

TEC CHANNEL COMPACT

IT EXPERTS INSIDE

Smartphone ■ Tablet ■ Notebook

Mobile IT



Geräte verwalten

- Mobile Device Management einsetzen
- iPhone & iPad einfach verwalten

Sicherheit

- Mobile Sicherheitsrisiken minimieren
- Android & Windows Phone absichern



Exchange

- Office 365 anbinden und verwalten
- Outlook-Rechte im Griff

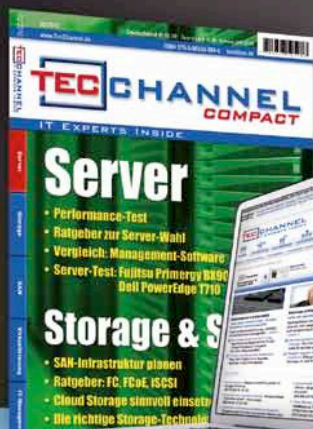
Google Drive &
SkyDrive richtig
nutzen

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

Inhalt

	Editorial	3
	Inhalt	4
1	Trends	8
1.1	Notebooks – Trends und neue Technologien	8
1.1.1	Formfaktoren – von Tablets bis Desktop-Replacement	9
1.1.2	Konsumerisierung der IT (BYOD)	11
1.1.3	Tablet-PCs im professionellen Einsatz	14
1.1.4	Sicherheit im Fokus	16
1.1.5	Allgemeine Notebook-Trends	18
1.2	Studie: Mobile Endgeräte gefährden IT-Sicherheit	21
1.2.1	Richtlinien und Durchsetzung	21
1.2.2	Häufigere Infektionen mit Malware	22
1.2.3	Private Geräte nutzen	22
1.2.4	Empfehlungen	22
1.3	Risikofaktoren für die IT: Smartphones und Tablets	23
1.3.1	Mobile IT ist Security-Problem Nummer eins	23
1.3.2	Aufgaben für die IT-Abteilung	25
1.3.3	Die positiven Erwartungen an Mobile IT	25
1.3.4	Tipps von Symantec	25
1.4	So gehen Smartphone-Hersteller mit Hackern um	26
1.4.1	Android: Rooting und eigene Apps erlaubt	26
1.4.2	Blackberry und Dingleberry	27
1.4.3	Windows Phone 7 und Chevron	28
1.4.4	Fazit: Im Firmenumfeld kritisch	28
1.5	Wie sich Tablets im Business einsetzen lassen	29
1.5.1	Alternative Exchange-Clients	30
1.5.2	Externe Tastatur unerlässlich	31
1.5.3	Unternehmens-Apps per Web	33
1.5.4	Fazit	34
1.6	Ratgeber: Sichere Cloud-Nutzung mit Smartphones	35
1.6.1	Mögliche Hintertür in die Cloud	35
1.6.2	Einmal-Passwörter für die mobile Cloud	35
1.6.3	Fingerabdruck-Scanner am Smartphone	37
1.6.4	Gesichtserkennung mit Smartphone-Kamera	37
1.6.5	Standortabhängige Zugriffskontrolle	38
1.6.6	Geräteerkennung als Zugriffsschutz	38
1.6.7	Fazit: große Vielfalt bei mobiler Zugangskontrolle	40
1.7	Dropbox, Google Drive, SkyDrive und Co. richtig nutzen	41
1.7.1	Dokumente mit Google Drive und Microsoft SkyDrive online bearbeiten	43
1.7.2	Sicherer Datenaustausch und verschlüsselte Dokumente speichern	44
1.7.3	iCloud – der Cloud-Speicher für iPhone, iPad, Mac und Co.	45
1.7.4	Auswahl des Cloud-Speichers und Alternativen	46

1.7.5	Cloud für Linux-Nutzer	47
1.7.6	Alternativen	47
1.8	Praxistest LTE: Breitband per Mobilfunk	48
1.8.1	Business-Anwendungen via LTE	48
1.8.2	LTE-800-Router dominieren	48
1.8.3	LTE 800 in der Praxis	49
1.8.4	Telekom LTE 800 mit stabilen Raten	50
1.8.5	AVM Fritzbox 6840 LTE – LTE 2600 wenig verbreitet	50
1.8.6	Lancom 1781-4G	52
1.8.7	VDSL-Feeling aus der Aktentasche	54
1.8.8	VDSL aus der Hosentasche	55
1.8.9	Fazit	56
1.9	NFC – Kontaktlose Technologie für mobiles Bezahlen und sicheren Zugang	57
1.9.1	Google und die Kreditwirtschaft	57
1.9.2	Durchbruch im Jahr 2013?	58
1.9.3	QR-Code ist günstiger als NFC	59
2	Administration	61
2.1	Ratgeber: Mobile Device Management – den mobilen Geräte-Zoo im Griff behalten	61
2.1.1	Was noch funktioniert – und was nicht mehr geht	61
2.1.2	Herausforderungen beim Management der Smart Devices	62
2.1.3	BYOD bringt weitere Anforderungen	62
2.1.4	Die Spezialisten für die mobilen Systeme: MobileIron	63
2.1.5	Die grundsätzliche Arbeitsweise der MobileIron-Plattform	65
2.1.6	Bekannter Player aus dem Markt der Managementsoftware: Matrix42	66
2.1.7	MDM mit Matrix42	68
2.1.8	Ein Newcomer im Bereich MDM: Baramundi	69
2.1.9	Microsofts bisher kleiner Beitrag zu MDM ...	71
2.1.10	Fazit: etablierter Anbieter oder Speziallösung – Entscheidung ist notwendig	72
2.2	iOS-Praxis: iPhone und iPad einfach verwalten	73
2.2.1	Das iPhone-Konfigurationsprogramm im Überblick	73
2.2.2	iPhone an iPhone-Konfigurationsprogramm anbinden	74
2.2.3	Konfigurationsprofile einlesen	75
2.2.4	Konfigurationsprofile einstellen	76
2.2.5	Konfigurationsprofile aktualisieren und löschen	77
2.2.6	Profile in der Praxis erstellen	77
2.2.7	MDM-Server und iPhones	79
2.3	Android 4 im Unternehmen einsetzen	80
2.3.1	Android professionell einsetzen – Einschränkungen und Möglichkeiten	80
2.3.2	Android sicher an Unternehmen anbinden – professionelle Lösungen	81
2.3.3	Android 4.0.4 – neue Oberfläche, bessere Bedienung	82
2.3.4	Datenvolumen überwachen	83
2.3.5	Favoriten synchronisieren	84
2.3.6	Android 4.0.4 testen – der Android-Emulator	84
2.3.7	Fazit	86
2.4	Smartphones mit Cloud-Diensten absichern	87
2.4.1	Abhilfe gegen mangelnde IT-Sicherheit	87

2.4.2	Vorteile von Cloud-Security-Lösungen	87
2.4.3	Geringe Anforderungen, einfache Administration	88
2.4.4	Alle Sicherheitsaufgaben werden abgedeckt	88
2.4.5	Mobile Verschlüsselung	88
2.4.6	Mobile Backups	89
2.4.7	Mobile Datenlöschung	89
2.4.8	App-Kontrolle	90
2.4.9	Device-Management	90
2.4.10	Spam- und Malware-Erkennung	91
2.4.11	Datenschutz nicht vergessen!	92
2.5	Ratgeber: Wie Sie Android-Smartphones und Tablets absichern	93
2.5.1	Android: das Betriebssystem	93
2.5.2	Das Betriebssystem und die Sicherheit	94
2.5.3	Welche Gefahren drohen	95
2.5.4	Was der Anwender tun kann (einfache Sicherheitstipps)	96
2.5.5	Software, die kostenlose Sicherheit bietet: AVG Free für Android	96
2.5.6	Weitere Vorteile dieser freien Lösung	97
2.5.7	Mehr Möglichkeiten: Lookout Mobile Security	98
2.5.8	Für Otto Normalanwender ...	99
2.5.9	... und für Fortgeschrittene	99
2.5.10	Fazit: Aufmerksamkeit ist geboten	100
2.6	Ratgeber: Wie Sie Windows-Phone-Smartphones absichern	101
2.6.1	Windows Phone ist nicht Windows Mobile	101
2.6.2	Das Sicherheitskonzept von Microsoft	101
2.6.3	Der Praxis-Test: Wie sieht die Nutzung im täglichen Einsatz aus?	102
2.6.4	Windows Phone 7: die einfachen Sicherheits-Tipps	103
2.6.5	Zusätzliche Sicherheitssoftware gibt es nicht	104
2.6.6	Praktische Helferlein	105
2.6.7	Fazit: Windows Phone 7 ohne Sicherheitslücken	106
2.7	Windows RT – Das Windows 8 für Tablets	107
2.7.1	Windows RT ohne Windows-Programme	107
2.7.2	Fehlende Funktionalitäten	108
2.7.3	Windows RT in Unternehmen verwalten	108
2.7.4	Richtlinien für Windows RT	109
2.7.5	Bring your own Device (ByoD) mit Windows RT	109
2.7.6	Self-Service-Portal	110
2.7.7	Fazit	110
2.8	Remote-Apps: PC-Software auf iPad und Android-Tablets nutzen	112
2.8.1	Apps für den mobilen Fernzugriff	112
2.8.2	Mehr Speicherplatz für iPad und Android	113
2.8.3	Spontane Unterhaltung	114
2.8.4	Ersatz für fehlende Apps	115
2.8.5	Das Tablet als tragbares Home-Office	116
2.8.6	Remote Desktop Apps: keine Chance für Datendiebe	116
2.8.7	Fazit: verlängerter Arm, aber keine Dauerlösung	117
3	Kommunikation	118
3.1	SP2 für Exchange Server 2010 – neue Funktionen und Installation	118
3.1.1	Address Book Policies – Adressbuchrichtlinien	119

3.1.2	Cross-Site Silent Redirection for Outlook Web App	121
3.1.3	Outlook Web App Mini	121
3.1.4	Mailbox Replication Service, Mailbox Replication Proxy und Multi-Valued Custom Attributes	122
3.1.5	Litigation Hold	123
3.1.6	SP2 installieren – Schemaänderungen beachten	123
3.1.7	Tipps zur Installation	124
3.2	Exfolders: Outlook-Rechte für Postfächer steuern	126
3.2.1	Exfolders und PFDAVAdmin	126
3.2.2	Download und Installation	127
3.2.3	Mit Exfolders.exe Rechte in Datenbanken bearbeiten	128
3.2.4	Erweiterte Funktionen – Protokollierung	128
3.2.5	Microsoft Exchange Server SMTP-Diagnose-Tool	129
3.2.6	Exchange Pre-Deployment Analyzer und Exchange Deployment Assistant	130
3.2.7	Exchange Remote Connectivity Analyzer	131
3.3	PST-Dateien einfach importieren: Microsoft Exchange PST Capture Tool	132
3.3.1	PST-Dateien mit Agenten von Client-Computern einlesen	132
3.3.2	Microsoft Exchange PST Capture einrichten	133
3.3.3	Agent für Microsoft Exchange PST Capture installieren	134
3.3.4	PST-Dateien im Netzwerk finden und PST Capture mit Office 365 verbinden	134
3.3.5	PST-Dateien importieren – lokal oder nach Office 365	135
3.3.6	Outlook Configuration Analyzer Tool (OCAT)	136
3.4	Workshop: Office 365 an die eigene Infrastruktur anbinden und verwalten	138
3.4.1	Office 365 und die Verwaltung	138
3.4.2	Postfächer migrieren	140
3.4.3	Koexistenz von Exchange mit Office 365	141
3.4.4	Sicherheit in Office 365 verwalten	141
3.4.5	Hybridbereitstellungen mit Exchange 2010 SP2	142
3.4.6	Office 365 mit der PowerShell verwalten	144
3.5	Exchange- und Outlook-Probleme lösen – das Calendar Checking Tool for Outlook	145
3.5.1	Kalender mit Calendar Checking Tool for Outlook prüfen	145
3.5.2	Reparaturoptionen	146
3.5.3	Probleme in Outlook und Exchange reparieren	147
3.5.4	Kalenderreparatur-Assistent (CRA) im Praxiseinsatz	148
3.5.5	Optionen und Einstellungen des Kalenderreparatur-Assistenten	149
3.5.6	Datenbanken mit neuen CMDlets reparieren	150
3.5.7	Outlook-Konfigurationsfehler mit OCAT entdecken	151
4	Apps und Tools	153
4.1	Die beliebtesten Smartphones	153
4.2	Die beliebtesten Tablet-PCs	157

Impressum	162
------------------	------------

2 Administration

Smartphones und Tablet-PCs sind die neuen mobilen Universalwerkzeuge. Die Geräte vereinen bei der Sprach- und Datenkommunikation Funktionen bisher separater Systeme und kommen ohne dabei spezielle Infrastruktur aus. Das stellt Administratoren vor neue Aufgaben: Es gilt, den Zugriff mobile Nutzer auf interne IT-Ressourcen auch außerhalb der abgesicherten Büroumgebungen zu steuern und einen sicheren mobilen Workflow zu gewährleisten.

2.1 Ratgeber: Mobile Device Management – den mobilen Geräte-Zoo im Griff behalten

Was mit dem IBM-PC begann, wird heute durch Smartphones und Tablets in eine ganz neue Dimension geführt: Unter Schlagwörtern wie BYOD (Bring Your Own Device) und Consumerization of IT gewinnen die Endanwender immer größeren Einfluss darauf, welche Hard- und Software in ihrer IT-Umgebung zum Einsatz kommt. War es bis vor wenigen Jahren noch so, dass Geräte wie PCs und Notebooks aus dem Firmen heraus langsam ihren Einzug in das private Umfeld der Anwender hielten, so ist es heute eher umgekehrt: Die Consumer-Geräte – allen voran Apples iPhones und iPads – drängen aus dem Freizeitbereich in das professionelle Umfeld der Unternehmens-IT.

Mag diese Verbreitung von Consumer-Geräten bis hin zum Einbringen der eigenen Endgeräte in das Firmennetz auch im weitesten Sinne durchaus so etwas wie eine „Demokratisierung“ der IT bewirken, entbindet sie dennoch Administratoren und IT-Verantwortlichen nicht von ihrer grundsätzlichen Verantwortung: Sie müssen das einwandfreie Funktionieren aller IT-Assets im Zusammenspiel mit der Firmen-IT garantieren und sind vor allen Dingen auch für die Sicherheit der IT und der Informationen verantwortlich, die damit verarbeitet werden.

2.1.1 Was noch funktioniert – und was nicht mehr geht

Die IT-Fachleute in den Firmen stehen dadurch vor neuen und anderen Herausforderungen als bisher: So begegnen sie zwar bei diesen neuen Geräten in ihrem „Zoo“ grundsätzlich den gleichen Problemen, die sie bisher bei Client-Systemen mit den Methoden des klassischen Gerätemanagements lösen konnten. Auch beim Management der „neuen“ mobilen Geräte geht es grundsätzlich darum:

- Geräte zu erfassen,
- die Software und Daten darauf auf dem aktuellen Stand zu halten und
- die Unternehmensdaten auf den Geräten zu schützen.

Trotzdem funktioniert hier die bekannte, traditionelle Verwaltung der Endgeräte nicht mehr. Es sind die Details bei der Betreuung der Geräte, die einen entscheidenden Unterschied zu der bisherigen Art des Gerätemanagements ausmachen.

Ein weiteres Problem: Bei den bisherigen Client-Systemen, ganz gleich ob es sich dabei um Windows-, Apple OS X- oder Linux-Systeme gehandelt hat, war es für die Administratoren nie eine Frage, dass die grundlegenden Verwaltungsdisziplinen – wie etwa die Möglichkeit einer Remote-Administration – auch gelöst sind. Das sieht nun aber gänzlich anders aus: Es kommen Geräte ins Netz, die unter dem Android-Betriebssystem, iOS, Windows Phone 7, BlackBerry, Windows Mobile oder einem anderen proprietären System arbeiten. Kommt beispielsweise noch das alte Windows Mobile (bis zur Version 6.5) zum Einsatz, so können die Systemverantwortlichen die üblichen Mechanismen einsetzen und unter anderem ihre Anwendungen auf die übliche Weise verteilen.

2.1.2 Herausforderungen beim Management der Smart Devices

Bei den heute am häufigsten zum Einsatz kommenden Smartphones und Tablets handelt es sich aber grundsätzlich um Geräte für den Consumer. So sind bei Apples iOS die Managementmöglichkeiten grundsätzlich weniger stark ausgeprägt; erst mit der aktuellen Version 5 des Betriebssystems hat Apple einige verbesserte Funktionen zur Verwaltung eingebaut.

Beispielsweise ist eine Verteilung von Apps ohne Anwenderinteraktion technisch nicht ohne Weiteres möglich. Um das Problem der Softwarebereitstellung auf iOS Geräten trotzdem zu lösen, bekommt der Apple-Anwender über die Mobile-Device-Management-Lösung in der Regel einen Corporate App Store – vergleichbar mit dem Apple AppStore – zur Verfügung gestellt, über den er Apps „einkaufen“ kann, die von der Unternehmens-IT bereitgestellt werden. Die Herausforderung besteht also zunächst einmal darin, die unterschiedlichen Betriebssysteme und damit auch die Variationen innerhalb dieser Betriebssysteme zu unterstützen. Zudem existieren in der Regel große Unterschiede zwischen den Möglichkeiten und Funktionen der einzelnen Betriebssystemversion. Eine gute Managementlösung für mobile Geräte wird dem Administrator diesen Schritt abnehmen: Er braucht dann nicht mehr zu wissen, welche Operationen er auf einem Android-Gerät mit der jeweiligen Betriebssystemversion ausführen kann: Die Lösung verfügt über die entsprechenden Informationen. Dabei existieren in der Regel große Unterschiede zwischen den Möglichkeiten und Funktionen der einzelnen Betriebssysteme.

2.1.3 BYOD bringt weitere Anforderungen

Unter dem Schlagwort „BYOD“ (Bring Your Own Device) kommt auf deutsche Firmen und damit deren IT-Abteilungen eine Entwicklung zu, die in den USA und

Großbritannien schon deutlich weiter verbreitet ist: Mitarbeiter kommen ins Unternehmen, bringen ihre eigenen Endgeräte mit und wollen damit im Firmennetzwerk arbeiten. Nun muss die IT irgendwie auch diese Geräte mit den „Corporate Services“ versorgen. Zudem muss sichergestellt werden, dass diese Geräte den Sicherheitsrichtlinien des Unternehmens entsprechen. Dazu gehören unter anderem die folgenden Punkte:

- Auf den Geräten muss ein bestimmtes, in den Sicherheitsrichtlinien des Unternehmens freigegebene Version des Betriebssystems laufen.
- Dieses Gerät darf weder „Gerootet“ (Android) noch „Gejailbroken“ (Apple iOS) sein.
- Weitere Absicherungen wie beispielsweise ein zwingendes Device Lock (Gerät wird immer und ohne Ausnahme über eine PIN-Eingabe abgesichert) sind zu überprüfen.
- Eventuell müssen sensible Unternehmensdaten sicher auf diese Geräte übertragen werden.
- Solche Unternehmensdaten müssen beim Ausscheiden des Mitarbeiters von dessen Privatgerät gezielt entfernt werden können („Corporate Wipe“), ohne dass die privaten Daten des Anwenders verloren gehen.

Wir haben uns auf dem Markt umgeschaut und stellen im Folgenden einige Lösungen vor, die sich mit dieser Thematik befassen und entsprechende Programme zur Verfügung stellen. Dieser Überblick kann dabei nur exemplarischen Charakter haben, da dieses Marktsegment seit Jahren ständig wächst.

2.1.4 Die Spezialisten für die mobilen Systeme: MobileIron

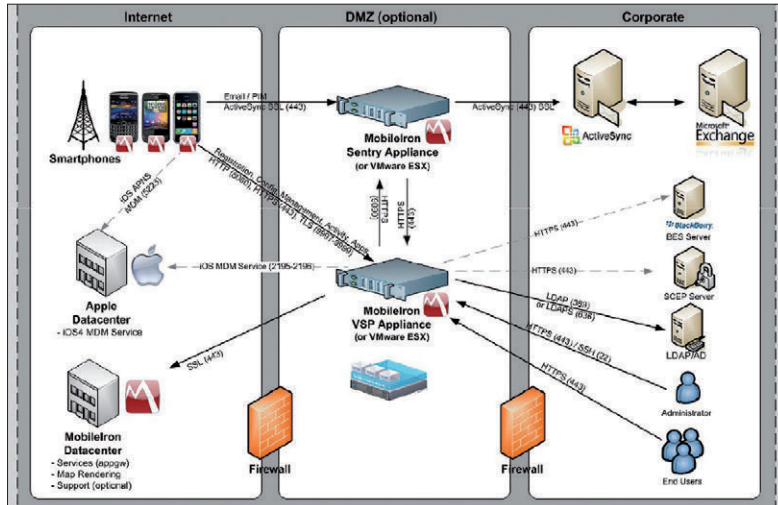
Wer sich heute mit dem Thema Mobile Device Management beschäftigt, wird mit großer Sicherheit immer wieder auf einen Namen stoßen: MobileIron (www.mobileiron.com/en/germany/).

Die erst 2007 in Mountain View, Kalifornien, gegründete Firma wird von den Analysten bei Gartner (www.gartner.com) als eines der führenden Unternehmen im „Magic Quadrant for Mobile Device Management Software“ angesehen.

Der Anbieter hat sich mit seinen Produkten ganz auf die Verwaltung und die Bereitstellung mobiler Geräte im Unternehmensumfeld konzentriert. Er verschafft mit seiner als Virtual Smartphone Platform (VSP) bezeichneten Lösung den Administratoren die Möglichkeit, sowohl Smartphones als auch Tablets unter den Betriebssystemen iOS, Android, BlackBerry, Symbian oder Windows in Echtzeit zu verwalten, zu kontrollieren und zu überwachen.

Das Kernstück und „Hub“ dieser Lösung ist die Sicherheits-Appliance VSP, die auf dem Managementserver installiert werden muss. Dabei handelt es sich um ein gehärtetes Linux-System, das komplett gegen Zugriffe abgeschottet ist: Der Administrator arbeitet nur mittels der Webkonsole auf diesem System. Diese Plattform

kann als Hardware-Appliance oder als virtuelle Appliance, auf einem VMware ESX-Server, betrieben werden. Der Anbieter rät zum Einsatz dieser Appliance innerhalb der DMZ (Demilitarized Zone), das ist aber nicht zwingend notwendig.



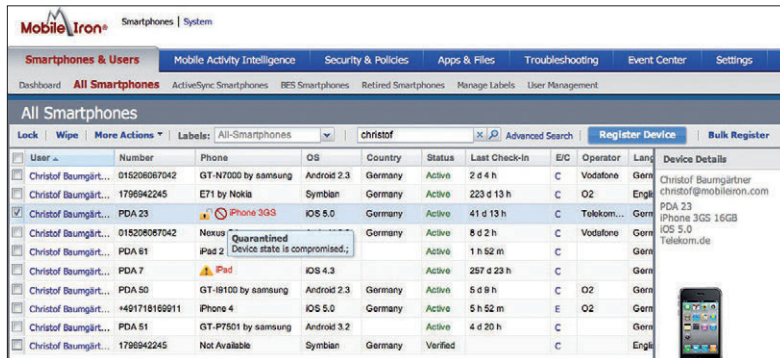
Umfangreiche Lösung mit vielen Möglichkeiten: Bei der MDM-Software des kalifornischen Anbieters MobileIron ist die virtuelle Appliance VSP der Dreh- und Angelpunkt, der alle Aufgaben erledigt und auch ein Repository beinhaltet. (Quelle: MobileIron)

Diese Managementplattform setzt dann auf ein zentrales Repository auf, in dem alle Daten der im Unternehmen eingesetzten Smartphones (firmeneigene sowie entsprechend genehmigte private Smartphones) gespeichert sind, die von der Systemadministration für ein sicheres Management benötigt werden.

Smartphones & Users									
Mobile Activity Intelligence									
Security & Policies									
Apps & Files									
Troubleshooting									
Dashboard All Smartphones ActiveSync Smartphones BES Smartphones Retired Smartphones Manage Labels User Management									
All Smartphones(1.1.2-3.0.1-57)									
Lock Wipe More Actions Labels: All-Smartphones Search by User Advanced Search Reg									
User	Number	Phone	OS	Country	Status	Last Connected	E/C	Registered	Opera...
Clarissa...	141560...	iPhone 3GS	iOS 4.0	United States	Active	4 h 15 m	C	2010-08-06 12:48:11...	AT&T
Eric Mid...	140820...	iPhone 3GS	iOS 4.0	United States	Active	6 d 7 h	C	2010-08-02 10:36:25...	AT&T
Greg Ge...	+16508...	iPhone 4	iOS 4.0	United States	Active	5 d 1 h	C	2010-08-03 5:58:43 PM	AT&T
JC Counts	PDA	Compromised Device	United States	Wiped	6 d 5 h	E	2010-08-02 1:43:21 PM	AT&T	
Jesse Li...	+12026...	OS Unlocked	United States	Active	2 d 4 h	C	2010-08-04 5:45:17 PM	AT&T	

Ein Blick auf das Dashboard mit den mobilen Geräten bringt es an den Tag: Hier hat ein Anwender sein Betriebssystem auf dem Smartphone „unlocked“, womit es nicht mehr den Sicherheitsrichtlinien des Unternehmens genügt. (Quelle: MobileIron)

Die Managementsoftware klinkt sich automatisch in das Unternehmensnetzwerk ein und baut die Verbindungen zu den Mobile-Iron-Anwendungen und den entsprechenden Unternehmensressourcen wie LDAP, Exchange Active Sync, den verschiedenen Zertifizierungsstellen und einem eventuellen Blackberry-Enterprise-Server auf. So stellt sie dann die Möglichkeit zur Verfügung, die Mobilgeräte zu überwachen und zu steuern. Zusätzlich bietet das Unternehmen unter dem Namen „Connected Cloud“ ein mandantenfähiges Mobile-Device-Management für die Cloud an. Durch einen sogenannten optionalen Enterprise Connector soll sich auch diese Verwaltungslösung leicht in die bestehende Sicherheitsinfrastruktur eines Unternehmens integrieren lassen.



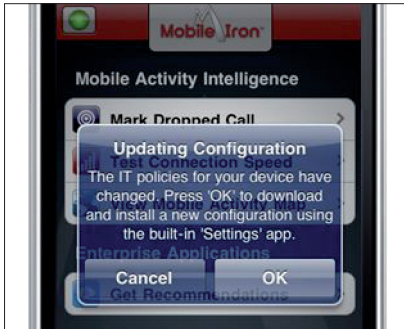
User	Number	Phone	OS	Country	Status	Last Check-In	EOC	Operator	Lang	Device Details
Christof Baumgärt...	015206087042	GT-N7000 by samsung	Android 2.3	Germany	Active	2 d 4 h	C	Vodafone	Ger	Christof Baumgärtner christof@mobileiron.com
Christof Baumgärt...	1796942245	E71 by Nokia	Symbian	Germany	Active	223 d 13 h	C	O2	Engl	PDA 23
Christof Baumgärt...	PDA 23	iPhone 3GS	iOS 5.0	Germany	Active	41 d 13 h	C	Telkom...	Ger	PDA 23 iPhone 3GS 16GB iOS 5.0 Telekom.de
Christof Baumgärt...	015206087042	Nexus	Android 4.3	Germany	Active	8 d 2 h	C	Vodafone	Ger	Quarantined Device state is compromised.
Christof Baumgärt...	PDA 61	iPad 2	iOS 4.3	Germany	Active	1 h 52 m	C		Ger	
Christof Baumgärt...	PDA 7	Pad	iOS 4.3	Germany	Active	257 d 23 h	C		Ger	
Christof Baumgärt...	PDA 50	GT-I9100 by samsung	Android 2.3	Germany	Active	5 d 9 h	C	O2	Ger	
Christof Baumgärt...	+491718169911	iPhone 4	iOS 5.0	Germany	Active	5 h 52 m	E	O2	Ger	
Christof Baumgärt...	PDA 51	GT-P7501 by samsung	Android 3.2	Germany	Active	4 d 20 h	C		Ger	
Christof Baumgärt...	1796942245	Not Available	Symbian	Germany	Verified		C		Engl	

Der nächste Schritt: Ein kompromittiertes mobiles Gerät ist gefunden und wird aus diesem Grund in die Quarantäne verschoben. (Quelle: MobileIron)

2.1.5 Die grundsätzliche Arbeitsweise der MobileIron-Plattform

Zunächst muss natürlich der Mobile-Iron-Server mit der Verwaltungssoftware im Rechenzentrum beziehungsweise in der DMZ installiert werden. Hier kann dann zusätzlich auch noch die „Sentry“ bezeichnete Lösung zum Einsatz kommen, die eine Zugriffskontrolle für E-Mail-Systeme bietet, die mit Microsofts ActiveSync arbeiten. Dazu gehören neben Microsoft Exchange auch IBM Lotus Notes, Google Mail und Microsoft Office 365. Auch dieser Teil der Lösung kann als virtuelle Maschine oder Hardware-Appliance betrieben werden. Das sogenannte „Advanced Management“-Paket des Herstellers beinhaltet diese Funktionalität, während die Hardware-Appliance extra erworben werden muss.

In einem nächsten Schritt wird dann der MobileIron-Client direkt auf die mobilen Geräte ausgerollt – dies geschieht „over-the-air“, sodass die Anwender nicht mit ihren Geräten zu den Administratoren kommen müssen. Entsprechende Privacy-Richtlinien regeln hier bereits den Zugang zu den mobilen Daten.



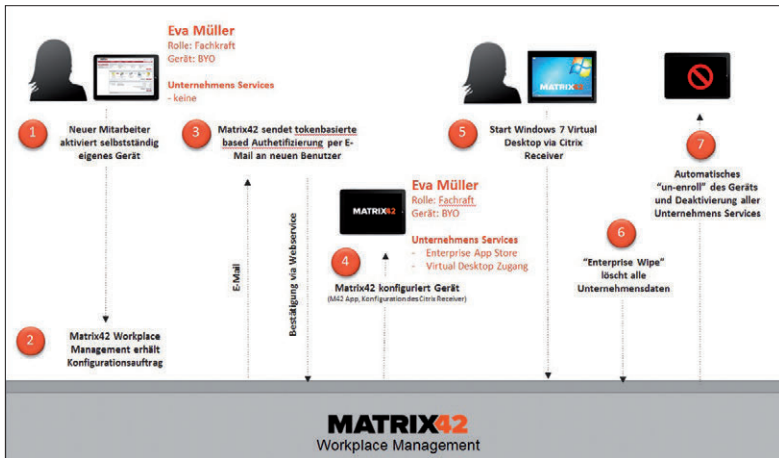
Ein grundsätzliches Problem bei den Apple-iOS-Geräten: Der Anwender muss bei vielen Update- und Installationsvorhaben jeweils die Aktion an seinem Telefon entsprechend bestätigen. (Quelle: MobileIron)

Die Administratoren können dann über die Webkonsole mithilfe eines Enterprise Smartphone Management Dashboards die entsprechenden Einstellungen vornehmen und dabei etwa auch mobile Geräte sperren, Daten auf diesen Geräten löschen oder die nötigen Updates einspielen. Durch geschicktes Ausnutzen der iOS-eigenen Mechanismen ist es den Entwicklern von MobileIron auch gelungen, die vom Anwender geforderte Interaktion auf ein minimales Maß zu reduzieren: Hat der Nutzer einmal der Verwaltung durch das Enterprise-Management zugestimmt, können fast alle Aktionen ohne sein Zutun ausgelöst und gesteuert werden. Dem Endanwender steht dabei mit der als MyPhone@Work bezeichneten Software ein Weg zur Verfügung, wie er ebenfalls über eine Webkonsole einen Teil (je nach Vorgaben der Firmenadministratoren) der Verwaltung selbst übernehmen und so beispielsweise auch ein verlorenes oder gestohlenen Gerät wieder auffinden kann.

2.1.6 Bekannter Player aus dem Markt der Managementsoftware: Matrix42

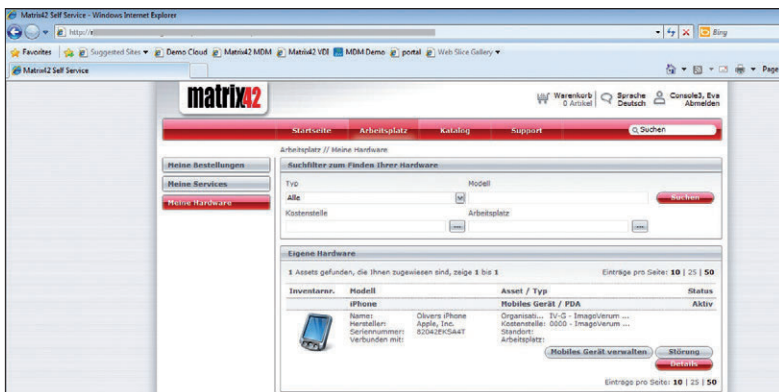
Der deutsche Anbieter Matrix42 stellt unter der Bezeichnung „Matrix42 Mobile Device Management“ (www.matrix42.de) ebenfalls eine MDM-Lösung zur Verfügung. Dabei kann er mit einem großen Vorteil punkten: Wenn es um die Verwaltung, Betreuung und das Management sowohl physischer als auch virtueller Geräte im Unternehmensumfeld geht, glänzt der Hersteller mit einer langen Historie und umfangreichen Lösungen.

Um ihre Managementlösungen auch um die Fähigkeit zur Verwaltung und Betreuung mobiler Geräte zu ergänzen, ist die Firma vergangenes Jahr eine Partnerschaft mit dem amerikanischen Anbieter Airwatch eingegangen und hat dessen Technik in das eigene Portfolio integriert. Dieser Hersteller wird von den Gartner-Analysten genauso wie MobileIron im rechten, oberen Bereich ihres „Magic Quadranten“ eingeordnet, also bei der führenden, innovativen Firma dieses Geschäftsfelds. Auch diese Lösung ist in der Lage, sowohl iOS- als auch Android-, BlackBerry-, Symbian- und Windows-Mobile-Geräte zu verwalten.



Ein Beispiel, das zeigt, wie die Verwaltung mobiler Geräte mit anderen Managementbereichen der IT verknüpft ist: die Konvergenz zwischen den Bereichen MDM, VDI (Virtual Desktop Infrastructure), BYOD (Bring Your Own Device) und letztlich auch ITSM (IT Service-Management). (Quelle: Matrix42)

Der Aufbau der Lösung: Die gesamte Software-Suite besteht aus verschiedenen Elementen, die zusammen die Verwaltung und Betreuung der mobilen Geräte erlauben. Je nach Art der zu verwaltenden IT-Umgebung und der vorhandenen mobilen Geräte können diese Komponenten auf einem einzelnen Server installiert oder auf mehrere Server verteilt werden, um so einen Load-Balancing-Effekt zu erreichen beziehungsweise die Verfügbarkeit zu erhöhen. Grundsätzlich teilt sich das System dabei in drei Gruppen auf:

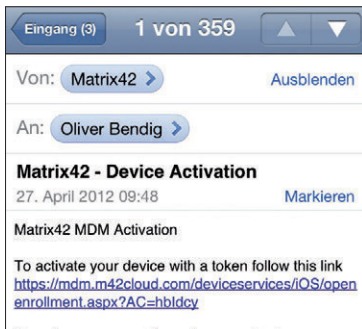


Vorteil moderner MDM-Lösungen: Über ein Portal kann man seine mobilen Geräte selbst verwalten, ohne dass dabei Firmenrichtlinien verletzt oder die Sicherheit beeinträchtigt wären. (Quelle: Matrix42)

- MDM-Datenbank: eine SQL-Datenbank, die als Repository dient und alle Daten zur Verwaltung und Betreuung der mobilen Geräte speichert.
- MDM-Webanwendungen: Anwendungen, die unter anderem Microsofts Webdienst IIS und die .Net-Bibliothek einsetzen. Sie bilden die Schnittstelle zu den Endanwendern und den Geräten-
- MDM-Windows-Dienste: Anwendungen, die auf Windows-Servern als Hintergrunddienste installiert werden und entsprechende Aufgaben verrichten.

2.1.7 MDM mit Matrix42

Eine typische Installation würde nach den Empfehlungen des Anbieters aus zwei Windows-2003- oder -2008-Servern bestehen, wobei das eine System als Application-Server (mit der Webkonsole, den Device-Diensten sowie API- und Windows-Diensten) und das andere als Datenbankserver mit der Datenbank (MS SQL-Server 2005 oder 2008) dient. Zwar ist es möglich, die verschiedenen Komponenten auch in virtualisierten Umgebungen einzusetzen, der Hersteller rät aber davon ab, dies auch für den Datenbankserver zu tun.



Ein wichtiger Schritt: Ein neues Gerät muss im Firmennetzwerk zunächst einmal aktiviert werden. So wird auch sichergestellt, dass sich nur Geräte im eigenen Netz befinden, die den vorgegebenen Richtlinien entsprechen. (Quelle: Matrix42)

Ähnlich wie bei der zuvor vorgestellten Lösung können Administratoren auch bei diesem MDM-Produkt einen rollenbasierten Zugriff konfigurieren, der beispielsweise den Schutz der entsprechenden Firmendaten garantieren kann. Funktionen wie „Corporate Wipe“ und die Lokalisierung sind bei dieser Lösung ebenfalls zu finden und funktionierten bei entsprechenden Demonstrationen sowohl mit iOS- als auch mit Android-Geräten völlig problemlos.

Die Software bietet zudem eine Integration in die verschiedenen Enterprise-Dienste wie LDAP und Active-Directory sowie zum BlackBerry Enterprise-Server, dem Microsoft System Center Operations Manager, und ein SDK, mit dem Client- und Server-Dienst integriert werden können.



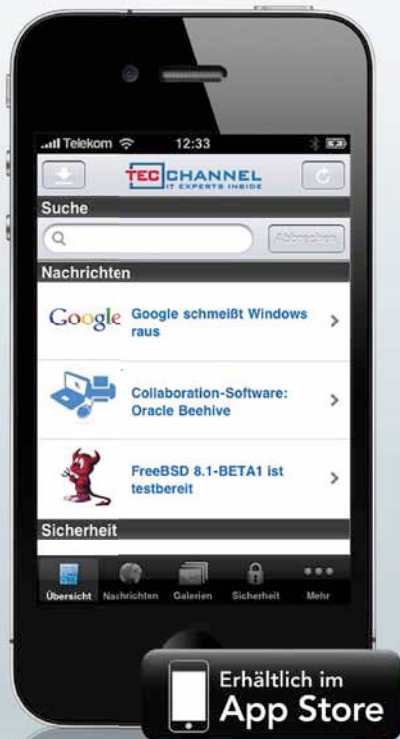
Die neue TecChannel App

Alles drin. Immer dabei. Jetzt fürs iPhone.

News, Infos,
Tipps & Tricks
für unterwegs!

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

» **Gratis laden**



Voraussetzungen: 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.