Dezember 2012 Deutschland € 15,90 Österreich € 17,90 Schweiz SFR 29,80
www.TecChannel.de

TECCHANNEL COMPACT

IT EXPERTS INSIDE

Sicherheit

PRAXIS ■ RATGEBER ■ TIPPS ■ TESTS

Mobile

- Sicherheitsrisiken erkennen
- Tablets und Smartphones einbinden
- Mehr Sicherheit mit Richtlinien

Cloud

- Kritische Dienste richtig auslagern
- Identity- und Access-Management integrieren
- Cloud Security Services im Check

Server

- Virtuelle Systeme überwachen und sichern
- IT-Infrastrukturen vor Ausfällen schützen

E-Mails richtig sichern

TECCHANNEL SILBER-PAKET

PRINT MEETS WEB

DAS INTELLIGENTE KOMPLETTPAKET

Jetzt 17% sparen!

Im neuen Silber-Paket beziehen Sie 8 Ausgaben TecChannel Compact versandkostenfrei, profitieren zusätzlich durch exklusiven Premium Content im Web, wählen aus einer Vielzahl hochwertiger Prämien und sparen deutlich gegenüber den Einzelpaketen.

Gratis für Sie

Prämienbeispiel: Lithium-Ionen-Schrauber von Bosch

Weitere Informationen zum TecChannel Silber-Paket finden Sie unter

www.tecchannel.de/silber

TecChannel erscheint im Verlag IDG Business Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg. Die Kundenbetreuung erfolgt durch den TecChannel Kundenservice, ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John, Tel.: 0180 5 72 7252-276 *, E-Mail: shop@tecchannel.de
(*aus dem dt. Festnetz nur 0,14 Euro pro Minute, Mobilfunkpreise max. 0,42 Euro pro Minute)

C-10-157

Inhalt

	Editorial	**3**
1	**Mobile**	**8**
1.1	**Sicher mobil arbeiten – eine Herausforderung für IT-Verantwortliche**	**8**
1.1.1	Mobile Endgeräte auf dem Vormarsch	10
1.1.2	Mobile Device Management steuert mobile Endgeräte	11
1.1.3	Mobile Device Management entlastet IT-Administration	11
1.1.4	ByoD: Mobilität verändert das Arbeitsverhalten	12
1.1.5	Helfer aus der Cloud	13
1.1.6	Transparenz und Sicherheit schaffen	13
1.1.7	Compliance und Sicherheit gewährleisten	14
1.1.8	IT-Prozesse für mobile Endgerätenutzung durchleuchten	15
1.2	**Studie: Privat-IT birgt Sicherheitsrisiken in Unternehmen**	**16**
1.2.1	IT-Security-Risiko: Facebook und Co.	17
1.2.2	SaaS und Cloud gefährden kritische Daten	18
1.3	**Sicherheitsstandards für mobile Geräte fehlen in Unternehmen**	**19**
1.3.1	Angriffe auf die IT-Systeme gelten als reale Gefahr	20
1.4	**Mobile Geräte: die Minimalstandards für Sicherheit**	**22**
1.4.1	Mobile-Governance-Richtlinien einführen	22
1.4.2	Mobile Geräte zentral und einheitlich verwalten	23
1.4.3	Nur geprüfte Apps verwenden	23
1.5	**Die Gefahren durch Dropbox, ByoD & Co.**	**24**
1.5.1	Sicherheitsrisiko Online-Speicher- und File-Sharing-Dienste	24
1.5.2	Mitarbeiter kennen die Gefahren	25
1.5.3	Prognosen für 2013	25
1.5.4	Fazit: trübe Aussichten für Virtualisierung und Cloud	26
1.6	**Bei ByoD fehlen dedizierte Sicherheitsregeln**	**27**
1.6.1	ByoD macht Mitarbeiter produktiver	27
1.6.2	Probleme mit der Compliance	28
1.6.3	Datenverluste programmiert	28
1.6.4	Mobile Schatten-IT blüht auf	29
1.7	**Studie: Mitarbeiter-Tablets soll man nicht überwachen**	**30**
1.7.1	Datenschutzansatz überdenken	30
1.7.2	Baustelle Mitarbeiter-Monitoring	31
1.7.3	Vorsicht bei Flash Cookies	32
1.8	**Mit Verschlüsselung Daten auf Desktops, Notebooks und Smartphones sichern**	**33**
1.8.1	Der sichere Datentransport	34
1.8.2	Komfort beim Management ist Pflicht	35
1.8.3	Kollaborativ einsetzbar	36
1.8.4	Verschlüsselungssysteme	36
1.9	**Sicherheitsrisiko App-Stores**	**37**
1.9.1	Gefährliche Schwachstellen in App-Stores	37
1.9.2	ENISA-Empfehlung teils nicht umgesetzt	37
1.9.3	Risiko 1: falsche Identität des App-Entwicklers	37
1.9.4	Risiko 2: unsichere Anmeldung des App-Entwicklers	39
1.9.5	Risiko 3: manipulierte App-Bewertungen	40
1.9.6	Risiko 4: unzureichende App-Reviews	41

1.9.7	Mehr App-Sicherheit: Angebote für Betreiber	41
1.9.8	Mehr App-Sicherheit: Lösungen für Nutzer	41
1.9.9	App-Store-Sicherheit im Überblick	42
1.10	**Sicherheitsrisiko – Biometrische Technologien auf Smartphones und Tablets**	**43**
1.10.1	Unbestechliche Biometrie	44
1.10.2	Identifikation per Fingerdruck	44
1.10.3	Datenschutz einhalten	44
1.11	**NFC auf dem Prüfstand – Technik und Sicherheit**	**45**
1.11.1	Schutz durch Secure Element	46
1.11.2	MicroSD-Karte nachrüsten	47
1.11.3	NFC-Adapter für Apple-User	47
1.11.4	NFC-Dienste brauchen Sicherheit	48
1.12	**Schwachstellen-Scanner für Smartphones und Tablets**	**49**
1.12.1	Jedes zweite Android-Smartphone betroffen	49
1.12.2	Fehlerbehebungen lassen auf sich warten	50
1.12.3	Schwachstellen-Scanner auch für mobile Geräte	50
1.12.4	Schwachstellen-Scanner speziell für Android	51
1.12.5	Risikoanalyse für Schwachstellen inklusive	52
1.12.6	Die „Schwachstelle“ Mensch nicht vergessen	53
1.12.7	Auch die Apps haben Schwachstellen	54
1.12.8	Auf den Lückenschluss kommt es an	55
1.12.9	Nicht ohne weitere mobile Sicherheitslösung	55
2	**Cloud und Server**	**56**
2.1	**Mehr Sicherheit im Unternehmen durch Cloud Computing**	**56**
2.1.1	Cloud-Computing-Strategie spart Geld	56
2.1.2	Security auf dem neuesten Stand	57
2.1.3	Cloud-Dienste decken Compliance ab	57
2.1.4	Sicherheitsmaßnahmen aus der Wolke	57
2.1.5	Projektverantwortung klar definieren	58
2.2	**Experten – Sicherheitsgefahren in der Cloud sind real**	**59**
2.2.1	Die Kontrolle über die Daten gehört nicht in fremde Hände	59
2.2.2	Apple und Amazon sind nicht sicher	59
2.2.3	Verschlüsselung hilft mehr als ein bloßes Backup	60
2.2.4	Falsche Prioritäten vermeiden	61
2.2.5	Sich nicht auf Hype- und Marketing-Gehabe einlassen	61
2.3	**Ratgeber – kritische Funktionen in die Cloud auslagern**	**62**
2.3.1	Die zehn größten Security-Risiken in der Cloud	63
2.3.2	Auslagern in die Public Cloud: So sollten Sie vorgehen	64
2.3.3	Diese Sicherheitsmaßnahmen sollten Sie treffen	67
2.3.4	Fazit: IT-Sicherheit und Cloud sind kein Widerspruch	68
2.4	**Serverinfrastrukturen wirksam vor Ausfällen schützen**	**69**
2.4.1	Auf die Größe kommt es an	69
2.4.2	Keine Sicherheit ohne Qualität	69
2.4.3	Netzwerk und Netzbetreiber	70
2.4.4	Permanente Verfügbarkeit ist das A und O	70
2.4.5	Service und Support	70
2.4.6	Fazit	71
2.5	**Darauf müssen Sie bei der Absicherung virtueller IT-Infrastrukturen achten**	**72**
2.5.1	Virtuelle Security-Appliances agieren in virtuellen Maschinen	72
2.5.2	Host absichern	73

2.5.3	Die Patch-Verteilung bei virtuellen Systemen	74
2.5.4	Host gegen Ausfall absichern	74
2.5.5	VMs durch das Host-System sichern	75
2.5.6	Storage-Ausfälle und -Engpässe durch Migration absichern	76
2.5.7	Netzwerkanbindung optimieren	77
2.6	**Mobile IT, Cloud Computing, IPv6 & Co. beeinflussen die Netzwerksicherheit**	**79**
2.6.1	Mobile Netzwerke, VPNs und Roaming	79
2.6.2	Gezielte Angriffe und APTs	79
2.6.3	Konsumerisierung und ByoD	79
2.6.4	Schutz von Webanwendungen und Webservern	80
2.6.5	Umstellung auf IPv6	80
2.6.6	Cloud Computing und SaaS	80
2.6.7	Trend zur Verschlüsselung	80
2.6.8	Das elastische Netz	81
2.7	**Identity- und Access-Management in der Cloud richtig anwenden**	**82**
2.7.1	Auf gute Zusammenarbeit	83
2.7.2	Brückenbau in die IT-Wolke mit Identity Federation	84
2.7.3	Federation-Vorreiter Autoindustrie	84
2.7.4	IAM richtig umsetzen	85
2.8	**Security-Mythen auf dem Prüfstand**	**86**
2.9	**Cloud Security Services im Check**	**90**
2.9.1	Trend Micro SafeSync for Business: sicherer Speicher in der Wolke	91
2.9.2	F-Secure Software Updater: immer auf dem aktuellen Stand	93
2.9.3	Check Point Threatcloud: Reputationsdienste aus dem Netz	94
2.9.4	Trend Micro Smart Protection Network: das Wissen der vielen	95
2.9.5	Bitdefender Safego: soziale Anwendungen schützen	96
3	**Praxis**	**97**
3.1	**Mit VMware vShield vSphere-Umgebungen absichern**	**97**
3.1.1	Der vShield Manager	98
3.1.2	Applikationsschutz durch vShield App	98
3.1.3	Der Grenzwall in vShield Edge	99
3.1.4	Schutz der virtuellen Maschinen durch vShield Endpoint	99
3.1.5	vShield Manager in den vCenter Server integrieren	100
3.1.6	Die virtuelle Appliance des vShield Managers starten	102
3.1.7	Konfiguration mittels Verwaltungskonsole	104
3.2	**Hyper-V und vSphere mit Veeam One Free Edition überwachen**	**105**
3.2.1	Veeam One installieren und einrichten	105
3.2.2	Fehler auslesen und Lösungen erhalten	106
3.2.3	E-Mails automatisiert zusenden lassen	107
3.2.4	Business View und Alarme verwalten	107
3.2.5	Berichte mit Veeam One erstellen und Weboberfläche nutzen	108
3.2.6	Echtzeitüberwachung der Ereignisprotokolle mit EventSentry	109
3.2.7	Mehrere Ping-Anfragen dauerhaft durchführen und überwachen	109
3.3	**Virtuelle Exchange-Server mit Veeam Backup Free Edition sichern und wiederherstellen**	**110**
3.3.1	Veeam Backup Free Edition im Überblick	110
3.3.2	Veeam Explorer für Microsoft Exchange	111
3.3.3	Veeam Backup Free Edition installieren	112
3.3.4	Hyper-V, VMware und System Center Virtual Machine Manager anbinden	112
3.3.5	Virtuelle Server mit VeeamZIP sichern	114
3.3.6	Daten und virtuelle Server aus Veeam Backup wiederherstellen	114
3.3.7	Veeam Backup verwalten und erweiterte Funktionen nutzen	115

3.4	**Mit Trend Micro Deep Security IT-Infrastrukturen absichern und überwachen**	**116**
3.4.1	Sicherheit mit oder ohne Agenten	117
3.4.2	Infrastrukturintegrität überwachen	118
3.4.3	Eindringlinge erkennen und abwehren	119
3.4.4	Angriffsfläche reduzieren	119
3.5	**Workshop – Trend Micro Deep Security richtig konfigurieren**	**120**
3.5.1	Clients in Deep Security einbinden	120
3.5.2	Policy bestimmen den Sicherheits-Level	121
3.5.3	Die Sicherheitsmodule von Deep Security	122
3.5.4	Alerts, Event und Reports	123
3.5.5	Das Dashboard	124
3.6	**Workshop: SSL Stripping erkennen und bekämpfen – Grundlagen und Hintergründe**	**125**
3.6.1	Theorie und Praxis – Zertifizierung mit SSL Stripping umgehen	126
3.6.2	Der MITM-Angriff auf ungesicherte Verbindungen	127
3.6.3	Vertrauensbasis durch TLS-Verschlüsselung	128
3.6.4	Schwachstellen der TLS	129
3.7	**Workshop: SSL Stripping erkennen und bekämpfen – Abwehr**	**130**
3.7.1	Von der Theorie zur Praxis	130
3.7.2	Ergebnisse des Angriffs auf verschiedene Verbindungen	131
3.7.3	Vielfältige Lösungen für Löcher im ARP-Konzept	132
3.7.4	Maßnahmen gegen SSL Stripping: ein Experiment	133
3.7.5	Fazit	135
3.8	**Workshop: Sophos Computer Security Scan**	**136**
3.8.1	Endpunkt einrichten, Report erstellen	137
3.8.2	Fazit	138
3.9	**So sichern Sie Ihre E-Mails ab**	**139**
3.9.1	Wie sicher ist der Inhalt einer E-Mail?	139
3.9.2	Reicht eine AV-Lösung auf dem System zum Schutz der E-Mail?	140
3.9.3	Wie kann ich E-Mail-Nachrichten sicherer versenden?	140
3.9.4	Security auch für Thunderbird	141
3.9.5	Warum sollte man keine HTML-Nachrichten verwenden?	142
3.9.6	Welche Sicherheitseinstellungen sind bei Outlook sinnvoll?	143
3.9.7	Ist vom Einsatz einer Web-Mail-Lösung grundsätzlich abzuraten?	144
3.9.8	Last but not least: sichern, sichern, sichern …	145
4	**Test**	**147**
4.1	**Test: Sicherheitslücken mit Nessus 5 aufspüren**	**147**
4.1.1	Installation und Oberflächenwahl	148
4.1.2	Scan durchführen	149
4.1.3	Scan-Ergebnisse auswerten	151
4.1.4	Policies erstellen und Plugins auswählen	152
4.1.5	Fazit	153
4.2	**Sophos UTM110/120 im Test**	**155**
4.2.1	Gerätedetails und Schnittstellen	155
4.2.2	Erste Konfiguration der UTM	156
4.2.3	Updates und neue Lizenzen	157
4.2.4	WLAN-Access-Points installieren	157
4.2.5	Funktionen und Features	158
4.2.6	Fazit	159
5	**Anhang: Die beliebtesten Sicherheits-Artikel (QR-Codes)**	**161**
	Impressum	162

1 Mobile

Mobile Endgeräte verändern die Sicherheitsanforderungen an die eigene IT-Infrastruktur nachhaltig. Einmal, weil mobile Benutzer IT-Dienste, Anwendungen und Daten über drahtlose Netzwerke fast wie stationäre Anwender verwenden wollen. Zum anderen, weil mobile Endgeräte in großer Produktvielfalt zum Einsatz kommen und raschen Innovationszyklen unterworfen sind.

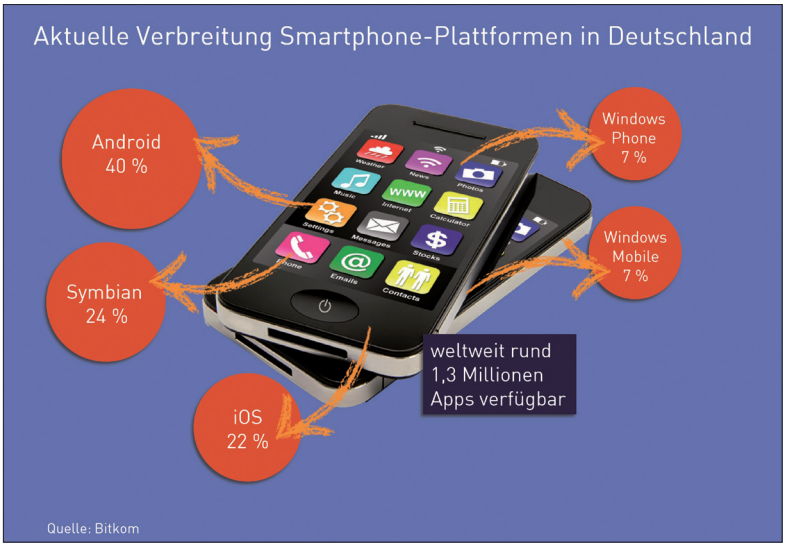
1.1 Sicher mobil arbeiten – eine Herausforderung für IT-Verantwortliche

Der digitale und mobile Arbeitsplatz der Zukunft stellt steigende Anforderungen an die IT-Verantwortlichen. In diesem Kontext sind neue IT-Strukturen und -Konzepte gefragt. Wir erläutern, welche Voraussetzungen die IT-Abteilungen für die sichere Nutzung von Smartphones und Tablets erfüllen müssen.

In der Vergangenheit hat die Unternehmens-IT maßgeblich die technologischen Entwicklungen vorangetrieben, und Endanwender haben die vielfältigen Innovationen in den privaten Bereich übernommen. Heute hat sich das Bild gewandelt: Viele Neuerungen, die das gesellschaftliche Miteinander beeinflussen, werden zuerst im privaten Bereich eingesetzt. Hierzu gehören die Nutzung sozialer Medien und mobiler Endgeräte, der Einsatz von Cloud-Diensten und eine Always-On-Mentalität.

Achtung: Die zunehmende Nutzung mobiler Geräte in einem Unternehmen schafft Probleme. (Quelle: Materna)

Privat sind die Nutzer meist mit leistungsfähigeren Geräten ausgestattet als am Arbeitsplatz. Die Folge: Mitarbeiter erwarten auch an ihrem Arbeitsplatz aktuelle Kommunikationstechnologien, Social-Media-Zugänge und einen produktivitätssteigernden Mix aus innovativen Cloud-Angeboten. Diese Entwicklung zwingt die Unternehmen zum Handeln, wollen sie auch künftig attraktive Arbeitsplätze insbesondere für die jüngere Generation anbieten.



Mobiler Wettbewerb: Nach einer aktuellen Bitkom-Studie ist Android zurzeit die populärste Smartphone-Plattform in Deutschland. (Quelle: Materna/Bitkom)

Der Arbeitsplatz der Zukunft setzt sich aus verschiedenen Elementen zusammen. Die Herausforderung liegt darin, die unterschiedlichen Technologien in geeigneter Weise in die vorhandene IT-Infrastruktur einzufügen. Die zunehmende Vernetzung sowie die Nutzung eigener Geräte erfordern eine geordnete und abgesicherte Integration von Mensch und Technik. Flexibel nutzbare Arbeitsplätze benötigen zudem neue Kommunikationswege wie Mitarbeiterportale und Collaboration-Plattformen. Eine ergonomische Arbeitsplatzumgebung, die eng mit Kundenserviceprozessen verbunden ist, rundet das Bild des Arbeitsplatzes der Zukunft ab.

Auch räumlich verteilte oder international arbeitende Teams müssen in die neuen Arbeitsmodelle integriert werden. Damit steigen die Anforderungen an eine flexible und mobile Nutzung der Devices. Das eigene mobile Endgerät muss dabei genauso einfach und sicher integrierbar sein wie PC oder Notebook. Diese Vielfalt an Technologien erfordert ein effizientes Arbeitsplatzmanagement, ein durchgängiges User- und Access-Management sowie eine sichere, virtuelle IT-Architektur.

1.1.1 Mobile Endgeräte auf dem Vormarsch

Mobile Endgeräte wie Smartphones und Tablet-PCs werden immer leistungsfähiger. Sie verdrängen zunehmend Festnetz- und klassische Mobilfunktechnologien. Die Nutzung der mobilen Begleiter hat sich aus dem privaten Bereich rasant in die Arbeitswelt ausgebreitet. Für die Anforderungen der Unternehmen an Datenschutz und Compliance sind viele der Geräte aber noch gar nicht ausgelegt. Beispielsweise fehlen Funktionen, die den Geräten Policies zuweisen und bestimmte Sicherheitseinstellungen durchsetzen.

Kampfansage: Smartphones und Tablets verdrängen immer mehr den traditionellen Desktop-PC beim Zugriff auf das Internet. (Quelle: Materna)

Hinzu kommt das fehlende Bewusstsein der Anwender für Sicherheitsaspekte des Unternehmens. Beispielsweise kommuniziert ein Großteil der Apps unverschlüsselt miteinander. Android-Geräte sind dafür bekannt, dass sich einige Apps untereinander austauschen, dem Endgerät Profile zuweisen oder Anwendungen zusenden können. Wer sich geschickt tarnt, kann so den Nutzer dazu verleiten, ein schadhaftes Profil als Update eines vertrauten Anbieters zu akzeptieren und dieses zu installieren.

Einige Hersteller haben das Gefährdungspotenzial erkannt und entwickeln Antivirenlösungen auch für mobile Endgeräte. Da Antivirensoftware in der Regel signaturbasiert und ohne Verhaltenserkennung arbeitet, identifizieren die mobilen Geräte nur einen Bruchteil der bereits bekannten Schadsoftware. Erstmals auftretende Malware wird vielfach nicht erkannt. Jedoch arbeiten die Hersteller bereits intensiv an Lösungen, die mit der Desktop-Welt vergleichbar sind.

1.1.2 Mobile Device Management steuert mobile Endgeräte

Unternehmen möchten smarte Mobilfunkgeräte in vollem Umfang nutzen, ohne dabei die Sicherheit der Unternehmensdaten zu beeinträchtigen. Daher setzen IT-Abteilungen auf ein effizientes Mobile Device Management (MDM) und steuern so ihre mobilen Endgeräte zentral und sicher. Darüber hinaus können MDM-Lösungen Hard- und Softwareinventarisierung übernehmen, Policies erzwingen oder Fernwartung ermöglichen.

Das Management mobiler Endgeräte ähnelt in Teilen dem klassischen Client-Management: In den vergangenen rund 15 Jahren wurden Dutzende von Lösungsansätzen entwickelt, um PCs kostengünstig zu betreiben. Auch beim Management der mobilen Endgeräte sind die Hersteller wieder den gleichen Weg gegangen: Nachträglich müssen Lösungen zum Management der Geräte integriert werden. Es wurde versäumt, diese von Anfang an zum Bestandteil der neuen Geräte zu machen. Beispielsweise muss für eine lückenlose Systemverwaltung bekannt sein, welche Geräte mit welcher Software und welcher Konfiguration im Einsatz sind, um eine sichere Integration in die IT-Infrastruktur zu ermöglichen. Die Anforderungen enden hier jedoch nicht, denn sie gehen weit über das klassische Client-Management hinaus, da es sich um einen sehr heterogenen Markt mit ganz unterschiedlichen Hardwareplattformen handelt.

MDM-Verfahren setzen voraus, dass alle Geräte auf dem MDM-Server registriert sind. Daher meldet sich ein Anwender zunächst an einem Self-Service-Portal an und registriert dort seine Hardware. Daraufhin werden die jeweiligen Compliance-Richtlinien und Sicherheitseinstellungen auf das Gerät verteilt. Je nach Betriebssystem sind die Möglichkeiten zur Gerätekonfiguration via MDM unterschiedlich: iOS-Geräte erhalten die Sicherheitseinstellungen beispielsweise in Form von Konfigurationsprofilen, die nach Anmeldung des Geräts im Self-Service-Portal übertragen werden. Bei Android hingegen ist eine App notwendig, die der Nutzer als Geräteadministrator bestätigen muss. Erst danach darf die App Einstellungen auf dem Gerät durchführen.

1.1.3 Mobile Device Management entlastet IT-Administration

Mit einer MDM-Lösung erfassen Unternehmen automatisiert und zentral die Gerätekonfigurationen und können Profile und Richtlinien, spezifisch für die eingesetzten Plattformen, auf die Geräte verteilen, um so den Compliance- und Sicherheitsanforderungen zu entsprechen. Das MDM-System unterstützt den Administrator bei der Konfiguration der Geräte und erkennt, welche Änderungen der Nutzer an seinem Gerät vorgenommen hat, welche Applikationen vorhanden sind und welche Netzwerkeinstellungen bestehen.

Erst wenn alle Sicherheitsanforderungen erfüllt sind, wird ein Zugriff auf das Firmennetz gewährt. Solche Regeln besagen beispielsweise, dass ein sicheres Kennwort und der Displayschutz eingerichtet sein müssen. Auch kann konfiguriert

werden, dass der Anwender nur dann E-Mails vom Mail-Server abrufen darf, wenn er mit einem registrierten Gerät zugreift und dort bestimmte Sicherheitseinstellungen erfolgt sind. Ist ein Gerät nicht mehr konform mit den Richtlinien, bekommt es auch keine E-Mails mehr. Darüber hinaus lassen sich Maßnahmen wie beispielsweise Sperren oder Löschen (Wipen) des Gerätes bei Verlust oder Diebstahl einleiten. Die IT-Abteilung wird insgesamt entlastet, da der Endanwender das Sperren beziehungsweise Löschen des Gerätes über das Portal selbst einleiten kann und die IT-Abteilung nicht eingreifen muss.

Auch der Aufbau eines eigenen Enterprise App Stores ist mit vielen MDM-Plattformen möglich, beispielsweise mit der Lösung SmartMan des Dortmunder Unternehmens Dialogs, das seit April 2012 zum Security-Spezialisten Sophos gehört und das Tool jetzt als Sophos Mobile Control den Anwendern zur Verfügung steht. Ein Enterprise App Store hat den Vorteil, dass unternehmenseigene Apps ohne Einbeziehen der Gerätehersteller verteilt werden können. Darüber hinaus kann das Unternehmen seinen Mitarbeitern weitere nützliche Apps bereitstellen, ohne dass der Anwender danach suchen muss.

Beim Einsatz von MDM bleiben die Nutzer von Smartphones und Tablet-PCs weiterhin „Herr“ ihrer Geräte. Der Anwender könnte also je nach Endgerät jederzeit die MDM-Konfigurationsprofile oder die App vom Gerät entfernen. Der Nutzer schließt sich damit automatisch aus der Unternehmenskommunikation aus und stellt keine Sicherheitsgefahr dar. Die IT-Administration erhält durch MDM die Möglichkeit, Fehlkonfigurationen mittels Monitoring zu erkennen und Zugänge zu Unternehmensressourcen für die betreffenden Geräte zu sperren beziehungsweise bei bestimmten Richtlinienverletzungen automatisiert sperren zu lassen.

1.1.4 ByoD: Mobilität verändert das Arbeitsverhalten

Privat- und Arbeitsleben vermischen sich in vielen Berufen immer mehr. Damit steigt die Produktivität der Mitarbeiter, da sie von ihren mobilen Endgeräten jederzeit auf Unternehmensapplikationen und -daten zugreifen können. MDM ebnet daher einem weiteren Bestandteil des Arbeitsplatzes der Zukunft den Weg: Bring Your Own Device (ByoD), die Integration privater Endgeräte in das Unternehmensnetzwerk.

Private Endgeräte lassen sich zwar auch ohne MDM-Technologien integrieren, doch sinkt das Sicherheitsrisiko deutlich, wenn auch diese Geräte in der Obhut der IT-Administration sind. ByoD wirft darüber hinaus auch rechtliche Fragen auf, beispielsweise bezüglich Haftung, Datenschutz, Trennung von Privat- und Firmendaten, Arbeitsrecht und Lizenzen. Unternehmen haben zum Beispiel das Bundesdatenschutzgesetz zu berücksichtigen. Dazu müssen sie die Hardware, die auf das Unternehmensnetzwerk zugreift, aber zumindest verwalten dürfen – also auch private Endgeräte. Die Entwicklung von ByoD steht in Deutschland erst am Anfang, sodass noch keine ausgereiften Antworten vorliegen, wie beispielsweise mit Daten auf privaten Endgeräten umgegangen werden darf. Viele Analysten sind

sich jedoch einig, dass sich dieser Trend langfristig durchsetzen wird und die IT-Abteilung die Antworten darauf entwickeln muss.

Visionen: Der Arbeitsplatz der Zukunft nutzt zahlreiche neue Technologien. (Quelle: Materna)

1.1.5 Helfer aus der Cloud

Neben den mobilen Endgeräten schleichen sich quasi nebenbei auch Cloud-Dienste als selbstverständliche Helfer in das Arbeitsleben. Cloud-Datenspeicher ermöglichen den schnellen und einfachen Datenaustausch in Teams und werden immer häufiger ohne Rücksicht auf Unternehmensrichtlinien genutzt.

So nehmen beispielsweise Übersetzungsdienste in der Cloud geschäftskritische Texte entgegen und verarbeiten sie dezentral irgendwo auf der Welt. Soziale Netzwerke, in denen sich Kommunikationsmechanismen unkompliziert entwickeln, bauen Bewegungsprofile von Mitarbeitern auf.

Hier gilt es für die IT, die Anforderungen der Benutzer zu erkennen und entsprechend sichere Alternativen anzubieten, denn die Cloud-Dienste sind bereits da, und die Adaption auf die private und berufliche Organisation der Mitarbeiter hat bereits stattgefunden. Nutzt ein Mitarbeiter bereits Cloud-Datenspeicher zum Bereitstellen von Bildern und Videos, wird er kaum verstehen, warum seine IT-Abteilung einen solch einfachen Dienst nicht auch für Unternehmensdaten anbietet.

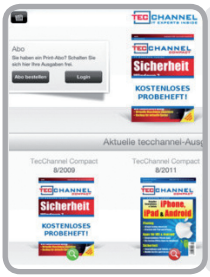
1.1.6 Transparenz und Sicherheit schaffen

Die Mobilität und hohe Integration von Diensten stellen besondere Anforderungen an Schutz und Sicherheit der Endgeräte sowie der genutzten Informati-

Mobile Webseite

Für Smartphones bieten wir eine in Design und Funktion angepasste Webseite, die automatisch gestartet wird wenn Sie mit Ihrem mobilen Gerät auf www.TecChannel.de surfen. Für das iPhone und für Android gibt es außerdem eigene Apps unter

www.tecchannel.de/iphone
www.tecchannel.de/android



iPad Kiosk-App

Machen Sie sich für ein neues Lesegefühl bereit: Ab sofort können Sie TecChannel-Compact auf Ihr Apple iPad laden, lesen und archivieren. Zum Start gibt es eine Ausgabe mit über 160 Seiten gratis zum Download. Die kostenlose TecChannel Kiosk-App informiert Sie außerdem direkt täglich mit den aktuellen Online-Beiträgen von TecChannel.de. Infos und Download unter

www.tecchannel.de/ipad

TecChannel-Newsletter

Das einspaltige Layout der neuen TecChannel-Newsletter haben wir so ausgelegt, dass die Informationen nicht nur auf PC, Notebook und Netbook perfekt dargestellt werden. Sie können die Newsletter nun auch direkt auf mobilen Geräten wie Smartphones und Tablet-PCs bequem lesen.

www.tecchannel.de/newsletter

Impressum

Verlag:
IDG Business Media GmbH
Lyonel-Feininiger-Straße 26
80807 München

Telefon: +49-89-360-86-0
Telefax: +49-89-36086-118

E-Mail: info@idgbusiness.de

Vertretungsberechtigter:
York von Heimburg,
Geschäftsführer
Registergericht:
Amtsgericht München
HRB 99187
Verantwortlicher für den redaktionellen Teil:
Michael Eckert, Chefredakteur
(Anschrift siehe Verlag)

Verantwortlicher für den Anzeigenteil:
Sebastian Wörle,
Gesamtanzeigenleiter
(Anschrift siehe Verlag)
089/36086-113,
swoerle@idgbusiness.de
Umsatzsteuer-identifikationsnummer:
DE 811 257 800

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

TecChannel ist Mitglied der IDG Business Media GmbH und somit ein Teil der IDG-Verlagsgruppe.
Darin erscheinen unter anderem auch folgende Zeitschriften:

IDG COMMUNICATIONS MEDIA AG
PC WELT · Macwelt · ChannelPartner · GameStar · CIO · COMPUTERWOCHE · DigitalWorld · GamePro

Die neue TecChannel App

Alles drin. Immer dabei. Jetzt fürs iPhone.

News, Infos, Tipps & Tricks für unterwegs!

- topaktuelle News
- Hintergründe
- Analysen
- Tests und Bilderstrecken

» Gratis laden

Erhältlich im App Store

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

www.tecchannel.de/iphoneapp

Einfach QR-Code mit dem Codereader Ihres iPhones einscannen.Sie werden direkt in den App-Store verlinkt und können die App downloaden. Einen kostenlosen Reader erhalten Sie z.B. unter http://get.beetagg.com/. Es entstehen lediglich Kosten für die Verbindung ins (mobile) Internet.

IDG BUSINESS MEDIA GMBH