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

TECCHANNEL 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

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

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 „Gejailbreaked“ (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

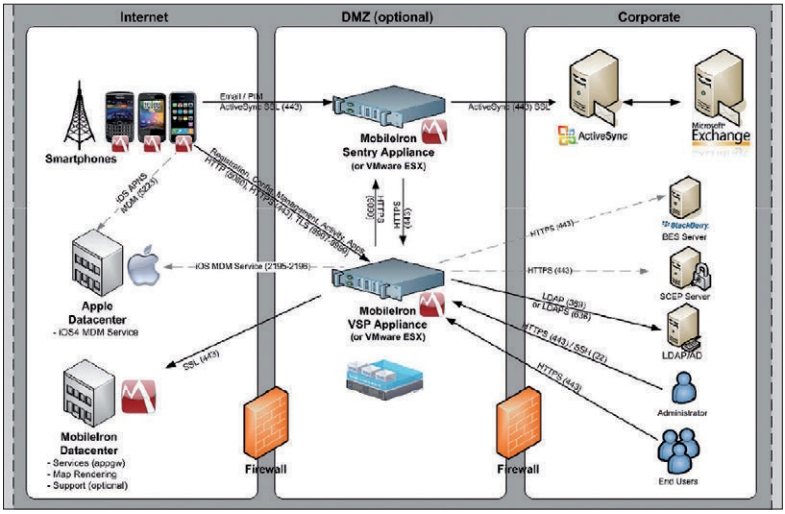
Wer sich heute mit dem Thema Mobile Device Management beschäftigt, wird mit großer Sicherheit immer wieder auf einen Namen stoßen: MobileIron (www.mobileiron.com/en/germany/).

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.

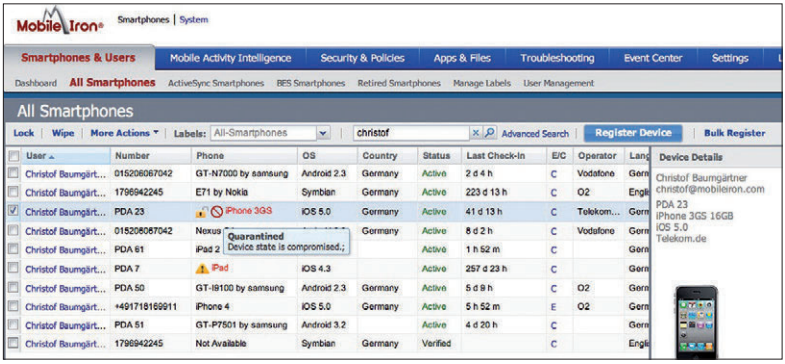


Umfangreiche Lösung mit vielen Möglichkeiten: Bei der MDM-Software des kalifornischen Anbieters MobileIron ist die virtuelle Appliance VSP der Dreh- und Angelpunkt, der alle Aufgaben erledigt und auch ein Repository beinhaltet. (Quelle: MobileIron)

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.

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 verschiedene 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.

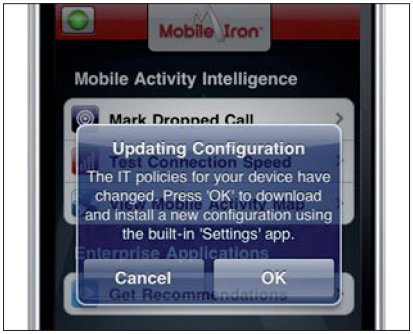


Der nächste Schritt: Ein kompromittiertes mobiles Gerät ist gefunden und wird aus diesem Grund in die Quarantäne verschoben. (Quelle: MobileIron)

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 als „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.



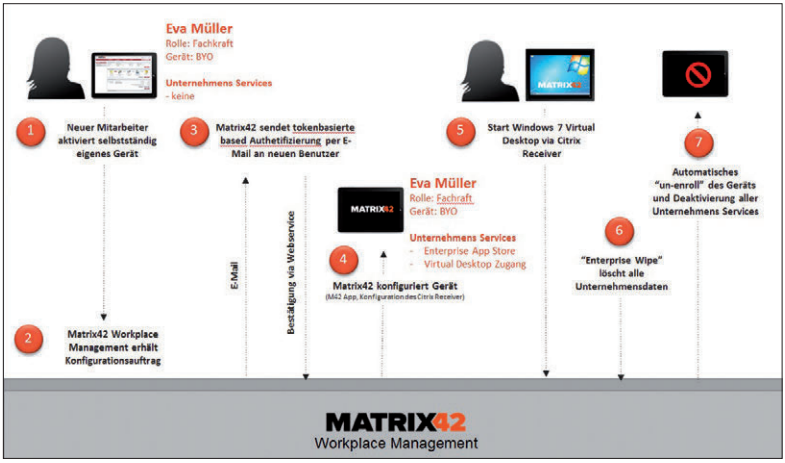
Ein grundsätzliches Problem bei den Apple-iOS-Geräten: Der Anwender muss bei vielen Update- und Installationsvorhaben jeweils die Aktion an seinem Telefon entsprechend bestätigen. (Quelle: MobileIron)

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 gestohlenes Gerät wieder auffinden kann.

2.1.6 Bekannter Player aus dem Markt der Managementsoftware: Matrix42

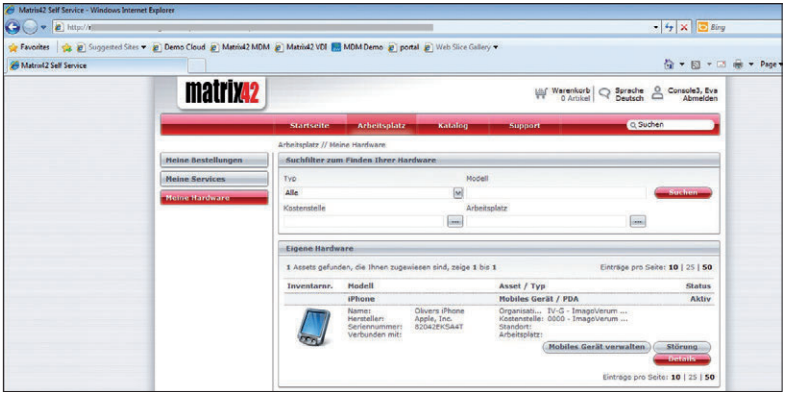
Der deutsche Anbieter Matrix42 stellt unter der Bezeichnung „Matrix42 Mobile Device Management“ (www.matrix42.de) ebenfalls eine MDM-Lösung zur Verfügung. Dabei kann er mit einem großen Vorteil punkten: Wenn es um die Verwaltung, Betreuung und das Management sowohl physischer als auch virtueller Geräte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

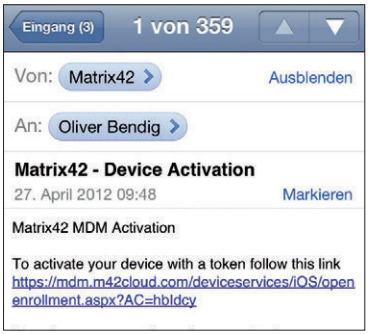


Vorteil moderner MDM-Lösungen: Über ein Portal kann man seine mobilen Geräte selbst verwalten, ohne dass dabei Firmenrichtlinien verletzt oder die Sicherheit beeinträchtigt wären. (Quelle: Matrix42)

- 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

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