkenntnisse beim Lesen

Bernhard Haluschak
Redakteur TecChannel



IDC-Studie: Schwachstellen der Unternehmens-IT

Inhalt

	Editorial	**3**
	Inhalt	**4**
	Impressum	**162**
1	**Herausforderungen**	**8**
1.1	**IT-Sicherheit 2012: Aktuelle und künftige Security-Risiken in Unternehmen**	**8**
1.1.1	2011 – Hacktivisten und Botnetze	9
1.1.2	2012 – neue Bedrohungen durch zunehmende Mobilität	12
1.1.3	Sicherheitstrends, über die Sie Bescheid wissen müssen	14
1.1.4	Künftige Sicherheitsbedrohungen wirksam abwehren	16
1.1.5	Security-Risiken durch Cloud-Technologien	18
1.2	**Cloud untergräbt IT-Kontrolle**	**21**
1.2.1	Schatten-IT ist kein neues Problem	21
1.2.2	Die Schatten der Cloud	21
1.2.3	Schatten-IT ist näher, als man denkt	22
1.2.4	Die zentrale IT im Kontrolldilemma	22
1.3	**Security-Risiko: Virtualisierung auf dem PC**	**24**
1.3.1	Der Super-GAU: Gefahr durch die Virtualisierungssoftware?	24
1.3.2	Wo befinden sich die Gefahren?	25
1.3.3	Schwachpunkt Nummer 1: ungeschützte Virtuelle Maschinen	25
1.3.4	Schwachpunkt Nummer 2: nicht autorisierte VMs	26
1.3.5	Schwachpunkt Nummer 3: Testmaschine wieder im Netzwerk	27
1.3.6	Schwachpunkt 4: Die Integrationsdienste	28
1.3.7	Die Theorie zum Abschluss: Was ist eigentlich Virtualisierung?	29
1.3.8	Fazit: Kaum eine Gefahr – wenn die Richtlinien stimmen	30
1.4	**Das können Next Generation Firewalls**	**31**
1.4.1	Firewalls als Torwächter	31
1.4.2	Bestimmung der Firewall-Position	31
1.4.3	Netzwerkregeln bestimmen den sicheren Kommunikationsfluss	32
1.4.4	Erweiterte Funktionen zur Angriffserkennung	33
1.4.5	Protokollierung der Aktivitäten schafft Sicherheit	33
1.4.6	Generationswechsel mit Next Generation Firwalls	34
1.4.7	Die Weiterentwicklung der klassischen Firewall	35
1.4.8	Anschlüsse überwachen	35
1.4.9	Ein Dschungel an Regeln für mehr Sicherheit	35
1.4.10	Umsetzung einer Security-Anforderung in eine Regel	37
2	**Ratgeber**	**38**
2.1	**Hacker-Angriffe: Wie sie funktionieren und wer dahintersteckt**	**38**
2.1.1	Zweck von Cyber-Angriffen	39
2.1.2	Jeder Zweck hat seine Angriffsmethoden	39
2.1.3	Vorgehensweise bei Online-Angriffen	40
2.1.4	Absoluten Schutz vor Hacker-Angriffen gibt es nicht	40

2.2	**So überleben Sie Denial-of-Service-Angriffe**	**42**
2.2.1	Populäre Attacken: SYN Floods und Smurf-Angriffe	43
2.2.2	Erste Hilfe und Gegenmaßnahmen	44
2.2.3	Abwehrmaßnamen mit Bordmitteln	44
2.2.4	Hardwarebasierte Lösungen gegen DoS-Angriffe	46
2.2.5	Innovative Gegenmaßnahmen: SpeakUp und DOS Deflate	46
2.2.6	Ungewolltes Denial of Service: Wenn die Seite zu populär wird	47
2.2.7	Fazit	48
2.3	**Die 10 wichtigsten Tipps für Ihre IT-Sicherheit**	**49**
2.3.1	Tipp 1: Führen Sie eine Risikoanalyse durch	49
2.3.2	Tipp 2: Informationssicherheit beginnt von oben	49
2.3.3	Tipp 3: Passwörter und Benutzernamen einrichten	50
2.3.4	Tipp 4: Virenscanner und Firewall sind ein Muss	50
2.3.5	Tipp 5: Daten regelmäßig sichern	50
2.3.6	Tipp 6: Erstellen Sie einen Notfallplan	50
2.3.7	Tipp 7: Private E-Mail- und Web-Nutzung regeln	51
2.3.8	Tipp 8: Mobile Datenträger absichern	51
2.3.9	Tipp 9: Server und Netzwerk schützen	51
2.3.10	Tipp 10: Zugriffsregel erleichtern Administration	51
2.4	**Ratgeber Verschlüsselung: So schützen Sie Ihre Daten**	**52**
2.4.1	Der Anfang: einzelne Dateien verschlüsseln	52
2.4.2	Ganze Partitionen und Systeme verschlüsseln	53
2.4.3	Verschlüsselung mit TrueCrypt	54
2.4.4	Freeware hilft, Verzeichnisse zu verschlüsseln und zu verstecken	55
2.4.5	Lösungen fürs Firmennetz: VPN oder gleich Direct Access	56
2.4.6	Die sichere Nachricht: E-Mail-Verschlüsselung	57
2.5	**Ratgeber: Die richtige Festplatten-verschlüsselung für mobile Geräte**	**59**
2.5.1	TrueCrypt: Freeware bietet Sicherheit und viele Möglichkeiten	59
2.5.2	TrueCrypt: Voraussetzungen für den Einsatz – Grundlagen und Tipps	60
2.5.3	TrueCrypt: Die Praxis – was die Software leisten kann	61
2.5.4	TrueCrypt: Nachteile beim Einsatz der Lösung	62
2.5.5	BitLocker: Windows-Systeme mit integrierter Festplattenverschlüsselung	62
2.5.6	BitLocker: Vorausetzung für den Einsatz – Grundlage und Fallstricke	62
2.5.7	BitLocker: Und ss geht doch – komplette Verschlüsselung ohne TPM	64
2.5.8	BitLocker: weitere Voraussetzungen für den Einsatz	65
2.5.9	Die Vor-und Nachteile von BitLocker im Überblick	65
2.5.10	Festplattenverschlüsselung: Freeware oder System – die Plattform entscheidet	66
2.6	**Ratgeber: Sicher bezahlen im Web**	**67**
2.6.1	Die häufigsten Fehler	68
2.6.2	Schutz durch PCI-Compliance	68
2.6.3	Drei E-Payment-Verfahren im Vergleich	69
2.6.4	E-Payment – per Turboüberweisung zum Geld	69
2.6.5	3D Secure – Sicherheit für Webshops?	71
2.6.6	Near Field Communications – das mobile Geld der Zukunft?	72
2.7	**VMware vShield: Cloud- und virtuelle Umgebungen absichern**	**74**
2.7.1	Virtuelle Security Appliances agieren in virtuellen Maschinen	74
2.7.2	vShield Zones	75

2.7.3	vShield Edge	76
2.7.4	vShield App	77
2.7.5	Firewall-Regeln	77
2.7.6	vShield Endpoint	78
2.7.7	vShield Manager	78
2.7.8	Integration des vShield Manager in den vCenter-Server	79
3	**Praxis**	**80**
3.1	**Windows-Praxis: Sicherheit per Gruppenrichtlinien**	**80**
3.1.1	Zugriff auf Wechselmedien regulieren	80
3.1.2	Eine neue Gruppenrichtlinie für sichere Kennwörter erstellen	82
3.1.3	Automatischen Neustart nach Updates deaktivieren	83
3.1.4	Windows bei ungültigen Anmeldeversuchen automatisch sperren lassen	84
3.1.5	Programme mit AppLocker sperren	84
3.1.6	Benutzerkontensteuerung konfigurieren	86
3.1.7	Bildschirmschoner mit Kennwortschutz aktivieren	86
3.1.8	BitLocker-Laufwerksverschlüsselung aktivieren – ohne TPM	87
3.1.9	Überwachung von Dateisystemzugriffen aktivieren	87
3.1.10	Firewall-Einstellungen über Gruppenrichtlinien setzen	89
3.1.11	Tunneln beim Einsatz von DirectAccess erzwingen	89
3.2	**Office 2010 sicher mit Gruppenrichtlinien betreiben**	**91**
3.2.1	Gruppenrichtlinienvorlagen verstehen	91
3.2.2	ADMX- und ADML-Dateien installieren	92
3.2.3	Neue Gruppenrichtlinien erstellen	92
3.2.4	Office-2010-Richtlinieneinstellungen setzen	93
3.2.5	Geschützte Ansicht aktivieren und gefährliche Dateien blockieren	94
3.2.6	Zugriffschutz steuern – gefährliche Dateien aussperren	94
3.2.7	Gruppenrichtlinie verknüpfen	96
3.2.8	Erweiterte Sicherheitseinstellungen setzen	97
3.2.9	Das Microsoft-Office-Anpassungs-Tool	97
3.3	**Outlook 2010 – mit Postfachberechtigungen arbeiten**	**99**
3.3.1	Benutzerberechtigungen in Outlook konfigurieren	99
3.3.2	Rechtevergabe in Outlook	101
3.3.3	Auf freigegebene Ordner und Postfächer zugreifen	102
3.3.4	Stellvertreter in Outlook definieren	103
3.3.5	Zusätzliche Postfächer in Outlook öffnen	104
3.3.6	E-Mails im Auftrag anderer Anwender senden	105
3.3.7	Berechtigungen in der Exchange-Verwaltungs-Shell setzen	105
3.4	**Workshop: Konfiguration der Netgear ProSecure UTM9S Security Appliance**	**107**
3.4.1	Die UTM9S im Detail	107
3.4.2	Einfaches Setup durch Assistenten	108
3.4.3	Interaktives Setup	109
3.4.4	Manuelles Feintunig der Konfiguration	112
3.4.5	Optionale Erweiterungen durch Einschubmodule	113
3.5	**Workshop: Symantec Critical System Protection**	**115**
3.5.1	ESX-Hosts mit Symantec Critical System Protection überwachen	115
3.5.2	Die Systemanforderungen	116
3.5.3	Die Verwaltungskonsole des Security-Systems	116

1 Herausforderungen

Vernetzte Infrastrukturen und das Internet transportieren Informationen binnen Sekunden um die Welt und machen unternehmenswichtige Daten global verfügbar. Der Schutz digitaler Unternehmensinformationen und persönlicher Daten ist deshalb wichtiger denn je. Moderne IT-Systeme sollen Daten jederzeit, schnell und unbegrenzt bereitstellen, jedoch jeden unerlaubten Zugriff verhindern. Die Einrichtung umfassender Sicherheits-Policies ist daher eine der wichtigsten Aufgaben für IT-Entscheidungsträger und Administratoren.

1.1 IT-Sicherheit 2012: Aktuelle und künftige Security-Risiken in Unternehmen

Das Thema IT-Security hielt im Jahr 2011 alle Verantwortlichen gewaltig auf Trab. Eine Fülle neuer Angriffe durch Botnetze, Malware, Trojaner und Pishing-Attacken bedrohte die Unternehmensdaten beziehungsweise -kommunikation. Eines hat sich im Bereich Security herauskristallisiert: Die Angreifer setzen immer auf „Qualität statt Quantität“, da sie gezielt Informationen in Firmen suchen, die sich zu Geld machen lassen. Das bedeutet für die Unternehmen, dass sie noch wachsamer sein müssen als bisher, da jeder Angriff auf sensible Firmendaten einen hohen wirtschaftlichen Verlust nach sich ziehen könnte. Ungeachtet der Planung neuer Security-Konzepte muss der IT-Verantwortliche allerdings darauf achten, dass er die herkömmlichen Abwehrmaßnahmen nicht vernachlässigt.

Worauf sich der Administrator und der Anwender in Bezug auf die künftigen Sicherheitsbedrohungen einstellen müssen, darüber geben die folgenden namhaften Security-Unternehmen Auskunft.

Zusätzlich erörtern die Sicherheitsspezialisten, welche Sicherheitsrisiken das Jahr 2011 geprägt haben und wie die steigende Zahl mobiler Geräte wie Smartphones, Tablets oder Notebooks sowie die Technologien Cloud, Social Media und andere Trends die Sicherheit in den Unternehmen im Jahr 2012 beeinflussen werden.

- **Markus Hennig**, CTO bei Sophos / Astaro (www.sophos.com)
- **Sascha Krieger**, Head of Corporate Communications bei eleven (www.eleven.de)
- **Stefan Ortloff**, Virus Analyst bei Kaspersky Lab (www.kaspersky.com/de/)
- **Toralv Dirro**, Security Strategist bei McAfee (www.mcafee.com/de/)
- **Thomas Hemker**, Principal Systems Engineer bei Symantec (www.symantec.de)
- **Raimund Genes**, CTO bei Trend Micro (www.trendmicro.com)