RATGEBER

Smartphones & Tablets im Unternehmen

Apple iOS ★ Android ★ BlackBerry OS ★ Windows Phone

› SICHERHEIT
› VERWALTUNG
› INTEGRATION

TECCHANNEL
IT EXPERTS INSIDE

TEC CHANNEL
SILBER-PAKET

Ratgeber

Smartphones & Tablets im Unternehmen

Sicherheit, Verwaltung, Integration

TECCHANNEL
IT EXPERTS INSIDE

Impressum

Chefredakteur: Michael Eckert (verantwortlich, Anschrift der Redaktion)
Redaktion TecChannel:
Lyonel-Feininger-Straße 26, 80807 München,
Tel.: 0 89/3 60 86-897
Homepage: www.TecChannel.de,
E-Mail: feedback@TecChannel.de
Autoren dieser Ausgabe werden bei den Fachbeiträgen genannt
Verlagsleitung: Michael Beilfuß

Grafik und Layout:
stroemung GmbH (Michael Oliver Rupp, Oliver Eismann)
Titel: Clemens Strimmer
Bilder, soweit nicht angegeben: Hersteller
Anzeigen: Anzeigenleitung: Sebastian Woerle
Tel.: 0 89/3 60 86-628
Ad-Management: Edmund Heider (Ltg.) (-127)
Anzeigenannahme: Martin Behringer (-554)

Gesamtvertriebsleitung IDG Deutschland:
Josef Kreitmair
Produktion: Jutta Eckebrecht (Ltg.)
Haftung:
Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Veröffentlichungen in TecChannel-Publikation 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-Feininger-Straße 26
80807 München
Tel.: 0 89/3 60 86-0, Fax: -118
Homepage: 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

Erschienen bei IDG Business Media GmbH
Printed in Germany
Druck und Bindearbeit: Strauss GmbH, 69509 Mörlenbach

ISBN: 978-3-942922-07-4

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

Inhalt

1 Mobile Geräte im Unternehmen

Mitarbeiter in Unternehmen sind längst nicht mehr an einen Ort gebunden. Sie sollen jederzeit erreichbar sein und unabhängig vom Aufenthaltsort auf die gesamte IT-Infrastruktur zugreifen können. Diese Erfordernisse lassen sich durch den Einsatz mobiler Geräte für geschäftliche Anwendungen meistern. Die Mobilisierung von Unternehmensprozessen wirkt sich auf die Leistungsfähigkeit und Wirtschaftlichkeit aus, bringt jedoch neue Sicherheitserfordernisse mit sich.

1.1 Die vier Typen mobiler Mitarbeiter

Der Anteil des mobilen Arbeitens wird kräftig ansteigen, da sind sich alle Analysten einig. Mit SAP hat sich nach der Sybase-Übernahme ein richtig Großer an die Spitze der mobilen Bewegung gestellt, iPhone und iPad sind allem Gerede von den Consumer Devices zum Trotz auch beim Business echte Renner.

Zudem denken viele große Unternehmen schon längst darüber nach, wie sie mit den „Own Devices" umgehen sollen, die ihre Mitarbeiter mit zur Arbeit bringen, und wie sie ihre wichtigsten Enterprise-Applikationen aufs Tablet bringen. Lesen Sie dazu den Beitrag BYoD – Private Hardware in der Firma (Webcode **2033617**).

Allem Hype zum Trotz meint Forrester-Analystin Michele Pelino in der von ihr verfassten Studie The Rise Of Wannabe And Maverick Mobile Workers, dass viele IT-Verantwortliche in den Unternehmen und ebenso zahlreiche Anbieter die Nachfrage nach mobilen Lösungen nach wie vor unterschätzen. Warum das so ist? Weil sie zwei wichtige Gruppen dabei nicht auf dem Schirm haben, meint Pelino: die „mobilen Möchtegerns" und die „mobilen Einzelgänger" („mobile wannabes" und „mobile mavericks").

1.1.1 Möchtegerns und Einzelgänger

Die Möchtergerns sitzen bei der Arbeit fast ausschließlich am Schreibtisch, sodass nicht nur die IT-Abteilung sie nicht als mobile Arbeiter führt. Dennoch würden es auch diese Mitarbeiter schick finden, mobile Endgeräte einsetzen zu können.

Die Einzelgänger nutzen zwar mobile Geräte für die Arbeit, klinken sich aber aus firmenweiten Beschaffungsaktionen weitgehend aus. Stattdessen kaufen sie lieber ihre eigenen Geräte und Apps.

Zusammen machen diese beiden Gruppen immerhin rund 22 Prozent aller Beschäftigten aus, hat Forrester in Umfragen herausgefunden. Bis 2015 wird ihr Anteil sogar auf 42 Prozent aller Mitarbeiter steigen. Wer auf Dauer im Mobile-Geschäft Gewinne erzielen möchte, schlussfolgert Forrester, muss seine Produkte auch auf diese Zielgruppen ausrichten.

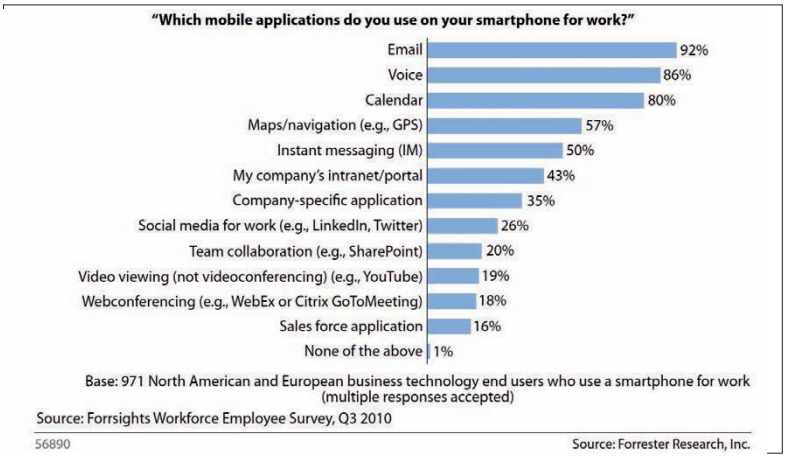
1.1.2 Aufgaben für IT-Abteilungen

Eine signifikante Zahl von Mitarbeitern arbeitet mittlerweile außerhalb klassischer Büros. Zwar waren 2010 noch 78 Prozent der in der *Forrsights Workforce Employee Survey* in Europa und Nordamerika befragten Angestellten in der Firma tätig. Immerhin 29 Prozent leisten aber mindestens einmal pro Woche Arbeit außerhalb, zum Beispiel beim Kunden, in Heimarbeit oder auf Reisen. Zusätzlich geben 18 Prozent an, mindestens einmal pro Woche von zu Hause aus zu arbeiten.

Mobile Technologien gehören zu den Top-Prioritäten der IT-Abteilungen. Immerhin drei von zehn Telekommunikationsprojekten gelten dem mobilen Arbeiten. Mehr als 45 Prozent der Unternehmen gehen davon aus, demnächst mehr Support für mobile Mitarbeiter leisten zu müssen. Weitere 43 Prozent rechnen damit, dass die Anzahl mobiler Geräte auch jenseits des klassischen Außendienstes ansteigen werde. Bemerkenswert im Zusammenhang mit der Ausgangsthese von Forrester ist, dass ein Drittel der Unternehmen ihr Sortiment an mobilen Apps auch für solche Mitarbeiter ausweiten wird, die nicht oder nur ausnahmsweise mobil arbeiten. Das wird die nahe Zukunft vielleicht am stärksten von der Vergangenheit unterscheiden, meint Forrester.

1.1.3 Wofür Mitarbeiter mobile Geräte nutzen

Viele Firmen leisten längst Support für Geräte in Privatbesitz. Mehr als 55 Prozent der befragten Unternehmen erlauben ihren Mitarbeitern, Privatgeräte mitzubringen. Die angepeilten Dienstleistungen reichen vom eingeschränkten Support für bestimmte bis zum Rundum-Sorglos-Paket für alle mobilen Geräte.



Umfrage: Wofür Mitarbeiter mobile Geräte nutzen.

Fast jeder fünfte Mitarbeiter (18 Prozent) nutzt Smartphones für die Arbeit. Im Jahr 2009 betrug der Anteil noch 13 Prozent. Diese Zahl wird weiter steigen, schätzt Forrester, weil es schon bald eine sehr viel größere Gerätevielfalt geben wird. Mitarbeiter nutzen ihre mobilen Geräte vor allem für Basisanwendungen wie Mail, Kalender oder Voice-over-IP. Auf den Plätzen folgen deutlich abgeschlagen Navigationsanwendungen und Instant Messaging. Der Gebrauch von Social-Media-Apps (Facebook, Twitter) wächst zwar, liegt mit 26 Prozent beruflicher Nutzung aber ebenfalls noch zurück. Für die Allgemeinheit eher unbedeutend sind spezielle Apps etwa für den Vertriebsaußendienst, die wiederum aber für bestimmte Gruppen naturgemäß sehr wichtig sind.

Gegenwärtig gehören weltweit 57 Prozent aller Mitarbeiter in den Unternehmen zu den mobilen Arbeitskräften, schreibt Forrester. Diese beeindruckend große Zahl verteilt Forrester auf vier Kategorien: mobile Information und Task Worker sowie die schon bekannten Möchtegerns und Einzelgänger.

1.1.4 Information Worker und Außendienstler

Die Informationsarbeiter (Information Worker) sind die Ersten, die im Unternehmen mobile Geräte und Anwendungen beziehen. Sie reisen viel und arbeiten oft außer Haus, benötigen aber einen regelmäßigen Kontakt zum Büro. Daher nutzen sie häufig Kommunikations- und Kollaborations-Tools. Der Arbeitgeber finanziert oder subventioniert die Geräte dieser Mitarbeiter oft.

Die Informationskräfte erwarten von der Unternehmens-IT Support, weil die Geräte für ihre produktive Arbeit enorme Bedeutung haben. Im Jahr 2010, so Forrester, fielen 25 Prozent aller mobilen Angestellten in diese Kategorie; bis 2015 werden es 30 Prozent sein. Klassische Außendienstmitarbeiter nutzen mobile Endgeräte mit vertikal ausgerichteten Anwendungen, etwa für Marketing oder Vertrieb, die sie oft bis regelmäßig für ihre Tätigkeiten außer Haus benötigen. Diese mobilen Einsatzkräfte machen derzeit rund elf Prozent der Belegschaft aus, bis 2015 wird ihr Anteil mutmaßlich bei 13 Prozent liegen.

1.1.5 Möchtegerns arbeiten stationär

Jenseits der klassischen Zielgruppen bewegen sich die mobilen Möchtegerns. Sie arbeiten stationär, möchten sich aber trotzdem mit mobilen Geräten und Applikationen schmücken. Heute machen die Möchtegerns schon 16 Prozent aller Mitarbeiter aus, 2015 sogar 30 Prozent. Sie – Büroangestellte, Führungsassistenten, Personalverantwortliche und Mitarbeiter aus dem Kundenservice – werden der Mobilisierung der Unternehmen starken Auftrieb geben, schätzt Forrester.

Zur stärksten Gruppe und damit zu den Treibern bei den Möchtegerns werden die Mitarbeiter gehören, die zwischen 1980 und 2000 geboren sind und nun in den Arbeitsmarkt drängen. Diese Kollegen sind mit mobilen Geräten aufgewachsen

und wollen sie selbstverständlich auch bei der Arbeit nutzen. Die meisten von ihnen bringen diese Geräte genauso selbstredend mit, sodass sie zunächst einmal der Kontrolle und dem Zugriff der IT-Abteilung entzogen sind. Dennoch erwarten diese Mitarbeiter natürlich, dass die IT auch ihr mobiles Equipment wartet.

1.1.6 Einzelgänger: eine kleine, aber schnell wachsende Gruppe

Die mobilen Einzelgänger bilden die kleinste, aber auch die am schnellsten wachsende Gruppe. Ihre Mitglieder sind überwiegend männlich, und sie nutzen Smartphones und Tablets ein bis zwei Stunden pro Tag für Aufgaben, die direkt mit ihrer Arbeit zu tun haben. Die Firmen-IT stuft solche Mitarbeiter durchaus als mobile Mitarbeiter ein, erreicht sie mit firmenweiten Beschaffungsmaßnahmen aber nicht. Mavericks kaufen ihre Geräte selber. Einzelgänger reisen viel und arbeiten oft außerhalb des Unternehmens.

2010 waren nur sechs Prozent solche mobilen Solisten. Bis 2015 wird sich diese Zahl aber mehr als verdoppeln, weil immer mehr Unternehmen ihre Mitarbeiter ermuntern werden, sich eigene Geräte zuzulegen und sie für die Arbeit zu verwenden, schätzt Forrester. Das jedenfalls werde die Kosten für mobile Endgeräte in Grenzen halten. Dennoch werden auch diese Arbeiter vom IT-Support unterstützt, damit sie auch außerhalb des Unternehmens produktiv arbeiten können.

Thomas Pelkmann

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation CIO.

TecChannel-Links zum Thema	Webcode	Compact
Die vier Typen mobiler Mitarbeiter	2034864	S.13
BYoD – Private Hardware in der Firma nutzen	2033617	S.17
BYoD – Super-GAU für die IT-Abteilung?	2035857	S.20
BYoD – Der Tod des Firmen-PCs?	2035860	S.24
iPad und iPhone zwingen zu WLAN-Ausbau	2034964	S.28
System Center Configuration Manager 2012 Beta 2 – neue Features und Funktionen	2035287	S.30

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

1.2 ByoD – Private Hardware in der Firma nutzen

ByoD ist das Akronym für eine typisch amerikanische Formulierung, die die Dinge auf den Punkt bringt: **B**ring **y**our **o**wn **D**evice oder ByoC (**B**ring **y**our **o**wn **C**omputer) bezeichnet den Trend, dass immer mehr Mitarbeiter ihre private Hardware auch geschäftlich nutzen. Das fängt beim PC zu Hause an, der per VPN auch geschäftlich genutzt wird, und geht mit dem Notebook, Smartphone und Tablet-PC weiter. Längst sind beispielsweise nicht nur die offiziellen BlackBerrys der Führungsmannschaft in der Lage, E-Mails überall verfügbar zu machen. Selbst Consumer-Smartphones verfügen über einen E-Mail-Client.

40 Prozent Kosten sparen

Was früher ein Horrorszenario für jede IT-Abteilung war, gilt es nun unter Kontrolle zu bekommen. Das ByoC-Modell bietet nämlich deutliche Vorteile, die die Nachteile aufwiegen können: Laut Gartner können Firmen bis zu 40 Prozent der Anschaffungs- und Unterhaltskosten sparen, die sie beispielsweise für den Notebook-Kauf aufwenden müssten. Ein gewollter Nebeneffekt dabei: Die Mitarbeiter sind stets erreichbar. Daher denken immer mehr Unternehmen über neue Modelle für den kostengünstigen Einkauf von IT nach und starten Pilotprogramme, wie etwa Procter & Gamble. Teilweise finanzieren Firmen wie Citrix, EMC und Kraft Foods bereits die Anschaffung privater Geräte mit Zuschüssen in der Größenordnung von bis zu 1500 Euro für das IT-Equipment, das dann auch in der Firma verwendet werden darf (und soll). Diese Art der IT-Beschaffung kann erheblich zur Zufriedenheit der Nutzer beitragen und auch Kosten senken.

1.2.1 Sicherheitskonzept an ByoD-Modell anpassen

Selbstverständlich müssen beim „ByoD-Modell“ die sich aufdrängenden Fragen der IT-Sicherheit beantwortet werden. Hier können im Sinne der notwendigen IT-Security Desktop-Virtualisierung und Terminal-Lösungen den Spagat zwischen privater und dienstlicher Nutzung erleichtern. Wichtige Unternehmensdaten und sensible personenbezogene Daten müssen natürlich auch auf den privaten PCs verschlüsselt werden. Eine bestimmte Mindestausstattung der privaten Geräte ist daher ebenso ein Muss wie der Einsatz standardisierter Software.

Das wirtschaftlich interessante und zukunftsgerichtete Geschäftsszenario für „Bring your own PC“ muss jedoch auch mit den Juristen und Steuerberatern abgeklärt werden. Denn die notwendige Trennung zwischen Firmendaten und privaten Daten ist auch bei diesem Modell eine Pflicht, die aus IT-Compliance und Datenschutz resultiert. Selbst wenn der PC dem Mitarbeiter gehört, muss der Arbeitgeber jederzeit Zugriff auf die unternehmenswichtigen Informationen haben. Hier müssen im Einklang mit dem Bundesdatenschutzgesetz (BDSG) rechtssi-

chere Konzepte für die revisionssichere Archivierung und entsprechende Einsichtsrechte des Arbeitgebers erarbeitet werden. Das BDSG sieht hier derzeit in Paragraf 32 Grenzen vor, die nicht überschritten werden dürfen. Zudem sollen das Datenschutzrecht vollständig überarbeitet und wohl Mitte 2011 sogar ein eigenständiges Beschäftigtendatenschutzgesetz geschaffen werden. Es liegt auf der Hand, dass alte Betriebsvereinbarungen oder IT-Richtlinien die Anschaffung privater IT-Geräte durch den Mitarbeiter nicht regeln. Auch diese Policies müssen daher überarbeitet werden.

1.2.2 Wer haftet bei Ausfall oder Verlust?

Dabei muss zudem verabredet werden, wer bei einem Ausfall oder Defekt der privaten Hardware haftet. Dies bedeutet, dass vor der Anschaffung privater IT genau zu regeln ist, wie die Wartung der privaten Geräte durchgeführt wird, ob und auf welchem Wege also vom Arbeitgeber Ersatz zu beschaffen ist, ob eventuell Leihgeräte für die Ausfallzeit bereitgehalten werden und wer für den Verlust eines Gerätes letztlich haftet. Denn normalerweise muss ein Betriebsmittel dem Mitarbeiter kostenfrei zur Verfügung gestellt werden, und ein Ausfall dieses Arbeitsmittels fällt in das Risiko der Firma. Hier kann ein Rundum-Sorglos-Paket eine Option sein; Hardwareanbieter offerieren bereits seit geraumer Zeit BYoD-Betreibermodelle, die auch Szenarien für den Ausfall privater Geräte beinhalten.

Der Zuschuss des Arbeitsgebers zum privaten PC muss darüber hinaus steuerlich betrachtet werden. Hier stellt sich die Frage, inwieweit der gewährte geldwerte Vorteil zu versteuern ist oder ob der Betrag, der gegebenenfalls über dem Zuschuss des Arbeitgebers liegt, sogar als Werbungskosten geltend gemacht werden kann. Zu regeln ist schließlich auch, wem die möglicherweise ebenfalls privat angeschaffte Software (etwa Apps) bei Beendigung des Arbeitsverhältnisses gehört oder ob ein Zuschuss zum Gerät nur als Darlehen gewährt wird und demgemäß in Raten zurückzuzahlen ist, sollte das Arbeitsverhältnis vorzeitig beendet werden.

1.2.3 Checkliste für Consumer-IT am Arbeitsplatz

- **IT-Security:** Welche Sicherheitsparameter gelten für die privaten Geräte? Welche Art der Verschlüsselung wird eingesetzt?
- **Lizenzen und Software:** Zentrale Softwarebeschaffung oder Eigenbezug der Software durch den Mitarbeiter, eventuell über Home-Use-Programme (wie beispielsweise Microsoft Home Use Program)?
- **(Un-)Managed Client und die Trennung zwischen geschäftlich und privat:** Wie kann zwischen geschäftlichen und privaten Daten unterschieden werden, wie passt diese Mischnutzung in das Informationsmanagement (Stichwort Archivierungskonzept) und wie erfolgt die Synchronisation? Kann eine Partitionierung bei der notwendigen Trennung helfen?

- **Den Business Case für ByoD richtig rechnen:** Wie hoch sind die Zusatzkosten für die Virtualisierung und den Ausbau der Server? Was kostet ByoD insgesamt (Total Cost of Ownership)?
- **Prüfung und Update der IT-Richtlinien:** Pflichtbestandteile der neuen UOD-Richtlinie sind Verantwortlichkeiten, Regelungen zu Wartung, Ersatz und Leihgeräte und Bestimmungen zum finanziellen „Zuschuss" (bei Ausscheiden des Mitarbeiters rückzahlbares Darlehen oder „verlorener Zuschuss", jährliche Beteiligung des Arbeitgebers).
- **Datenschutzrecht:** Einsicht, Nutzungs- und Zugriffsrechte des Arbeitgebers auf die privaten Geräte explizit regeln, die Grenzen des Beschäftigtendatenschutzes einhalten!
- **Steuerrecht:** Anschaffung des PC als Werbungskosten oder Anrechnung des geldwerten Vorteils bei Überlassung von Firmensoftware zu privater Nutzung?

Michael Rath

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

Michael Rath ist auf IT-Recht spezialisierter Anwalt bei der Luther Rechtsanwaltsgesellschaft mbH in Köln.

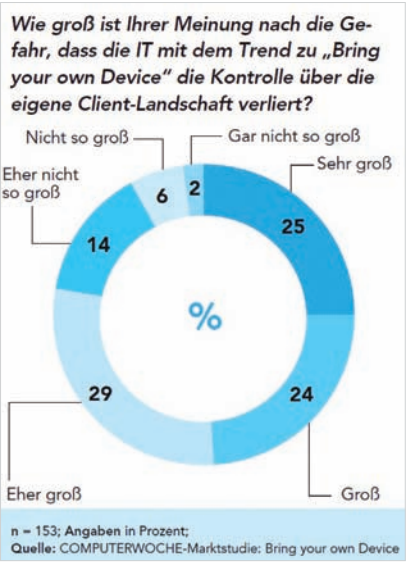
TecChannel-Links zum Thema	Webcode	Compact
ByoD – Private Hardware in der Firma nutzen	2033617	S.17
Die vier Typen mobiler Mitarbeiter	2034864	S.13
ByoD – Super-GAU für die IT-Abteilung?	2035857	S.20
ByoD – Der Tod des Firmen-PCs?	2035860	S.24
iPad und iPhone zwingen zu WLAN-Ausbau	2034964	S.28
System Center Configuration Manager 2012 Beta 2 – neue Features und Funktionen	2035287	S.30

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

1.3 ByoD – Super-GAU für die IT-Abteilung?

Der Angriff kam von unerwarteter Seite: Der Geschäftsführer trat mit seinem neuen iPhone aus der Deckung und wollte damit jederzeit auf seine E-Mails zugreifen können. Kurz darauf klopfte der Vertriebschef in der IT-Abteilung an, ob es nicht möglich sei, die aktuellen Verkaufszahlen auf seinem neuen iPad abzurufen. Und dann brachen die Dämme: Führungskräfte, Abteilungsleiter bis hin zum einfachen Angestellten schleppten mehr und mehr persönliche Devices vom Smartphone über Tablets bis hin zum Netbook in die Firma ein und verlangten Zugang zur Unternehmens-IT. Dieses Szenario dürfte so manchem IT-Leiter bekannt vorkommen. Experten fassen es unter den Schlagworten „Consumerization" beziehungsweise „Bring your own Device" (ByoD) zusammen. Im Grunde treffen dabei jedoch verschiedene Trends aufeinander:

- Die **Grenzen zwischen Arbeitswelt und Privatleben** lösen sich zunehmend auf. Nach Feierabend wird noch einmal gemailt oder an der Präsentation für das nächste Abteilungs-Meeting gefeilt.
- Das Engagement vieler Mitarbeiter in **sozialen Netzen** unterstützt diese Entwicklung: Auf Facebook, Twitter und Co. mischen sich die Kontakte, Privates und Berufliches wird kaum noch voneinander getrennt.



Marktstudie: Fast vier von fünf IT-Verantwortlichen befürchten, durch den Trend „Bring your own Device" (ByoD) die Kontrolle über ihre Client-Landschaft zu verlieren. Ein Viertel stuft diese Gefahr sogar als „sehr groß" ein.

- Dazu kommt der Siegeszug mobiler Endgeräte. Mit breitbandigen Mobilfunkverbindungen und leistungsfähigen Gadgets wie **Smartphones und**

Tablets gehen Anwender jederzeit und von überall ins Netz. Sie sehen einen großen Produktivitätsvorteil darin, auf diese Weise auch auf das Firmennetz und „ihre" Daten zugreifen zu können.

- Durch **Cloud Computing** entwickeln sich Anwendungen, die früher nur innerhalb der Firmengrenzen zu nutzen waren, mehr und mehr zu flexiblen Software-Services.

1.3.1 IT-Abteilungen im Brennpunkt

Wie sollen IT-Organisationen reagieren? Angesichts des vielfältigen und genussvollen privaten IT-Konsums wächst unter Anwendern der Wunsch, auch beruflich schnell und flexibel mit den bekannten Werkzeugen arbeiten zu können. Dass die Nutzer dabei nicht mehr zwischen dem Firmenrechner und ihrem persönlichen Device zu Hause oder unterwegs unterscheiden möchten, ist eine logische Folge.

Das macht die Sache für die IT-Verantwortlichen in den Unternehmen nicht leichter. Sie sehen sich plötzlich mit Forderungen konfrontiert, die ihren Bemühungen der vergangenen Jahre zuwiderlaufen. Ging es zuletzt oft um Standardisierung und Konsolidierung der eigenen IT, um der wachsenden Komplexität Herr zu werden, droht jetzt mit Smartphones und Tablets ein neuer massiver Wildwuchs.

1.3.2 Komplexität kontra Zufriedenheit

Nachdem Apple die Lawine mit seinem iPhone und später dem iPad losgetreten hat, ist der Markt nun für die Wettbewerber geöffnet. Daraus zieht vor allem Google Nutzen: Die offene Android-Plattform findet großen Anklang im Smartphone-Bereich und kommt auch auf Tablet-PCs in Schwung. Während sich Apple und Google in erster Linie an Consumern orientieren und den Administratoren in Sachen Gerätemanagement wenig entgegenkommen, kann BlackBerry-Hersteller Research In Motion (RIM) zumindest in puncto Sicherheit auf offene Ohren bei den IT-Leitern hoffen. Schwer einzuschätzen sind die Aussichten von Microsoft mit Windows Phone 7 sowie Hewlett-Packard mit WebOS.

Angesichts der Plattformvielfalt fragen sich IT-Leiter, wie sie das drohende Chaos in den Griff bekommen sollen. Ihre Steuerungsmöglichkeiten sind gering, weil sich die Mitarbeiter privat je nach Vorliebe für das eine oder das andere Modell entscheiden. Das Thema spaltet die Betroffenen in den IT-Abteilungen in zwei Lager:

- **Die Gegner** warnen vor mehr Komplexität sowie größeren Sicherheitsrisiken und würden am liebsten jedes private Gerät aus ihrem Hoheitsbereich verbannen.
- **Die Befürworter** verweisen auf eine höhere Nutzerzufriedenheit und damit einhergehend auf steigende Produktivität. Sie würden die Client-Verantwortung gerne ganz auf die Nutzer übertragen. Manche Unternehmen gehen

schon dazu über, ihren Mitarbeitern einen Pauschalbetrag in die Hand zu drücken, mit dem sie sich ihre Geräte selbst beschaffen sollen.

IDC-Analystin Eszter Morvay: „Ich denke nicht, dass sich Tablet-PCs in breiter Masse in den Unternehmen durchsetzen werden, da sie weder einen PC noch ein Notebook vollständig ersetzen können."

Inwieweit sich neue Devices wie Tablets im Firmenumfeld durchsetzen werden, ist noch unklar. Während so mancher Experte schon von einem Siegeszug von iPad und Co. spricht, ist IDC-Analystin Eszter Morvay vorsichtiger: „Ich denke nicht, dass sich Tablet-PCs in breiter Masse in den Unternehmen durchsetzen werden, da sie weder einen Desktop-PC noch ein Notebook vollständig ersetzen können." Allerdings seien die Geräte dafür auch nicht gedacht, schränkt die Analystin ein. Vielmehr würden sie zusätzlich je nach Bedarf eingesetzt.

1.3.3 CIOs müssen reagieren

Einig sind sich die Experten darin, dass die IT-Verantwortlichen eine Antwort auf den Trend haben müssen. Zwar werde das Leben für CIOs nicht leichter, sagt Gartner-Analystin Nicole McCormick. Ignorieren lasse sich die Tendenz jedoch nicht mehr, und es helfe auch nicht, den Kopf in den Sand zu stecken.

Trägt man die Empfehlungen der verschiedenen Analysten zusammen, ergibt sich folgendes Bild:

- IT-Leiter sollten offen für die Wünsche der Anwender sein. Der Trend zur Consumerization lässt sich nicht aufhalten. Nur wer sich darauf einlässt, wird den wachsenden Druck meistern und die Vorteile umsetzen können.
- Die IT-Organisation sollte eine Strategie ausarbeiten, wie sie ihre Client-Landschaft gestalten will und welche Techniken – etwa Desktop-Virtualisierung – sie dafür benötigt. Wichtig dabei ist, auch festzulegen, welche Geräte wozu genutzt werden dürfen.
- Sicherheit ist ein wichtiges Thema: Doch wer den Gebrauch privater Geräte rigoros zu reglementieren versucht, riskiert im Endeffekt ebenso viele Sicherheitslecks, weil die Devices dann an der IT vorbei ihren Weg ins Unternehmen finden werden.

- Die Security-Infrastruktur muss in Ordnung sein. Die IT sollte Richtlinien aufstellen, wer auf welche Informationen zugreifen darf. Zudem sollte es Notfallpläne geben für den Fall, dass Geräte mit sensiblen Daten abhandenkommen.
- Beweisen Sie Fingerspitzengefühl bei der Definition der Regeln. Wer beispielsweise damit droht, die Geräte in bestimmten Situationen zu beschlagnahmen, treibt die User dazu, die Devices unter dem Radar der IT-Abteilung durchzuschleusen.
- Angesichts der wachsenden Komplexität rund um neue Endgeräte und Apps empfiehlt Forrester Research, die Verantwortlichkeit für das Management der damit verbundenen Infrastruktur zu bündeln und beispielsweise die Position eines Chief Mobility Officers einzurichten.

Martin Bayer

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

Martin Bayer ist Redakteur der Zeitschrift Computerwoche. Er befasst sich unter anderem mit Business-Software, PC- und Notenbook-Themen sowie Speicherlösungen und Home-IT.

TecChannel-Links zum Thema	Webcode	Compact
ByoD – Super-GAU für die IT-Abteilung?	2035857	S.20
Die vier Typen mobiler Mitarbeiter	2034864	S.13
ByoD – Private Hardware in der Firma nutzen	2033617	S.17
ByoD – Der Tod des Firmen-PCs?	2035860	S.24
iPad und iPhone zwingen zu WLAN-Ausbau	2034964	S.28
System Center Configuration Manager 2012 Beta 2 – neue Features und Funktionen	2035287	S.30

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

1.4 BYOD – Der Tod des Firmen-PCs?

Die Zeichen der Zeit stehen auf Veränderung. Immer mehr Mitarbeiter wollen auch in ihrem Arbeitsalltag nicht auf iPhone, iPad oder andere schicke Smartphones und Tablet-PCs verzichten. Während der Trend „Bring your own Device" (BYOD) in vielen IT-Abteilungen noch auf etliche (berechtigte)Vorbehalte trifft und vielerorts rigide Regeln den Gebrauch persönlicher Devices innerhalb der eigenen Firmen-IT verbieten, verweisen Experten auch auf die Vorteile.

„Bring your own Device" lasse sich eben nicht auf Probleme rund um Sicherheit und höhere Anforderungen in Sachen Client-Management reduzieren. Dem stünden eine höhere Produktivität und eine größere Nutzerakzeptanz gegenüber – Aspekte, von denen die Unternehmen durchaus profitieren könnten. Den IT-Verantwortlichen raten die Analysten von Gartner, IDC, Forrester und Co. deshalb dringend, sich auf das kommende IT-Zeitalter vorzubereiten und sich von den herrschenden Vorurteilen zu verabschieden.

1.4.1 BYOD – nur eine Frage der Zeit

Aus Sicht von Analysten ist es nur noch eine Frage der Zeit, bis IT-Abteilungen dem Drängen der Anwender nach Bring your own Device nachgeben müssen:

- **IDC** (www.idc.com) zufolge nutzen 95 Prozent aller Mitarbeiter mindestens ein privates Endgerät auch für berufliche Zwecke.
- **Gartner** (www.gartner.com) geht davon aus, dass 2014 rund 90 Prozent aller Unternehmen Business-Applikationen auf Devices unterstützen werden, die den Endanwendern gehören.
- **Forrester Research** (www.forrester.com) hat herausgefunden, dass 37 Prozent der fast 2800 befragten Anwender in nordamerikanischen und europäischen Unternehmen ein Smartphone besitzen. Doch lediglich 17 Prozent nutzten diese Geräte für berufliche Belange. Damit verspielten die Unternehmen etliches Produktivitätspotenzial, so das Fazit der Analysten.

1.4.2 Vorurteil 1: BYOD bringt keine Produktivitätsvorteile

Mit dem Aufkommen leistungsstarker Smartphones und Tablet-Rechner bekommt die Mobilisierung der IT und damit auch die der eigenen Mitarbeiter einen zusätzlichen Schub. Nach Schätzungen der Analysten von IDC arbeiten bereits heute mehr als eine Milliarde Menschen weltweit auch mobil. Mittlerweile sei es die Regel, die eigenen Mitarbeiter mit mobilen Endgeräten, meist einem Notebook, auszustatten. Die IT ist in der Post-PC-Ära angekommen, lautet daher das einhellige Fazit der Experten. Mit der zunehmenden Mobilisierung nimmt die Produktivität in den Unternehmen zu, haben Marktforscher festgestellt.

Vor allem steige mit der Nutzung eigener Devices die Akzeptanz der User, meinen Analysten von Gartner. Statt wie früher Anträge in der IT-Abteilung stellen zu müssen, die zudem nicht selten abgelehnt wurden, könnten die Anwender nach dem ByoD-Prinzip mit den Geräten arbeiten, die ihrem persönlichen Stil entsprechen. Berücksichtigten Firmen diese individuellen Vorlieben, stiegen automatisch die Zufriedenheit der Nutzer und damit ihre Produktivität.

Das schlägt sich offenbar in messbaren Produktivitätsgewinnen nieder. Laut einer Studie von iPass (www3.ipass.com) arbeiten Angestellte mit mobilen Geräten, die sie für persönliche Anliegen wie für Unternehmenszwecke einsetzen dürfen, im Schnitt 240 Stunden mehr pro Jahr. Dass sich dabei die Grenzen zwischen Privatleben und Arbeit zunehmend auflösen, sei insbesondere für Digital Natives, die mit diesen Geräten und dem Internet groß geworden sind, kein Problem.

Im Gegenteil: Die nachwachsende Generation, die in den kommenden Jahren in die Unternehmen drängt, ist ständig online und organisiert sich – sei es privat oder im Arbeitsleben – über soziale Netze. Dies mit dem persönlich favorisierten Device jederzeit und von jedem Ort aus tun zu können wird zunehmend zu einer Bedingung. Mehr Produktivität verspricht auch die kommende Generation von Business-Applikationen. Softwarehersteller wie SAP und Oracle arbeiten mit Hochdruck daran, ihre Anwendungen zu mobilisieren. Beispielsweise ist das Management von Anwenderunternehmen so in der Lage, Auswertungen und Analysen aktueller Business-Zahlen via iPad abzurufen. Damit ließen sich Geschäftsentscheidungen schneller und sicherer treffen, so das Versprechen der Anbieter. Mit einer breiten Unterstützung verschiedener Endgeräte steigt auch die Bereitschaft, diese Anwendungen zu nutzen.

1.4.3 Vorurteil 2: ByoD erschwert Support und Management

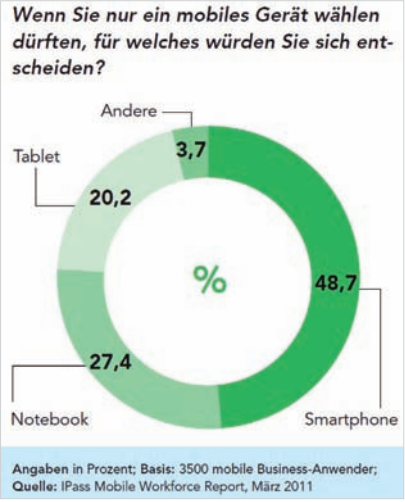
Mit der neuen Mitarbeitergeneration werde sich auch die Rolle der IT-Abteilungen massiv verändern, prognostizieren die Experten von Gartner. Die Befürchtungen vieler CIOs, Support und Management seien in einer zunehmend heterogenen Client-Landschaft nicht mehr zu bewältigen, wollen sie nicht gelten lassen. Vielmehr würden die Mitarbeiter mehr Verantwortung für die eigenen Geräte übernehmen, sagt Gartner-Analyst Jack Santos. Es liege in der menschlichen Natur, sich um die Dinge besser zu kümmern, die man auch selbst kontrolliert.

Mit der stärkeren Verantwortung der User würden letztendlich auch die IT-Abteilungen entlastet. Gartner schätzt, dass Unternehmen im Rahmen einer gut geplanten ByoD-Strategie bis zu 40 Prozent des Aufwands für die Anschaffung und das Management der eigenen Client-Landschaft einsparen könnten. Darüber hinaus seien die künftigen IT-Nutzer in den Unternehmen technisch versierter, sind sich die Experten von iPass sicher. Kleinere Probleme ließen sich selbstständig lösen, ohne sofort den Helpdesk der firmeneigenen IT-Abteilung bemühen zu müssen. Und auch bei größeren Problemen würden die User nicht sofort verzweifeln. Vielmehr machten sie sich auf eigene Verantwortung im Netz schlau und suchten

nach Lösungen, beispielsweise in Foren, sozialen Netzen beziehungsweise bei Kollegen. Auf Basis des wachsenden technischen Know-hows würden die Anwender künftig auf mehr Mitspracherecht bei IT-Entscheidungen pochen. Gartner-Analyst Ken McGee verweist auf die Entwicklungen rund um Cloud Computing. Oft würden Entscheidungen, bestimmte Software-Services einzukaufen, schon heute in den Fachabteilungen getroffen, ohne die IT hinzuzuziehen. „Die Technik ist nicht mehr das alleinige Revier des CIOs. Sie entwickelt sich zu jedermanns Gut und damit zu jedermanns Problem."

1.4.4 Vorurteil 3: BYoD reißt tiefe Sicherheitslücken in die Firmen-IT

Wenn jeder Mitarbeiter sein eigenes Device mitbringt, leidet die IT-Sicherheit. Das ist das Hauptargument, das viele IT-Verantwortliche gegen BYoD ins Feld führen. Dabei dürften die damit verbundenen Folgen für die meisten Unternehmen nicht neu sein, sagen die Gartner-Experten. Schon in der Vergangenheit hätten vielerorts externe Fachkräfte mit ihren eigenen Geräten innerhalb der Firmen-IT agiert.



Offenbar keine eindeutige Sache: Welches mobile Gerät hätten Sie gerne?

Das gelte etwa für Berater, die sich um die Implementierung neuer Systeme oder Prozesse gekümmert haben. Im Rahmen dieser befristeten Engagements sei es in der Regel nicht möglich, alle sensiblen Unternehmensanwendungen und -daten hermetisch vor den Externen abzuschotten, stellt Gartner-Analyst Chris Wolf fest. Das sei durchaus brisant, gerade weil diese Wanderarbeiter eventuell für ihren nächsten Auftrag bei einem Konkurrenten arbeiten.

Daher hätten sich die IT-Verantwortlichen schon in der Vergangenheit darum kümmern müssen, dass der Zugang zu kritischen Informationen reglementiert und dafür gesorgt sei, dass keine Firmendaten auf den Devices externer Mitarbeiter verbleiben, wenn sie das Unternehmen wieder verlassen.

Die Unsicherheit im Zusammenhang mit ByoD sei deshalb so groß, weil die meisten IT-Verantwortlichen noch nicht die Zeit gefunden hätten, sich mit allen Sicherheitsrisiken und -lösungen rund um iPhone, iPad und Co. wirklich auseinanderzusetzen, glaubt IDC-Analyst Ian Song. Dabei seien im Markt bereits Techniken verfügbar, mit deren Hilfe sich unterschiedlich zusammengesetzte Client-Landschaften absichern ließen. Beispielsweise könnten Unternehmen mittels Virtual-Desktop-Infrastructure- (VDI-) und Terminal-Lösungen dafür sorgen, dass sich keine kritischen Unternehmensdaten auf den Endgeräten einnisteten, sagt Mark Bowker, Analyst der Enterprise Strategy Group (www.enterprisestrategygroup.com). Das nehme dem Gespenst des Diebstahls oder Verlusts, der vielen CIOs den Schlaf raubt, den Schrecken. Müssten dennoch einmal Daten auf das Device geladen werden, sorgen Verschlüsselungslösungen für deren Sicherheit. Klare Regeln, wer wie auf welche Daten im Firmennetz zugreifen darf, sowie Lösungen rund um Virtual Private Networks (VPN) und Identity-Management sicherten die Firmen-IT auch mit iPhone und iPad ab.

Viele Experten warnen die IT-Verantwortlichen zudem davor, sich mithilfe rigider Vorschriften zu sehr absichern zu wollen. Viele persönliche Devices würden trotzdem an der IT vorbei ihren Weg in die Firmen-IT finden und dort dann ein unkalkulierbares Sicherheitsrisiko darstellen. Der Trend in Richtung Consumerization ist aus Sicht der Analysten von Gartner nicht mehr aufzuhalten. Die nächste Phase dieser Entwicklung sei bereits in Sicht, sagt Brian Gammage, Vice President von Gartner. Dabei werde sich die Aufmerksamkeit der Nutzer und IT-Abteilungen abwenden von Geräten, Infrastruktur und Anwendungen. In Zukunft gehe es hauptsächlich darum, wie Informationen verteilt werden und die Zusammenarbeit zwischen Kollegen und verschiedenen Mitgliedern in einem Netz geregelt wird.

Martin Bayer

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

TecChannel-Links zum Thema	Webcode	Compact
ByoD – Der Tod des Firmen-PCs?	2035860	S.24
ByoD – Super-GAU für die IT-Abteilung?	2035857	S.20
Die vier Typen mobiler Mitarbeiter	2034864	S.13
ByoD – Private Hardware in der Firma nutzen	2033617	S.17
iPad und iPhone zwingen zu WLAN-Ausbau	2034964	S.28
System Center Configuration Manager 2012 Beta 2 – neue Features und Funktionen	2035287	S.30

1.5 iPad und iPhone zwingen zu WLAN-Ausbau

Der zunehmende Einsatz von Smartphones und Tablet-PCs in Firmen wird weltweit für ein starkes Wachsen von drahtlosen Netzen sorgen. Laut aktuellen Studien bauen Unternehmen neue drahtlose Netze auf und erweitern bestehende Infrastrukturen. Eine Herausforderung für IT-Abteilungen.

Beim Ingolstädter Automobilkonzern Audi arbeitet man bereits seit einem halben Jahr daran, für den Einsatz von iPad und iPhone in der Fahrzeugfertigung die drahtlosen Netze zu erweitern. „Durch das iPad werden sich Änderungen in der gesamten Netzwerkarchitektur ergeben, weil wir zunehmend über WLAN und UMTS auf unsere Daten zugreifen", meinte dazu schon im Oktober 2010 Jürgen Holderried. Dafür, so der Leiter der IT-Services bei der Audi AG, sei es erforderlich, die Sicherheitszonen umzubauen, „um so eine geeignete, sichere und stabile Umgebung für den Betrieb gewährleisten zu können – egal, ob der Anwender sich im Firmennetz aufhält oder unterwegs ist". So wie Audi geht es derzeit wahrscheinlich vielen Unternehmen weltweit, die an Projekten arbeiten, iPad und iPhone im Unternehmen produktiv einzusetzen. Davon sind – auch das zeigt das Beispiel Audi – längst nicht nur drahtlose Netze außerhalb der Firmen betroffen, sondern zunehmend auch die innerhalb der IT-Infrastruktur.

Der Boom, haben aktuelle Studien ergeben, sorgt auch bei den Produzenten von WLAN-Ausrüstung für Hochzeiten. So haben die Marktforscher von Infonetics Research herausgefunden, dass der weltweite Umsatz mit Drahtloszubehör allein im vierten Quartal 2010 um 28 Prozent im Vergleich zum Vorjahresquartal auf 769 Millionen US-Dollar (rund 558 Millionen Euro) gestiegen ist.

1.5.1 Cisco, Aruba und HP liegen vorne

Ein Report von Marktforscher Dell'Oro bestätigt diesen Wachstumstrend: Für das komplette Jahr 2010 seien die Umsätze mit WLAN-Accessoires um 25 Prozent auf einen Gesamtwert von mehr als fünf Milliarden US-Dollar – das entspricht rund 3,6 Milliarden Euro – gestiegen. Dabei würden die firmeninternen Netze den Löwenanteil ausmachen.

Allerdings rangiert der weltweite Umsatz in Höhe von 18,8 Milliarden US-Dollar (rund 13,6 Milliarden Euro) mit Netzwerktechnologien noch immer deutlich vor dem der WLANs. Bei den Wachstumsraten dagegen liegen die Drahtlostechnologien mit zehn Prozent deutlich vorne (Netzwerktechnologien: plus ein Prozent).

Die wachsende Zahl mobiler Endgeräte habe bei den Firmen Aktivitäten für den Aufbau neuer und den Ausbau bestehender Drahtlosnetzwerke ausgelöst, so das Ergebnis beider Studien. Die Netzwerke müssten in der Lage sein, immer mehr Smartphones und Tablet-PCs mit dem Internet und den firmeneigenen Netzwer-

ken zu verbinden. Wo das nicht gehe, müsse man die bestehenden Kapazitäten eben erweitern. Beim Umsatz vorne liegen drahtlose Systeme von Cisco, gefolgt von Aruba Networks, Hewlett-Packard und Motorola, hat Infonetics in seiner Studie herausgefunden.

Allein in den vergangenen sechs Monaten habe sich der Markt stärker verändert als in den sechs Jahren davor, stellt Roger Hockaday, Marketingdirektor des Anbieters Aruba in Europa, fest. Der größte Teil dieses Wachstums gehe auf das Konto von Apples iPad. Vor der Auslieferung des Tablet-PCs seien drahtlose Netze in Unternehmen eher ein Luxusgut gewesen, beispielsweise, um Besuchern Internetempfang zu ermöglichen.

1.5.2 Netzwerkarchitekturen müssen auf den Prüfstand

Heutzutage sei daraus aber schon eine Notwendigkeit geworden, weil die Mitarbeiter eher auf drahtlose Verbindungen Wert legten als auf drahtgebundene. So könnten sie Geräte wie das iPad nicht nur in ihrem Büro oder in Konferenzräumen, sondern überall im Unternehmen einsetzen.

Die IT-Abteilungen in den Unternehmen müssten daher ihre Netzwerkarchitekturen auf den Prüfstand stellen, fordert Hockaday. Es seien mit Drahtlosnetzen größere Gebiete abzudecken als zuvor.

Durch neue Geräte mit wachsenden Fähigkeiten – so verfügt zum Beispiel das Apple iPad 2 über zwei integrierte Kameras und FaceTime-Technologie für einfache Videokonferenzen – entsteht in exponentieller Größenordnung zusätzlicher Bedarf an Bandbreite.

Thomas Pelkmann

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation CIO.

TecChannel-Links zum Thema	Webcode	Compact
iPad und iPhone zwingen zu WLAN-Ausbau	2034964	S.28
Die vier Typen mobiler Mitarbeiter	2034864	S.13
ByoD – Private Hardware in der Firma nutzen	2033617	S.17
ByoD – Super-GAU für die IT-Abteilung?	2035857	S.20
ByoD – Der Tod des Firmen-PCs?	2035860	S.24
System Center Configuration Manager 2012 Beta 2 – neue Features und Funktionen	2035287	S.30

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

1.6 System Center Configuration Manager 2012 Beta 2 – neue Features und Funktionen

Wer sich einen Überblick über die neuen Möglichkeiten von System Center Configuration Manager (SCCM) 2012 machen will, kann die englische Beta-2-Version kostenlos bei Microsoft herunterladen.

Allerdings ist die Beta-Version noch deutlich eingeschränkt. So können Sie Smartphones und Linux-Computer erst mit der endgültigen Version von SCCM 2012 oder durch nachgereichte Patches verwalten. In der Beta-Version fehlt diese Unterstützung. Ausführliche Hilfen zum Produkt finden Sie auf der TechNet-Seite von SCCM 2012 (http://technet.microsoft.com/de-DE/evalcenter/ff687182.aspx).

1.6.1 Anwender intelligent anbinden

System Center Configuration Manager 2012 stellt bei der Verwaltung die Anwender in den Mittelpunkt. Microsoft spricht von einer benutzerorientierten Verwaltung (User Centric Management, UCM). Anwender können beim Verwenden von System Center Configuration Manager 2012 mit mehreren Endgeräten arbeiten, zum Beispiel Arbeitsstation, Heimarbeitsplatz, Notebook und Smartphone.

Eine wichtige Neuerung ist die Möglichkeit, für Anwender ein primäres Endgerät festzulegen und umgekehrt jedem Endgerät einen primären Anwender zuzuweisen. Geräten, die Sie im Schichtbetrieb einsetzen, können Sie auch mehrere primäre Anwender zuteilen. Über diesen Weg lässt sich die IT-Infrastruktur also sehr detailliert darstellen.

Neue Version: Zentrale Installationsoberfläche des System Center Configuration Manager 2012.

Mit diesen Zuordnungen lassen sich Regeln definieren, mit denen Anwendern Applikationen effizienter und situationsbedingt zur Verfügung gestellt werden. Meldet sich der User zum Beispiel an seinem primären Gerät in der Zentrale an, installiert SCCM die notwendigen Anwendungen direkt auf dem Computer. Bei der Anmeldung an anderen Computern, zum Beispiel zu Hause oder in Niederlassungen, erkennt der SCCM dies und bindet den Nutzer entweder über virtualisierte Anwendungen mit App-V oder den Remote-Desktop-Diensten an. Diese intelligente Unterscheidung konnten die Vorgängerversionen noch nicht treffen. Ermöglicht wird das durch die neue Funktion, einem Softwarepaket mehrere Bereitstellungsszenarien zuzuordnen. Administratoren können in SCCM jetzt verschiedene Regeln und Wege festlegen, mit denen eine Anwendung zur Verfügung steht. Das kann eine echte Installation sein, die Bereitstellung als virtuelles App-V-Paket oder über den Remote-Desktop. Auch Apps für mobile Endgeräte verwalten Sie auf diese Weise. Neben diesen Möglichkeiten lassen sich Anwendungen auch in Abhängigkeit voneinander setzen. Soll auf einem Computer zum Beispiel die Anwendung A installiert werden, die von B abhängig ist, dann installiert SCCM erst die Anwendung B und anschließend die Anwendung A.

1.6.2 Software bereitstellen

Neben der automatisierten Installation können Sie in SCCM 2012 auch Applikationen auf diesem Weg wieder vom Computer oder Endgerät des Nutzers entfernen. Das Entfernen funktioniert für App-V-Anwendungen genauso wie bei herkömmlich installierten Programmen. Betreiben Sie eine Testumgebung mit SCCM 2012, in der Sie die Kompatibilität von Programmen testen, haben Sie die Möglichkeit, sie in die Produktionsumgebung zu übernehmen, sobald Sie mit den Einstellungen zufrieden sind. In SCCM 2012 können Anwender im Software Center ihre Arbeitszeiten hinterlegen. Muss SCCM Wartungsarbeiten am Computer des Users durchführen, zum Beispiel Patches oder Programme installieren, kann der Server das dann außerhalb der Arbeitszeit durchführen. Dieses Software Center ist eine Weboberfläche in SCCM, über die Benutzer auch Anwendungen anfordern und installieren können. Die Installation erfolgt dann automatisiert nach der Genehmigung durch den Administratoren. Die Verwaltung dieser Oberfläche ist sehr einfach gehalten und erfordert keine komplizierte Einarbeitung.

Administratoren können auf dieser Basis festlegen, dass zum Beispiel bei der Anmeldung an einem Computer in einer Niederlassung keine Anwendungen installiert werden, sondern der User die entsprechenden Remote-Desktop-Dienste-Verbindungen erhält. In der Zentrale kann der gleiche User an seinem Computer aber mit der Anwendung lokal arbeiten. Anwendungen lassen sich in der neuen Version also auf verschiedenen Wegen bereitstellen, und die User erhalten überall Zugriff auf die wichtigsten Daten und Applikationen. Auf diesem Weg können Administratoren auch festlegen, ob Benutzer bestimmte Applikationen selbst zur Installation auswählen dürfen, oder ob SCCM die Anwendung automatisch bereitstellt.

Auch hierzu dient dann das Software Center. Weiterhin integriert sind Funktionen zur Inventarisierung der Geräte sowie eine Patch-Verwaltung. Diese basiert auf Windows Server Update Services. In diesem Zusammenhang unterstützt SCCM auch die Netzwerkzugriffsrichtlinien von Windows Server 2008 und Windows Server 2008 R2. Auf deren Basis lässt sich feststellen, ob Client-Computer über die entsprechenden Sicherheitseinstellungen verfügen, bevor eine vollständige Netzwerkanbindung erfolgt.

1.6.3 Betriebssysteme verteilen

Der System Center Configuration Manager 2012 kann nicht nur Anwendungen mit verschiedenen Regeln bereitstellen und Geräte inventarisieren, sondern auch Betriebssysteme auf Endgeräten automatisiert bereitstellen. Im Gegensatz zu Vorgängerversionen müssen Sie im SCCM 2012 nicht für jede Site eigene Boot-Medien bereitstellen. Diese sind jetzt in der gesamten Infrastruktur verfügbar und lassen sich zentral verwalten. Ebenfalls integriert ist das User State Migration Tool (USMT) 4.0, das dazu dient, Benutzereinstellungen zu übernehmen. Das Booten über Netzwerk (PXE) funktioniert wesentlich zuverlässiger und einfacher. Installationen von Anwendungen und Patches lassen sich in Offline-Bereitstellungen von WIM-Images integrieren und an angebundene Clients verteilen. Auch hier arbeitet SCCM 2012 wesentlich zuverlässiger als die Vorgängerversionen.

1.6.4 Linux, Unix und Smartphones anbinden

Im System Center Configuration Manager 2012 ist eine bessere Unterstützung für Linux und Unix-Server enthalten. Ohne Zusatzanwendungen können Sie diese Server jetzt nach der Installation anbinden. Diese Möglichkeiten sind allerdings noch nicht in der Beta-Version verfügbar; das gilt auch für die Verwaltung von Smartphones auf Basis von Windows Phone 7, iOS oder Android. Erst nach der Veröffentlichung der RTM werden diese Funktionen nachträglich integriert. Geplant ist eine Einbindung von AIX, HP-UX, Red Hat Enterprise Linux, Solaris und Suse Linux Enterprise Server. Andere Editionen stehen zumindest offiziell nicht auf der Liste der unterstützten Betriebssysteme. Android, iOS und Windows Phone 7 sollen nach der Veröffentlichung der RTM-Version ebenfalls verwaltet werden können. Allerdings geht auch hier SCCM 2012 nicht sonderlich weit. Grundsätzlich hat Microsoft in System Center Configuration Manager 2012 die Funktionen des weniger erfolgreichen System Center Mobile Device Managers 2008 integriert. Neben iOS, Android und Windows Phone 7 sollen auch Symbian-Geräte verwaltbar sein. Leider bietet SCCM hier keine umfassenden Möglichkeiten, sondern im Grunde genommen nur die Weiterleitung von Richtlinien auf Basis von Exchange ActiveSync. Ob hier Microsoft mit Patches für SCCM 2012 nach der Veröffentlichung der RTM-Version nachbessert, ist noch nicht bekannt.

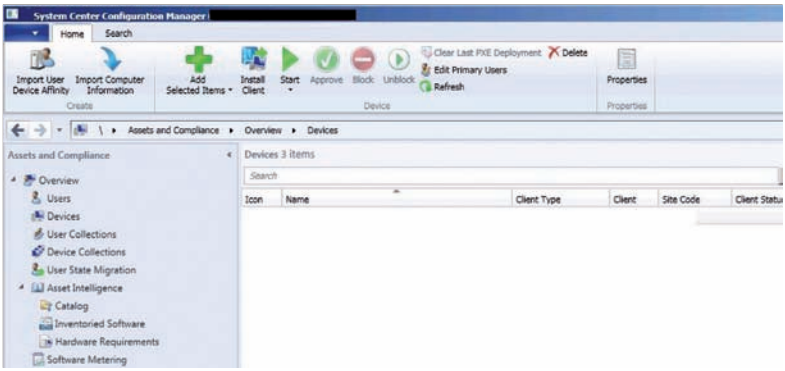
1.6.5 Änderung an den Standorten und verbesserte Verwaltung

Wie schon die Vorgängerlösungen, bindet sich auch SCCM 2012 eng in das Active Directory ein, um die verwalteten Computer und angebundenen Benutzer auszulesen. Als Datenbank für die Konfiguration der Daten und der Berichte lässt sich der Server an SQL Server 2008 anbinden, die Beta-Version unterstützt SQL Server 2008 R2 nicht. Ob sich das mit der RTM ändert, ist noch nicht klar. Die Schemaerweiterungen für SCCM 2012 sind die gleichen wie bei SCCM 2007.

Neu ist die Aufteilung der verschiedenen Sites in SCCM 2012. Zum Beispiel spielen primäre Sites nicht mehr eine so große Rolle in der Konfiguration wie noch in den Vorgängerversionen. Hier hat Microsoft neue Möglichkeiten integriert. Um Anwendungen optimal zu verteilen, müssen Sie nicht mehr alle wichtigen Standorte als primäre Standorte definieren. Die oberste Ebene einer SCCM-2012-Installation stellt die Central Administration Site (CAS) dar. Mit ihr lassen sich alle Standorte, egal ob primäre oder sekundäre, anbinden und verwalten. Dieser Site sind keinerlei Clients zugeordnet, sondern Sie verwenden diesen neuen Site-Typ nur zur Verwaltung und zum Erstellen von Berichten. Diese basieren auf den Reporting-Services von SQL-Server.

1.6.6 Von Sites und Rollen

Mit jeder primären Site können Sie bis zu 100.000 Clients verwalten. Außerdem lassen sich diese Sites nicht unterhalb von primären Sites zuordnen. Primäre Sites stellen nicht länger eine Grenze für Sicherheitseinstellungen, Rechte oder Einstellungen für Clients dar. Aus Stabilitäts- und Redundanzgründen bietet es sich an, auch in kleineren Umgebungen mehrere primäre Sites zu betreiben.



Arbeitsgerät: Über die neue Konsole des SCCM 2012 nehmen Administratoren die Änderungen vor.

Primäre Sites lassen sich nicht mehr herabstufen, die Möglichkeit der Herabstufung haben Sie aber weiterhin bei sekundären Sites. Auf diese Weise können Sie sekundäre Sites zu Distribution Points umwandeln. Auf Servern, auf denen Sie eine sekundäre Site betreiben, installiert der Assistent SQL Server 2008 Express Edition. Die Server tauschen ihre Daten hauptsächlich mit der SQL-Server-Replikation aus. Allerdings gibt es auch weiterhin dateibasierte Replikation zwischen den Servern, zum Beispiel für Patches, Softwarepakete und Betriebssystem-Images. Zusammen mit Windows 7 Ultimate oder Enterprise unterstützt SCCM 2012 auch die BranchCache-Funktionalität zum besseren Datenaustausch.

Wie bei den meisten aktuellen Serverprodukten von Microsoft lassen sich auch in SCCM 2012 rollenbasierte Berechtigungen erteilen und Aufgaben zuweisen. Die neue Verwaltungsoberfläche zeigt dann die Befehle an, für die der entsprechende Administrator auch berechtigt ist. Die Konsole baut nicht mehr auf der Managementkonsole auf, sondern wurde komplett geändert. Sie ist schneller, leichter zu überblicken und bietet mit Registerkarten eine bessere Verwaltung. Sie haben die Möglichkeit, vorgefertigte Rollen zu verwenden, aber auch, eigene zu erstellen. Grundsätzlich arbeitet SCCM 2012 genauso mit der rollenbasierten Zugriffsberechtigung (RBAC) wie Exchange Server 2010.

1.6.7 Kompatibilität und Systemanforderungen

Um den Server zu installieren, bietet sich Windows Server 2008 R2 SP1 an. Auf diesem Server sind alle Serverrollen unterstützt. SCCM 2012 gibt es, wie alle neuen Serverversionen – zum Beispiel Exchange Server 2010, SharePoint Server 2010 und auch Windows Server 2008 R2 -, nur noch als 64-Bit-Version.

Microsoft bietet eine umfangreiche Liste (http://go.microsoft.com/?linkid=9766556) der unterstützten Serverversionen. Distribution Points sollen sich mit der RTM aber auch auf 32-Bit-Systemen betreiben lassen, sicher ist das jedoch noch nicht. Die Datenbank vom SCCM 2012 muss auf einer 64-Bit-Installation von SQL Server 2008 SP1 CU 10/11 installiert werden. Die aktuelle Beta 2 des SCCM 2012 unterstützt weder das SP2 für SQL Server 2008 x64 noch SQL Server 2008 R2.

An die aktuelle Beta-2-Version können Sie die 32-Bit-Version von Windows XP Professional SP3 sowie Windows XP x64 mit SP2 anbinden. Windows Vista kann SCCM 2012 in den Editionen Business, Enterprise und Ultimate verwalten, Sie müssen aber das Service Pack 2 installieren. Natürlich können Sie Windows 7 in den Editionen Enterprise und Ultimate anbinden. Windows 7 Professional ist aktuell nicht auf der Liste der unterstützten Betriebssysteme zu finden. Unterstützt sind die 32-Bit- und 64-Bit-Versionen. Ebenfalls verwalten können Sie Windows Server 2003 SP2/2003 R2/2008/2008 R2 in den Editionen Standard, Enterprise und Datacenter. Windows Server 2008 für Itanium-basierte Systeme unterstützt SCCM 2012 dagegen nicht. Neben einer vollständigen Installation lassen sich auch Core-Server von Windows Server 2008/2008 R2 integrieren.

1.6.8 Exchange-ActiveSync-Richtlinien und SCCM 2012

In der Beta-Version lässt sich noch Exchange Server 2010 für die Verwendung des Exchange-Server-Connectors anbinden. Über diesen Connector liest der System Center Configuration Manager 2012 Exchange-ActiveSync-Richtlinien ein und leitet diese an die angebundenen Endgeräte weiter.

SCCM 2007 unterstützt ältere Windows-Mobile-Versionen mit eigenen Verwaltungsfunktionen. Diese überschneiden sich allerdings mit den ActiveSync-Richtlinien. Daher geht SCCM 2012 einen anderen Weg und bindet die Exchange-ActiveSync-Richtlinien direkt von den Exchange-Servern ein – eine Technologie, die SCCM 2012 von System Center Device Manager 2008 übernommen hat.

Die entsprechenden Einstellungen dazu nehmen Sie direkt in den Eigenschaften des Exchange-Server-Connectors vor. Über diesen Connector können Administratoren angebundene Endgeräte auch über das Internet löschen (Remote Wipe). Der Connector kann aber nicht nur Richtlinien von Exchange an die Clients weiterleiten, sondern auch Inventuren der angebundenen Geräte durchführen.

1.6.9 Migration und Test

Sie können System Center Configuration Manager 2007 nicht direkt auf SCCM 2012 aktualisieren (In-Place-Update), es gilt den Server neu zu installieren. Die Site-Struktur ist neu aufzubauen und parallel zu installieren, da die zahlreichen Änderungen keine direkte Aktualisierung durchlassen. Wollen Sie SCCM 2012 einsetzen, müssen Sie die Infrastruktur daher parallel zu bestehenden Installationen einsetzen. Es gibt aber integrierte Werkzeuge zur Migration.

Um SCCM 2012 in eine Infrastruktur mit SCCM 2007 zu installieren, muss mindestens das SP2 für SCCM 2007 installiert sein. Während des Migrationszeitraums führt SCCM 2012 eine Synchronisierung der Daten zur neuen Infrastruktur durch. Softwarepakete müssen Sie nicht neu erstellen, diese bleiben in SCCM 2012 erhalten. Um die neuen Funktionen zu nutzen, sind die die Pakete aber manuell umzuwandeln.

Distribution Points gibt SCCM automatisch während der Migration frei. Auf diese Weise können SCCM 2007- und SCCM 2012-Clients parallel auf die Daten freigeben. Um eine Testinstallation durchzuführen, benötigen Sie eine recht umfangreiche Anleitung; besuchen Sie hierfür am besten einen TechNet-Blog.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

2 Sicherheit

Die zunehmende Nutzung von Smartphones und Tablet-PCs im geschäftlichen Umfeld zwingt die IT-Sicherheitsverantwortlichen zur Anpassung ihrer bisherigen Security-Strategien. Von den mobilen Kommunikationsgeräten geht ein erhebliches Gefährdungspotential aus, weil die Nutzer häufig viel zu sorglos sind.

2.1 Smartphones: Malware-Gefahr wächst

Es ist eigentlich nicht anders zu erwarten, als dass ein Security-Anbieter die Sicherheitsbedrohungen im Netz in den schwärzesten Farben malt. Schließlich will er seine Lösungen ja verkaufen, mit denen Anwender sich vor Cyber-Piraten schützen können. Das gilt auch für das Unternehmen Trusteer (www.trusteer.com), das sich um sichere Web Access Services kümmert. Deren Warnung: In ein bis spätestens zwei Jahren sind 5,6 Prozent aller Android-Handys und iPhones mit Finanz-Malware und Trojanern infiziert, die den Usern das Geld von ihrem Konto saugen wollen. Möglich mache dies zum einen, dass Google neue Apps von Herstellern im Android Market nicht auf Sicherheitsrisiken durchleuchtet. „Im Vergleich zu Apples App Store is der Android Market der Wilde Westen", schreibt Trusteer-CEO Mickey Boodaei. Aber auch das iPhone-Betriebssystem iOS sei stark gefährdet – durch Jailbreak. Viele User öffneten Schadcodes Tür und Tor, indem sie mit einem Jailbreak ihres Smartphones Software den Weg ebnen, die nicht von Apple freigegeben wurde. Kürzlich sei wieder eine Sicherheitslücke aufgetaucht, über die Malware-Programmierer iPhones ganz ohne Zustimmung des Besitzers vom Internet aus jailbreaken können. Die Rede ist von infizierten PDF-Dokumenten, die beim Öffnen durch den User das Handy knacken. Jetzt sei es nur noch eine Frage der Zeit, bis Cyber-Kriminelle Apple iOS systematisch nach Lücken durchforsten – und diese dann in Black Hole Exploit Kits integrieren. Diese Kits könnten dann ein iPhone nach dem anderen automatisiert infizieren.

2.1.1 Mobile Banking ist das Hauptziel der Angreifer

Beim Mobile Banking mit Android-Handys bedienen sich Cyber-Gangster laut Trusteer gerne einer Man-in-the-Mobile-Attacke (MITMA). Dabei wird sowohl das Online-Banking-Portal der Bank als auch das Handy infiziert. Der User glaubt, die Bank wolle eine Sicherheits-Software aufspielen, bestätigt eine entsprechende Nachricht, und gibt so den Weg frei für die Ganoven. Die können dann in Seelenruhe sein Konto leerräumen. Trusteer-Chef Boodaei spricht vom „größten Sicherheitsproblem für Kunden, das wir kennen". Noch böten Handy-Nutzer zwar nicht die größte Angriffsfläche, weil Mobile Banking noch nicht weit verbreitet sei. Doch dies werde sich in den nächsten zwölf bis 24 Monaten ändern.

Mehr Angriffsziele: 2011 sollen in Deutschland erstmals 10 Millionen Smartphones verkauft werden.

Zum Schutz vor derartigen Attacken sollten Handybesitzer bei jeder neuen App vorsichtig sein – und nichts herunterladen, was neu im Store oder Market ist oder schlecht bewertet ist. Wenn Android-Apps um Zugriff auf SMS und persönliche Daten bitten, sollten die Alarmglocken schrillen. Eine Security-Software am PC, auch speziell für Online Banking, hilft. Zu guter Letzt sollten die Handynutzer regelmäßig Updates für ihr mobiles Gerät aufspielen.

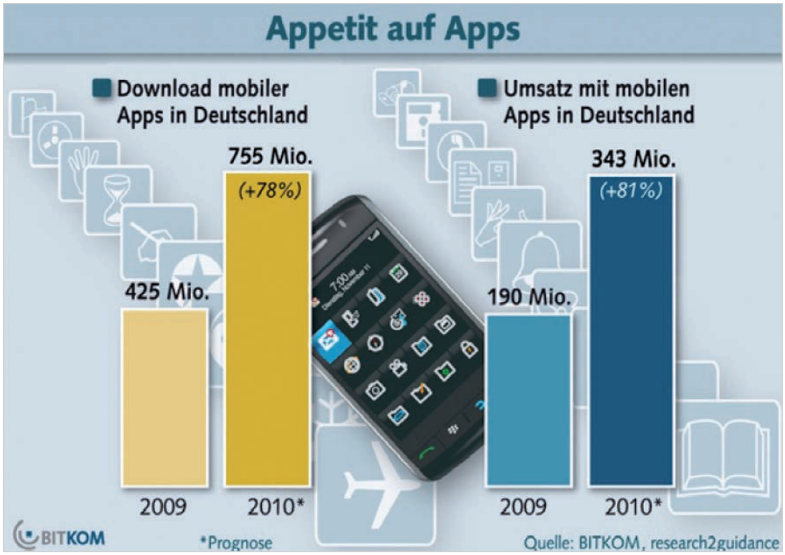
Das Bedrohungsszenario von 5,6 Prozent infizierter iOS- und Android-Smartphones errechnet der Sicherheits-Anbieter aus seinen eigenen Statistiken. Im Juni 2011 habe das Black Hole Kit pro Tag einen von 1500 Usern infiziert – oder 667 aus einer Million. Wenn es im Schnitt drei Wochen dauert, bis Apple oder Google eine Sicherheitslücke schließen und die Kunden das Update installiert haben, werden aus den 667 Usern in 21 Tagen 14.000. Treten vier solcher Lücken im Jahr auf, kommt Trusteer auf 56.000 Infektionen im Jahr. Das entspricht 5,6 Prozent.

2.1.2 Sicherheitssoftware bald unverzichtbar wie auf PCs

„Nutzer sind sich der Gefahren, die bei Mobilgeräten lauern, noch nicht so bewusst wie der letztendlich gleichen Gefahren auf dem PC“, erklärt Juniper-Analyst Nitin Bhas gegenüber pressetext (www.juniperresearch.com). Dabei kann auch eine Architektur wie die von Apples iOS nicht vor allen Risiken schützen. „Um eine sichere Umgebung für den Endnutzer zu schaffen, braucht es Betriebssystem-Sicherheit plus Drittanbieter-Lösungen“, stellt Bhas klar. Er prognostiziert daher,

dass der Mobile-Security-Markt bis 2016 auf ein Volumen von 3,5 Mrd. Dollar wachsen wird – vorerst getrieben durch Unternehmenskunden.

Googles Android hat durch verseuchte Apps im offiziellen Marktplatz für Negativ-Schlagzeilen gesorgt. Das sollte beim vergleichsweise abgeschotteten iOS zwar nicht passieren. „Angesichts der schieren Menge der Apple-Geräte wird iOS für Malware-Schreiber sehr attraktiv", warnt Bhas dennoch. Denn potenziell brandgefährliche Sicherheitslücken sind nie ganz auszuschließen, was vergangenen Sommer JailbreakMe 2.0 bewiesen hat. Zudem ist Malware nur ein Teilproblem.



Viele potenzielle Angreifer: 755 Millionen Apps wurden im Jahr 2010 in Deutschland heruntergeladen, schätzte der Verband BITKOM.

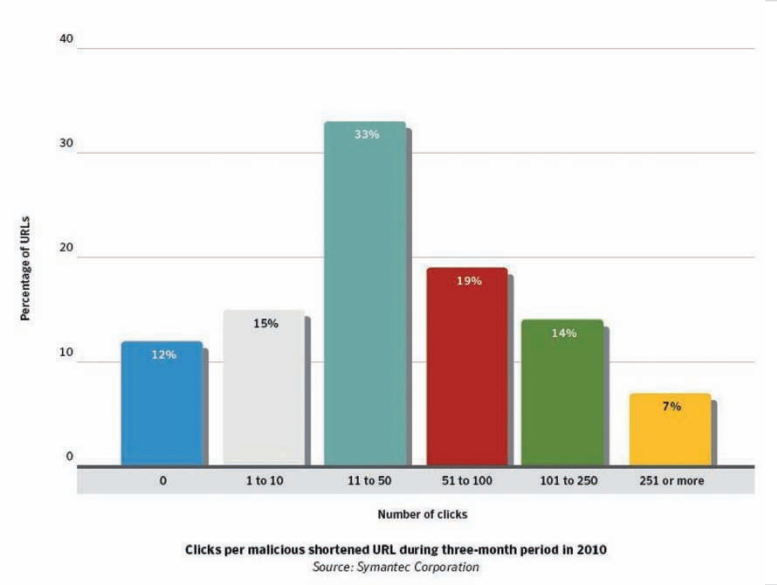
„Es ist wichtig sich darüber im Klaren zu sein, dass das Internet das gleiche Internet bleibt, egal, ob man vom Smartphone oder Laptop darauf zugreift", betont der Juniper-Analyst. Egal, wie sicher iOS oder ein anderes mobiles Betriebssystem ist – viele Bedrohungen wie Phishing kann es gar nicht unterbinden. Dabei greifen immer mehr User mit dem Smartphone auf E-Mails sowie Webseiten zu und führen auch Online-Transaktionen durch. Juniper kommt daher im Bericht „Mobile Security Opportunities" zum Schluss, dass Sicherheitssoftware für Smartphones ebenso unverzichtbar wird wie auf Desktop-PCs.

Kolja Kröger

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation CIO.

2.2 Angriffsziel Tablets: Die Attacken kommen

Vertrauen zu Kollegen kann fatal sein. Die Angriffe auf Computersysteme durch den Wurm Stuxnet 2011 waren wohl nur möglich, weil Unternehmen Mitarbeiter eigene USB-Sticks an Firmenrechner anstecken ließen. Blindes Vertrauen nutzte auch ein anderer Schädling aus, der 2010 im Wirbel um Stuxnet fast unterging: Hydraq. Programmiert in der Absicht, geistiges Eigentum von Unternehmen zu stehlen, kam er daher in Form vertrauenswürdig erscheinender E-Mails mit Links und Anhängen daher, die sich als Falle entpuppten.



Simpel, aber effektiv: Der Sicherheitsbericht von Symantec zeigt, dass drei von vier Kurz-Links auf bösartige Seiten elf Mal oder öfter angeklickt wurden. Diese Methode für Online-Angriffe sei gerade in sozialen Netzwerken weit verbreitet.

Für die Experten des US-amerikanischen Sicherheitsanbieters Symantec (www.symantec.com) zeigen die beiden Beispiele, dass Arglosigkeit gegenüber Arbeitskollegen und Bekannten der am leichtesten nutzbare Schlüssel für Cyber-Kriminelle ist, um die Tür zu IT-Systemen von Firmen zu öffnen. Mit gezielten Attacken, die diesen Weg nutzen, sei daher für die Zukunft wiederholt zu rechnen, schreiben sie in ihrem jetzt erschienenen Sicherheitsbericht, der die Bedrohungslage des Jahres 2010 zusammenfasst (www.symantec.com/business/threatreport/).

2.2.1 USB-Ports sperren

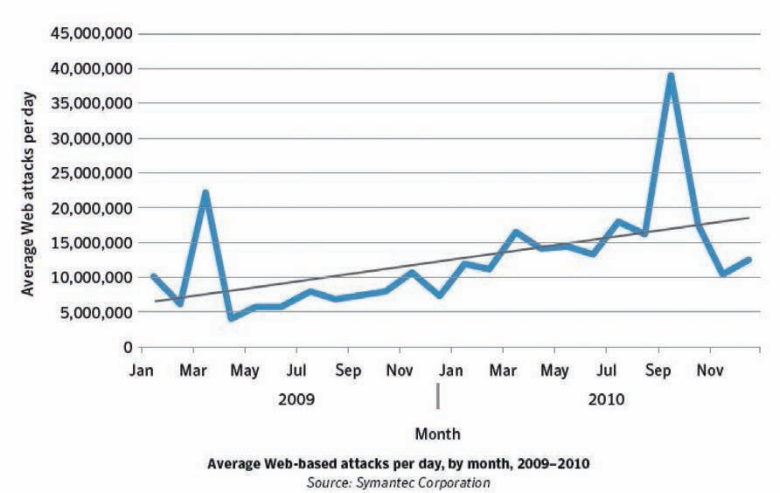
Gezielte Angriffe auf Firmen waren laut den Beobachtungen der Sicherheitsexperten einer der Schwerpunkte der kriminellen IT-Aktivitäten. Die bei solchen Attacken genutzte Schadsoftware sei zunehmend darauf ausgelegt, sich über Wechselmedien wie USB-Sticks zu verbreiten. Sie hängt sich in den meisten Fällen an ausführbare Dateien an und gelangt auf andere Computer, wenn ein Nutzer ein Programm auf einem Datenträger weitergibt. Eine Lehre daraus müsse sein, auch auf den ersten Blick isolierte Netzwerke ähnlich zu schützen wie typische Anwenderumgebungen. Das bedeute zum Beispiel, USB-Schnittstellen zu sperren und mobile Geräte streng zu kontrollieren. Lesen Sie dazu auch unsere Praxisbeiträge Datenleck USB richtig absichern (Webcode **2034261**) und Windows-Praxis: USB-Nutzung per Gruppenrichtlinie reglementieren (Webcode **2034183**).

Als zweiten Brennpunkt der Internetsicherheit identifiziert der „Symantec Internet Security Threat Report – Trends for 2010" soziale Netzwerke. Wer immer sich in ihnen bewegt, hinterlässt Spuren, mit deren Hilfe Verbrecher ihre Angriffe gezielt auf ihr Opfer zuschneiden können. Sie informieren sich über private Interessen, den Arbeitgeber und den Freundeskreis. Vorbei seien folglich die Zeiten, als Phishing-Versuche von auf den ersten Blick verdächtigen Mail-Adressen aus verschickt wurden, in schlechtem Englisch daherkamen und den Empfänger auf offensichtlich bösartige Webseiten lenkten. Für nahezu aussichtslos halten es die Verfasser der Symantec-Studie demgegenüber, einen gut gemachten Angriff zu entlarven, der auf „Social Engineering" aufbaut – so das Fachwort für das Ausnutzen von Informationen, die Menschen in sozialen Netzwerken preisgeben.

2.2.2 Rootkit Tidserv befällt Windows-Rechner

Als spezielle Gefahr in sozialen Netzwerken hat Symantec verkürzte Links ermittelt. Ein Angreifer schreibt den Link an die Pinnwand im Profil eines Opfers, gleichzeitig erscheint er dadurch auch bei dessen Kontakten. Symantec wertete eine Dreimonatsperiode des Jahres 2010 aus und fand heraus, dass fast zwei Drittel der auf diese Weise verbreiteten bösartigen Links verkürzte Links waren. Obwohl diese Links verbergen, wohin sie führen, ist das Misstrauen ihnen gegenüber gering: 73 Prozent der Kurz-Links wurden mindestens elf Mal angeklickt.

Auf einer für einzelne Anwender weniger sichtbaren Ebene liegen die Schauplätze weiterer Angriffswellen, die der Sicherheitsanbieter 2010 beobachtet hat. Zum einen seien sogenannte Zero-Day-Schwachstellen in Verbindung mit Rootkits ein Sicherheitsrisiko. Bei dieser Art von Angriffen nutzen Kriminelle Sicherheitslücken in Programmen wie zum Beispiel Internet-Browsern aus, wenn diese noch nicht öffentlich und auch dem Hersteller der Software noch nicht bekannt sind. Rootkits helfen den Angreifern, dass ihr Tun unentdeckt bleibt. Sie sind Werkzeuge, die das Treiben eines Schadprogramms vor dem PC-Nutzer verbergen und auch verhindern, dass Unregelmäßigkeiten im Betriebssystem auffallen.



Tendenz steigend: Die kriminelle Internetaktivität nimmt laut Symantec weiter zu. Ausschläge nach oben wie unten sind sichtbar.

Eines der derzeit am häufigsten verwendeten Rootkits ist demnach Tidserv. Es verändert die Master Boot Record auf Windows-Rechnern und bemächtigt sich ihrer, bevor das Betriebssystem geladen wird. Eine Reihe Infektionen mit diesem Schädling wurden im Februar 2010 zufällig entdeckt, als Microsoft ein Sicherheits-Patch für Windows herausgab.

2.2.3 Handel mit Verbrecher-Werkzeug

Als weiteren Gefahrenherd beschreibt der Symantec-Bericht den Handel mit Angreifer-Sets. Im Untergrund würden solche Sets verkauft, mit denen der gewöhnliche Cyber-Kriminelle sein Gefahrenpotenzial erhöhen könne. Vorher nur wenigen bekannte Zero-Day-Schwachstellen würden so weithin publik. Wer als Internetkrimineller aktiv sei, für den sei es kein Problem, an solche Werkzeuge zu kommen. Sie waren laut Symantec mit für die mehr als 286 Millionen neuen Schadcode-Varianten verantwortlich, die 2010 entdeckt wurden. Der Handel mit Angriffs-Sets mache deutlich, dass Internetkriminalität ein Geschäft sei: Verbrecher investierten Geld, erwarteten dafür aber auch einen Ertrag. Diese Logik erkläre auch, warum der nächste Schwerpunkt der Online-Kriminalität 2010 noch nicht so recht in Gang gekommen sei: Angriffe auf mobile Geräte.

Eigentlich seien alle Voraussetzungen für hohe Kriminalitätsraten auf diesem Feld vorhanden. Die Zahl der weltweit genutzten Smartphones und Tablet-PCs sei groß genug. Auf den Geräten liefen ausgefeilte Betriebssysteme mit ihren unvermeid-

lichen Schwachstellen. Außerdem gebe es eine simple und effektive Methode, Schädlinge in Umlauf zu bringen: Trojaner in Apps unterzubringen, die sich Tausende Nutzer herunterladen.

2.2.4 Gefahr mobiler Angriffe wächst

Das Einzige, was nach Ansicht von Symantec 2010 noch gefehlt habe, sei die Möglichkeit gewesen, dieses Szenario gewinnbringend auszunutzen. Sicherheitsanbieter Symantec rechnet allerdings damit, dass Angriffe auf mobile Geräte bald zum lohnenden Geschäftsmodell werden – Privatpersonen und Unternehmen, die Smartphones und Tablets wie das iPad nutzen, müssten daher auf der Hut sein und zur Vorbeugung beispielsweise nur Apps aus vertrauenswürdiger Quelle herunterladen und nutzen. Der im April veröffentlichte „Symantec Internet Security Threat Report – Trends for 2010" ist die 16. Ausgabe des jährlichen Berichts des Sicherheitsanbieters (www.symantec.com/business/threatreport/). Die Erkenntnisse beruhen auf Auswertungen von Symantec. Nach Angaben der Autoren sammeln 240.000 Sensoren in mehr als 200 Ländern über Symantec-Lösungen Daten. Informationen über Schadcode trägt Symantec von mehr als 133 Millionen Systemen zusammen, die mit seinen Antivirenprodukten ausgestattet sind. Angaben zu Spam und Phishing listet Symantec in 86 Ländern auf. Mehr als acht Milliarden E-Mails werden dafür jeden Tag ausgewertet.

Der vollständige Bericht kann auf www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=threat_report_16 gegen Angabe von Namen und Mail-Adresse heruntergeladen werden.

Nicolas Zeitler

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation CIO.

TecChannel-Links zum Thema	Webcode	Compact
Angriffsziel Tablets: Die Attacken kommen	2035208	S.39
Smartphones: Malware-Gefahr wächst	2036827	S.36
Smartphones und Tablets sicher im Unternehmen einsetzen	2035129	S.43
Private Smartphones und Tablets sicher einbinden	2035485	S.47
Sicherheitsrisiken von Smartphones und Tablets minimieren	2035249	S.50

2.3 Smartphones und Tablets sicher im Unternehmen einsetzen

Nach Aussagen von Sicherheitsexperten geraten immer öfter Smartphones und Tablets in den Focus von Hackern. Dies belegen in den letzten Monaten die zahlreichen gemeldeten Fälle, bei denen Handys gehackt und mit Malware infiziert wurden. Besonders das iOS- und das Android-Betriebssystem sind gefährdet. Allerdings ist im Vergleich mit der Situation im Computerbereich die Bedrohungslage bei Handys zurzeit noch relativ entspannt. Dennoch sollten die IT-Verantwortlichen jetzt entsprechende Sicherheitsmaßnahmen definieren und im Unternehmen durchsetzen. Gerade Unternehmen wo Smartphones und Tablets als mobiles Produktivmittel eingesetzt werden, stehen vor neuen sicherheitstechnischen Herausforderungen. Neben den direkten Bedrohungen durch Viren, Trojaner und andere Malware müssen die IT-Verantwortlichen zusätzlich das hohe Risiko von Verlust oder Diebstahl dieser Geräte ins Kalkül aufnehmen. Durch die wachsende Beliebtheit der leistungsfähigen Smartphones und Tablets für den Unternehmenseinsatz rücken diese Aspekte immer mehr in den Vordergrund.

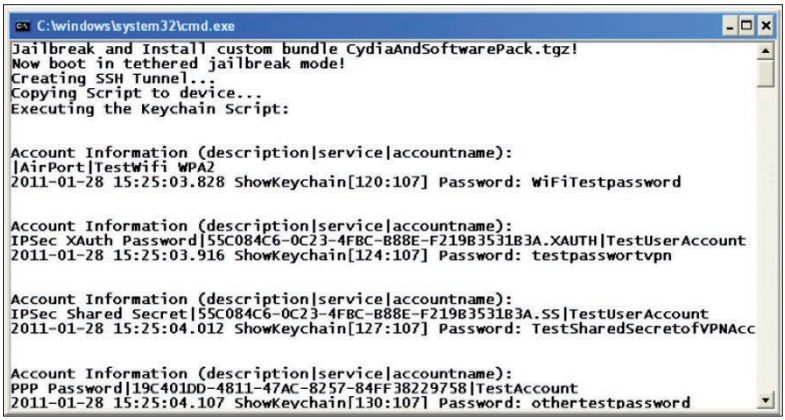
2.3.1 Für Security-Anbieter tun sich neue Märkte auf

Während der Anstieg der Bedrohung zahlenmäßig belegbar ist, betonen Kritiker allerdings, dass die Sicherheitsanbieter bei neuen Handy-Viren weitgehend im Dunkeln tappten und daher kaum echten Schutz anbieten könnten. Ihr primäres Ziel liege vielmehr darin, frühzeitig einen Fuß in den absehbaren Wachstumsmarkt Mobile Security zu bekommen. Unabhängig davon können Business-Nutzer ohnehin nicht allein darauf bauen, dass die installierte Antivirenlösung die aktuellsten Virensignaturen kennt. Womöglich wurde die Malware speziell zum Ausspionieren eines bestimmten Unternehmens entwickelt – und die Smartphones und Tablets der Manager als schwächstes Glied in der Verteidigungskette identifiziert. Grundsätzlich kann man jedoch feststellen, dass die zur Absicherung von Desktop-PCs gedachten Maßnahmen nicht zum Schutz von mobilen Endgeräten ausreichen. Es gilt daher, einen wirkungsvollen Basisschutz aufzubauen, um zu verhindern, dass geschäftskritische Informationen an Unbefugte gelangen.

2.3.2 Mobile Sicherheit braucht eine geeignete Plattform

Die wohl wichtigste Voraussetzung für eine gute Grundabsicherung ist die Auswahl eines geeigneten Mobile-Betriebssystems. Nicht ohne Grund dominierten mit RIMs BlackBerry OS und Windows Mobile lange Zeit zwei gut abgesicherte und einfach verwaltbare Plattformen den Markt für Business-Smartphones. Und auch dem iPhone gelang der breite Einzug ins Unternehmen erst, als Apple mit dem Betriebssystem-Update iOS 4.0 wichtige Device-Management- und Sicher-

heits-Features nachlieferte. Allerdings scheint das System noch Kinderkrankheiten aufzuweisen, so zumindest eine Meldung des Fraunhofer-Instituts für Sichere Informations-Technologie (SIT), die kürzlich die Runde machte. Mitarbeitern des Instituts gelang es, die Geräteverschlüsselung des iPhone auszuhebeln und in nur sechs Minuten viele der auf dem Gerät in der Keychain gespeicherten Passwörter zu entschlüsseln. Dabei mussten die Tester nicht einmal die 256-Bit-Verschlüsselung knacken, sondern machten sich nur eine Schwäche im Sicherheitsdesign zunutze: Der Schlüssel, auf dem die Verschlüsselung basiert, wird nicht auf Basis des geheimen Nutzer-Passworts generiert. Das grundlegende Geheimnis wird vielmehr direkt vom iOS-Betriebssystem der Apple-Hardware gebildet und ist auf dem betreffenden Gerät gespeichert.



So wird's gemacht: Jailbreak und Tunnel sichern das Smartphone ab.

Immerhin besteht seit iOS 4.0 die Möglichkeit, Daten auf dem iPhone zusätzlich zu sichern. Anderen Newcomer-Systemen wie Windows Phone 7 und Android fehlt eine native Geräteverschlüsselung dagegen noch komplett. Microsoft habe beim Aufbau seiner neuen Mobile-Plattform aktuell noch andere Prioritäten, erklärt Markus Müller, Gründer des Münchner Mobile-Device-Management-Experten Ubitexx. Windows Phone 7 sei deswegen derzeit noch nicht für den Enterprise-Einsatz geeignet. Googles Mobile-Betriebssystem, das viele bereits als weitere Alternative für den Business-Einsatz sehen, hat erst seit dem Honeycomb-Update eine native On-Board-Verschlüsselung.

2.3.3 Aus den Augen – nicht aus dem Sinn

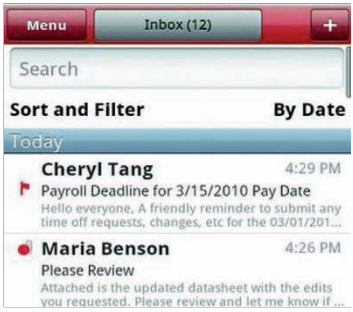
Unabhängig davon, wie sicher die Daten auf den Firmen-Smartphones abgelegt sind – als Zugangstor zu Kundendatenbanken, Preislisten und anderen geschäfts-

kritischen Informationen benötigen die Geräte ständigen Schutz. Dazu zählt insbesondere die Möglichkeit für Administratoren, jederzeit remote auf die Geräte zugreifen zu können. Nur so sind sie in der Lage, Smartphones bei Verlust oder Diebstahl zu sperren, die gespeicherten Daten zu löschen, wichtige Updates aufzuspielen oder die Einhaltung von Policies zu überwachen und durchzusetzen.

2.3.4 Sehr filigrane Kontrolle bei BlackBerry und Windows Mobile

Die wahrscheinlich bekannteste Mobile-Device-Management-Lösung ist der BlackBerry Enterprise Server (BES). Das System erlaubt neben der verschlüsselten Übertragung von Mails und PIM-Daten eine filigrane Kontrolle der angebundenen BlackBerry-Smartphones. In Verbindung mit einer Zwei-Faktor-Authentisierung eignen sich bestimmte Gerätemodelle sogar für den Einsatz in Hochsicherheitsumgebungen, etwa Militär und Regierungskreisen. Lediglich der Transport des Mail-Verkehrs über ein zentrales Rechenzentrum (NOC = Network Operating Center) bereitet manchen Sicherheitsbeauftragten Kopfschmerzen. Hierzulande setzt die Bundesregierung daher auf Windows-Mobile-Geräte, die neben dem Exchange-ActiveSync-Protokoll auch über eine Smartcard-basierende Lösung von Certgate/T-Systems (SimKo 2) abgesichert und verwaltet werden. Was danach kommt, ist fraglich: Nach der Entscheidung von Microsoft, künftig auf das noch nicht Business-taugliche Windows Phone 7 als mobile Plattform zu setzen, fehlt hier – abgesehen von BlackBerry – kurz- bis mittelfristig noch eine geeignete Alternative. Auch Android und iPhone/iOS nutzen das von Microsoft lizenzierte ActiveSync-Protokoll für ihre Mobile-Lösungen. Google beschränkt sich dabei allerdings auf die darin enthaltenen rudimentären Management-Funktionen wie Passwortschutz und Remote Lock and Wipe. Diese bilden die Grundlage für die meisten Verwaltungslösungen für Android. Eine Ausnahme ist „Good for Enterprise – Android" vom US-Anbieter Good Technology – hier werden Mails und andere geschäftskritische Daten in einer verschlüsselten Anwendung aufbewahrt und über einen externen Server gemanagt.

Alternativen: Good for Enterprise schließt geschäftskritische Daten ein.



Im Gegensatz dazu hat Apple einer Reihe von Drittanbietern wie MobileIron, Sybase oder hierzulande Ubitexx zusätzliche Schnittstellen für das Mobile-Device-Management bereitgestellt. Mit den daraus hervorgegangenen Lösungen können Unternehmen ihre iPhones und iPads weitaus besser verwalten. Unter anderem lassen sich über die Luftschnittstelle spezifische Einstellungen, Sicherheitsparameter und Policy-Profile ohne Benutzerinteraktion installieren und verwalten. Das remote Aufspielen von Anwendungen wird jedoch nicht unterstützt, auch filigranere Vorgaben wie die Sperrung bestimmter Web-Seiten (außer YouTube) oder Apps für den Benutzer sind nicht möglich.

2.3.5 Nutzungsregeln schließen technische Lücken

Überall dort, wo sich Vorgaben nicht allein technisch durchsetzen lassen, muss der Nutzer über eine spezielle Mobile User Policy ins Boot geholt werden. Darin sollte unter anderem klar definiert werden, welche Daten (geschäftlich und privat) auf den mobilen Endgeräten genutzt werden dürfen. Experten empfehlen, besonderes Augenmerk auf die allerseits beliebten Apps zu legen. So rät etwa Boris Sharov, CEO des russischen Sicherheitsanbieters Dr. Web, generell die Installation eigener Apps zu untersagen – über Tools oder, falls nicht möglich, via Policy. Man könne nie wissen, wie intensiv App-Store-Betreiber wie Apple oder Google die Anwendungen vor dem Einstellen geprüft hätten, so Sharovs Erklärung. Um Malware komplett ausschließen zu können, müssten sie theoretisch den gesamten Code durchsuchen – die Arbeit von mehreren Tagen oder Wochen. Tatsächlich ist solche Gründlichkeit wohl eher selten, iPhone-Entwickler müssen Apple nicht einmal den Quellcode vorlegen. Zeitweise wurden außerdem im Android Market über 50 Anwendungen entdeckt, die mit dem Trojaner DroidDream infiziert waren – dieser leitete sensible Telefondaten an einen Server in Kanada weiter.

Manfred Bremmer

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

TecChannel-Links zum Thema	Webcode	Compact
Smartphones und Tablets sicher im Unternehmen einsetzen	2035129	S.43
Smartphones: Malware-Gefahr wächst	2036827	S.36
Angriffsziel Tablets: Die Attacken kommen	2035208	S.39
Private Smartphones und Tablets sicher einbinden	2035485	S.47
Sicherheitsrisiken von Smartphones und Tablets minimieren	2035249	S.50
Mobile Geräte wirkungsvoll gegen Missbrauch absichern	2034906	S.55

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

2.4 Private Smartphones und Tablets sicher einbinden

Die aus den USA stammende Strategie, private Smartphones, Tablets oder Rechner ins Unternehmen zu integrieren („Bring your own Device" – ByoD), hat ihre Vor- und Nachteile. Zwar lassen sich damit die Motivation und die Produktivität der Mitarbeiter erhöhen sowie im Idealfall durch die Übertragung von Verantwortung und Support auf den Nutzer Spareffekte erzielen. Gleichzeitig wird die IT-Abteilung jedoch mit eine Reihe von bislang unbekannten – sowohl rechtlicher wie technischer Art – Problemen konfrontiert. Sicherlich: Für eine Vielzahl der mit ByoD auftretenden Probleme müssen Anwender und Unternehmen Kompromisse eingehen und klare Vereinbarungen (User Policies) treffen. Daneben gibt es aber bereits eine Reihe von Tools und Lösungen am Markt, mit denen die Integration von Endnutzergeräten auf technischer Seite erleichtert wird. Hier ein Überblick.

2.4.1 Welche Plattformen?

Während die Nutzung privater Apple-Rechner dank der Dual-Boot-Funktion für Windows und Mac OS X die IT-Abteilung kaum vor größere Probleme stellt, bereiten die zahlreichen Plattformen im Mobile-Bereich deutlich mehr Kopfzerbrechen. Die IT-Verantwortlichen müssen sich im schlimmsten Fall auf eine Situation einstellen, die sich am besten mit dem sprichwörtlichen „Sack Flöhe hüten" vergleichen lässt. So handelt es sich nicht nur vom Begriff her um „mobile Endgeräte". Die Devices befinden sich tatsächlich nicht nur im Büro, sondern werden häufig auf Kundenbesuche oder Dienstreisen mitgenommen. Damit besteht ständig die Gefahr, dass sie mitsamt brisanter Daten und Zugangscodes verloren gehen – ein Szenario, für das entsprechende Vorkehrungen getroffen werden müssen.

Erschwerend kommt hinzu, dass die einzelnen Betriebssysteme wie Android, BlackBerry OS, das in iPhone und iPad genutzte iOS, Symbian, webOS oder Windows Phone 7 unterschiedlich gut (beziehungsweise schlecht oder überhaupt nicht) für den Einsatz im Enterprise geeignet sind. Zusätzlich erfordern sie teilweise auch angepasste Anwendungen und individuelle Verwaltungs-Tools.

2.4.2 Verwaltung tut not

Wer den Wildwuchs an mobilen Endgeräten besser in den Griff bekommen will, steht vor der Entscheidung, die Zugriffsrechte einzudämmen oder die Anzahl der zulässigen Plattformen von vornherein einzuschränken. Die gute Nachricht dabei: Angesichts der Unzahl an Smartphones und (mit Einschränkung) auch Tablets werden die Anwender selbst bei nur zwei unterstützten Betriebssystemen nicht vor allzu große Entscheidungsnöte gestellt: Sieht man von Apple (iPhone, iPad) ab,

gibt es von allen Herstellern und Plattformen Geräte mit unterschiedlichen Formfaktoren – angefangen vom klassischen Candybar-Handy über Messaging-Smartphones mit ausziehbarer Qwertz-Tastatur bis hin zu reinen Touchscreen-Devices.

Daneben haben sich aber schon heute Anbieter wie Good Technology, MobileIron, Sybase oder Ubitexx auf den ByoD-Trend eingestellt. So gibt es am Markt bereits einige Mobile-Device-Management-Lösungen, mit denen sich Smartphones und Tablets plattformübergreifend verwalten sowie Netzwerk- und Sicherheitseinstellungen einrichten lassen – zumindest was die wichtigsten Mobile-Systeme anbelangt.

2.4.3 Self-Service-Portale entlasten die IT-Abteilung

Einige MDM-Lösungen besitzen dabei sogar eine spezielle Selbstbedienungsfunktion. Mit deren Hilfe können Anwender ihr neues Gerät eigenständig aktivieren, für Mail- und Netzzugang konfigurieren und im Falle eines Verlusts oder Diebstahl sogar orten und ohne Unterstützung des Helpdesk sperren oder löschen.

Wichtig dabei: Um späteren Ärger zu vermeiden, sollte der Anwender darauf hingewiesen werden, dass bei einer solchen Maßnahme möglicherweise neben den geschäftskritischen auch seinen persönlichen Daten der Garaus gemacht wird. Es gibt allerdings Ausnahmen wie die Lösung „Good for Enterprise“ oder die Kill-Pill-Funktionen in Sybase „iAnywhere Mobile Office“, bei denen ausschließlich Unternehmensdaten entfernt werden. Außer den speziellen MDM-Lösungen deckt bereits das von Plattformlieferanten wie Apple, Google & Co. lizenzierte Microsoft-Synchronisationsprotokoll „Exchange ActiveSync“ eine Reihe wichtiger Features wie Backup, Lock & Wipe ab. Ähnliches gilt – wenn auch in eingeschränktem Rahmen – für Lotus-Notes/Domino-Nutzer über die Kombination Notes Server und die mobile „Lotus Traveler“-App. Ist dieser Client auf dem Endgerät installiert, lassen sich Apple- und Windows-Mobile-Smartphones remote in den Auslieferungszustand zurückversetzen (Hard Reset). Bei Android- und Symbian-Smartphones besteht immerhin die Möglichkeit, die PIM-Anwendung samt zugehöriger Daten sowie die Inhalte der Speicherkarte (geht auch bei Windows Mobile) aus der Ferne zu löschen.

2.4.4 Welche Anwendungen eignen sich?

Exchange ActiveSync und Lotus Traveler sind selbstverständlich auch für den mobilen Zugriff gedacht beziehungsweise für den Abgleich von E-Mails, Kontakt- und Kalenderdaten. Untersagt die User Policy aus Sicherheitsgründen die Speicherung geschäftskritischer Daten auf den mobilen Endgeräten, sollte das Unternehmen dem Anwender zumindest einen webbasierten Zugriff auf seine Firmen-Mails einrichten. Ähnliches gilt im weitesten Sinne auch für Business-Anwendungen. Hier sind internetgestützte Apps oder an die genutzten Endgeräte angepasste mobile Webseiten (der Übergang ist fließend) unter Umständen eine

günstige Möglichkeit, auf den gegenwärtigen Trend zu ByoD oder allgemein zur IT-Consumerization zu reagieren: Da sie es erlauben, Geräte mit verschiedenen Plattformen und Formfaktoren anzusprechen, können Nutzer ihre privaten Endgeräte verwenden, ohne ein Loch in die Sicherheitsstrategie des Unternehmens zu reißen. Ein weiterer Vorteil: Es ist kein umständlicher Roll-out notwendig, Veränderungen können ohne viel Aufhebens vorgenommen werden. Auch die Frische der Daten ist kein Problem, da diese direkt aus der zentralen Datenbank abgegriffen werden. Die Anwendungen können jedoch nicht eins zu eins übernommen, sondern müssen angepasst werden – etwa an die kleinen Displays, an Fingerbedienung. Gleichzeitig ist zu berücksichtigen, dass sich die Geräte nicht zur Eingabe von längeren Texten eignen und häufig nur eine geringere Bandbreite zur Übertragung von Daten vorhanden ist. Daneben gibt es aber auch Middleware-Lösungen, mit denen Unternehmen native mobile Anwendungen für verschiedene Plattformen erstellen und verwalten können. Bekanntester Anbieter ist vermutlich der von SAP übernommene Spezialist Sybase mit seiner „Unwired Platform". Es sind aber noch zahlreiche andere Spezialisten auf dem Markt, hierzulande etwa das Mannheimer Start-up Movilitas („Movilizer") oder die GIA mbH aus Leverkusen mit ihrer Lösung „BI.apps".

Virtualisierung und Remote-Desktop- sowie Terminal-Dienste sind eine andere Möglichkeit, mit der Nutzer auch über potenziell unsichere Endgeräte auf geschäftskritische Daten zugreifen können, ohne deren Integrität zu gefährden. So erlauben es die schier zahllosen Remote-Desktop-Lösungen, die es mittlerweile für Android und iOS gibt, Rechner im Büro oder Home-Office über die Luftschnittstelle fernzusteuern. Auf diese Weise können Nutzer nicht nur sensible Daten sicher einsehen. Es ist beispielsweise auch möglich, die anderweitig nicht unterstützten Flash-Inhalte auf iPhone oder iPad zu beamen. Das Thema Virtualisierung kommt dagegen – anders als im PC-Umfeld – bei Smartphones und Tablets nur langsam in Fahrt. Dies gilt vor allem für Typ-2-Hypervisoren, die wie VMwares Mobile Virtual Platform auf einem bestehenden Betriebssystem aufsetzen. Zwar demonstrierte der Spezialist bereits im Dezember 2010 gemeinsam mit LG ein Android-Smartphone mit isoliertem virtuellen Business-Account, das irgendwann in diesem Jahr auf den Markt kommen soll. VMware profitierte dabei jedoch von der offenen Android-Plattform und der Kooperation mit einem Hardwarehersteller. Eine Verbreitung auf geschlossene und streng kontrollierte Architekturen wie Apple iOS ist schwer vorstellbar. Außerdem dürfte die Lösung ähnlich wie entsprechende PC-Varianten sehr ressourcenhungrig sein.

Weiter ist der Konkurrent Citrix zu nennen, der mit seiner „Citrix-Receiver"-Serie auf Typ-1-Hypervisoren setzt. Die Gratis-Lösung zur Virtualisierung von Anwendungen ist mit Clients für Android, BlackBerry OS, iOS (iPhone/ iPad), Symbian und Windows Mobile für fast alle Plattformen verfügbar. Als Voraussetzung müssen im Unternehmen Citrix XenApp oder XenDesktop im Einsatz sein, dies ist inzwischen aber eine weit verbreitete Praxis. Experten gehen davon aus, dass der Anwendungsvirtualisierung die Zukunft gehört – im Mobile- wie im Desktop-Bereich.

Manfred Bremmer

2.5 Sicherheitsrisiken von Smartphones, Tablets und Handys minimieren

Die mobilen Geräte wie Smartphones und Tablets sind aus dem Geschäftsprozess kaum mehr wegzudenken und werden immer häufiger in die IT-Infrastruktur fest integriert. Dabei werden diese Geräte zunehmend intelligenter und nähern sich den Einsatzmöglichkeiten eines PCs an. Doch bei der Vielfalt der Geräte, Betriebssysteme und Anwendungen kommt die Sicherheit dieser mobilen Systeme oft zu kurz. Der Erfolg eines Unternehmens hängt heute oft von der Geschwindigkeit der Informationen ab, sodass es nicht verwunderlich ist, dass die mobilen Geräte auch gerne für geschäftskritische Anwendungen genutzt werden. Dies stellt jeden IT-Verantwortlichen vor eine große Herausforderung, wenn es darum geht, in diesem Umfeld eine angemessene Sicherheit auf diesen Geräten zu gewährleisten.

Der für die Unternehmens-IT Zuständige muss nicht nur eine entsprechender IT-Infrastruktur zur Verfügung stellen, sondern auch entsprechende funktionierende Prozesse aufsetzen. Dabei ist ein Spagat zwischen Sicherheit und Funktionalität gefragt, um den mobilen Vorteil nicht durch diverse Restriktionen aufzuheben. Aber auch wenn bereits etablierte Systemlösungen wie der BlackBerry zum Einsatz kommen, unterschätzen die IT-Verantwortlichen den Sicherheitsaspekt allzu oft. Wir geben Ratschläge und Tipps, wie Sie das Sicherheitsrisiko mobiler Geräte in Unternehmen minimieren.

2.5.1 Smartphone-Verlust mit fatalen Folgen

Der Einsatz von Smartphones und Tablets stellt Unternehmen vor die gleichen Herausforderungen, wie sie seinerzeit für die Absicherung von IT-Infrastrukturen, Desktop- und Server-Systemen bestanden. Es gibt so gut wie keine technischen Lösungen zur dauerhaften Absicherung von Smartphones und mobilen Endgeräten. Außerdem wächst durch die ständig steigende Kapazität dieser Geräte die Menge vertraulicher Daten, die sie aufnehmen können, kontinuierlich. Der Verlust eines einzigen Smartphones kann daher fatale Auswirkungen auf ein gesamtes Unternehmen haben. Diese können vom kleinen finanziellen Schaden bis hin zum Firmenbankrott reichen.

2.5.2 Kinderkrankheiten in Sachen Sicherheit

Hinzu kommt, dass es sich bei Smartphones um eine junge Technologie handelt, die mit zahlreichen Kinderkrankheiten in puncto Sicherheit zu kämpfen hat und mit hoher Wahrscheinlichkeit Angriffsvektoren bietet, die bisher noch nicht entdeckt wurden. Man braucht in diesem Zusammenhang nur an die bisher als sicher geltenden SMS-TAN-Verfahren der Internetbanken zu denken. Verwendet ein Be-

nutzer sein Smartphone sowohl für Online-Banking als auch zum Empfang der TAN per SMS, ist die grundsätzliche Sicherheit des Verfahrens sofort hinfällig.

2.5.3 Smartphones sind lohnende Angriffsziele

Smartphones sind lohnende Angriffsziele, denn sie vereinen Eigenschaften von Serversystemen mit denen der mobilen Kommunikation. Permanente Internetanbindung, Erreichbarkeit rund um die Uhr, Geolokalisierung, private und dienstliche Daten wie E-Mail, Credentials, VPN-Zertifikate, Adressbücher und Dokumente lassen aus einem Smartphone für einen Angreifer das ideale Sprungbrett in gut gesicherte Infrastrukturen werden.

2.5.4 Mobile Endgeräte ungefährlicher machen

Neue Angriffsvektoren präventiv zu entschärfen ist kaum möglich. Daher empfiehlt sich beim Einsatz von Smartphones grundsätzlich eine konservative Einstellung. Mit geeigneten technischen und organisatorischen Maßnahmen lassen sich zumindest bekannte Risiken minimieren und Anwender so sensibilisieren, dass sie beim Umgang mit mobilen Endgeräten ausreichend Sorgfalt walten lassen.

2.5.5 Sicherheitsaspekte bei Endgeräteauswahl beachten

Die Auswahl von Smartphones und mobilen Endgeräten sollte nicht nur unter finanziellen und funktionalen Gesichtspunkten, sondern von Anfang an auch unter dem Aspekt der Sicherheit erfolgen. Neben gerätespezifischen Merkmalen – wie zum Beispiel der Verschlüsselung der Gerätedaten, Zugriffsschutz und Schnittstellen – ist beim Betrieb vieler mobiler Endgeräte die zentrale Verwaltung eine ganz wichtige Frage. Idealerweise sollten sich die Endgeräte in vorhandene Administrations- und Sicherheitsmechanismen eingliedern lassen beziehungsweise die Möglichkeit bieten, ihre eigenen Mechanismen mit den bereits vorhandenen zu koppeln. Nur durch die Aggregation und Auswertung von Gerätedaten an zentraler Stelle erhält der Betreiber einen Überblick über den Zustand der Geräte, über Verstöße gegen Richtlinien und ähnliche Informationen.

2.5.6 Smartphones auf Sicherheitsrichtlinien prüfen

Ein wichtiger Aspekt ist auch, ob bereits Richtlinien zum Umgang mit mobilen Endgeräten (zum Beispiel für Notebooks) und der damit einhergehenden Verarbeitung von Daten außerhalb der eigenen IT-Infrastruktur im Unternehmen existieren. Ist dies der Fall, sollte ein weiteres Entscheidungskriterium bei der Auswahl einer Smartphone-Plattform die Frage sein, ob sich die vorhandenen

Richtlinien auch auf dem neuen Gerät umsetzen lassen. Dürfen Daten beispielsweise nur auf verschlüsselten Datenträgern und Endgeräten das Unternehmen verlassen, scheiden Geräte ohne eine angemessene Möglichkeit zur Verschlüsselung bereits im Vorfeld aus der Betrachtung aus. Wie bei der Verwaltung von Desktop-Systemen gilt auch bei Smartphones: Je fragmentierter die Geräte- und Betriebssystembasis, desto höher der Administrationsaufwand. Weniger ist also auch hier mehr, denn je unterschiedlicher die eingesetzten Geräte sind, desto schwieriger wird es, einheitliche Sicherheitsrichtlinien auf allen Geräten umzusetzen.

2.5.7 Vier Faktoren für den sicheren Betrieb

Zum sicheren Betrieb von Smartphones gehören vier Faktoren:

- die Sicherheit der Endgeräte,
- die Sicherheit der Schnittstellen zur Unternehmens-IT,
- die organisatorischen Prozesse und Richtlinien im Unternehmen sowie
- das Gefahrenbewusstsein der Mitarbeiter.

1. Sicherheit der Endgeräte

Nach der Auswahl einer Plattform sollte als Erstes eine Sicherheitsrichtlinie zur Konfiguration der Smartphones aufgestellt werden. Diese Regeln sollten sich am Schutzbedarf der auf den Smartphones verfügbaren Daten orientieren sowie an unternehmensweit geltenden IT-Sicherheitsstandards. Wichtige Elemente einer solchen Richtlinie sind die Einrichtung automatischer Sperren, Vorgaben zur Stärke von Passwörtern, die Sicherheitskonfiguration des Internet-Browsers, eine Regelung der Verwendung externer Speichermedien am Smartphone und die Erlaubnis respektive das Verbot der Installation von Programmen (Apps) durch den Benutzer. Nicht benötigte Schnittstellen sollten aus Sicherheitsgründen deaktiviert und nicht benötigte Software von den Geräten entfernt werden.

2. Anbindung an die Unternehmens-IT

Der zweite Schritt in Richtung Sicherheit betrifft die Geräteanbindung an die Unternehmens-IT. Hier sind die Möglichkeiten so vielfältig wie die verfügbaren Endgeräte. Für die Verwendung von BlackBerry ist die Integration eines BlackBerry Enterprise Servers (BES) in die eigene IT notwendig. iPhone und iPad lassen sich direkt an Exchange- oder Notes-Umgebungen ankoppeln und darüber auch managen, so auch auf anderen Plattformen basierende Endgeräte. Eine Richtlinie zur Anbindung sollte Regelungen darüber enthalten, ob die Anbindung über VPN-Verbindungen erfolgt oder ob der Zugriff auf E-Mails über traditionelle Wege verläuft wie beispielsweise IMAP und SMTP. Beim Thema E-Mail kommt in der Regel die Frage nach Verschlüsselungsmöglichkeiten auf.

RIM bietet für den BlackBerry verschiedene Möglichkeiten der E-Mail-Verschlüsselung. Auch ist die E-Mail-Kommunikation zwischen Geräten eines Unterneh-

mens über den unternehmenseigenen BES als sicher zu betrachten. Anders sieht es bei iOS aus, also bei iPhone und iPad. Apple hat bis heute weder das Datenverschlüsselungsprogramm Pretty Good Privacy (PGP) noch Secure/Multipurpose Internet Mail Extensions (S/MIME) in iOS integriert, sodass iOS-basierte Geräte keine Möglichkeit zur Verschlüsselung von E-Mails bieten. Problematisch kann das Thema E-Mail-Verschlüsselung werden, wenn Mitarbeiter E-Mails parallel auf Smartphone und Desktop bearbeiten, was in der Regel der Fall ist. Verschlüsselt das Smartphone E-Mails mit einer eigenen Lösung, sind diese E-Mails auf dem Desktop nicht lesbar. Kommt umgekehrt eine Desktop-Lösung zum Verschlüsseln zum Einsatz, beispielsweise PGP oder das freie Kryptografiesystem GNU Privacy Guard (GPG), bleiben diese E-Mails auf dem Smartphone unlesbar. Abhilfe können Gateways schaffen, die E-Mails beim Empfang oder Senden durch den zentralen Mail-Server transparent ent- oder verschlüsseln.

3. Management und Richtlinien im Unternehmen

Wichtiges Merkmal des zentralen Managements ist die regelmäßige Aktualisierung der Smartphones inklusive der installierten Programme. Ohne eine zentrale Kontrollinstanz gibt es keinen Überblick über die Softwarestände, und Mitarbeiter arbeiten unter Umständen jahrelang mit veralteter Software, die entsprechend viele Sicherheitslücken aufweist. Smartphones sollten daher zwingend in den normalen Patch-Management-Zyklus eingebunden werden, so wie alle Systeme eines Unternehmens. Die Richtlinie zum Anbinden und Managen der Smartphones sollte vorsehen, verlorene oder gestohlene Geräte aus der Ferne löschen zu können, um zu verhindern, dass Unternehmensdaten in unbefugte Hände gelangen. Hierzu müssen die technischen Voraussetzungen geschaffen und die mobilen Endgeräte entsprechend konfiguriert werden. Neben dem Löschen bieten moderne Smartphones auch die Möglichkeit der Lokalisierung über die Managementschnittstelle. Für die Nutzung dieser Funktion nach Diebstahl und Verlust sollte die Richtlinie Vorgaben machen, nicht zuletzt, weil diese Funktion ein enormes Missbrauchspotenzial bietet (Stichwort Mitarbeiterüberwachung). Sinnvoll kann auch sein, Geräte mit einem Hinweis über den Eigentümer zu versehen, entweder über eine Anzeige auf dem Bildschirm oder über einen Aufkleber. Das erhöht nachweislich die Chance, dass ehrliche Finder das Gerät an das Unternehmen zurückschicken. Ein wichtiger Aspekt der organisatorischen Sicherheit – gerade bei Verwendung von Endgeräten, die vom Provider gemietet wurden – ist das sichere Löschen im Schadens- oder Rückgabefall. Die Richtlinien sollten diese Fälle vorsehen und passende Maßnahmen definieren. Dasselbe gilt für die Entsorgung von Geräten: Auch dann müssen im Vorfeld alle sensiblen Daten sicher gelöscht werden.

4. Mitarbeiter für Sicherheit sensibilisieren

Der Umgang mit dem Gefahrenbewusstsein der Mitarbeiter ist beim Einsatz von Smartphones eine Gratwanderung. Auf der einen Seite berauben zu restriktiv konfigurierte Smartphones diese häufig zentraler Funktionen, womit die Akzeptanz durch die Mitarbeiter schwindet und der ursprünglich erhoffte Vorteil ausbleibt.

Auf der anderen Seite können zu laxe Regeln Angreifern Tür und Tor öffnen. Das unkontrollierte Installieren von Apps durch die Mitarbeiter ist beispielsweise ein klassisches Sicherheitsrisiko. Wollen Unternehmen in diesem Punkt ganz auf Nummer sicher gehen, bleibt ihnen häufig keine andere Wahl, als ein komplettes App-Verbot auszusprechen. Hier müssen Unternehmen sorgfältig abwägen. Viele wählen eine Zwischenlösung und entwickeln einen Corporate App Store, der auf Sicherheit geprüfte Apps für die Mitarbeiter bereitstellt. So können die Mitarbeiter innerhalb bestimmter Grenzen selber Apps installieren.

2.5.8 Sicherheit ist die Summe vieler Einzelaspekte

Sicherheit beim Unternehmenseinsatz von Smartphones ist nicht allein eine technische Frage. Neben der sicheren Konfiguration von Endgeräten sind deren Integration in die Unternehmens-IT und das Management der Geräte wichtige Bausteine der Gesamtsicherheit. Richtlinien sind aber nur dann sinnvoll, wenn sie angemessen und umsetzbar sind. Die ISO-Norm 27001 definiert zahlreiche Vorgaben und Prozesse, aus denen sich Richtlinien für den Einsatz mobiler Endgeräte ableiten lassen. Ein Unternehmen, das nach ISO 27001 aufgestellt ist, sollte daher zumindest mit den organisatorischen Aufgaben keine Probleme haben. Hingegen lassen sich die Auswahl einer sicheren Plattform sowie die sichere Konfiguration der Endgeräte aus keinem Standard ableiten. Hier ist Erfahrung gefragt. Denn wie bereits gesagt: Die Geschichte wiederholt sich. Man muss nur zehn Jahre zurückdenken und die seinerzeit gewonnenen Erkenntnisse über die Sicherheit von Systemen und Infrastrukturen auf mobile Lösungen übertragen. Das ist einfacher, als es auf den ersten Blick aussieht. Gleich geblieben ist: Der Angreifer will noch immer an Unternehmensdaten kommen. Er nutzt jetzt nur einen anderen Weg.

2.5.9 Checkliste

- Sicherheit zum zentralen Kriterium bei der Produktauswahl machen.
- Richtlinien für Installation, Anbindung, Betrieb und Entsorgung von Endgeräten entwickeln.
- Sichere Konfiguration der Endgeräte berücksichtigen.
- Sichere Integration in Unternehmens-IT umsetzen.
- Endgeräte in relevante Prozesse wie das Patch-Management einbinden.
- Benutzerrichtlinien für den Umgang mit Endgeräten definieren.

Klaus Rodewig

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

Klaus Rodewig ist Senior Consultant im Bereich IT-Sicherheit bei Logica in Deutschland.

2.6 Mobile Geräte wirkungsvoll gegen Missbrauch absichern

Für Rainer Speer hat das Thema Mobile Computing eine ungeahnte Dynamik entfaltet. Am 30. Oktober 2009 kam ihm sein Notebook abhanden. Seinen Angaben zufolge wurde ihm der Laptop aus seinem Dienstwagen gestohlen. Das war in mehrfacher Hinsicht ärgerlich. Neben dem materiellen Verlust erlitt Speer nämlich noch einen anderen Nachteil – er verlor seinen Job. Nicht irgendeinen. Speer war brandenburgischer Innenminister gewesen. Im September 2010 musste er zurücktreten, als Teile des E-Mail-Verkehrs zwischen ihm und einer Frau publik wurde. Diese befanden sich auf einer DVD, die der Potsdamer Staatsanwaltschaft und dem Landeskriminalamt Brandenburg anonym zugeschickt wurde. Die E-Mails auf der DVD sollen von Speers Laptop stammen.

Die „Süddeutsche Zeitung" zitierte den Potsdamer Oberstaatsanwalt Helmut Lange seinerzeit mit den Worten: „Wir gehen derzeit von der Authentizität der Daten aus." Aus den E-Mails konnte man den Verdacht herleiten, dass die Landesbedienstete vom Staat Unterhalt bezog für ein Kind, dessen Vaterschaft der SPD-Politiker Speer offiziell zunächst nicht anerkannt hatte. Die digitale Briefschaft scheint zu belegen, dass der Minister sich seiner Vaterschaft durchaus bewusst war. Anders gesagt: Es entstand so der Verdacht, der hochrangige Politiker und seine ehemalige Geliebte hätten Sozialbetrug begangen. Speer weist Anschuldigungen, er habe Sozialbetrug begangen, umfassend zurück. Etwaige Anschuldigungen, sollten sie denn Substanz haben, wären mittlerweile allerdings verjährt.

Völlig unnötiges Risiko

So gut es ist, wenn solche Tatbestände ans Licht kommen, so deutlich macht der Fall auch, dass Kindsvater und -mutter nicht in die prekäre Lage geraten wären, hätten sie dem Thema Mobile Security etwas mehr Bedeutung beigemessen. Die beiden hatten Überlegungen zur Absicherung von mobilen Geräten offensichtlich zu locker gesehen. Auf die fatalen Folgen solcher Hemdsärmeligkeit weist Astrid Fey hin, wenn sie feststellt: „Es wäre interessant zu erfahren, ob der verantwortliche IT-Leiter seinen Posten noch innehat."

Übertrieben: Astrid Fey, Leiterin des IT-Referats des Bundesinstituts für Berufsbildung (BIBB), hält manche Risiken bei der Nutzung mobiler Clients für völlig unnötig.

Das Risiko, dass Daten wie die privaten Mails des Politikers in falsche Hände geraten, sei „völlig unnötig“ eingegangen worden, meint die Leiterin des IT-Referats des Bundesinstituts für Berufsbildung (BIBB). Für solche Anwendungsfälle gebe es sichere Lösungen. „Dort, wo es sie noch nicht gibt, sollte der Markt darauf drängen, dass sie eingeführt werden – Stichwort iPad.“

2.6.1 Keine Sicherheitskonzepte

Fey spricht ein Problem an, dass den IT-Verantwortlichen landauf landab auf den Nägeln brennt: Wie können Unternehmen mit dem Wildwuchs mobiler Endgeräte und den damit verbundenen Sicherheitsrisiken umgehen? Wie drängend das Problem ist, beweist eine Studie, die Frost & Sullivan in seiner „Global Information Security Workforce Study“ 2011 veröffentlichte. Die Unternehmensberatung hatte im Auftrag der Organisation zur Weiterbildung und Zertifizierung von Fachkräften für Informationssicherheit weltweit 10.413 IT-Sicherheitsexperten befragt.

Nicht mehr Viren-, Würmer- und Hackerangriffe bereiten CIOs demnach die größten Sorgen. Die meisten grauen Haare holen sich IT-Manager, wenn sie an Gefahren denken, die durch den Einsatz mobiler Endgeräte aufkommen könnten. Die Sicherheit mobiler Clients rangiert auf der Skala der Bedrohungen in Firmen an zweiter Stelle. Sorgen bereiten zudem die Themen Cloud Computing, soziale Netze und unsichere Softwareapplikationen, die eng mit der Nutzung mobiler Geräte verknüpft sind. Tenor der Studie von Frost & Sullivan: IT-Verantwortliche können bei der Entwicklung von Sicherheitsstandards nicht mehr mit der Entwicklung neuer Technologien Schritt halten. Die Befragten gaben an, nur über uneinheitliche Richtlinien und mangelnde Sicherheitskonzepte zu verfügen. Fast 30 Prozent räumten ein, ihr Unternehmen habe keine Sicherheitsrichtlinien.

2.6.2 Mobile Geräte und soziale Netze

Wie sehr die hippen Tragbaren verknüpft sind mit Web 2.0 und sozialen Netzen, zeigt indirekt eine Untersuchung des Industrieverbands Bitkom (www.bitkom.org). Diesem zufolge verdoppelte sich die Zahl derer, die per Handy im Internet surfen, innerhalb eines Jahres. 18 Prozent der Internet-Nutzer in Deutschland surfen mittlerweile via Mobiltelefon. Im Jahr zuvor waren es erst zehn Prozent gewesen. In absoluten Zahlen sind es jetzt neun Millionen. Damit sind die Risiken enorm gestiegen.

René Schuster, Mitglied des Bitkom-Präsidiums, geht davon aus, dass „die Zahl der Handy-Surfer weiter stark zunehmen wird“. Wesentliche Gründe für diesen Trend: Verstärkt würden Smartphones mit größeren und hochwertigen Displays angeboten und gekauft. Zudem stehe der Ausbau schneller Breitbandnetze auf LTE-Basis vor der Tür. LTE beschleunigt die mobile Übertragung von Daten erheblich. Die Mobilfunktechnik der vierten Generation dürfte Geschwindigkeiten von bis zu

100 Megabit/s ermöglichen. Experten bezweifeln allerdings, ob in diesem Szenario Smartphones und Netbooks mit ihren langsameren Bussystemen in der Lage sein werden, die via LTE einprasselnden Daten schnell genug zu verarbeiten.

2.6.3 Safety first und sicher geht vor stylish

Dem Gefährdungspotenzial, das sich durch die Einbindung von mobilen IT-Geräten für die Unternehmens-IT ergibt, begegnet BIBB-IT-Chefin (www.bibb.de) Fey mit der schlichten Devise: „Safety first". Übersetzt bedeutet das: Die Daten auf jedem mobilen BIBB-Gerät sind verschlüsselt. Zudem verfügen alle Systeme über einen speziellen Boot-Schutz. Als weitere Form der Diebstahlsprävention seien alle neueren Laptops auf dem Deckel mit einer Lasergravur des BIBB-Logos versehen. Das sehe sehr schick aus, diene der Corporate Identity – und verschrecke potenzielle Diebe, sagt Fey.

Eine Online-Verbindung zum Hausnetz besitzen mobile Geräte beim BIBB ausschließlich über eine BSI-zertifizierte VPN-Anbindung. Diese Vorgabe sorgt allerdings manchmal für Ärger, wie Fey schildert: „Bei Smartphones schränkt das die Produktauswahl erheblich ein, es können nur Systeme mit Windows Mobile eingesetzt werden." Deshalb würden einzelne Anwender von Zeit zu Zeit durchaus auch „toben". Denn „Android-Devices, iPads und so weiter sind wirklich verlockend". Aber die Institutsleitung trage den rigiden Sicherheitskurs mit. Es gelte: Sicher geht vor stylish. „Die Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte sind sehr dankbar für diese Strategieentscheidung", sagt Fey.

Neue Chancen: Für Klaus Straub, CIO bei der Audi AG, ist der Einsatz mobiler Clients auch eine Möglichkeit, die Attraktivität eines Unternehmens zu steigern.

Diese Haltung ist konsequent insofern, als sie Sicherheitsaspekte in den Vordergrund rückt, ohne mobile Geräte zu verteufeln. Viele deutsche CIOs suchen derzeit Antworten auf die Probleme, die sich aus Mobile Computing und Consumerization ergeben. Das zeigte sich etwa auf der Veranstaltung „CIO Beyond", die von der TecChannel-Schwesterzeitschrift „CIO" initiiert wurde. Audis CIO Klaus Straub (www.audi.de) gab die Meinung vieler wieder, als er sagte, die Consumer-IT sei „Impulsgeber für die Business-IT". Ähnlich drückte es Thomas Henkel, CIO von Amer Sports, aus: „Wir müssen die positiven Aspekte der Consumer-IT für

das Unternehmen nutzen." Aufzuhalten ist der Trend zu iPhones, iPads und dergleichen mobilen Endgeräten in Unternehmen ohnehin nicht mehr. Das sieht man auch in einer übernationalen Behörde so: Das Europaparlament will alle seine Abgeordneten mit iPads ausstatten.

2.6.4 Any time, any place, any device

Jürgen Renfer, Abteilungsleiter Informationstechnologie im Bayerischen Gemeindeunfallversicherungsverband / Bayerische Landesunfallkasse (GUVV/LUK, www.guvv-bayern.de), ist überzeugt, dass mobile Geräte zum Alltag der Unternehmens-IT gehören werden. Seine Erklärung: „Netbooks, Tablets, Smartphones & Co. erlauben die Fortsetzung und vielleicht sogar die Vollendung der alten Vision der Informationskommunikationsbranche: Any time, any place, any device." Den Erfolg der Geräte dieses Typs erklärt Renfer damit, dass sie mehr oder minder standardisierte Techniken über Geräte- beziehungsweise Herstellergrenzen hinweg erlauben. Außerdem: „Laufzeiten, Leistungsfähigkeit, Gewicht sowie Beschaffungskosten haben anwenderfreundliche Formen angenommen."

Neue Wege: Jürgen Renfer, Abteilungsleiter IT im Bayerischen Gemeindeunfallversicherungs-Verband/ Bayerische Landesunfallkasse (GUVV/LUK), sagt, dass mit den mobilen Endgeräten die alte Vision der IT-Branche vom Any time, any place, any device wahr werden könnte.

IT-Verantwortliche könnten deshalb beginnen, „zügig Mobile Devices zu ordern, um damit innovative ICT-Konzepte anzubieten – eingebettet in die Architektur der Unternehmen". Allerdings schränkt Renfer ein: „Prinzipiell besteht der Zielkonflikt zwischen Flexibilität beziehungsweise Mobilität einerseits und Datensicherheit respektive Datenschutz andererseits weiter."

Sicherheit geht vor: Niels Diekmann, IT-Leitung und Head of IT der Bartscher GmbH, plädiert dafür, dass auf den mobilen Clients keine Firmendaten lagern.

Niels Diekmann, IT-Leitung und Head of IT der Bartscher GmbH (www.bartscher.de), nimmt schon mal das Wort von der „Endgerätediktatur“ in den Mund. Sein Unternehmen hat daraus Konsequenzen gezogen: Um der „stark wachsenden Mobilität und den gesellschaftlichen Veränderungen und der daraus erwachsenden Konsumerisierung von IT“ Rechnung zu tragen, „nehmen wir immer mehr Abstand von der restriktiven Endgeräteabsicherung. Im Gegenzug müssen die Nutzer aber die Kröte schlucken, dass dies ein ‚Always-on-Szenario‘ voraussetzt.“ Mit dem würden sie sich die hohe Mobilität und Flexibilität erkaufen. Allerdings soll hierbei die Sicherheit der Unternehmensdaten nicht gefährdet werden.

Diekmanns IT-Abteilung setzt auf ein sicheres Design der gesamten IT-Infrastruktur. Die Idee ist, dass die Zentralisierung von Anwendungen und Daten im Rechenzentrum für umfassende Sicherheit sorgt, da auf den mobilen Endgeräten keine Unternehmensdaten vorgehalten werden müssen, „sondern lediglich Bildschirminhalte, Mausbewegungen und Tastatureingaben über das Netz verschlüsselt übertragen werden“.

2.6.5 Applikationen als Service

Das Konzept, Applikationen als Service bereitzustellen, bedeutet die Verlagerung der Anwendungen ins Rechenzentrum. Dort werden sie zentral verwaltet und den Benutzern in allen Unternehmensstandorten nach Bedarf zur Verfügung gestellt. Diekmann: „Dabei findet die Online-Nutzung von unterschiedlichen Endgeräten und Betriebssystemen auf hochleistungsfähigen Servern im Rechenzentrum statt.“

Neue Einsatzgebiete: Gerald Scheurmann-Kettner, CIO der Event Holding GmbH & Co KG in Köln, sagt, die Begehrlichkeit der Mitarbeiter, mobile Clients auch geschäftlich zu nutzen, wachse mit jedem neu auf den Markt kommenden Gerät.

Gerald Scheurmann-Kettner, CIO der Event Holding GmbH & Co KG. in Köln (www.eventholding.com), sieht sich wie alle seine Kollegen mit der Herausforderung konfrontiert, dass die Anforderungen der Mitarbeiter an mobile Kommunikation sich „nahezu täglich und mit jedem neu auf den Markt kommenden Gerät ändern. Damit wächst die Begehrlichkeit der Mitarbeiter, diese Geräte auch geschäftlich zu nutzen.“ Für die IT ergebe sich daraus der Zwang, all diese Geräte auf Herz und Nieren zu prüfen und zu eruieren, „ob es überhaupt Sinn gibt, sie im operativen Geschäft einzusetzen“. Bei der Event Holding entschied man sich be-

reits vor Jahren, „auf stabile und funktionsfähige Systeme zu wechseln, die auch Push-Dienste unterstützen". Im Ergebnis setzt das Unternehmen BlackBerry-Server ein. Scheurmann-Kettner: „Diese Plattform wurde im Lauf der Jahre weiter ausgebaut, so dass es derzeit keinen wirtschaftlichen Sinn hat, hier parallel Plattformen für iPhone und Co. in Betrieb zu nehmen."

2.6.6 Gut schlafen mit VPN

Trotzdem wünschen sich immer mehr Mitarbeiter, Tablet-PCs wie das iPad oder Samsungs Galaxy Tab beruflich zu verwenden, sagt der CIO. Für die IT gelte es erst einmal, „das firmeneigene Netzwerk zu schützen". Dabei setzt die Event Holding auf ein Konzept, das viele IT-Chefs bemühen: Verbindungen zum Firmennetz ausschließlich über sichere VPN-Verbindungen. So gehen Unternehmensdaten verschlüsselt und quasi durch einen Tunnel im Internet sicher auf die Reise.

Ausschließlich via VPN-Verbindung ans Firmennetz anzudocken ist die Strategie, die auch Markus Grimm, Direktor IT-Management bei der DKV Euro Service GmbH & Co. KG (www.dkv-euroservice.com), gewählt hat. Ähnlich halten es weitere Befragte, darunter Thomas Fischer, IT-Leiter beim Gesamtverband der Deutschen Versicherungswirtschaft (GDV, www.gdv.de), Frank Mauderer, der beim Autoveredler Mercedes-AMG GmbH (www.mercedes-amg.com) die IT-Sicherheit verantwortet, und Matthias Mehrtens, Leiter Informationsmanagement der Stadtwerke Düsseldorf AG (www.swd-ag.de). Allerdings lösen sie damit noch nicht das Problem, das dem ehemaligen Innenminister von Brandenburg zum Verhängnis wurde.

2.6.7 Firmendaten nie lokal speichern

Bei der Event Holding laufen laut Scheurmann-Kettner alle Arbeiten „ausschließlich über Citrix-Desktops, so dass – auch bei Verlust egal welchen Geräts – die Firmendaten niemals lokal gespeichert werden".

Markus Grimm vom DKV Euro Service nennt weitere Sicherheitsmaßnahmen, die in der unternehmensinternen Security-Policy festgeschrieben sind. Hierzu gehöre etwa, dass für die BlackBerry-Smartphones der Web-Zugang nur über interne Firewalls statthaft sei. Insbesondere bei Notebooks gilt als grundsätzliche Voraussetzung eine Festplattenverschlüsselung mit benutzerbezogenem Kennwort. Auch Grimm setzt auf den Zugang zum Firmennetz über VPN mit entsprechenden Kennwörtern. Zudem darf nur über das Firmennetz im Internet gesurft werden.

Rigide ist auch der Kurs in Sachen Schnittstellen: Auf den Windows-7-Rechnern der DKV werden die USB-Ports für Datenträger jeglicher Art gesperrt. Ausnahmen gibt es nur für „von der Firma freigegebene USB-Geräte. Die Daten müssen zudem stark verschlüsselt sein", erläutert Grimm. Im Moment liefen, so der IT-Verantwortliche des DKV Euro Service, noch Tests bezüglich des Einsatzes von

iPads und iPhones. Hier verwendet das Unternehmen etwa für die E-Mail-Kommunikation die Software „Good for Enterprise“. Sie verschlüsselt die E-Mail-Daten und „hält alle Firmendaten in einer App, die per benutzerbezogenes Kennwort geschützt ist“, sagt Grimm.

Wichtig: Markus Grimm, Direktor IT-Management bei der DKV Euro Service GmbH & Co. KG, besteht Notebooks gilt als grundsätzliche Voraussetzung eine Festplattenverschlüsselung mit benutzerbezogenem Kennwort.

Für Dominik Spannheimer, Leiter Organisation und Datenverarbeitung der Tyczka Totalgaz GmbH, waren mobile Endgeräte bis Dezember 2010 eher ein No-Go: „Im Jahr 2010 hatten wir uns noch der Öffnung für verschiedene Mobile-Funktionen verschlossen.“ Besonders iPhone-Lösungen seien aus verschiedensten Gründen nicht zugelassen gewesen. Spannheimer sagt: „Hauptsächliche Kritikpunkte waren und sind Themen wie das Herunterladen von Apps – hier ist von Apple nur eine Whitelist vorgesehen.“ Eine Blacklist zur Kontrolle der Apps sei im Business-Bereich aber unverzichtbar. Weiteres Kopfzerbrechen bereitete ihm der immer mögliche Verlust von Daten, wenn ein Gerät gestohlen wird oder sonst abhanden kommt. „Ein gestohlenes Endgerät kann doch sehr schnell mit entsprechenden Tools geknackt werden.“ Passwörter sowie wichtige geheime Unternehmensdaten seien dann nicht mehr sicher.

Im Detail: Dominik Spannheimer, Leiter Organisation und Datenverarbeitung der Tyczka Totalgaz GmbH, sagt, wichtig sei dem Unternehmen ein Software-Tool, mit dem „die Mobile Security entsprechend unseren Firmen-Policies“ umgesetzt werden kann.

Allerdings sah sich der Energieversorger Tyczka Totalgaz (www.tytogaz.de) seitens seiner Kunden und auch der eigenen Mitarbeiter immer häufiger mit Anfragen nach mobilen Lösungen konfrontiert. Man habe sich deshalb im Dezember 2010 entschieden, ein Tool zu verwenden, „das es uns erlaubt, die Mobile Security ent-

sprechend unseren Firmen-Policies umzusetzen". Mit dem Werkzeug „Ubitexx" könne man „alle mobilen Endgeräte unabhängig vom Betriebssystems steuern". Das ist insofern wichtig, als Tyczka Totalgaz zurzeit insbesondere Windows Phone 7 einsetzt, „aber auch mobile Betriebssysteme wie Apples iOS4 und zukünftig Android 3.0 Honeycomb", so Spannheimer. „Mit der Lösung können wir Endgeräte remote aktivieren, deaktivieren und den entsprechenden Support erledigen."

2.6.8 Sperrung via Fernwartung

Politiker Speer hätte sich sicher gewünscht, alle Daten auf seinem gestohlenen Notebook aus der Ferne sperren oder lieber noch ganz löschen zu können. Auch Thomas Fischer vom Gesamtverband der Deutschen Versicherungswirtschaft sieht in dieser Option eine grundsätzliche Voraussetzung für den Einsatz mobiler Endgeräte. Die sinnvolle Nutzung von Smartphones sei, so Fischer, ohnehin nicht mehr wegzudiskutieren. BlackBerrys zu benutzen sei insofern einfach „und besser, weil diese Geräte auch remote gemanagt werden können. Selbst die Sperrung ist möglich." Das ginge mittlerweile zwar auch bei iPhones. Allerdings setze Apple für diese Funktion einen persönlichen „MobileMe"-Account voraus: „Daher nutzen wir diese Möglichkeit noch nicht."

Fischer moniert beim Blick auf die bisher angebotene Sicherheitssoftware für Smartphones, es gebe gegenüber dem Desktop- oder Notebook-Markt noch einen deutlichen Optimierungsbedarf: „Hier muss etwas passieren", so der IT-Verantwortliche, „auch wenn die Angriffe heute noch überschaubar sind."

2.6.9 Zum Glück gezwungen

Frank Mauderer von Mercedes-AMG (www.mercedes-amg.com) verriegelt die Firmen-Clients „innerhalb des Corporate Networks bei AMG über die bekannten Schutzmechanismen AV, Firewall, Proxy mit Content Protection, Port-Security etc." Nach außen sichert sich die AMG-IT über VPN-Clients ab, die bei Verbindungen mit „jeglichen Netzwerken versuchen, ihren Heimathafen, hier das Corporate LAN, über eine gesicherte VPN-Verbindung zu erreichen". Mauderer ist sich bewusst, dass dieser Ansatz den Anwendern nicht viel Spielraum lässt: „Ein Ausbruch aus dieser Verbindung ist nicht möglich, der User wird zu seinem sicheren ‚Glück' gezwungen." Für den Fall, dass das Corporate LAN nicht erreicht werden kann, „befindet sich der Client entweder in einem Netzwerk ohne Internet-Zugang und ist somit relativ sicher, oder er hat kein Netz und ist damit noch viel sicherer", erklärt Mauderer lächelnd.

Das ist nicht alles, was Mercedes-AMG unternimmt, um die Sicherheit beim Einsatz mobiler Endgeräte zu wahren. Robert Münch, der beim Autohersteller für die Netzwerke verantwortlich ist, führt dazu aus: „Firmenfremde mobile Geräte werden nur nach Inspektion der sicherheitsrelevanten Merkmale im Netz erlaubt.

Nach der Nutzung werden sie wieder aus dem Netz ausgesperrt – Stichwort: Fremdhardware-Prozess und MAC-Schleuse." So sei jederzeit gewährleistet, dass ein vorgegebener Sicherheitslevel im Unternehmensnetz eingehalten wird.

2.6.10 Itil als Basis

Matthias Mehrtens von den Stadtwerken Düsseldorf konstatiert, dass Mobility zunehmend an Bedeutung gewinnen werde, an diesem Thema kämen auch die Stadtwerke nicht vorbei. Der Honorarprofessor und Lehrbeauftragte für Wirtschaftsinformatik an der Hochschule Niederrhein sagt, der Ruf nach komfortablen, intuitiv zu bedienenden Geräten wie dem iPad sowie nach nicht ortsgebundener Verfügbarkeit von Informationen über Mobile VPN werde lauter.

Die Implementierung von mobilen Services erfolge bei den Stadtwerken Düsseldorf dabei grundsätzlich in Anlehnung an das Itil-Lifecycle-Modell. „Disziplinen wie Demand-Management, Service- Portfolio-Management und Sicherheits-Management bilden hier den Rahmen für eine intelligente Vernetzung von Kundenanforderungen und IT-Sicherheit."

Stimmiges Gesamtpaket: Matthias Mehrtens, Leiter Informationsmanagement der Stadtwerke Düsseldorf AG, setzt bei den Sicherheitsmaßnahmen für mobile Clients auf Ende-zu-Ende-Verschlüsselung, eine starke Authentifizierung, Patch-Management und einen verlässlichen Virenschutz

Gefährdungen und Bedrohungspotenzialen für mobil einsetzbare Hardware, Betriebssysteme, Anwendungen und Kommunikationswege beuge man mit Schutzmaßnahmen vor. Dazu zählten beispielsweise die Ende-zu-Ende-Verschlüsselung, eine starke Authentifizierung, Patch-Management und ein verlässlicher Virenschutz. Services würden im eigenen Testcenter zertifiziert. Dabei gilt, was auch andere Unternehmen als Vorgabe gesetzt hätten: „Geräte und Anwendungen, die nicht den Vorgaben der Security-Policy entsprechen, werden ausschließlich außerhalb des Bürokommunikationsnetzwerks eingesetzt."

2.6.11 Attraktivität des Unternehmens

Für Klaus Straub von der Audi AG steht außer Zweifel, dass „mobile, leicht bedienbare und zum großen Teil aus dem privaten Umfeld bekannte Endgeräte, so weit

sinnvoll, im Unternehmen integriert werden sollten". Wie der von Computerwoche und „CIO" ernannte CIO des Jahres 2006 weiter ausführt, genießen solche Geräte nicht nur eine hohe Akzeptanz bei den Anwendern, sie erschließen auch ganz neue Möglichkeiten im Business-Einsatz. Außerdem, so ist sich Straub sicher, „erhöhen sie nicht zuletzt die Attraktivität des Unternehmens".

Herausfordernd seien allerdings die unterschiedlichen Plattformen und die „schnellen Innovationszyklen der Consumer Products". Straub umreißt, wie bei Audi das Thema Mobile Security behandelt wird: „Komplexitätsreduzierung im angebotenen und unterstützten Lösungs- und Gerätespektrum, plattformunabhängige Lösungen für die Entwicklung und Bereitstellung von Anwendungen, Verschlüsselung von Übertragungswegen, Dokumenten und Daten sowie die Kapselung der eingesetzten Applikationen."

Jan-Bernd Meyer

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

Jan-Bernd Meyer ist Redakteur bei der Computerwoche.

TecChannel-Links zum Thema	Webcode	Compact
Mobile Geräte wirkungsvoll gegen Missbrauch absichern	2034906	S.55
Smartphones: Malware-Gefahr wächst	2036827	S.36
Angriffsziel Tablets: Die Attacken kommen	2035208	S.39
Smartphones und Tablets sicher im Unternehmen einsetzen	2035129	S.43
Private Smartphones und Tablets sicher einbinden	2035485	S.47
Sicherheitsrisiken von Smartphones und Tablets minimieren	2035249	S.50
Verwalten, Sichern, Sperren: Notfallplan für verlorene Smartphones	2035516	S.65
Juniper Pulse Mobile Security für Smartphones	2036370	S.74
Smartphone- und Tablet-Sicherheit: Daten richtig verschlüsseln	2036785	S.81
Sicherheitsratgeber: Smartphones fernlöschen, orten und sperren	2036926	S.91
Empfehlenswerte Security-Apps für Android	2034879	S.99
Test: Sicherheitslösungen für Smartphones	2035250	S.104

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

2.7 Verwalten, Sichern, Sperren: Notfallplan für verlorene Smartphones

Wenn ein Smartphone mit geschäftskritischen Daten verschwindet, hilft nur noch Fernlöschen oder Sperren. Doch viele Unternehmen sind darauf nicht vorbereitet, und auch die mobilen Betriebssysteme unterstützen solche Sicherheitsoptionen nur unzureichend. Wir zeigen, welche Lösungen helfen.

Um den Schaden zu minimieren, der durch den Verlust von Mobilfunkgeräten entstehen kann, gibt es folgende Möglichkeiten:

- Sicherheitsfunktionen nutzen, die der Hersteller bereits in das Mobiltelefon integriert hat;
- Remote-Management-Funktionen einsetzen, die Anbieter von Online-Anwendungen wie Google (Google Apps) oder von Messaging-Produkten wie Microsoft (Exchange Server) oder BlackBerry (BlackBerry Enterprise Server) in ihre Programme integriert haben;
- Tools und Services von IT-Sicherheitsspezialisten verwenden, etwa von Absolute Software, Bak2U und IT Agents. Sie erlauben es, abhandengekommene Geräte zu lokalisieren, etwa mittels GPS, und ein Fernlöschen durchzuführen. Die Software von F-Secure, Kaspersky, McAfee, Symantec und anderen bekannten IT-Sicherheitsfirmen enthält zudem einen Virenschutz und eine Firewall. Häufig sind die Produkte der letztgenannten Anbieter Bestandteil von komplexeren Endpoint-Protection-Lösungen;
- ein Endgerätemanagement (Mobile Device Management) implementieren, mit dem sich alle Smartphones, gegebenenfalls auch Notebooks und Tablet-Rechner, im Unternehmen verwalten lassen.

Gleich, für welche Lösung sich ein Anwender entscheidet. Wichtig ist laut Gert Hansen, Geschäftsführer der deutschen IT-Security-Firma Astaro, dass sie folgende Sicherheitsfunktionen unterstützt: das Fernlöschen von Daten, die Verschlüsselung der Daten auf dem Gerät, die Möglichkeit, eine Passwort-"Policy" durchzusetzen, sowie die Option, den Standort eines Smartphones zu ermitteln.

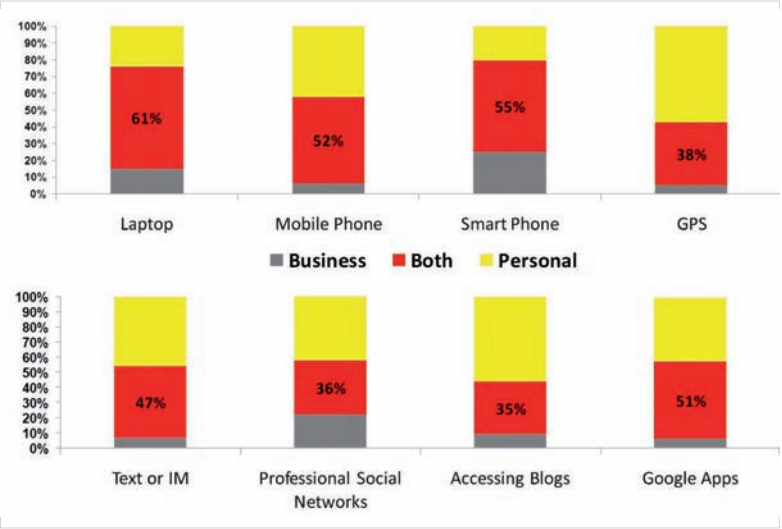
2.7.1 Zehntausende von Notebooks und Smartphones „verschwinden"

Darüber, wie viele Firmen-Notebooks „verschwinden", gibt es kaum verlässliche Zahlen. Das amerikanische Beratungsunternehmen Ponemon Institute hat 2010 rund 330 Firmen in den USA dazu befragt. Das erschreckende Ergebnis: Diesen Unternehmen kamen innerhalb eines Jahres 84.500 mobile Rechner abhanden. Nur 4000 wurden wiedergefunden. Rund 25 Prozent der Systeme wurden gestohlen, weitere 15 Prozent gerieten höchstwahrscheinlich in die Hände von Langfingern; an die 60 Prozent wurden von ihren Besitzern verloren.

Nach einer Studie des deutschen Hightech-Verbandes Bitkom räumten zehn Millionen Bundesbürger ein, dass ihnen bereits einmal ein Mobiltelefon abhandenkam. Laut der Umfrage vom Sommer 2010 wurden vier Millionen Bürger Opfer eines Diebstahls, rund sieben Millionen haben ein Mobiltelefon verloren. Mehr als eine Million Handy- und Smartphone-Nutzer gaben an, dass sie jeweils ein Mobilgerät verloren haben und mindestens ein weiteres gestohlen wurde.

2.7.2 Sicherheitsfunktionen des Smartphone nutzen

Etliche Hersteller von Mobiltelefonen bieten für Geräte der gehobenen Leistungs- und Preiskategorie erweiterte Sicherheitsfunktionen an. Samsung beispielsweise offeriert für Geräte unter dem hauseigenen Betriebssystem Bada und Android die kostenlose „uTrack"-Funktion. Sie sendet eine SMS-Nachricht an eine Telefonnummer, die der Nutzer zuvor festgelegt hat. Wird die SIM-Karte des Mobiltelefons ausgetauscht, übermittelt uTrack per SMS die Mobiltelefonnummer und weitere persönliche Daten, die auf der Karte des neuen Besitzers abgelegt sind.



Geschäftskritisch: Laut einer Studie von Unisys und IDC vom Juni 2010 setzen mehr als die Hälfte aller Beschäftigten weltweit private mobile Geräte wie Notebooks, Handys und Smartphones auch für geschäftliche Zwecke ein.

Bei Modellen mit dem Betriebssystem Android stehen zudem Funktionen für das Fernorten und -sperren sowie für „Remote Wipe" (Löschen) zur Verfügung. Das Fernlöschen erfolgt über den Google-Service „Google Remote Wipe", das Orten

und Sperren des Geräts über den Online-Dienst „Samsung Dive“. Ein vergleichbares Verfahren bieten Motorola mit „Motoblur“ und HTC mit „HTC Sense“ an, ebenfalls für Android-Smartphones.

Das Problem bei diesem Ansatz: Zum einen dürfte ein professioneller Dieb kaum seine eigene SIM-Karte in ein gestohlenes Gerät einsetzen. Den Übeltäter zu identifizieren wird daher nicht klappen. Zum anderen kann es laut Google bis zu drei Stunden dauern, bis das Fernlöschen tatsächlich erfolgt. Dies ist dann der Fall, wenn ein Mobiltelefon keine Verbindung zum Netz und damit zum Google-Server hat. Das lässt einem Angreifer genügend Zeit, Daten von dem Gerät zu kopieren.

Zudem gibt es zumindest bei Android-Gadgets keine einheitliche Linie: HTC ermöglicht beispielsweise das Remote Wipe des gesamten Geräts, inklusive der Speicherkarte. Bei Motoblur bleiben die Daten auf einer SD-Karte dagegen erhalten.

2.7.3 Apple setzt auf MobileMe/iCloud – Microsoft auf Windows Live

Auch Apples iPhone und die Smartphones der BlackBerry-Reihe von Research In Motion (RIM) sind mit ähnlichen Funktionen wie die Android-Geräte ausgestattet. Apple stellt Fernverwaltungsfunktionen wie Remote Wipe und Fernsperren bislang über seinen Online-Service „MobileMe“ zur Verfügung, dies wird künftig durch Apples iCloud ersetzt. Über MobileMe lassen sich iPhones sowie iPads sperren. Der Benutzer kann das Gerät dann nur nach Eingabe eines vierstelligen Zahlencodes aktivieren. Zudem ist es möglich, alle Daten aus dem Speicher des Systems zu löschen oder auf Google-Maps den Standort des Mobilgeräts anzuzeigen.

Ein vergleichbares Konzept hat Microsoft für Geräte unter Windows Phone 7 entwickelt. Besitzer solcher Smartphones, die einen kostenlosen Windows-Live-Account besitzen, werden künftig auf die gleichen Funktionen wie iPhone-Nutzer zurückgreifen können. SD-Speicherkarten lassen sich jedoch nicht fernlöschen. Allerdings verschlüsselt Windows Phone 7 die Daten auf solchen Karten automatisch mithilfe eines Keys, der auf das jeweilige Gerät zugeschnitten ist. Daher kann ein Angreifer die Daten nicht auslesen, indem er die Karte entnimmt und in ein anderes Smartphone oder einen Kartenleser steckt. Wer dagegen ein BlackBerry-Smartphone verwendet, hat die Möglichkeit, die Anwendung „BlackBerry Protect“ von RIM zu installieren. Mit ihr kann der Nutzer das Mobiltelefon sperren und alle Daten löschen, auch die auf Speicherkarten. Das ist für private User oder Mitarbeiter von kleinen Unternehmen praktisch, die keinen BlackBerry Enterprise Server (BES) betreiben. Ähnlich wie der BES bietet BlackBerry Protect eine Funktion, die das Sichern der Daten des Mobiltelefons auf Storage-Systemen von RIM erlaubt. Somit lassen sich die Sicherungskopien der Anwendungen und Daten auf ein neues BlackBerry-System überspielen. Die genannten „Bordmittel“ eignen sich in erster Linie für Selbstständige und kleine Unternehmen, die auf ein zentrales Management der Sicherheitsfunktionen für Smartphones verzichten können.

2.7.4 Kopplung mit Exchange oder Google Apps

Anders sieht es aus, wenn ein Unternehmen einen Messaging-Server nutzt, etwa Microsoft Exchange oder den BlackBerry Enterprise Server, eventuell auch eine gehostete Version, wie sie beispielsweise Microsoft mit Exchange Online anbietet. In diese Lösungen sind bereits Funktionen für das Management mobiler Geräte integriert. Microsoft Exchange Server 2007 und 2010 unterstützen beispielsweise über „Exchange ActiveSync" (EAS) Mobilgeräte unter Windows Mobile. Aber auch iPhones, Nokia-Smartphones unter Symbian und Android-Systeme ab Version 2.2 lassen sich damit verwalten. Das schließt das Fernlöschen von Daten mit ein. Speziell bei Exchange ist jedoch zu berücksichtigen, dass Android-Smartphones nicht in vollem Umfang unterstützt werden. Dies gilt auch für die aktuelle Exchange-Server-Version 2010 SP1. Einige Sicherheits-Policies, wie etwa das Verschlüsseln externer Speicherkarten oder das Wiederherstellen von Passwörtern, lassen sich nur auf Umwegen umsetzen. Für Android bietet beispielsweise Nitrodesk mit „Touchdown with Exchange ActiveSync" eine entsprechende Client-Software an. Touchdown erlaubt unter anderem das Remote Wipe mittels einer E-Mail, deren Betreff einen „Kill-Code" enthält.

Für Kunden seiner Online-Office- und Collaboration-Umgebung „Google Apps for Business" bietet Google „Apps Device Policy for Android" an. Mit der Managementapplikation können Systemverwalter Nutzern von Android-Geräten beispielsweise vorgeben, dass sie Passwörter verwenden sollen. Auch das Fernlöschen von Daten ist möglich. Das Smartphone wird in diesem Fall in den Auslieferungszustand zurückversetzt. Google Apps Device Policy for Android unterstützt die Android-Versionen ab 2.2. Auf Geräten mit Android 3.0 können Administratoren zusätzlich das Verschlüsseln des Anwendungs- und Datenspeichers aus der Ferne veranlassen – für Geschäftskunden ein absolutes „Muss".

2.7.5 Geschlossene, aber sichere Welt: BlackBerry

Nicht verwunderlich ist, dass Research In Motion (RIM) für seine BlackBerry-Smartphones ein umfassendes Management- und Sicherheitskonzept anbietet. Der Hersteller adressiert mit seinen Geräten vorzugsweise Geschäftskunden. Anwender, die den BlackBerry Business Enterprise Server (BES) im Unternehmensnetz einsetzen, haben die Möglichkeit, BlackBerrys, inklusive Speicherkarten, „remote" zu löschen oder zu sperren.

Als bislang einziger Hersteller bietet RIM zudem die Möglichkeit, ein Gerät „remote" komplett unbrauchbar zu machen. Selbst ein Zurücksetzen des Smartphones auf die Basiseinstellungen, mit dem sich andere Smartphones reaktivieren lassen, hilft nicht weiter. Mithilfe von Security-Policies lässt sich festlegen, wann ein Löschen der Daten oder ein Fernsperren erfolgt, etwa nach zu häufiger Fehleingabe des Passworts oder nach Austauschen der SIM-Karte.

Wipe Device: Für BlackBerry-Smartphones hat RIM die Sicherheitssoftware BlackBerry Protect entwickelt. Sie erlaubt es auch ohne BlackBerry Enterprise Server oder Microsoft Exchange, ein Smartphone zu sperren oder die Daten darauf remote zu löschen.

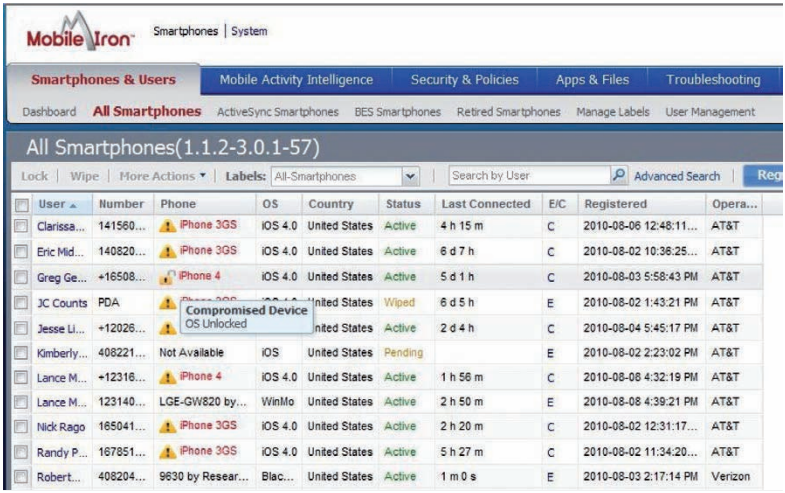
2.7.6 Virtualisierung: Privates und Geschäftliches auf einem Smartphone

Ein Trend, der IT-Sicherheitsmanagern Kopfzerbrechen bereitet, ist die „Consumerization" der IT in Unternehmen. Das heißt, immer mehr Mitarbeiter nutzen private Notebook-Rechner oder Smartphones auch für geschäftliche Zwecke. Ein Problem, das dadurch entsteht: Es gibt keine klare Trennung zwischen privaten und geschäftlichen Daten und Anwendungen. Ein Sicherheitsloch, das beispielsweise durch privat genutzte Apps auf dem Smartphone entsteht, kompromittiert möglicherweise auch geschäftskritische Informationen oder erlaubt Angreifern gar den Zugriff auf Daten im Unternehmensnetz. Um beide Welten – privat und geschäftlich – zu trennen, bietet sich der Einsatz von Virtualisierungssoftware an. Für mobile Rechner, wie etwa Notebooks, gibt es bereits Lösungen, etwa von VMware, Citrix-Xen oder Parallels. Auf dem System wird in diesem Fall eine virtualisierte Arbeitsumgebung eingerichtet, die ausschließlich für Business-Anwendungen und entsprechende Daten reserviert ist. Für Smartphones gab es eine solche Lösung bislang nicht. VMware hat Anfang Februar mit der „Mobile Virtualization Platform" (MVP) den Prototypen einer Virtualisierungssoftware für Smartphones vorgestellt. Sie soll im Laufe des Jahres auf den Markt kommen. Die erste Version unterstützt Android. IT-Verwalter können per Fernzugriff Sicherheitsregeln für die Virtual Machine festlegen, inklusive Fernlöschen von Daten, das zwangsweise Aufspielen von Sicherheitssoftware sowie das Deaktivieren von potenziell gefährlichen Funktionen wie Bluetooth oder der integrierten Kamera.

2.7.7 Tools von Drittanbietern

Wer sich in den App-Stores der Smartphone-Anbieter umsieht, stößt auf eine Unzahl von Anwendungen („Apps"), die das Aufspüren, Sperren oder Fernlöschen solcher Geräte ermöglichen sollen. Beispiele dafür sind „Anti-Theft" von Bak2u

Mobile Security, „Lookout“ von Lookout Mobile Security, „Snuko Anti-Theft“ von Snuko und „Theft Aware“ von IT Agents. Die Preise für diese Programme sind höchst unterschiedlich. Sie bewegen sich zwischen wenigen Euro bis hin zu etwa 30 Dollar pro Jahr und Gerät.



Unterstützung: Mobile-Device-Management-Programme wie Mobile Iron erlauben es dem IT-Verwalter, eine Vielzahl von Smartphones von einer Konsole aus zu managen.

Wie der Name der Programme bereits nahelegt, sollen sie den Diebstahl von Smartphones erschweren beziehungsweise die Daten darauf unbrauchbar machen. Die meisten dieser Anwendungen erkennen, wenn die SIM-Karte ausgetauscht wird, und versenden dann an eine hinterlegte Handynummer eine SMS mit Daten wie der neuen Rufnummer und weiteren Kenndaten, die auf der neuen SIM-Karte gespeichert sind. Der Eigentümer des Smartphones kann dann – ebenfalls per SMS – bestimmte Funktionen auf dem Gerät aktivieren, etwa Remote Wipe oder das Übermitteln von Positionsdaten. Computrace Mobile von Absolute Software hat sich auf das Aufspüren und Wiederbeschaffen von gestohlenen Mobilsystemen spezialisiert. Der Anbieter ermittelt den Standort eines Geräts und informiert anschließend die Polizei. Der Vorteil solcher Antidiebstahlsoftware und der entsprechenden Services ist, dass sie meist relativ einfach zu installieren und zu verwalten sind. Dies erfolgt über eine webgestützte Schnittstelle. Der Nutzer muss sich allerdings beim Anbieter registrieren und ihm den Zugriff auf Funktionen der verwalteten Smartphones einräumen. „Das ist vor allem für mittelständische Firmen ein Problem“, sagt Gert Hansen von Astaro. „Deutsche Unternehmen erlauben solchen Anbietern, die meist in den USA beheimatet sind, nur ungern den Zugang zu Geschäfts-Smartphones.“

2.7.8 Mit Firewall und Virenschutz

Vom wachsenden Sicherheitsbedürfnis von Smartphone-Nutzern wollen natürlich auch etablierte IT-Security-Spezialisten profitieren. Sie kombinieren in ihren Produkten klassische Funktionen wie Virenschutz, Firewall und Browser-Sicherheit mit Eigenschaften wie Fernlöschen und Fernsperren von Geräten. Zu den Anbietern zählen unter anderem F-Secure (Mobile Security), Kaspersky (Mobile Security 9), McAfee (Wavesecure) und Symantec (Norton Mobile Security).

Einige Produkte, wie etwa Wavesecure, bieten als Ergänzung ein Online-Backup an. Der Nutzer kann die Daten auf seinem Smartphone auf Servern von McAfee speichern und bei Bedarf auf ein Mobilgerät zurückspielen. Auch in diesem Fall gilt jedoch, dass dieser Ansatz für Firmenkunden hierzulande aus Datenschutzgründen problematisch ist. Wer auf seinem Firmen-Smartphone beispielsweise Kundendaten speichert, und seien es nur die E-Mail-Adressen und Telefonnummern im Kontakteordner, unterliegt den Regelungen des Bundesdatenschutzgesetzes. Dies schränkt das Speichern von sensiblen Informationen auf IT-Systemen außerhalb der EU drastisch ein.

2.7.9 Verfahren für den Schutz mobiler Geräte

Um mobile Geräte und die darauf befindlichen Daten zu schützen, ist ein mehrstufiges Konzept erforderlich. Die IT-Sicherheitsbehörde ENISA (European Networks and Information Security Agency) der Europäischen Union empfiehlt unter anderem folgende Maßnahmen:

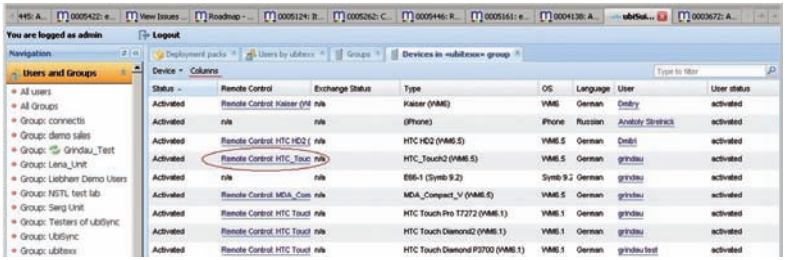
- **Passwörter für das Entsperren des Gerätes einsetzen:** Wird das Smartphone einige Minuten lang nicht genutzt, sollte es automatisch gesperrt werden. Nur nach Eingabe des Passworts ist es wieder zugänglich. Viele User deaktivieren diese Funktion jedoch aus Gründen der Bequemlichkeit. Das Passwort sollte „stark“ sein, das heißt aus einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Passwörter wie „12345“ oder der Vorname sind tabu.
- **Datenverschlüsselung und Backup:** Sie sollten in jedem Fall implementiert sein. Eine Verschlüsselung verhindert den direkten Zugriff auf Informationen durch Unbefugte. Wichtig ist, dass ein Backup der Daten auf dem Gerät erstellt wird, damit sich die Informationen nach Verlust der Hardware wiederherstellen lassen. Auch die Sicherung sollte verschlüsselt werden.
- **So wenige Firmendaten wie möglich auf dem Gerät speichern:** Besser ist es, mit dem Smartphone über verschlüsselte Verbindungen Geschäftsdaten abzurufen, die auf einem Server- oder Storage-System im Firmenrechenzentrum lagern.
- **Fernlöschen von Daten (Remote Wipe) ermöglichen:** Für Firmen-Smartphones ist dies ein „Muss“. Das Löschen muss auch dann möglich sein, wenn

die SIM-Karte gewechselt wurde. Empfehlenswert ist, das Fernlöschen automatisch zu starten, wenn zu oft ein falsches Passwort oder eine unrichtige PIN eingegeben wurden. Wichtig: Auch Massenspeicher wie SD-Karten sollten sich löschen lassen.

- **Fernsperren (Remote Lock):** Das Unbrauchbarmachen des Geräts durch Remote Lock funktioniert derzeit nur beim BlackBerry in der gewünschten Weise. Alle anderen Systeme lassen sich durch Zurücksetzen auf die Werkseinstellungen und Flashen des internen Speichers wieder benutzbar machen. Allerdings werden dann auch die auf dem Gerät gespeicherten Daten gelöscht.
- **Den Aufenthaltsort von Geräte bestimmen (Tracking):** Services wie Absolute Computrace, Mylook oder Prey Project (für Notebooks) ermöglichen es, den Aufenthaltsort eines Mobilgeräts zu bestimmen. Auch Hersteller wie Dell und HP ermitteln den Standort von Notebooks und Smartphones, etwa mittels GPS, über die Ortung mittels Mobilfunk oder das Erfassen der IP-Adresse beim Aufbau einer Internetverbindung.
- **Protokollierung (Audit Logs):** Falls ein Smartphone „verschwindet", verlangen Compliance-Vorschriften, dass ein Unternehmen nachweist, welche vertraulichen Informationen verloren gingen oder entwendet wurden. Zudem muss eine Firma belegen, dass sie Informationen auf einem solchen Gerät ferngelöscht hat, und nachweisen, welche Daten dies waren. Um diese Vorgaben zu erfüllen, ist ein Mobile Device Management erforderlich, am besten in Verbindung mit einem Log-Management-System, das auch die Aktivitäten von IT-Systemverwaltern mitprotokolliert, etwa BalaBit Shell Control Box.

2.7.10 Der ganz große Ansatz: Mobile Device Management

Spätestens dann, wenn mehr als 50 bis 100 mobile Geräte im Unternehmen vorhanden sind, sollte sich ein Unternehmen mit dem Thema „Mobile Device Management" (MDM) beschäftigen. Denn Smartphones, eventuell noch mit diversen Betriebssystemen, „von Hand" auf demselben Sicherheitsniveau zu halten ist so gut wie unmöglich. Gängige MDM-Lösungen sind beispielsweise „Afaria" von Sybase, „Good Mobile Control" von Good Technology, „ubi Suite" der deutschen Firma Ubitexx, „Symantec Mobile Management", „Junos Pulse Mobile Security" von Juniper Networks, die „Virtual Smartphone Management Platform" von Mobile Iron und auch Microsofts „System Center Mobile Device Manager". Zu den Newcomern in diesem Bereich zählt Kaseya mit „Kaseya Mobile Device Management 1.0". „Tarmac" von Euqinux fokussiert sich auf das Management von iPhones und iPads. Selbst Cloud-gestützte Lösungen erscheinen auf der Bildfläche. Dazu zählt HPs „Cloud Services Enablement for Device Management as a Service". Es versetzt Service-Provider in die Lage, die mobilen Endgeräte von Kunden im Rahmen eines Software-as-a-Service-Angebots zu verwalten.



Details: Ein Mobile Device Management (MDM) wie das von Ubitexx ermöglicht es nicht nur, Sicherheits-Policies auf Smartphones und Notebooks durchzusetzen, sondern auch, Daten auf gestohlenen Geräten fernzulöschen und die Systeme zu sperren.

Mobile-Device-Management-Lösungen bieten weit mehr Funktionen als Remote Wipe, Fernsperren und das Aufspüren verloren gegangener Geräte. Es handelt sich in der Regel um relativ komplexe Systemmanagementprogramme, die den gesamten Lebenszyklus eines mobilen Geräts abdecken: vom „Roll-out" bis zum sicheren Entsorgen nach sicherem Löschen aller Daten auf einem Notebook oder Smartphone. Mit einer MDM-Software lassen sich benutzerspezifische Sicherheitsregeln umsetzen, Anwendungen und Updates über die Luftschnittstelle („over the air") aufspielen und der Zugriff auf Daten und Anwendungen im Unternehmensnetz via Smartphone reglementieren. Der Preis liegt im Jahr bei etwa 20 bis 50 Euro pro Gerät. Juniper verlangt beispielsweise an die 2400 Dollar pro 50 Nutzer.

2.7.11 Fazit

Unternehmen, die mehr als 50 bis 100 Smartphones und andere mobile Geräte wie Tablet-Rechner und Notebooks auf effiziente Weise verwalten wollen, kommen um ein „Mobile Device Management" nicht herum. Das gilt vor allem für Firmen, in denen mehrere Smartphone-Plattformen parallel im Einsatz sind, etwa BlackBerry und iPhone. Mithilfe entsprechender Managementpakete kann die IT-Abteilung weitergehende Security-Policies umsetzen, etwa das Verschlüsseln von Daten auf dem Gerät und Speicherkarten oder die Kommunikation zwischen Smartphone und Anwendungen im Firmennetz über gesicherte Verbindungen.

Für kleine Unternehmen und private Nutzer sind weniger leistungsstarke, dafür preisgünstigere Lösungen ausreichend, die grundlegende Funktionen wie Remote Wipe, ein (Online-)Backup der Daten und das Lokalisieren eines Smartphones bereitstellen. Allerdings sollte der Nutzer im Vorfeld klären, welche Funktionen eine solche Lösung konkret bereitstellt, etwa ob sie auch Daten auf SD-Karten löscht.

Bernd Reder

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

2.8 Juniper Pulse Mobile Security für Smartphones

Smartphones sind mittlerweile Grundausstattung in Unternehmen; immer mehr Anwender nutzen sie. Sie wollen E-Mail-Anbindung, Internetzugang, WLAN und andere Funktionen des Smartphones auch in der Firma nutzen. Auch SharePoint, Exchange, Kalender und Aufgaben sowie Dokumente synchronisieren immer mehr Nutzer zwischen PC und Smartphone.

Die gleichen Smartphones finden aber auch im Privatleben Einsatz. Die Mitarbeiter installieren private Apps, binden die Geräte im heimischen Netzwerk und an öffentlichen Hotspots an. Ein Sicherheitsbewusstsein wie bei PCs gibt es bei Smartphones nicht oder zumindest nur sehr eingeschränkt. Geht ein solches Gerät verloren, besteht die Gefahr, dass Unbefugte Zugriff auf die abgespeicherten Daten, E-Mails und das Unternehmensnetzwerk erhalten, da die Zugriffsinformationen im System gespeichert sind.

Junos Pulse: Security-Suite für Smartphones.

Aus diesem Grund ist es notwendig, dass sich Administratoren Gedanken über die Sicherheit der Geräte und deren Anbindung an das Netzwerk machen. Neben den Standardmitteln, die Android, iPhone, iPad, Windows Phone 7, BlackBerry, Symbian und Co. bieten, können spezielle Verwaltungsapplikationen ebenfalls für Sicherheit sorgen, da diese zentral alle Plattformen verwalten und absichern können. Ein solches Beispiel ist Juniper Pulse Mobile Security.

2.8.1 Unterstützte Systeme und Smartphones

Juniper Pulse Mobile Security (www.juniper.net) unterstützt die meisten Smartphone-Systeme, aber nicht alle Funktionen durchgehend in allen Systemen. Das liegt daran, dass die einzelnen Anbieter selbst bestimmen können, welche Funktionen externe Anwendungen auf den Smartphones steuern können. Vor allem

Apple ist mit iOS hier absolut restriktiv und lässt fast keine Änderungen oder Zugriffe zu. Die Anbindung an das Firmennetzwerk über SSL-VPN unterstützen iOS 4.x, Google Android ab 2.0, Windows Mobile ab 6.0 – allerdings noch kein Windows Phone 7 – sowie Nokia Symbian und BlackBerry. Letzteres erlaubt aber nur webbasierten Zugriff.

Der Antivirenschutz lässt sich für alle Systeme nutzen – mit Ausnahme von iOS, hier sperrt Apple externe Anwendungen komplett aus. Das gilt auch für Personal Firewall, Anti-Spam, Überwachung, Datensicherung und Wiederherstellung sowie Diebstahlschutz. Alle diese Funktionen sind nicht mit iPhones und iPads möglich. Das heißt, falls Sie auf Apple-Systeme setzen, ist Juniper Pulse Mobile Security nur eine passende Lösung, wenn Sie die VPN-Funktionalität nutzen wollen. Zusätzlich müssen Sie beim Einsatz von iPhones und iPads auf weitere Lösungen oder Bordmittel setzen. Google Android unterstützt alle Funktionen, aber nur sehr eingeschränkt die Firewall und den Spamschutz. Windows Mobile, Nokia Symbian und BlackBerry sind ebenfalls universell einsetzbar, wogegen BlackBerry nicht alle Möglichkeiten der Firewall und des Spam-Schutzes nutzen kann. Windows Phone 7 findet sich aktuell nicht auf der Liste der unterstützten Geräte. Da sich das System deutlich von Windows Mobile 6.5 unterscheidet, ist zu erwarten, dass die Systeme mit dem neuen System nicht kompatibel sind. Auch eine entsprechende App für Windows Phone 7 findet sich nicht im Marktplatz.

2.8.2 Junos Pulse Mobile Security Gateway

Damit Sie zentral auf den Clients über die entsprechende Junos-App (http://itunes.apple.com/de/app/junos-pulse/id381348546?mt=8) die Smartphones absichern können, müssen Sie im Unternehmen ein Junos Pulse Mobile Security Gateway einsetzen. Voraussetzung dafür ist, dass Sie einen eigenen Server betreiben; Sie können ein solches Gateway aber auch direkt bei Juniper über die Cloud als Software-as-a-Service (SaaS) buchen.

Junos Pulse: Auswahlbildschirm der iPhone-App.

Verwaltung und Überwachung der Endgeräte steuern Administratoren über eine webbasierte Oberfläche. Über das Gateway laufen Sicherheitsrichtlinien, Virenschutz und Anti-Spam. Auch Berichte über Infektionen, Angriffe, Firewall, Updates und andere Bereiche rufen Sie an dieser Stelle ab. Unabhängig von den eingesetzten Systemen können Sie überprüfen, welche Apps installiert und welche davon nicht erlaubt sind. Auch das Lokalisieren, Sperren, Löschen, Sichern oder Wiederherstellen nehmen Sie über diese Verwaltungsoberfläche vor. Sie können an dieser Stelle zudem steuern, ob Geräte, die nicht den Sicherheitsvorschriften entsprechen, über das VPN eine Verbindung zum Netzwerk aufbauen können, oder diese Geräte sperren. Der Schutz besteht also aus einer Client-Komponente und einem Servergegenstück, über das Sie die Endgeräte verwalten.

Junos Pulse auf dem iPad: Konfigurieren der VPN-Verbindung.

2.8.3 Sicherheit für Smartphones zentral verwalten

Juniper Pulse Mobile Security bietet eine Firewall, Anti-Spam, einen Diebstahlschutz, sowie Überwachungsmöglichkeiten für Smartphones. Die Möglichkeit der Datensicherung und Wiederherstellung über das Internet besteht ebenfalls. Auch die Funktion der Fernlöschung (Remote Wipe) unterstützt die Suite, allerdings nicht für alle Geräte.

Ein Bestandteil der Suite ist ein Client, der auf den Smartphones installiert werden muss. Juniper unterstützt aktuell Apple iOS (iPhone/iPad), Google Android, Windows Mobile, Nokia Symbian und BlackBerry. iOS wird dagegen nur sehr rudi-

mentär unterstützt, Sie können bei den Apple-Systemen nur die SSL-VPN-Verbindung nutzen. Installation und Einsatz sind allerdings recht kompliziert, Administratoren sollten für den Umgang mit der Lösung geschult werden. Sie benötigen zusätzlich zur Client-App noch eine Anbindung an ein Security Gateway. Dieses bietet Juniper auch als Cloud-Dienst an. Den jeweiligen Client für Juniper Pulse können Sie direkt im entsprechenden App-Store der Smartphone-Lösung kostenlos herunterladen und installieren.

Durch den Client ist es möglich, dass sich die Smartphones über eine gesicherte VPN-Verbindung mit dem Unternehmensnetzwerk verbinden, um Daten abzurufen. Diese Funktion läuft auch problemlos auf iPhones und iPads. Stellen Sie als Administrator im Unternehmen oder als Cloud-Lösung das Gateway zur Verfügung, können Anwender auch selbst den Juniper-Pulse-Client aus dem App-Store (Android, iOS), Marketplace (Windows Mobile 6, nicht Windows Phone 7) oder Ovi-Store (Nokia) herunterladen und installieren.

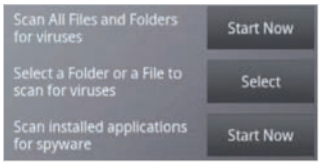
Administration: Juniper-Client nach der erfolgreichen Verbindung mit dem Gateway konfigurieren.

Dank einer einfach gehaltenen Anleitung kann der Client problemlos eingerichtet werden. Generell müssen Anwender nur die URL für die Verbindung zum Gateway selbst eintragen; alle anderen Einstellungen nehmen Administratoren über die Verwaltungsoberfläche durch.

2.8.4 Integrierter Virenschutz

Der integrierte Virenschutz scannt Dateien auf dem Smartphone, sobald ein Anwender darauf zugreift. Dabei spielt es keine Rolle, ob der Anwender die Datei per FTP, HTTP, SharePoint, Mail, SMS oder Dateifreigabe verwendet. Smartphone-Systeme mit SD-Karten sind ebenfalls geschützt, da Juniper auch diese scannen kann. Auch den Datenstrom zwischen Server und Smartphone scannt die Software auf verdächtigen Code und Viren. Neben dem Echtzeitschutz lassen sich zudem installierte Anwendungen, Dateien oder das ganze Smartphone nach Viren durchsuchen. Die Definitionsdateien aktualisieren sich automatisch, lassen sich in der Software aber auch manuell herunterladen und aktualisieren. Der Virenschutz lässt sich allerdings nicht in iOS-Geräten nutzen, dafür aber auf Android-Geräten,

die ohnehin anfälliger für Viren sind, sowie in Geräten mit Windows Mobile und BlackBerry. Während Apple sehr streng kontrolliert, welche Apps im App-Store verfügbar sind, ist der Google-App-Store wesentlich offener und damit auch stärker gefährdet, Apps zur Verfügung zu stellen, die virenverseucht sind. Viren für Smartphones sind aktuell noch dünn gesät. Allerdings gibt es durch die steigende Verbreitung solcher Geräte auch immer mehr Viren. Hier sollten Unternehmen daher besser agieren als nur zu reagieren.



Schutz: Antivirenlösung in Android verwalten.

2.8.5 Personal Firewalls für Smartphones

Neben der sicheren SSL-VPN-Datenleitung und dem Virenschutz enthält Juniper Pulse auch eine Firewall für Smartphones. Diese filtert und blockiert mit entsprechenden Regeln den TCP/IP-Verkehr von Smartphones. Die Regeln unterstützen bidirektionale Verbindungen, Ports oder IP-basiertes Filtern des Datenverkehrs. Die Lösung kann dazu eingehenden und ausgehenden Datenverkehr überwachen.

Anwender können die Firewall auf zwei Stufen einstellen. In der hochsicheren Stufe darf der Anwender nur erlaubten Netzwerkverkehr nutzen, der in einer speziellen Whitelist integriert ist.

Alle anderen Ports und Daten blockiert die Anwendung. Umgekehrt darf das Smartphone in der niedrigen Stufe den ganzen Netzwerkverkehr nutzen mit Ausnahme des Verkehrs, der in der Blacklist festgelegt ist. Die Firewall kann Datenverkehr auch von bestimmten IP-Bereichen zulassen oder auf Wunsch blockieren. Auch hier sind Anwender mit iPhones/iPads ausgesperrt, da Apple die Netzwerkkommunikation nicht von externen Anwendungen überwachen lässt.

2.8.6 Spam-Schutz

Selbst wenn Sie auf dem E-Mail-Server im Unternehmen einen Spam-Schutz betreiben, ist ein weiterer Schutz auf dem Endgerät durchaus sinnvoll. Vor allem wenn Anwender zusätzlich zur Unternehmensanbindung einen privaten E-Mail-Anschluss auf dem Smartphone konfiguriert haben, ist dieser meistens nicht vor Spam und auch nicht vor Viren geschützt.

Auch hier hilft Juniper Pulse. Mit dem Spam-Schutz können Anwender unter anderem Sprachanrufe blockieren, zum Beispiel während einer Besprechung, und SMS-Spam verhindern. Es lassen sich wieder schwarze und weiße Listen definie-

ren. Mit den Standardmitteln von Smartphones können Anrufe zwar generell blockiert oder Klingeltöne abgestellt werden, über Juniper können Anwender aber bestimmte wichtige Nummern und Kontakte durchlassen und andere blockieren.

Der Spam-Schutz reagiert bei dieser Funktion intelligent und fragt ab, ob Nummern von Anrufen, die Sie abweisen, zu einer der Listen hinzugefügt werden sollen. Der Nutzer kann steuern, ob alle Nachrichten oder Anrufe von Nummern aus der schwarzen Liste blockiert werden sollen oder nur einzelne Anrufe und Nachrichten. Auch der Speicherort blockierter Nachrichten lässt sich festlegen. Diese Funktion steht in iPhones/iPads nicht zur Verfügung.

2.8.7 Diebstahlschutz für Smartphones

Eine weitere Funktion in Juniper Pulse ist der Diebstahlschutz. Die Suite ermöglicht die Lokalisierung von Smartphones über GPS und der Anzeige auf einer Online-Karte. Sowohl Anwender als auch der Admin im Unternehmen können verloren gegangene Geräte über das Internet sperren, löschen oder einen lauten Alarm abspielen lassen, sodass sich das Gerät orten lässt.

Das kann zum Beispiel auf Messen sehr hilfreich sein, da eine reine Lokalisierung dann nicht ausreicht. Neben diesen Funktionen können Anwender die Daten auf dem Gerät auch remote sichern und auf einem neuen Gerät wiederherstellen. Dazu muss das verloren gegangene Gerät natürlich eine Verbindung zum Internet haben. Auch die Wiederherstellung über das Internet ist auf diesem Weg möglich. Leider sind diese Funktionen nicht in iPhones/iPads integriert. Hier können Sie aber notfalls auf den Dienst MobileMe setzen.

2.8.8 Smartphones und installierte Apps überwachen

Junos Pulse ermöglicht es, Sicherheitsrichtlinien auf Endgeräten durchzusetzen. Natürlich ist es hier nur möglich, diejenigen Funktionen zu nutzen, die die Endgeräte auch zulassen. Vor allem iOS ist hier sehr restriktiv, Android dagegen sehr offen. Administratoren können auch die Apps steuern, die auf den Endgeräten installiert werden dürfen. Auch kann der Systemverwalter schwarze Listen pflegen und so festlegen, welche Apps Anwender nicht installieren dürfen. Auch die Aktionen des Anwenders bezüglich E-Mail-Verkehr, SMS, MMS, Kontakte und Fotos lassen sich überwachen.

Somit hat der Admin immer die Kontrolle darüber, welche Apps auf dem Gerät installiert sind, unabhängig vom eingesetzten System. Im Rahmen der Überwachung kann der Junos-Client dem Systemverwalter Bescheid geben, wenn der Anwender die SIM im Gerät wechselt. Mit iPhones/iPads ist das nicht möglich.

2.8.9 Fazit

Der Smartphone-Markt ist auf Wachstumskurs. Da aber die Anwender die Geräte nicht nur privat, sondern auch im Unternehmen nutzen, steigen die Gefahren für die Sicherheit mit dem Nutzungsgrad der Smartphones. Aus diesem Grund sollten Administratoren diese Systeme nicht ignorieren, da erhebliche Gefahr besteht, dass über Smartphones Viren ins Netzwerk eingeschleust oder wichtige Unternehmensdaten verloren gehen. Da es auf diesem Markt hauptsächlich um iOS, Android, BlackBerry, Symbian und Windows Mobile/Phone geht, muss eine Anwendung zum zentralen Verwalten der Smartphones auch alle Systeme unterstützten. Hier fängt allerdings das Problem an: Vor allem Apple ist mit iOS sehr restriktiv und lässt nahezu keine Eingriffe in das Betriebssystem zu. Das ist auf der einen Seite sicher, aber auf der anderen Seite sperrt Apple dadurch Sicherheitsanbieter aus.

Im Falle von Juniper können Sie für iOS-Geräte, also iPhone und iPad, nur die SSL-Funktion nutzen. Windows Mobile 6.0/6.5 ist ein Auslaufmodell, und Microsoft bietet mit Windows Phone 7 ein neues System an. Dieses ist noch nicht auf der aktuellen Liste der unterstützten Smartphones von Juniper Pulse Mobile Security zu finden, doch bereits im Herbst soll mit Mango (Windows Phone 7.5) eine aktualisierte Version kommen. Aktuell lässt sich also festhalten, dass Juniper Pulse Mobile Security vor allem für Android und BlackBerry sowie das alte Windows-Mobile-System optimiert ist. Der Preis für die Software liegt etwa bei 2.600 Euro für 50 Benutzer. Die Apps im entsprechenden Store stehen kostenlos zur Verfügung.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

TecChannel-Links zum Thema	Webcode	Compact
Juniper Pulse Mobile Security für Smartphones	2036370	S.74
Verwalten, Sichern, Sperren: Notfallplan für verlorene Smartphones	2035516	S.65
Smartphone- und Tablet-Sicherheit: Daten richtig verschlüsseln	2036785	S.81
Sicherheitsratgeber: Smartphones fernlöschen, orten und sperren	2036926	S.91
Empfehlenswerte Security-Apps für Android	2034879	S.99
Test: Sicherheitslösungen für Smartphones	2035250	S. 104

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

2.9 Smartphone- und Tablet-Sicherheit: Daten richtig verschlüsseln

Bei professionell eingesetzten Business-Notebooks längst Standard: ein ordentlicher Zugriffsschutz und die Verschlüsselung der Daten. Gerät so ein Notebook in die falschen Hände, können die Daten nicht ohne Weiteres in ebensolche gelangen. Derlei Engagement in Sachen Sicherheit ist bei Smartphones noch nicht so häufig anzutreffen. Dabei handelt es sich bei den aktuellen Geräten ja im Prinzip auch nur um mobile Rechner, mit denen man eben zusätzlich noch telefoniert.

Leider bieten die Smartphone-Hersteller in Sachen Verschlüsselung ab Werk nur begrenzte Möglichkeiten. Vor allem Geräte mit Windows Phone 7 lassen sich nicht verschlüsseln, auch nicht über Zusatz-Apps. Bei den anderen Systemen wie iPhone, iPad oder Android sind aktuell die Verschlüsselungstechnologien nur sehr eingeschränkt nutzbar. Sie benötigen in allen Fällen Zusatz-Apps, die teilweise aber auch kostenlos zur Verfügung stehen. Setzen Sie ein sicheres Kennwort, verschlüsselt iOS mit AES-256-Bit E-Mails und die dazugehörigen Anhänge. Allerdings gilt dies nicht für SMS, Notizen und Kontakte. Mit zusätzlichen Apps wie Cortado oder GoodReader lassen sich weitere Dateien auf dem Endgerät direkt verschlüsseln oder derart geschützt auf einem kostenlosen Online-Speicher ablegen. Nachfolgend haben wir für Sie einige Wege der Verschlüsselung von Daten auf Smartphones zusammengefasst.

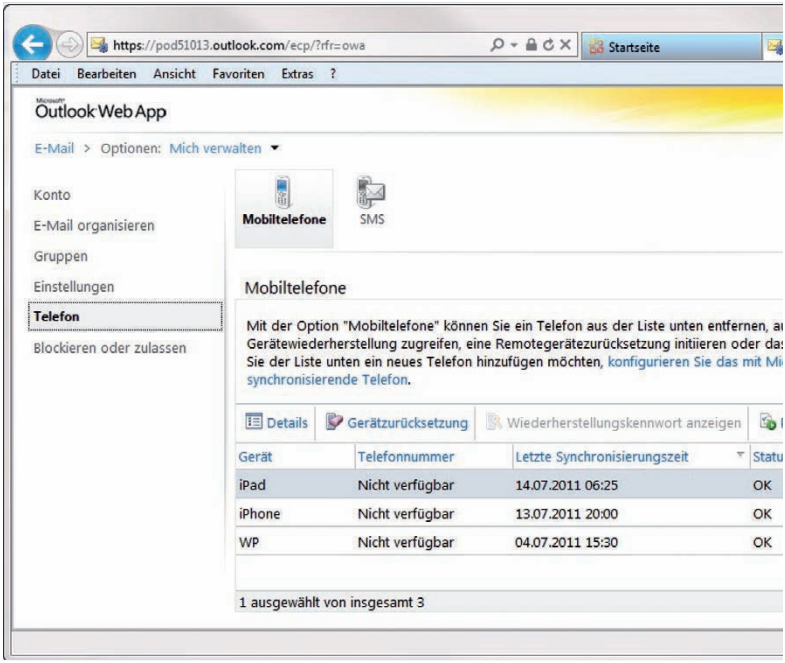
2.9.1 iPhones/iPads fernlöschen (Remote Wipe)

Wenn Sie die Fernlöschung von iPhones/iPads aktivieren, zum Beispiel über Exchange oder MobileME, müssen die Geräte nicht alle Daten löschen und mit Nullen überschreiben, sondern sie löschen einfach den Schlüssel für die Verschlüsselung. Auf diese Weise sind gespeicherte Daten auf dem Endgerät noch gespeichert, aber nicht mehr nutz- oder wiederherstellbar.

Intern verwenden iPhones/iPads eine 256-Bit-AES-Verschlüsselung. Mit entsprechenden Werkzeugen lässt sich die interne Verschlüsselung in iPhones und iPads in wenigen Minuten knacken, wenn Sie nur ein unsicheres Kennwort mit vier Stellen verwenden. Gehen iPhones/iPads verloren oder werden gestohlen, kann der Finder auf die Daten des Endgeräts zugreifen, wenn er den Code für den Zugriff kennt. Hat der Anwender keinen Code gesetzt, ist das iPhone/iPad vollkommen ungeschützt, ganz egal ob Daten verschlüsselt sind oder nicht. Verwenden Anwender statt eines komplexen Codes den einfachen Code mit vier Stellen, lässt sich dieser durch spezielle Tools in sehr kurzer Zeit auslesen.

Um solche Zugriffe auf das eigene iPhone zu verhindern, können Sie zum Beispiel ein komplexeres Kennwort in den Einstellungen festlegen. Das lässt sich nicht so einfach auslesen wie der vierstellige Code. Dies gilt natürlich prinzipiell auch für alle anderen Smartphones. Liegen wichtige Daten oder Zugangsinformationen auf

dem Gerät, sollten Anwender auf jeden Fall mit möglichst komplexen Kennwörtern arbeiten. Allerdings bietet derzeit leider kein Smartphone-Hersteller eine weiterführende Sicherheitsoption oder die Verschlüsselung von Dateien an. Hier gibt es aber Zusatz-Apps, die zum größten Teil die notwendigen Anforderungen erfüllen und dazu noch kostenlos sind.



Sicherheit: Smartphones lassen sich beispielsweise über Outlook Web App löschen.

2.9.2 Cortado – Dokumente auf iPhone und iPad per App verschlüsseln

Mit der kostenlosen App Cortado, die für iPhone und iPad zur Verfügung steht (http://itunes.apple.com/de/app/cortado-workplace/id318124129), können Anwender Dokumente direkt auf dem Gerät verschlüsseln und in einem sicheren Verschlüsselungs-Container auf dem Gerät speichern. Die App steht auf für BlackBerry, Symbian und Android zur Verfügung.

Daten speichert die App aber nicht nur auf dem Smartphone, sondern auch auf einem Server im Internet, direkt beim Anbieter. Bis zu 2 GByte ist die Verwendung kostenlos; benötigen Sie mehr Speicher, können Sie diesen dazubuchen.

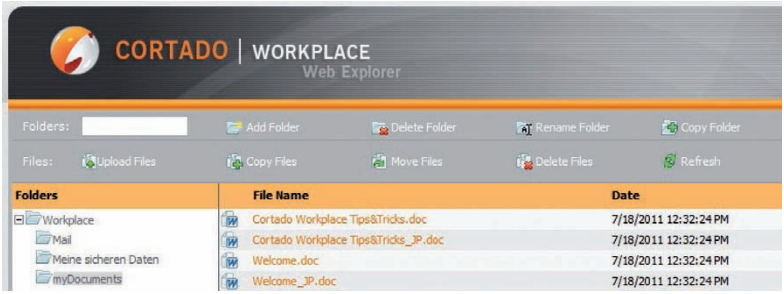
Smartphone-Sicherheit: Der Zugriff auf die Daten kann per App erfolgen.

Für größere Unternehmen bietet der Hersteller auch eine Enterprise-Lösung an. Bei diesem Cortado Corporate Server (www.cortado.com) speichern die Anwender ihre Daten auf einem Server und können mit jedem unterstützten Endgerät auf die Daten des Unternehmensnetzwerks zugreifen. Unterstützt werden neben iOS-Geräten auch BlackBerry, Symbian und Android. Anwender können auch über ihre Desktop-PCs auf die verschlüsselten Daten zugreifen.

Bereits die kostenlose Einzelplatzlösung bietet aber schon eine recht gute Sicherheit und ermöglicht zusätzlich noch das Ausdrucken von Dokumenten auf Netzwerkdruckern. Dazu muss der Drucker nicht AirPrint-fähig sein, sondern Sie können jeden Netzwerkdrucker anbinden. Um Cortado zu nutzen, installieren Sie die kostenlose App über den Market oder den App Store. Beim ersten Start müssen Sie eine E-Mail-Adresse eingeben. Zu dieser sendet der Dienst ein Anmeldekennwort. Dieses müssen Sie beim ersten Aufrufen ändern, zum Beispiel wenn Sie über einen Browser auf Ihre Daten zugreifen.

2.9.3 Cortado-App im Einsatz

Wenn Sie per Browser auf Ihre Daten zugreifen wollen, verwenden Sie dazu den Link http://www.cortado.com/myworkplace. Mit dem Konto können Sie die App auch auf anderen Endgeräten nutzen. Der Nachteil bei dieser App ist, dass die Anwender selbst auswählen müssen, welche einzelnen Dateien sie verschlüsseln wollen. Alle anderen Dateien sind also weiterhin ungeschützt. Die Verschlüsselung lässt sich leider weder automatisieren noch über Richtlinien vorgeben.



Myworkplace: So können Sie auf die Daten im Cortado-Online-Speicher zugreifen.

Mit dem GoodReader lassen sich Dateien schneller und umfassender verschlüsseln. Allerdings kostet dieser Geld und bietet nicht so komfortable Möglichkeiten zum Datenaustausch. Über die erwähnte Internetadresse zum eigenen Cortado-Konto können Sie auch von jedem PC aus auf Ihren Online-Speicher zugreifen und Daten hochladen oder speichern. Um auf dem iPhone/iPad die Daten zu synchronisieren, öffnen Sie Cortado, melden sich an und klicken dann auf Workplace.

Datenabgleich: Die Daten der Cortado-App lassen sich mit dem Online-Speicher synchronisieren.

Über das Werkzeugkastensymbol im unteren rechten Bereich können Sie die App mit dem Inhalt des Online-Speichers synchronisieren. Klicken Sie eine Datei an, öffnet sich diese, und Sie können den Inhalt betrachten oder bearbeiten. Das lässt sich ganz leicht bewerkstelligen und erfordert auch keine komplexe Einarbeitung.

Drucken: Über Cortado können Sie Dateien auch ausdrucken.

Über den Werkzeugkasten können Sie per Druckersymbol auch Dokumente ausdrucken. Sind Sie via iPhone/iPad mit dem WLAN verbunden, in dem sich auch der Drucker befindet, erkennt das Endgerät swn Drucker und ermöglicht eine Verbindung. Unterstützt die App den Drucker, können Sie problemlos synchronisierte Dokumente über Cortado ausdrucken.

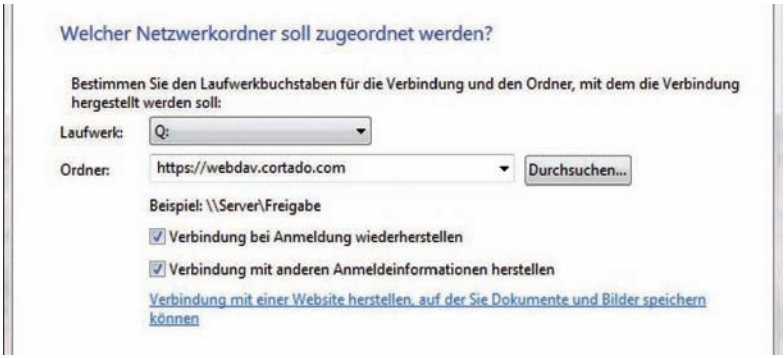
2.9.4 Container als Netzlaufwerk einbinden und Daten sicher austauschen

Beim Zugriff auf sensible Daten auf Smartphones liegen die Dateien in den meisten Fällen zusätzlich entweder auf dem heimischen PC oder auf einem Netzlaufwerk im Unternehmen. Dass Sie Dateien, die Sie häufig benötigen, schnell, einfach und vor allem auch sicher zwischen iPhone/iPad und dem entsprechenden Computer synchronisieren können, ermöglicht ebenfalls Cortado. Sie können entweder Dateien, wie oben beschrieben, über das Web-Frontend hochladen und anschließend über die Cortado-App auf die Daten zugreifen. Dazu rufen Sie Workplace in der App auf und lassen über den Werkzeugkasten die Daten synchronisieren. Um schneller Daten auszutauschen, können Sie Ihr Cortado-Laufwerk aber auch als normales Netzlaufwerk auf Ihrem Computer einbinden. Der Verbindungsaufbau findet dazu mit WebDAV (Web-based Distributed Authoring and Versioning) statt:

1. Klicken Sie mit der rechten Maustaste auf *Computer*.
2. Wählen Sie *Netzlaufwerk verbinden*.
3. Wählen Sie den Laufwerksbuchstaben aus, den Sie verwenden wollen.
4. Geben Sie als Adresse für den Ordner die Adresse *https://webdav.cortado.com* ein.
5. Aktivieren Sie die Option *Verbindung mit anderen Anmeldeinformationen herstellen*.

6. Geben Sie im neuen Fenster Ihre Anmeldedaten für Cortado ein.
7. Anschließend verbindet Windows das Netzlaufwerk. Sie können jetzt Daten in dieses Laufwerk kopieren und die Daten genauso verwalten wie Daten auf herkömmlichen Laufwerken.

Sie können nach dem erfolgreichen Verbinden über den Windows-Explorer einfach Dateien in den Online-Speicher kopieren. Die Dateien sind dann sofort auf dem entsprechenden Endgerät verfügbar, ohne dass Sie eine komplexe Synchronisierung starten müssen.



Praktisch: Sie können den Cortado-Online-Speicher als Netzlaufwerk verbinden.

Der Verbindungsaufbau über WebDAV erfolgt durch den Dienst *WebClient Service*. Dieser ist in der Regel in Windows XP, Windows Vista und Windows 7 enthalten, aber in Windows Server 2008 und Windows Server 2008 R2 nicht installiert. Aus diesem Grund können Sie auf Servern standardmäßig nicht mit WebDAV arbeiten. Sie haben aber die Möglichkeit, über den Servermanager das Feature *Desktopdarstellung* zu installieren. Dieses enthält auch den WebClient-Service. Sollte auch nach der Installation des Features der Verbindungsaufbau nicht funktionieren, starten Sie den Systemdienst WebClient neu. Der Verbindungsaufbau mit WebDAV ist in manchen Umgebungen langsam. Meistens lässt sich das Problem beheben, indem Sie die Option *Automatische Suche der Einstellungen* im Internet Explorer deaktivieren. Sie finden diese Einstellung in den *Internetoptionen* auf der Registerkarte *Verbindungen* über die Schaltfläche *LAN-Einstellungen*.

2.9.5 Lokale Dateien auf iPhone/iPad sicher speichern

Notizen und Bilder, die Sie auf dem iPhone/iPad speichern, sind zwar von der Grundverschlüsselung des Geräts geschützt. Sobald ein Anwender jedoch Zugriff auf das Gerät hat und das Kennwort kennt, kann er auf diese Daten zugreifen. Wollen Sie Bilder, die Sie mit der Kamera des iPhones/iPads machen, sicher able-

gen, können Sie das mit Bordmitteln in iOS nicht tun. Hier hilft aber die App CameraSafe (http://itunes.apple.com/de/app/camerasafe/id314324287). Ihre Notizen wiederum können Sie mit der App Codebook (http://itunes.apple.com/de/app/codebook-secure-notebook/id361921889) sicher verschlüsselt ablegen. Die beiden Apps verschlüsseln die Daten lokal auf dem Endgerät, nicht über einen Online-Speicher, wie zum Beispiel Cortado oder Dropbox. Mit CameraSafe können Sie die Daten vom iPhone/iPad SSL-verschlüsselt auf den PC übertragen.

Zusammenspiel: Per USB-Disk-App übertragen Sie verschlüsselte Daten auf das iPhone.

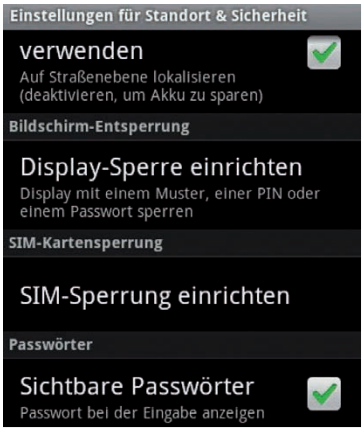
Wollen Sie Daten mit Standard-Tools wie Truecrypt (www.truecrypt.org) verschlüsseln, bleibt Ihnen nur der Weg über einen herkömmlichen PC, auf dem Sie die entsprechende Anwendung installieren. Nutzen Sie das iPhone/iPad als USB-Stick, zum Beispiel mit der kostenlosen App USB Disk (http://itunes.apple.com/de/app/usb-disk/id370531520), können Sie den Container, den Truecrypt erstellt, also das verschlüsselte Image, einfach mit iTunes auf das iPhone übertragen. Haben Sie USB Disk installiert, übertragen Sie beliebige Dateien, egal ob sie verschlüsselt vorliegen oder nicht, auf folgendem Weg:

1. Verbinden Sie das iPhone mit dem PC.
2. Öffnen Sie iTunes.
3. Klicken Sie bei *Geräte* auf das iPhone.
4. Klicken Sie auf *Apps*.
5. Klicken Sie bei Apps auf die App *USB Disk*.
6. Klicken Sie auf *Hinzufügen*.

7. Wählen Sie die Datei aus, die Sie auf das iPhone übertragen wollen. Wenn Sie mit Truecrypt arbeiten, kopieren Sie den verschlüsselten Truecrypt-Container der Datei.

2.9.6 Verschlüsselung mit Android

Neben dem bereits erwähnten Cortado Workplace gibt es für Android-Geräte weitere Apps, die bei der Verschlüsselung von Daten helfen.



Grundschutz: Konfigurieren Sie zunächst die Gerätesicherheit in Android entsprechend.

Allerdings gilt für Android-Geräte das Gleiche wie für iPhones/iPads in Sachen Basissicherheit: Für eine optimale Sicherheit müssen Anwender die Codesperre aktivieren. Viele Einstellungen finden Sie dazu in den Einstellungen im Bereich *Standort und Sicherheit*. Über den Menüpunkt *Display-Sperre einrichten* legen Sie zum Beispiel fest, dass das Android erst wieder den Homescreen anzeigt, wenn Sie eine PIN oder ein Kennwort eingegeben oder eine Geste gezeichnet haben.

Wählen Sie die Entsperrung über eine Geste aus, müssen Sie mindestens vier von neun Punkten auf dem Bildschirm angeben, die zum Entsperren notwendig sind. Verbindungen sind senkrecht, waagerecht oder diagonal möglich. Sie dürfen jeden Punkt nur einmal nutzen. Sie müssen zum Entsperren das Muster nur auf dem Display malen, keine Tasten drücken.

Über *SIM-Sperrung* einrichten legen Sie fest, dass Anwender beim Starten des Telefons die PIN eingeben müssen, die auf der SIM-Karte hinterlegt ist. Diese PIN hat allerdings nichts mit der PIN zu tun, die Sie zum Entsperren des Endgeräts eingeben. Die PIN auf der SIM-Karte ist auf der Karte hinterlegt, die PIN zum Entsperren im Gerätespeicher. Sperrt sich das Gerät nach einiger Zeit, müssen Sie die PIN eingeben, die Sie bei *Display-Sperre einrichten* vorgegeben haben.

Wahlweise: Sie können Android-Geräte über Gesten entsperren.

2.9.7 Apps für Android

Mit der Anwendung Kryptos können Sie zum Beispiel den Datenfluss von Telefonaten verschlüsseln, sodass Unberechtigte keine Gespräche mithören können. Allerdings funktioniert die App nur, wenn beide Gesprächsteilnehmer sie installiert haben und nutzen. Mit der App können Anwender normal über das Telefonnetz reden, aber auch über WLAN. Die App ist zwar generell kostenlos, allerdings fällt für die Teilnahme eine Servicegebühr von 10 US-Dollar im Monat an.

Sicherheits-Tool: Mit DroidCrypt können Sie Ihre Daten auf Android-Geräten verschlüsseln.

Um herkömmliche Dateien auf dem Android-Gerät zu verschlüsseln helfen Apps wie DroidCrypt. Die App steht als Testversion kostenlos zur Verfügung. Die Vollversion kostet 1,99 Euro. Mit der App können Sie sehr leicht Ordner und Dateien verschlüsseln.

Sie haben mit DroidCrypt die Möglichkeit, Dateien, die Sie auf dem Android-Gerät löschen, zu schreddern, sodass sich die Daten nicht mehr wiederherstellen lassen. Die Bedienung des Tools ist recht einfach. Sie können mit DroidCrypt schnell und problemlos Dokumente, aber auch Bilder, Musik und Videos verschlüsseln. Das Tool kann alle Arten von Dateien auf diese Weise sichern. Sie lassen sich weiterhin ganz normal verwenden. Wer Daten auf Android-Geräten verschlüsseln will, findet derzeit keine günstigere Software mit vergleichbaren Funktionen. Mit dem Tool schützen Sie auch Daten auf der angebundenen SD-Karte.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

TecChannel-Links zum Thema	Webcode	Compact
Smartphone- und Tablet-Sicherheit: Daten richtig verschlüsseln	2036785	S.81
Smartphones: Malware-Gefahr wächst	2036827	S.36
Angriffsziel Tablets: Die Attacken kommen	2035208	S.39
Smartphones und Tablets sicher im Unternehmen einsetzen	2035129	S.43
Private Smartphones und Tablets sicher einbinden	2035485	S.47
Sicherheitsrisiken von Smartphones und Tablets minimieren	2035249	S.50
Mobile Geräte wirkungsvoll gegen Missbrauch absichern	2034906	S.55
Verwalten, Sichern, Sperren: Notfallplan für verlorene Smartphones	2035516	S.65
Juniper Pulse Mobile Security für Smartphones	2036370	S.74
Sicherheitsratgeber: Smartphones fernlöschen, orten und sperren	2036926	S.91
Empfehlenswerte Security-Apps für Android	2034879	S.99
Test: Sicherheitslösungen für Smartphones	2035250	S.104

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

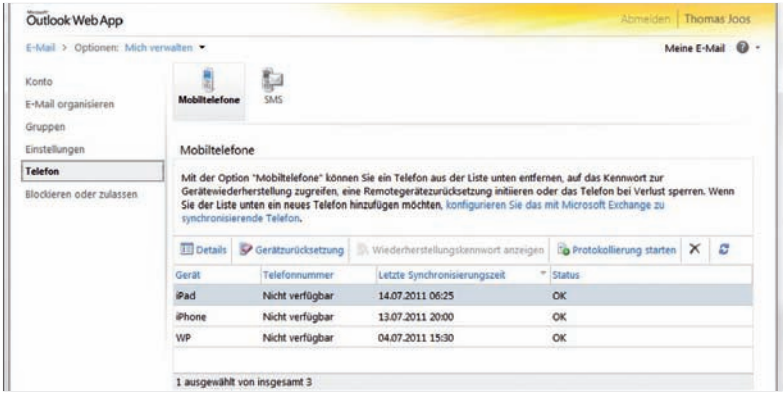
2.10 Sicherheitsratgeber: Smartphones fernlöschen, orten und sperren

Was einst nur für die Notebooks eines Unternehmens galt, lässt sich problemlos auf Smartphones übertragen: Ein verloren gegangenes oder sogar gestohlenes Gerät ist ein Sicherheitsrisiko. Daher ist es sinnvoll, Mittel einzusetzen, um das Smartphone wiederzufinden oder zumindest alle Daten vom Gerät remote löschen zu können. Wir haben nachfolgend einige Vorgehensweisen und Apps für verschiedene Smartphone-Plattformen zusammengestellt. Die Liste erhebt selbstverständlich keinen Anspruch auf Vollständigkeit. Abseits der beschriebenen Lösungen empfiehlt es sich in jedem Fall, sich auch beim Gerätehersteller nach entsprechenden Lösungen umzusehen. Viele Anbieter wie Samsung oder HTC stellen eigene Programme zur Verfügung, um Smartphones wiederzufinden.

2.10.1 Fernlöschen mit Exchange

Setzen Unternehmen Exchange ein, lassen sich angebundene Smartphones durch Administratoren oder von den Anwendern selbst löschen. Systemverwalter nehmen diese Funktion über das Kontextmenü des Empfängers in der Exchange-Verwaltungskonsole oder mit Outlook Web App vor. Hier sind alle angebundenen Geräte verfügbar und lassen sich auch löschen.

Anwender verwenden dazu direkt Outlook Web App. Sobald Sie an OWA angemeldet sind, rufen Sie über den Menüpunkt rechts die Einstellungen Ihres Postfachs auf. Sie erreichen die Verwaltung Ihres Telefons über *Telefon\Mobiltelefone\<Name des Gerätes>*. Über die Schaltfläche *Geräterücksetzung* löschen Sie das Endgerät, sobald es sich das nächste Mal mit dem Exchange-Server verbindet.

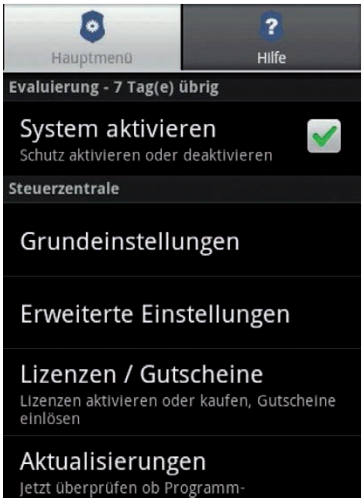


Simpel: Per Exchange angebundene Smartphones kann man per Outlook-Web-App löschen.

Diese Einstellungen stehen auch in den meisten gehosteten Exchange-Lösungen zur Verfügung, zum Beispiel ebenfalls in Office 365. Die Möglichkeit zum Fernlöschen haben Sie nicht nur mit iOS-Geräten, sondern auch mit Android ab Version 2.2, in Windows Phone 7 und den meisten anderen Smartphones, die Exchange ActiveSync unterstützen. Darauf sollten auch Anwender achten, die ihr Privat-Smartphone mit dem Unternehmens-Exchange-Server verbinden. Jeder Exchange-Administrator darf kommentarlos und ohne Genehmigung des Anwenders jedes Smartphone mit allen Daten löschen.

2.10.2 Apps für Android

Android bietet im Market verschiedene Anti-Theft-Lösungen an. Eine der bekanntesten Apps für den Diebstahlschutz von Android-Geräten ist Theft Aware. Nach Installation der App, die als Testversion auch über einen begrenzten Zeitraum kostenlos zur Verfügung steht, können Sie das Telefon entweder laut aufheulen lassen oder alle Daten löschen. Die Einrichtung ist schnell abgeschlossen.



Konfiguration: Sie können in Theft Aware verschiedene Einstellungen vornehmen.

Ist die App installiert und eingerichtet, kann man sie auf dem Gerät nicht mehr sehen, sodass ein Dieb den Diebstahlschutz nicht so einfach beenden kann. Sie können auswählen, welchen Sound Sie abspielen lassen wollen, wenn das Gerät nicht mehr auffindbar ist, und auch alle anderen Einstellungen selbst festlegen.

Die Software lässt sich per SMS auslösen, indem Sie eine Kurznachricht an Ihr verloren gegangenes Gerät senden, oder Sie verwenden ein Web-Interface, um das Gerät zu orten, zu sperren oder zu löschen.

Heulboje: Auf Wunsch spielt das Smartphone einen Sirenenton ab.

Mit der App Plan b haben Sie die Möglichkeit, eine Anwendung auf das Android-Gerät zu pushen, wenn dieses verloren oder gestohlen wurde. Die Installation erfolgt über den PC. Der Nachteil dieser Lösung ist allerdings, dass die Installation sichtbar abläuft und ein potenzieller Dieb die Installation abbrechen kann. Die Lösung hat also nur dann noch einen Wert, wenn Sie keine andere Möglichkeit mehr haben, auf das Gerät zuzugreifen.

2.10.3 MobileMe und iCloud

Mit dem Apple-Dienst MobileMe können Anwender ebenfalls ihr Handy orten und notfalls auf dem Gerät einen Sound abspielen lassen. Mit MobileMe können Anwender iPhones/iPads remote löschen, auch ohne Exchange ActiveSync zu nutzen. Zusätzlich lassen sich ein iPhone/iPad über die Software orten und Nachrichten senden oder ein sehr lauter Ton abspielen, sodass Sie das iPhone/iPad schneller finden. Sie müssen nur das Konto auf dem iPhone einrichten und die Funktion zur Suche des iPhones aktivieren. Apple stellt den Dienst kostenlos zur Verfügung.

MobileMe: So richten Sie ein MobileMe-Konto ein.

Mit iOS 5 stellt Apple den Dienst MobileMe ein und überführt alle Funktionen in den neuen Dienst iCloud. Anwender, die auf iOS 5 setzen, können nach Veröffentlichung der neuen Version die MobileMe-Funktionen kostenlos in iCloud nutzen. Wer aktuell schon MobileMe-Nutzer ist, kann den Dienst weiterhin nutzen, allerdings nimmt der Dienst keine neuen Abonnenten mehr an. Haben Sie einen Account, fügen Sie über *Einstellungen\E-Mail, Kontakte, Kalender\Account hinzufügen* einen neuen MobileMe Account hinzu, genauso wie einen neuen E-Mail-Account.

Im unteren Bereich müssen Sie außerdem manuell die Funktion iPhone suchen aktivieren, wenn Sie Ihr verloren gegangenes iPhones suchen wollen. Haben Sie diese Funktion aktiviert, können Sie über die MobileMe-Website (www.apple.com/de/mobileme/) die Suche starten. Sie sehen den Standort über eine Google-Maps-Seite. Wenn Sie auf Ihr iPhone in der Karte klicken, können Sie es mit einem Mausklick sperren oder löschen oder eine Nachricht auf dem Gerät anzeigen.

Ortung: Das gesuchte iPhone ist gefunden und Sie können es sperren oder löschen lassen.

Die Nachricht erscheint sofort auf dem Display. Zusätzlich ertönt ein sehr lauter Ton, damit Sie hören, wo sich Ihr iPhone genau befindet, falls Sie in der Nähe sind. Wollen Sie auf Nummer sicher gehen, können Sie durch einen Klick das iPhone ohne weitere Meldungen löschen lassen. In diesem Fall sind auf dem Gerät keinerlei Benutzerdaten mehr verfügbar. Diese Sicherheitsfunktion ist natürlich nur dann sinnvoll, wenn das iPhone angeschaltet und mit dem Internet verbunden ist; das gilt aber für alle Apps dieser Art.

2.10.4 Windows Mobile, Android und Symbian – kostenloser Diebstahlschutz von F-Secure

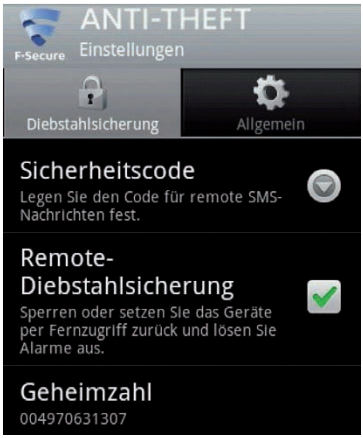
Anwender mit Windows Mobile 5 und 6 sowie Besitzer von Android-Geräten oder Symbian-Smartphones können auch die kostenlose Anwendung Anti-Theft for Mobile von F-Secure einsetzen. Das Tool unterstützt ebenfalls Symbian-Geräte, al-

lerdings kein Windows Phone 7 und kein iOS. Sie können mit der Anwendung verlorene Smartphones dieser Systeme sperren oder alle Daten löschen lassen.

Um die App zu installieren, gehen Sie in Android folgendermaßen vor:

1. Öffnen Sie den Browser.
2. Rufen Sie die Website http://f-secure.mobi auf.
3. Klicken Sie auf Download Anti-Theft
4. Laden Sie die Software herunter.
5. Rufen Sie mit einem Dateimanager den Inhalt der SD-Karte auf und klicken Sie die Installationsdate an, um die App zu installieren.
6. Folgen Sie den Anweisungen der App.
7. Rufen Sie die App auf und starten Sie den Einrichtungsassistenten. Dieser erfordert eine Internetverbindung.

Einstellungen: So richten Sie Anti-Theft auf dem Smartphone ein.



Haben Sie die Einrichtung abgeschlossen, steht der Dienst zur Verfügung. Sie können mit dieser App Ihr Smartphone orten, wenn es nicht mehr auffindbar ist. Auch das Sperren ist möglich, ebenso natürlich die Fernlöschung. Die einzelnen Befehle laden Sie per SMS auf das Mobiltelefon. Dazu stehen verschiedene Befehle zur Verfügung. Wie Sie dabei vorgehen, zeigt F-Secure auf seiner Webseite.

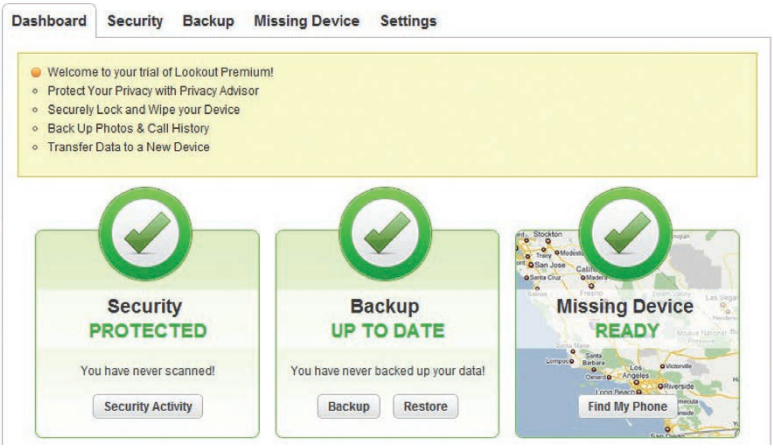
2.10.5 Lookout für Android, BlackBerry und Windows Mobile

Eine weitere kostenlose Lösung ist Lookout. Diese unterstützt Android und BlackBerry sowie das mittlerweile veraltete Windows Mobile. Mit dem kostenlosen Dienst können Sie über ein Google-Mail-Konto ebenfalls verlorene Geräte orten

und finden sowie löschen lassen. Zusätzlich bietet die Anwendung einen Virenschutz und eine Datensicherungsmöglichkeit.

Komplettpaket: Lookout ist Diebstahlschutz, Datensicherung und Virenschutz in einem.

Nach der Installation der kostenlosen App haben Ihnen die verschiedenen Möglichkeiten offen, also Ortung, Fernlöschen, der Signalton und die Sperrung des Gerätes. Ein Vorteil der Anwendung ist, dass Sie mit einem Dashboard mehrere Geräte auf einmal verwalten können. Dazu müssen Sie sich lediglich im Web-Interface (www.mylookout.com) anmelden.



Lookout: So sieht es aus, wenn man Android-Geräte über die Weboberfläche verwaltet.

Sie können das Konto auch mit Premium-Features erweitern (www.mylookout.com/premium). In diesem Fall können Sie kostenpflichtig weitere Dienste nutzen. Die kostenlosen Features dürften für viele Anwender aber vollkommen ausreichen. Vor allem wegen des integrierten Virenschutzes und des Schutzes vor Phishing ist diese kostenlose App durchaus empfehlenswert.

2.10.6 BlackBerry Protect

Anwender von BlackBerry-Geräten können auf den kostenlosen Schutz von BlackBerry Protect (https://appworld.blackberry.com/webstore/content/20844) setzen.

Schutzmann: Mit BlackBerry Protect sichern Sie Ihr Smartphone ab.

Installieren Sie die App auf dem BlackBerry. Anschließend können Sie auch über das Web-Interface von BlackBerry auf die Funktionen der App zugreifen. Hier bietet BlackBerry Protect die gleichen Funktionen wie MobileMe von Apple und die anderen Anti-Diebstahl-Apps.

Sie können über das Web-Interface das Gerät orten, einen Ton abspielen lassen oder es löschen beziehungsweise sperren. Der Vorteil dieser App ist, dass Sie die Daten auf dem Gerät auch sichern können. Für Anwender von BlackBerry-Geräten ist diese kostenlose und einfach zu bedienende App so gut wie Pflicht.

2.10.7 Diebstahlschutz mit Windows Phone 7

Anwender, die Windows Phone 7 nutzen, sollten sich eine kostenlose Windows Live ID zulegen. Sobald Sie sich am Windows-Phone-7-Gerät mit einer Windows-Live-ID angemeldet haben, erweitert sich Ihr Live-Konto mit Mobile-Funktionen. Auf diesem Weg können Sie Ihr Gerät anrufen, sperren oder lokalisieren. Den Dienst stellt Microsoft kostenlos zur Verfügung. Sie sehen auf der Live-Seite im In-

ternet Ihr Telefon, und in der Weboberfläche stehen alle Funktionen zur Verfügung, die bei anderen Systemen nur über eine App integrierbar sind.

Kontaktaufnahme: Windows-Phone-7-Geräte können Sie über Windows Live verwalten.

Sie müssen für diese Funktionen in Windows Phone 7 keine App installieren, sondern beim Einrichten des Telefons lediglich ein Live-Konto hinterlegen. Alle Funktionen stehen dann direkt in Ihrem Windows-Live-Konto zur Verfügung, ohne dass Sie irgendetwas einrichten oder installieren müssen. Aus diesem Grund ist dies für jeden zu empfehlen, der ein Windows-Phone-7-Gerät sein Eigen nennt.

2.10.8 Fazit

Kommt ein Smartphone – wie auch immer – abhanden, ist der Ärger groß, und die Probleme, die daraus entstehen, können sehr komplex werden – genauso gut hätte man seinen Desktop-Firmen-PC mit allen Zugängen und Kontaktdaten in fremde Hände geben können. Ist das Gerät „nur" verloren gegangen, entsteht im besten Fall kein größerer Schaden. Problematischer wird es beim Diebstahl. Für alle Plattformen, von iPhone und iPad über Android und Symbian bis hin zu Windows Phone 7 und BlackBerry, stehen ausreichend – auch kostenlose – Sicherheitslösungen zur Verfügung. Mit ihnen lassen sich Smartphones im besten Fall wiederfinden oder zumindest die Daten darauf aus der Ferne löschen.

Wichtig ist nur, dass Sie vor dem Verlust an das Einrichten denken und den Vorgang auch testen beziehungsweise dokumentieren. So sind Sie für den Ernstfall gewappnet und können Ihr Gerät suchen lassen, im Notfall sperren und, wenn es hart auf hart kommt, sogar löschen. Unternehmen, die Smartphones mit Exchange über Exchange ActiveSync verbinden, haben den Vorteil, dass das Löschen schnell und einfach über Outlook Web App vonstattengeht. Allerdings lässt sich über diesen Weg kein Smartphone orten.

Thomas Joos

2.11 Empfehlenswerte Security-Apps für Android

In einer Zeit, in der Anwender verstärkt E-Mails, Kontakte und andere persönliche Daten auf dem Smartphone anhäufen, gibt das Mobiltelefon ein hervorragendes Ziel für Datendiebe ab. Spätestens seit den letzten Angriffen auf Anwender mit dem Mobilbetriebssystem Android, bei denen infektiöse Apps im Market verbreitet wurden, ist klar, dass Mobile Malware im Kommen ist. Es handelt sich um einen der Security-Brennpunkte im Jahr 2011, mit dem sich User auseinandersetzen müssen. Das bestätigt auch die den Kaspersky Labs angehörige Internetseite Securelist. In einem aktuellen Report zum Thema Mobile Malware (www.securelist.com/en/analysis/204792168/Mobile_Malware_Evolution_An_Overview_Part_4) stellen die Sicherheitsexperten die wachsende Bedrohung durch Schadsoftware für Mobiltelefone heraus.

Das Resümee: Die rasant wachsende Verbreitung von Smartphones – und nicht zuletzt auch Tablets – mit dem mobilen Betriebssystem Android macht die Plattform immer interessanter für Malware-Entwickler. Neben den Schadprogrammen existieren noch weitere Schauplätze in Sachen Smartphone-Sicherheit – beispielsweise Backup & Restore, Zugangskontrolle sowie das richtige Vorgehen bei Diebstahl oder Verlust eines Smartphones. Lesen Sie hier Informationen zu einigen Security-Apps, mit denen Sie die Smartphone-Sicherheit verbessern können.

2.11.1 Security-Suiten für Android

Zwei bis dato kostenlose Security-Suiten für Android sind Lookout Mobile Security und Norton Mobile Security (Beta). NetQin Antivirus Free wurde zwischenzeitlich eingestellt. Nur noch die Version mit kostenpflichtigem Abo-Modell ist im Market zu finden. Alle drei Anwendungen versprechen den Schutz vor Malware auf dem Smartphone. Konkret sind damit zum Beispiel infizierte Apps aus dem Android Market gemeint, die unbemerkt im Hintergrund IMEI- und IMSI-Nummer, Adressdaten, SMS und Co. übertragen, sobald sie einmal installiert sind.

Hierfür überwachen alle Programme die laufenden Prozesse unter Android, behalten den Hauptspeicher des Smartphones im Blick und führen regelmäßige Scans des Telefonspeichers durch. Aber auch schon beim Download aus dem Market schlägt das Scanner-Modul Alarm. Alle drei Programme besitzen jedoch Funktionen, die über die eines bloßen Malware-Scanners hinausgehen. Die Anwendungen von Lookout und NetQin etwa besitzen eingeschränkte Funktionen für Backup und Restore. Beide Apps erlauben es, Kontaktdaten auf den Servern des Herstellers zwischenzuspeichern und im Falle eines Verlusts wieder auf das Gerät zurückzuspielen. Norton Mobile Security kann eingehende Telefonanrufe sowie SMS von unliebsamen Kontakten filtern – praktisch bei störenden Werbebotschaften. Dabei werden sogar Notifications unterdrückt.

Lookout Mobile Security: Die Software erkennt infizierte Apps und warnt rechtzeitig.

Typische „Find my Phone"-Funktionen sind in alle drei integriert und finden, sperren oder löschen das verlorene Telefon aus der Ferne. Dabei gilt es jedoch zu beachten, dass keines der Programme den Telefon- beziehungsweise SD-Kartenspeicher sicher überschreiben kann. Für gängige Recovery-Tools dürfte die Wiederherstellung der Daten also kein Problem darstellen.

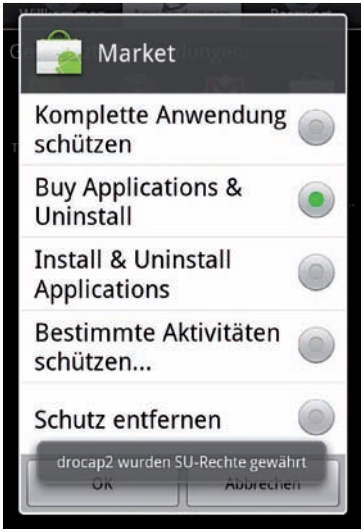
2.11.2 Unbefugten den Zugriff verweigern

Wer sein Smartphone regelmäßig aus der Hand gibt, kennt das ungute Gefühl, eigene SMS, Fotos oder E-Mails den neugierigen Blicken eines anderen auszusetzen. Mit einigen Programmen aus dem Android Market lassen sich jedoch bestimmte Smartphone-Bereiche durch einen PIN-Code schützen.

Einstellungssache: Welche Apps geschützt werden sollen, kann der Anwender selbst bestimmen.

Lock ist eine solche Software. Die App versieht andere Programme mit einem PIN-Code, der erst eingegeben werden muss, bevor sich die verriegelte Anwendung ausführen lässt. Die Einstellungen, SMS/MMS sowie Lock selbst zählen zu den Programmen, die serienmäßig gesperrt werden. Zu den möglichen Optionen gehört auch das Hinzufügen eigener Apps, die in Zukunft PIN-geschützt sein sollen. Auch wenn Lock gewaltsam per Task-Manager beendet wird, ist der Schutz nicht aufgehoben. Im Test ist die App nach Sekunden neu gestartet und hat den Schutz wieder aufgebaut. Die zur Verfügung stehenden Optionen sind ausreichend, zumal Lock kostenlos im Android Market angeboten wird.

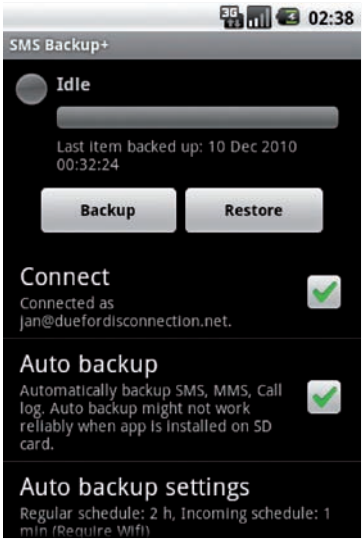
Praktisch: Auch einzelne Funktionen von Apps können gesperrt werden.



Eine Alternative mit mehr Funktionen ist Protector. Genauso wie Lock versieht auch die Protector-App einzelne Programme mit einem PIN-Schutz. Zusätzlich können jedoch auch gezielt Funktionen aus Apps per Geheimzahl gesichert werden. So lässt sich beispielsweise einrichten, dass der Android Market selbst aufgerufen werden kann, jedoch vor dem Kaufen oder Installieren einer App die Geheimnummer eingegeben werden muss. Kompatible Aktionen sind für viele Anwendungen verfügbar. In der kostenlosen Version können bis zu zehn Apps abgesichert werden. Bevor Protector funktioniert, muss das Android-Phone neu gestartet werden. Bei allen Programmen dieser Art gibt es jedoch zu beachten, dass der Schutz immer nur auf dem laufenden System selbst wirkt und sich mit vertretbarem Aufwand umgehen lässt. Wird das Smartphone etwa per USB mit einem PC verbunden, können Bilder und Co. leicht vom Gerät heruntergeladen werden. Und schon das einfache Herausnehmen der Speicherkarte genügt, um Zugriff auf dort gespeicherte private Daten zu erlangen.

2.11.3 Backup und Datenwiederherstellung

Nur wenn das Smartphone ordentlich und in regelmäßigen Abständen gesichert wird, lässt sich ein vollständiger Verlust der Daten verhindern. Hierfür hält der Market viele Anwendungen bereit.



Auto-Datensicherung: In den Optionen wird die automatische Datensicherung aktiviert.

SMS Backup+ ist ein solches Programm. Die quelloffene Software überträgt SMS und MMS zu Google Mail, wo sie unter einem eigenen Label sortiert werden und sich so leicht von normalen E-Mails unterscheiden lassen. Anrufe werden unter Google Kalender zusammengefasst und mitsamt Rufnummer und genauem Zeitpunkt erfasst. Die Wiederherstellung ist im Falle eines Geräteverlustes ebenso möglich. Voraussetzung für die korrekte Funktion der App ist das Aktivieren der IMAP-Funktion bei Google Mail.

Mehr Sicherungspotenzial bietet die Kauf-App Sprite Backup 2.0. Neben den Daten, die auch SMS Backup+ sichert, legt das Programm unter anderem Reservekopien von Systemeinstellungen, Home Screens, App-Einstellungen und vielem mehr an – und zwar bei den Cloud-Speicherdiensten Dropbox und Box.net. Damit die zu übertragende Datenmenge handhabbar bleibt, überlässt Sprite Backup dem Anwender die Auswahl darüber, welche Daten gesichert werden sollen und welche nicht. Backup-Tasks werden über einen Aufgabenplaner automatisiert. Obendrein ist die Software vollständig eingedeutscht.

Ausführlicher mit der Datensicherung in der Praxis beschäftigt sich dieser TecChannel-Artikel „Android – Datensicherung in der Praxis“ (Webcode **2034104**).

2.11.4 Firewall, Passwort-Safe und mehr

Eine Firewall gehört auf dem Desktop-PC quasi zur Grundausstattung, jetzt lässt sich mit DroidWall eine vergleichbare Software für Android installieren. Die App setzt auf die Linux Firewall-Funktion iptables, um Apps zuverlässig vom Netzzugriff auszuschließen. Dafür erfordert DroidWall jedoch einen Root-Zugriff auf das Smartphone – bei vielen Geräten ein Garantieproblem. Praktische Nutzungsmöglichkeiten für die Freeware ergeben sich nicht nur aus Sicherheitsaspekten. Auch bei beschränktem Datenvolumen kann eine abgesicherte Datensperre sinnvoll sein. Seien Sie mal ehrlich: Wie oft beachten Sie ernsthaft die Installationshinweise einer jeden App, die Sie aus dem Android Market laden? Oftmals, wenn nach der Freigabe von Berechtigungen gefragt wird, wird einfach blindlings der OK-Button betätigt – ungeachtet der potenziellen Gefahren. aSpotCat listet alle jemals gewährten Freigaben zu jeder installierten Anwendung auf und bietet ihre schnelle Beseitigung an. So kommen Sie Apps auf die Schliche, die heimlich Premium-SMS verschicken können oder laufend das GPS-Modul des Smartphones beanspruchen – selbst wenn dies kein Geld, sondern nur etwas Akku-Laufzeit kostet.

SecureMemo ist ein einfach gehaltener Datentresor für Zugangsdaten, Passwörter oder Kreditkartennummern unter Android. Die kostenlose App speichert alle Informationen als AES-verschlüsselten Container auf der SD-Speicherkarte und setzt für die Entschlüsselung immer ein valides Passwort voraus.

Eine App ist abgestürzt – was war die Ursache? SendLog hilft hier Entwicklern und interessierten Anwendern gleichermaßen bei der Fehlersuche. Die kostenfreie Android-App verschickt komfortabel Betriebssystem-Logdateien per E-Mail. Auch eine aktuelle Prozessliste mitsamt Speicherauslastung und mehr lässt sich ausgeben. Beim Versand stehen verschiedene Log-Formate zur Auswahl, die die spätere Verwertbarkeit der Informationen beeinflussen können.

Florian Horner

Als Trainee Content-Manager betreut **Florian Horner** unter anderem die TecChannel-Produktdatenbank. Darüber hinaus ist er für den Bereich iPhone bei TecChannel zuständig.

TecChannel-Links zum Thema	Webcode	Compact
Empfehlenswerte Security-Apps für Android	2036785	S.99
Juniper Pulse Mobile Security für Smartphones	2036370	S.74
Smartphone- und Tablet-Sicherheit: Daten richtig verschlüsseln	2034879	S.81
Sicherheitsratgeber: Smartphones fernlöschen, orten und sperren	2036926	S.91
Test: Sicherheitslösungen für Smartphones	2035250	S.104

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

2.12 Test: Sicherheitslösungen für Smartphones

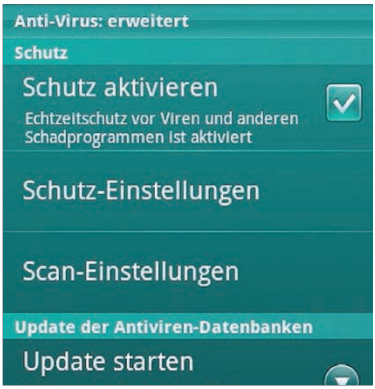
Wer im geschäftlichen oder auch im privaten Bereich einen genaueren Blick auf die „Landschaft“ der Mobiltelefone wirft, wird die Euphorie der Industrie schnell verstehen: Moderne Geräte von Typ Smartphone verbreiten sich rasant. Immer mehr Anwender sind mit ihren Telefonen im Internet unterwegs und dank entsprechend günstiger Tarife auch immer häufiger online – zumeist sogar konstant.

Für IT-Beauftragte und Systemadministratoren sind diese Geräte aber nicht nur ein Grund zur Freude: Sie sehen sich mit den gleichen Problemen konfrontiert, mit denen sie schon bei der ersten Welle der Mobilität durch den Einsatz von Note- und Netbooks aller Art zu kämpfen hatten. So vermischen sich auf den mobilen Geräten immer häufiger die privaten mit den geschäftlichen Daten mit oft kaum zu überwachenden Sicherheitsrisiken. Denn welcher Anwender hat schon auf seinem Smartphone eine entsprechende Sicherheitssoftware im Einsatz? Sogar professionelle Nutzer, die selber im Umfeld der IT tätig sind, vernachlässigen diesen Schutz häufig geradezu sträflich. Das muss aber nicht sein, denn die großen und bekannten Hersteller aus dem Bereich der Security- und Antivirenlösungen sind auch auf diesem Feld vertreten und versprechen, mit ihren Lösungen auch moderne Mobiltelefone vor Angriffen schützen zu können.

2.12.1 Zwei Lösungen für Android im praktischen Einsatz

Zwei Produkte haben wir während eines mehrwöchigen Testzeitraums auf einem HTC Legend unter dem Betriebssystem Android 2.2 (Froyo), das auf den Linux-Kernel 2.6.32 aufsetzt, auf ihre Praxistauglichkeit untersucht.

McAfee: WaveSecure



Kaspersky: Mobile Security 9

Beide Softwarelösungen stammen von Firmen, die im Security-Umfeld bekannt sind: Die Intel-Tochter McAfee (www.mcafee.com) stellt uns mit WaveSecure in der Version 4 eine Lösung zur Verfügung, deren Fokus auf Datensicherung und Wiederherstellung liegt und die dadurch die Anwender und deren Daten vor allen bei einem möglichen Diebstahl oder Verlust schützen soll. Die russische Softwareschmiede Kaspersky (www.kaspersky.com) bleibt ihrer Richtung treu und stellt mit der Mobil Security in der Version 9 ein Paket bereit, das in Funktion und Umfang den bekannten Antivirenlösungen auf den PCs sehr ähnlich ist.

Wie unterscheiden sich die Lösungen? Während sich die Software der russischen Sicherheitsfirma auch auf den Mobiltelefonen im „klassischen Gewand" einer Antivirenlösung mit Ergänzungen für die mobilen Belange präsentiert, hat McAfee die eigene Lösung komplett auf die Sicherung und Wiederherstellung eines Smartphones ausgerichtet.

2.12.2 WaveSecure: Backup und Wiederherstellung im Fokus

Die erste Software unseres Tests bietet keinen Schutz von Viren oder bösartigen Programmen: Ihre Stärken liegen eindeutig in den Bereichen Schutz der persönlichen Daten sowie deren Backup und Wiederherstellung. So definiert Hersteller McAfee sie denn auch als Sicherheitssoftware, die dem Benutzer den Schutz seiner Daten und seiner Privatsphäre beim Diebstahl des Geräts ermöglicht.

Installation des Programms: Die McAfee-Software kann direkt aus dem Android-Markt auf das Telefon gebracht und von dort aus gestartet werden. Dies verlief ohne größere Probleme. Allerdings zeigt der Installationsvorgang, dass der Hersteller hier vor allen Dingen eine Lösung präsentieren will, die vor Diebstahl und Verlust des Gerätes schützen soll.

Die McAfee-Lösung WaveSecure: Sie kann mit dem Telefon direkt von der Webseite des Anbieters heruntergeladen werden und erkennt dabei vielfach bereits das verwendete Endgerät.

Was ist dabei zu beachten? Schon während der ersten Schritte dieses Vorgangs wird der Anwender aufgefordert, eine Mobilfunknummer zur Überprüfung anzugeben. An diese schickt die Lösung dann vom Server aus eine SMS – erst wenn diese Authentifizierung klappt, kann weiterinstalliert werden. Aber damit sind die Hürden noch nicht überwunden: Als Nächstes taucht die Forderung auf dem Bildschirm des Telefons auf, man möge nun die Telefonnummer eines Freundes einge-

ben, der per SMS benachrichtigt werden soll, falls das Telefon gestohlen oder eine andere SIM-Karte eingelegt wird. Erst danach kann eine – hier sechsstellige – PIN-Nummer eingegeben werden, die zum Entsperren der Software auf dem Handy dient. Anschließend ist es mithilfe der Telefonnummer (oder der E-Mail-Adresse) sowie dieser PIN-Nummer möglich, sich auf der Website von WaveSecure einloggen und von dort aus sein Telefon zu verwalten oder zu überwachen.

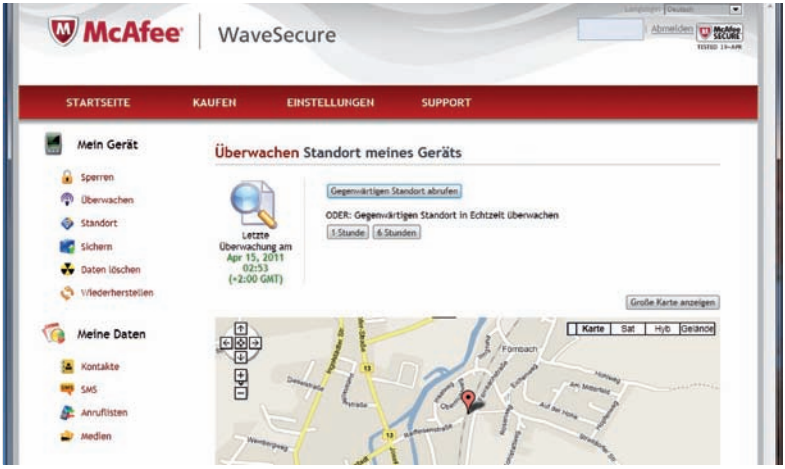
2.12.3 Was kann WaveSecure – und was nicht?

Die Software stellt auf dem Telefon verschiedene Möglichkeiten zur Verfügung, um beispielsweise die Kontakte, aber auch die Anruflisten oder die auf dem Gerät gespeicherten SMS direkt auf den Server bei McAfee zu sichern. Wurde eine solche erste Sicherung eingerichtet, so sichert die Lösung die Daten inkrementell weiter, was in unserem Testszenario auch gut funktionierte. Neben einer manuellen Sicherung kann der Anwender diese auch automatisieren, damit er sich immer sicher sein kann, dass sich auch auf dem Server der aktuelle Stand seiner Daten befindet. Auch Video- und Fotodateien kann die Lösung mit auf den Server übertragen. Von der Website aus kann der Anwender dann die Daten problemlos wieder auf das Gerät zurückspielen.

Geschafft: Nach der Anmeldung auf der WaveSecure-Seite kann das Telefon nicht nur aus der Ferne gesteuert werden, sondern verschiedene Sicherungsaufgaben können auch über die Webseite erledigt werden.

Der Sicherheitsdienst der Software sperrt das Telefon automatisch, sobald eine neue SIM-Karte eingelegt wird. Einem ehrlichen Finder kann dabei auch eine frei konfigurierbare Nachricht gesendet werden, die ihm mitteilt, wie er Kontakt zum rechtmäßigen Besitzer aufnehmen kann. Auch die Lokalisierung des Telefons mittels der Software ist möglich, was bei unseren Tests auch weitgehend erfolgreich verlief. So konnten wir mittels der Website dann direkt den aktuellen Standort des Telefons auf einer eingeblendeten Karte von Google Maps abrufen.

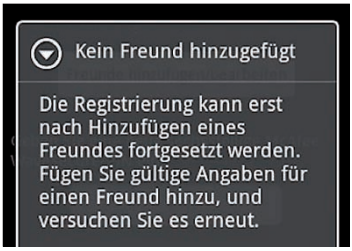
Der Anwender kann direkt von der Website aus auf das Telefon zugreifen und ein Löschen sowohl der persönlichen Daten als auch der Fotos und Videos veranlassen. Das funktionierte im Test auch, wenn es um Daten auf der zusätzlichen SD-Karte des Gerätes ging.



Ein weiterer Baustein für den Schutz vor Diebstahl: Durch einen Remote abgesetzten Befehl kann der Standort des Geräts ermittelt und angezeigt werden.

Was bietet diese Software nicht? Im Gegensatz zu Kaspersky stellt McAfee hier keine Antivirenlösung zur Verfügung – das ist auch nicht das Ziel dieser Lösung. Es enttäuscht ein wenig, dass eine Lösung, die gezielt auf den Schutz vor Diebstahl und Missbrauch der Daten ausgelegt wurde, keine Möglichkeit bietet, Daten durch eine Verschlüsselung zu sichern. Die Idee, die Nummer eines Freundes zu hinterlegen, der beim Einlegen einer anderen SIM-Karte per SMS benachrichtigt wird, ist prinzipiell sicher gut – uns hat allerdings extrem gestört, dass es nicht möglich ist, diesen Schritt zu überspringen: Die Installation wird nicht fortgesetzt, bis diese Nummer eingegeben wird.

Etwas lästig: Die Registrierung verlangt zwingend nach der Angabe eines „Freundes" (es muss eine Telefonnummer sein!) an die im Verlustfall des Telefons eine Nachricht geschickt werden kann.



McAfee WaveSecure	
Unterstütze Smartphone-Betriebssysteme	• Android 1,5 bis 2.3 • BlackBerry 4.2 bis 5.x • Symbian S60 3rd Edition und 5th Edition • Windows Mobile 6.0 bis 6.5
Preis	19,90 US-Dollar für ein Smartphone (Laufzeit ein Jahr)
Plus	• Umfangreiche Backup- und Wiederherstellungs-Funktionen • Remote-Fernsteuerung und -Sicherung über die Website • Auch Video- und Fotodateien können gesichert werden • Lokalisierung des Telefons
Minus	• Kein Schutz vor Schadsoftware und Viren • Keine Verschlüsselung der Daten • Umständliche Prozedur bei der Installation

2.12.4 Die Kaspersky-Lösung: PC-Feeling für das Smartphone

Die Lösung von Kaspersky kann der Anwender sowohl aus dem Android-Market als auch direkt von der Mobile-Security-Website des Herstellers herunterladen. Wer das Programm zunächst einmal nur ausprobieren will, kann dies leider nur für sieben Tage tun.

Installation des Programms: Die Installation ähnelt grundsätzlich dem zuvor geschilderten Vorgang: Auch hier konnten wir das Programm schnell und problemlos auf dem Testgerät installieren. Beim Start des Programms muss der Anwender nach dem üblichen „Abnicken" des Lizenzvertrages das Programm aktivieren, wenn er eine Vollversion des Programms erworben hat.

Genau wie es die Anwender vom PC kennen: Die Datenbank der Antivirus-Lösung kann automatisch aber auch manuell auf den aktuellen Stand gebracht werden.

Hier benimmt sich das Programm, wie man es von Antivirenlösungen auf dem PC kennt: Ein Aktivierungscode, den der Anwender zuvor käuflich erworben hat, wird eingegeben, und das Programm wird aktiviert. Danach ist zwingend die Ein-

gabe eines Geheimcodes erforderlich. Dieser wird grundsätzlich abgefragt, wenn der Anwender auf das Programm zugreifen möchte. Er kommt auch zum Einsatz, wenn mittels Fernzugriff (über SMS-Befehle) bestimmte Sicherheitsfunktionen auf dem Telefon gesteuert werden sollen. Der Code ist eine reine Ziffernfolge, die mindestens vierstellig sein muss.

Was ist dabei zu beachten? Die Software bietet direkt nach der Aktivierung die Möglichkeit, diesen Geheimcode mittels einer E-Mail-Adresse wiederherstellen. Diese Wiederherstellung sollte unbedingt eingerichtet werden, da man einen Geheimcode schnell mal vergessen kann und der Anwender sich so selbst den Zugriff auf die Kaspersky-Lösung verwehrt. Schlussendlich hätte der Verlust zur Folge, dass selbst eine Deinstallation nicht mehr möglich ist.

Zunächst sicher noch etwas ungewohnt: Der Antivirus-Scan auf einem Android-Smartphone untersucht alle Dateien, wozu auch die auf der SD-Karte im Gerät gehören.

Ist das Programm installiert, verhält es sich auf dem mobilen Telefon fast genauso, wie man es vom PC her gewohnt ist. Unsere zunächst bestehende Angst, dass der Einsatz dieser Software die Verarbeitungsgeschwindigkeit des Smartphones deutlich bremsen würde, bestätigte sich zum Glück nicht. Das ist besonders bemerkenswert, da es sich beim HTC Legend um ein bereits „älteres" Modell handelt, das nur mit einem 600-MHz-Prozessor aufwarten kann. Am oberen Rand des Bildschirms weist ein kleines rotes Logo darauf hin, dass die Schutzsoftware aktiv ist, und wer in das Menü der Software wechselt, wird mit dem bekannten „Kaspersky-Grün" begrüßt.

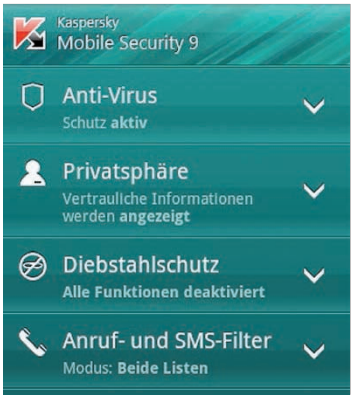
2.12.5 Was kann die Mobile Security 9 – und was nicht?

„Kernkompetenz" der Lösung ist zweifellos der Schutz vor Viren und Bedrohungen aus dem Internet. Deshalb haben wir gleich zu Beginn der Testperiode einen kompletten Scan des Geräts gestartet, das mit einer 8-GByte-SD-Karte ausgerüstet ist. Zu unserem großen Erstaunen, zeigte die Software nach fast einer Stunde, dass sie mehr als 23.000 Dateien auf diesem Telefon gefunden und unter-

sucht habe – wir hätten nie an derartige Dimensionen gedacht. Hier zeigt sich einmal mehr, dass Smartphones in Wirklichkeit Computer im Hosentaschenformat sind. Einsatz und Gebrauch dieser Funktionalität verlaufen auf die gleiche Art und Weise, wie es der Nutzer vom PC her kennt.

Neben dem bekannten Antivirenschutz bietet die Software Funktionen zum Diebstahlschutz, die es dem Anwender unter anderem ermöglichen, das Telefon remote mittels einer vordefinierten SMS zu blockieren.

Sehr gut hat uns die folgende Funktionalität gefallen: Ein Anruf- und SMS-Filter läuft wahlweise im Whitelist-Modus (Anrufe und Nachrichten von bestimmten Kontakten) oder im Blacklist-Modus (alle Anrufe und Nachrichten von allen Nummern werden angenommen, außer von denen auf der Liste). Dabei kann der Anwender entscheiden, ob er diese Funktion komplett ausschalten will oder mit einer sowie mit einer Kombination beider Listen arbeiten möchte. Ist die Verblüffung zunächst groß, wenn bei einem Anruf von einer bisher unbekannten Nummer ein grünes Fenster auftaucht und fragt, wie mit dieser Nummer verfahren werden soll, so lernt der Benutzer diese bequeme Möglichkeit, unliebsame Werbeanrufe und ähnliche Nachricht komfortabel auszublenden, schnell schätzen.



Mehr als nur Antivirus: Neben den Anruffiltern stellt die Software auch einen Schutz von Diebstahl und eine Möglichkeit zur Wahrung der Privatsphäre zur Verfügung.

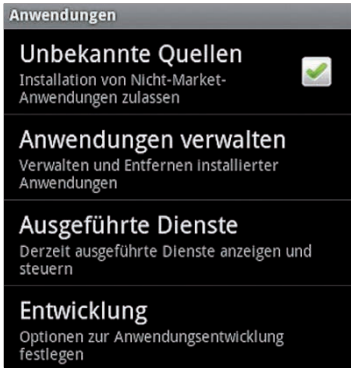
Neben der Antiviren- und der Filterfunktion stellt diese Software auch Features zur Verfügung, mit deren Hilfe der Anwender seine privaten Daten auf dem Telefon verschlüsseln und verbergen kann. Eine Sicherung und Wiederherstellung der Daten, die sich auf dem mobilen Telefon befinden, stellt die Lösung nicht zur Verfügung. Einige Funktionen, die Möglichkeiten anbieten, das Handy aus der Ferne via SMS zu blockieren und die persönlichen Daten zu löschen, fallen sicher auch in den Bereich Schutz vor Diebstahl. Sie sind hier aber nicht so konsequent durchgedacht, wie das beim McAfee-Produkt der Fall ist. Die Verschlüsselung wird zudem leider nicht auf allen Plattformen angeboten; so steht zurzeit für Android und BlackBerry nicht zur Verfügung.

Kaspersky Mobile Security 9	
Unterstütze Smartphone-Betriebssysteme	• Android Version 1.6 bis 2.2 • BlackBerry 4.5 bis 6.0 • Symbian (Nokia) 3 oder Symbian Series 60 9.1, 9.2, 9.3, 9.4 • Windows Mobile 5.6 bis 6.5
Preis	24,95 Euro für ein Smartphone (Laufzeit ein Jahr)
Plus	• Antiviren und Malware-Schutz • Anruf- und SMS-Filter • Verschlüsselung • Diebstahlschutz durch SMS-Befehle • Lokalisierung des Telefons
Minus	• Keine Backup- und Wiederherstellungs-Funktionen • Verschlüsselung nicht für alle Mobilplattformen

2.12.6 Grundsätzliches zur Installation von Software auf Smartphones

Zwei wichtige Hinweise im Zusammenhang mit der Installation von Software auf Smartphones dürfen in diesem Zusammenhang nicht fehlen: Wie immer, wenn es gilt, Programme auf das mobile Telefon herunterzuladen, sollte man dazu auch in diesem Fall auf eine WLAN-Verbindung zurückgreifen. Das ist in der Regel nicht nur die kostengünstigere, sondern auch die stabilere Verbindung.

Oftmals der erste Schritt, der zur Installation einer Sicherheitssoftware nötig ist: Standardmäßig lässt das Android-Betriebssystem keine Installationen zu, die nicht aus dem Android-Market kommen – hier wird es geändert.



Wer es hingegen vorzieht, die Software über seinen PC herunterzuladen, muss beachten, dass er das APK-Archiv (Android Package) nicht so ohne Weiteres auf seinem Android-Telefon installieren kann. Das Betriebssystem betrachtet standard-

mäßig alle nicht über den Android-Markt bezogenen Programme als unsicher und erlaubt deren Installation nicht. Dies gelingt erst, wenn der Anwender unter *Menü/Anwendungen/Unbekannte Quellen* das grüne Häkchen gesetzt hat. Danach reicht in der Regel ein Klick auf Download – noch besser geht es unter Einsatz einer der vielen File-Manager, die für Android zur Verfügung stehen.

2.12.7 Fazit

Beide Lösungen funktionierten problemlos auf unserem Testgerät unter Android 2.2. Was ebenfalls wichtig ist: Beide Programme ließen sich nach Eingabe des Sicherheitscodes problemlos wieder entfernen. Was uns ebenfalls positiv überrascht hat, war die Tatsache, dass beide Lösungen das nicht übermäßige starke Gerät nur wenig belasteten – im täglichen Betrieb ergaben sich keine Einschränkungen.

Die Ausrichtungen der getesteten Lösungen unterscheiden sich grundsätzlich voneinander: Wer eine klassische Antiviren- und Sicherheitslösung mit sinnvollen Erweiterungen für den Betrieb auf einem mobilen Telefon möchte, der sollte zum Kaspersky-Produkt greifen. Geht es hingegen vor allen Dingen darum, das Gerät und ganz besonders die Daten auf dem Telefon bei Verlust und Diebstahl zu schützen, dann lohnt ein Blick auf die McAfee-Lösung, bei der auch die Möglichkeiten eines Fernzugriffs in Kombination mit der Website überzeugen konnten.

Frank-Michael Schlede, Thomas Bär

Frank-Michael Schlede blickt auf über zwanzig Jahre Erfahrung als IT-Fachjournalist zurück, so war er unter anderem als Chefredakteur der Zeitschriften UNIXopen und Windows IT Pro tätig. Zu seinen Themengebieten gehören neben der kompletten Palette der Windows- und Linux/Unix-Betriebssysteme im Unternehmenseinsatz unter anderem die Bereiche Systemmanagement, Virtualisierung und Sicherheit. Er lebt und arbeitet in Pfaffenhofen an der Ilm.

Thomas Bär ist freier Journalist.

TecChannel-Links zum Thema	Webcode	Compact
Test: Sicherheitslösungen für Smartphones	2035250	S.104
Juniper Pulse Mobile Security für Smartphones	2036370	S.74
Smartphone- und Tablet-Sicherheit: Daten richtig verschlüsseln	2034879	S.81
Sicherheitsratgeber: Smartphones fernlöschen, orten und sperren	2036926	S.91
Empfehlenswerte Security-Apps für Android	2036785	S.99

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

3 iPhone

Für die Zufriedenheit und Motivation der Anwender ist auch das mobile Endgerät entscheidend. Apples iPhone spielt hier eine wichtige Rolle, belegt es in Unternehmen doch immer häufiger einen der vordersten Plätze auf den Wish Lists der Mitarbeiter. Dieses Kapitel beschäftigt sich mit der Einbindung und Absicherung von iOS-Clients in Unternehmensnetze, der Synchronisation und der Nutzung von Apps. Zudem geht es um die Nutzung von WLAN-Tethering mit dem iPhone.

3.1 iPhone-Praxis: Datensicherung und -wiederherstellung

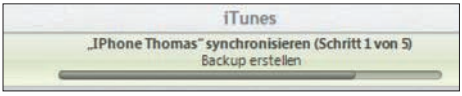
Apps, Zugänge, Daten – auf dem iPhone befinden sich in aller Regel Informationen, die gesichert werden sollten. Neben dem automatischen Sicherungsvorgang bieten sich auch weitergehende Optionen an, wie der folgende Beitrag erläutert.

Das zentrale Instrument zur Datensicherung und -wiederherstellung von iPhones ist iTunes. Das Programm erstellt automatisch bei jeder Synchronisierung eine Datensicherung des Gerätes. Sie haben aber auch die Möglichkeit, mit Zusatz-Tools auf die Backups zuzugreifen, manuell Sicherungen zu erstellen oder selbige wiederherzustellen. Die Mediathek lässt sich ebenso sichern.

3.1.1 iPhone-Datensicherung

Sobald Sie ein iPhone mit dem PC verbinden, auf dem Sie iTunes installiert und mit dem entsprechenden Endgerät verbunden haben, startet automatisch eine Synchronisierung, bei der iTunes auch eine Datensicherung des Geräts anlegt. Die Sicherung startet immer zuerst, bevor die eigentliche Synchronisierung beginnt.

Automatismus: iTunes erstellt vor der Synchronisierung zunächst automatisch ein Backup.



Den Stand des letzten Backups sehen Sie über *Bearbeiten\Einstellungen* auf der Registerkarte *Geräte*. Hierüber können Sie unter Umständen auch Probleme beheben, wenn sich das iPhone nicht mehr korrekt synchronisieren kann. iTunes sichert immer nur ein Backup für jedes Gerät. Das heißt, Sie sollten den Speicherort der iTunes-Sicherung in die Backup-Strategie Ihrer Daten einbinden. Geht das iPhone verloren und ist die Datensicherung auf dem iTunes-PC nicht verfügbar, sind alle Daten auf dem iPhone weg.

Rückblick: Sie können sich die Geräte-Backups anzeigen lassen.

Die Datensicherung des iPhones enthält vielfältige Daten (siehe Datensicherung mit iTunes und Verschlüsselung, nächster Absatz), die Sie bei der Wiederherstellung der Werkseinstellungen wieder auf das iPhone übertragen können. Sie können an der Konfiguration keine Änderungen vornehmen. Die erste Sicherung dauert immer etwas länger, da die Sicherung dann erst eine Vollsicherung durchführt. Bei weiteren Sicherungen muss iTunes nur noch die Änderungen sichern, was deutlich schneller geht.

3.1.2 Datensicherung mit iTunes und Verschlüsselung

Bei der Datensicherung berücksichtigt iTunes folgende Daten auf dem iPhone:

- Adressbuch
- Daten für Programme aus dem App Store
- Programmeinstellungen
- Daten für das automatische Ausfüllen von Webseiten
- CalDAV und Kalenderabonnements
- Kalenderaccounts
- Kalendereregnisse
- Anrufverlauf
- Fotos, Screenshots, Bilder und Videos
- Kennwörter für E-Mail-Accounts und Wi-Fi-Kennwörter
- Liste der externen Synchronisierungsquellen (MobileMe, Exchange ActiveSync)
- Mail-Accounts und Microsoft-Exchange-Account-Konfigurationen
- Netzwerkeinstellungen
- Notizen
- Gekoppelte Bluetooth-Geräte
- Lesezeichen, Cookies, Verlauf, Offline-Daten und aktuell geöffnete Seiten in Safari
- SMS- und MMS-Nachrichten (Bilder und Videos)
- Hintergrundbilder

Sie haben die Möglichkeit, die Datensicherung von iPhones zu verschlüsseln, sodass sichergestellt ist, dass nur Sie diese Sicherungen verwenden können und kein unbefugter Benutzer an Ihre Daten kommt. Nicht verschlüsselte Sicherungen lassen sich problemlos mit externen Tools auslesen.

Diese Einstellung nehmen Sie ebenfalls in iTunes vor, wenn Sie das Gerät verbunden haben. Klicken Sie dazu auf das iPhone, dessen Sicherungen Sie verschlüsseln wollen, und wählen dann im oberen Bereich *Übersicht* aus. Aktivieren Sie im Bereich Optionen die Option *iPhone-Backup verschlüsseln*. Anschließend müssen Sie ein Kennwort für diese Sicherung eingeben; das brauchen Sie, um die Daten auf dem iPhone wiederherzustellen. Das Kennwort speichert iTunes, sodass Sie es nicht immer wieder neu eingeben müssen, wenn Sie das Gerät synchronisieren. Haben Sie das Kennwort nicht mehr zur Verfügung, können Sie das gesicherte iPhone mit dieser Sicherung nicht mehr wiederherstellen. Zwar existieren Tools, die das Wiederherstellen des Kennworts erlauben sollen, doch ob dies zuverlässig funktioniert, kann niemand garantieren.

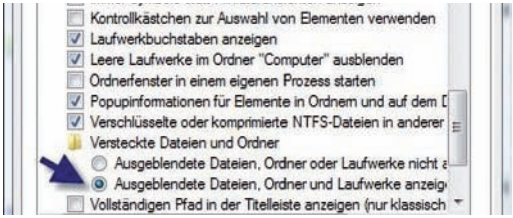
3.1.3 Schlüsselbund-Daten

In diesen Dateien speichert das iPhone die Kennwörter von E-Mail-Konten, angebundene WLAN-Netzwerke und Kennwörter, die Sie auf Webseiten und in anderen Applikationen eingeben. Ab iOS 4 können Sie das Backup Ihres Schlüsselbunds auf ein neues Gerät übertragen. Das Backup muss dazu verschlüsselt sein.

Im Schlüsselbund liegen alle wichtigen Kennwörter der verbundenen Konten, die Sie gespeichert haben. iTunes speichert die Datensicherung des iPhones auf dem lokalen PC. Der Speicherort variiert entsprechend der jeweiligen Betriebssysteme. Ein Backup besteht aus einem Ordner und zahlreichen Dateien, die sich standardmäßig nicht öffnen lassen. Sie sollten mit der Datensicherung Ihres Computers auch regelmäßig diesen Ordner mit sichern:

- Mac: *~/Library/Application Support/MobileSync/Backup/*
- Windows XP: *\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Apple Computer\MobileSync\Backup*
- Windows Vista und Windows 7: *\Users\<Benutzername>\AppData\Roaming\Apple Computer\MobileSync\Backup*

Sichtbarkeit: Zunächst müssen die Explorer-Ordneroptionen angepasst werden.

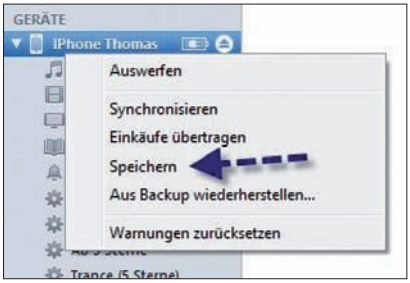


Sie sehen den Ordner erst, wenn Sie die versteckten Ordner im Windows-Explorer einblenden lassen. Der Windows-Explorer in Windows 7 und Windows Vista blendet standardmäßig viele wichtige Dateien aus. Für Profianwender kann es notwendig sein, dass alle Dateien, auch die versteckten und die Systemdateien, angezeigt werden. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie den Windows-Explorer.
2. Klicken Sie auf *Organisieren/Ordner- und Suchoptionen*.
3. Wechseln Sie zur Registerkarte *Ansicht*.
4. Deaktivieren Sie die Option E*rweiterungen bei bekannten Dateitypen ausblenden* und bestätigen Sie die Warnmeldung mit *Ja*. In diesem Fall werden auch die Endungen der Dateien angezeigt.
5. Deaktivieren Sie die Option *Geschützte Systemdateien ausblenden*.
6. Aktivieren Sie die Option *Ausgeblendete Dateien, Ordner oder Laufwerke anzeigen* im Abschnitt *Versteckte Dateien und Ordner*.

3.1.4 Manuell sichern und wiederherstellen

Neben der automatischen Erstellung von Datensicherungen können Sie auch manuell zu jeder Zeit eine Sicherung durchführen. Dazu klicken Sie mit der rechten Maustaste auf das Gerät in iTunes und wählen *Speichern*. Sie müssen keine Einstellungen vornehmen, vielmehr sichert iTunes bei diesem Vorgang die gleichen Daten wie bei der automatischen Sicherung.



Auf einen Klick: Eine manuelle Sicherung ist gleichfalls möglich.

Sie haben über diesen Weg auch die Möglichkeit, das iPhone wiederherzustellen, indem Sie die Option *Aus Backup wiederherstellen* auswählen. Vorhandene Sicherungen können Sie selbstverständlich auch löschen. Klicken Sie dazu auf *Bearbeiten\Einstellungen*. Wechseln Sie auf die Registerkarte *Geräte* und wählen die Sicherung aus. Klicken Sie anschließend auf *Backup löschen*, um diese zu entfernen. Die nächste Datensicherung kann in diesem Fall aber wieder etwas länger dauern, da iTunes erneut alle Daten sichern muss, nicht nur die geänderten Dateien.

3.1.5 iPhone-Backups mit iPhone Backup Extractor und Decipher auslesen

Den Inhalt von Sicherungen können Sie mit Standardmitteln weder auslesen noch extrahieren, auch nicht mit iTunes. Hier hilft das Tool iPhone Backup Extractor (www.iphonebackupextractor.com) weiter. Dieses Tool kann Daten aus der Sicherung auslesen und wiederherstellen, auch einzelne Bereiche.

Sie können nach dem Extrahieren auf alle Daten einzeln zugreifen und verschiedene Bereiche auslesen. iPhone Backup Extractor steht als eingeschränkte Freeware-Version zur Verfügung, lässt sich aber auch registrieren. Die kostenlose Version kann bereits auf Sicherungen zugreifen und Daten wiederherstellen, allerdings nur zwei Dateien in einem bestimmten Zeitraum. Zur Verwendung müssen Sie das Tool nur entpacken und starten, eine Installation ist nicht notwendig. Der Vorteil dabei ist, dass Sie auf diese Weise das Tool auch mobil, zum Beispiel über einen USB-Stick, nutzen können. Der iPhone Backup Extractor steht in einer Windows-Version und für MacOS zur Verfügung.

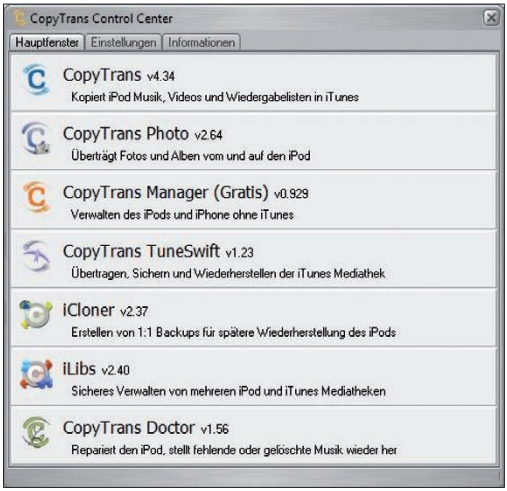
Hilfreich: Der Zugriff auf die Daten einer Sicherung ist per Tool möglich.

Sie müssen das Tool nur starten; auch eine Einrichtung ist nicht erforderlich. iPhone Backup Extractor greift automatisch auf vorhandene Sicherungen auf dem PC zu und erlaubt ein Recovery. Dazu klicken Sie im unteren Bereich auf die Daten, die Sie zurückholen wollen, und wählen den Ordner aus, in dem das Tool die Daten wiederherstellen soll. Anschließend können Sie im Dateisystem auf dem Rechner auf die rekonstruierten Daten zugreifen. Mit verschlüsselten Backups funktioniert das allerdings nicht.

Ein weiteres Tool, um Voicemail-Nachrichten oder SMS aus der Datensicherung auszulesen, ist Decipher (http://decipher-media.com/iphone-tools/). Das Tool steht aber nur für MacOS zur Verfügung. Datensicherungen von iPhones auslesen kann zudem das Tool JuicePhone (www.addpod.de/juicephone). Auch dieses läuft nur in MacOS, kann aber ebenfalls Datensicherungen auslesen und einzelne Daten wiederherstellen. Auch hier dürfen die Datensicherungen nicht verschlüsselt sein.

3.1.6 iTunes-Ersatz CopyTransManager

Anwender, die nicht gerne iTunes einsetzen, können als Ersatz den CopyTransManager (www.copytrans.de) nutzen. Das Tool kann Daten zwischen iPhone und Computer austauschen sowie Titelinformationen und Wiedergabelisten bearbeiten.



Substitut: Der CopyTransManager fungiert als kostenloser iTunes-Ersatz.

Nachdem Sie das Tool heruntergeladen und installiert haben, verbindet es sich mit dem iPhone. Sie haben mit dem Tool auch die Möglichkeit, Daten zu sichern und wiederherzustellen. Allerdings ist CopyTransManager nicht unbedingt dazu geeignet, parallel zu iTunes zu arbeiten. Dateien, die Sie per CopyTransManager auf iPhones kopiert haben, lassen sich teilweise in iTunes nicht mehr ohne Weiteres einlesen, da sie dann in einigen Fällen nicht mehr kompatibel zu iTunes sind.

3.1.7 Mediathek sichern und wiederherstellen

Mit iTunes können Sie auch Ihre Wiedergabelisten und Ihre Mediathek mit MP3, Bildern und Videos sichern. Klicken Sie dazu auf *Datei\Mediathek\Sicherheitsko-*

pie auf Speichermedium. Sie haben im neuen Fenster die Möglichkeit, alle Wiedergabelisten und die enthaltenen Videos, MP3s und Bilder der Mediathek auf CD/DVD zu brennen. Die Datensicherung berücksichtigt folgende Bereiche:

- Programme
- Hörbücher
- Spiele
- Filme
- Musik
- Musikvideos
- Podcasts
- Klingeltöne
- Fernsehsendungen

Leider ist auf diesem Weg keine Sicherung auf Netzwerkfreigaben oder externe Festplatten möglich, Sie können die Daten nur brennen.

Auslagerung: Die Mediathek können Sie auf Datenträger brennen.

Wenn die Daten nicht auf einen eingelegten Datenträger passen, erhalten Sie einen Hinweis, wie viele Rohlinge Sie noch benötigen. Sobald ein Datenträger voll ist, meldet iTunes, dass Sie den nächsten Datenträger einlegen müssen.

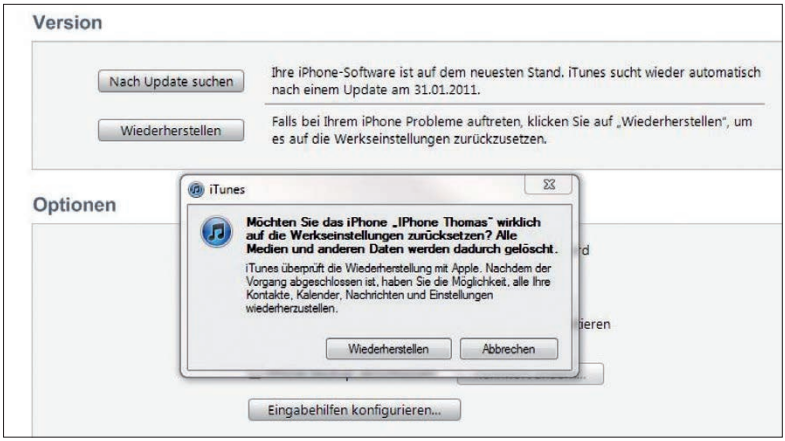
Haben Sie iTunes neu installiert oder wollen die Mediathek wiederherstellen, legen Sie den ersten Datenträger des Sicherungssatzes ins Laufwerk. iTunes erkennt automatisch, dass es sich um eine Datensicherung handelt, und fragt Sie, ob Sie die Sicherung wiederherstellen wollen.

Ein sehr wichtiges Verzeichnis für Wiedergabelisten und die Konfiguration von iTunes ist der Speicherort von iTunes Media. Sie sollten den Inhalt des Ordners in regelmäßigen Abständen sichern, um iTunes wiederherstellen oder den Inhalt auf einen anderen Computer übertragen zu können. In iTunes haben Sie die Möglichkeit, den Speicherort dieses Verzeichnisses zu ändern. Die Einstellungen dazu finden Sie über *Bearbeiten\Einstellungen* auf der Registerkarte *Erweitert*.

Lokalisierung: den aktuellen Speicherort von iTunes Media anpasen und anzeigen.

3.1.8 iPhone-Werkseinstellungen wiederherstellen

Wenn Sie Probleme mit Ihrem iPhone haben, die sich nicht beheben lassen, bietet iTunes die Möglichkeit, das Handy zu den Werkseinstellungen zurückzusetzen. Bei diesem Vorgang löscht iTunes alle Daten auf dem iPhone.



Alles auf Anfang: iPhone auf die Werkseinstellungen zurücksetzen.

Da diese aber in iTunes gesichert sind, können Sie nach der Wiederherstellung diese Daten wieder auf das iPhone übertragen. Zum Werks-Reset verbinden Sie das iPhone mit iTunes und klicken im Bereich Geräte auf das iPhone, das Sie zurücksetzen wollen. Klicken Sie dann auf *Wiederherstellen*. Es erscheint noch ein weiteres Fenster, in dem Sie die Zurücksetzung bestätigen müssen. Anschließend setzt iTunes das Gerät zurück. Dazu verwendet iTunes die erstellte Datensicherung.

Thomas Joos

3.2 iPhone-Praxis: VPN richtig einrichten und nutzen

Mit dem iPhone lässt sich wie mit PC-Clients ein sicherer Zugriff aufs Unternehmensnetzwerk via VPN realisieren. Bei der Anbindung an ein VPN verhält sich das iPhone dann wie ein üblicher PC. Das heißt, Unternehmen benötigen einen ganz normalen VPN-Zugang. Das kann ein VPN-Router oder ein Windows-Server sein. Die Anbindung erfolgt über interne Einstellungen auf dem iPhone. Von Herstellern wie Juniper (http://www.juniper.net/de/de/) oder Cisco (www.cisco.com) stehen im App-Store Apps zur Anbindung bereit, die die Konfiguration und den Start des VPNs vereinfachen und den Datenverkehr steuern.

3.2.1 VPN-Protokolle für das iPhone – Cisco und Co.

Das iPhone unterstützt als Protokolle L2TP/IPSec, PPTP und Cisco IPSec. Das bedeutet, Sie können jeden VPN-Server einsetzen, der diese Protokolle unterstützt. Die Benutzer-Authentifizierung können Sie über MS-ChapV2, RSA SecurID mit CryptoCard oder über einen symmetrischen Schlüssel (Shared Secret) konfigurieren. Point-to-Point-Tunnel-Protocol (PPTP)-basierter VPN-Datenverkehr besteht aus einer TCP-Verbindung zum TCP-Port 1723 auf dem VPN-Server, um den Tunnel zu verwalten, und aus GRE (Generic Routing Encapsulation)-gekapselten Paketen für die VPN-Daten. PPTP-Datenverkehr kann jedoch Probleme mit Firewalls, NATs und Webproxys haben. Um Probleme zu vermeiden, müssen Firewalls so konfiguriert sein, dass sie sowohl die TCP-Verbindung als auch GRE-gekapselte Daten ermöglichen PPTP ermöglicht die verschlüsselte Einkapselung von verschiedenen Netzwerkprotokollen. Nachdem die Authentifizierung durchgeführt ist, verschlüsselt ein PPTP-VPN die Verbindung. Die Verschlüsselung baut auf dem Kennwort der Authentifizierung auf. Je komplexer das Kennwort ist, umso besser ist die Verschlüsselung. Da die Verschlüsselung und der Transport der einzelnen IP-Pakete durch das GRE-Protokoll durchgeführt werden, müssen Sie darauf achten, dass die Hardware-Firewall beziehungsweise der DSL-Router, den Sie verwenden, dieses Protokoll beherrscht. Wer eine aktuelle FritzBox einsetzt, kann auch diese als VPN-Server konfigurieren, der mit iPhones funktioniert. Mehr Informationen dazu finden Sie auf der Website von AVM (www.avm.de).

3.2.2 VPN per L2TP

Die zweite Variante, ein VPN aufzubauen, ist das Layer 2 Tunnel Protocol (L2TP). Dieses Protokoll ist sicherer als PPTP, aber dafür komplexer in der Einrichtung. L2TP verwendet IPSec, um eine Verschlüsselung aufzubauen. Beim Aufbau eines VPN mit L2TP wird der Datenverkehr, im Gegensatz zu PPTP, bereits vor der Authentifizierung zuverlässig verschlüsselt. Da L2TP zur Verschlüsselung des Daten-

verkehrs IPSec verwendet, können Sie mit diesem VPN-Typ auch eine 3DES-Verschlüsselung durchführen. Der Einsatz eines VPN auf Basis von L2TP setzt eine Zertifizierungsstelleninfrastruktur voraus. Sie können auch Juniper Junos Pulse und Cisco AnyConnect einsetzen. Für diese Methoden stehen im App-Store entsprechende Apps zur Verfügung, mit denen Sie die Einrichtung durchführen. Die Einrichtung können auch normale Anwender leicht durchführen, wenn die entsprechenden Verbindungsdaten des VPN zur Verfügung stehen.

3.2.3 Der Cisco-AnyConnect-Client

Mit dem Cisco-AnyConnect-Client lassen sich iPhones an Cisco-VPN-Server, zum Beispiel der ASA-5500-Serie oder der IronPort-S-Serie, anbinden. Der Client dazu steht als App kostenlos im App-Store zur Verfügung. Die Software verwendet SSL (Secure Sockets Layer) und DTLS (Datagram Transport Layer Security). Der AnyConnect-VPN-Client benötigt mindestens iOS 4.1 und unterstützt iPhone 3G, iPhone 3GS, iPhone 4 und die aktuellen iPod-touch-Geräte.

Einrichtung: Der Cisco-VPN-Client erlaubt die manuelle Konfiguration.

Der Client erlaubt die manuelle Konfiguration, aber auch den Import von Profilen mit dem iPhone-Konfigurationsprogramm. Die Konfiguration des AnyConnect-Clients ist genauso einfach wie die Konfiguration mit Bordmitteln des iPhones. Die Größe des Clients beträgt etwa 7.4 MByte, die Einrichtung ist nur in englischer Sprache möglich. Anwender geben die Daten ein, die Administratoren ihnen mitteilen. Zur Authentifizierung lassen sich auch Zertifikate einsetzen. Das ist Voraussetzung, wenn Sie Connect-on-Demand nutzen wollen. Auf diese Weise lassen sich bestimmte Zugriffe auf Ressourcen, zum Beispiel Exchange-Postfach oder SharePoint, automatisch über das VPN routen.

Im unteren Bereich der App stehen über den Menüpunkt *Statistics* weitere Informationen zur Nutzung des Clients zur Verfügung. In diesem Bereich sehen Anwender den Status der Verbindung sowie Informationen zu den gesendeten und heruntergeladenen Daten.

Im unteren Bereich der App stehen über den Menüpunkt *Statistics* weitere Informationen zur Nutzung des Clients zur Verfügung. In diesem Bereich sehen Anwender den Status der Verbindung sowie Informationen zu den gesendeten und heruntergeladenen Daten.

Datenübergabe: Hier geben Sie die Daten für das Cisco-VPN ein.

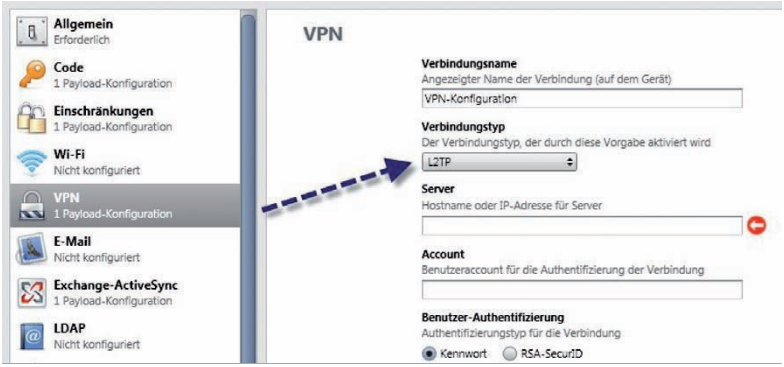
Wenn Sie ein zertifikatsbasiertes VPN einsetzen, können Sie Zertifikate in den Formaten PKCS#1 (.cer, .crt, .der) und PKCS#12 (.p12, .pfx) verwenden. Der Import der Zertifikate erfolgt entweder manuell oder über das iPhone-Konfigurationsprogramm. Grundlage des iPhone-Konfigurationsprogramms sind Konfigurationsprofile (siehe auch iPhone-Praxis: Einstellungen per Konfigurationsprogramm automatisieren, Webcode **2033060**).

Hierbei handelt es sich um XML-Dateien, in denen Sie Einstellungen des iPhones vordefinieren und verteilen können. Dies können zum Beispiel Einstellungen für VPN sowie Zertifikate sein, die Sie für VPN benötigen.

3.2.4 VPN auf dem iPhone einrichten

Die Konfiguration von VPN nehmen Sie entweder über das iPhone-Konfigurationsprogramm (Webcode **2033060**) vor, um das Profil an mehrere iPhones zu verteilen, oder Sie verwenden eine manuelle Konfiguration.

Wählen Sie zur manuellen Einstellung *Einstellungen\Allgemein\Netzwerk\VPN*. Klicken Sie auf *VPN hinzufügen* und tragen Sie die Daten des VPN-Servers ein. Haben Sie alle Daten für die VPN-Verbindung eingetragen, müssen Sie die Funktion VPN noch aktivieren. Wenn Sie per VPN verbunden sind, zeigt das iPhone die Verbindung in der Statusleiste an. Sie können im iPhone natürlich mehrere VPN-Konfigurationen verwenden und diese wechseln. Die Einstellungen dazu finden Sie wieder über *Einstellungen\Allgemein\Netzwerk\VPN*.



VPN auf dem iPhone einrichten: Konfigurieren von VPNs über das iPhone-Konfigurationsprogramm.

3.2.5 Alternative VPN verwenden

Natürlich besteht auch die Möglichkeit, dass Anwender den Internetverkehr über ein VPN laufen lassen. Der Vorteil dabei ist, dass die Datenverbindungen sicherer sind und sich gesperrte IP-Adressen umgehen lassen, was unter Umständen hilfreich sein kann.

Simpel: Das Konfigurieren eines HotspotShield-Zugangs.

Ein bekannter Anbieter eines kostenloses VPN ist Hotspotshield (http://hotspotshield.com/clientless/iphone/get_started.php). Sie müssen sich ein Konto anlegen und können dann auf dem iPhone eine VPN-Verbindung einrichten, mit der Sie IP-Adressen-Sperren umgehen können. Die Einrichtung ist sehr einfach:

1. Deaktivieren Sie zunächst die Wi-Fi-Verbindungen im iPhone über *Einstellungen\Wi-Fi*.
2. Richten Sie ein neue VPN-Verbindung ein über *Einstellungen\Allgemein\Netzwerk\VPN* und fügen Sie diese dann der Auswahl von *VPN* hinzu.
3. Aktivieren Sie die Option *IPSec*.
4. Tragen Sie bei Beschreibung *HotspotShield* ein.
5. Tragen Sie bei Server den Wert *68.68.107.101* ein.
6. Bei Account tragen Sie *ietghz* ein.
7. Bei Kennwort tragen Sie *ietghz* ein.
8. Deaktivieren Sie die Verwendung von Zertifikaten.
9. Bei Gruppenname tragen Sie *hss* ein.
10. Bei Shared Secret tragen Sie ebenfalls *hss* ein.
11. Klicken Sie auf *Sichern*.
12. Aktivieren Sie als Nächstes Wi-Fi auf dem iPhone wieder.

Im nächsten Schritt aktivieren Sie das VPN. Dazu klicken Sie auf Einstellungen und aktivieren VPN auf dem iPhone.

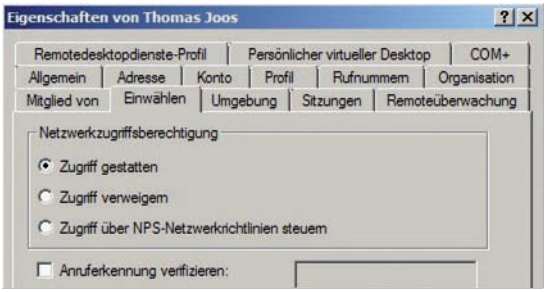
Verbindung herstellen: Aktivieren Sie die VPN-Funktionalität auf dem iPhone.

Anschließend verbindet sich das iPhone mit dem VPN und zeigt den Status als verbunden an. Sie sehen die Dauer der Verbindung sowie den VPN-Status im oberen Bereich des iPhones. Die Verbindung zum VPN ist leider nicht immer stabil, dafür aber kostenlos. Vor allem im Ausland, wenn IP-Sperren den Zugang auf bestimmte Seiten unmöglich machen, kann der Zugang helfen.

Eine Alternative zum kostenlosen Zugang ist zum Beispiel Overlay (www.overplay.net). Der Zugang kostet allerdings knapp 10 US-Dollar im Monat. Die Einrichtung erklärt der Anbieter Schritt für Schritt (www.overplay.net/blog/vpn-for-ipad-howto/). Die Anbindung ist auch über das iPad möglich.

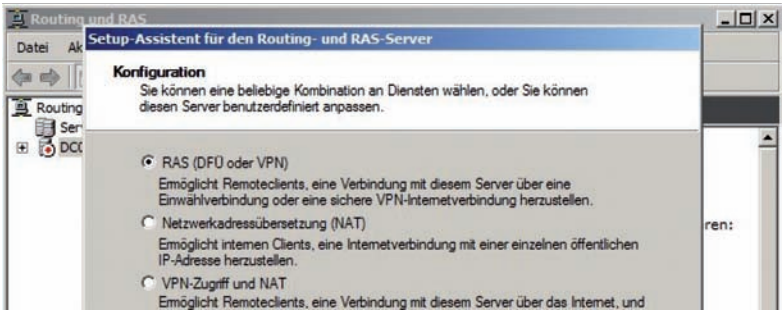
3.2.6 VPN mit Windows Server, ISA oder TMG

Viele Unternehmen setzen als VPN-Server entweder einen Windows-Server oder einen ISA-Server beziehungsweise dessen Nachfolger TMG 2010 ein (siehe auch Microsoft Forefront – Das Threat Management Gateway 2010, Webcode **2026446**). Unabhängig von der verwendeten Serverversion können Sie beim Einsatz von Active Directory im Unternehmen auch die Einwahlberechtigungen in das VPN steuern. Diese Rechte gelten dann auch für iPhones.



Erlaubnis erteilen: So berechtigen Sie Benutzer im Active Directory für die VPN-Einwahl.

Aktivieren Sie auf der Registerkarte *Einwählen* im Bereich *Netzwerkzugriffsberechtigung* in der Verwaltungskonsole *Active Directory-Benutzer und -Computer* die Option *Zugriff gestatten*. In einer produktiven Umgebung können Sie auch die Option *Zugriff über NPS-Netzwerkrichtlinien steuern* wählen. In diesem Fall erstellen Sie eine Gruppe im Active Directory, zum Beispiel mit der Bezeichnung VPN-Zugriff, und nehmen die Benutzerkonten in die Gruppe mit auf, denen Sie VPN-Zugriff gestatten wollen. Auf dem Netzwerkrichtlinienserver können Sie dann dieser Gruppe die Einwahl gestatten. Dies hat den Vorteil, dass Sie nicht die einzelnen Benutzerkonten konfigurieren müssen, sondern die Einwahl über Gruppenmitgliedschaft steuern.



Voraussetzung: Routing und RAS in Windows Server 2008 R2 konfigurieren und aktivieren.

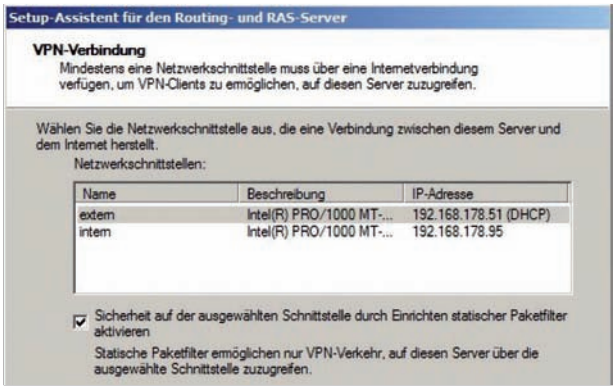
Ein VPN-Server auf Basis von Windows Server sollte zwei Netzwerkkarten verwenden. Für die Remote-Einwahl müssen Sie auf dem VPN-Server die Rolle *Netzwerkrichtlinien- und Zugriffsdienste* installieren. Zusätzlich müssen Sie noch den Rollendienst Routing- und RAS-Dienste auswählen. Haben Sie die Rolle *Netzwerkrichtlinien- und Zugriffsdienste* bereits installiert, klicken Sie im Servermanager auf *Rollen/Netzwerkrichtlinien- und Zugriffsdienste* und dann in der Mitte der Konsole auf *Rollendienste hinzufügen*.

Wählen Sie an dieser Stelle den Rollendienst *Routing- und RAS-Dienste* aus. Nach der Installation des Rollendienstes starten Sie die Verwaltung über *Start/Ausführen/rrasmgmt.msc* oder über *Start/Verwalten/Routing und RAS*. Nachdem Sie die Konsole gestartet haben, klicken Sie mit der rechten Maustaste auf den Servernamen und wählen im Kontextmenü den Eintrag *Routing und RAS konfigurieren und aktivieren* aus. Daraufhin startet ein Assistent, mit dessen Hilfe Sie die Einwahlmöglichkeiten per VPN konfigurieren können.

3.2.7 VPN auf dem Server konfigurieren

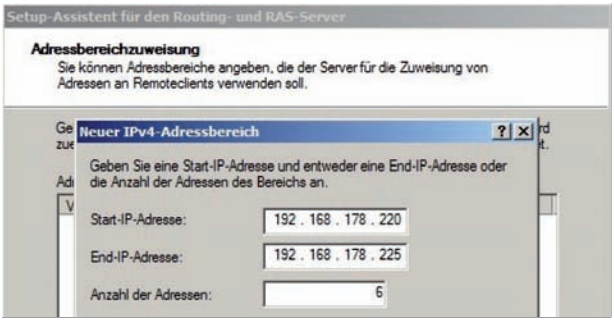
Nach dem Willkommensbildschirm konfigurieren Sie auf der nächsten Seite des Assistenten zunächst die Funktion des RAS-Servers. Für die Einwahlmöglichkeiten per DFÜ oder VPN wählen Sie die Option *RAS* (DFÜ oder VPN). Auf der nächsten Seite des Assistenten aktivieren Sie das Kontrollkästchen *VPN*. Anschließend legen Sie fest, an welcher Schnittstelle der Server auf Verbindungen warten soll.

Auswahl: Sie müssen die externe Schnittstelle für die VPN-Einwahl festlegen.



Hier verwenden Sie natürlich die Schnittstelle, die mit dem externen Netzwerk verbunden ist. Haben Sie im Server zwei Netzwerkkarten eingebaut, benennen Sie im Netzwerk- und Freigabecenter diese Verbindungen am besten in *intern* und *extern* um, damit Sie diese einfacher zuordnen können. Deaktivieren Sie zusätzlich noch die Option *Sicherheit auf der ausgewählten Schnittstelle durch…* .

Dadurch ist sichergestellt, dass die VPN-Clients Verbindung mit dem VPN-Server aufbauen können, um diesen etwa zu pingen, ohne dass eine Route gesetzt sein muss. Auf der nächsten Seite des Assistenten legen Sie fest, welche IP-Adresse die Clients bei der Einwahl erhalten sollen; das gilt auch für iPhones, da auch diese eine IP-Adresse erhalten. Wählt sich ein Client per VPN in das Netzwerk ein, erhält er eine IP-Adresse im internen Netzwerk.



Eingrenzung: Sie können einen IPv4-Adressbereich für die VPN-Clients festlegen.

Sie können entweder die IP-Adressen über einen DHCP-Server zuweisen lassen, indem Sie die Option *Automatisch* auswählen, oder über die Option *Aus* einen angegebenen Adressbereich manuell die IP-Adressen im internen Netzwerk eingeben, die VPN-Clients verwenden. Wählen Sie in diesem Beispiel diese Option aus. So können Sie einen IP-Bereich festlegen. Auf der nächsten Seite geben Sie den IP-Bereich ein, aus dem die VPN-Clients IP-Adressen zugeteilt bekommen.

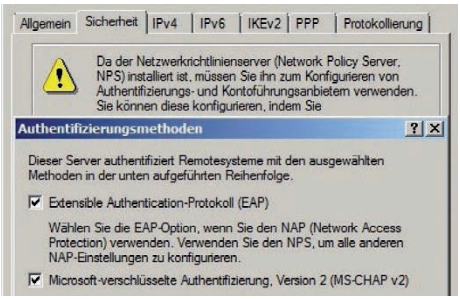
3.2.8 DHCP-Relay einrichten

Nach Abschluss der Konfiguration startet Windows den Routing- und RAS-Dienst. Sie erhalten anschließend noch verschiedene Meldungen, die Sie darauf hinweisen, dass Sie die Authentifizierungsoptionen festlegen und den DHCP-Relay-Agenten konfigurieren müssen.

Einrichtung: Es gilt zunächst, den DHCP-Relay-Agenten zu konfigurieren.

Im DHCP-Relay-Agenten wird die IP-Adresse des DHCP-Servers hinterlegt. Der Relay-Agent antwortet auf die Anfragen von Clients und leitet diese an den DHCP-Server weiter. Dieser teilt eine IP-Adresse zu, die dann wiederum vom Relay-Agenten dem Client mitgeteilt wird. Wenn Sie DHCP für VPN verwenden möchten, müssen Sie die IP-Adresse Ihres DHCP-Servers als Relay-Agent im RAS-Server eintragen, damit die Anfragen des RAS-Clients an den DHCP-Server weitergeleitet werden können.

Trau, schau, wem: Die VPN-Authentifizierungsmethode muss festgelegt werden.



Sie erhalten beim ersten Start des Dienstes eine entsprechende Warnung. Klicken Sie dazu nach dem Starten des RAS-Dienstes auf *IPv4/DHCP-Relay-Agent* und rufen Sie die Eigenschaften auf. In den *Eigenschaften* tragen Sie die IP-Adresse Ihres DHCP-Servers ein. Der nächste Schritt besteht darin, dass Sie den VPN-Server noch konfigurieren. Sie müssen zum Beispiel noch die Authentifizierung für Clients festlegen. Starten Sie dazu die Verwaltungskonsole für Routing und RAS:

1. Rufen Sie die Eigenschaften des VPN-Servers in der Konsole auf und wechseln Sie auf die Registerkarte *Sicherheit*.
2. Klicken Sie anschließend auf *Authentifizierungsmethoden*.
3. Stellen Sie sicher, dass *Extensible Authentication Protocol (EAP)* und *Microsoft-verschlüsselte Authentifizierung, Version 2 (MS-CHAP v2)* ausgewählt sind. PAP (Password Authentication Protocol) verwendet Kennwörter mit Klartext und ist das einfachste Authentifizierungsprotokoll. Beim Aktivieren von PAP als Authentifizierungsprotokoll werden Benutzerkennwörter als Klartext gesendet. Durch das Abfangen von Paketen während des Authentifizierungsprozesses kann das Kennwort leicht entschlüsselt und für nicht autorisierten Intranetzugriff verwendet werden.

Sobald die Konfiguration abgeschlossen ist, können Anwender über das Internet auch mit dem iPhone auf das interne Netzwerk zugreifen. Die Konfiguration ist auf diese Weise ebenfalls für Small Business Server geeignet, auch in der neuen Version SBS 2011 (siehe auch Windows Small Business Server 2011 – Neuerungen und Versionen, Webcode **2033028**).

Thomas Joos

3.3 iPhone-Praxis: Kalender optimal synchronisieren

Eine wichtige Anwendung bei Smartphones ist die Verwaltung von Terminen. Neben der reinen Planung von Terminen mit Geräten wie dem iPhone ist natürlich auch die Synchronisierung mit anderen Kalendern wichtig, zum Beispiel mit dem Exchange-Postfach oder Outlook. Dazu gehört natürlich auch die Verwaltung von Besprechungsanfragen.

Im iPhone ist eine Standard-App für die Verwaltung der Termine integriert, die Benutzern eine recht gute Hilfe ist. Doch für Power-User und Profis sind zusätzliche Apps notwendig, wenn Termine optimal verwaltet werden sollen. iPhones lassen sich problemlos mit allen wichtigen Diensten synchronisieren, um auch unterwegs terminlich immer auf dem neuesten Stand zu sein.

3.3.1 iPhone und Exchange

Wenn Sie das iPhone über Exchange ActiveSync mit einem Exchange-Postfach verbunden haben, synchronisiert sich automatisch auch der Kalender mit dem Exchange-Postfach. In diesem Fall ist der Kalender in Outlook ebenfalls aktuell, auch wenn Sie über Outlook Anywhere arbeiten. Die Einstellungen für die Synchronisierung des Kalenders nehmen Sie im iPhone über *Einstellungen\Mail, Kontakte, Kalender* vor. Auf diese Weise verbinden Sie sich zudem mit Google-Konten, die Einstellungen zur Synchronisierung sind dabei identisch.

Rufen Sie die Einstellungen des Exchange-Kontos auf, für das Sie den Kalender verwalten wollen. In der Verwaltung der Synchronisierung für das entsprechende Postfach finden Sie für die drei Bereiche *Mail, Kontakte* und *Kalender* jeweils einen Schieberegler, über den Sie generell die Synchronisierung ein- oder ausschalten.

iPhone und Exchange: Ein- oder Ausschalten der Kalendersynchronisierung.

Alternativ können Sie auf der Hauptseite, in der Sie die Konten verwalten, nach unten zum Bereich *Kalender* scrollen. An dieser Stelle legen Sie zum Beispiel den Standardkalender fest und konfigurieren, welche Zeiträume die Kalendersynchronisierung berücksichtigen soll. Die Zeitzone wird ebenfalls hier eingestellt. Die Einstellungen gelten dann für alle Konten, deren Kalender Sie synchronisieren.

Die Einstellung der Zeitzone ist besonders wichtig. Haben Sie auf dem iPhone eine andere Zeitzone als in Ihren Kalendern eingestellt, mit denen Sie synchronisieren, kann es zu Problemen kommen. Dann sind Termine, die Sie im iPhone eintragen, unter Umständen nicht korrekt synchronisiert und stehen in den synchronisierten Kalendern mit anderen Daten.

3.3.2 Kalendereinstellungen

Weitere Einstellungen finden Sie direkt im Kalender, wenn Sie die Standard-App aufrufen und auf die Schaltfläche *Kalender* tippen. Hier können Sie einstellen, welche Kalender auf dem iPhone zur Verfügung stehen sollen. Im unteren Bereich haben Sie noch die Möglichkeit, die Kategorie *Geburtstage* zu aktivieren. Sie können diese Kategorie aber nicht beim Erstellen von Terminen auswählen; vielmehr liest das iPhone die Daten aus den Kontakten aus und fügt sie dem Kalender hinzu.

Details: Sie können für den Kalender im iPhone die Synchronisationseinstellungen festlegen.

Dazu müssen Sie den Kontakt, dem Sie einen Geburtstag hinzufügen möchten, bearbeiten und im Eigenschaftsfenster ein neues Feld hinzufügen. Wählen Sie hier Geburtstag aus und füllen Sie Daten aus. Das iPhone übernimmt die Daten automatisch in den Kalender. Bevor Sie die Kalendersynchronisierung starten, sollten Sie auf diese Weise die Geburtstagtermine in den Kontakten pflegen und selbst erstellte Termine löschen.

Happy Birthday: Sie können zu einem Kontakt ein Geburtstagsfeld hinzufügen.

Wenn Sie wiederholende Geburtstagtermine importieren, legt das iPhone unter Umständen hierfür verschiedene Einzeltermine an, was den Kalender unnötig aufbläht. Generell ist der Standardkalender im iPhone sehr leicht zu bedienen, weil er nur sehr wenige Optionen bietet. Bevor Sie eine Synchronisierung starten, sollten Sie Ihren Kalender zunächst aufräumen und Daten korrekt pflegen, um Datenmüll zu vermeiden.

3.3.3 Synchronisierung mit Outlook oder Google

Wollen Sie ein iPhone mit einem Outlook-Kalender synchronisieren, der nicht mit Exchange verbunden ist, konfigurieren Sie diese Möglichkeit in iTunes auf dem entsprechenden Rechner. Die Synchronisierung erfolgt dann nur, wenn Sie das Gerät mit Outlook und iTunes verbinden.

Gleichtakt: Den iPhone-Kalender mit Outlook synchronisieren.

In diesem Fall sollten Sie besser den Kalender in Outlook mit einem Google-Kalender synchronisieren und den Google-Kalender mit dem iPhone. Auf diese Weise können Sie dann auch über das Internet synchronisieren. Dazu verbinden Sie das iPhone mit dem PC und starten iTunes. Die Konfiguration der Synchronisierung direkt mit Outlook nehmen Sie vor, wenn Sie das Gerät im Navigationsbereich von iTunes anklicken und zu *Info* wechseln. Aktivieren Sie die Option *Kalender synchronisieren mit Outlook* und legen Sie fest, welchen Outlook-Kalender Sie synchronisieren wollen.

Erfahrungsgemäß funktioniert diese Synchronisierung aber nicht immer ordnungsgemäß. Sie sollten daher die Termine stichprobenartig kontrollieren. Vor allem, wenn Sie wiederholende Termine in Outlook pflegen, funktioniert die Synchronisierung nicht immer sauber. Wenn Sie über ein Google-Konto verfügen, können Sie auch über Ihren Google-Mail-Account den Kalender online pflegen. Im iPhone synchronisieren Sie dann über das eingetragene Google-Konto auch den Kalender. Die Einstellungen sind identisch mit der Konfiguration bei Exchange-Postfächern. Setzen Sie eine andere Kalendersoftware ein, bietet es sich an, in dieser Software die Termine zu exportieren, zum Beispiel als *.csv-Datei, und im Google-Kalender zu importieren. Das geht ganz leicht, und auf diese Weise bekommen Sie die Termine schnell und einfach auf das iPhone, indem Sie das Google-Konto anbinden und die Kalendersynchronisierung einrichten.

3.3.4 Das iPhone mit dem Google-Kalender synchronisieren

Die meiste Arbeit bei der Synchronisierung zwischen Google-Kalender und iPhone nehmen Sie in der Weboberfläche des Google-Kalenders vor. Diesen müssen Sie zunächst an Ihre Bedürfnisse optimal anpassen. Das anschließende Einrichten auf dem iPhone ist ein Kinderspiel und funktioniert genauso wie bei Exchange.

Sie fügen ein neues Konto hinzu und wählen *Google Mail* aus. Für die Anbindung müssen Sie nur E-Mail-Adresse, Ihren Namen und das Kennwort des Kontos eingeben. Die Serverdaten füllt das iPhone automatisch aus. Haben Sie alle notwendigen Daten eingegeben, synchronisiert sich das Telefon automatisch.

Wenn Sie auf dem iPhone bereits einen Kalender angelegt haben, erhalten Sie eine Meldung, in der Sie auswählen müssen, ob Sie den Kalender auf dem iPhone beibehalten oder löschen wollen. In diesem Fall sollten Sie den Kalender natürlich beibehalten – löschen sollten Sie ihn nur dann, wenn Sie die Daten des Kalenders auf dem iPhone nicht mehr benötigen. Falls Sie einen lokalen Kalender beibehalten, synchronisiert das iPhone die Termine nicht mit dem Google-Mail-Kalender. Hier trennt das iPhone strikt zwischen lokalen und synchronisierten Kalender.

Wenn Sie mehrere E-Mail-Konten mit dem iPhone synchronisieren, übernimmt das Smartphone die Termine aus allen Kalendern und zeigt diese in der Kalender-App an. Der beste Weg zur Synchronisierung besteht darin, dass Sie externe Kalender zunächst im Google-Kalender importieren und dann den Google-Kalender

mit dem iPhone synchronisieren lassen. Wollen Sie mehrere Google-Kalender mit dem iPhone synchronisieren, müssen Sie dazu zunächst die entsprechenden Einstellungen in Ihrem Google-Kalender vornehmen.

Dazu müssen Sie auf dem iPhone mit Safari zur Seite *http://m.google.com/sync* wechseln. Durch einen Bug bei Google erhalten Sie eine Meldung, dass die Seite nicht kompatibel ist. Klicken Sie dazu auf den Link Sprache und ändern die Sprache auf *Englisch (US)*. Anschließend müssen Sie sich an Ihrem Google-Konto anmelden. Im Fenster sehen Sie die mobilen Geräte, mit denen Sie sich mit dem Konto synchronisieren, und können Einstellungen vornehmen.

3.3.5 Apps für die Terminverwaltung

Generell sind die Verwaltung von Terminen und die Synchronisierung mit verschiedenen Kalendern recht einfach. Der Standardkalender im iPhone bietet ebenfalls wertvolle Hilfe bei der Verwaltung dieser Termine, ist aber nicht sehr umfangreich. Im App-Store gibt es jedoch zahlreiche weitere Apps, welche die Verwaltung Ihrer Termine enorm erleichtern. Vor allem Anwender, die intensiv mit dem Kalender arbeiten, sollten sich diese Apps ansehen.

Wenn Sie bei der Terminplanung vor allem auf den Google-Kalender setzen, sollten Sie sich die kostenpflichtige App CalenGoo (5,49 Euro) ansehen. Diese App kann wesentlich effizienter mit dem Google-Kalender umgehen als die Standard-App des iPhone. Sie lässt sich offline nutzen und synchronisiert sich automatisch bei der nächsten Internetverbindung. Sie können verschiedene Ansichten aktivieren und Farbeinstellungen anpassen. Vor allem Power-User, die auch beruflich den Google-Kalender intensiv nutzen, kommen um diese App kaum herum.

Auf einen Blick: Mit PocketCal lässt sich eine Jahresübersicht anzeigen.

Eine weitere wertvolle App ist Week Calendar (1,59 Euro). Diese App kann Termine in Wochenansichten effizient anordnen und bietet vor allem für solche Anwender eine optimale Ergänzung, die ihre Arbeitswoche effizient planen wollen.

Die App funktioniert auch zusammen mit Exchange, kann aber nur einen Exchange-Kalender unterstützen. Die Übersichtsfunktionen des Kalenders gleichen diesen Nachteil jedoch wieder aus.

Wer eine schnelle Übersicht über ein ganzes Jahr erhalten will, ist mit der kostenlosen App PocketCal gut beraten. Die App ist einfach zu bedienen und ideal für Anwender, die sich rasch einen Überblick verschaffen möchten. Es ist auch möglich, zum aktuellen Datum zu springen und mit einem einfachen Antippen das Jahr zu wechseln. Die Ansicht lässt sich so anpassen, dass die App auch weniger Monate auf einer Seite anzeigt, wenn Sie nicht das ganze Jahr sehen wollen.

Eine weitere App zur Terminverwaltung ist miCal. Auch sie erweitert die Funktionen des Standardkalenders. Sie können mit der App beispielsweise Ansichten wechseln und den Kalender in Queransicht anzeigen lassen. Mit dem Dashboard haben Sie alle Termine des Tages perfekt in der Übersicht. Die App unterstützt sämtliche Kalender, die Sie mit dem iPhone synchronisieren können, also Outlook, Exchange, Google, Facebook, etc.

Kalender-Kosmetik mit Quick Calendar

Ein Helfer in eher optischer Hinsicht ist die App Quick Calendar. Mit ihr können Sie den Startbildschirm des iPhones mit einem Kalender integrieren. Standardmäßig ist das mit dem iPhone nicht möglich. Quick Calendar kann beliebige Hintergrundbilder so anpassen, dass Sie künftig im Lockscreen einen Kalender sehen.

Integration: Quick Calendar kann Hintergrundbilder so anpassen, dass Sie künftig im Lockscreen einen Kalender sehen.

Sie sehen aber auf dem Kalender nicht den aktuellen Tag und auch nicht Ihre Termine, sondern lediglich die nächsten zwei bis drei Monate, zusammen mit dem Hintergrundbild, als statische Aufnahme. Der Kalender ist nicht dynamisch, sondern wird als Screenshot erstellt. Das heißt, Sie müssen nach spätestens drei Mona-

ten erneut eine Änderung vornehmen, was aber verschmerzbar ist. Nachdem Sie die App aus dem Store installiert haben, starten Sie diese auf dem iPhone. Anschließend nehmen Sie über *Settings* zunächst die Einstellungen vor. Klicken Sie dann auf *Library* und wählen Sie das Bild aus, das Sie im Lockscreen als Kalenderbild hinterlegen wollen.

Passend machen: So legen Sie die Einstellungen für Quick Calendar fest.

Haben Sie das Bild ausgewählt, sehen Sie über Preview eine Vorschau. Anschließend müssen Sie einen Screenshot erstellen. Dazu ist keine App erforderlich. Um vom lokalen Bildschirm einen Screenshot zu erstellen, halten Sie kurz die Standby-Taste des iPhones gedrückt. Drücken Sie zusätzlich kurz auf die Home-Taste in der Mitte des iPhones erstellt das iPhone einen Screenshot und speichert diesen bei den Fotos. Verlassen Sie jetzt die App und klicken auf *Einstellungen\Hintergrundbild*. Achten Sie aber darauf, den Screenshot im Preview-Fenster zu erstellen, da ansonsten auf dem Bild auch die Quick-Calendar-Einstellungen zu sehen sind. Wählen Sie den erstellten Screenshot aus, den Sie als Lockscreen nutzen wollen.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

TecChannel-Links zum Thema	Webcode	Compact
iPhone-Praxis: Kalender optimal synchronisieren	2033865	S.130
iPhone-Praxis: Datensicherung und -wiederherstellung	2033621	S.113
iPhone-Praxis: VPN richtig einrichten und nutzen	2033393	S.121

3.4 iPhone-Praxis: Einstellungen per Konfigurationsprogramm automatisieren

Setzen Unternehmen das iPhone für zahlreiche Anwender ein, ist es notwendig, Einstellungen, wie zum Beispiel die Anbindung an WLANs, VPNs und Sicherheitseinstellungen, automatisch zu erledigen. Die Installation von Apps lässt sich gleichfalls automatisieren. Beim Einsatz von Exchange Server 2007/2010 können Administratoren zwar über Exchange ActiveSync-Richtlinien zumindest Sicherheits- und E-Mail-Einstellungen automatisieren, aber für weitergehende Automatismen benötigen Administratoren zusätzliche Mittel.

Apple stellt dazu das kostenlose iPhone-Konfigurationsprogramm zur Verfügung (www.apple.com/de/support/iphone/enterprise/). Auch geübte Anwender, die Einstellungen lieber bequem am PC oder Mac vornehmen und dann auf ihr iPhone importieren, profitieren von dem Tool. Es steht für Windows und MacOS zur Verfügung und ermöglicht die weitreichende Konfiguration von iPhones.

3.4.1 Einstieg in das iPhone-Konfigurationsprogramm

Administratoren, die im Unternehmen zahlreiche iPhones verwalten müssen, finden bei Apple ausführliche Informationen zum Thema iPhone-Deployment im Unternehmen sowie den Download-Link zum iPhone-Konfigurationsprogramm und verschiedene Anleitungen.

Basisarbeit: Ein neues Konfigurationsprofil für das iPhone anlegen.

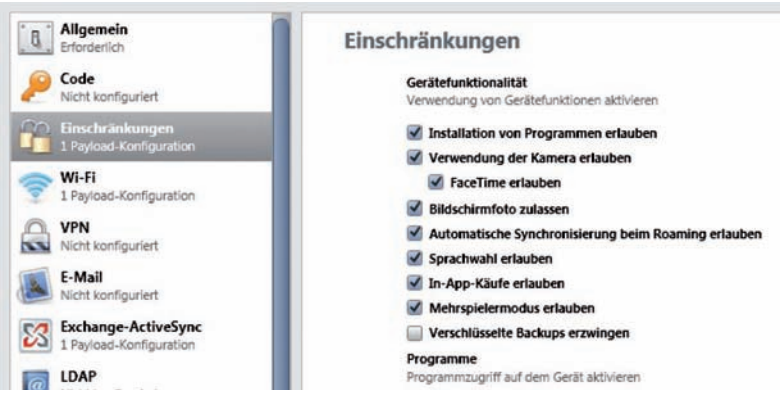
Das Tool ermöglicht die Erstellung, Verwaltung, Verschlüsselung und Bereitstellung von Profilen, die sich auf iPhones anwenden lassen. Diese Profile enthalten verschiedene Einstellungen für iPhones. Sie können problemlos auch mehrere Profile zur Verfügung stellen, die verschiedene Einstellungen auf dem iPhone anpassen können. Auch Apps lassen sich über das Tool verteilen, und die Installation von Apps durch Anwender lässt sich darüber verhindern.

Zusätzlich können Administratoren mit dem Tool Informationen von iPhones auslesen, zum Beispiel das Konsolenprotokoll, das ausführliche Daten enthält. Ab Version 3.1 unterstützt das iPhone-Konfigurationsprogramm das aktuelle iOS 4.x.

Grundlage des Tools sind Konfigurationsprofile. Hierbei handelt es sich um XML-Dateien, in denen Sie Einstellungen des iPhones vordefinieren und verteilen können. Einstellungen können zum Beispiel Sicherheitsrichtlinien, Einstellungen für VPNs und WLANs, die Anbindung an Exchange, sonstige E-Mail-Einstellungen sowie Zertifikate sein. Welche Möglichkeiten es gibt, sehen Sie direkt in der grafischen Oberfläche, die sich sehr leicht bedienen lässt.

3.4.2 Einschränkungen festlegen

Ab Version 3.1 unterstützt das Tool auch die neuen MDM (Mobile Device Management)-Funktionen in iOS sowie die funkgestützte Übertragung von Konfigurationsprofilen. MDM ermöglicht die Verwaltung und Konfiguration von verschiedenen Einstellungen auf iPhones, die Sie mit Konfigurationsprofilen steuern. Zusätzlich bietet diese Funktion das Auslesen von Informationen, wie zum Beispiel die genaue iOS-Version des iPhones, des Netzbetreibers, installierte Apps oder bereits gesetzte Einstellungen. Im englischsprachigen Apple-Forum finden Sie Hilfen und Tipps zum Tool (http://discussions.apple.com/).



Sicherheitshalber: Mit dem Konfigurationsprogramm können Sie diverse Funktionalitäten für den Nutzer einschränken.

Mit dem Tool lassen sich auch einzelne Funktionen im iPhone sowie installierte Apps deaktivieren und ausblenden. Die Installation neuer Apps lässt sich gleichfalls verhindern, ebenso die Anbindung an unsichere WLANs. Die entsprechenden Punkte finden Sie vor allem im Bereich Einschränkungen bei *Konfigurationsprofile*. Einschränkungen geben Sie als Konfigurationsprofil weiter, wie alle anderen Einstellungen auch. Sie haben in diesem Bereich verschiedene Möglichkeiten der Einschränkung. Setzen Sie eine bestimmte Einstellung, wenn Sie zum Beispiel die Verwendung von Safari oder Youtube verbieten, blendet das iPhone auch die entsprechenden Icons auf dem iPhone aus. Das Programm ist also für den Anwender nicht mehr sichtbar. Auf diese Weise unterbinden Sie zudem die Installation von Apps aus dem App-Store, da auch das App-Store-Icon auf dem iPhone nicht mehr verfügbar ist. Die Verwendung der Kamera oder das Erstellen von Bildschirmfotos lässt sich auf die gleiche Weise verhindern.

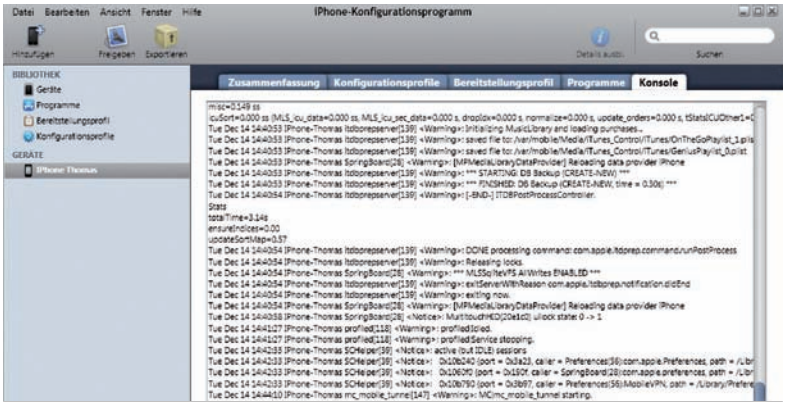
3.4.3 iPhone an das Konfigurationsprogramm anbinden

Wenn Sie das Konfigurationsprogramm auf einem PC oder Mac betreiben, auf dem Sie iTunes installiert haben, bindet sich das jeweilige iPhone automatisch in das Konfigurationsprogramm ein. Sobald Sie das iPhone mit dem Computer verbinden, liest das Konfigurationsprogramm die Daten aus.

Informativ: Im iPhone-Konfigurationsprogramm lassen sich die Geräteinformationen einlesen.

Auf verschiedenen Registerkarten erhalten Sie die zugewiesenen Konfigurations- und Bereitstellungsprofile sowie Informationen zu den installierten Apps und das Konsolenprotokoll mit Fehlern und Daten zum iPhone.

Auf der Registerkarte *Konfigurationsprofile* sehen Sie die Konfigurationsprofile, die Sie angelegt haben. Durch einen Klick auf Install überträgt das Tool die Einstellungen auf das iPhone. Sie haben auch die Möglichkeit, die Daten des iPhones zu speichern und per E-Mail zu versenden (*Datei\Per E-Mail senden*). Auf diese Weise lassen sich die Informationen auf anderen Computern mit installiertem Konfigurationsprogramm einlesen.



Was bisher geschah: Im Konfigurationsprogramm kann man sich das Konsolenprotokoll anzeigen lassen.

Die Erstellung eines Profils ist denkbar einfach. Sie klicken auf *Konfigurationsprofile*, legen einen Namen, eine Kennung und eine Beschreibung fest und klicken sich durch die verschiedenen Einstellungen. Im Fenster haben Sie die gleichen Möglichkeiten wie auf dem iPhone selbst. Sie sollten aber möglichst nicht alle Einstellungen in einem einzelnen Profil festlegen, sondern besser mehrere Konfigurationsprofile anlegen.

3.4.4 WLAN-Anbindung

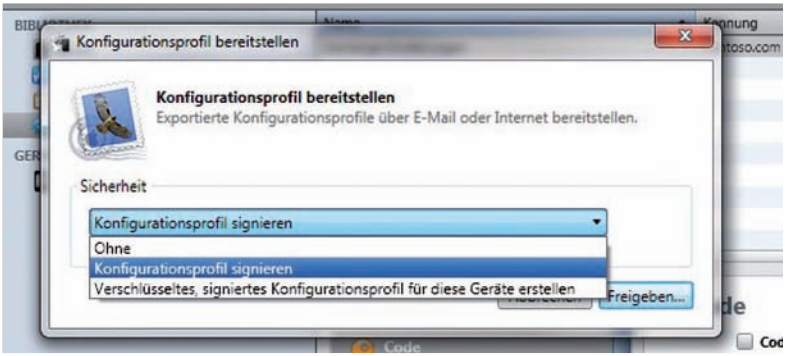
Vor allem die Konfiguration für Exchange-Postfächer oder die Anbindung an WLANs lässt sich mit dem Tool automatisieren. Die Anbindung an zertifikatsbasierte 802.1x-WLANs ist ebenfalls möglich. Die entsprechenden Einstellungen finden Sie wieder über *Konfigurationsprofile*. Im Bereich Wi-Fi geben Sie die SSID des WLANs ein und legen den Sicherheitstyp sowie das Kennwort fest. Abhängig von Ihrer Auswahl erscheinen weitere Felder, in die Sie Daten eintragen können.

Arbeiten Sie mit zertifikatsbasierten WLANs, müssen Sie das entsprechende Zertifikat über die Schaltfläche *Authentifizierung* auswählen. Damit Sie das Zertifikat auswählen können, müssen Sie dieses natürlich zuerst installieren. Die Zertifikate, die Sie mit dem Konfigurationsprogramm verteilen, steuern Sie über *Konfigurati-*

onsprofile\Zertifikate. Es lassen sich nur Zertifikate mit Kennwörtern integrieren, da das iPhone keine leeren Kennwörter ermöglicht. Wenn Sie ein korrektes Zertifikat ausgewählt und integriert haben, können Sie dieses in der Konfiguration für WLANs anbinden. Installiert ein Anwender auf dem iPhone dieses Konfigurationsprofil, übernimmt das iPhone das Zertifikat und die Einstellungen.

3.4.5 Konfigurationsprofile bereitstellen

Alle Einstellungen, die Sie in den Konfigurationsprofilen festlegen, sind auf den iPhones selbstredend erst dann verfügbar, wenn Sie das entsprechende Konfigurationsprofil übertragen haben. Der einfachste Weg ist das Versenden des Profils per E-Mail. Dazu müssen Sie nach den Einstellungen einfach auf *Freigeben* klicken und können dann das Profil per E-Mail versenden. Empfängt der Anwender die E-Mail auf dem iPhone, kann er das Profil einfach anklicken und die Einstellungen durch einen Klick installieren.



Zugänglich: Ein erstelltes Konfigurationsprofil können Sie auf unterschiedliche Weise bereitstellen.

Die Installation beginnt natürlich erst dann, wenn der Anwender nach dem Anklicken des Profils noch explizit Installieren auswählt. Eine weitere Möglichkeit, das Konfigurationsprofil zu veröffentlichen, ist der Download über eine Website oder die direkte Installation per Dateifreigabe. Dazu kopieren Sie die Datei des Profils an den entsprechenden Speicherort, auf den die Anwender dann zugreifen dürfen: Geben Sie ein Konfigurationsprofil frei, müssen Sie festlegen, welche Sicherheitsoption Sie einsetzen.

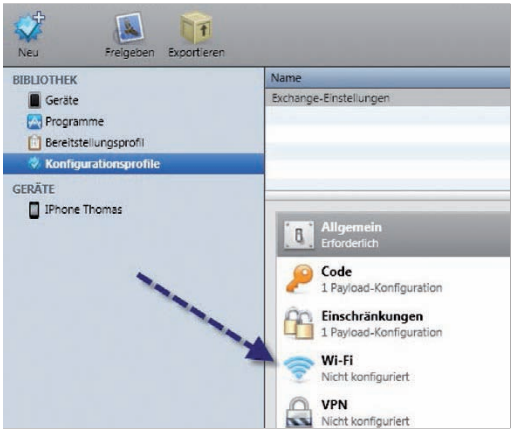
Sie haben hier drei verschiedene Möglichkeiten, um die Sicherheit des entsprechenden Konfigurationsprofils zu konfigurieren:

- **Ohne:** Die Konfigurationsdatei lässt sich auf jedem beliebigen iPhone einlesen. Sicherheitsrelevante Daten sind in der Datei aber aus Sicherheitsgründen nicht auslesbar.

- **Konfigurationsprofil signieren:** Das Profil wird signiert und lässt sich bei Änderungen an der Datei nicht auf dem Gerät installieren. Ein so installiertes Profil lässt sich nur aktualisieren, wenn Sie dieselbe Kennung verwenden und den gleichen PC mit gleichem iPhone-Konfigurationsprogramm verwenden.
- **Verschlüsseltes, signiertes Konfigurationsprofil für diese Geräte erstellen:** Wählen Sie diese Option aus, verschlüsselt das Konfigurationsprogramm die Datei noch. Das Profil lässt sich in diesem Fall aber nur von einem bestimmten Endgerät einlesen. Dazu müssen Sie das entsprechende iPhone einmal mit dem Computer verbinden und auswählen, damit das Konfigurationsprogramm Zugriff auf den Verschlüsselungscode des iPhones hat.

3.4.6 Verschiedene Konfigurationsprofile nutzen

Anstelle eines einzelnen, großen Konfigurationsprofils bietet es sich an, mehrere Profile zu erstellen, in denen Sie verschiedene Einstellungen vornehmen. Im Unternehmen ist es sicherlich sinnvoll, ein eigenes Konfigurationsprofil für Exchange zu erstellen und mit diesem die Exchange-Anbindung zu steuern. Das Gleiche gilt für weitere Profile für Sicherheit, WLAN und Zertifikaten.



Untergliederung: Im Konfigurationsprofil können Sie verschiedene Payload-Segmente konfigurieren.

Sicherheitseinstellungen, die Exchange betreffen, führen Sie zusätzlich mit Exchange-ActiveSync-Richtlinien durch. Apple unterscheidet zwischen Konfigurationsprofilen und Payload-Segmenten. Die gesamte XML-Datei enthält alle Einstellungen, die Sie im Profil festgelegt haben und die das Konfigurationsprogramm zur Verfügung stellt. Payload-Segmente sind einzelne Einstellungsbereiche im Konfigurationsprofil, zum Beispiel VPN, E-Mail oder Exchange-ActiveSync. Wenn Sie ein Konfigurationsprofil installieren, das nur ein bestimmtes Payload-Segment

steuert, zum Beispiel Exchange-ActiveSync, bleiben die anderen Einstellungen auf dem iPhone erhalten, etwa die installierten Zertifikate oder Einstellungen für VPNs. Ein Profil überschreibt nur die Einstellungen, die im entsprechenden Profil und im konfigurierten Payload-Segment ausgewählt und konfiguriert sind.

3.4.7 Mit Profilen arbeiten

Wenn Sie in einem Profil nicht alle Einstellungen eines Payload-Segments angeben, erhalten Anwender eine Information vom iPhone und müssen die fehlenden Daten selbst eingeben, zum Beispiel Benutzernamen und Kennwörter. Erstellen Sie ein Konfigurationsprofil, dann sollten Sie im Bereich *Allgemein* auf jeden Fall das Feld *Kennung* pflegen. Über diese Daten erkennt das iPhone, ob bereits Einstellungen und Profile mit gleichem Namen vorhanden sind. Die Kennung definiert sozusagen die Konfigurationsprofile und unterscheidet diese voneinander.

Entscheidend: In den allgemeinen Einstellungen für ein Konfigurationsprofil legen Sie auch die Kennung fest.

Stimmt die Kennung eines Profils mit der Kennung eines bereits installierten Profils überein, überschreibt das iPhone die bisherigen Einstellungen mit den neuen Einstellungen. Daher ist es wichtig, dass Sie für jeden Einstellungsbereich bestimmte Payload-Segmente verwenden und den Namen eindeutig festlegen. Sie können den Namen der Kennung frei bestimmen.

Ändern Sie jedoch Exchange-Einstellungen auf dem iPhone, muss zuerst ein existierendes Profil gelöscht werden, bevor Sie neue Einstellungen einlesen. Löschen Sie ein solches Konfigurationsprofil auf dem iPhone, dann löschen Sie damit auch die Exchange-Einstellungen und hinterlegten Exchange-Konten auf dem iPhone. In den allgemeinen Einstellungen eines Konfigurationsprofils können Sie im Bereich Sicherheit festlegen, ob ein Benutzer selbst ein installiertes Konfigurationsprofil löschen darf. Setzen Sie hier die Option *Nie*, lässt sich das entsprechende Konfigurationsprofil zwar mit neuen Einstellungen überschreiben, aber nicht vom Anwender löschen.

3.4.8 Aktualisieren und Löschen von Konfigurationsprofilen

Wenn Sie ein Konfigurationsprofil aktualisieren, müssen Sie dieses erneut freigeben und den Anwendern zuschicken. Anschließend müssen die Anwender das aktualisierte Profil installieren wie ein neues Profil. Bei diesem Vorgang überschreibt das iPhone die alten Einstellungen und setzt die neuen vom aktualisierten Profil. Allerdings müssen dazu die Kennung sowie die Signatur übereinstimmen, wenn Sie diese Option aktiviert haben. Einstellungen, die Sie über ein Konfigurationsprofil vorgeben, lassen sich auf dem iPhone nicht mehr manuell anpassen. Für den Fall, dass Sie ein Konfigurationsprofil löschen, entfernt das iPhone alle Einstellungen, die das Profil betreffen, und alle Einstellungen der verschiedenen Payload-Segmente, die Sie im Profil gesetzt haben. Von diesem Löschvorgang können auch E-Mails betroffen sein, die zu dem Konto gehören, das Sie mit dem Profil auf dem iPhone konfiguriert haben.

3.4.9 Sicherheitseinstellungen beachten

Im Bereich Code des Konfigurationsprofils legen Sie Einstellungen fest, die für Kennwörter auf dem iPhone gelten. Sie können diese Einstellungen mit Exchange ActiveSync-Richtlinien kombinieren. Das iPhone verwendet automatisch eine Kombination der beiden Richtlinien und berücksichtigt dabei die sichere Einstellung der entsprechenden Richtlinie.

Zusätzlich zu den Einstellungen des Konfigurationsprofils haben Sie mit Exchange-ActiveSync-Richtlinien noch folgende Möglichkeiten:

- Fernlöschen (Remote Wipe)
- Erzwingung eines Codes zum Sperren des Gerätes
- Mindestlänge für Kennwörter
- Mindestanzahl/Maximale Anzahl falscher Eingaben, bis sich das Gerät selbst löscht oder sperrt
- Kennwort muss Ziffern und Buchstaben erhalten
- Inaktivitätszeit
- Einfaches Kennwort zulassen
- Kennwortablauf und Kennwortverlauf
- Aktualisierungsintervall für Richtlinien
- Mindestanzahl komplexer Zeichen im Kennwort
- Kamera zulassen oder sperren

Ausführliche Informationen zur Anbindung des iPhones an Microsofts Mail-Server liefert Ihnen der Beitrag iPhone-Praxis: Anbindung an Exchange und SharePoint Server (Webcode **2032686**).

Thomas Joos

3.5 iPhone-Praxis: Anbindung an Exchange und SharePoint Server

Die Anbindung des iPhone an Exchange über ActiveSync ist genauso möglich wie die Verbindung zu SharePoint. Kosten entstehen dabei keine, da die notwendigen Tools gratis zur Verfügung stehen oder im iPhone schon integriert sind. Anwender können entweder direkt mit Safari eine Verbindung mit SharePoint aufbauen, oder sie verwenden spezielle Apps, im Fall von Exchange die integrierte E-Mail-Funktion. Exchange Server 2010 und SharePoint 2010 arbeiten eng zusammen, vor allem, wenn es um E-Mail-Nachrichten für Aufgaben, Systembenachrichtigungen und Informationen geht. Aus diesem Grund ergibt es durchaus Sinn, im Unternehmen die Anbindung von iPhones an Exchange und SharePoint zu berücksichtigen, am besten parallel. SharePoint sendet dann E-Mails über Exchange an die Postfächer von Anwendern, die diese E-Mails dann wiederum mit dem iPhone empfangen und auf SharePoint zugreifen können, entweder über Apps oder den Browser.

Apropos Apps: Im Beitrag Die besten Business-iPhone-Apps (Webcode **2028201**) haben wir eine Bestenliste essentieller Business-iPhone-Apps zusammengestellt, die sich zum produktiven Arbeiten eignen und den Anwender sinnvoll unterstützen. Einen grundlegenden Workshop zum Thema Synchronisieren eines Smartphones mit einem Exchange-Postfach bietet Ihnen der Beitrag Mobiler Zugriff auf Exchange-Postfächer mit Exchange ActiveSync (Webcode **2028696**).

3.5.1 iPhone und Exchange ActiveSync

Apple hat die Anbindung von Exchange ActiveSync bei Microsoft lizenziert und im iOS eingebunden. Das bedeutet, Sie können Apple iPhones mit Exchange synchronisieren, ohne den Umweg über IMAP, POP3 oder Produkte von Drittherstellern gehen zu müssen. Die Anbindung erfolgt dazu direkt im iPhone. Mit Exchange ActiveSync (EAS) können Anwender ihr Postfach mit E-Mails, Kontakten und Kalendereinträgen über das Telefonnetz synchronisieren, E-Mails empfangen und E-Mails senden. Verbindet sich ein iPhone mit dem internen Firmen-WLAN, verwendet es zur Synchronisierung automatisch die leistungsfähige und günstige Netzwerkverbindung. Sobald das iPhone ein WLAN findet, erhalten Sie ein Informationsfenster und können das WLAN im iPhone konfigurieren. Sie finden diese Optionen später auch über *Einstellungen\Wi-Fi*. Sobald Sie einmal ein WLAN konfiguriert haben, verbindet sich das iPhone künftig automatisch mit diesem Netzwerk. Das funktioniert auch, wenn Sie mehrere WLANs einbinden. Eine erfolgreiche Anbindung sehen Sie im oberen Bereich am WLAN-Symbol links neben der Uhr. Unternehmen, die Exchange einsetzen, haben meistens auch die Möglichkeit geschaffen, über das Internet mit Outlook Web App (vor Exchange Server 2010 noch als Outlook Web Access bekannt), Outlook Anywhere (auch

RPC über HTTPS genannt) oder auch Exchange Active Sync zuzugreifen. Um ein iPhone entsprechend zu konfigurieren, müssen Sie keinerlei Drittprodukte installieren. Die Anbindung ist denkbar einfach. Sie haben ebenfalls die Möglichkeit, mehrere verschiedene Postfächer, auch verschiedene Exchange-Postfächer, auf unterschiedlichen Servern einzubinden.

Präferenzen: Verbindet sich ein iPhone mit dem internen Firmen-WLAN, verwendet es zur Synchronisierung automatisch die leistungsfähige und günstige Netzwerkverbindung.

Das iPhone kommt auch problemlos mit selbst signierten Zertifikaten auf Exchange-Servern zurecht. Hier erscheint bei der Anbindung lediglich ab und zu eine Warnung, dass das iPhone den Server nicht verifizieren kann. Diese können Sie allerdings bestätigen, sodass das iPhone selbst signierte Zertifikate automatisch akzeptiert. Bestätigen Sie diese Meldung, bindet Sie das iPhone dennoch an.

3.5.2 Schritt-für-Schritt-Anbindung

Auf dem iPhone sind folgende Schritte notwendig, um eine Anbindung an Exchange durchzuführen:

1. Rufen Sie *Einstellungen* auf.
2. Wählen Sie in den Einstellungen die Option *Mail, Kontakte, Kalender*. Wollen Sie später Einstellungen ändern, nehmen Sie das wieder in diesem Bereich vor.
3. Wählen Sie im neuen Fenster *Account hinzufügen*. Einmal angebundene Accounts sind künftig hier zu sehen.
4. Hier sehen Sie alle Anbieter, die das iPhone unterstützt. Anwender, deren Unternehmen auf Exchange Server 2003/2007 oder 2010 setzen, verwenden hier *Microsoft Exchange*.
5. Im neuen Fenster tragen Sie die Daten des Exchange-Kontos ein:

- E-Mail: Hier tragen Sie die E-Mail-Adresse ein, die Sie im iPhone einbinden wollen.

- Domain: Hier tragen Sie den Namen der Windows-Domäne ein, an der Sie sich authentifizieren wollen. Bei der Anbindung an ein 1&1-Exchange-Postfach ist das zum Beispiel die Domäne exchange.

iPhone und Exchange ActiveSync: Auswählen der E-Mail-Kontenkonfiguration.

- Benutzername: Hier geben Sie den Namen ein, mit dem Sie sich an der Domäne anmelden, zum Beispiel auch am lokalen Computer. Bei der Anbindung eines 1&1-Postfaches verwenden Sie hier den gleichen Namen, den Sie auch in Outlook einsetzen.
- Kennwort: Kennwort des Benutzerkontos
- Beschreibung: Hier tragen Sie ein, was das iPhone anzeigen soll, wenn Sie in die E-Mail-App gehen, um das E-Mail-Konto abzurufen. Verwenden Sie also keine zu langen Namen.

6. Klicken Sie anschließend auf *Weiter*.
7. Im nächsten Schritt blendet das iPhone das Feld *Server* ein. Hier tragen Sie den Namen des Servers ein, mit dem Ihr Exchange-Server an das Internet angebunden ist. In den meisten Fällen handelt es sich hier um den gleichen Namen, den Sie auch in OWA verwenden. Beim Einsatz von 1&1 ist das zum Beispiel profimailer.de. Neben einem Namen können Sie hier natürlich auch eine IP-Adresse eingeben. Ist das iPhone mit einem WLAN verbunden, funktioniert auch die interne Anbindung.

iPhone und Exchange ActiveSync: Auswählen der zu synchronisierenden Objekte.

8. Haben Sie den Namen eingegeben, klicken Sie wieder auf *Weiter*, um die Anbindung abzuschließen. Erhalten Sie eine Meldung, dass das iPhone den Server nicht verifizieren kann, bestätigen Sie diese einfach.

9. Im nächsten Schritt wählen Sie aus, was Sie synchronisieren wollen, und klicken anschließend auf *Sichern*, um die Konfiguration zu speichern.

3.5.3 Anpassen der Konfiguration

Erhalten Sie Meldungen, dass das iPhone das Konto nicht überprüfen kann, bestätigen Sie diese und fahren Sie mit der Einrichtung fort. In den meisten Fällen liegt es am Zertifikat des Servers, dessen Zertifizierungsstelle das iPhone nicht vertraut. Sie können über *Details* das Zertifikat anzeigen lassen und es akzeptieren.

Über *Mehr Details* lassen Sie sich die Daten des Zertifikats anzeigen und können diese überprüfen, bevor Sie die Verbindung akzeptieren. Mit der Safari-Version können Sie auch auf OWA zugreifen. Allerdings lässt sich dann nur die eingeschränkte Light-Version von Outlook Web App nutzen. Das Lesen von E-Mails in OWA ist nicht so bequem wie über die E-Mail-Funktion des iPhones. Der direkte Zugriff per Exchange ActiveSync ist wesentlich effizienter. Allerdings können Sie über die Optionen in OWA zum Beispiel Einstellungen für Ihr Exchange-Postfach ändern, was in den E-Mail-Einstellungen des iPhones nicht möglich ist. Auf diese Weise aktivieren Sie zum Beispiel den globalen Abwesenheitsassistenten für Ihr Postfach bequem über das iPhone oder konfigurieren weitere Einstellungen.

Haben Sie die erste Einrichtung abgeschlossen, sollten Sie die Einstellungen verfeinern. Rufen Sie dazu wieder E*instellungen\Mail, Kontakte,Kalender* auf. Im Bereich *Accounts* sehen Sie für jedes angebundene Postfach einen eigenen Bereich.

Hier zeigt das iPhone als Namen für das Postfach die Beschreibung an, die Sie eingegeben haben. Haben Sie das entsprechende Konto aufgerufen, können Sie für jedes einzelne Exchange-Postfach Einstellungen vornehmen. Sie können an dieser Stelle zum Beispiel konfigurieren, von welchem Zeitraum das iPhone die E-Mails auf dem Server abruft. An dieser Stelle lassen sich einzelne Konten auch wieder löschen. Im Bereich *Mail* in den Einstellungen von *E-Mail, Kontakte und Kalender* können Sie darüber hinaus Einstellungen vornehmen, die für alle angebundenen Postfächer gelten. Hier geben Sie zum Beispiel auch die Signatur an, die das iPhone automatisch an jede gesendete E-Mail hängt. Außerdem wählen Sie an dieser Stelle das Standardkonto aus, von dem aus Sie E-Mails schreiben.

3.5.4 Aufgaben und Notizen synchronisieren

Leider unterstützt das iPhone keine Synchronisierung von Exchange-Aufgaben oder Notizen. Hier bietet es sich aber an, dass Sie die App iMExchange 2 installieren. Diese gibt es als kostenlose Testversion oder als Vollversion im App-Store für knapp sechs Euro. Mit dieser App können Sie künftig problemlos Ihre Aufgaben und Notizen mit Exchange synchronisieren, auch über Exchange ActiveSync. Sie können mit der App einige Synchronisierungen kostenlos durchführen und dann entscheiden, ob Sie die App kaufen wollen.

iMExchange 2: Mit der zusätzlichen App lassen sich Aufgaben und Notizen synchronisieren.

3.5.5 E-Mails abrufen, lesen und schreiben

Der Vorteil von Exchange Active Sync ist, dass Sie durch den Push der E-Mails keine manuelle Synchronisierung durchführen müssen. Das iPhone informiert Die im E-Mail-Bereich, wenn neue E-Mails eingegangen sind. Sobald Sie aber den Posteingang öffnen, führt das iPhone auch eine manuelle Synchronisierung durch.

Wenn Sie auf den E-Mail-Bereich klicken, zeigt das iPhone alle angebundenen Konten an, und Sie sehen, für welches Konto E-Mails eingegangen sind. Auch hier trennt das iPhone auf Wunsch zwischen verschiedenen Exchange-Konten, zeigt aber auch alle E-Mails aller angebundenen E-Mail-Konten auf einmal an, wenn Sie auf *Alle* klicken. Haben Sie ein Konto aufgerufen, sehen Sie die E-Mails und können diese durch Anklicken öffnen. Setzen Sie im Unternehmen auch SharePoint 2010 ein, können Sie die E-Mails von SharePoint lesen und in Safari direkt die SharePoint-Verbindung öffnen, indem Sie die entsprechenden Links auswählen.

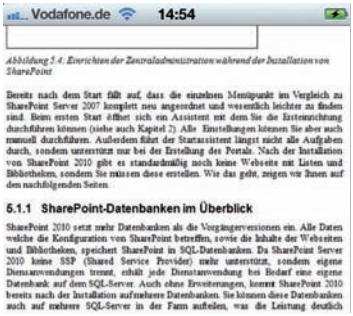
E-Mails, die Sie senden, sind zudem in den gesendeten Elementen im Exchange-Postfach auf dem Exchange-Server verfügbar, also auch über Outlook und Outlook Web App. Löschen Sie eine E-Mail auf dem iPhone, ist diese auf dem Server ebenfalls gelöscht, da sich das iPhone mit dem Server regelmäßig synchronisiert. Rufen Sie die E-Mails ab, können Sie im unteren Bereich bei Accounts die einzelnen Konten aufrufen. Setzen Sie Exchange ein, sehen Sie hier auch die anderen Ordner Ihres Exchange-Postfaches.

3.5.6 iPhone und SharePoint 2010

Sie können mit dem iPhone auch auf Daten von SharePoint-2010-Servern zugreifen. Microsoft unterscheidet zwei Stufen bei den Webbrowsern für die Unterstützung von SharePoint 2010. Browser der Ebene 1 können alle Funktionen in SharePoint nutzen, einschließlich der Zentraladministration.

Im Zugriff: Mit dem iPhone können Sie auch SharePoint 2010 nutzen.

Zu diesen Browsern gehören Internet Explorer 7, Internet Explorer 8 und Mozilla Firefox ab Version 3.x. Die 64-Bit-Versionen von Windows 7 und Windows Vista werden nicht in allen Funktionen uneingeschränkt unterstützt, was an der etwas anderen Struktur des Betriebssystems liegt.



Nutzung: Das Lesen von Word-Dokumenten aus SharePoint-Bibliotheken auf dem iPhone klappt ebenfalls.

Browser der Ebene 2 bieten Grundfunktionen und sind bei der Verwendung von SharePoint eingeschränkt, lassen sich aber nutzen. Zu diesen Browsern gehören Apple Safari 4.x und Mozilla Firefox, wenn Sie diesen unter Apple Mac OS X Leopard oder unter Linux betreiben. Auch der Zugriff über iPad und iPhone funktioniert. Sie können hier entweder angepasste Apps herunterladen oder den integrierten Browser Safari im iPhone oder iPad benutzen.

Neben den Lesen von Links können Sie auf diese Weise auch auf Bibliotheken und Dokumente zugreifen, ferner auf Word-Dateien innerhalb Bibliotheken. Sie müssen dazu keine Programme oder Apps installieren, auch wenn der Zugriff mit Apps wesentlich komfortabler für Anwender ist.

3.5.7 Apps und SharePoint 2010

Es gibt mehrere Apps, die SharePoint unterstützen, darunter auch die neue Version SharePoint 2010. Eine bekannte und kostenlose App ist Moshare, die die Anbindung an SharePoint 2010 ebenfalls problemlos unterstützt. Vor allem die Anzeige

von Kalendern ist über die App besser gelöst als der Zugriff über den Safari-Browser. Moshare eignet sich allerdings, wie die anderen kostenlosen Apps, nur für den lesenden Zugriff auf Word-, PowerPoint, Excel-, PDF-, Text-Dokumente und Bilder. Visio-Zeichnungen oder InfoPath-Formulare können Sie nicht lesen.

Lesezugriff: Mit Moshare lassen sich SharePoint-Kalender anzeigen.

Für den Zugriff auf im Browser integrierte InfoPath-Formulare können Sie Safari verwenden. Aber auch hier funktionieren nicht alle. Moshare kann problemlos über das Internet auf SharePoint zugreifen, allerdings müssen Sie dazu die SharePoint-Site im Internet veröffentlichen oder per VPN zugänglich machen. Ist das iPhone per WLAN verbunden, funktioniert natürlich auch der interne Zugriff per WLAN und interner IP-Adresse. Eine weitere kostenlose App, mit dem sich das iPhone mit SharePoint verbindet, ist SharePlus Lite Office Mobile Client. Beide Apps finden Sie im App-Store zum kostenlosen Download. Es spricht generell nichts dagegen, mehrere Apps zu testen, da sich die Konfigurationen und der Betrieb der beiden Apps gegenseitig nicht stören.

Konfiguration: Vor dem Verbindungsaufbau zu SharePoint konfigurieren Sie die Anmeldedaten an die SharePoint-Site.

Die Bedienung beider Apps ist sehr einfach, und auch das Bewegen durch die SharePoint-Daten stellt kein größeres Problem dar. Geübte Anwender kommen

schnell mit der App zurecht. Rufen Sie Moshare auf, besteht der erste Schritt darin, dass Sie eine Seite konfigurieren sowie die Anmeldedaten an SharePoint übergeben. Achten Sie darauf, die Anmeldedaten im Format *<Domäne>\<Benutzer>* einzugeben. Sie können in Moshare zudem mehrere verschiedene SharePoint-Websites einbinden, auch mit verschiedenen Anmeldedaten. Auf diese Weise können Sie sich mit wenigen Klicks erst mit einem Benutzerkonto und dann als Administrator einloggen.

3.5.8 Apps nutzen

Nach der Konfiguration zeigt Moshare alle angebundenen Seiten an, wenn Sie die App starten. Klicken Sie auf eine Seite, baut Moshare eine Verbindung mit dem entsprechenden Server auf und zeigt die Listen, Websites und Bibliotheken an. Auch neue Objekte in den Bibliotheken lassen sich mit Moshare filtern. Wenn Sie eine Bibliothek aufrufen, sehen Sie alle enthaltenen Dokumente – hier auch ein Icon zu der entsprechenden Anwendung, die mit dem Dokument verknüpft ist.

Klicken Sie ein Dokument an, öffnet es Moshare in seinem Fenster, und Sie können den Text lesen, auch wenn es sich um ein Word-Dokument handelt. Über eine eigene Schaltfläche im unteren Bereich des Readers können Sie den Link zum Dokument kopieren oder das Dokument per E-Mail senden.

Haben Sie das iPhone an Exchange eingebunden, können Sie auf diese Weise bequem die App mit der E-Mail-Funktion des iPhones verknüpfen und geöffnete Dokumente aus der SharePoint-Bibliothek per E-Mail versenden. Neben Dokumenten zeigt die App auch Kalenderlisten in SharePoint an, und zwar wesentlich schöner als über den Browser.

Mit SharePlus Lite Office Mobile Client gehen Sie ähnlich vor. Auch hier müssen Sie zuerst die Daten für die Anmeldung eingeben und können dann in der App mit Ihren Benutzerinformationen in SharePoint Daten abrufen. Das Lesen von Dokumenten ist mit dieser App ebenfalls problemlos möglich.

SharePlus Lite Office Mobile Client unterstützt neben der standardmäßige Windows-Authentifizierung auch die formularbasierte Authentifizierung in SharePoint 2010. Auch die App iShare ist kostenlos, aber mittlerweile veraltet und nicht kompatibel mit iOS4 und vor allem nicht mit SharePoint 2010. Weitere Apps, die allerdings kostenpflichtig sind, finden Sie über PocketPoint, SharePlus Office Mobile Client, iSP-Browser und Attaché SharePoint Client.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

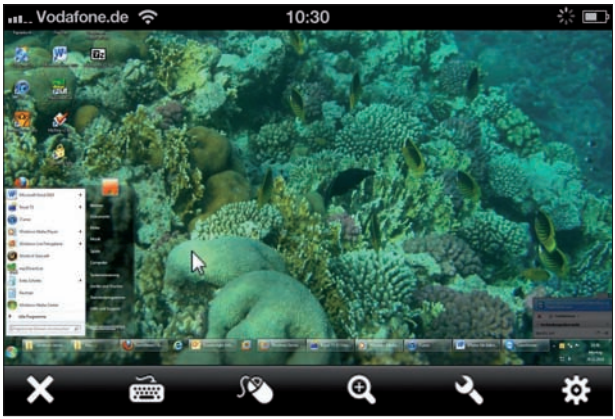
Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

3.6 iPhone-Praxis: Apps für Admins

Administratoren erhalten mit dem iPhone umfangreiche Möglichkeiten, das Netzwerk auch von unterwegs im Blick zu behalten und wichtige Aufgaben durchzuführen. Viele der nachfolgend erwähnten Apps sind kostenlos und unterstützen den Administrator bei alltäglichen Aufgaben wie der Fernwartung von Windows-Rechnern, auch über das Internet und über Firewalls hinweg. Ebenso existieren Programme für Smartphones für Messungen im Netzwerk oder den Verbindungsaufbau per RDP. Neben Fernwartungs-Tools finden Administratoren im App-Store aber auch zahlreiche andere Tools, die das iPhone zu einem echten Werkzeug für den IT-Alltag machen.

3.6.1 Fernwartung in Windows-Netzwerken

Mit der kostenlosen App Teamviewer können sich Admins mit dem iPhone vollkommen problemlos mit Windows-Rechnern verbinden, beispielsweise, um Anwendern bei der Behebung von Fehlern zu helfen. Es besteht auch die Möglichkeit, den ferngewarteten Rechner zu steuern. Zwar können Sie keine Daten austauschen, zumindest nicht mit der kostenlosen Version, aber Sie können zum Beispiel über den Windows-Explorer des ferngesteuerten Rechners auf Dokumente zugreifen und diese auf dem iPhone lesen.



Teamviewer: Mithilfe der App können Sie problemlos auf einen Windows-PC zugreifen.

Die bekannte Freeware Teamviewer gibt es auch direkt für Windows. Damit eine Fernwartung möglich ist, muss der Anwender auf dem Gast-PC Teamviewer herunterladen und starten. Eine Installation der Freeware ist möglich, aber nicht Voraussetzung für eine Fernwartung. Anschließend erhält der Anwender eine ID und ein Kennwort, das er dem Admin mitteilen muss. Der Admin gibt die Daten in sei-

ner Teamviewer-App ein und verbindet sich mit dem Rechner. In den umfangreichen Optionen der App lassen sich Verbindungen auch fest hinterlegen. Auf diese Weise kann zum Beispiel die App eine Verbindung mit dem Admin-PC aufbauen, ohne dass ein Anwender vor dem Rechner sitzt.

Die Fernwartung mit der kostenlosen Version ist aber nur für Privatanwender erlaubt! Professionelle User können die App natürlich trotzdem installieren und testen. Unternehmensanwender müssen diese aber lizenzieren, wenn sie zufrieden sind. Der große Vorteil dieser Lösung ist die vollkommen unkomplizierte Fernwartung, auch über das Internet und durch Firewalls. Admins, die Teamviewer regelmäßig nutzen wollen, sollten sich die Pro-App kaufen. Diese erlaubt das Zugreifen auf beliebig viele Client-Computer, die wiederum keine Lizenz benötigen. Die App gibt es übrigens auch für Android-Handys und für das iPad.

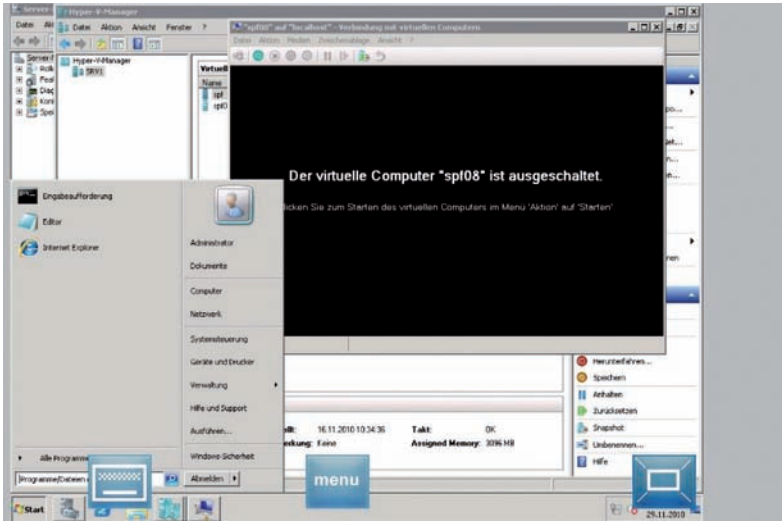
Administratoren, die auf VNC setzen, sollten sich die kostenlose App Mocha VNC Lite ansehen. Diese kann per VNC eine Verbindung zu Windows-Computern aufbauen. Dazu muss natürlich der VNC-Server auf dem entsprechenden Gerät installiert sein. Allerdings ist die App nicht gerade sehr zuverlässig. Wer VNC professionell und regelmäßig nutzt, setzt besser auf die kostenpflichtige App VNC Viewer. Diese ist im App-Store für 7,99 Euro zu haben.

3.6.2 RDP-Sitzungen vom iPhone aus

Administratoren in Windows-Netzwerken benötigen für die Fernwartung in den meisten Fällen das RDP-Protokoll. Auch hierfür gibt es verschiedene Apps, teilweise kostenlos. Eine der bekanntesten ist iTAP RDP für 9,99 Euro. Sie können mit der App per RDP auf Rechner mit Windows XP/Vista und Windows 7 zugreifen, aber natürlich auch auf Server mit Windows Server 2000/2003/2008/2008 R2. Natürlich lassen sich zudem Server mit SBS 2000/2003/2008 und sowie der neue Small Business Server 2011 verwalten.

Administratoren, die Linux-Server verwalten müssen, freuen Sie über die Unterstützung von XRDP. Sehr interessant, vor allem für Anwender, die viel unterwegs sind, ist die Unterstützung von Remote-Desktop-Gateways in der App. Mit diesen Gateways stellen Sie RDP-Server über das Internet sicher zur Verfügung. Das heißt, Sie können mit der App auch über das Internet auf Ihre Server per RDP zugreifen, vorausgesetzt, Sie betreiben ein RDP-Gateway im Unternehmen.

Es gibt noch die kostenlose App Mocha Remote Desktop Lite, allerdings unterstützt diese App offiziell nur Windows-Clients und keinen RDP-Zugriff auf Windows Server-Systeme. Geben Sie jedoch den Benutzernamen mit *Domäne\Benutzer* ein, können Sie problemlos auch auf Windows-Server Systeme, zum Beispiel Windows Server 2008 R2, zugreifen. Administratoren sollten daher die kostenlose App auf jeden Fall testen, da sie für schnelle Administrationsaufgaben oder Serverneustarts Gold wert sein kann.



Praktisch: Mit iTAP RDP lassen sich RDP-Sitzungen vom iPhone zum Windows Server 2008 realisieren.

Die App speichert die letzte Verbindung und ermöglicht den erneuten Verbindungsaufbau durch Antippen. Über Menu können Sie eigene Verbindungen konfigurieren, inklusive der Anmeldedaten an den Servern. Die Konfiguration ist sehr simpel. Sie klicken einfach auf eine noch nicht konfigurierte Verbindung und geben im Fenster die IP-Adresse des Rechners, den RDP-Port (standardmäßig 3389), den Benutzer, das Kennwort und eine Beschreibung ein. Auch die Auflösung des Bildschirms steuern Sie auf diese Weise sehr unkompliziert.

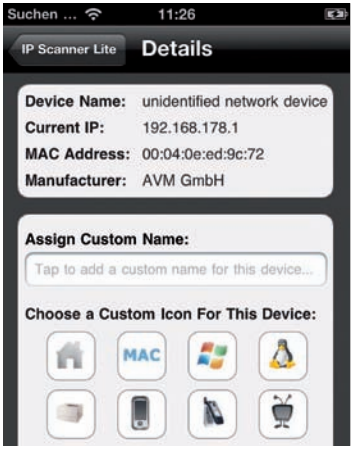
3.6.3 Apps für Netzwerker – Ping, Telnet, Netzwerk-Scanner

Eine sehr interessante App für Admins ist das kostenlose Network Ping Lite. Ist das iPhone per WLAN verbunden, können Sie mit der App einzelne Netzwerkgeräte oder ein ganzes Subnetz anpingen. Aktive Geräte hebt die App grün hervor.

Bereits im Startfenster legen Sie fest, ob Sie ein einzelnes Gerät oder alle Geräte in einem Subnetz anpingen wollen. Über die Startseite können Sie auch auswählen, ob Sie eine Route anzeigen oder eine Telnet-Verbindung öffnen wollen. Außerdem zeigt das iPhone auf dem Fenster die lokale IP-Adresse sowie die IP-Adresse des Geräts im Internet an. Neben dem einfachen Pingen von Geräten und Subnetzen starten Sie mit der App auch die Funktion zum Tracerouten und/oder den Verbindungsaufbau per Telnet. Auf diese Weise können Sie zum Beispiel einfache Verbindungen zu Routern oder Servern aufbauen. Die App sollte also zum Werkzeugkasten eines jeden Administrators gehören.

Anwesenheitskontrolle: Per App lassen sich Geräte im Netzwerk anpingen.

Ebenfalls eine sehr wertvolle und kostenlose App ist der IP Network Scanner Lite. Starten Sie diese App, beginnt diese sofort mit dem Scanvorgang. Dieser listet alle gefundenen Geräte, teilweise auch nach Namen und Typ, auf. Dazu scannt die App das Netzwerk und versucht, von den gefundenen Geräte Informationen zu erhalten. Sie können den Geräten nach dem Scanvorgang ein Icon und eine Funktion zuweisen, sodass diese beim nächsten Scanvorgang berücksichtigt wird. Dazu klicken Sie nicht identifizierte Geräte an und geben die Daten an, die die App künftig anzeigen soll. Für diese Geräte können Sie auch einen Namen vergeben.



Identifizierung: Netzwerkgeräte lassen sich per App anzeigen.

Auf diese Weise erhalten Sie eine schnelle Übersicht über die Geräte, die sich in Ihrem Netzwerk befinden. Bei einem Scanvorgang sehen Sie sofort, ob ein neues Gerät gefunden wird. Das Tool kann dabei auch Hersteller, MAC-Adresse, IP-Adresse

und den internen Namen anzeigen, liefert also wichtige Informationen für Admins. Über Tools lassen Sie die Liste in ein Textformat exportieren. Haben Sie das iPhone an einen E-Mail-Account angebunden, erstellt die App automatisch eine neue E-Mail mit dem Inhalt des Scanergebnisses als Text. Die kostenlose Lite-Version des Apps ist auf fünf Geräte limitiert. Für 3,99 Euro bekommen Sie die Vollversion, die keine Limits hat.

Auskunft: Es lassen sich wichtige Netzwerk- und Internetinformationen abrufen.

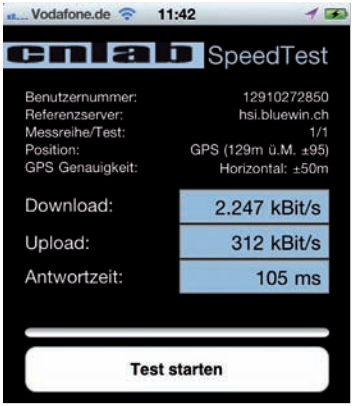
Ebenfalls kostenlos und hilfreich ist die App Network Utility. Diese kann den Status eines Servers überprüfen, pingen sowie WHOIS-Abfragen und Port-Scans durchführen. Durch Verwendung von Google Maps kann das Tool sogar die geografische Lage eines Servers anzeigen. Auch eine Namensauflösung per DNS ist möglich. Die Bedienung ist sehr einfach: Sie geben im Feld *Remote Hostname or IP Address* einfach die IP-Adresse oder den Servernamen des Servers ein, den Sie testen wollen. Im unteren Bereich sehen Sie dann die verschiedenen Felder, mit denen Sie die eingegebene Adresse testen können.

3.6.4 Netzwerke planen und testen

Netzwerkplaner, die IP-Subnetze planen, benötigen in den meisten Fällen entsprechende Unterstützungs-Tools. Auch in diesem Bereich gibt es zahlreiche kostenpflichtige, aber auch kostenlose Apps, die beim Berechnen von Subnetzen Unterstützung liefern. Die kostenlose App Subnet Calc unterstützt bei der Berechnung von IP-Subnetzen. Die kostenlose App Net Calc hilft ebenfalls bei der Berechnung von IPv4-Netzwerken. Der parallele Einsatz der beiden Apps ist durchaus möglich. Wer Subnetze plant oder sich auf Prüfungen vorbereiten muss, findet mit den beiden Apps eine wertvolle Unterstützung.

Admins, die ihre aktuelle Geschwindigkeit im Mobilnetz oder Internet per WLAN testen wollen, zum Beispiel vor einer Fernwartung oder Datenübertragung, finden

mit der kostenlosen App cnlab SpeedTest eine brauchbare Lösung. Der Test ist einfach aufgebaut, grafisch ansprechend und bietet die notwendigen Informationen über die aktuelle Netzwerkgeschwindigkeit.



Da geht was: Das Tool zeigt die aktuelle Verbindungsgeschwindigkeit an.

Das Tool misst Mobilnetze, aber auch die Anbindung über ein WLAN an das Internet. Das heißt: Sie erhalten nicht die Geschwindigkeit des aktuellen Netzwerkes, sondern Ihrer Anbindung an das Internet. Der Umgang ist sehr einfach. Sie starten die App und klicken auf *Test starten*. Nach dem Start wählen Sie aus, wo Sie den Test durchführen, also unterwegs, in einem Zug oder einem Gebäude. Anschließend zeigt die App die aktuelle Geschwindigkeit an. Im unteren Bereich sehen Sie bereits durchgeführte Testergebnisse, sodass Sie vergleichen können. Ganz genau ist der Test nicht, aber er zeigt Ihnen in etwa, wie es um die aktuelle Geschwindigkeit bestellt ist.

3.6.5 Screenshots für Anwender erstellen

Das schnelle Verfassen von Anleitungen für Anwender gehört immer wieder zum Alltag von Administratoren. Beispielsweise, um zu zeigen, wie man ein iPhone an den eigenen Exchange-Server anbindet. Dazu ist es oft notwendig, Screenshots zu erstellen, um diese in die Anleitung einzubauen. Sie benötigen mit einem iPhone dazu nicht mal eine App. Um vom lokalen Bildschirm einen Screenshot zu erstellen, halten Sie kurz die Stand-by-Taste des iPhones gedrückt.

Diese finden Sie oben rechts. Drücken Sie zusätzlich kurz auf die Home-Taste in der Mitte des iPhones; während Sie die Stand-by-Taste gedrückt halten, erstellt das iPhone einen Screenshot und speichert diesen bei den Fotos. Um auf das Bild zuzugreifen, verbinden Sie das iPhone mit einem Rechner. Ist iTunes auf dem PC installiert, finden Sie im Windows Explorer bei *Tragbare Geräte* einen Link direkt

zum Fotospeicher des iPhones. Hierüber können Sie auf die Fotos im iPhone zugreifen. Wenn Sie einen Screenshot erstellen, während das iPhone mit dem Computer verbunden ist, sehen Sie das neue Foto allerdings erst dann, wenn Sie das Verbindungskabel des iPhones kurz abziehen und wieder verbinden. Auf diese Weise können Sie sehr einfach und effizient Anleitungen für das iPhone schreiben.

3.6.6 Sicherheit für Admins

Arbeiten Sie mit Apps zur Netzwerkverwaltung, Fernwartung und E-Mails, sollten Sie die Sicherheit des iPhones erhöhen, vor allem, wenn Sie Anmeldedaten hinterlegt haben. Verlieren Sie Ihr iPhone oder wird es gestohlen, hat der Finder oder Dieb ansonsten Zugriff auf alle wichtigen Daten. Bei der Anbindung von Servern zur Fernwartung ist außerdem Ihre Netzwerkinfrastruktur in Gefahr. Es ist in diesem Fall sehr empfehlenswert, dass Sie eine Codesperre aktivieren.

Verschlusssache: Die Code-Sperre im iPhone sollte aktiviert werden.

Das heißt, man kann auf das iPhone erst zugreifen, wenn man den Code eingibt. Verlieren Sie das iPhone oder spielt ein anderer mit dem Gerät herum, kann er so lange nicht auf die Apps zugreifen, bis Sie den Code eingeben. Sie finden diese Möglichkeit über *Einstellungen\Allgemein\Code-Sperre.* Hier können Sie eingeben wann das iPhone sich sperren soll. Dieser Code hat nichts mit der PIN des iPhones zu tun, sondern ist im iPhone-Speicher hinterlegt. Eine weitere Sicherheitsfunktion des iPhones löscht alle Daten auf dem Gerät, wenn dieses Kennwort zehnmal falsch eingegeben wird. Dazu aktivieren Sie die Option *Daten löschen* im Fenster, in dem Sie auch den Code eingeben. Diese ist standardmäßig nicht aktiviert.

Thomas Joos

3.7 iPhone-Praxis: Das iPhone 4 als WLAN-Hotspot nutzen

Dank der neuen Technologie im iOS können Anwender mit Notebooks oder iPads ohne Internetzugang surfen, indem sie sich mit dem iPhone verbinden. Hierfür bietet das iPhone die normale USB-Kabel-Connectivity, Bluetooth oder WLAN an. Bei der Verbindung über WLAN können sogar drei Clients den Internetzugang nutzen. Insgesamt können also fünf externe Clients gleichzeitig das iPhone als Gateway zum Internet verwenden. Allerdings lassen sich nur iPhone-4-Geräte als WLAN-Zugangspunkt nutzen, die alten 3GS-Modelle bleiben außen vor, können den persönlichen Hotspot aber über Bluetooth und per USB-Kabel zur Verfügung stellen. Wenn Sie während der Verbindung telefonieren, trennt das iPhone teilweise die Internetverbindung, baut diese danach aber wieder automatisch auf.

Apple stellt ein umfangreiches Handbuch als PDF-Datei zur Verfügung (http://manuals.info.apple.com/de_DE/iphone_benutzerhandbuch.pdf); dort werden die neuen Funktionen ausführlich erläutert.

3.7.1 Provider und Verträge beachten

Alle detaillierten Bedingungen des jeweiligen Mobilfunkvertrages zu kennen ist in dem Angebotsdickicht kaum noch möglich. Die Tethering-Funktion, bei der mehrere Geräte die Internetleitung eines anderen Gerätes nutzen, ist bei Providern nicht gern gesehen. Aus diesem Grund unterstützen nicht alle Provider und vor allem nicht alle Verträge diese Funktion. Fragen Sie also vorher bei Ihrem Provider nach, ob Ihr Vertrag für Tethering freigeschaltet ist.

Bei aktuellen Verträgen, die ab Oktober 2010 abgeschlossen wurden, ist das meistens der Fall, bei älteren Verträgen müssen Sie unter Umständen die Tethering-Funktion nachbuchen. Bei manchen Verträgen müssen Sie für die Nutzung der Funktion extra bezahlen. Die Telekom bietet augenscheinlich mit den Complete-Mobile-Tarifen, die Ende 2010 abgeschlossen wurden, eine kostenlose Nutzung. Aber auch hier sollten Sie sicherheitshalber vorher nachfragen. Wer einen älteren Tarif hat, muss Tethering nachbuchen. Die Telekom stellt gesonderte Informationen zum Thema Tethering online bereit (http://www.telekom-hilft.de/servicenotizen/2011/03/wlan-tethering-mit-ios-4.3).

Vodafone erlaubt die Nutzung ebenfalls, hier werden je nach Vertrag zusätzliche Beiträge fällig. Auch hier sollten Sie besser nachfragen. Bei aktuellen Tarifen, die seit Oktober 2010 laufen, ist die Funktion offensichtlich im Preis enthalten. Wer O2 als Provider nutzt, kann ebenfalls Tethering nutzen, muss aber genauso auf den Vertrag und die Bedingungen achten.

Unabhängig vom Provider gilt: Sie sollten auf jeden Fall vorher Rücksprache halten, um Überraschungen auf der Rechnung zu vermeiden.

3.7.2 iPhone als UMTS-Router vorbereiten

Damit sich Computer oder andere Geräte an das iPhone anbinden können, müssen Sie diese Funktion erst einmal in den Einstellungen aktivieren. Rufen Sie dazu *Einstellungen\Persönlicher Hotspot* auf. Sehen Sie den Menüpunkt nicht, müssen Sie unter Umständen diese Funktion noch aktivieren. Rufen Sie dazu *Einstellungen\Allgemein\Netzwerk* auf. Aktivieren Sie die Option Mobile Daten.

Das iPhone 4 als WLAN-Hotspot nutzen: Aktivieren des persönlichen Hotspots im iPhone.

In den Einstellungen des persönlichen Hotspots sehen Sie die drei Möglichkeiten, die die Anbindung anderer Geräte ermöglichen. Damit Sie das iPhone als Zugangspunkt nutzen können, müssen Sie zunächst die Option Persönlicher Hotspot aktivieren. Standardmäßig ist diese Funktion nach der Aktualisierung zu iOS 4.3 deaktiviert. Ab dann sind alle drei Zugangsmöglichkeiten aktiv: USB, WLAN und Bluetooth. Sie können an dieser Stelle keine weitreichenden Einstellungen vornehmen. Als Geschwindigkeit nutzt das iPhone 54 MBit/s auf 2,4 GHz und WPA2 oder WPA als Sicherheitsprotokoll. Die SSID lässt sich nicht anpassen, hier verwendet das iPhone den Gerätenamen. Diesen können Sie nur in iTunes ändern, nicht im Gerät selbst.

Der nächste Schritt besteht darin, dass Sie das Kennwort für den WLAN-Zugang vom Standard abändern. Klicken Sie dazu auf *Wi-Fi-Kennwort*. Geben Sie hier ein sicheres Kennwort ein, das am besten aus zahlreichen Zahlen, Groß- und Kleinschrift, sowie Sonderzeichen besteht. Klicken Sie anschließend auf *Fertig*. Beachten Sie dabei aber, dass das Kennwort in Klartext angezeigt wird. Hat ein anderer Anwender also kurz Zugang zu Ihrem iPhone und kann das Kennwort lesen oder den Zugang aktivieren, besteht Gefahr für Ihre Daten. Sie sollten daher den persön-

lichen Hotspot nur dann aktivieren, wenn Sie diesen auch benötigen. Anschließend können Sie ihn wieder deaktivieren.

Haben Sie diese Konfiguration vorgenommen, können Sie schon schnell und einfach andere Geräte mit dem iPhone verbinden. Dazu verwenden Sie in den meisten Fällen die WLAN-Funktion, da auf diese Weise die meisten Geräte problemlos Zugriff erhalten. Bei der Verbindung über WLAN arbeitet das iPhone als normaler Funknetzwerk-Router und wird von den Betriebssystemen auch so angezeigt. Wollen Sie ein iPad mit dem iPhone über WLAN verbinden, um die schnelle Leitung des iPhones zu nutzen, sollten die iOS-Versionsstände der Geräte identisch sein (z.B. iOS 4.3). Setzen Sie verschiedene Versionen ein, gelingt die Verbindung nicht oder läuft nur sehr instabil.

3.7.3 Windows 7 per WLAN an iPhone anbinden

Im folgenden Abschnitt zeigen wir Ihnen, wie Sie schnell und unkompliziert ein Windows-7-Notebook über das iPhone mit dem Internet verbinden. Haben Sie den persönlichen Hotspot auf dem iPhone aktiviert und das Kennwort gesetzt, können Sie relativ einfach eine Verbindung herstellen. Klicken Sie dazu in der Taskleiste auf das WLAN-Symbol, um sich alle WLANs in der Umgebung anzeigen zu lassen. Verbinden Sie sich mit dem WLAN, das Ihr iPhone zur Verfügung stellt.

Auswahl: Windows 7 zeigt das WLAN des iPhones an.

Auf ähnlichem Weg funktioniert die Anbindung natürlich auch für alle anderen Betriebssysteme und Geräte, die sich mit WLANs verbinden können. Zeigt Windows das WLAN noch nicht an, klicken Sie oben rechts auf die Schaltfläche zum Aktualisieren der Verbindungen. Wird es dann immer noch nicht angezeigt, liegt es unter Umständen daran, dass das iPhone aktuell bereits mit einem WLAN ver-

bunden ist. In diesem Fall können Sie das Notebook ebenfalls mit diesem WLAN verbinden. Hierzu benötigen Sie das iPhone als Hotspot natürlich nicht. Wollen Sie die UMTS-Verbindung des iPhones nutzen, müssen Sie die WLAN-Verbindung des iPhones trennen, denn das Smartphone kann nicht gleichzeitig als Client an einem WLAN teilnehmen und den Hotspot über WLAN bereitstellen.

Abschalten: Das iPhone kann nicht gleichzeitig WLAN-Client sein und einen Hotspot bereitstellen.

Rufen Sie dazu *Einstellungen* auf und klicken dann auf Wi-Fi. Deaktivieren Sie an dieser Stelle die Wi-Fi-Technik und starten Sie diese anschließend wieder. Alternativ rufen Sie die Einstellungen des WLANs auf und trennen sich von diesem. Starten Sie anschließend die Funktion *Persönlicher Hotspot* neu.

Zeigt Windows das WLAN jetzt an, verbinden Sie sich mit diesem. Nach einiger Zeit erscheint das Kennwortfenster. Hier müssen Sie das Kennwort eingeben, das Sie in der Konfiguration des iPhones für den persönlichen Hotspot festgelegt haben. Windows speichert das Kennwort, und Sie müssen es bei der nächsten Verbindung nicht erneut eingeben.

3.7.4 Sicherheit und IP-Adressen

Für die Verbindungssicherheit nutzt iOS 4.3 bei Windows 7 WPA2, wenn das Endgerät diese Verbindung unterstützt, aber auch WPA für ältere Systeme. Die Abkürzung WPA steht für Wi-Fi Protected Access. Mithilfe der WPA-Verschlüsselung können Sie Ihr drahtloses Netzwerk relativ unkompliziert und schnell absichern. Der Pre-Shared Key ist ein Schlüssel, der dem Access Point (dem iPhone) und allen WLAN-Teilnehmern zur Verfügung stehen muss.

Mithilfe dieses Master-Schlüssels ändert der Access Point in regelmäßigen Intervallen die Verschlüsselung. Dieser Vorgang wird dynamischer Schlüsselwechsel genannt. WPA2 stellt eine verbesserte Variante seiner Vorgängerversion WPA dar.

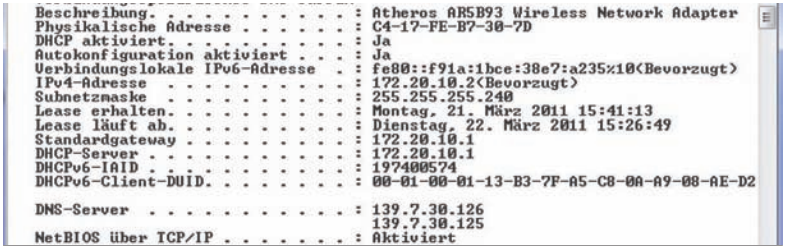
Durch ein neu aufgenommenes Verschlüsselungsverfahren mit der Bezeichnung AES-CCM (Advanced Encryption Standard – Counter with CBC-MAC) ist die Sicherheit verbessert worden. Das Verfahren stellt allerdings auch deutlich höhere Anforderungen an die Hardware, sodass Geräte, die mit WPA umgehen können, nicht automatisch auch WPA2 beherrschen.

Der Verbindungsaufbau klappt nur dann, wenn das iPhone nicht selbst als WLAN-Client konfiguriert und mit einem WLAN verbunden ist. Haben Sie das Notebook mit dem iPhone verbunden, können Sie bereits die Internetleitung nutzen. Clients, die an das iPhone angebunden sind, erhalten eine IP-Adresse durch einen internen DHCP-Server im iPhone. Dazu ist es aber notwendig, dass Sie die Netzwerkverbindung auf dem Client auch für DHCP konfiguriert haben. Verwenden Sie für die Verbindung eine statische Adresse, kann der Computer keine Verbindung zum Internet aufbauen. In Windows finden Sie die Konfiguration der Netzwerkadapter im Netzwerk- und Freigabecenter oder wenn Sie ncpa.cpl im Suchfeld des Startmenüs eingeben.

3.7.5 Netzwerkkonfiguration und DNS-Server

Ist das Notebook mit dem iPhone verbunden, hat aber keine Verbindung zum Internet, liegt es in den meisten Fällen an statischen IP-Adressen oder einem anderen DHCP-Server, der die Verbindung stört. Sie erkennen eine fehlerhafte Verbindung am gelben Warnschild mit schwarzem Ausrufezeichen des WLAN-Symbols in Windows. Sobald Sie die Netzwerkverbindung auf DHCP konfiguriert haben, erkennt Windows dies, und die Internetverbindung ist hergestellt. Auf dem iPhone erhalten Sie ebenfalls die Meldung, dass sich ein Client verbunden hat. Sie sehen die Information im oberen Bereich des Fensters und auf dem Sperrbildschirm.

Geben Sie auf dem Notebook *ipconfig* in der Befehlszeile ein, sehen Sie, dass das Notebook eine IP-Adresse durch das iPhone erhalten hat und das iPhone als Standard-Gateway für die Internetverbindung nutzt. Außerdem ist als DHCP-Server ebenfalls die IP-Adresse des iPhones eingetragen. Als DNS-Server verwendet das iPhone aber andere Server. Normalerweise kommen hier die DNS-Server Ihres Providers zum Einsatz.



Ipconfig: Hier sehen Sie die IP-Konfiguration von Windows nach dem Verbindungsaufbau.

Die erweiterten Informationen sehen Sie, wenn Sie *ipconfig /all* in einer Befehlszeile eingeben. Wollen Sie den Namen der verwendeten DNS-Server anzeigen, geben Sie den Befehl *nslookup <IP-Adresse des DNS-Servers>* in einer Befehlszeile ein.

Oft lässt sich die Geschwindigkeit ein wenig steigern, wenn Sie nicht die DNS-Server des Providers verwenden, sondern zum Beispiel die von Google. Hinzu kommt, dass die DNS-Server vieler Provider nicht alles auflösen. Geben Sie dazu in der Netzwerkkonfiguration in Windows die IP-Adresse 8.8.8.8 ein. Hierbei handelt es sich um einen Google-DNS-Server. Vertrauen Sie diesem nicht, können Sie an der Stelle auch die IP-Adresse eines freien DNS-Servers verwenden. Eine Liste alternativer DNS-Server findet sich etwa unter http://wiki.ak-zensur.de/index.php/Unzensierte_DNS_Server.

3.7.6 Verbindung über USB-Kabel herstellen

Wenn Sie den persönlichen Hotspot auf dem iPhone aktiviert haben, können bis zu drei Clients eine Verbindung per WLAN mit dem iPhone aufbauen. Zusätzlich kann noch ein Client über das USB-Ladekabel des iPhones arbeiten und ein weiterer Client via Bluetooth Kontakt aufnehmen. Insgesamt lassen sich daher bis zu fünf externe Geräte an das iPhone anbinden.

Per USB: Bei der Kabelverbindung verwendet der Hotspot eine Netzwerkverbindung.

Wollen Sie die USB-Kabel-Verbindung nutzen, müssen Sie auf dem Computer iTunes installieren. Verbinden Sie das iPhone mit dem Computer und haben die Hotspot-Funktion aktiviert, erstellt Windows eine zusätzliche Netzwerkverbindung. Diese sehen Sie, wenn Sie ncpa.cpl im Suchfeld des Startmenüs eingeben. Die Verbindung erscheint nur, wenn Sie das iPhone mit dem Computer verbinden. Achten Sie darauf, dass auch bei dieser Verbindung DHCP aktiviert ist. Sie können für die Kabelverbindung ebenfalls einen eigenen DNS-Server angeben.

Haben Sie die Hotspot-Funktion aktiviert und verwenden das Kabel nur zum Laden des Akku und synchronisieren mit iTunes, verwendet der Computer allerdings auch meistens die Kabelverbindung des iPhones und ignoriert andere Verbindungen. Das liegt daran, dass Windows die Verbindung zum iPhone in der Reihen-

folge der Netzwerkverbindungen ganz oben anordnet. Um diese Einstellung zu ändern oder zu überprüfen, gehen Sie folgendermaßen vor:

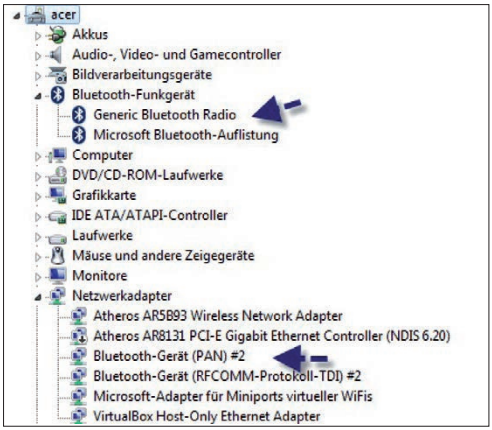
1. Geben Sie *ncpa.cpl* im Suchfeld des Startmenüs ein.
2. Drücken Sie die ALT-Taste, damit Windows das Menü einblendet.
3. Wählen Sie *Erweitert\Erweiterte Einstellungen*.
4. Auf der Registerkarte *Adapter und Bindungen* sehen Sie die Reihenfolge der Netzwerkverbindungen.
5. Ändern Sie die Reihenfolge so ab, dass die iPhone-Verbindung unter der Netzwerkverbindung steht, mit der Sie normalerweise eine Internetverbindung aufbauen.

Alternativ können Sie über das Kontextmenü der Apple-Netzwerkverbindung in Windows den Befehl *Deaktivieren* auswählen, um diese zu deaktivieren.

3.7.7 Bluetooth zur Verbindung verwenden

Aktivieren Sie den Hotspot, verwendet dieser zusätzlich zu WLAN und USB auch die Bluetooth-Technologie zum Verbindungsaufbau. Um diese zu nutzen, können Sie zum Beispiel Windows 7 verwenden.

Wenn Sie eine Bluetooth-Schnittstelle im Computer eingebaut haben oder einen USB-Bluetooth-Stick verwenden, installiert Windows 7 automatisch den passenden Treiber und die Unterstützung von Bluetooth.

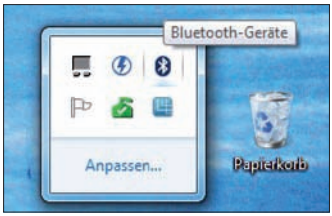


Übersicht: Die Bluetooth-Netzwerkkomponenten finden Sie im Gerätemanager unter den Netzwerkadaptern.

Allerdings arbeiten nicht alle Bluetooth-Schnittstellen problemlos mit dem iPhone zusammen. Die Geräte, die das Empfangen von Bluetooth-Informationen ermöglichen, werden im Gerätemanager angezeigt. Die Bluetooth-Geräte zeigt Win-

dows in einem eigenen Bereich an. Zusätzlich sehen Sie die entsprechenden Netzwerkkomponenten bei den Netzwerkadaptern im Gerätemanager.

Symbolik: Sind Bluetooth-Geräte installiert, erkennen Sie dies im Info-Bereich der Taskleiste.



Überprüfen Sie daher zunächst im Gerätemanager, ob alle Bluetooth-Geräte ohne Fehlermeldung angezeigt werden. Sollten dennoch einige Fehler auftreten, entfernen Sie den Treiber vom System und lassen noch einmal nach neuer Hardware suchen. Da bei der Installation von Bluetooth-Geräten mehrere Hardwarekomponenten installiert werden, kann es durchaus sein, dass Windows 7 einzelne Komponenten nicht installieren kann, aber beim zweiten Versuch dann erfolgreich ist. Den Gerätemanager starten Sie zum Beispiel durch Eingabe von *devmgmt.msc* im Suchfeld des Startmenüs. Wenn Sie Bluetooth-Geräte installiert haben, wird auch ein entsprechendes Symbol im Info-Bereich der Taskleiste angezeigt.

3.7.8 Bluetooth konfigurieren

Sie können per Rechtsklick mit der Maus auf das Bluetooth-Symbol in der Taskleiste die Konfiguration der Bluetooth-Geräte durchführen und Windows mit dem iPhone verbinden. Die Konfiguration starten Sie über *Einstellungen öffnen* im Kontextmenü. Nachdem Sie die Einstellungen gestartet haben, erscheint ein neues Fenster, mit dessen Hilfe Sie über mehrere Registerkarten die Bluetooth-Einstellungen und Verbindungen zwischen mehreren Geräten konfigurieren können.

Es stehen Ihnen die folgenden Registerkarten zur Auswahl:

- Geräte
- Optionen
- COM-Anschlüsse
- Hardware

Über die Registerkarten verwalten Sie alle Bluetooth-Geräte, mit denen Ihr Computer eine Verbindung herstellen kann. Über den Menüpunkt *Gerät Hinzufügen* im Kontextmenü des Bluetooth-Symbols startet ein Assistent, der Sie bei der Anbindung des Gerätes unterstützt. Nach einiger Zeit erscheint hier Ihr iPhone. Achten Sie darauf, dass Bluetooth auf dem iPhone auch aktiv ist. Sie finden die Bluetooth-Konfiguration im iPhone über *Einstellungen\Allgemein\Bluetooth*.

Sicherheitshalber: Überprüfen Sie die Bluetooth-Aktivierung auf dem iPhone.

Lassen Sie für den Verbindungsaufbau dieses Fenster auf dem iPhone geöffnet. Sobald Sie die Verbindung hergestellt haben, erscheint in Windows 7 eine PIN, die Sie auf dem iPhone zur Koppelung eintragen müssen. Nach erfolgreicher Verbindung installiert Windows den Treiber für das iPhone. Auch ist es hilfreich, wenn Sie iTunes auf dem Gerät installiert haben.

Erst wenn der Treiber ordnungsgemäß installiert und die Netzwerkverbindung auf dem Computer angelegt sind, können Sie über Bluetooth die Internetverbindung nutzen. Deaktivieren Sie den persönlichen Hotspot auf dem iPhone, bleibt Bluetooth allerdings aktiviert. Wollen Sie Bluetooth nicht nutzen, müssen Sie diese Funktion über *Einstellungen\Allgemein\Bluetooth* gesondert deaktivieren.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

TecChannel-Links zum Thema	Webcode	Compact
iPhone-Praxis: Das iPhone 4 als WLAN-Hotspot nutzen	2034536	S.160
iPhone-Praxis: Datensicherung und -wiederherstellung	2033621	S.113
iPhone-Praxis: VPN richtig einrichten und nutzen	2033393	S.121
iPhone-Praxis: Kalender optimal synchronisieren	2033865	S.130
iPhone-Praxis: Einstellungen per Konfigurationsprogramm automatisieren	2033060	S.137
iPhone-Praxis: Anbindung an Exchange und SharePoint Server	2032686	S.145
iPhone-Praxis: Apps für Admins	2032906	S.153
Test – Apple iPhone 4 mit iOS 5	2036930	S.169

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

3.8 Test – Apple iPhone 4 mit iOS 5

Apple will mit dem neuen iOS 5 dem iPhone mehr Features und Bedienkomfort spendieren. Das integrierte iCloud sorgt für Datensicherung und Synchronisation, aber auch PCs lassen sich einbinden. Mehr als 200 neue Funktionen hat Apple nach eigenem Bekunden in iOS 5 integriert.

Auf dem iPad haben wir Apples neues iOS 5 ebenfalls getestet, den Artikel finden Sie im Kapitel zum iPad. Vor allem neue Funktionen im Safari-Browser sowie das runderneuerte Benachrichtigungssystem gefallen. Doch auf dem iPhone gibt es durch das kleinere Display, die integrierte Kamera, das Geotagging und den Schwerpunkt auf Mobilität Unterschiede zum iPad. Zwar ist vieles neu für das iPhone mit iOS 5, am gewohnten Bedienkonzept hält Apple allerdings fest. Während es ein paar auffällige Änderungen wie das neue Benachrichtigungssystem, die Integration von Twitter und iCloud gibt, fallen die vielen Kleinigkeiten erst während der Benutzung angenehm auf. Wir stellen Ihnen die neuen Funktionen vor und zeigen die Einsatzmöglichkeiten von iCloud auf dem iPhone und dem PC. Außerdem gibt es bei iOS 5 ein paar Unterschiede zwischen den Versionen für das iPhone und das iPad.

Im Herbst 2011 soll das neue Betriebssystem für das iPhone 3GS und iPhone 4 sowie den iPod touch der dritten und vierten Generation verfügbar sein. Die Variante für das iPad und iPad 2 wird es laut Apple dann ebenfalls geben.

3.8.1 Kabellose Aktivierung und iCloud-Restore

Mit iOS 5 gibt es für die Aktivierung eines neuen iPhones – oder beim Wiederherstellen des Betriebssystems – verschiedene Möglichkeiten.

Drahtlos: Mit iOS 5 gibt es die Möglichkeiten, sein iPhone neu aufzusetzen sowie ein Backup aus iTunes oder iCloud zurückzuspielen.

Beim ersten Einschalten fragt iOS 5 zuerst nach der PIN der SIM-Karte, alternativ lässt sich die Karte auch später entsperren. Dann beginnt das Setup mit der Wahl der Sprache und Ländereinstellung. Jetzt folgt die Einbindung eines verfügbaren WLANs. Ist eine Internetverbindung vorhanden (GSM oder WLAN), so wird das iPhone aktiviert. Wer will, kann es für diesen Vorgang aber auch an den PC oder Mac anschließen und klassisch über iTunes zum Leben erwecken.

Nach der drahtlosen Aktivierung bietet iOS 5 die drei Optionen *Set Up as new iPhone*, *Restore from iCloud Backup* und *Restore from iTunes* an. Will man das iPhone als neues Gerät einrichten, lässt sich jetzt eine vorhandene Apple-ID eingeben oder ein neuer Account wählen. Alternativ kann hier auch auf „Skip this Step" getippt werden. Das iPhone ist nun betriebsbereit. Bei der Wahl Restore from iTunes wird man aufgefordert, das iPhone mit dem PC oder Mac via iTunes anzuschließen. Jetzt lässt sich ein vorhandenes Backup auf das Gerät zurückspielen.

iCloud Backup: Wurde bereits ein Backup in Apples iCloud angelegt, so lässt sich ein neu aufgesetztes Gerät damit wiederherstellen.

Um die Option *Restore from iCloud Backup* nutzen zu können, muss vorher natürlich bereits ein Backup auf iCloud durchgeführt worden sein. Bei unserem Test haben wir das schon erledigt. Welche Optionen es beim iCloud-Backup auf dem iPhone gibt, lesen Sie später im Artikel. Wenn nun auf R*estore from iCloud Backup* getippt wird, so fragt iOS 5 die Apple-ID ab. Danach zeigt das iPhone die vorhandenen iCloud-Backups auf dem Gerät an. Unser vorher in iCloud angelegtes Backup mit zirka 700 MByte Größe wurde via WLAN in ungefähr 15 Minuten zurückgespielt. Alle Accounts, Apps und deren Daten sowie sämtliche Einstellungen waren wieder vorhanden. Musiktitel und Videos müssen noch „klassisch" via iTunes aufgespielt werden.

3.8.2 Drahtlose Softwareaktualisierung

Mit iOS 5 erfolgen Software-Updates ebenfalls „over the Air". Dabei wird bei einem OS-Update nur geladen, was sich geändert hat – sogenannte Delta-Updates. Somit muss nicht stets ein komplett neues iOS-Image mit einer typischen Größe von 600 bis 700 MByte heruntergeladen werden. Eine Pop-up-Nachricht zeigt automatisch an, dass ein *Software Update* verfügbar ist.

Over the Air: Updates des Betriebssystems können über iOS 5 drahtlos aufgespielt werden.

Wird auf Details bei der Nachricht getippt, so landet man direkt in den Einstellungen bei *Softwareaktualisierung*. Nach dem Laden des Updates auf dem iPhone muss noch auf *Jetzt installieren* getippt werden. iOS führt daraufhin einen Neustart des Geräts durch und aktualisiert sich. Die klassische Aktualisierung über iTunes funktioniert alternativ weiterhin. Drahtlose Updates führt iOS 5 nur durch, wenn der Akku des Geräts mindestens zu 50 Prozent geladen ist.

3.8.3 iCloud – Synchronisierter Foto- und Datenstream

Die Cloud ist für Apple nicht neu, der vorhandene Dienst MobileMe bietet E-Mail-Dienste wie auch Online-Speicherplatz an. Den kostenpflichtigen Dienst ersetzt Apple jetzt schrittweise durch iCloud. Apple nimmt für MobileMe auch schon keine neuen Abonnenten mehr an, doch für Mitglieder lässt sich MobileMe bis zum 31. Juni 2012 noch nutzen.

Fotos und Daten: Zu den iCloud-Diensten zählen auch ein Fotostream sowie die Synchronisation von Daten und Dokumenten bei Apps.

Apples iCloud ist ein zentraler Bestandteil von iOS 5. Insgesamt stellt Apple jedem Nutzer einen 5 GByte fassenden Speicherplatz in iCloud kostenlos zur Verfügung. Über iCloud lassen sich die Apple-Dienste *E-Mail* mit MobileMe-Adresse, *Kontakte, Kalender, Erinnerungen, Lesezeichen* von Safari, *Notizen* sowie *Bilder* synchronisieren. Jeder einzelne Dienst kann über Schalter in den Einstellungen bei iCloud aktiviert oder deaktiviert werden.

Bei der E-Mail wird eine *beispiel@me.com* eingerichtet. Die Me-Adresse ist mit der Apple-ID verknüpft und nutzt das identische Passwort. Praktisch ist die Synchronisierung der Lesezeichen für Nutzer mehrere Apple-Geräte. Wird beispielsweise auf dem iPad in Safari ein Lesezeichen gesetzt oder gelöscht, so aktualisieren sich auch auf dem iPhone die Bookmarks.

Wird bei den iCloud-Einstellungen auf dem iPhone der Dienst *Fotostream* aktiviert, so findet sich auch in der Foto-App das neue Album *Fotostream*. iOS 5 speichert alle selbst gemachten Fotos oder Screenshots nicht mehr nur im Album Gesicherte Fotos ab, sondern schiebt diese auch automatisch in das Cloud-Album Fotostream. Neue Fotos bleiben laut Apple jeweils 30 Tage in der iCloud, maximal aber 1000 Bilder gleichzeitig. iOS 5 bietet auch die iCloud-Funktion *Documents & Data*. Damit können Apps ihre Dokumente und Daten in der iCloud speichern und somit allen iOS-Geräten eines Benutzers zur Verfügung stellen. Bei den Einstellungen von *Documents & Data* lässt sich noch wählen, ob der Cloud-Dienst nur bei einer Wi-Fi-Verbindung genutzt werden soll.

3.8.4 iCloud – App für Windows und Mac OS X

Apple bietet mit dem iCloud-Dienst auch für Windows und Mac OS X ein Tool mit der Bezeichnung iCloud an. Das getestete Windows-Programm installiert sich in der Windows-Systemsteuerung und lässt sich als Hintergrunddienst betreiben.

iCoud für Windows: Apple bietet mit dem iCloud-Dienst auch für Windows und Mac OS X ein Tool mit der Bezeichnung iCloud an.

In iCloud für Windows gibt es die Option *Photo Stream*. Alle auf dem iPhone 4 gemachten Fotos oder Screenshots speichert iCloud automatisch in einem wählbaren Download-Ordner. Im Test war ein mit dem iPhone 4 gemachtes Foto zirka 15 Sekunden später im Download-Ordner des Windows-PCs. Über den ebenfalls wählbaren Upload-Ordner können vom PC aus Bilder in den iCloud-Fotostream hochgeladen werden. Auch hier sind die Bilder rund 15 Sekunden später im Ordner Fotostream auf dem iPhone oder iPad.

Direkter Stream: In iCloud für Windows gibt es unter anderem die Option Fotostream. Alle auf dem iPhone 4 gemachten Fotos oder Screenshots speichert iCloud automatisch in einem wählbaren Download-Ordner.

iCloud für Windows zeigt ständig den verfügbaren Speicherplatz in iCloud an. Die Detail-Infos informieren über die vorhandenen Backups von iOS-5-Geräten sowie den belegten Speicherplatz von E-Mails. Backups lassen sich direkt im Programm zum Freigeben von mehr Speicherplatz löschen. Die iCloud-Windows-App ermöglicht neben dem Fotostream noch eine Synchronisation der Mails, Kontakte und Kalender von Outlook. iCloud unterstützt dabei Outlook ab der Version 2007. Des Weiteren können die Lesezeichen des Internet Explorer und Safari synchronisiert auf den Safari-Browser des iPhones oder iPads übertragen werden.

3.8.5 iCloud – Backup mit Optionen

In iOS 5 lässt sich der iCloud-Dienst für ein Backup des Geräts nutzen. Beim Backup speichert iOS 5 neben den eigenen Fotos alle eingerichteten Accounts, Dokumente der Apps und die Einstellungen. iCloud führt automatisch täglich ein Back-

up des Geräts aus, wenn das iPhone an einer Ladestation hängt, gesperrt ist und eine aktive WLAN-Verbindung hat. Ein Backup lässt sich aber auch jederzeit manuell in den iOS-5-Einstellungen von iCloud starten.

iCloud-Backup: Beim Backup speichert iOS 5 neben den eigenen Fotos alle eingerichteten Accounts, Dokumente der Apps und die Einstellungen.

Das neue iOS 5 bietet beim iCloud-Backup Optionen an, von welchen installierten Apps die Daten und Dokumente zu sichern sind. Praktischerweise wird bei jeder App der notwendige Speicherplatz angezeigt. So lassen sich bei Bedarf speicherfressende Apps vom Backup ausschließen. Wer will, kann für die iCloud mehr Speicherkapazität einkaufen. Die iCloud-Backups können jederzeit vom iPhone – wie auch von der iCloud-App für Windows oder Mac OX – aus gelöscht werden.

Ab in die Wolke: In den Backup-Optionen gibt es die Möglichkeit, die zu sichernden Apps mit ihren zugehörigen Daten zu wählen.

Beim Aktivieren von *Datensicherung in iCloud* weist iOS 5 noch darauf hin, dass beim Anschluss des Geräts an iTunes nicht mehr automatisch eine lokale Datensicherung auf den PC erfolgt. Diese kann aber jederzeit manuell durchgeführt werden (Rechtsklick auf das iPhone-Symbol).

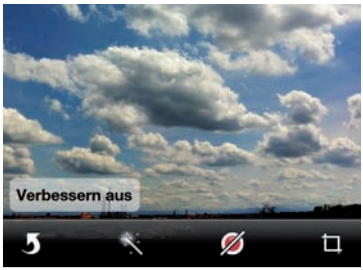
3.8.6 Foto-App mit erweiterter Funktionalität

Apple verbessert in iOS 5 die Bedienung der Kamera. So wird ein schnellerer Kamerastart ermöglicht, wenn sich das iPhone im gesperrten Zustand (Stand-by) befindet. Ein Doppelklick auf den Home-Button ruft rechts neben dem Regler *Entsperren* ein Symbol für die Kamera auf. Ein Tipp darauf startet nun die Kamera-App.

Schnellschuss: Ein Doppelklick auf die Sperrtaste bringt jetzt das Fotosymbol rechts unten hervor. Damit lässt sich die Foto-App starten, ohne den Bildschirm entsperren zu müssen.

Zum Auslösen von Fotos kann neben dem gewohnten Knopf auf dem Bildschirm nun auch die „+"-Taste der Lautstärkeregler gedrückt werden. Damit entfällt das richtige Treffen der Bildschirmauslösung. Zwischen den eingeblendeten Symbolen für Blitz und Kameraumschaltung befindet sich in iOS 5 eine Schaltfläche Optionen. Während bei iOS 4.3 hier nur die HDR-Funktionalität aktiviert wird, lässt sich jetzt auch ein Raster einblenden. Die Linien im Bildschirm dienen zur besseren Orientierung und Ausrichtung der Kamera an horizontalen oder vertikalen Objekten. In der Foto-App kann man per Fingerwisch nach rechts nun direkt zum Album *Aufnahmen* wechseln – nach links dann wieder zurück. Der alternative, aber langsamere Weg über einen Tipp auf das Fotosymbol links unten steht dem User weiterhin offen.

Neu: Auf dem iPhone 4 erlaubt iOS 5 jetzt eine sehr einfache Bildbearbeitung. Neben dem Drehen des Bildes gibt es eine automatische Bildverbesserung, Entfernen von roten Augen sowie die Funktion Zuschneiden.



Auf dem iPhone 4 erlaubt iOS 5 jetzt eine sehr einfache Bildbearbeitung. Rechts oben im Bild gibt es die neue Schaltfläche *Bearbeiten*. Neben dem Drehen von Bildern in 90-Grad-Schritten kann eine automatische Bildverbesserung aktiviert werden. Außerdem gibt es eine Funktion zum Entfernen von roten Augen bei

Blitzaufnahmen. Ein Zuschneiden von Bildern komplettiert die Bearbeitungsfunktionen. Wird ein Foto aus dem Ordner Aufnahmen bearbeitet, so überschreibt iOS 5 dieses beim Tipp auf das Symbol *Sichern*. Geänderte Bilder aus anderen Alben speichert das Betriebssystem im Ordner *Aufnahmen*.

In der Bilder-App können wie beim iPad neue Alben angelegt werden. Außerdem ist das Kopieren von Bildern in andere Alben möglich.

3.8.7 iMessages – kostenlose Nachrichten zwischen iOS-5-Geräten

Apple führt bei iOS 5 den neuen Messaging-Service iMessages ein In der deutschen Lokalisierung wird die App als Nachrichten angezeigt. Auf dem iPhone 4 ist somit wie gewohnt die Nachrichten-App vorhanden, die in iOS 5 um den iMessages-Service erweitert ist. Auf dem iPad und iPod touch gibt es dagegen die Nachrichten-App mit iOS 5 zum ersten Mal.

iMessages: Beim Tipp auf Neue Nachricht in der App überprüft iMessages, ob der gewählte Kontakt eine iMessages-Registrierung vorgenommen hat. Besitzt der Kontakt ebenfalls ein iOS-5-Gerät, so wechselt die Farbe des Kontakts und des Sendeknopfs von Grün auf Blau.

Mit iMessages lassen sich zwischen iOS-5-Nutzern nicht nur Nachrichten, sondern auch Fotos und Videos kostenlos austauschen – eine Internetverbindung natürlich vorausgesetzt. Für iMessages lassen sich in den Einstellungen bei iOS 5 neben der Apple-ID mit Telefonnummer eine oder mehrere E-Mails als Adresse verknüpfen. Beim Tipp auf *Neue Nachricht* in der App überprüft iMessages, ob der gewählte Kontakt eine iMessages-Registrierung vorgenommen hat. Besitzt der Kontakt ebenfalls ein iOS-5-Gerät, so wechselt die Farbe des Kontakts und des

Sendeknopfs von *Grün* auf *Blau*. Bleibt die Farbe auf *Grün*, so wird die Nachricht wie gewohnt als SMS behandelt, *Blau* ist immer für iMessages kennzeichnend.

Bitte bestätigen: Neben einer Empfangsbestätigung gibt es auch eine einschaltbare Lesebestätigung. Ist diese aktiviert, so wird „Gelesen HH:MM" angezeigt, wenn der Empfänger die Nachricht öffnet.

Wenn der iMessages-Service eine Nachricht nicht zustellen kann, dann bietet die App den optionalen Versand als SMS an. Neben einer Empfangsbestätigung gibt es auch eine einschaltbare Lesebestätigung. Ist diese aktiviert, so wird *Gelesen HH:MM* angezeigt, wenn der Empfänger die Nachricht öffnet. Wer iMessages nicht verwenden will, kann den Dienst in den Einstellungen der Nachrichten deaktivieren.

iMessages erlaubt zudem das Versenden und Empfangen von Bildern und Videos. Hier kann der Anwender entweder aus den vorhandenen Alben auswählen oder ein neues Foto beziehungsweise Video aufnehmen. Empfangene Fotos können gesichert werden. Der Messaging-Service läuft auf dem iPhone über Wi-Fi und 3G.

3.8.8 Nachrichten und Wetter per Fingerwisch

Bei iOS 5 werden die bisherigen Push-Nachrichten von einem neuen Benachrichtigungssystem abgelöst. Im Artikel „Test – Apple iPad mit iOS 5" berichten wir über die Funktion des neuen Systems. Wie beim iPad mit iOS 5 lassen sich auch beim Apple iPhone 4 die neuen Nachrichten und Ereignisse durch das Ziehen eines Fingers vom oberen Bildschirmrand nach unten jederzeit öffnen. Neben ungelesenen E-Mails sammelt das Benachrichtigungssystem beim iPhone beispielsweise auch entgangene Anrufe oder neue SMS beziehungsweise iMessages. Neu eintreffende Ereignisse blendet iOS 5 ohne Störung der aktuell laufenden App für ein paar Sekunden am oberen Bildschirmrand ein.

Schnellzugriff: Bei iOS 5 gibt es ein neues Benachrichtigungssystem. Neuigkeiten wie ungelesene E-Mails lassen sich durch das Ziehen eines Fingers vom oberen Bildschirmrand nach unten jederzeit öffnen.

Im Sperrbildschirm zeigt iOS 5 ebenfalls die neuen Nachrichten an. Für jede einzelne App sind die generelle Anzeige im Benachrichtigungssystem und das Erscheinen im Sperrbildschirm konfigurierbar. Sehr praktisch ist, dass sich bei ausgeschaltetem Gerät (Stand-by) das Display bei neuen Nachrichten für ein paar Sekunden einschaltet. So lässt sich die Meldung kurz lesen und bei Bedarf auch direkt öffnen durch einen seitlichen Fingerwisch auf das Nachrichtensymbol. Beim iPhone kann das Nachrichtensystem auch sehr bequem per Einhandbedienung mit dem Daumen geöffnet werden, im Gegensatz zum größeren iPad.

Ohne Unterbrechung: Neu eintreffende Ereignisse blendet iOS 5 ohne Störung der aktuell laufenden App für ein paar Sekunden am oberen Bildschirmrand ein.

Bei der iPhone-Version von iOS 5 lassen sich auch die im Betriebssystem enthaltenen Apps Wetter und Aktien im Benachrichtigungssystem als Widget einschalten. Beim Wetter zeigt das iPhone immer ortsbezogene Daten vom aktuellen Standort in den Nachrichten an. Bei einem Wisch nach links oder rechts auf die Wettereinblendung wird zu einer Sechs-Tage-Vorschau gewechselt. Auch in der Wetter-App selbst gibt es die neue Ansicht Lokales Wetter mit dem jeweils aktuellen Standort. Ist im Benachrichtigungssystem auch das Stock Widget aktiviert, so werden die aktuellen Aktienkurse (in der Aktien-App ausgewählte) in einem Lauf-

band angezeigt. Es gibt auch Ereignisse, bei denen iOS 5 weiterhin auf die bisherigen Push-Nachrichten zurückgreift. Hierzu zählen beispielsweise die Warnungen bei niedrigem Akku-Ladezustand. Bei 20 und später 10 Prozent warnt iOS 5 mit einer Pop-up-Nachricht.

3.8.9 Safari in Details verfeinert

Bei iOS 5 für das iPad beherrscht Safari Tabbed Browsing wie bei Desktop-Browsern. Die iPhone-Version von Safari nutzt dagegen weiterhin das Bedienkonzept mit dem Fenstersymbol rechts unten zum Anzeigen der offenen Tabs. An der Anzahl von maximal neun geöffneten Tabs hat sich bei iOS 5 nichts geändert.

Wie gehabt: Der Browser präsentiert sich mit iOS 5 auf dem iPhone im gewohnten Design. Neu ist dagegen der Reader. Die Funktion dient dem bequemeren Lesen von Artikeln auf Webseiten. Safari blendet bei Artikeln automatisch nach dem Laden in der Adresszeile ein Icon Reader ein. Wird darauf getippt, so startet die Reader-Ansicht des Artikels.

Neu im Safari-Browser bei iOS 5 ist die Suchfunktion innerhalb von Webseiten. Der Suchbegriff wird nicht wie beim iPad-Safari in ein Extra-Suchfenster über der Tastatur, sondern in das (Google-)Suchfeld eingetippt. Allerdings wird statt „Suchen" auf der Tastatur zu drücken, was die Google-Suche startet, mit dem Finger das Ergebnisfeld nach oben gezogen. Jetzt lässt sich auf *Auf dieser Seite (Anzahl Treffer) „Begriff" suchen* tippen. Treffer werden farblich hervorgehoben, mit Pfeiltasten lässt sich durch die Treffer navigieren.

Den neuen Safari Reader gibt es bei iOS 5 auch in der iPhone-Version. Die Funktion dient dem bequemeren Lesen von Artikeln auf Webseiten. Safari blendet bei Artikeln automatisch nach dem Laden in der Adresszeile ein Icon *Reader* ein. Wird darauf getippt, so startet die Reader-Ansicht des Artikels. Selbst bei mehrseitigen

Artikeln wird mit Safari Reader alles auf einer scrollbaren Seite angezeigt. Über das Symbol *Weiterleiten* können Artikel zu einer Leseliste hinzugefügt werden. Entsprechende Artikel werden dann via iCloud synchronisiert. So lassen sich Artikel beispielsweise auf dem iPad weiterlesen, die auf dem iPhone geladen wurden.

Safari Reader: Selbst bei mehrseitigen Artikeln wird mit Safari Reader alles auf einer scrollbaren Seite angezeigt.

Der iCloud-Service Lesezeichen-Synchronisation funktionierte bei unserem Test mit dem iPad und iPhone 4 sehr gut. Neue Lesezeichen, Löschen von Booksmarks, Umbenennungen oder Verschiebungen finden sich zirka 15 Sekunden später auf dem anderen iOS-5-Gerät, das über die gleiche Apple-ID registriert ist.

3.8.10 Twitter-Integration, E-Mail und Tastatur

Auf dem iPhone besitzt iOS 5 die identische Integration von Twitter wie bei der iPad-Variante. Entsprechend lassen sich direkt Fotos, Lesezeichen, Youtube-Videos und Standorte aus der Karten-App twittern. Beim jeweiligen Tipp auf das Symbol Weiterleiten ist der zusätzliche Eintrag Tweet zu sehen.

Schneller Tweet: Durch die Twitter-Integration in iOS 5 lassen sich direkt Fotos, Lesezeichen und Youtube-Videos senden.

Beim E-Mail-Client hat sich an der Optik und der grundlegenden Bedienung bei iOS 5 kaum etwas geändert. Neu ist, wie in der iPad-Variante die Möglichkeit, E-Mails durch ein Etikett hervorzuheben und Mails als wieder ungelesen zu markieren. Zitatebenen können ebenso verwendet werden wie die Textformatierungen Fett, Kursiv und Unterstrichen. Die Mail-App in iOS 5 erkennt nun auch Zertifikate und unterstützt S/MIME. Statt maximal die letzten 200 anzuzeigenden E-Mails können nun zusätzlich auch 500 und 1000 Nachrichten eingestellt werden.

Umlaute: Mit iOS 5 gibt es neben dem bisherigen QWERTZ-Layout der iPhone-Tastatur nun auch eine Variante mit ä, ö und ü.

Mit iOS 5 gibt es neben dem bisherigen QWERTZ-Layout der iPhone-Tastatur nun auch eine Software-Tastaturbelegung Deutsch. Jetzt zeigt die Tastatur auch die deutschen Umlaute ä, ö und ü auf Extra-Tasten an. Die Umlaute sind rechts außen angeordnet und verringern den Tastenabstand damit ein wenig.

3.8.11 Erweitertes Geotagging und AssistiveTouch

In iOS 5 führt Apple erweiterte Optionen für das Geotagging ein. Wie bisher wird durch einen Pfeil in der oberen Statusleiste angezeigt, wann eine App auf die Geodaten zurückgreift. Apple erläutert bei der Aktivierung der Ortungsdienste, dass neben GPS eine „Crowd-sourced"-Datenbank aus Wi-Fi-Hotspots und Mobilfunkmasten den aktuellen Standort berechnen.

Für jede App, die Ortungsdienste verwendet, lässt sich weiterhin das Geotagging einzeln ein- oder ausschalten. In den Einstellungen der Ortungsdienste zeigt dabei ein lilafarbener Pfeil an, welche App gerade den aktuellen Standort verwendet. Ein

grauer Pfeil neben der App weist darauf hin, dass innerhalb der letzten 24 Stunden ein Geotagging-Zugriff erfolgte. Neu in iOS 5 sind die wählbaren Systemdienste mit Geotagging. Hier lässt sich beispielsweise der Ortungsdienst für *Locaction-Based iAds* oder das *Cell Network Search* deaktivieren.

Ortungsdienste: Neu bei iOS 5 sind die wählbaren Systemdienste mit Geotagging . Hier lässt sich beispielsweise der Ortungsdienst für „Locaction-Based iAds“ oder das „Cell Network Search“ deaktivieren.

Bei iOS 5 führt Apple mit Assistive Touch eine weitere Bedienhilfe ein. Assistive Touch soll Anwendern mit Handicap helfen, die die Tasten für Lautstärke oder den Home-Button nur unter Schwierigkeiten oder gar nicht betätigen können. Ist Assistive Touch aktiviert, so blendet iOS 5 rechts unten im Display einen „Touch-Punkt“ ein, der beim Berühren verschiedene Funktionen ermöglicht. Damit lässt sich beispielsweise die Lautstärke regeln, der Home-Button auslösen, das Gerät schütteln oder der Bildschirm rotieren. Außerdem können durch einen einzigen Fingertipp Gesten für zwei, drei, vier oder fünf Finger, Wischen oder Zusammenziehen ausgelöst werden. Eigene Gesten, die für bestimmte Apps notwendig sind, kann der User ebenfalls speichern.

Assistive Touch: Die Bedienhilfe ermöglicht es beispielsweise, die Lautstärke zu regeln oder den Home-Button zu drücken.

3.8.12 Zusätzliche Features

Apple spricht bei iOS 5 von mehr als 200 neuen Features. Im Test von iOS 5 auf dem iPhone 4 sind dabei folgende Funktionen aufgefallen:

- **Benutzung:** Praktisch ist in den *Allgemeinen Einstellungen* der Eintrag *Benutzung*. Hier wird der belegte Speicherplatz jeder einzelnen App angezeigt.
- **Kurzbefehle:** In den *Allgemeinen Einstellungen* unter *Tastatur* findet sich der neue Eintrag *Kurzbefehl*. Hier lassen sich Kurzformen definieren. So wird beispielsweise „mfg" beim Schreiben automatisch in „Mit freundlichen Grüßen" umgewandelt.
- **Music:** In iOS 5 wurde der Musik-Player iPod in Music umbenannt worden. Das Layout ist aber im Gegensatz zur iPad-Version unverändert geblieben. Lieder können nun auch direkt auf dem Gerät gelöscht werden.
- **Synchronisation:** Während der Synchronisation lässt sich die Arbeit auf dem iPhone weiterführen. Außerdem zeigt iOS 5 links oben in der Statusleiste einen rotierenden Kreis während der Synchronisation an.
- **App-Download:** Mit iOS 5 ist das parallele Laden mehrerer Apps möglich.
- **Videos:** Filme und Videos finden sich wieder in einer eigenen App und nicht mehr als Unterpunkt bei iPod wie in iOS 4.3.
- **Zeitungskiosk:** Die App sammelt zentral alle E-Magazine, die über ein Abo bezogen werden. Neue verfügbare Ausgaben werden automatisch geladen, sodass diese sofort im News-Stand sind.
- **Name:** In den *Allgemeinen Einstellungen* unter *Info* kann bei iOS 5 der Name des Geräts geändert werden. Bisher ist das nur mit iTunes möglich.

Christian Vilsbeck

TecChannel-Links zum Thema	Webcode	Compact
Test – Apple iPhone 4 mit iOS 5	2036930	S.169
iPhone-Praxis: Datensicherung und -wiederherstellung	2033621	S.113
iPhone-Praxis: VPN richtig einrichten und nutzen	2033393	S.121
iPhone-Praxis: Kalender optimal synchronisieren	2033865	S.130
iPhone-Praxis: Einstellungen per Konfigurationsprogramm automatisieren	2033060	S.137
iPhone-Praxis: Anbindung an Exchange und SharePoint Server	2032686	S.145
iPhone-Praxis: Apps für Admins	2032906	S.153
iPhone-Praxis: Das iPhone 4 als WLAN-Hotspot nutzen	2034536	S.160

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

4 Android

Smartphones mit Android als Betriebssystem werden immer beliebter, im Gegenzug liefern die Hersteller besser ausgestattete und leistungsfähigere Geräte aus. Googles Android treibt die neuesten Smartphone-Modelle von HTC, LG, Motorola, Samsung und Sony Ericsson an. Von den über 10 Millionen Smartphones, die jährlich weltweit verkauft werden, sind inzwischen mehr Geräte mit Android ausgestattet als mit Apples iOS-Betriebssystem.

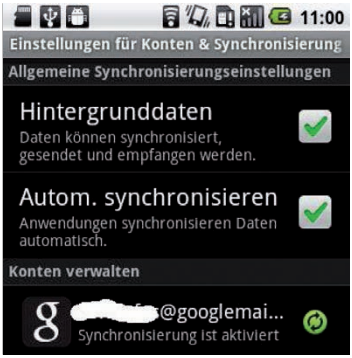
4.1 Android – Datensicherung in der Praxis

Meist wird auch Smartphone-Anwendern erst im Notfall, sprich bei Datenverlust, klar, dass auch auf diesen Geräten eine Datensicherung eine unabdingbare Aufgabe ist. Dies gilt natürlich für Anwender, die ihr Smartphone professionell einsetzen, umso mehr. Ein serienmäßiges Datensicherungsinstrument wie etwa iTunes bei Apple existiert für Android in dieser Form nicht. Dass iTunes allerdings in Sachen Benutzerfreundlichkeit und Stabilität nicht zwangsläufig das Maß der Dinge ist, darüber lässt sich trefflich diskutieren. Hinsichtlich einer benutzerfreundlichen Verwaltungssoftware herrscht auf allen Plattformen noch Handlungsbedarf.

Für die Sicherung von Android-Smartphones müssen Anwender daher auf andere Mittel setzen und teilweise verschiedene Werkzeuge einsetzen. Zwar sichern Android-Handys teils automatisch Daten auf SD-Karte und Google-Konto, wenn Sie dieses einrichten. Allerdings funktioniert dieser Vorgang nicht auf allen Endgeräten und bei allen Herstellern. Aus diesem Grund tun Anwender gut daran, auf zusätzliche Anwendungen zu setzen oder sich die Anwendung anzusehen, die der Hersteller mit dem Gerät ausliefert. Wir zeigen Ihnen in den folgenden Abschnitten bekannte und gut bewertete Apps, mit denen Sie Android-Geräte sichern können. Darunter finden sich sowohl kostenlose als auch kostenpflichtige Apps, deren Einsatz sich allerdings durchaus lohnen kann.

4.1.1 Sicherung von Kalender und Kontakten

Die Kontakte und Kalendereinträge auf Ihrem Android-Smartphone sichern Sie am effizientesten, wenn Sie eine Synchronisierung mit einem kostenlosen Google-Account einrichten. Achten Sie aber darauf, dass bei einer Synchronisierung die Daten auch im verbundenen Google-Konto gelöscht werden, wenn Sie einen Kontakt löschen. Ist Ihr Gerät defekt oder tauschen Sie es aus anderen Gründen aus, reicht eine Synchronisierung des neuen Telefons mit dem aktuellen Google-Konto, um die Daten wiederherzustellen. Um eine Sicherung durchzuführen, können Sie zum Beispiel Kalender und Kontakte mit einem Google-Account synchronisieren und diese Daten dann in der Weboberfläche des Google-Accounts exportieren.



Gleichstand: Das Telefon kann mit dem Google-Konto synchronisiert werden.

Um die Daten auf dem Android wiederherzustellen, können Sie dann einfach erneut eine Synchronisierung starten und vorher die Daten im Google-Konto wieder aus der exportierten *.csv-Datei importieren. Manche Hersteller von Android-Smartphones stellen selbst entwickelte Sicherungsprogramme zur Verfügung.

Sicherheitshalber: Kontakte lassen sich zur Sicherung in Google-Konten ex- oder importieren.

Sie sollten überprüfen, ob bei Ihrem Gerät eine solche Lösung beiliegt, und diese entsprechend einsetzen. Ist das nicht der Fall, müssen Sie auf Software setzen, die generell für Android zur Verfügung steht. Es spricht aber auch nichts dagegen, wenn Sie weitere Apps zur Sicherung installieren. Achten Sie aber möglichst darauf, nur Apps zu verwenden, die auch eine automatische Sicherung ermöglichen, wenn Sie Daten sichern wollen, die sich ständig ändern, zum Beispiel Fotos, Favoriten, SMS oder Anruflisten.

4.1.2 Vollständige Sicherung mit Root-Rechten

Leider spielen auch bei der Sicherung von Android-Smartphones die Root-Rechte eine besondere Rolle. Ohne diese Rechte lassen sich Android-Smartphones schlicht und ergreifend nicht effizient vollständig sichern und wiederherstellen. Dieses leidige Thema zieht sich bei Android-Smartphones durch alle Bereiche. Ob wichtige Tools, VPN oder Admin-Werkzeuge, für die meisten Aufgaben, die tiefer

in das System gehen, sind Root-Rechte notwendig – anders als bei iPhone oder Windows Phone 7, die auch mit normalen Rechten vernünftige VPN-Lösungen oder Datensicherungen möglich machen.

Das bedeutet: Anwender, die ihr Smartphone vollständig sichern wollen, müssen den eher unbequemen Weg gehen und ihr Smartphone rooten. Die Anwendungen für Android basieren vor allem auf Java. Der normale Anwender des Handys hat keine weitreichenden Rechte, sondern nur der Benutzer Root. Dieser ist der Administrator des Geräts. Anwender können sich aber selbst sehr leicht diese Root-Rechte zuweisen (rooten). Hierzu gibt es zahlreiche Anleitungen im Internet.

Nach einem solchen Vorgang arbeiten Sie dann nicht mit den normalen Benutzerrechten, die deutlich eingeschränkt sind, sondern im Kontext eines Super-Users. In diesem Fall haben Sie und die Anwendungen, die Sie installieren, vollständige Rechte in Android, was aber auch die Sicherheit deutlich eingrenzt. Mit Root-Zugriff haben Sie die Möglichkeit, ein angepasstes Android auf Ihrem Endgerät zu installieren, was Ihnen umfassende Rechte gibt. Mit Root-Rechten können Sie auch Systemprogramme austauschen, Apps auf der SD-Karte installieren, Themes installieren und Anwendungen nutzen, die Root-Rechte benötigen, zum Beispiel einige Netzwerkprogramme und Datensicherungs-Tools.

4.1.3 SMS sichern

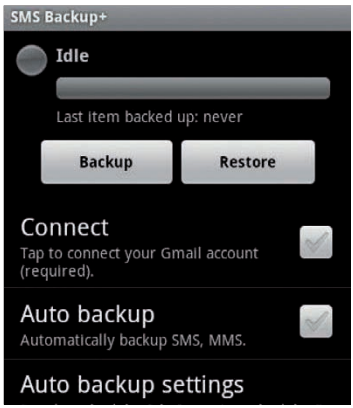
Wie bei der Sicherung von Kalender und Kontakten haben Sie aber auch die Möglichkeit die anderen Daten des Telefons, wie zum Beispiel SMS, zu sichern. Leider müssen Sie hierzu verschiedene Werkzeuge verwenden und mehrere Schritte durchführen, um das Telefon zu sichern.

SMS Backup & Restore: Mit der App lassen sich Kurznachrichten sichern.

Mit der kostenlosen App **SMS Backup & Restore** können Sie SMS sichern und wiederherstellen. Laden Sie sich die kostenlose App aus dem Market und installieren Sie diese auf dem Android. Anschließend können Sie mit der Anwendung die SMS-Nachrichten auf dem Smartphone auf der SD-Karte sichern. Achten Sie aber darauf, dass Sie auch die SD-Karte sichern müssen. Denn ist das ganze Handy weg oder auch die SD-Karte defekt, bringt Ihnen die Sicherung auf der Karte auch nichts mehr. Der Vorteil der Software ist, dass Sie die SMS-Nachrichten auf jedem

anderen Android-Handy wiederherstellen können. Zur Sicherung oder Wiederherstellung wählen Sie einfach die entsprechende Schaltfläche aus. Anschließend geben Sie einen Namen für die Sicherung ein. Das Tool sichert die SMS in einer XML-Datei. Sie haben über SMS Backup & Restore auch die Möglichkeit, den Inhalt der Datensicherungen anzusehen und diese wiederherzustellen.

Synchronisierung: SMS und Anruflisten über Goolgle Mail mit SMS Backup+ sichern.

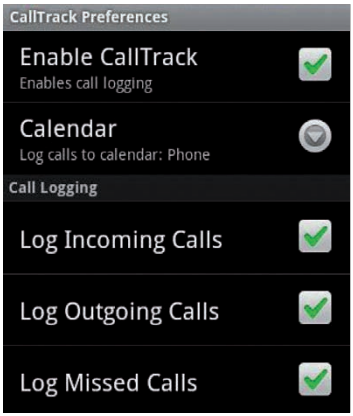


Eine weitere Möglichkeit, SMS-Nachrichten zu sichern, ist **SMS-Backup+**. Im Gegensatz zu SMS Backup & Restore speichert SMS Backup seine Daten nicht auf dem Smartphone, sondern lädt sie in einen Google-E-Mail-Account. Die Software kann aber nur Daten sichern, keine wiederherstellen. Im Market können Sie auch SMS Backup+ herunterladen. Diese Anwendung ist ebenfalls kostenlos und ermöglicht die automatische Datensicherung von SMS-Nachrichten. Die Anwendung kann die Anruflisten sichern und auf anderen Android-Handys wiederherstellen. Dazu nutzt SMS Backup+ ebenfalls die Synchronisierung mit einem Google-Mail-Konto. Haben Sie das gleiche Konto auf einem anderen Android-Gerät verbunden, können Sie die Daten zurücksichern. Allerdings sind hier viele Benutzererfahrungen nicht gerade positiv. Aus diesem Grund sollten Sie vorher testen, ob die Wiederherstellung bei Ihnen auch optimal funktioniert. Sie müssen zur Sicherung erst einen Google-Mail-Account hinterlegen – dies empfiehlt sich bei der vollständigen Nutzung eines Android-Smartphones ja aber ohnehin.

4.1.4 Anruflisten und Favoriten sichern mit Call Logs Backup & Restore

Um Ihre Anruflisten mit dazugehörigen Nummern zu sichern, können Sie, neben dem erwähnten SMS Backup+, die Anwendung **Call Logs Backup & Restore** verwenden. Die Software speichert die Daten ebenfalls in einer XML-Datei und er-

möglicht die automatische Sicherung. Sie können diese Daten mit jedem XML-Reader oder auch mit einem Browser öffnen und den Inhalt lesen.



CallTrack: Anrufe lassen sich mit der Anwendung ordentlich protokollieren.

Interessant in diesem Bereich ist zudem die kostenlose Anwendung **CallTrack**. Haben Sie auf dem Android-Handy auch eine Synchronisierung mit dem Google Kalender eingerichtet, können Sie mit der Anwendung Telefonlisten in Ihrem Kalender synchronisieren lassen. Sobald Sie einen Anruf getätigt, entgegengenommen oder verpasst haben, erstellt CallTrack einen Kalendereintrag mit Namen, Nummer und Dauer des Anrufs. Auf diese Weise haben Sie eine optimale Übersicht über Ihre getätigten Anrufe. Setzen Sie keinen Google-Kalender ein, kann die Anwendung diese Daten auch auf dem lokalen Kalender speichern. In diesem Fall verfügen Sie aber über keine Datensicherung, sondern nur über eine Protokollierung der Anrufe. Wer sein Android-Gerät zum Surfen benutzt, sollte auch die Favoriten auf dem Gerät sichern. Dazu gibt es zum Beispiel die kostenlose App **Bookmark Sort & Backup**. Sie kann die Favoriten sichern und auch wiederherstellen. Die Verwaltung und Sortierung übernimmt die Anwendung gleichfalls. Die App kann zwar keine anderen Daten sichern, aber wer sein Android-Handy wechselt oder die Favoriten zwischen PC und Android synchronisieren will, ist mit Bookmark Sort & Backup gut beraten.

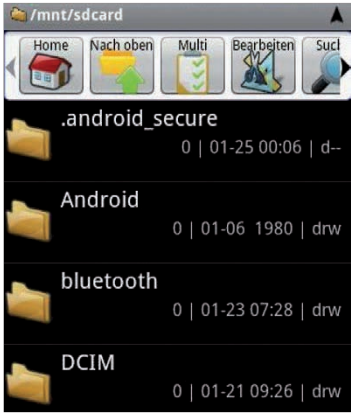
4.1.5 Anwendungen und Verzeichnisse sichern

Android bietet serienmäßig keine effiziente Möglichkeit, Anwendungen optimal zu sichern. Nur Anwendungen, die auf dem Android-Endgerät über den Market installiert wurden, bieten auch die Möglichkeit für ein automatisches Update.

Wollen Sie dennoch die lokal installierten Anwendungen sichern, bietet sich zum Beispiel die Anwendung **Astro Datei-Manager** an. Diesen laden Sie ebenfalls über

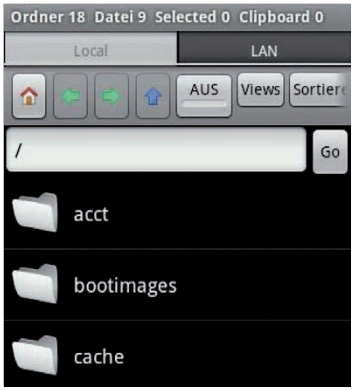
den Market herunter. Die App gibt es als kostenlose Testversion oder als Vollversion für 2,93 Euro. Der Datei-Manager ermöglicht die Verwaltung und Sicherung von Ordnern auf dem Android-Gerät und die Sicherung auf der SD-Karte.

Ordnungshalber: Mit dem Astro Datei-Manager lassen sich Ordner sichern.



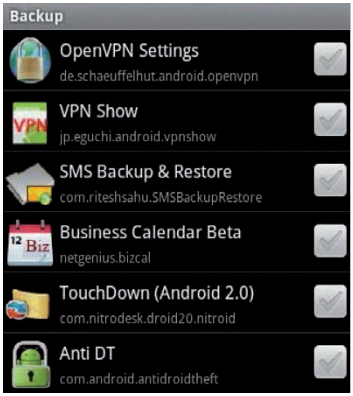
Über den Datei-Manager sichern Sie zusätzlich alle anderen Daten auf dem Gerät. Wer wichtige Dokumente, Fotos oder andere Dateien auf dem Android sichern will, ist mit der kostenpflichtigen Version gut beraten. Ein weiterer beliebter Datei-Manager ist **Linda Manager**. Auch dieser kann auf Daten des Telefons zugreifen und diese sichern.

Im Zugriff: Mit dem Linda Manager kann man auf Daten zugreifen und diese sichern.



Eine weitere App für die Verwaltung von Ordnern ist **File Manager**. Auch diese App steht kostenlos im Market zur Verfügung. Mit der App können Sie Daten auf SD-Karte und dem Telefonspeicher sichern. Die Sicherung von Apps beherrscht

die Anwendung gleichfalls, ebenso das Packen und Entpacken von Archiven. Zur Sicherung des kompletten Telefons eignet sich die App **Backup Everything**. Das Tool steht ebenfalls kostenlos im Market zur Verfügung. Im Gegensatz zu anderen Anwendungen benötigt diese App keine Root-Rechte, kann dafür aber nicht alles sichern. Die Daten sichert das Tool auf SD-Karte. Teilweise hat die Anwendung Probleme bei der Wiederherstellung von Kontakten auf verschiedenen Geräten.



Transporthilfe: Sichern der Liste von installierten Apps auf Android.

Wer nur eine Liste seiner Anwendungen mit einer Verknüpfung zum Market sichern will, kann die kostenlose App **Zemna AppList Backup** einsetzen. Auf einem neuen Android-Handy können Sie auf diese Weise die vorher installierten Anwendungen leicht über den Market erneut installieren. Um seine Apps zu sichern, können Sie auch die Anwendung **AppMonster** testen. Auch sie steht kostenlos zur Verfügung und ermöglicht die leichte und schnelle Sicherung der installierten Anwendungen. Allerdings kann das Tool keine weiteren Daten sichern.

4.1.6 Sichern mit Root-Rechten – Titanium Backup und MyBackup

Wer seine kompletten Einstellungen und auch Daten effizient sichern und dabei nur auf ein einzelnes Programm setzen will, kommt um Root-Rechte nicht herum.

Eine der beliebtesten Anwendungen zur Sicherung von gerooteten Android-Geräten ist **Titanium Backup Root**. Die Anwendung steht kostenlos im Market zur Verfügung und kann Daten und Apps auf dem Endgerät sichern und wiederherstellen. Um effizient ein Android zu sichern, kommen Sie um diese App nicht herum, müssen aber vorher das Telefon rooten. Wer sein Android ohnehin schon gerootet hat, findet mit der App die derzeit beste Sicherungslösung. Ohne Root-Rechte kann die Anwendung nicht starten.

MyBackup: Die komplette Sicherung des Telefons erfordert Root-Rechte.

Eine weitere bekannte Sicherungssoftware, die Root-Rechte benötigt, ist **MyBackup**. Auch sie kann Android-Handys optimal sichern. MyBackup und Titanium Backup haben einen ähnlichen Funktionsumfang. Welche der Anwendungen für Sie am besten geeignet ist, müssen Sie selbst ausprobieten, denn nicht alle Anwendungen laufen auf allen Endgeräten gleich stabil.

4.1.7 Fazit

Wer eine Datensicherung seines Android-Smartphones durchführen will, sollte sich vorher darüber im Klaren sein, welche Daten gesichert werden sollen. Eine universale Lösung ist ohne Root-Rechte schwer möglich. Sie können entweder Sicherungen auf der internen SD-Karte vornehmen oder mit einem Google-Konto synchronisieren. Außerdem müssen Sie darauf achten, ob die Anwendung auch automatisch Daten sichern kann und welche Daten die einzelnen Tools überhaupt sichern. In der Regel benötigen Sie zur Sicherung mehrere Tools, zumindest wenn Sie das Gerät nicht rooten wollen. Ein manuelles Backup birgt die Gefahr, dass Anwender dieses vergessen oder gerade die Daten nicht gesichert sind, die bei einem Datenverlust notwendig sind. Wer alle Daten auf dem Android schnell und einfach sichern will, muss das Gerät rooten und eine Anwendung einsetzen, die über diese gerooteten Rechte das komplette Endgerät sichert. Ein weiteres Problem bei Datensicherungsanwendungen für Android ist die Vielzahl der verfügbaren Geräte und Hersteller. Nicht alle Anwendungen laufen auf allen Geräten problemlos, und auch wenn der erste Eindruck positiv ist, ist nicht sicher, dass die Sicherungs-App auch optimal in allen Bereichen funktioniert. Hier offenbaren sich erfahrungsgemäß oft bei der Wiederherstellung Schwächen. Aus diesem Grund sollten Sie nicht nur die Sicherung testen, sondern auch ausgiebig die Wiederherstellung. Anwender sollten in jedem Fall das mitgelieferte Sicherungsprogramm des Android einsetzen und bei Drittherstellerprodukten ausführlich testen.

Thomas Joos

4.2 Android-Praxis: VPN einrichten und nutzen

Sollen Anwender eine sichere Verbindung über das Internet mit Ressourcen im Unternehmen aufbauen, ist eine Anbindung per VPN der beliebteste und sicherste Weg (siehe auch Ratgeber – Sicherer Netzzugang mit VPN-Technologie, Webcode **2024769**). Auf dem Client ist dazu einfach eine Verbindung zum VPN-Server einzurichten, und mit einem Klick befindet sich das Endgerät im Firmennetzwerk, gesichert durch eine verschlüsselte Verbindung. Prinzipiell können sich auch Smartphones per VPN mit dem Firmennetzwerk verbinden. So sind die notwendigen Clients in den aktuellen Versionen von iPhone (iOS), Windows Phone 7 und Android integriert. Allerdings fehlt Android eine Unterstützung in Sachen integrierter Verschlüsselung oder hinsichtlich des Ablaufens von Passwörtern. Generell finden nur VPNs auf Basis von OpenVPN (openvpn.net) und PPTP/IPsec optimal Unterstützung. Wie mit dem iPhone oder mit Windows-Phone-7-Geräten kann man auch mit Android-Smartphones eine VPN-Anbindung standardmäßig aufbauen, allerdings ist in vielen Fällen etwas Mehrarbeit erforderlich.

4.2.1 Android und VPN

Wer vernünftig mit VPN arbeiten und zusätzliche Apps für den Verbindungsaufbau nutzen will, muss das Android häufig „rooten", da die meisten VPN-Apps erweiterte Rechte benötigen und die Standardrechte des Benutzers nicht ausreichen.

Android basiert auf Linux (Android 2.2 beispielsweise auf Kernel 2.6) und verwendet wie dieses ebenfalls das Root-Prinzip. Der normale Anwender des Smartphones hat keine weitreichenden Rechte, sondern nur der Benutzer Root. Dieser ist der Administrator des Geräts. Anwender können sich aber selbst sehr leicht diese Root-Rechte zuweisen (rooten); hierzu gibt es zahlreiche Anleitungen im Internet. Durch diese Lücke können Anwender dann alles auf dem Android durchführen und installieren, was technisch möglich ist, zum Beispiel auch Systemprogramme. In den meisten Fällen ist dazu aber eine Aktualisierung des Systems notwendig. Standardmäßig unterstützt Android PPTP mit Shared Secret, L2TP und L2TP/IPSec entweder mit Zertifikat oder Shared Secret.

Mit Android 2.1/ 2.2 lassen sich zwar viele VPNs über den integrierten Standard-Client einrichten, aber längst nicht alle. Die erste Wahl sollte immer die Verwendung des internen Clients sein, da dieser keine Root-Rechte benötigt und kompatibel mit vielen VPN-Servern ist. Außerdem ist der Client sehr einfach einzurichten und von Anwendern leicht zu bedienen. Vor allem, wenn Sie zusätzliche VPN-Clients, zum Beispiel für den Aufbau zu speziellen Geräten wie SonicWALL oder Cisco, verwenden wollen, lassen sich diese Clients nur mit Root-Rechten installieren und konfigurieren. Außerdem unterscheiden sich die verschiedenen Geräte der unterschiedlichen Hersteller sehr stark voneinander. Clients, die auf dem einen

Mobiltelefon laufen, müssen nicht zwingend auf allen Android-Handys funktionieren. Hier sind vor dem Einsatz grundlegende Tests angesagt.

4.2.2 VPN einrichten und Router anpassen

Für die meisten VPNs benötigen Sie keinen gesonderten VPN-Client, sondern können den internen Client in Android verwenden. Generell ist die Verwendung eines kompatiblen VPNs die beste Lösung, weil Sie dann auf dem Android keine Änderungen vornehmen müssen und die Anbindung stabil läuft.

Leider funktioniert der Standard-Client aber nicht mit allen VPN-Servern, sodass in vielen Fällen Anpassungen notwendig sind. Im Hinblick auf die Sicherheit ist das allerdings nicht immer zufriedenstellend. Denn auch wenn Sie einen sicheren Cisco-Router als VPN-Server einsetzen, erhöhen Sie die Sicherheit für die Anwender bestimmt nicht, wenn im Gegenzug die Handys gerootet werden müssen und die Anwender fortan mit Administratorrechten auf den Handys arbeiten. So lässt sich der Cisco-kompatible Client aus dem Android-Market beispielsweise nur bei gerooteten Geräten einsetzen.

Einstellungssache: Unter der Konfiguration für Drahtlosnetzwerke findet sich auch der Punkt für die VPN-Einstellungen.

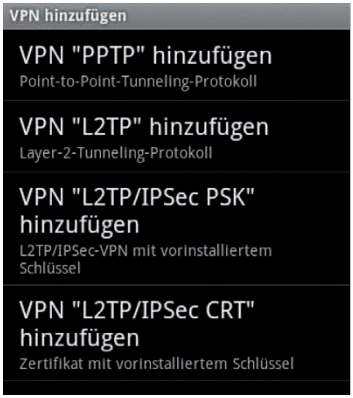
Wenn Sie ein Standard-VPN-Protokoll wie PPTP oder L2TP verwenden, müssen Sie auf den Android-Geräten meistens nichts installieren, sondern können direkt mit den Standardtools arbeiten.

Die Einrichtung nehmen Sie dann über *Einstellungen\Wireless\VPN-Einstellungen* vor. Bei der Anbindung an ein VPN verhalten sich Android-Handys wie PCs. Sie benötigen einen VPN-Server, der auch für andere Geräte die Verbindung zur Ver-

fügung stellt. Smartphones brauchen keinen eigenen VPN-Server, sondern begnügen sich mit einem VPN-Router oder einem Windows- beziehungsweise Linux-Server. Die Anbindung erfolgt über interne Einstellungen in Android, oder über zusätzliche Apps, die Sie aus dem Market installieren.

4.2.3 VPN auf dem Smartphone einrichten

Wenn Sie in den VPN-Einstellungen auf *VPN hinzufügen* klicken, können Sie auf der nächsten Seite auswählen, welche Art von VPN Sie aufbauen wollen. Als Protokolle unterstützt Android L2TP/IPSec und PPTP. VPN-Datenverkehr, der auf Point to Point Tunnel Protocol (PPTP) basiert, besteht aus einer TCP-Verbindung zum TCP-Port 1723 auf dem VPN-Server. Diese Art von VPN ist am einfachsten zu betreiben, und so gut wie jeder VPN-Server beherrscht diese Technik. Um Probleme zu vermeiden, muss die Firewall TCP-Verbindungen auch als Generic-Routing-Encapsulation (GRE)-gekapselte Daten ermöglichen.



Verbindungsfrage: Hier wählen Sie die Art der VPN-Verbindung aus.

Nachdem die Authentifizierung am VPN-Server erfolgt ist, verschlüsselt ein PPTP-VPN die Verbindung. Die Verschlüsselung baut auf dem Kennwort der Authentifizierung auf. Je komplexer das Kennwort, umso besser die Verschlüsselung. Die zweite Variante ist das Layer 2 Tunnel Protocol (L2TP). Dieses Protokoll ist in Verbindung mit IPSec sicherer als PPTP, aber dafür auch komplexer in der Einrichtung. L2TP verwendet IPSec, um eine Verschlüsselung aufzubauen. Beim Aufbau eines VPN mit L2TP wird der Datenverkehr, im Gegensatz zu PPTP, bereits vor der Authentifizierung zuverlässig verschlüsselt. Da L2TP zur Verschlüsselung des Datenverkehrs IPSec verwendet, können Sie mit diesem VPN-Typ auch eine 3DES-Verschlüsselung durchführen. Der Einsatz eines VPN auf Basis von L2TP setzt eine Zertifizierungsstelleninfrastruktur voraus, und Sie müssen auf dem Android ein Zertifikat installieren. Das ist aber beispielsweise per SD-Karte kein Problem.

Übergabe: Nach der Auswahl des VPN sind dessen Daten einzugeben.

Haben Sie sich für eine Variante entschieden, müssen Sie die Daten des VPN eingeben. Bei der Einrichtung von PPTP-VPN handelt es sich um einen freien Namen, die IP-Adresse oder DNS-Namen des VPN-Servers sowie die Anmeldedaten. Wenn Sie mit einem zertifikatgesicherten VPN arbeiten, müssen Sie vor dem Verbindungsaufbau das Zertifikat auf die SD-Karte des Android kopieren und über *Einstellungen\Standort und Sicherheit\Von SD-Karte installieren* installieren.

4.2.4 Verbindung aufnehmen

Haben Sie alle Daten eingegeben, können Sie sich jederzeit mit dem VPN verbinden, wenn Sie zu *Einstellungen\Wireless\VPN-Einstellungen* wechseln.

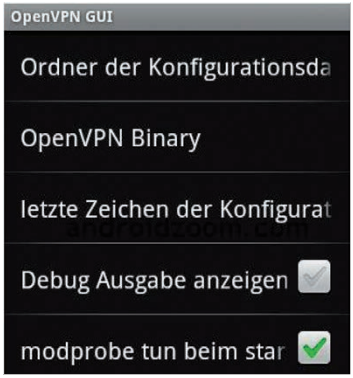
Die Einrichtung und das Aufrufen von VPNs vereinfacht beispielsweise die App **VPN Show** aus dem Market. Diese hat aber keine andere Funktion, als einfach sofort direkt in das Fenster zur Konfiguration der VPNs zu springen. Sie ersparen sich also lediglich die Navigation zu den Standardeinstellungen des Telefons. Anwender, die häufiger auf VPNs zugreifen müssen, können auf diese Weise die Verbindung schneller starten. Ohne eine solche App müssen Sie sich für jeden Verbindungsaufbau erst zu den *VPN-Einstellungen* hangeln. Da es sich bei dieser App nur um eine Hilfe beim Aufrufen der VPN-Verbindungen handelt, benötigt sie keine Root-Rechte. Bauen Anwender eine VPN-Verbindung auf, müssen sie Benutzernamen und Kennwort eingeben. Das Kennwort lässt sich allerdings nicht dauerhaft speichern. Auch hier kann eine App aus dem Market wertvolle Hilfestellung leisten: Mit der **5 VPN App** können Sie VPN-Verbindungen leichter aufbauen und Kennwörter für die Verbindung speichern. Diese App benötigt ebenfalls keine Root-Rechte, erleichtert den Umgang mit VPNs aber deutlich.

4.2.5 OpenVPN und Cisco-VPN mit Android

Unternehmen, die OpenVPN einsetzen, können Android-Handys per VPN verbinden, indem sie die App OpenVPN aus dem Market auf den Endgeräten installieren. Wenn Sie OpenVPN verwenden, benötigen Sie auch einen OpenVPN-Server, der

die Anfragen entgegennimmt (siehe auch Workshop: Sichere Einwahlverbindungen mit OpenVPN auf einem Windows-Server , Webcode **2027706**).

OpenVPN baut auf SSL auf und ist bezüglich der Konfiguration sehr flexibel. Die Authentifizierung kann über Zertifikate oder über Shared Secrets erfolgen. Die Verbindungsdaten geben Sie dann im Client auf dem Handy ein. Damit Sie die App **OpenVPN GUI (Root)** verwenden können, benötigen Sie Root-Rechte auf dem Telefon. Eine weitere App, die die Einstellung von OpenVPN auf dem Android vereinfacht, ist **OpenVPN Settings**. Auch diese App benötigt Root-Rechte. Bei beiden Apps können Sie die Konfiguration in einer Konfigurationsdatei hinterlegen und über eine USB-Verbindung auf die Android-Handys übertragen. Als VPN-Server lassen sich problemlos Internet-Router einsetzen. Selbst kleinere Router für den Heimeinsatz sind in vielen Fällen kompatibel zu OpenVPN-Clients auf Android-Geräten.



Vorbedingung: Damit Sie die App OpenVPN GUI (Root) verwenden können, benötigen Sie Root-Rechte auf dem Telefon.

Wenn Sie spezielle Router für die Anbindung per VPN einsetzen, sollten Sie im Market überprüfen, ob es angepasste VPN-Clients in Form von Apps gibt. Der große Nachteil dieser Apps ist aber, dass so gut wie alle Root-Rechte benötigen. Das mag bei Android-Handys von Administratoren noch in Ordnung sein, aber bei Otto Normalanwender sollten die Telefone nicht in diesem Modus agieren.

Zum Beispiel stellt auch SonicWALL für die meisten seiner Geräte im Market eine VPN-App zur Verfügung. Wollen Sie ein VPN mit einem Cisco-Router aufbauen, müssen Sie in jedem Fall das Smartphone rooten. Anschließend benötigen Sie die App **VPNC**, die die Verbindung zu Cisco-Routern ermöglicht. Arbeiten Sie mit speziellen Geräten, wie zum Beispiel SonicWALL, ist natürlich nicht immer ein gesonderter Client notwendig. Sie können in den meisten Fällen auch mit den Standardeinstellungen in Android arbeiten, wenn der VPN-Server entsprechend konfiguriert ist. Verwenden Sie zum Beispiel ein VPN mit der Einstellung L2TP/IPSec PSK-VPN auf dem Android, deaktivieren Sie die Option *L2TP-Schlüssel aktivieren* in den Einstellungen, wenn die Verbindung nicht funktioniert.

Konfiguration: Ein L2TP-VPN unter Android einrichten.

4.2.6 Fazit

Wenn Unternehmen auf Standard-VPN-Protokolle wie PPTP und L2TP setzen, haben sie die Chance, dass sich Android-Smartphones problemlos verbinden lassen. Da sich an dieser Stelle aber die verschiedenen Hersteller respektive deren Geräte deutlich unterscheiden, sind grundlegende Tests erforderlich. Wer Android-Handys mit dem Firmen-VPN verbinden will, sollte auf jeden Fall nur auf kompatible Verbindungen setzen und die Installation von zusätzlichen Apps vermeiden. Da viele VPN-Clients Root-Rechte auf den Telefonen benötigen, sind diese Clients für den Durchschnittsanwender schlicht und ergreifend ungeeignet. Vor allem die fehlende Unterstützung von Cisco-VPN kann für größere Unternehmen oft problematisch sein. Administratoren jedoch, die Systemanwendungen auf dem Gerät installieren müssen und das Handy ohnehin rooten, können selbstverständlich die erweiterten Möglichkeiten nutzen.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

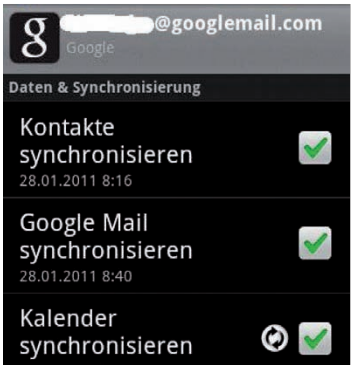
TecChannel-Links zum Thema	Webcode	Compact
Android-Praxis: VPN einrichten und nutzen	2033962	S.192
Android – Datensicherung in der Praxis	2034104	S.184

4.3 Android-Praxis: Kalender richtig synchronisieren

Wer unterwegs seine Termine verwalten oder überprüfen will, hat mit Android-Smartphones zahlreiche Möglichkeiten der Kalendersynchronisierung. Am besten bietet es sich an, den Kalender für die eigene Terminplanung zu verwenden, der ebenfalls im E-Mail-Account für die Synchronisierung hinterlegt ist. Setzen Sie einen anderen Kalender ein, empfiehlt es sich, die Daten zu exportieren und im E-Mail-Konto zu importieren. Besonders geeignet dazu sind natürlich Exchange-Postfächer oder Google-Mail-Konten. Verwenden Sie ein E-Mail-Programm auf Ihrem PC, zum Beispiel Outlook, können Sie auch hier den Weg gehen, die Daten zunächst mit einem Google-Konto zu synchronisieren und das Google-Konto dann an Android anzubinden. Nachfolgend haben wir die verschiedenen Lösungswege sowie nützliche Apps für Sie zusammengestellt.

4.3.1 Android-Terminverwaltung

Sobald Sie ein E-Mail-Konto an das Android-Gerät angebunden haben, zum Beispiel über Exchange- ActiveSync oder Google-Mail, aktiviert Android gleichzeitig die Synchronisierung des Kalenders. Um diese Konfiguration zu überprüfen, klicken Sie auf *Einstellungen\Konten & Synchronisierung* und wählen dann das Konto aus, das Sie synchronisieren wollen. Sie können für E-Mail-Konten an dieser Stelle die generelle Aktivierung der Synchronisierung für Kontakte, E-Mail und Kalender aktivieren oder deaktivieren. Weitere Einstellungen können Sie an dieser Stelle nicht vornehmen.



Zusammenspiel: An dieser Stelle konfigurieren Sie die Kalendersynchronisierung in Android.

Den Standardkalender von Android finden Sie in den Anwendungen. Er bietet zwar keine komfortable Oberfläche, reicht aber zumindest aus, um eine rudimen-

täre Terminverwaltung durchzuführen. Hier unterscheiden sich iPhone und Android kaum voneinander. Bei beiden Systemen brauchen Sie zusätzliche Anwendungen, wenn Sie Termine effizient verwalten müssen. Wollen Sie zum Beispiel Besprechungsanfragen beantworten, kann das die Standard-App in Android nicht optimal, HTC-Androids arbeiten hier etwas besser, aber keineswegs optimal.

Der Kalender unterscheidet sich bei vielen Herstellern von Android-Smartphones, in den Anwendungen finden Sie aber meistens die Standard-App für den Kalender von Android. Wer sich allerdings professioneller mit Terminen auf Android-Handys befassen und seine Terminplanung möglichst effizient auf dem Smartphone verwalten will, kommt um zusätzliche Apps nicht herum. Gute Apps kosten zwar Geld, erhöhen den Nutzen der Kalenderverwaltung jedoch extrem. Welche Apps dazu am besten geeignet sind, zeigen wir Ihnen in den folgenden Abschnitten.

4.3.2 Widgets, Apps und Homescreen konfigurieren

Wenn Sie mit Android-Anwendungen arbeiten, müssen Sie zwischen Widgets und Apps unterscheiden. Apps laden Sie aus dem Market, um die Funktionalität des Handys mit Zusatzleistungen zu erhöhen. Viele Apps enthalten auch Widgets, und manche Apps im Market sind eigentlich keine App, sondern ein Widget.

Widgets sind Erweiterungen des Homescreens des Androids, also des Standardbildschirms, den Sie sehen, wenn Sie den Bildschirm starten. Solche Widgets haben keine weitere Funktionalität wie Apps, sondern dienen hauptsächlich der Anzeige von Informationen aus Apps, zum Beispiel der Kalender-App. Welche Widgets Sie auf dem Homescreen anzeigen wollen, können Sie dort selbst bestimmen: Klicken Sie mit dem Finger auf einen leeren Bereich. Anschließend öffnet sich ein neues Fenster, über das Sie zusätzliche Anwendungen hinzufügen können.

Widgets: das Auswählen von Widgets für den Homescreen.

Wenn Sie im neuen Fenster *Widgets* auswählen, können Sie aus einer Auswahl der installierten Widgets für diejenige entscheiden, die Sie auf dem Homescreen anzeigen wollen. Die Standard-Kalender-App hat ebenfalls ein Widget, das Sie dort anzeigen können. Haben Sie das Widget ausgewählt, sehen Sie es künftig auf dem Homescreen. Durch Anklicken eines Widgets können Sie die dazugehörige App öffnen, wenn eine solche vorhanden ist. Über das Widget der Standardkalender-App können Sie zum Beispiel direkt in Ihre Terminplanung wechseln und die aktuellen Termine des Tages oder des Monats einsehen.

Wollen Sie ein Widget vom Homescreen entfernen, halten Sie den Finger auf das Widget und ziehen es auf den Papierkorb, der unten erscheint. Sobald es rot aufleuchtet, entfernt Android es vom Homescreen; sie können es aber jederzeit wieder darauf integrieren. Viele Apps, die Sie aus dem Market installieren, haben ein dazugehöriges Widget, das Sie auf dem Homescreen integrieren können. Über dieses Widget erhalten Sie zum Beispiel Termin-Infos und können die dazugehörige Anwendung direkt starten. Apps finden Sie in den Anwendungen auf dem Android im unteren Bereich bei den Downloads.

4.3.3 Apps für die Terminverwaltung

Setzen Sie zur Synchronisierung den Google-Kalender ein, ist eine der besten App zur Kalenderverwaltung die Anwendung **CalenGoo**. Diese ist für die Anzeige des Google-Kalenders optimiert und beherrscht verschiedene Kalenderansichten (Tag, Woche, Monat, Liste, Querformat). Die Ansichten lassen sich anpassen, und das Anlegen von Terminserien ist sehr gut gelöst.

Business Calendar Beta: eine komfortable App für die Terminverwaltung.

Durch die direkte Synchronisierung mit dem Google-Kalender lassen sich auch Icons und ältere Kalenderdaten synchronisieren. Die Schalter am Android-Handy können Sie zur Steuerung des Kalenders ebenfalls frei belegen, beispielsweise um zum aktuellen Datum zu springen. Die Synchronisierung der Google-Aufgaben ist

gleichfalls möglich. Die App kostet aktuell 4,53 Euro und erleichtert Anwendern, die viele Termine planen, das Leben.

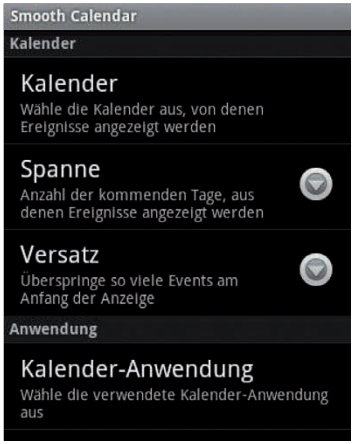
Wer für eine App kein Geld ausgeben will und dennoch eine bessere Anwendung sucht als die Standard-App, findet im **Business Calendar Beta** eine ebenfalls wertvolle und kostenlose Alternative – wie lange die App kostenlos bleibt, lässt sich nicht genau sagen. Sie installieren sie direkt über den Market.

Die App ist für den Google-Kalender optimiert. Das heißt, alle Termine, die Sie in der App pflegen, synchronisiert diese mit dem Google-Konto. Die App kann stufenlos Mehrtagesansichten erstellen und lässt sich vielfältig konfigurieren. Wenn Sie mehrere Kalender im Google-Kalender anlegen, kann die App auch diese verwalten sowie einzeln ein- und ausblenden. Die Erstellung von Terminen ist ebenfalls sehr übersichtlich. Zum Business Calendar Beta gehört ein Widget, das Sie auf dem Homescreen einblenden können. Es zeigt die Termine des aktuellen Tages an und ermöglicht das direkte Öffnen des Kalenders.

4.3.4 Weitere praktische Kalender-Apps

Eine weitere interessante App ist **Smooth Calendar**. Sie ist ebenfalls kostenlos und besteht aus einem Widget, das Sie auf dem Homescreen des Android einblenden können. Auf diese Weise haben Sie alle Termine des Tages im Blickfeld, ohne den Terminkalender öffnen zu müssen. Das Widget bietet vielfältige Einstellungsmöglichkeiten, was den anderen Kalender-Apps oft fehlt. Sie können mit dem Widget natürlich ebenso die Termine anzeigen, die Sie mit einer anderen Kalender-App erstellt haben. Die App dient lediglich der Anzeige und startet die Kalender-App, die Sie in der Konfiguration eintragen. Zur Einrichtung rufen Sie die Einstellungen der Apps in den Anwendungen auf dem Android-Smartphone auf.

Im Blickfeld: das Smooth-Calendar-Widget konfigurieren.



Eine weitere kostenlose Kalender-App ist **Pocket Informant**; auch sie steht im Market zur Verfügung. Im Gegensatz zu vielen anderen Kalender-Apps kann diese Anwendung Termine mit unterschiedlichen Farben kennzeichnen, was bei der Unterscheidung zwischen privaten und beruflichen Terminen sehr hilfreich sein kann. Mit diesem Kalender können Sie mehrere Ansichten definieren, Filter festlegen, Aufgaben verwalten und Vorlagen für Termine speichern.

Die App nutzt die Datenbank des Android-Kalenders, kann also alle Kalender einsetzen, die Sie auch in Android als Konto verwenden können. Die generelle Übersicht von Pocket Informant ist sehr gut,, und die Verwaltung von Aufgaben und Terminen ist gut gelöst. Die Anwendung hat kein eigenes Widget für den Homescreen, Sie können aber problemlos in den Einstellungen von Smooth Calendar den Pocket Informant als Kalenderanwendung auswählen. Wenn Sie dann Smooth Calendar einblenden, können Sie direkt über das Widget Pocket Informant starten. Die Anwendung kann allerdings keine Aufgaben mit Exchange oder Lotus Notes synchronisieren.

4.3.5 Outlook direkt mit Android synchronisieren – Kalender und Kontakte

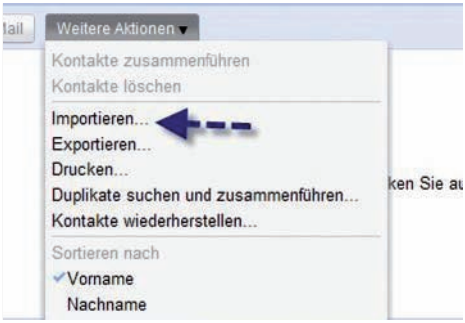
Wer mit dem Android-Smartphone seinen Outlook-Kalender synchronisieren will, kann die Anwendung Outlook **USB-Sync nutzen**. Mit Bordmitteln kann Android leider keine Synchronisierung mit Outlook vornehmen – ein erheblicher Nachteil gegenüber Windows-Phone-7-Geräten und Apples iPhone.

Die Anwendung für das Android-Gerät steht kostenlos zur Verfügung, Sie benötigen aber auf dem PC, mit dem Sie synchronisieren wollen, eine kostenpflichtige Zusatzlösung. Die App kann Kalender und Kontakte mit Outlook, Outlook mit Business Contact Manager, Lotus Notes, Sage ACT!, GroupWise, Palm Desktop, und Salesforce CRM synchronisieren und bietet dabei umfangreiche Anzeigemöglichkeiten. Sie benötigen für die App noch die Zusatzsoftware **CompanionLink** auf dem PC. Die deutsche Oberfläche ist nicht optimal übersetzt, aber die Anwendung funktioniert auf den meisten Android-Geräten problemlos. Anwender, die professionell Daten zwischen Outlook und Android-Geräten synchronisieren wollen, finden mit dem Bundle CompanionLink und Outlook USB-Sync eine wertvolle Möglichkeit, die derzeit im Bereich Android unübertroffen ist.

4.3.6 Outlook mit Google-Konto synchronisieren

Wer kein Geld für die Synchronisierung ausgeben will, kann sehr einfach Outlook direkt mit seinem Google-Konto synchronisieren und dann über das Google-Konto das Android-Gerät. Wollen Sie Kalender- und Kontaktdaten zwischen Google-Konto und Outlook importieren, starten Sie zunächst die Weboberfläche von Google Mail. Wählen Sie im linken Feld den Menüpunkt *Kontakte* aus, nachdem

Sie sich angemeldet haben. Sie können nicht nur Ihre Google-Mail-Kontakte nach Outlook exportieren, sondern ebenso Outlook-Kontakte in Google Mail importieren. Der Vorgang dabei ist nahezu identisch. Für den Import in Google Mail erstellen Sie am besten zunächst mit dem Export-Assistenten von Outlook eine kommagetrennte Datei. In Google Mail können Sie zwar .vcf-Dateien als Visitenkarten importieren, allerdings nur einzeln.



Einlesen: Kontakte lassen sich nach Google Mail importieren.

Um Daten zu importieren, klicken Sie als Nächstes auf *Weitere Aktionen\Importieren*, nachdem Sie im Web-Interface von Google Mail auf Kontakte geklickt haben. Klicken Sie dann auf Durchsuchen und wählen Sie auf dem Rechner die erstellte .csv-Datei aus. Sodann können Sie noch die Gruppe auswählen, in die Google Mail die Kontakte importieren soll. Wenn Sie auf *Importieren* klicken, beginnt Google Mail mit der Übertragung der Kontakte aus der Datei. Die Kontakte sehen Sie anschließend in der entsprechenden Gruppe. Sobald Sie Android mit einem Google-Mail-Konto synchronisieren, erhalten Sie auf diese Weise auch die Outlook-Kontakte auf das Android-Smartphone.

4.3.7 Hilfreiche Tools

Wenn Sie die Kontakte oder Kalendereinträge zwischen Google und Outlook nicht ständig manuell synchronisieren wollen, steht Ihnen das Tool gSyncit zur Verfügung (www.daveswebsite.com/software/gsync/). Es kostet 15 US-Dollar, für Testzwecke können Sie aber eine Evaluierungsversion herunterladen und bis zu 20 Kontakte und einen Kalender synchronisieren. Mit dem Tool können Sie automatisiert Kontakte und Kalendereinträge auch zu Exchange-Postfächern synchronisieren und diese dann mit Android synchronisieren.

Sobald Sie in Android dieses Postfach anbinden, erhält das Smartphone die Kalendereinträge und Kontakte, ohne dass Sie ein weiteres Tool oder eine zusätzliche App benötigen. Nach der Installation von gsync starten Sie die Einrichtung und erstellen eine neue Konfiguration, indem Sie auf Contact Sync und dann auf New

klicken. Anschließend geben Sie die Login-Daten zum Google-Mail-Konto ein und wählen aus, welche Kontakte Sie synchronisieren wollen und in welchen Ordner das Tool die Kontakte kopieren soll. Über die weiteren Registerkarten passen Sie die Einstellung an Ihre Erfordernisse an. Neben Kontakten können Sie über die Optionen weitere Synchronisierungsaufgaben einrichten. Über das Kontextmenü des Symbols in der Taskleiste oder automatisiert startet die Synchronisierung der Kontakte. Neben Kontakten kann das Tool Kalender und Dokumente mit Google synchronisieren.

Wollen Sie nur Kalendereinträge zwischen Google Mail und Outlook synchronisieren, können Sie ebenso das kostenlose Google-Tool Google Calendar Sync (http://pack.google.com/intl/de/pack_installer.html) verwenden; es kann allerdings keine Kontakte synchronisieren.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

TecChannel-Links zum Thema	Webcode	Compact
Android-Praxis: Kalender richtig synchronisieren	2034375	S.198
Android – Datensicherung in der Praxis	2034104	S.184
Android-Praxis: VPN einrichten und nutzen	2033962	S.192
Android-Praxis: Apps und Tipps für Admins	2034620	S.205
Android-Praxis: Bereitstellung im Unternehmen	2035262	S.213
Android-Praxis: Anbindung an Exchange	2034788	S.219
Test: Samsung Galaxy Tab 10.1	2036790	S.227
Nützliche App-Grundausstattung für Android-Smartphones	2032538	–
Die beliebtesten Android-Apps	2028765	–
Empfehlenswerte Security-Apps für Android	2034879	–

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

4.4 Android-Praxis: Apps und Tipps für Admins

Im Android Market stehen viele hilfreiche Zusatz-Tools für Administratoren parat, teilweise auch kostenlos. Damit lassen sich beispielsweise Server per RDP fernwarten, Screenshots für Anwenderanleitungen anfertigen oder Netzwerkanalysen durchführen. Wir zeigen Ihnen wertvolle Apps, die Administratoren und Power-Usern, aber auch Entwicklern das Leben mit Netzwerken und Android-Smartphones deutlich erleichtern. Leider laufen nicht alle Apps auf allen Endgeräten. Wir haben aus diesem Grund möglichst immer mehrere Alternativen vorgestellt, sofern welche verfügbar sind. Im Fokus der Tools stehen kostenlose Apps, die möglichst wenig Werbung enthalten.

4.4.1 Android – Root-Rechte sind häufig Voraussetzung

Für die Nutzung vieler Apps sind Root-Rechte erforderlich. Das heißt für Sie: Arbeiten Sie nicht mit den normalen Benutzerrechten, die deutlich eingeschränkt sind, sondern im Kontext eines Super-Users. In diesem Fall haben Sie und die Anwendungen, die Sie installieren, vollständige Rechte in Android – allerdings mit dem Nachteil, dass die Sicherheit deutlich beschränkt ist.

Mit dem Root-Zugriff haben Sie die Möglichkeit, ein angepasstes Android auf Ihrem Endgerät zu installieren, was Ihnen umfassende Rechte gibt. Mit Root-Rechten können Sie Systemprogramme austauschen, Apps auf der SD-Karte installieren, Themes installieren und Anwendungen nutzen, die Root-Rechte benötigen – beispielsweise einige Netzwerkprogramme.

Wie Sie Ihr jeweiliges aktuelles Handy rooten können, entnehmen Sie am besten den entsprechenden Anleitungen aus dem Internet. Die passenden „Howtos“ sind für nahezu jedes Gerät zu finden. Sie benötigen diese Root-Rechte aber nicht gezwungenermaßen. Nur wenn Sie dringend eine Anwendung installieren wollen, die Root-Rechte benötigt, sollten Sie solche Anleitungen umsetzen. Oft gibt es bereits fertige Tools, die ein Android-Handy rooten können. Prüfen Sie aber auf jeden Fall vorher den genauen Typ des Handys sowie den Softwarestand. Diesen sehen Sie in den *Einstellungen* über die Auswahl von *Telefoninfo*.

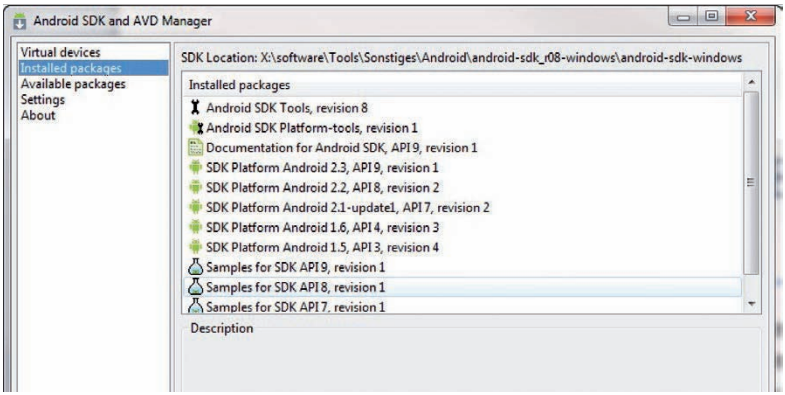
4.4.2 Java SDK und Android SDK

Softwareentwickler und Administratoren, aber auch Power-User kommen beim Einsatz von Android-Geräten nicht um das Android SDK herum – beispielsweise wenn sie Screenshots für Anleitungen anfertigen wollen oder Fehler auf dem Endgerät suchen. Dazu müssen Sie das Android-Handy per USB mit dem Computer verbinden und in die Einstellungen gehen. Klicken Sie hier auf *Anwendungen\Ent-*

wicklung und setzen den Haken bei *USB-Debugging*. Auf diesem Weg können Sie dann später mit dem Android-SDK direkt auf das Handy zugreifen.

Voraussetzung: Um auf das Handy direkt zugreifen zu können, müssen Sie in den Einstellungen das USB-Debugging aktivieren.

Das Android-SDK enthält Werkzeuge zur Entwicklung von Anwendungen, aber auch zur Verwaltung von Android-Handys. Sie müssen dazu die Anwendung nicht installieren, der Download und das Entpacken reichen vollkommen aus (http://developer.android.com/sdk/).



Ordnungshalber: Hier verwalten Sie die vorhandenen Komponenten des Android SDK.

Die Anwendungen, die auf Android-Handys laufen, basieren auf Java. Aus diesem Grund benötigen Sie das Java SDK (www.oracle.com). Sie müssen es nur in den Standardeinstellungen installieren, eine Einrichtung ist nicht erforderlich. Wenn Sie das Java SDK installiert haben, können Sie das Android SDK entpacken. Der Standard-Download enthält nicht alle Funktionen des SDK, aber Sie können diese schnell und leicht nachladen und Pakete aktualisieren, wenn Sie das Tool *SDK Manager.exe* starten – etwa wenn das SDK keine Verbindung zu Ihrem Telefon aufbauen kann, weil Dateien fehlen.

4.4.3 Screenshots anfertigen

Damit Sie das SDK nutzen können, müssen Sie den Inhalt des Ordners *platform-tools* in den Ordner *tools* kopieren. Ist der Ordner leer, laden Sie das entsprechende Paket über den Download-Manager des SDK einfach nach.

Lassen Sie dabei keine Dateien ersetzen, sondern nur Dateien kopieren. Anschließend starten Sie per Doppelklick auf die Datei ddms.bat im Verzeichnis tools des Android SDK das Tool Dalvik Debug Monitor. Dieses sollte ohne Fehlermeldung starten. Erhalten Sie eine Fehlermeldung, aktualisieren Sie das Android SDK noch einmal und kopieren Sie den Inhalt des Verzeichnisses platform-tools in das Verzeichnis tools. Im linken Teil des Fensters sehen Sie Ihr angeschlossenes Android-Handy. Dazu muss das Handy per USB verbunden sein, und auf dem Handy muss der USB-Debugging-Modus aktiviert sein.

Dalvik stellt die virtuelle Maschine zur Verfügung, mit deren Hilfe Anwendungen auf dem Android laufen. Die Funktion führt Anwendungen, die für Java Virtual Machine (JVM) entwickelt wurden, auf den Android-Handys aus. Sie haben im Dalvik Debug Monitor die Möglichkeit, über den Menüpunkt *Device* direkt auf das Android-Handy zuzugreifen sowie Daten auszulesen und zu verwalten. Über *Device\Screen capture* greift das Tool direkt auf den Bildschirminhalt des Handys zu, und Sie können einen Screenshot des aktuellen Bildschirminhalts erstellen.

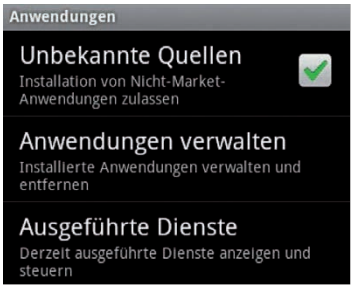
Screenshots von Android: Erstellen von Screenshots für Android-Handys mit dem Android-SDK.

Mit der App **ShootMe** aus dem Market können Sie ebenfalls Screenshots anfertigen. Allerdings müssen Sie dazu das Gerät rooten, also mit stark erweiterten Rech-

ten starten – das erinnert ein wenig an das Sprichwort „Mit Kanonen auf Spatzen schießen". Eine weitere Möglichkeit ist die Verwendung eines speziellen Treibers für Android-Handys auf dem Computer. Damit lassen sich dann über Windows Screenshots erstellen. Das Webblog Mobiles Internet stellt eine entsprechende Anleitung parat (http://mobiles-internet.buemo.net/mobiles-internet/).

4.4.4 Anwendungen außerhalb des Markets installieren – AppsInstaller

Die meisten Anwendungen für Android-Handys finden Sie im Market, den Sie direkt auf dem Handy öffnen und nach Tools durchsuchen können. Wer will, kann aber auch Anwendungen von anderen Quellen auf dem Android-Gerät installieren. Dazu benötigen Sie das Tool **AppsInstaller**, das Sie ebenfalls im Market finden. Zusätzlich zur Installation des AppsInstallers müssen Sie auf dem Handy die Installation von anderen Quellen erst genehmigen. Rufen Sie dazu *Einstellungen* auf und klicken Sie auf Anwendungen. Aktivieren Sie die Option *Unbekannte Quellen*. Denken Sie jedoch daran, dass Sie damit in Sachen Sicherheit eine potenzielle Lücke öffnen.



Erlaubnis erteilt: Die Option der Installation von Anwendungen außerhalb des Markets ist aktiviert.

Wenn Sie diese beiden Schritte durchgeführt haben, können Sie beliebige *.apk-Dateien auf das Mobiltelefon kopieren, zum Beispiel per USB. Anschließend müssen Sie das Handy vom PC trennen und das Tool Appsinstaller starten. Das Tool greift auf die Speicherkarte des Handys zu und zeigt *.apk-Dateien an. Um diese zu installieren, müssen Sie sie nur noch anklicken.

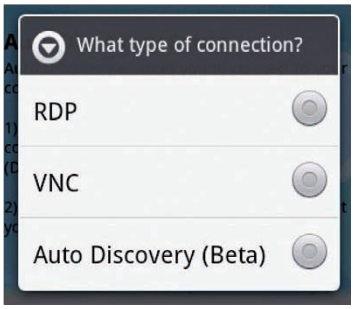
4.4.5 Mit Android-Handys auf Computer und Server zugreifen – RDP und VNC

Haben Sie in Windows den Remote Desktop aktiviert, können Sie mit einer RDP-Sitzung über das Android-Handy auf den PC oder Server zugreifen. Hierzu gibt es

sowohl kostenpflichtige als auch kostenlose Tools im Market. Das Tool **Wyse PocketCloud RDP/VNC** ist kostenlos und erlaubt die Fernwartung von Computern per RDP und VNC. Beim Starten der Anwendung wählen Sie aus, ob Sie eine RDP- oder eine VNC-Sitzung aufbauen wollen.

Haben Sie diese Auswahl getroffen, geben Sie auf der nächsten Seite IP-Adresse und Anmeldedaten für den Computer ein. In der kostenlosen Version können Sie nur die Daten eines einzelnen Computers eingeben.

Fernzugriff: RDP und VNC zur Fernwartung von Computern oder Servern sind per kostenloser App möglich.



Ein weiteres kostenloses Tool ist Remote RDP Lite. Das Tool unterstützt aber nur das RDP-Protokoll, nicht VNC. Arbeiten Sie mit dynamischen IP-Adressen und Diensten wie DynDNS zur Auflösung dieser Adressen, können Sie von unterwegs auf den heimischen Rechner zugreifen. Dazu müssen Sie im Router den Port 3389 vom Internet-Router auf den Server weiterleiten lassen, den Sie fernwarten wollen.

Arbeiten Sie nur mit VNC, gibt es im Market vor allem drei beliebte und kostenlose Anwendungen:

- **Wyse PocketCloud** (siehe oben)
- **Android-vnc-viewer**
- **Remote VNC**

Welche der Anwendungen Sie bevorzugen, hängt zum Gutteil vom persönlichen Geschmack ab. Es spricht aber auch nichts dagegen, alle drei Apps zu installieren.

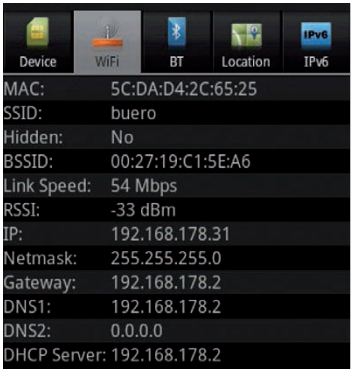
4.4.6 Netzwerkscanner und -übersicht

Admins, die Ihr Android-Handy mit dem Netzwerk verbunden haben, finden im Market zahlreiche kostenlose Anwendungen, die Netzwerkübersichten zur Verfügung stellen und Ihnen alle Geräte im Netzwerk anzeigen können.

Ein Pflicht-Tool für Admins, die Android-Handys verwenden, ist die App **Overlook Fing**. Das Tool zeigt innerhalb weniger Sekunden alle Systeme im Netzwerk an und liefert einen schnellen Überblick über die vorhandenen IP-Adressen,

MAC-Adressen und DNS-Namen, wenn diese verfügbar sind. Sie müssen die Anwendung nur starten, um den Scan-Vorgang zu beginnen. Zusätzlich wird der Hersteller des Gerätes angezeigt. Klicken Sie ein einzelnes Gerät an, können Sie diesem einen eigenen Namen oder ein spezielles Icon zuweisen, das die App beim nächsten Scan-Vorgang anzeigt.

Ein weiteres wertvolles, aber trotzdem kostenloses Tool ist **Network Info II**. Es zeigt Ihnen detaillierte Informationen zum aktuellen Netzwerkstatus des Handys an. Wenn Sie das Tool starten, sehen Sie die aktuelle IP-Adresse des Handys und können Daten über das derzeit verbundene Telefonnetz oder WLAN anzeigen lassen. Zusätzlich können Sie auslesen, was das Gerät als Ihren aktuellen Standort übermittelt, und Sie erhalten die Geschwindigkeit des verbundenen WLANs, den Namen, die IP-Adresse des DHCP-Servers und die DNS-Server angezeigt. Die Daten, die sich auslesen lassen, können Sie kopieren, beispielsweise zu Dokumentationszwecken oder bei der Fehlersuche.



Netzwerk-Apps für Android: Anzeigen von Informationen zum aktuellen WLAN mit Network Info II.

Ein ebenfalls sehr interessantes Tool ist **Net Status**. Mit ihm können Sie IP-Adressen im Netzwerk pingen und den Status des Netzwerks (NetStat) sowie die aktuelle Konfiguration anzeigen. Sie können Arp-Konsolen-Befehle eingeben und einen ganzen IP-Bereich scannen lassen. Nach dem Scan zeigt das Tool an, welche IPs aktiv sind und wie die MAC-Adressen der verbundenen Geräte lauten.

4.4.7 Android-Gerät als Internet-Router einsetzen

Interessant ist das kostenlose Tool **Wireless Tether for Root Users**. Wenn Sie mit einem gerooteten Android-Handy arbeiten, können Sie mit diesem Tool Ihr Handy als Internet-Router für PC oder Notebook einsetzen.

Die enthaltenen Funktionen sind wesentlich umfangreicher als die Standardeinstellung in Android 2.2. Ab dieser Version haben Sie mit Bordmitteln die Möglich-

keit, die Internetanbindung des Handys mit dem Notebook zu nutzen. Wenn Sie über eine Flatrate verfügen, können Sie auf diese Weise bequem mit dem Android-Handy als Internet-Router arbeiten.

Einrichtung: Hier konfigurieren Sie die Netzwerkverbindungen des Android-Smartphones.

Diese Konfiguration nehmen Sie in den Einstellungen über T*ethering & mobiler Hotspot* vor. Die Einstellungen in der Zusatz-App sind aber umfangreicher. Sie müssen den PC, mit dem Sie die Internetverbindung des Android nutzen wollen, entweder per WLAN oder über Bluetooth verbinden. Um im Android-Gerät Bluetooth zu aktivieren, ziehen Sie die obere Menüleiste mit dem Finger nach unten. Anschließend öffnet sich ein neues Fenster, über das Sie die einzelnen Verbindungen konfigurieren können, darunter Bluetooth.

Leider laufen nicht alle Apps auf allen Android-Handys. Wollen Sie ein Android-Handy als Internet-Router einsetzen, stehen noch folgende kostenlose Apps im Market zur Verfügung:

- **Barnacle Wifi Tether**
- **PdaNet**
- **EasytetherLite**

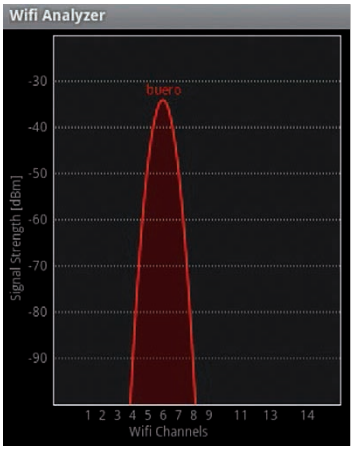
4.4.8 WLANs verwalten

Wenn Sie Ihr Android-Gerät häufiger mit unterschiedlichen WLANs verbinden, können zusätzliche Apps die Arbeit enorm erleichtern.

Mit der kostenlosen App **Wifi Manager** können Sie alle WLANs, mit denen Sie sich verbinden, anzeigen und die Verbindung verwalten. Außerdem können Sie sich die Signalstärke aller WLANs in Reichweite anzeigen lassen und so leichter auswählen, mit welchem Sie sich verbinden wollen.

Hilfreich: Der Wifi Manager unterstützt bei der Verwaltung von WLANs.

Die App **WiFi OnOff** erlaubt es, mit einem einzelnen Klick die WLAN-Verbindung des Androids zu trennen.



Da geht was: Mit dem Wifi Analyzer sehen Sie die Signalstärke des Access Points.

Wollen Sie WLANs analysieren und Signalstärken genauer anzeigen, bietet die App **Wifi Analyzer** wertvolle Hilfe. Vor allem, wenn Sie mehrere Access Points einrichten, können Sie auf diese Weise mit einem Android-Handy die Signalstärke für die Positionierung messen. Das Tool zeigt mit einer Grafik die aktuelle Signalstärke an. Um die Anzeige zu ändern, fahren Sie mit dem Finger über das Display.

Thomas Joos

4.5 Android-Praxis: Bereitstellung im Unternehmen

Wollen Sie im Unternehmen mehreren Benutzern ein identisches Android zur Verfügung stellen, sollten Sie vor der Bereitstellung prüfen, welche Apps Sie auf den Handys installieren und ob Sie mit speziellen Richtlinien arbeiten möchten.

Leider bieten Android-Geräte noch nicht die gleichen Möglichkeiten wie beispielsweise iPhones und das iPhone-Konfigurationsprogramm. Mit Drittherstellerprodukten und sogar Freeware lassen sich aber viele notwendigen Einstellungen und Vorgänge bei der Bereitstellung von Android-Handys automatisieren. Manche Hersteller bieten auch eigene Programme, diese sind allerdings an die jeweiligen Geräte des Herstellers gebunden. Aus diesem Grund ist die Bereitstellung von Android-Handys in Enterprise-Umgebungen oft kein einfaches Unterfangen, zumindest dann nicht, wenn Sicherheit und Automatisierung eine wichtige Rolle beim Projekt einnehmen.

4.5.1 Google Apps Device Policy

Google bietet mit dem kostenlosen Tool **Google Apps Device Policy** die Möglichkeit, Android-Handys mit Sicherheitsrichtlinien zu versorgen und Geräteadministratoren festzulegen. Auf diese Weise lassen sich Smartphones deutlich effizienter absichern als mit Android-Bordmitteln.

Hilfreich: Mit Google Apps Device Policy können Sie Android-Geräte absichern.

Die Anwendung funktioniert aber erst ab Android 2.2, ältere Versionen lassen sich nicht mit Richtlinien absichern. Das gilt auch für Exchange ActiveSync-Postfachrichtlinien. Auch diese werden erst ab Android 2.2 unterstützt, allerdings funktioniert die Umsetzung nicht zuverlässig, und die Richtlinien lassen sich leicht aushe-

beln. Google Apps Device Policy läuft dazu auf dem Endgerät als Systemdienst und tauscht sich mit einem Google-Server aus, über den Administratoren Einstellungen vornehmen. Über den Server lassen sich Geräte bei Verlust auch löschen (Remote Wipe). Im Unternehmenseinsatz ist dies ein elementares Feature.

Generell erweitert Google Apps Device Policy die Sicherheit für Android-Handys für den Unternehmenseinsatz, was den Einsatz durchaus lohnenswert macht. Allerdings ist die Funktionalität stark eingeschränkt, das Tool benötigt ein Google-Konto für den Betrieb und lässt sich nur über die Google-Apps-Seite steuern. Außerdem funktioniert die Lösung leider nicht auf jedem Android-Endgerät, sodass umfassende Tests notwendig sind.

Sie müssen die App mit den Endgeräten im Market herunterladen und installieren. Erst dann können Sie auf dem Handy Richtlinien einsetzen. Nach der Installation lassen sich verschiedene Sicherheitseinstellungen festlegen:

- Erzwingen von Kennwörtern bei der Anmeldung
- Komplexe Kennwörter erzwingen
- Bildschirmsperre nach bestimmten Zeiten
- Löschen von Geräten über das Internet

4.5.2 Google-Tool einsetzen

Nachdem Sie die App installiert haben, starten Sie diese und führen den Einrichtungsassistenten fort. Sie müssen für die Verwendung der App auf dem Gerät ein Google-Konto einrichten. Leider lässt sich die Einrichtung nicht automatisieren oder über eine Softwareverteilung bereitstellen. Google-Konten stehen zwar kostenlos zur Verfügung, allerdings sind sie nicht gerade für den Firmeneinsatz optimiert, geschweige denn für den Einsatz in sehr großen Unternehmen.

Sie können ein solches Konto direkt in der App erstellen. Nach der Anmeldung setzen Sie anschließend die Richtlinien. Ausführliche Anleitungen dazu stellt Google zur Verfügung:

- **Übersicht: Using Google Apps Device Policy**
  (www.google.com/support/mobile/bin/answer.py?answer=190930)
- **Sicherheitseinstellungen für Mobilgeräte**
  (www.google.com/support/a/bin/answer.py?answer=173393)

Auf den Hilfeseiten finden Sie auch Anleitungen, wie Sie in der Weboberfläche von Google Apps Device Policy die einzelnen Richtlinien setzen. Auch wenn die Lösung nicht gerade optimal ist, sollten Sie diese einsetzen, wenn Sie keine Managementlösung eines Drittherstellers verwenden wollen. Ohne diese Suite sind Android-Handys nicht sehr umfassend abzusichern. Für manche Unternehmen ist es sinnvoll, dass Anwender über den Windows-Explorer auf die SD-Karte im Android-Telefon zugreifen können. Damit das funktioniert, müssen Sie in den Android-Handys aber über *Einstellungen\Anwendungen\Entwicklung* den USB-Debugging-

Modus aktivieren. Der Zugriff funktioniert in diesem Fall auch problemlos über 64-Bit-Betriebssysteme wie Windows 7 x64 oder Windows Vista x64. Generell müssen Sie die USB-Anbindung erst aktivieren. Ziehen Sie dazu die obere Menüleiste nach unten, um USB zu aktivieren. Leider lassen sich diese Einstellungen nicht automatisieren.

4.5.3 Enterprise-Management-Software für Android

Speziell für Android gibt es keine Konfigurationslösungen von Google oder ein Verwaltungsprogramm ähnlich wie das iPhone-Konfigurationsprogramm von Apple. Das bedeutet: Sie können keine Automatisierung durchführen oder Einstellungen über Richtlinien festlegen, geschweige denn Programme sperren oder die Installation von Apps verhindern. Es bieten aber immer mehr Hersteller plattformunabhängige Verwaltungs-Suites für Smartphones an. Vor allem Unternehmen, die den Anwendern zahlreiche Smartphones zur Verfügung stellen, sollten diese zentral verwalten. Das erhöht die Sicherheit und bietet die Möglichkeit, interne Anwendungen über ein zentrales Portal zur Verfügung zu stellen. Solche Lösungen kosten Geld und natürlich auch Verwaltungsaufwand. Ein Beispiel für eine solche Lösung ist **Sybase Afaria** (www.sybase.de/products/mobileenterprise/afaria): Mit der Suite verwalten und sichern Sie die Anwendungen und Geräte. Außerdem kann die Suite komplexe Managementaufgaben für Smartphones übernehmen. Das Tool unterstützt iOS4 und Android-Geräte. Mit der Anwendung können Administratoren zwar nicht vollständig automatisiert Apps auf Android-Geräten installieren. Dazu stellt die Suite aber ein internes Portal zur Verfügung, das ähnlich funktioniert wie der Market. Über dieses Portal laden sich Anwender die einzelnen Anwendungen herunter. Für die Verwaltung der Smartphones steht eine Verwaltungsoberfläche zur Verfügung, die die parallele Verwaltung mehrerer Smartphone-Typen und -Hersteller unterstützt. Natürlich lassen sich auch Sicherheitsrichtlinien auf den Endgeräten umsetzen und Geräte über das Internet löschen.

4.5.4 Managementlösungen

Zenprise MobileManager (www.zenprise.com/products/zenprise_mobilemanager/) ist in der Lage, Richtlinien und Sicherheitseinstellungen zentral vorzugeben. Mit der Suite lassen sich Snapshots der Geräte erstellen und neue angebundene Endgeräte entdecken sowie anbinden. Die Software kann den Standort der Geräte bestimmen und bei nicht aktiven Geräten automatische Sperren oder Löschvorgänge durchführen. Eine Lizenzverwaltung sowie Prozessautomatisierung sind integriert. Der Vorteil dabei ist, dass Unternehmen mit einer Software mehrere verschiedene Smartphone-Typen verwalten können. Eine Weboberfläche sowie eine Remote-Verwaltung zur Problemlösung sind integriert. Viele Einstellungen und Sicherheitsvorgaben lassen sich automatisieren. Neben dieser Lösung bietet auch Symantec mit **Symantec Mobile Management** (www.symantec.com/de/de/busi

ness/mobile-management) eine zentrale Lösung für Smartphones an. Über diese Suite lassen sich Anwendungen für die Geräte zentral bereitstellen, Richtlinien vorgeben, Inventuren durchführen, Lizenzen verwalten und vieles mehr.

Eines der bekanntesten Drittherstellerprodukte für die Verwaltung von Smartphones ist **Good for Enterprise** von Good (www.good.com) Technology. Das Programm bietet eine webbasierte Oberfläche, mit der Anwender alle Arten von Smartphones zentral verwalten und fernsteuern können. Die Anwendung dient nicht nur der Verwaltung der Smartphones, sondern kann ebenso die Synchronisierung des Postfachs über Exchange oder Lotus Notes synchronisieren. Zusätzlich benötigen Sie bei dieser Anwendung aber einen eigenen Server, die App allein reicht nicht aus.

4.5.5 Open-Source-Lösungen

Kleinere Unternehmen, die keine teure Lösung suchen, finden im Open-Source-Bereich einige Anwendungen, die aber extrem eingeschränkt sind und nur Android-Handys unterstützen. Solche Tools können etwa einzelne Anwender nutzen.

Android Commander (www.androidcommander.com) – Das Tool kann von einem PC aus die Daten und Anwendungen von Android-Handys verwalten. Sie können Dateien zwischen Handy und Smartphone kopieren, Anwendungen installieren und Screenshots erstellen. Allerdings unterstützt die Anwendung nicht alle Smartphones. Für den Zugriff ist das Android SDK auf dem Computer erforderlich. Sie müssen dazu das SDK aber nicht installieren, Download und Entpacken reichen vollkommen aus.

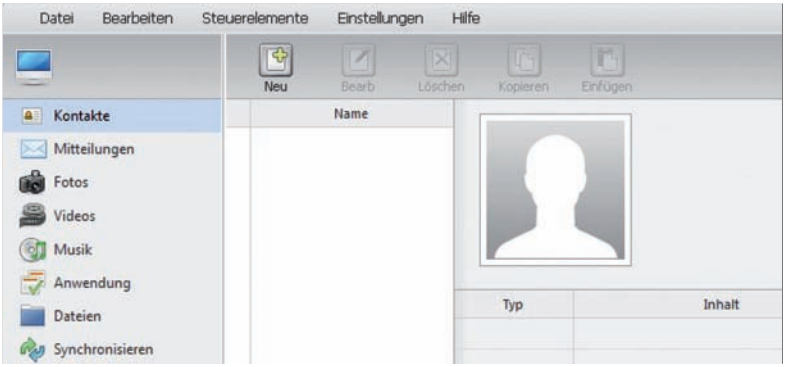
PC Suite for Android (www.pandaapp.com) – Auch diese Lösung steht kostenlos zur Verfügung. Die Anwendung ist allerdings nicht sehr stabil. Sie können mit der Anwendung ebenfalls Daten zwischen Android und PC bewegen. Hat Ihr Telefon Probleme mit der Anwendung, finden Sie im Blog-Eintrag auf AndroidPIT zahlreiche Informationen zur Suite (www.androidpit.de/de/android/blog/).

4.5.6 Daten synchronisieren

Unabhängig von der Bereitstellung der Handys sollten Administratoren den Anwendern die Möglichkeit geben, Daten auf das Smartphone zu übertragen, zum Beispiel, um Kontakte zu synchronisieren. Standardmäßig fehlt bei den meisten Herstellern ein Desktop-Programm, mit dem Anwender selbstständig Daten austauschen oder synchronisieren können.

Hier gibt es eine kostenlose Alternative mit der Bezeichnung Android Sync Manager WiFi. Mit dem Tool lassen sich Android Smartphones über WiFi synchronisieren. Auf diese Weise kann man ein Android-Handy zum Beispiel auch mit Outlook verbinden. Auch der Abgleich von Dokumenten und anderen Dateien ist möglich. Die Software besteht aus zwei Teilen. Zunächst müssen Sie auf dem An-

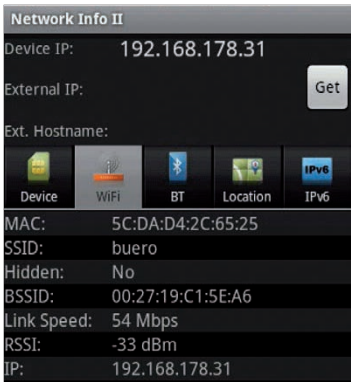
droid-Handy über den Market die App **Android Sync Manager WiFi** installieren. Auf der Seite des Herstellers (http://global.mobileaction.com/product/product_AM.jsp) laden Sie sich die PC-Komponente herunter und installieren diese auf dem PC, auf dem Sie die Synchronisierung einrichten wollen.



Praktisch: So richtet man den Android Sync Manager WiFi ein.

Download und Betrieb der Software sind kostenlos. Damit sich der PC-Client und die App auf dem Android austauschen können, erhalten Sie beim Start der App auf dem Handy eine Zahl. Diese tragen Sie in der Software auf dem PC als Kennwort für die Verbindung ein, inklusive der IP-Adresse des Android-Handys. Um sich die IP-Adresse anzuzeigen, können Sie zum Beispiel ebenfalls bequem eine App herunterladen und installieren. Hilfreich dazu ist das Tool **Network Info II**. Es zeigt Ihnen detaillierte Informationen zum aktuellen Netzwerkstatus des Handys an. Wenn Sie das Tool starten, sehen Sie die aktuelle IP-Adresse des Handys und können Daten über das derzeitig verbundene Telefonnetz oder WLAN anzeigen.

Network Info II: Das Tool zeigt Ihnen unter anderem die IP-Adresse Ihres Android-Gerätes an.



Sie können sich die IP-Adresse und Daten zum WLAN mit Bordmitteln anzeigen lassen. Klicken Sie dazu auf *Einstellungen\Wireless\Wi-Fi-Einstellungen* und dann auf das WLAN, mit dem Sie verbunden sind. Android zeigt jetzt die IP-Adresse, die Verbindungsgeschwindigkeit und die Signalstärke des Netzwerks an. Nach dem Start des PC-Clients richten Sie eine neue Verbindung ein und geben die IP-Adresse des Telefons sowie die Zahlenkolonne ein.

Ist die Verbindung eingerichtet, können Sie die Daten zwischen Handy und PC synchronisieren. Die Anwendung funktioniert weit besser als viele Tools, die Hersteller mit dem jeweiligen Handy mitliefern, und bietet zusätzlich noch die Möglichkeit, auf den Market zuzugreifen. Leider funktioniert das Tool nicht zuverlässig auf 64-Bit-Betriebssystemen, ist aber für Anwender leicht zu bedienen.

4.5.7 Fazit

Für Administratoren existieren durchaus leichter zu verwaltende Smartphone-Plattformen als Android. Zum einen verhalten sich die verschiedenen Geräte der einzelnen Hersteller vollständig unterschiedlich, zum anderen ist die Standardsicherheit in Android nicht sehr hoch. Exchange-ActiveSync-Postfachrichtlinien kann man aushebeln, Sicherheitsrichtlinien ausschalten, und das Gerät lässt sich durch Rooten komplett offenlegen.

Außerdem unterstützen Android-Handys standardmäßig keine Verschlüsselung und auch keine Verwaltung komplexer Kennwörter. Leider bietet Google kein Äquivalent zum iPhone-Konfigurationsprogramm an, mit dem sich Telefone vereinheitlichen lassen. Unternehmen, die Android zentral bereitstellen wollen, müssen daher in vielen Fällen auf die Software von Drittherstellern setzen. Diese muss natürlich auch gesondert lizenziert, gepflegt und verwaltet werden. Außerdem ist die Bedienung nicht immer einfach, sodass in einigen Fällen sicherlich Schulungsbedarf vorliegen wird. Viele Tools erfordern zudem einen eigenen Server.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

TecChannel-Links zum Thema	Webcode	Compact
Android-Praxis: Bereitstellung im Unternehmen	2035262	S.213
Android-Praxis: VPN einrichten und nutzen	2033962	S.192
Android-Praxis: Kalender richtig synchronisieren	2034375	S.198
Android-Praxis: Apps und Tipps für Admins	2034620	S.205

4.6 Android-Praxis: Anbindung an Exchange

Neben den iPhones kommen auch Android-Handys in Unternehmen immer mehr zum Einsatz. Der größte Vorteil der Android-Handys ist neben dem Preis die offene Struktur für Anwendungen. Im Gegensatz zu Apples iPhone geben die Android-Hersteller nicht vor, welche Apps zur Verfügung stehen dürfen, sondern die Entwickler haben relativ freie Hand.

Die Anbindung an Exchange-Server über die ActiveSync-Technologie ist mit Android-Handys genauso möglich wie beim iPhone. Entsprechende Anwendungen sind bereits vorinstalliert oder lassen sich einfach nachrüsten. Anwender können den integrierten Browser für Outlook Web App oder andere Webdienste im Unternehmen nutzen. Es bietet sich aber meistens an, hier auf spezielle Apps zu setzen.

Die auf Android-Smartphones vorinstallierten Anwendungen wie Facebook sind im Firmeneinsatz allerdings eher ein Nachteil. Flugs ist bei Fehlkonfiguration das interne Exchange-Adressbuch via Facebook zur Verfügung gestellt, und aus Kunden werden „Freunde". Ältere Android-Versionen beherrschen keine Sicherheitsrichtlinien oder sichere Anmeldungen und auch keine Synchronisierung mit Exchange-Kalendern. Außerdem benötigen Sie für den effizienten Betrieb von Android-Handys ein Google-Konto, was bei der Bereitstellung vieler Smartphones im Unternehmen Probleme bereiten kann. Das System Android kann hier zudem Administratoren Kopfzerbrechen bereiten, denn die Vorgaben der unterschiedlichen Smartphone-Hersteller unterscheiden sich voneinander.

Viele verwenden keine Standard-Android-Installation, sondern passen diese an. Dies gilt es zu beachten, wenn Sie unterschiedliche Android-Smartphones im Unternehmen einsetzen. Achten Sie beim Erwerb des Handys darauf, welche Funktionen vorinstalliert sind. Generell lassen sich mit Android alle Exchange-Versionen ab 2003 synchronisieren. Ab Android 2.2 unterstützen die Handys auch Exchange ActiveSync-Postfachrichtlinien, allerdings lassen sich diese aushebeln.

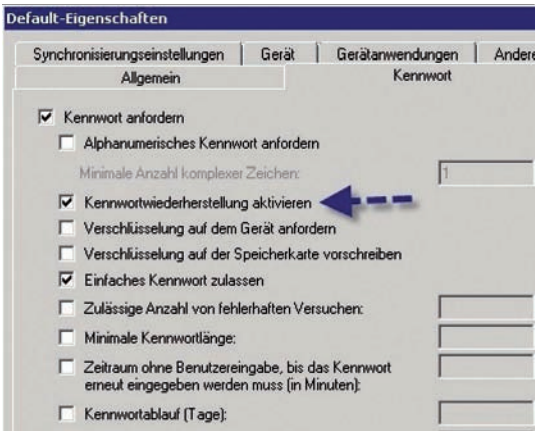
4.6.1 Android 2.2 und Exchange ActiveSync

Mit den meisten Android-Handys können Sie den Posteingang problemlos über Exchange ActiveSync synchronisieren. Das funktioniert auch in der Standardversion, ohne Anpassungen des Herstellers. Unternehmen, die intern Exchange einsetzen, tun gut daran, nur solche Smartphones zu verwenden, die Exchange ActiveSync unterstützen. Zum einen ist die Synchronisierung wesentlich schneller, stabiler und vor allem zuverlässiger, zum anderen gehen keine E-Mails verloren und Anwender können auch mit mehreren Geräten synchronisieren.

Mit Exchange ActiveSync (EAS) können Anwender ihr Postfach mit E-Mails, Kontakten und Kalendereinträgen über das Telefonnetz synchronisieren, E-Mails

empfangen und E-Mails senden. Wer Android-Handys mit Exchange professionell synchronisieren will, sollte mindestens auf Version 2.2 (Codename Froyo) setzen.

Achten Sie beim Kauf darauf, ob Ihr Gerät kompatibel zu 2.2 ist oder noch die alte Version 2.1 nutzt. Ab Version 2.2 sind Sicherheitsrichtlinien optimal unterstützt, und die Kennwörter lassen sich wesentlich effizienter gestalten. Mit der Version 2.2 können Administratoren Voraussetzungen für Kennwörter über Exchange-ActiveSync-Postfachrichtlinien vorgeben.



Praktisch: Android-Smartphones unterstützen auch Exchange-ActiveSync-Postfachrichtlinien.

4.6.2 Remote Wipe und Synchronisation

Ab Version 2.2 können Anwender und Administratoren außerdem verloren gegangene Geräte remote löschen (Remote Wipe). Außerdem erlauben Android-Handys erst ab Version 2.2. die Synchronisierung von Exchange-Kalendern.

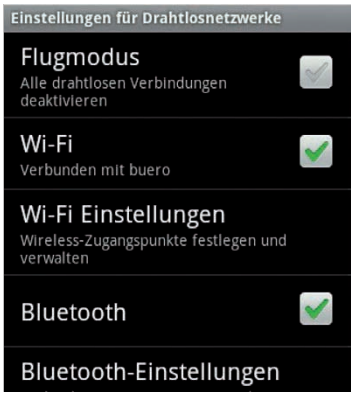
Ebenfalls erst ab Android 2.2 ist die Verwendung der Auto-Discovery-Funktion möglich. Hier müssen Anwender nur E-Mail-Adresse und Kennwort eingeben, den Rest der Einrichtung erledigt Android über Exchange automatisch, entsprechend konfigurierte Server vorausgesetzt. Diese Funktion entlastet die IT-Abteilung deutlich. Eine weitere Neuerung seit Android 2.2 ist die Unterstützung der globalen Adressliste in Exchange, sodass Anwender mit Android-Handys das Firmenverzeichnis durchsuchen können, wenn sie eine E-Mail schreiben wollen.

Neben der Synchronisierung über das Telefonnetz können Sie dies mit Android-Handy auch über WLANs durchführen. Sobald das Handy eine Verbindung zu einem Funknetzwerk hat, läuft die Synchronisierung über die kostenlose und schnellere Funkverbindung. Anwender müssen dazu keine Einstellungen vornehmen, vielmehr verbindet das Gerät automatisch mit dem verfügbaren WLAN und verwendet dieses für die Internetanbindung.

4.6.3 Netzwerkanbindung mit Android

Wenn Sie ein Android-Handy mit Exchange synchronisieren wollen, ist es der effizienteste Weg, das Gerät an diejenigen WLANs anzubinden, die Sie am häufigsten verwenden. Die Einstellung finden Sie über die Anzeige der Anwendungen und *Einstellungen\Wireless*. Sobald Sie ein WLAN konfiguriert haben, verbindet sich das Handy künftig automatisch mit diesem Netzwerk. Das funktioniert auch, wenn Sie mehrere WLANs einbinden. Eine erfolgreiche Anbindung erkennen Sie am WLAN-Symbol im oberen Bereich.

WLAN einrichten: Über die Wi-Fi-Einstellungen konfigurieren Sie die WLANs.



Über *Wi-Fi* können Sie die Anbindung an das aktuelle Netzwerk trennen, mit *Wi-Fi-Einstellungen* konfigurieren Sie die Anbindung an WLANs. Hier legen Sie fest, mit welchen Netzwerken sich das Handy verbinden soll, und können Kennwörter für die entsprechenden WLANs hinterlegen.

Anbindung: Das Smartphone verbindet sich automatisch mit dem eingerichteten WLAN.

Ab Android 2.2 haben Sie die Möglichkeit, die Internetanbindung des Handys mit dem Notebook zu nutzen. Einen entsprechenden Mobilfunkvertrag vorausgesetzt, können Sie das Smartphone im Bedarfsfall als Internet-Router einsetzen. Bei den iPhones funktioniert dies ab iOS 4.3, siehe auch Praxis: das iPhone 4 als WLAN-Hotspot nutzen (Webcode **2034536**).

4.6.4 Android mit Exchange synchronisieren

Um ein Handy mit Android 2.2 für die Exchange-Anbindung zu konfigurieren, müssen Sie keinerlei Drittprodukte installieren. Allerdings haben die Standardkalender so mancher Android-Handys Probleme mit der Anzeige von Exchange-Terminen. Aus diesem Grund ersetzen viele Hersteller die Standardanwendungen oder passen diese an. Hier bietet es sich an, dass Sie im Market verschiedene Kalender testen, wenn Ihr Gerät Probleme hat. Unternehmen, die neue Smartphones kaufen, sollten auf jeden Fall erst die verschiedenen Hersteller testen, bevor sie sich für ein Gerät entscheiden. Konfiguration und Anbindung von Exchange sind von Gerät zu Gerät unterschiedlich stabil; das gilt vor allem für den Kalender.

Achten Sie darauf, eine aktuelle Version zu laden, wenn Sie eine Zusatz-App für den Kalender nutzen. Lange nicht mehr aktualisierte Kalender-Apps können Exchange-Kalender nicht oder nur instabil anzeigen, da hier Funktionen von Android 2.2 notwendig sind. Die generelle Anbindung des Exchange-Postfachs funktioniert auf allen Android-Smartphones mit der Standard-App identisch.

4.6.5 Schritt-für-Schritt-Anleitung

Auf dem Smartphone sind folgende Schritte notwendig, um eine Anbindung an Exchange durchzuführen:

1. Klicken Sie auf den Anwendungen-Knopf im Homescreen.
2. Klicken Sie auf *E-Mail*. Alternativ klicken Sie auf *Einstellungen\ Konten & Synchronisierung*. An dieser Stelle können Sie ebenfalls neue E-Mail-Konten hinzufügen.
3. Wählen Sie *Microsoft Exchange ActiveSync*.
4. Geben Sie Ihre E-Mail-Adresse und das Kennwort für das Konto ein.
5. Klicken Sie auf *Weiter*.
6. Auf der nächsten Seite geben Sie den Benutzernamen ein. Diesen müssen Sie in der Syntax *<Domäne>\<Benutzername>* eintragen. Hier tippen Sie den Namen der Windows-Domäne ein, an der Sie sich authentifizieren wollen. Bei der Anbindung an ein 1&1-Exchange-Postfach ist das zum Beispiel die Domäne exchange. Bei Benutzernamen geben Sie den Namen ein, mit dem Sie sich an der Domäne anmelden. Bei der Anbindung eines 1&1-Postfaches verwenden Sie hier den gleichen Namen, den Sie auch in

Outlook nutzen. Hierbei handelt es sich nicht um die E-Mail-Adresse, sondern um den Benutzernamen, den Sie auch bei der Anmeldung an einem Computer verwenden.

Servereinstellungen: Es ist der Benutzername und der Servers für die Anbindung anzugeben.

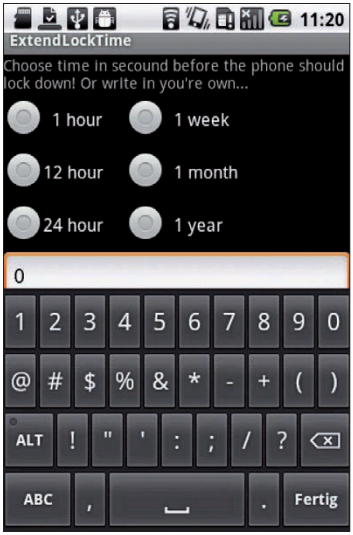
7. Im Feld *Server* tragen Sie den Namen des Servers ein, mit dem Ihr Exchange-Server an das Internet angebunden ist. In den meisten Fällen handelt es sich hier um den gleichen Namen, den Sie auch in OWA verwenden. Beim Einsatz von 1&1 ist das zum Beispiel profimailer.de.
8. Klicken Sie anschließend auf *Fertig*.
9. Aktivieren Sie noch die beiden Optionen *Sichere Verbindung (SSL) verwenden* und *Alle SSL-Zertifikate akzeptieren* und klicken Sie auf *Weiter*.
10. Anschließend versucht das Gerät, eine Verbindung herzustellen, und blendet Hinweise ein, dass bestimmte Sicherheitseinstellungen auf dem Geräte geändert werden müssen. Nach der Einrichtung können Sie dann die Änderungen vornehmen.
11. Danach können Sie dem Konto noch einen Namen geben. Haben Sie auf dem Server Richtlinien gesetzt, müssen Sie auf dem Gerät in den meisten Fällen noch Einstellungen vornehmen, zum Beispiel eine PIN festlegen, mit der Sie das Gerät entsperren können. Anschließend stehen die E-Mails über das Anwendungsfenster im Bereich *E-Mails* zur Verfügung.

4.6.6 Webzugriff auf Exchange und Einstellungen ändern

Per Browser ist auf dem Android-Gerät auch ein Zugriff auf Outlook Web App möglich. Allerdings können Sie dann nur die eingeschränkte Version von OWA nutzen. Das Lesen von E-Mails in OWA ist nicht so bequem wie über die E-Mail-

Funktion des Androids, ist aber möglich. Der direkte Zugriff per Exchange ActiveSync ist hier effizienter. Allerdings können Sie über die Optionen in OWA zum Beispiel Einstellungen für Ihr Exchange-Postfach ändern, etwa den globalen Abwesenheitsassistenten für Ihr Postfach oder die automatische Signatur. Diese Einstellungen können Sie nicht direkt im Android anpassen, außer Sie installieren zusätzliche Apps. Haben Sie die erste Einrichtung abgeschlossen, können Sie die Einstellungen verfeinern. Rufen Sie dazu die Anwendungen auf dem Handy auf und klicken Sie auf *Einstellungen\Konten & Synchronisierung*. Hier sehen Sie alle Konten, die Sie eingerichtet haben, auch Ihr Exchange-Konto.

Wenn Sie die Standard-App verwenden, lassen sich mehrere Exchange-Konten einrichten. Sie können über das Konto einstellen, ob das Handy auch die Kontakte und den Kalender synchronisieren soll. Beide Bereiche sind nach der Anbindung von Android an Exchange automatisch aktiv. Allerdings unterstützen Android-Handys keine verschiedenen Ordner für Kontakte. Sie können nur die generelle Synchronisierung aktivieren oder deaktivieren, anders als beim iPhone.

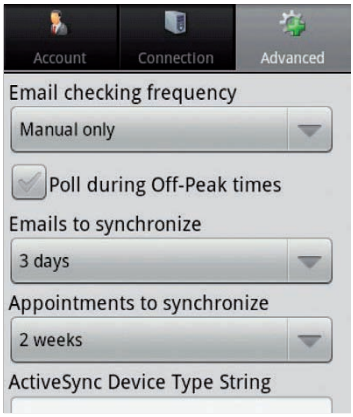


Individuell: Per App können Sie die Sperrzeit auf dem Smartphone konfigurieren.

Leider unterstützen weder iPhone noch Android eine Synchronisierung von Exchange-Aufgaben oder Notizen. Hier müssen Sie auf Zusatzanwendungen setzen. Wenn die Administratoren vorgeben, dass sich ein Handy nach einer bestimmten Zeit automatisch sperren soll und bei Reaktivierung eine PIN erfordert, sperren sich Android-Handys mit Version 2.2. spätestens nach 15 Minuten. Anwender können diese Einstellungen mit der App **ExtendLockTime** selbst ändern. Die kostenlose Anwendung lässt sich leicht über den Market auf dem Handy installieren.

4.6.7 Zusatzanwendungen für Exchange-Anbindung

Wer Android-Handys mit Exchange verbinden will, findet im Market zahlreiche – zum Teil kostenlose – Apps, die viele Probleme der Standardanwendung in Android 2.2 beheben. **Nitrodesk TouchDown** gibt es auch als 30-Tage-Testversion im Market. Allerdings läuft die App nicht auf allen Android-Handys. Mit ihr lassen sich weitere Einstellungen vorgeben und auch Aufgaben synchronisieren. Eine weitere interessante Anwendung ist **Enhanced Email**. Damit lassen sich weitergehende Einstellungen ändern sowie Ports und Zertifikate besser verwalten. **Corporate Addressbook** hingegen ermöglicht einen besseren Zugriff auf die globale Adressliste (GAL) von Exchange, und **Out of Office Assistant** kann den Abwesenheitsassistenten über das Android steuern.



Erweiterungen: Mit Apps können Sie die Exchange-Funktionalität von Android deutlich ausbauen.

Viele Hersteller, zum Beispiel HTC, bauen eigene Anwendungen für die Exchange-Anbindung ein, die wesentlich besser funktionieren als die Standard-App. Wollen Sie zum Beispiel Besprechungsanfragen beantworten, kann das die Standard-App nicht optimal, HTC-Androids arbeiten hier etwas besser, wenngleich nicht optimal. Die Standardanwendung unterstützt problemlos das Anbinden mehrerer Exchange-Konten. Hat ein Hersteller diese Anwendung aber ersetzt, lässt sich häufig nur noch ein Exchange-Konto anbinden, was zum Beispiel bei HTC der Fall ist.

4.6.8 Fazit

Was früher nur mit Windows Mobile-Geräten möglich war, haben mittlerweile viele Handy-Anbieter lizenziert: Exchange ActiveSync. Unternehmen, die selbst Exchange betreiben, oder Anwender, die ein Hosted-Exchange-Postfach verwenden, tun gut daran, ihr Postfach über diese Technologie zu synchronisieren.

Auf diese Weise lassen sich schnell und unkompliziert E-Mails lesen und schreiben, die später auch in Outlook verfügbar sind. Die Synchronisation von Kalendern und Kontakten ist ebenfalls möglich. Da Android ein sehr offenes Systems ist, unterscheiden sich Einrichtung und Geschwindigkeit zwischen den verschiedenen Herstellern. Im direkten Vergleich zwischen iPhone-4- und Android-2.2-Geräten haben es Administratoren mit dem Apple-Gerät leichter. Mit dem iPhone-Konfigurationsprogramm (siehe auch iPhone-Praxis: Einstellungen per Konfigurationsprogramm automatisieren, Webcode **2033060**) lässt sich genauer und besser festlegen, welche Anwendungen auf den Endgeräten installiert sein dürfen, und auch die Exchange-Konfiguration ist sehr viel einfacher zu automatisieren.

Durch die Pflichteinrichtung eines Google-Kontos auf vielen Android-Smartphones ist die Bereitstellung im Unternehmen unnötig komplex. Dass spezielle Apps die Exchange-ActiveSync-Postfachrichtlinien einfach aushebeln, dürften sicherheitsbewusste Administratoren ebenfalls nicht gerne sehen.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

TecChannel-Links zum Thema	Webcode	Compact
Android-Praxis: Anbindung an Exchange	2034788	S.219
Android – Datensicherung in der Praxis	2034104	S.184
Android-Praxis: VPN einrichten und nutzen	2033962	S.192
Android-Praxis: Kalender richtig synchronisieren	2034375	S.198
Android-Praxis: Apps und Tipps für Admins	2034620	S.205
Android-Praxis: Bereitstellung im Unternehmen	2035262	S.213
Test: Samsung Galaxy Tab 10.1	2036790	S.227
Nützliche App-Grundausstattung für Android-Smartphones	2032538	–
Die beliebtesten Android-Apps	2028765	–
Empfehlenswerte Security-Apps für Android	2034879	–

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

4.7 Test: Samsung Galaxy Tab 10.1

Geht es um Tablets, so ist schnell von Apples iPad 2 die Rede. Seit Ende März 2011 gibt es die zweite Tablet-Generation der in Cupertino ansässigen Firma. Die Konkurrenz hinkt Apple seit dem ersten iPad in Sachen Bedienbarkeit, Design, Haptik und Wertigkeit hinterher. Die Defizite wollen viele Tablets mit üppiger Hardwareausstattung und diversen Anschlüssen, Kameras und Co. wettmachen.

Doch ein großer Erfolg bleibt Apples Konkurrenz bisher verwehrt. Ausbleibende Verkaufserfolge konnten den meisten Tablets schon nach dem ersten Anfassen und wenigen Minuten der Bedienung leicht prophezeit werden. Samsungs neues Galaxy Tab 10.1 hinterlässt dagegen auf Anhieb einen guten Eindruck. Das Tablet ist so flach wie das iPad 2, es ist angenehm leicht und liegt gut in der Hand. Zwar besitzt das Galaxy Tab 10.1 kein Gehäuse aus Aluminium, die Kunststoffumhausung wirkt aber hochwertig und gibt keine Knarzgeräusche von sich.

Mit einem 10,1 Zoll großen Display und Android 3.1 als Betriebssystem steht das Galaxy Tab 10.1 ab August 2011 in den Regalen der Händler. Die unverbindliche Preisempfehlung von 629 Euro wirkt selbstbewusst. Denn mit dem inkludierten SIM-Karten-Slot und 16 GByte Speicher kostet es 30 Euro mehr als ein entsprechendes iPad 2. Ob der Preis für das Samsung Galaxy Tab 10.1 im Vergleich zum iPad 2 gerechtfertigt ist, klärt unser Test.

4.7.1 Ausstattung & Akku-Laufzeit

Samsung verbaut im Galaxy Tab 10.1 einen Dual-Core-Prozessor NVIDIA Tegra 2 mit 1,0 GHz Taktfrequenz. Damit setzt das Tablet auf die für Honeycomb-Geräte übliche CPU-Ausstattung – wie der Konkurrent Motorola Xoom. Dem ARM-Prozessor stellt Samsung einen mit 1 GByte großzügig bemessenen Arbeitsspeicher zur Seite. Den internen Flash-Speicher dimensioniert der Hersteller auf 16 GByte, wie beim Einstiegsmodell von Apple. Varianten mit 32 oder 64 GByte Flash – wie es sie beim iPad 2 gibt – offeriert Samsung nicht.

Auf einen micro-SD-Kartenslot, den beispielsweise das Motorola Xoom besitzt, verzichtet das Galaxy Tab 10.1 ebenso wie ein iPad 2. Das Galaxy Tab 10.1 lässt sich auch nicht über einen Mini- oder Micro-USB-Anschluss mit dem PC verbinden, Samsung legt ein Datenkabel mit eigenem Connector bei. Selbst der Stecker sieht dem Apple-Pendant zum Verwechseln ähnlich. Ebenfalls wie beim iPad 2 gibt es für den Anschluss von LCD-TVs ein HDTV-Adapterkabel für zirka 40 Euro. Auch einen Steckplatz für SD-Karten suchen Sie beim Galaxy Tab 10.1 vergeblich, für rund 30 Euro gibt es das USB-Connection-Kit. Samsung eifert bei all dem Apple etwas zu sehr nach.

Drahtlose Verbindung nimmt das Galaxy Tab 10.1 über WLAN 802.11 a/b/g/n und Bluetooth 3.0 auf. Zudem gibt es einen SIM-Karten-Slot für HSPA+. Dabei nimmt das Tablet SIM-Karten normaler Größe auf.

An der Gehäusefront gibt es für Videotelefonate und Schnappschüsse eine integrierte 2,0-Megapixel-Kamera. Auf der Rückseite findet sich zudem eine 3,2-Megapixel-Kamera. Einen LED-Blitz hat Samsung neben der Rückkamera integriert. Die Bilder zeigen bei der gebotenen Auflösung eine gute Qualität. Die Foto-App bietet unter anderem Funktionen für Weißabgleich, Blende und Fokus.

Reduziert: Einen SD-Karten-Slot oder USB-Anschluss sucht man wie beim iPad 2 vergeblich. Samsung verwendet einen proprietären Connector.

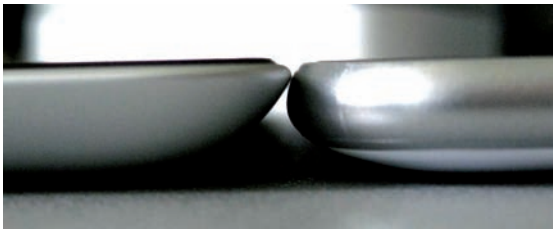
Samsung verbaut beim Galaxy Tab 10.1 einen Lithium-Polymer-Akku mit 7000 mAh. Beim Surfen im Internet via WLAN hält das Galaxy Tab 10.1 im Test fast acht Stunden durch, und beim Abspielen von Videos mit voller Displayhelligkeit macht das Xoom erst bei etwa mehr als sieben Stunden schlapp. Zwar kann das Galaxy Tab beim Videotest knapp mit den Konkurrenten Xoom und iPad 2 mithalten, doch beim Surfen macht es etwa vier Stunden eher schlapp.

4.7.2 Maße und Bildschirm

Während Apples iPad 2 einen 9,7-Zoll-Bildschirm im 4:3-Format besitzt, bringt das Samsung Galaxy Tab 10.1 ein 10,1-Zoll-Display im 16:10-Widescreen-Format mit. Die Auflösung des Bildschirms beträgt 1280 mal 800 Bildpunkte, das iPad/iPad2 löst 1024 mal 768 Pixel auf. Samsung setzt somit auf die Display-Merkmale, die auch ein Motorola Xoom verwendet. Durch seinen Widescreen wartet das Galaxy Tab 10.1 bei 175 x 257 x 8,6 mm auch mit anderen Abmessungen auf als das Apple iPad 2 (186 x 241 x 8,8 mm).

Formfrage: Während das iPad 2 (links) auf einen 4:3-Formfaktor beim 9,7-Zoll-Display setzt, nutzt das Galaxy Tab 10.1 (rechts) ein 16:10-Format für den 10,1-Zoll-Bildschirm.

Bei einer Gehäusedicke von nur 8,6 mm ist das Galaxy Tab 10.1 sogar minimal dünner als das bereits sehr schlanke iPad 2 mit 8,8 mm. Mit einem Gewicht von zirka 569 Gramm liegt das Galaxy Tab 10.1 zudem ein wenig leichter in der Hand als Apples iPad 2 in der 3G-Version mit 613 Gramm. Für ein Tablet ist die Qualität des Bildschirms essenziell. Und hier kann der kapazitive PLS-Touchscreen des Galaxy Tab überzeugen. Durch die hohe Auflösung von 1280 mal 800 Bildpunkten wirkt die Darstellung von Webseiten, Text, Bildern und anderen Inhalten scharf.



Flachmann: Bei einer Gehäusedicke von nur 8,6 mm ist das Galaxy Tab 10.1 (rechts) sogar minimal dünner als das bereits sehr schlanke iPad 2 (links) mit 8,8 mm.

Bei einer gemessenen maximalen Helligkeit von zirka 300 cd/m² ist in hellen Umgebungen sowie im Freien für eine gute Ablesbarkeit gesorgt. Der Spiegeleffekt bei Lichteinfall ist allerdings wie bei so vielen Displays leider sehr ausgeprägt. Eine rühmliche Ausnahme stellt Fujitsus Business-Pad Stylistic Q550 mit entspiegelter Oberfläche dar. Das Galaxy-Tab-Display bietet zudem befriedigende Einblickwinkel. In puncto Displayqualität ist insbesondere bei der Farbbrillanz und beim Einblickwinkel das iPad 2 allerdings noch eine Spur besser.

4.7.3 Haptik und Bedienelemente

Zwar besitzt das Samsung Galaxy Tab 10.1 kein Aluminiumgehäuse wie das iPad 2 oder das Motorola Xoom, doch die Kunststoffbehausung wirkt trotzdem edel und wertig. Das Tablet fasst sich angenehm an und liegt gut in den Händen. Das Galaxy Tab bietet eine gute Verwindungssteifigkeit, Knarzgeräusche sind dem Gehäuse nicht zu entlocken. Neben dem Einschaltknopf auf der oberen Gehäusekante findet sich beim Galaxy Tab 10.1 nur noch ein Kippschalter für die Lautstärke.

Samsungs Galaxy Tab 10.1 ist mit Android 3.1 ausgestattet. Das Betriebssystem ist für eine hohe Auflösung und Bedienung mit Tablet-Bildschirmen angepasst. Leider ist Letzteres nicht wirklich gelungen – was nicht an Samsung liegt, sondern an Google. Denn Hardwaretasten für Zurück, Home und Letzte Apps sind mit Android 3.1 nicht vorgesehen. Die Bedienelemente sind jetzt im Touch-Bereich links unten fest angeordnet. Beim Halten des Tablets in den Händen muss so der linke Daumen für die Navigation ganz nach links unten auf dem Display wandern. Dies funktioniert nur, wenn der Handrücken gleichzeitig nach außen wandert – das Ganze wirkt unkomfortabel.

Beim Halten des Tablets im Hochformat nervt die Bedienung noch mehr, weil hier die linke Hand noch stärker bewegt werden muss. Außerdem sind die drei „Soft-Tasten“ etwas klein und eng angeordnet, Nutzern mit groß geratenem Daumen wird das exakte Treffen der Bedienelemente erschwert.

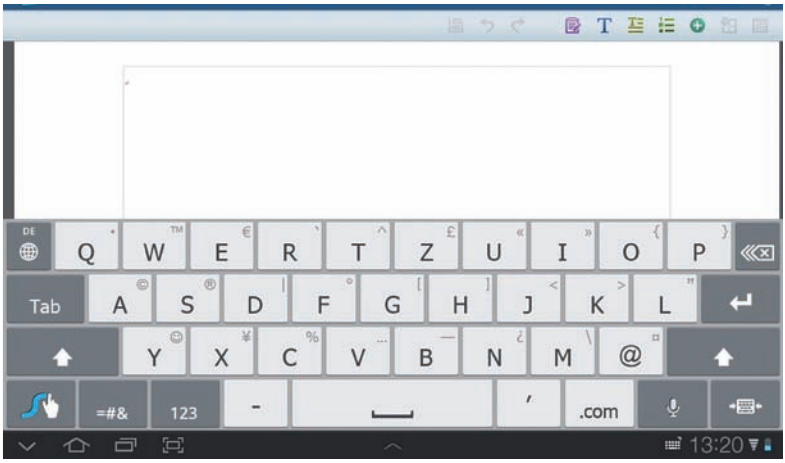
Gute Qualität: Das Gehäuse ist aus Kunststoff gefertigt. Dabei weist das Tablet eine hohe Stabilität auf, auch Knarzgeräusche gibt es nicht.

Einen Schnellzugriff auf die wichtigsten Funktionen gibt es beim Tipp auf die Kontrollleiste rechts unten, wo Uhrzeit, Akku-Zustand und Netzverbindung angezeigt werden. Dort lassen sich beispielsweise der Flugmodus einschalten, die Display-Ausrichtung sperren oder die Bildschirmhelligkeit regulieren. In der Kontrollleiste werden auch Statusmeldungen wie die erfolgreiche Installation neuer Apps eingeblendet.

Softie: Die Bedienelemente sind beim Android 3.1 im Touch-Bereich links unten fest angeordnet. „Echte“ Tasten gibt es nicht mehr.

4.7.4 Tastatur und Schreibgefühl

Als gelungen lässt sich die virtuelle Tastatur beim Galaxy Tab 10.1 mit Android 3.1 bezeichnen. Das Schreiben funktioniert flüssig, Buchstaben werden nur sehr selten „verschluckt". Im Querformat geht die Tastatur über die komplette Bildschirmbreite und nimmt fast die Hälfte der Displayhöhe ein. Nach Empfinden des Autors kann damit schnell und präzise geschrieben werden, wenn das Ganze mit zwei bis vier Fingern erfolgt.



Virtuelle Tastatur: Gut gefällt beim Galaxy Tab 10.1 die Tastatur, das Schreiben funktioniert flüssig, Buchstaben werden nur sehr selten „verschluckt".

Ein Zehnfingersystem funktioniert weniger gut, weil die Finger nicht auf der Tastatur ruhen können und das Layout darauf nicht optimiert ist. Es ist somit schwierig, alle Finger über den anvisierten Tasten im Schwebezustand ruhen zu lassen. Beim Halten des Galaxy Tab 10.1 mit den Händen fällt allerdings das Tippen nur mit den beiden Daumen bei den innen liegenden Tasten schwer – man erreicht sie kaum. Im Hochformat belegt die Tastatur ungefähr das untere Viertel des Bildschirms. Durch die reduzierte Tastengröße geht man jetzt primär zum Zweifingertippsystem über. Tippgeschwindigkeit und Treffsicherheit nehmen gegenüber dem Querformat allerdings merklich ab. Zum Texteschreiben ist das Querformat deutlich besser geeignet. Wird das Xoom im Hochformat gehalten, so lassen sich jetzt alle Tasten auch mit den Daumen gut erreichen. Swype zum Wischen von Wörtern wird vom Galaxy Tab unterstützt.

Zum Schreiben von Texten kann auf dem Galaxy Tab die vorinstallierte Office-Suite Polaris 3.0 verwendet werden. Polaris beinhaltet eine Textverarbeitung, Tabellenkalkulation sowie eine Präsentationssoftware.

4.7.5 Homescreen, Browser und Flash

Android 3.1 bietet insgesamt fünf Homescreens. Die Navigation zwischen den Schirmen erfolgt einfach per Fingerwisch, der Wechsel wird durch einen 3-D-Effekt grafisch untermalt. Sehr praktisch ist die mögliche Personalisierung der Startbildschirme. Neben dem üblichen Platzieren von Apps oder Lesezeichen für Webseiten lassen sich auch Inhalte via Widgets dort anzeigen. Hierzu zählen E-Mail-Eingänge, Wetter, Social-Media-Neuigkeiten oder aktuelle Kalendereinträge. Neu bei Android 3.1 ist die konfigurierbare Größe vieler Widgets.

Beim Galaxy Tab 10.1 lassen sich beim mittigen Tipp auf die untere Statusleiste einige Apps öffnen. So gibt es einen schnellen Zugriff auf den Task-Manager, Kalender, Weltuhr, Memo, Rechner und MP3-Player. Leider lässt sich die Auswahl der Apps nicht konfigurieren.

Nettes Feature: Sehr praktisch ist die mögliche Personalisierung der Startbildschirme. Neben dem üblichen Platzieren von Apps oder Lesezeichen für Webseiten lassen sich auch Inhalte dort anzeigen. Hierzu zählen E-Mail-Eingänge, Facebook-Neuigkeiten oder aktuelle Kalendereinträge.

Beim Zoomen mit den Fingern in Bilder erfolgt die Vergrößerung mit Android 3.1 jetzt endlich auch da, wo man es macht – im Gegensatz zu den älteren Android-Versionen. Allerdings schärft das Galaxy Tab 10.1 nach dem Zoomen mit einer knapp einsekündigen Verzögerung die Bilder erst nach – das langweilt. Beim Scrollen durch Webseiten zeigt sich das Tablet sehr flink, ein Ruckeln ist nur noch schwach vorhanden. Auch das Zoomen von Webseiten mit den Fingern funktioniert schon sehr gut und nur mit leichten Verzögerungen. Alles erfolgt beim iPad 2 allerdings wieder etwas flüssiger und „organischer“. Auch das Kontrollieren der

Scroll-Geschwindigkeit ist beim Galaxy Tab 10.1 nicht so gut gelöst wie beim iPad 2. Die beschriebenen Unterschiede gelten für Webseiten ohne Flash-Elemente, denn das iPad kann diese nicht darstellen. Und hier trumpft das Xoom mit Android 3.0 natürlich auf. Die Darstellung von Webseiten mit Flash-Elementen oder Flash-basierten Videos funktioniert im Test bei den besuchten Seiten überwiegend problemlos. Auch die Geschwindigkeit beim Surfen auf Webseiten mit Flash-Elementen ist zufriedenstellend. Der Dual-Core-Prozessor sowie der 1 GByte fassende Arbeitsspeicher machen sich hier positiv bemerkbar.

Desktop-Feeling: Der Browser bietet Tabs zum Wechseln zwischen mehreren Websites an.

Beim Browser nervt allerdings unabhängig vom Inhalt, dass kein schneller Sprung wieder an den Seitenanfang nach langem Scrollen möglich ist. Beim iPad / iPad 2 wird hier nur an den oberen Bildschirmrand getippt, schon scrollt die Seite nach ganz oben. Dafür gefällt das Tab-Browsing, hier kann man wie bei Desktop-Browsern einfach mit Tabs navigieren. Zudem gibt es die Möglichkeit, ein Inkognito-Tab zu öffnen.

4.7.6 Technische Daten im Überblick

Hersteller	Samsung (www.samsung.de)
Produkt	Galaxy Tab 10.1
Preis (UVP)	629 Euro
Technische Hotline	01805/67267864
Prozessor	NVIDIA Tegra 2 / Dual-Core / 1 GHz
Maße (L x B x H)	175 x 257 x 8,6 mm
Gewicht	569 Gramm

Betriebssystem	Android 3.1
Bildschirm	10,1 Zoll / 1280 x 800 Pixel
Integrierter Speicher (Art)	1 GByte (Flash)
Wireless-LAN / Bluetooth	802.11n / 3.0
USB	via Connector-Kabel
HDMI	via Connector-Kabel
Kartenleser	Nein
Einschub für SIM-Karte	ja (Standardgröße)
Kamera	ja (2,0 Megapixel Vorderseite / 3,2 Megapixel Rückseite)
Dockinganschluss	ja
Audioausgang	1
Mikrofon	ja
Lieferumfang	Netzteil, USB-Connector-Kabel
Lagesensor / Lichtsensor	ja / ja
Spracheingabe / Flugzeugmodus	ja / ja

4.7.7 Fazit

Samsung hat es mit Galaxy Tab 10.1 geschafft, die erste „fast" ebenbürtige Alternative zum iPad 2 anzubieten. Das Android-3.1-Tablet ist so flach wie das Apple-Gerät, wiegt sogar noch etwas weniger und wirkt sehr wertig – trotz Kunststoffgehäuse. Der sofortige positive Eindruck beim ersten „Anfassen" manifestiert sich auch im Betrieb. Das Galaxy Tab 10.1 reagiert auf alle Aktionen flott, unterstützt Webseiten mit Flash-Inhalten und unterstützt sehr viele Audio- und Videoformate. Die Softwareausstattung mit Office-Suite und einigen Samsung-Tools passt ebenfalls.

Wir schreiben allerdings von einer „fast" ebenbürtigen Alternative, weil beim iPad 2 die Bedienung weiterhin einen Tick flüssiger, durchdachter und komfortabler funktioniert. Hier kann das verwendete Android 3.1 dem Apple-Betriebssystem iOS noch nicht das Wasser reichen. Außerdem knausert das Galaxy Tab 10.1 mit Anschlüssen ebenso wie das iPad 2

Zu guter Letzt steht sich das Galaxy Tab 10.1 mit einem UVP von 629 Euro ein wenig selbst im Weg. Ein ebenfalls mit 16 GByte Flash-Speicher und 3G ausgestattetes iPad 2 kostet 599 Euro. Zwar wird das ab August 2011 erhältliche Galaxy Tab 10.1 im Preis sicherlich noch leicht fallen, doch bei ähnlichem Preis greifen die meisten sicherlich lieber zum „Original".

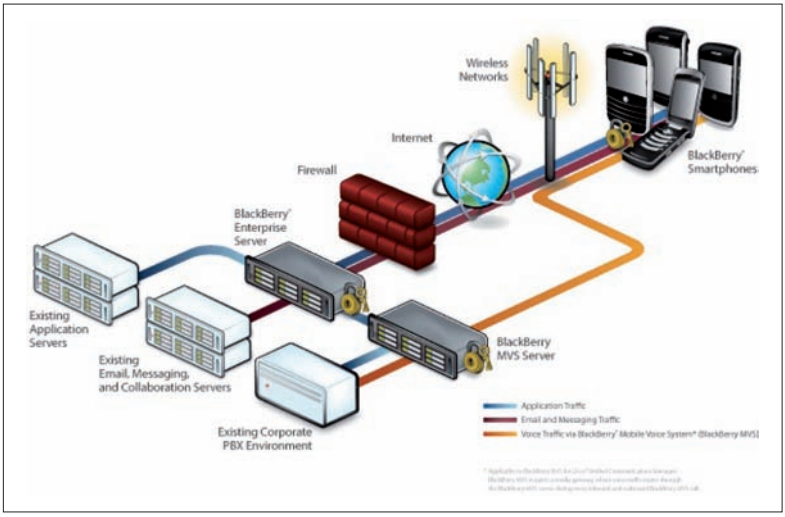
Christian Vilsbeck

5 BlackBerry

Die Situation bei Smartphones für den Unternehmenseinsatz hat sich grundlegend verändert: Erst gab es BlackBerrys – und dann kam lange nichts. Ein BlackBerry galt über Jahre als Synonym für den Zugang von Mitarbeitern zu Unternehmensinformationen – jederzeit und überall. Inzwischen ist die Konkurrenz aus dem Apple- und Android-Lager groß und zwingt Hersteller Research In Motion zu neuen Lösungen für die Erreichbarkeit und Zusammenarbeit an jedem Ort.

5.1 Vergleich – BlackBerry BES gegen BES Express

Um ein BlackBerry-Smartphone zentral zu verwalten oder mit der E-Mail-Infrastruktur eines Unternehmens zu verbinden, benötigt die Lösung einen BlackBerry Enterprise Server, kurz BES. Diese Software ist das Herzstück des BlackBerry-Systems: Sie stellt die verschlüsselte Verbindung zwischen den Smartphones und dem Firmennetzwerk her. Der Server sorgt auch für den bekannten BlackBerry-Effekt: E-Mail-Nachrichten kommen nahezu ohne Zeitverzögerung auf den Smartphones an. Der BES sorgt zudem für die Verwaltung der mobilen Geräte. Über die für jedes Gerät einzigartige PIN kann der Server die am System angemeldeten Smartphones überwachen und managen.

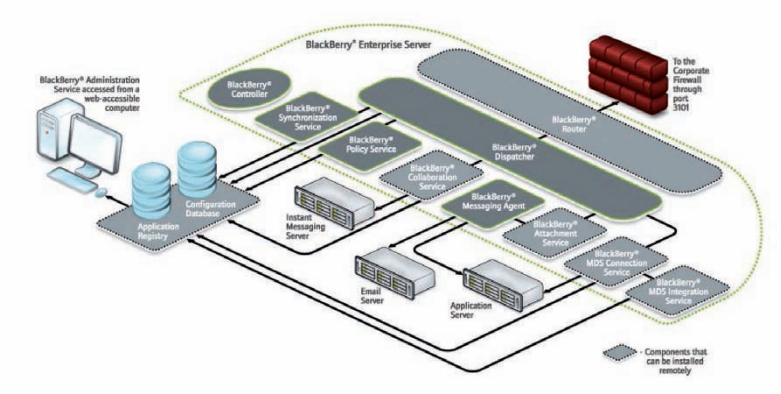


Aufbau: Das Diagramm zeigt, wie das BlackBerry-System arbeitet.

Neben der E-Mail haben die Nutzer auch Zugriff auf Kontakte, Aufgaben und den Kalender. Ein großer Vorteil des Systems ist, dass der BES innerhalb des sicheren Firmennetzwerks sitzt. Dadurch werden die Smartphones Teil des internen Firmennetzes – das bedeutet beispielsweise auch, dass BlackBerrys ohne zusätzliche Programme auf die internen Ressourcen wie etwa Intranetanwendungen zugreifen können. Neben dem kostenpflichtigen BlackBerry Enterprise Server (BES) bietet Hersteller RIM seit 2010 auch eine kostenlose Version, den BES Express. Grundlegend ähneln sich die beiden Serversysteme, allerdings gibt es durchaus Unterschiede, wie unser Artikel zeigt.

5.1.1 BlackBerry Enterprise Server Express

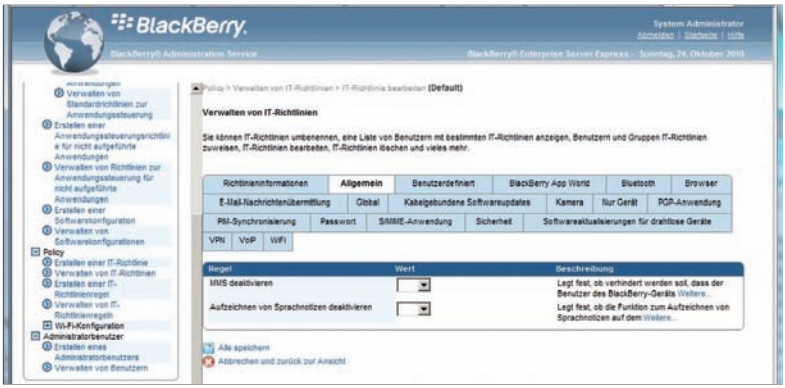
Der BES Express ist das jüngste Mitglied der Serverfamilie von RIM. Die kostenlose Software steht dem großen Server lediglich in wenigen Punkten nach. Er unterstützt beispielsweise nur die Groupware-Server Microsoft Exchange und Lotus Domino – zumindest wenn sie Windows-Betriebssysteme als Grundlage nutzen. Was die Hauptfunktionen betrifft, so muss sich der BES Express kaum hinter dem BES verstecken. Am System angeschlossene Nutzer erhalten die Nachrichten aus ihren Postfächern direkt auf das Smartphone, ebenso wie Anhänge, die auf dem Smartphone verändert werden können. Zudem kann man mithilfe des Systems das eigene Postfach auch nach Nachrichten durchsuchen, die nicht mehr auf dem Smartphone gespeichert sind. Neben den Nachrichten werden auch Kalenderinformationen und Kontakte vom zentralen Server auf das Smartphone übertragen.



Komponenten: die verschiedenen Funktionen und Komponenten des BlackBerry-Systems.

Der Vorteil des BES Express ist, dass er auf dem gleichen Server installiert werden kann, auf dem etwa Exchange läuft. Bis zu 75 Nutzer lassen sich also verwalten, ohne dass ein separater Server aufgesetzt werden muss. Wer die Software auf sepa-

raten Servern einrichtet, kann mehr als 2000 Nutzer verwalten. Der größte Unterschied zum kostenpflichtigen BlackBerry Enterprise Server liegt in den Nutzerrollen und den verfügbaren Regelsätzen. Beim BES Express können die Benutzer fest vorgegebenen Rollen zugeordnet werden – Admins können keine neuen Gruppen erstellen. Ebenso ist es mit den Richtlinien: Der BES Express enthält etwas mehr als 75 Richtlinien in 20 Kategorien, welche die wichtigsten Szenarien abdecken. Größter Vorteil des Systems: Nicht nur die Software ist kostenlos, Unternehmen müssen auch nichts für die Lizenzierung der einzelnen Clients zahlen.

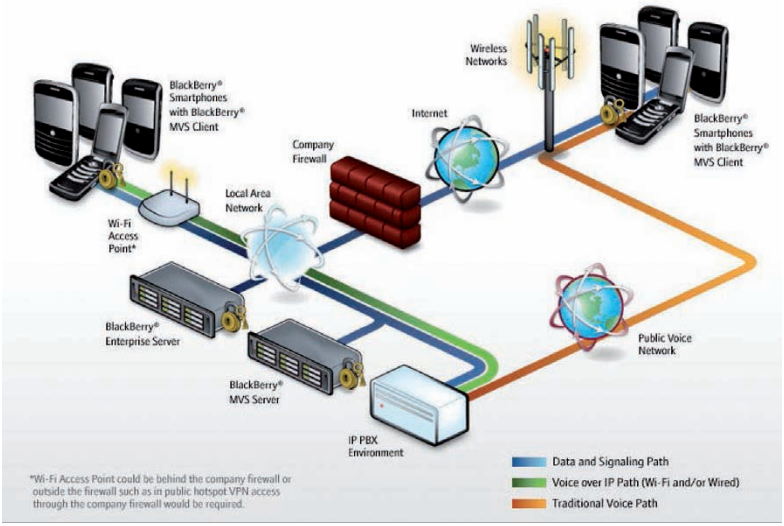


BES Express Richtlinien: Die allgemeinen Richtlinen, der Bereich Benutzerdefiniert ist leer.

5.1.2 BlackBerry Enterprise Server

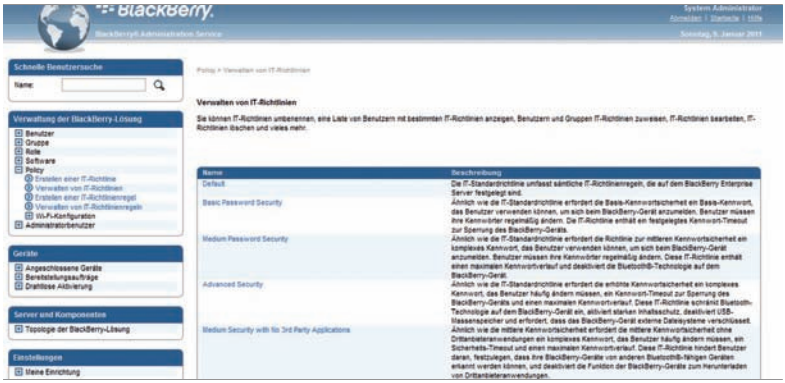
Der BES ist neben den BlackBerry-Smartphones das Hauptprodukt von RIM. Er bietet alle Funktionen des kostenlosen BES Express sowie zusätzliche Features. Zusätzlich zu Exchange und Domino unterstützt das System etwa auch Novell Groupwise. Das Grundpaket kostet laut RIM 3.999 US-Dollar – darin enthalten sind Client-Lizenzen (CAL) für 20 Nutzer. Wer mehr CALs benötigt, kann diese einzeln oder als Pakete von fünf, zehn, 50 oder sogar größeren Blöcken erwerben.

Der Unterschied zur kostenlosen Version zeigt sich vor allem bei den Richtlinien und den Gruppen. Der BES liefert Administratoren mehr als 500 IT-Policies, mit denen sich die Nutzung gezielt definieren lässt. Ein eindrucksvolles Beispiel ist etwa der Punkt „Wi-Fi“. Kann man im BES Express lediglich die Nutzung von WLAN erlauben oder verbieten, hält der BES eine Vielzahl an zusätzlichen Optionen bereit. Neben zusätzlichen Rollen und Gruppen bietet der BES noch weitere Profi-Funktionen für Unternehmen. Dazu gehört etwa eine Option zur Hochverfügbarkeit. So lassen sich zwei oder mehr BlackBerry Enterprise Server zusammenschalten – fällt einer aus, kann der andere einspringen. Nutzer merken davon im besten Fall nichts, die Nachrichten werden einfach weiter übermittelt.



Unified Communications: Mithilfe des Mobile-Voice-Systems lässt sich das Smartphone als Erweiterung des lokalen Telefonanschlusses nutzen.

Eine andere Möglichkeit ist der Einsatz des Mobile-Voice-Systems, kurz MVS. Dabei handelt es sich um eine Unified-Communications-Lösung. Damit ist es beispielsweise möglich, dass die Festnetznummer eines Nutzers mit seinem BlackBerry-Smartphone gekoppelt wird – selbst wenn er nicht am Arbeitsplatz ist, kann man ihn unter seiner regulären Nummer erreichen. Die Telefongespräche können dabei auch über Internet und Wi-Fi übertragen werden – so spart man beispielsweise Roaming-Gebühren.



BlackBerry Enterprise Server: Die Richtlinien.

5.1.3 Fazit

Im Grunde könnte man sich wundern, warum RIM mit dem BES Express überhaupt das Herzstück seines Angebots kostenlos zum Download anbietet – und noch dazu, ohne für die Clients einzelne Lizenzen zu verlangen. Doch es wäre zu einfach, den BES Express als eine Art „Einstiegsdroge" darzustellen.

Der kostenlose BES Express eignet sich nicht nur für kleinere Unternehmen, die nur wenige BlackBerrys verwalten, sondern er kann auch separat zu einem bereits bestehenden BES betrieben werden. So lässt sich etwa neben dem firmeneigenen System auch eine weitere, separate Infrastruktur aufbauen, etwa um private Geräte einzelner Nutzer anzuschließen, ohne dafür teure CALs zu erwerben.

Moritz Jäger

Dieser Artikel basiert auf einem Beitrag unserer Schwesterpublikation Computerwoche.

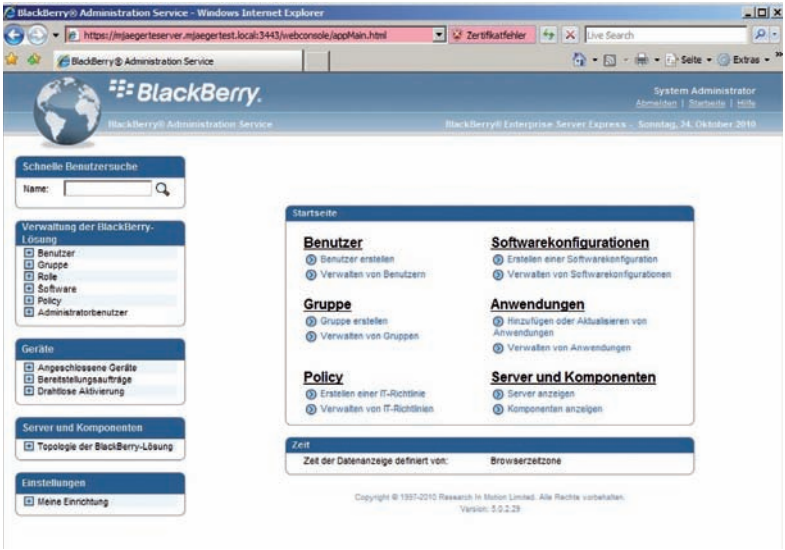
Moritz Jäger ist freier Autor und IT-Journalist aus München. Seine Themengebiete umfassen IT-Sicherheit, Netzwerk, Windows sowie Lösungen und Tools für die mobile Arbeitswelt, etwa Push-Mail, Übertragungstechnologien, USB-Anwendungen oder Endgeräte und deren Absicherung. Unter anderem schreibt er regelmäßig für TecChannel, PC-Welt, ComputerWoche und ZDNet.de.

TecChannel-Links zum Thema	Webcode	Compact
Vergleich – BlackBerry BES gegen BES Express	2034908	S.235
Workshop – BlackBerry Enterprise Server Express installieren und konfigurieren	2032009	S.240
Workshop – Google-App-Account mit BlackBerry-Server koppeln	2033814	S.244
Test: BlackBerry PlayBook	2035357	S.247

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

5.2 Workshop – BlackBerry Enterprise Server Express installieren und konfigurieren

Der BlackBerry Server Express ist RIMs kleine Version des im Unternehmen installierten BlackBerry Enterprise Servers. Vorteil gegenüber einem „normalen" BES: Der BlackBerry Server Express ist kostenlos erhältlich (http://de.blackberry.com/services/business/server/express/). RIM hat den Server allerdings eingeschränkt. Der BES Express richtet sich explizit an BlackBerry-Einsteiger und kleinere Installationen mit Exchange-Umgebungen. Der BES Express lässt sich auf dem gleichen Server installieren wie Exchange und unterstützt dann bis zu 75 angeschlossene Endgeräte. Wenn Sie mehr benötigen, müssen Sie den Server auf einem separaten Server installieren. In diesem Fall werden dann pro Server bis zu 2000 Geräte unterstützt. Wer eine andere Groupware einsetzt, der muss zum BES greifen, denn nur er unterstützt Novell Groupwise oder IBM Domino.

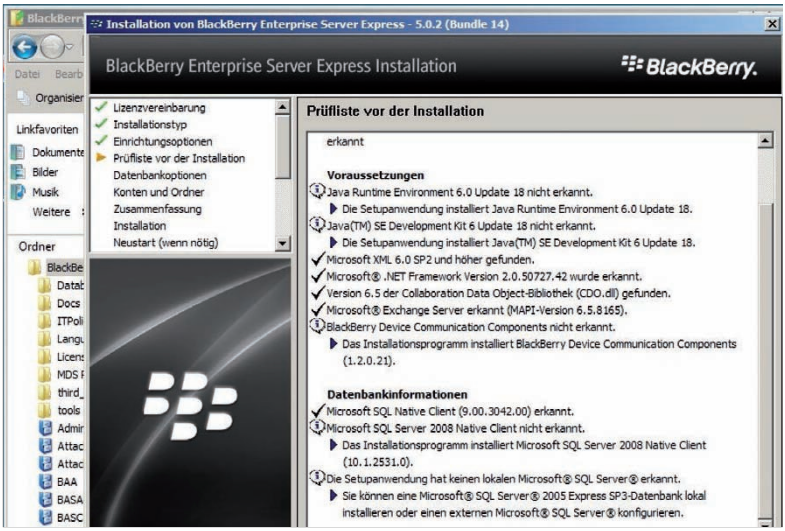


Smartphone-Verwaltung: Das Web-Interface des BES Express.

Ebenfalls eingeschränkt sind Richtlinien und die Rollen der Admins. Der BES Express liefert vorgegebene Rollen für die Verwaltung, die sich nicht anpassen lassen. Zudem sind deutlich weniger Richtlinien enthalten als in der kostenpflichtigen Version. Diese sind laut RIM allerdings so ausgesucht, dass sie die Anforderungen der meisten Nutzer erfüllen. Zudem sind Enterprise-Funktionen, etwa zur Hochverfügbarkeit oder der BlackBerry Monitoring Service nicht enthalten.

5.2.1 Systemanforderungen und Vorbereitung

Der BES Express lässt sich wie eingangs erwähnt nur zusammen mit Microsoft Exchange nutzen. Unterstützt werden Exchange 2003, 2007 sowie 2010, ebenso die jeweiligen Ausgaben des Small Business Servers oder des Essential Business Servers. Der BES Express selbst kann kostenlos über die Website *http://de.blackberry.com/services/business/server/express/* heruntergeladen werden. Der Download läuft über einen Webshop an, bei dem man sich zunächst mit diversen Daten registrieren muss, darunter Name, Firma und E-Mail-Adresse. Nach kurzer Zeit erhält man auf die hinterlegte E-Mail-Adresse eine Nachricht mit den Informationen zum Download.



Überprüfung: Vor der Installation untersucht der BES Express das System und meldet etwaige Probleme.

Der zugeschickte Link enthält zudem weitere wichtige Informationen: die SRP-ID, SRP Authentication Key, CAL ID sowie CAL Authentication Key. Diese Informationen werden für die Lizenzierung während der Installation des BES Express benötigt. Der Link ist personalisiert und verfällt nicht auch nach mehreren Monaten noch kann man den Download sowie die Schlüssel abrufen.

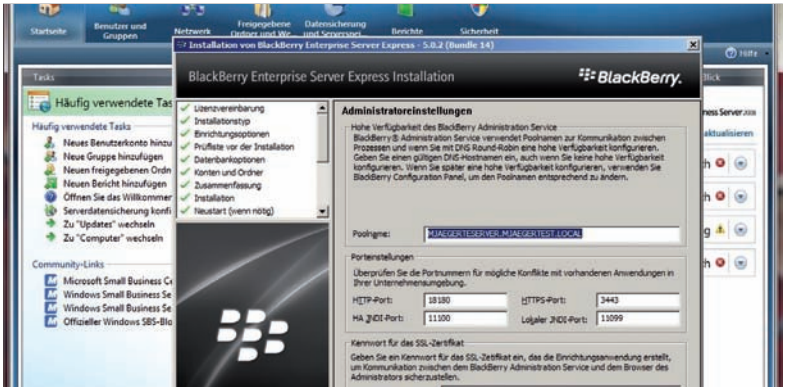
Der BES Express überprüft in einem der ersten Schritte, ob die notwendige Software lokal vorhanden ist. Bei einem System ab Exchange 2007 fehlen oftmals zwei Microsoft-Komponenten, die Message API (MAPI) sowie Collaboration Data Objects. Zwar bringt der BES Express die meisten anderen Informationen und Installationspakete mit, MAPI und CDO muss der Nutzer allerdings manuell installieren, Microsoft stellt das notwendige Paket, das keinen Serverneustart erfordert, auf

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=94274318-27c4-4d8d-9bc5-3e6484286b1f zum Download bereit. Für den Workshop nutzten wir einen lokalen Testserver auf Basis des Microsoft Small Business Server 2008. Die Installation wurde in einer virtuellen Maschine durchgeführt.

5.2.2 Installation und Abschlusskonfiguration

Die Installation des BES Express ist relativ einfach gehalten. Seit Version 5.0.2 ist zudem das komplette Interface lokalisiert, was die Installation weiter vereinfacht. Der rund 546 MByte große Download des BES Express liefert eine sich selbst extrahierende ZIP-Datei, anschließend startet das Setup automatisch. Während des Setups durchläuft die Software zwei verschiedene Stadien: die eigentliche Installation sowie das abschließende Setup. Nach der ersten Hälfte muss dabei der Server neu gestartet werden. In der ersten Hälfte der Installation werden die Grundlagen für den BES Express festgelegt. Dazu gehören die Annahme der Lizenzvereinbarungen, das Festlegen des Installationstyps, die Auswahl der zu installierenden Optionen, die Auswahl der Datenbank sowie Informationen zu Konto und Kennwort. Die Bilderstrecke zeigt die Installation im Detail. Die Fragen sind relativ einfach zu beantworten, im Zweifelsfall sollte man einfach alles installieren.

Ein wenig trickreicher, aber dennoch machbar ist die Abschlusskonfiguration nach dem Neustart des Servers. Nach der Eingabe der Informationen zur Datenbank müssen die Lizenzschlüssel (CAL- und SRP-Informationen) eingegeben werden; diese erhält man über den Link in der E-Mail. Im Test traten die einzigen Probleme bei der Konfiguration der MAPI-Einstellungen auf – genauer gesagt konnte der BES Express nicht auf die MAPI-Funktionen zugreifen. Nach einigen Versuchen brachte die Eingabe von „localhost“ beim Microsoft Exchange Server die Lösung, anschließend lief die Konfiguration weiter.



Abschlusskonfiguration: Die administrativen Einstellungen.

Schlägt die Verbindung zum ActiveDirectory fehl, kann man alternativ einen lokalen Administrator anlegen. Hierbei ist allerdings Vorsicht geboten: Das vergebene Passwort lässt sich nicht ohne Weiteres zurücksetzen; geht es verloren, muss der Server unter Umständen neu installiert werden.

5.2.3 Administration per Web-Interface

Seit RIM die Serverkomponente auf Version 5 aktualisiert hat, kann der BES über ein Web-Interface statt einen separaten Client konfiguriert werden. Sind alle Dienste erfolgreich gestartet, zeigt die Installation zum Abschluss die entsprechenden Links an. Greift man vom Server selbst auf das Interface zu, muss die URL zur sicheren Zone hinzugefügt werden, eher kann man sich nicht anmelden.

Beim Login kann man die Sprache ändern und zudem festlegen, ob man sich per ActiveDirectory oder über den bei der Installation vergebenen Admin-Account anmelden möchte. Anschließend wird das Hauptmenü angezeigt; von diesem aus kann man die am häufigsten genutzten Funktionen direkt wählen. Auf der linken Seite sind vier weitere Menüs zu sehen; hier erhält man Zugriff auf die Verwaltung der BlackBerry-Lösung, kann die Geräte einrichten, auf Serverkomponenten zugreifen oder Einstellungen ändern. Die bereits auf dem System eingerichteten User werden vom BES Express automatisch integriert, neue Benutzer lassen sich einzeln anlegen oder über eine Datei importieren.

Neue BlackBerry-Smartphones lassen sich direkt über den Server aktivieren und mit einem Benutzerkonto verknüpfen. Dazu wird zum jeweiligen Nutzer ein entsprechendes Passwort erstellt. Die User können anschließend durch Eingabe der E-Mail-Adresse und des erstellten Passworts aktiviert werden. Der wahrscheinlich interessanteste Teil des Servers sind die Policies. Damit kann man Richtlinien erstellen und auf die jeweils angeschlossenen BlackBerrys verteilen. Wie bereits erwähnt, enthält der BES Express deutlich weniger Richtlinien als der BES, die wichtigsten sind aber an Bord, wie die Bilderstrecke zeigt. Angeschlossene Smartphones lassen sich ebenfalls direkt verwalten. Wie von einem BES gewohnt, kann Software auf die Systeme ausgerollt werden. Geht ein BlackBerry verloren, kann man das Smartphone zudem vom BES Express aus sperren oder komplett löschen.

Moritz Jäger

Moritz Jäger ist freier Autor und IT-Journalist aus München. Seine Themengebiete umfassen IT-Sicherheit, Netzwerk, Windows sowie Lösungen und Tools für die mobile Arbeitswelt, etwa Push-Mail, Übertragungstechnologien, USB-Anwendungen oder Endgeräte und deren Absicherung. Unter anderem schreibt er regelmäßig für TecChannel, PC-Welt, ComputerWoche und ZDNet.de.

5.3 Workshop – Google-App-Account mit BlackBerry-Server koppeln

Google hält mit Apps for your Domain ein Cloud-Angebot bereit, mit dem Firmen die verschiedenen Google-Dienste für ihre eigene E-Mail-Struktur nutzen können (http://www.google.com/apps/). So kann man etwa Googlemail und auch Google Kalender, Texte und Tabellen, Sites oder Video unter der eigenen Firmendomain betreiben.

Zusatzverbindung: Über den Connector kann der BES auf Google Apps for your Domain zugreifen. (Quelle: Google)

Zusammen mit einem Connector für den Outlook-Client bietet Google auch ein Tool an, mit dem man Google Apps mit dem BlackBerry Enterprise Server oder dem BES Express verknüpfen kann. Zwar lassen sich mit einem BlackBerry die Nachrichten auf dem Google-Apps-Konto auch ohne zusätzliche Software abrufen, doch wer die Geräte auch verwalten will, benötigt dazu den entsprechenden Server. Die Unterschiede zwischen BES und dem kostenlosen BES Express erläutern wir im Kapitel 4.1 dieses Compacts (Webcode **2034908**). Allerdings ist die Lösung ein wenig umständlich einzurichten. Neben dem eigentlichen Connector benötigt man auf dem Windows-Server noch ein installiertes Exchange, einen Outlook-2007-Client und einen BlackBerry-Server. Zudem muss man Google Apps in der kostenpflichtigen Premier-Version verwenden. Google stellt auf *www.postini.com/webdocs/gapps_connector/wwhelp/wwhimpl/js/html/wwhelp.htm* eine Installationsanleitung für BlackBerry Enterprise Server zur Verfügung.

5.3.1 Connector: vorbereiten und installieren

Der Google Connector verbindet sich nicht direkt mit dem BlackBerry-Server. Stattdessen nutzt das Tool die Verbindung zwischen Exchange und BES, um sich dazwischenzuschalten. Für den BlackBerry-Server sieht es so aus, als würde er einfach weiter mit dem Exchange kommunizieren, in Wahrheit wird die Verbindung aber an Google Apps weitergereicht. Dazu benötigt der Google Connector das

MAPI-Protokoll. Um es auf dem Server zur Verfügung zu haben, muss zunächst eine Version von Outlook 2007 SP 2 installiert werden – wobei diese nicht unbedingt mit dem Exchange-Server gekoppelt werden muss.

Zugangsdaten: Per OAuth kann der Connector auf die Konten zugreifen. (Quelle: Google)

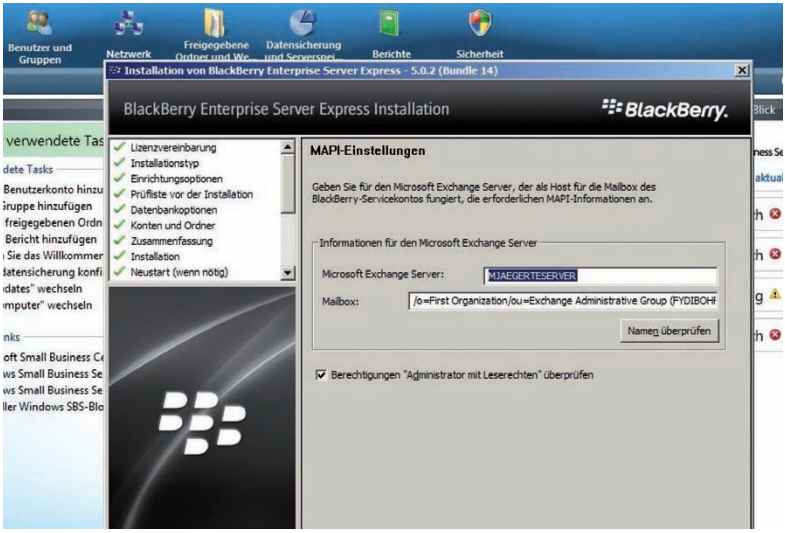
Nun muss im Google-Apps-Kontrollcenter die OAuth-Funktion aktiviert werden. Diese sorgt dafür, dass sich der Connector bei dem Dienst anmelden kann – erst dann ist der Zugriff auf die Informationen möglich. Man findet ihn dort unter „Erweiterte Tools – OAuth-Zugriff auf Drittanbieter-Clients verwalten". Zusätzlich muss ein passender Nutzer, etwa besadmin, angelegt werden. Google empfiehlt zudem, dass dieser Time Zone Hotfix von Microsoft (http://support.microsoft.com/kb/979306/) installiert wird.

Anschließend kann der Google Connector heruntergeladen und installiert werden. Die Software schreibt sich in die „Programme" ein und kann hier konfiguriert werden. Hier müssen der E-Mail-Account, der OAuth Consumer Key und das Secret eingegeben werden, das im Kontrollzentrum festgelegt wurde.

5.3.2 BlackBerry-Server installieren

Ist der Google App Connector eingerichtet, ist als Nächstes der eigentliche BlackBerry-Server zu installieren. Dabei ist es egal, ob man den kostenlosen BES-Express- oder den „kompletten" BlackBerry-Enterprise-Server verwendet, der Connector arbeitet mit beiden Systemen.

Der Server selbst ist eine Exe-Datei. Ein Doppelklick startet den Assistenten, der durch die Installation führt und zunächst überprüft, ob alle notwendigen Komponenten vorhanden sind. Unter Umständen fehlen zwei Komponenten, Message API (MAPI) sowie Collaboration Data Objects. Ein Installationspaket liefert diese Funktionen nach und lässt sich unter *www.microsoft.com/downloads/en/details.aspx?FamilyID=94274318-27c4-4d8d-9bc5-3e6484286b1f* kostenlos herunterladen.



Abschlusskonfiguration: Die MAPI-Einstellungen waren im Test ein wenig trickreich, am Ende half der Eintrag localhost.

Der Installationsvorgang unterteilt sich in zwei Teile – zunächst in die eigentliche Installation und nach einem Neustart in die Konfiguration des BlackBerry-Servers. Weitere Details zur Einrichtung finden Sie im Artikel „BES Express einrichten und konfigurieren“ (Webcode **2032009**). Mit dem Connector selbst muss der BES nicht verbunden werden, das erledigt die Verbindung zum ActiveDirectory.

5.3.3 Fazit: umständlich, aber sinnvoll

Der Connector von Google ist nicht gerade eine elegante Lösung, im Gegenteil: Google verlangt, dass einiges an zusätzlicher Software installiert wird. Wer sich allerdings die Mühe macht und das System um den Connector erweitert, erhält dafür einiges an zusätzlichen Features. Highlight sind dabei natürlich die Verwaltungsfunktionen, mit denen sich die BlackBerry-Smartphones von einem zentralen Platz nahezu komplett steuern lassen.

Der Google Connector zeigt aber auch ein sinnvolles Einsatzfeld für den BES-Express-Server. Steigt eine Firma beispielsweise von Exchange auf Google Apps um, sind die notwendigen zusätzlichen Lizenzen (Exchange und Outlook) meist noch ausreichend vorhanden. Mit dem BES Express erhält man ohne zusätzliche Kosten einen deutlichen Mehrwert, denn kaum ein anderes Smartphone-System lässt sich so umfangreich an Unternehmensrichtlinien anpassen.

Moritz Jäger

5.4 Test: BlackBerry PlayBook

2011 gilt als das Jahr der Tablet-PCs, und mit dem BlackBerry PlayBook hat der kanadische Hersteller RIM ein interessantes Gerät im Sieben-Zoll-Format veröffentlicht – in den USA ist das BlackBerry PlayBook bereits seit Ende April 2011 erhältlich. Nach dem Auspacken besticht das Tablet durch sein Design: RIM verwendet Glas auf der Vorder- und einen gummiartigen Überzug auf der Rückseite. Der kapazitive Multi-Touchscreen ist von einem schwarzen Rahmen umgeben – dieser ist ebenfalls berührungsempfindlich und Teil des Bedienkonzeptes.

Das PlayBook: Nicht nur der Bildschirm, auch der Rahmen ist berührungsempfindlich.

Wischt man von unten nach oben, verkleinert das PlayBook die aktuelle Anwendung und zeigt das Hauptmenü. Wird in einer App von oben nach unten gewischt, klappt das Konfigurationsmenü der jeweiligen Anwendung herunter.

Start: Die Hauptansicht des PlayBooks, samt drei geöffneter Apps.

Anders als etwa das Galaxy Tab oder das iPad/iPad 2 hält man das PlayBook hauptsächlich quer. Der Bildschirm selbst unterteilt sich in drei Bereiche: Oben ist die Statusleiste, in der beispielsweise Uhrzeit, Batterieladung und eingehende E-Mails angezeigt werden. In der Mitte sind die minimierten Ansichten der gestarteten Apps zu sehen. Darunter sind die Menüs zu finden, diese teilen sich in *Alle, Spiele, Medien, Favoriten* und *BlackBerry Bridge* auf.

5.4.1 Hardwareausstattung und QNX-OS

Das PlayBook verfügt über vier Schalter: einen Ein-/Ausschalter, jeweils eine Taste für Lauter und Leiser sowie einen Bedienknopf für Abspielen/Pause. Auf der Vorder- und Rückseite ist jeweils eine Kamera angebracht – vorne mit drei, hinten mit fünf Megapixeln Auflösung. Außerdem findet sich dort noch der Anschluss für Kopfhörer und Headset. Auf der gegenüberliegenden Seite, am unteren Ende des PlayBooks, sind die weiteren Anschlüsse angebracht: Neben Micro-USB finden sich dort der Anschluss für Mini-HDMI sowie Kontakte für künftige Adapter.

Einrichtung: Die Auswahl des WiFi-Zugangspunktes – wenn ein Captive-Portal vorhanden ist, muss man unten links auf „Hotspot Setup" klicken, um die Anmeldung abzuschließen.

Im Inneren des PlayBooks arbeitet aktuelle Hardware: Dem Dual-Core-Prozessor mit 1 GHz Taktfrequenz steht 1 GByte Arbeitsspeicher zur Seite. Zum Speichern von Daten warten je nach Modell 16, 32 oder 64 GByte auf den Nutzer. Jedes PlayBook verfügt über Bluetooth mit 2.1 + EDR sowie Wi-Fi, das im 2,4- und 5-GHz-Band arbeitet. Unterstützt wird WLAN 802.11 a/b/g/n, GPS ist ebenfalls integriert.

Aktuell gibt es noch keine Modellvariante mit 3G oder LTE – entsprechende Versionen sollen aber folgen. Das ist auch kein schlechter Zug: Solange kein Mobilfunk-

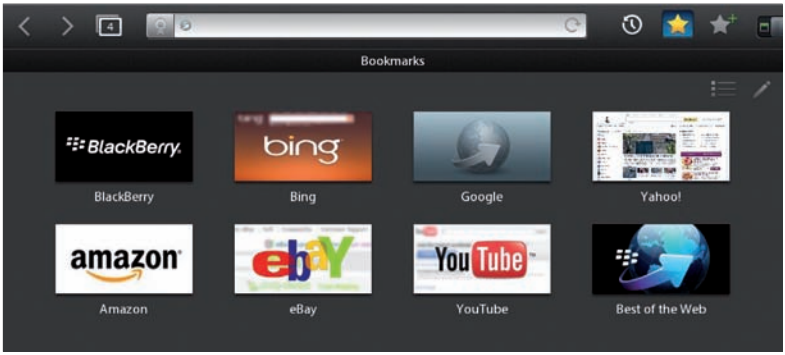
provider involviert ist, kann RIM Updates veröffentlichen, ohne dass die Provider diese zusätzlich absegnen und so die Auslieferung verzögern können. Hintergrund ist, dass RIM erstmals auf QNX als Betriebssystem setzt. Der Hersteller hat das auf Embedded-Systeme spezialisierte Betriebssystem 2010 akquiriert.

QNX ist alles andere als ein neues Betriebssystem – es gilt als robust und kommt beispielsweise in Fahrzeugen von Audi, Porsche oder BMW, im Cisco-CRS-1-Carrier-Router und sogar in Nuklearanlagen zum Einsatz. Die Benutzeroberfläche reagiert schnell und sieht noch dazu gut aus – sie entstand in Kombination mit Adobe, die Flash-Technologie ist Bestandteil des kompletten Betriebssystems.

Bei der Akku-Laufzeit bleibt das PlayBook hinter dem iPad zurück: RIM nennt zwar offiziell noch keine Laufzeit, aus der Praxis lässt sich aber sagen, dass das PlayBook etwa sechs Stunden durchhält. Die Lebensdauer des Akkus verringert sich noch mehr, wenn WLAN und Bluetooth samt BlackBerry Bridge aktiv sind.

5.4.2 Browser, Office, Multimedia

Größtes Manko von Apples iPad/iPad 2 und vielen Android-Tablets ist die fehlende oder schwache Flash-Unterstützung im Browser. Das PlayBook teilt diese Schwäche nicht: Der Browser ist nicht nur schnell, er kann neben Flash-Inhalten auch JavaScript ausführen. Allerdings gibt es dabei immer wieder Probleme, Genaueres dazu lesen Sie im Kapitel „Schattenseiten“. Dazu kommt die Unterstützung für Tabbed Browsing. Im Test konnten wir mehr als 30 Tabs öffnen, ohne dass das Gerät merklich langsamer wurde. In den Browser integriert ist ein privater Modus, wie ihn etwa auch aktuelle Desktop-Browser bieten.



Browser: Die Startseite des Browsers mit Seitenvorschlägen.

Für den Office-Bereich sind sowohl Adobe Reader als auch die Premiumversionen von Word-, Sheet- und Slideshow to Go installiert. Die Programme stammen von DataViz, einer Firma, die RIM 2010 gekauft hat. Damit lassen sich Office-Doku-

mente in Formaten wie *.doc oder *.docx nicht nur anzeigen, sondern auch gleich bearbeiten. Besonders praktisch in Slideshow to Go: Die Software unterstützt den HDMI-Ausgang des PlayBooks. So kann man auf einem Bildschirm die Präsentation anzeigen, während man auf dem Tablet die Wiedergabe steuern und die jeweiligen Notizen zu den einzelnen Folien einsehen kann. Das klappt mit allen HDMI-fähigen Geräten und benötigt glücklicherweise keinerlei Treiberinstallation.

Die HDMI-Ausgabe funktioniert auch mit dem integrierten Video-Player. Das PlayBook erweist sich als sehr leistungsfähig, selbst HD-Inhalte mit 1080p kann das Gerät ohne Ruckeln auf einem anderen Gerät wiedergeben. Zu den unterstützten Formaten gehören AVI, WMV, H.264 und MPEG4. Auch Musik spielt das Tablet ab, wobei der integrierte Player ein wenig umständlich zu bedienen ist und beispielsweise nur eine Playlist zulässt. Hier bleibt zu hoffen, dass RIM nachbessert oder Drittthersteller entsprechende Player liefern – wie es ja beispielsweise bei Android inzwischen auch der Fall ist.

5.4.3 E-Mail, Kontakte, PIM: die BlackBerry Bridge

Bereits während des Einrichtungsvorgangs schlägt das Tablet vor, eine Paarung mit einem BlackBerry-Smartphone einzurichten. Diese Funktion nennt sich BlackBerry Bridge. Die Bridge verwandelt das PlayBook effektiv in einen Thin Client, mit dem man bestimmte Funktionen des Smartphones nutzen kann. Dazu gehören beispielsweise *E-Mail, Kontakte, BlackBerry Messenger, Aufgaben* oder *Notizen*. Um die Bridge nutzen zu können, ist auf BlackBerry Smartphone eine separate App notwendig. Diese ist für nahezu alle Smartphones verfügbar, die mindestens über Version 5.0 des Betriebssystems verfügen. Alle kompatiblen Geräte sind unter *http://appworld.blackberry.com/webstore/content/19435* aufgeführt.

Das Bridge-System bringt mehrere Vorteile: BlackBerry-Besitzer müssen, abgesehen von einem Bluetooth-Pairing, keinerlei Konfiguration vornehmen, um auf die E-Mails zugreifen zu können. Firmen profitieren dagegen von dem verringerten Managementaufwand. Die Daten sind nur zugänglich, solange eine aktive Verbindung zum jeweiligen BlackBerry besteht. Reißt diese ab, werden alle Funktionen gesperrt. Mit Ausnahme eines verschlüsselten Caches sind keine Informationen auf dem Tablet gespeichert – selbst wenn das PlayBook also verloren geht, sind sensible Daten wie E-Mails oder Kontakte nicht zugänglich. Ein Austausch von Dateien zwischen Bridge und restlichem Speicherbereich ist, mit Ausnahme der Dokumentenbearbeitung, nicht vorgesehen. Mit der Bridge kann man nicht nur auf die PIM-Funktionen und den BlackBerry Messenger zugreifen, sondern erhält zudem den Bridge Browser. Dieser unterscheidet sich in einer zentralen Option vom regulären Browser: Er nutzt den BlackBerry als Proxy und setzt auf dessen Datenverbindung, um ins Web zu gelangen. Der positive Nebeneffekt: Das PlayBook wird zum Teil des Unternehmensnetzwerks und kann auf Intranet-Ressourcen hinter der Firewall zugreifen – immer vorausgesetzt, dass auch der BlackBerry die jeweiligen Zugriffsrechte besitzt.

Einstellungen: Das PlayBook kann Smartphones per Bluetooth als Modem nutzen – zusätzliche Software ist weder auf Smartphone noch auf dem PlayBook notwendig.

Der größte Vorteil der Bridge ist zugleich ihr Nachteil: Ohne BlackBerry-Smartphone verliert das PlayBook zahlreiche Funktionen, schließlich ist beispielsweise kein anderer E-Mail-Client vorinstalliert. Die konstante Bluetooth-Verbindung fordert zudem ihren Tribut, die Akkus vom Smartphone und dem Tablet werden dadurch zusätzlich belastet.

5.4.4 IT-Verwaltung – PlayBook Administration Service und Project Fuse

Die Verwaltung des PlayBook ist in mehreren Schritten geplant: Zunächst wird es ein Update für den BES geben, mit dem sich lediglich definieren lässt, ob die Bridge-Funktion erlaubt ist oder nicht. Zusätzlich kann man die integrierte Log-Funktion abschalten. Im Rahmen der Konferenz BlackBerry World wurden für den Herbst 2011 auch native E-Mail- und PIM-Apps angekündigt. Diese verwandeln das Tablet effektiv in einen BlackBerry, komplett mit Zugriff auf BIS oder BES sowie der Möglichkeit der Administration.

Sobald diese Dateien verfügbar sind, will RIM einen separaten Managementserver für PlayBooks veröffentlichen; er nennt sich PlayBook Administration Service. Wie der BES Express Server wird diese Software kostenlos und ohne Lizenzkosten zu haben sein. Anfangs werden laut RIM Microsoft Exchange und Lotus Domino als Serverumgebung unterstützt. Damit werden „richtige“ Richtlinien, eine Nutzerverwaltung, eine App-Verwaltung sowie die Enterprise-Aktivierung möglich.

Zeitnah soll zudem die nächste Version des BES folgen, der aktuelle Codename dafür ist Project Fuse. Der neue Server soll PlayBooks und Smartphones unter einer

Oberfläche verwalten können. Möglicherweise ist auch die Verwaltung von Android- und iOS-Geräten möglich, zumindest kündigte RIM die Übernahme des Münchner Managementanbieters Ubitexx (www.ubitexx.com) an. Dessen Lösung soll künftig in die Produkte des kanadischen Herstellers integriert werden.

PlayBook Administration Service im Vergleich

Feature	PlayBook Administration Service	BlackBerry Enterprise Server Express	BlackBerry Enterprise Server
Free Software and CALs	X	X	
Base IT policies	X	X	X
Advanced IT policies			X
User and Device Management	X	X	X
Application Management	X	X	X
Enterprise Catalog support	X		
OTA Enterprise Activation	X	X	X
Monitoring			X
High Availability			X
BlackBerry Mobil Voice System			X
Enterprise IM & social networking			X
Chalk Pushcast integration			X

5.4.5 Schattenseiten, Early-Adopter-Probleme und Kinderkrankheiten

In der Praxis klappt die Flash-Wiedergabe zwar meistens, sie ist deutlich besser als bei vielen anderen Tablet-Browsern oder bei Apps wie Skyfire. Allerdings sind hier Grenzen gesetzt: Während beispielsweise Videos von TecChannel, PC-Welt oder Computerwoche problemlos wiedergegeben werden, gibt es bei komplexeren Seiten wie der Mediathek des ZDF Probleme (www.zdf.de/ZDFmediathek). Ähnliches gilt für Video-Streaming-Seiten: Vimeo (www.vimeo.com) klappt sehr gut, YouTube (www.youtube.com) machte im Test zeitweise Probleme. Zwar liefert RIM eine spezielle YouTube-App – eleganter wäre es aber, die Videos direkt im Browser zu sehen. Anders dagegen, wenn die Videos in einer Seite wie Facebook (www.facebook.com) eingebettet sind – dann klappt die Wiedergabe meist problemlos. Ein Grund dafür könnte der massive Verbrauch von RAM sein – sobald man die Videos lädt, geht der zur Verfügung stehende Speicher deutlich nach unten, über die Einstellungen und den Punkt Hardware lässt sich das überprüfen.

Auch komplexe Flash-Anwendungen wie Grooveshark (www.grooveshark.com) lassen sich nicht starten. Der Browser ist zudem nicht immer stabil: Im Test stürzte er öfter ab, vor allem wenn wir versuchten, auf aufwendige Seiten zuzugreifen.

Nach einem Neustart waren einige Webseiten, beispielsweise die ZDF Mediathek, dagegen problemlos abrufbar – der Browser verschlingt dann allerdings fast 200 MByte des Arbeitsspeichers. Es liegt also nahe, dass es teilweise zu wenig Arbeitsspeicher gibt, vor allem, wenn mehrere Programme gestartet wurden oder im Hintergrund laufen. Early Adopter leiden zudem unter regionalen Beschränkungen. So hat ein in den USA aktiviertes PlayBook im Test beispielsweise einen komplett anderen Podcast-Katalog als ein in Deutschland aktiviertes Gerät. Auch andere Applikationen, etwa Slacker Radio (www.slacker.com), arbeiten hier nicht. Die App World (http://de.blackberry.com/services/appworld/) scheint aktuell (noch) nicht beeinträchtigt zu sein, zumindest wichtige Apps wie Facebook sind allen Nutzern zugänglich. Das PlayBook hat zudem das Problem aller neuen Plattformen: Die Auswahl an verfügbaren Apps ist nicht besonders groß, die Qualität größtenteils eher mittelmäßig. Es gibt einige Ausnahmen, etwa Facebook, FourPlay (ein Foursquare-Client) oder Scrapbook.

Android-Apps, wie von RIM angekündigt, laufen noch nicht auf dem PlayBook. Allerdings soll im Herbst 2011 ein Software-Update für die Integration der Android-Apps sorgen. Die Apps werden dann laut RIM über den normalen App Store installiert. Optisch wird es keinen besonderen Unterschied geben.

5.4.6 Fazit

Nein, RIM (www.rim.com) schafft es nicht, im ersten Anlauf ein perfektes Tablet zu veröffentlichen. Dennoch ist das PlayBook alles andere als ein Ladenhüter. Die Hardware kann sich durchaus sehen lassen, QNX als Betriebssystem ist ebenfalls eine stabile und gute Wahl. Es bleibt zu hoffen, dass RIM die Softwareprobleme, vor allem beim Browser, in den Griff bekommt. Bislang sieht es dafür allerdings recht gut aus: Zum Testzeitpunkt war die Version 1.0.3.1868 installiert, das zweite Update für das Tablet seit dem Kauf. Diese Firmware behebt viele Mankos, die RIM in früheren Versionen angekreidet wurden: Beispielsweise ist nun eine Video-Chat-App installiert, und das Büropaket kann Office-Dokumente, die per BlackBerry Bridge auf dem Tablet geöffnet wurden, bearbeiten und neu abspeichern.

Vor allem in Kombination mit einem BlackBerry-Smartphone ist das PlayBook bereits jetzt ein praktisches Tablet – kein anderer Hersteller schaffte bislang eine derart gute Integration von Smartphone und Tablet. Unternehmen profitieren von der sicheren Infrastruktur – auch diese kann kein anderes Smartphone und kein anderes Tablet derzeit bieten. So ist das PlayBook in der Lage, nahezu ohne Konfiguration auf Daten hinter der Firewall des Unternehmens zuzugreifen, E-Mails sicher anzuzeigen sowie Office-Dokumente zu bearbeiten. RIMs Tablet besticht zudem durch ein sehr gutes Display und angenehme Haptik.

Ein gutes Beispiel für die gelungene Integration ist, dass auf dem BlackBerry gespeicherte WLAN-Verbindungen auf das PlayBook übertragen werden. Anschließend kann sich das Tablet sofort mit den bekannten Wi-Fi-Zugangspunkten verbinden. Eine andere clevere Funktion findet man im Menü Tethering: Das PlayBook kann mithilfe von Bluetooth und Profilen wie DUN ein gepaartes Smartphone als Modem nutzen – in nur drei Schritten war das Tablet über das Smartphone mit dem Internet verbunden.

Es bleibt zu hoffen, dass zum Start des PlayBooks in Deutschland im Laufe des zweiten Quartals 2011 die Softwareprobleme bereits behoben sind. Versprochen hat der kanadische Konzern, spätestens alle zwölf Wochen ein neues Update zu liefern. Im Herbst 2011 sollten dann auch die Android-Apps auf dem PlayBook laufen. Interessant ist auch der Preispunkt: Ähnlich wie das Apple iPad 2 kostet es zwischen 499 und 699 US-Dollar.

Moritz Jäger

Anhang: Technische Daten BlackBerry PlayBook

Preis (unverbindliche Preisempfehlung)	499 bis 699 US-Dollar plus Steuern
Prozessor	Texas Instruments OMAP 4430, 32 Bit, 1 GHz
Maße (L x B x H) / Gewicht (mit Akku)	19,4 x 13 x 1,0 Zentimeter / 425 Gramm
Betriebssystem	QNX Neutrino
Integrierter Datenspeicher	16 bis 64 GByte
Wireless-LAN / Bluetooth / UMTS / GPS	802.11n / 2.1 + EDR / nein / ja
USB	Micro-USB
VGA	Nein
HDMI	Micro-HDMI
Kartenleser	Nein
Einschub für SIM-Karte	Nein
Kamera	Ja, Rückseite, 5 Megapixel
Internetkamera	Ja, Vorderseite, 3 Megapixel
Dockinganschluss	1
Audioausgang	1
Mikrofon	Ja
Lagesensor / Lichtsensor	ja / ja
Spracheingabe / Flugzeugmodus	Nein / Nein
E-Mail-Zugang: POP3 / Imap / Exchange	Nein, nur BlackBerry Bridge

6 Windows Phone 7

Mit Windows Phone 7 wagt Microsoft einen kompletten Neuanfang, weil der Vorgänger Windows Mobile 6.5 der Konkurrenz von Apple und Google in jeder Hinsicht weit hinterher hinkte. Herausgekommen ist ein intuitiv zu bedienendes und flottes Betriebssystem für leistungsstarke Smartphones. Mit dem jüngsten Update unterstützt Windows Phone nun auch Multitasking, was das mobile Betriebssystem für den Unternehmenseinsatz interessant macht.

6.1 Windows Phone 7 im Unternehmenseinsatz

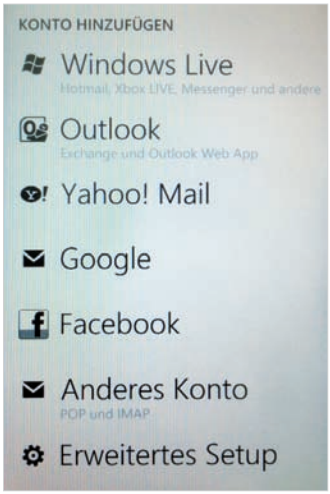
Zwar blicken die Marktforscher, was Microsofts Smartphone-OS betrifft, relativ optimistisch in die Zukunft, derzeit ist der Marktanteil von Windows Mobile und Windows Phone aber auch zusammengenommen alles andere als berauschend. Für Unternehmen, die auf stark Microsoft-geprägte Umgebungen setzen, hält das mobile Betriebssystem aber einige interessante Punkte bereit. Administratoren, die Smartphones mit SharePoint, Exchange und Office im engen Zusammenspiel betreiben wollen, sollten zumindest mal einen Blick auf Windows Phone 7 riskieren. Sowohl die Anbindung an Exchange oder SharePoint als auch das integrierte Office Mobile können Unternehmensanwendern durchaus Vorteile bieten – auch was den Einsatz von Office 365 im Unternehmen betrifft.

Das Erste, was Anwendern auffallen dürfte, ist, dass die Oberfläche in Windows Phone 7 komplett neu ist. Die Bedienung erfolgt generell über zwei Seiten. Auf der Startseite sehen Anwender die Kacheln, welche die verschiedenen Applikationen darstellen. Auf der zweiten Seite, die über einen kleinen Pfeil oder durch Weiterblättern erreichbar ist, sind die Einstellungen sowie weitere Programme abgelegt. Die Kacheln auf der Startseite zeigen verpasste Anrufe, SMS und E-Mails an. Per Drag&Drop lassen sich diese löschen und verschieben. Auf diese Weise kann jeder Anwender seine eigene Oberfläche relativ einfach erstellen.

6.1.1 Exchange mit Outlook Mobile

Die Anbindung an Exchange ist mittlerweile problemlos auch mit iPhones und Android-Geräten möglich, Windows Phone 7 bringt hier aber ein bisschen mehr mit. Vor allem wer mit ActiveSync-Richtlinien arbeitet, um Geräte optimal abzusichern, findet mit Windows Phone 7 bessere Möglichkeiten. Der Umgang mit Exchange-Postfächern und das produktive Arbeiten mit E-Mails über Exchange funktionieren in Windows Phone sehr intuitiv. Die Anbindung an Office 365 gelingt relativ schnell und einfach, genauso wie die Anbindung an lokale Server.

Bevor Sie aber eigene Exchange-Server anbinden, müssen Sie sicherstellen, dass das Zertifikat, das Sie auf dem Exchange-Server verwenden, von einer Zertifizierungsstelle ausgestellt wurde, der Windows Phone 7 vertraut. Ist das nicht der Fall, müssen Sie das Zertifikat der Zertifizierungsstelle im Smartphone installieren, ansonsten ist keine Anbindung möglich.



Wahlweise: Windows Phone lässt sich an verschiedene Postfächer anbinden.

Um ein Postfach anzubinden, starten Sie Outlook, klicken auf die drei Punkte am rechten Rand und dann auf *E-Mail-Konto hinzufügen*. E-Mail-Signaturen ändern Sie über *Einstellungen*; hier legen Sie auch fest, welche Objekte Sie synchronisieren wollen. Auf der zweiten Seite der Startoberfläche von Windows Phone 7 finden Sie den Menüpunkt *Einstellungen\E-Mail-konten & andere*. Über diesen Bereich können Sie Windows Phone 7 an verschiedene E-Mail-Systeme anbinden, unter anderem an Exchange und Office 365.

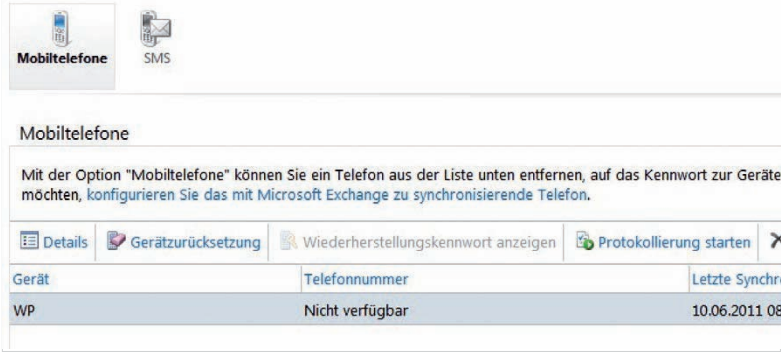
Bei der Neueinrichtung von Windows Phone 7 lässt sich das E-Mail-Setup direkt über eine Kachel auf der Startseite öffnen. Dank der einfachen Bedienung können auch Anwender eine Anbindung an das Exchange-System durchführen, es ist nicht zwingend ein Administrator notwendig. Nur wenn das Zertifikat nicht korrekt installiert ist, schlägt die Anbindung an Exchange fehl.

6.1.2 AutoDiscovery per Exchange und Fernlöschen

Windows Phone 7 unterstützt AutoDiscovery von Exchange Server 2007/2010. Das heißt, Anwender müssen nur ihre E-Mail-Adresse und das Kennwort des Kontos eingeben. Den Rest bezieht das Smartphone automatisch, wenn Sie AutoDisco-

very konfiguriert haben. Auch ohne AutoDiscovery ist eine Anbindung möglich. In diesem Fall erhält der Anwender eine Fehlermeldung bei der Anbindung und kann Domäne, Anmeldenamen und Server manuell eintragen. Diese Daten lassen sich jederzeit nachträglich in den Synchronisierungseinstellungen pflegen.

Sobald sich ein Gerät mit dem Server synchronisiert, ist es im Bereich Telefon in Outlook Web App (OWA) zu sehen. Das gilt ebenso für Office 365, wenn Anwender der Outlook Web App öffnen.



Outlook Web App: An dieser Stelle können Sie das Smartphone verwalten.

Sobald Sie an OWA angemeldet sind, rufen Sie über den Menüpunkt rechts oben die Einstellungen Ihres Postfachs auf. Sie erreichen die Verwaltung Ihres Telefons über *Telefon\Mobiltelefone\<Name des Gerätes>*. Über Wiederherstellungskennwort lassen Sie sich das Kennwort anzeigen, welches das Smartphone verlangt, wenn es aufgrund falscher Kennworteingaben gesperrt ist.

Diese Einstellungen lassen sich über ActiveSync-Richtlinien festlegen. Sie sehen alle mobilen Geräte, die sich per Exchange ActiveSync mit dem Postfach synchronisieren. Für die einzelnen Telefone können Sie sich auch die Details anzeigen lassen und sehen, ob Richtlinien angewendet wurden beziehungsweise wann der letzte Synchronisierungsvorgang stattgefunden hat.

Über die Schaltfläche *Geräterücksetzung* löschen Sie das Smartphone, sobald es sich das nächste Mal mit dem Exchange-Server verbindet. Auch Administratoren können einen solchen Löschvorgang starten, indem sie über das Kontextmenü des Benutzerpostfachs in der Exchange-Verwaltungskonsole die Option *Mobiltelefone verwalten* aufrufen. Beim Löschen entfernt Windows Phone 7 alle Daten vom Gerät und setzt es auf den Werkszustand zurück. Das Gerät lässt sich weiterhin verwenden, hat aber keinerlei Daten mehr. Soll es erneut mit dem Server verbunden werden, müssen Sie es aus der Liste der Telefone löschen. Erst dann lässt es sich neu synchronisieren. Ansonsten führt Windows Phone 7 bei jedem neuen Synchronisierungsvorgang eine Löschung durch.

6.1.3 Termine und E-Mail verwalten

Anwender, die viel unterwegs sind, können Termine relativ einfach in Windows Phone 7 verwalten, ändern und auch Terminüberschneidungen auflösen sowie auf Besprechungsanfragen antworten. Hier bietet Windows Phone 7 nahezu die gleichen Möglichkeiten wie ein normales Outlook.

iPhones können zwar auch problemlos Termine aus Exchange abrufen, diese aber nicht bearbeiten und schon gar nicht Terminüberschneidungen auflösen. Wie bei Outlook, erscheinen Besprechungsanfragen auch in Windows Phone 7 im Kalender als solche; sie lassen sich einfach beantworten und bearbeiten.

Zwiespalt: Outlook Mobile erkennt Planungskonflikte und kann diese lösen.

Wie in Outlook, können Sie auch in Windows Phone 7 für Besprechungsanfragen andere Termine vorschlagen. Diese Anfragen zeigt das Smartphone bereits als vorläufig im Kalender an. Erhalten Anwender mehrere Besprechungsanfragen, die sich gegenseitig blockieren, oder ist bereits ein Termin im Kalender eingetragen, der sich mit Anfragen überschneidet, erscheint direkt in der Anfrage der E-Mail eine Information über den Konflikt. Auf diese Weise können Anwender den Konflikt lösen und bei Besprechungsanfragen andere Termine vorschlagen.

6.1.4 Exchange-Konten

Windows Phone 7 ermöglicht das Anbinden mehrerer Exchange-Konten, die sich über Exchange ActiveSync synchronisieren. Die Kontakte der verschiedenen Konten kann Windows Phone 7 zusammenfassen und gemeinsam bei den Kontakten anzeigen. Diese stehen über eine eigene Kachel zur Verfügung. Außerdem können Sie mehrere Kalender synchronisieren. Die Termine zeigt Windows Phone 7 im Telefonkalender an; jeder synchronisierte Kalender erhält eine eigene Farbe.

Besprechungsanfragen lassen sich genauso verwenden wie in der Desktop-Version von Outlook. Im Kalender können mit wenigen Klicks alle Teilnehmer einer Besprechung oder nur der Organisator per E-Mail darüber informiert werden, dass Sie zu spät kommen. Dazu steht in den Optionen des Termins im unteren Bereich eine eigene Schaltfläche zur Verfügung. Windows Phone 7 lässt sich mit Exchange Server 2003/2007/2010 synchronisieren und unterstützt sämtliche Möglichkeiten der Exchange-ActiveSync-Richtlinien der Serverversion. Optimal arbeitet Win-

dows Phone 7 mit Exchange Server 2010 und Office 365 zusammen, vor allem was die Auflösung von Empfängerdaten in der globalen Adressliste betrifft. Ein weiterer Vorteil beispielsweise gegenüber aktuellen iPhones ist, dass Windows Phone 7 anstehende Termine direkt auf dem Startbildschirm anzeigt. Es ist nicht notwendig, dass Anwender erst den Kalender öffnen müssen.

6.1.5 Office Mobile und SharePoint

Neben Outlook Mobile sind in Windows 7 auch die anderen Office-Programme als Mobile-Versionen integriert. Sie können Tabellen mit Mobile Excel, Dokumente mit Mobile Word, Notizen mit Mobile OneNote und Präsentationen mit Mobile PowerPoint anzeigen und bearbeiten. OneNote kann Notizbücher über Windows Live Sky Drive im Internet speichern oder mit SharePoint 2010 synchronisieren. Word-Dokumente lassen sich mobil erstellen, bearbeiten und formatieren. Die Formatierungen bleiben erhalten, wenn Sie die Daten im Netzwerk speichern. Office-Dokumente kann man direkt aus E-Mails oder aus anderen Netzwerkspeichern öffnen und auf diese Weise auch speichern.

Komplett: Neben Outlook Mobile sind in Windows 7 auch die anderen Office-Programme als Mobile-Versionen integriert.

Die gleiche Unterstützung bieten Excel und PowerPoint. Präsentationen lassen sich in Mobile PowerPoint anzeigen und bearbeiten. Excel-Tabellen sind zwischen der richtigen Excel-Version und Mobile Excel ebenfalls vollkommen kompatibel.

Ebenfalls möglich ist die direkte Anbindung an SharePoint. Dazu müssen Anwender einfach die URL des SharePoint-Servers in Office Mobile eintragen und können sich mit dem Server verbinden. Auf diese Weise lassen sich Dokumente in Bibliotheken genauso leicht öffnen wie Listen bearbeiten. Durch die Integration von SharePoint Workspace können Anwender Dokumente auf das Smartphone herunterladen und bearbeiten. Auch eine direkte Synchronisierung mit SharePoint

zum Speichern der Dokumente ist möglich. Neben lokal betriebenen Exchange-Servern können Sie in SharePoint Workspace auch problemlos Office 365 anbinden. Die kostenlose Version SharePoint 2010 Foundation funktioniert ebenfalls zusammen mit Windows Phone 7.

6.1.6 Internet Explorer Mobile

Der integrierte Internet Explorer Mobile identifiziert sich als mobiler Browser, sodass Sie Webseiten im Unternehmen speziell auf die Bedürfnisse mobiler Anwender auslegen können. Der User Agent String des Browsers ist:

```
Mozilla/4.0 (compatible; MSIE 7.0; Windows Phone
➥ OS 7.0; Trident/3.1; IEMobile/7.0; <Hersteller des
➥ Gerätes>;<Gerätemodell>)
```

Windows-Phone-7-Geräte verfügen über einen Zurück-Button, der konsistent auch im Internet Explorer Mobile funktioniert. Ebenfalls möglich ist Registerbrowsen. Leider basiert Internet Explorer Mobile noch auf den alten Desktop-Versionen des Internet Explorer, doch dafür verfügt er über Microsoft Jscript-Funktionen und .xhtml-Unterstützung. Die Schriftartgröße in Webseiten können Entwickler für Windows-Phone-7-Benutzer optimieren. Dabei hilft die CSS-Eigenschaft *-ms-text-size-adjust*. Durch die Integration von Microsoft Silverlight können Business-Anwendungen problemlos Daten zwischen Windows-Phone-7-Geräten und Servern austauschen. Mit Silverlight können Unternehmen eigene Business-Anwendungen entwickeln, die auf den Smartphones laufen. Microsoft stellt für iOS-App-Entwickler das API Mapping Tool zur Verfügung. Mit ihm lassen sich Anwendungen von iOS zu Windows Phone 7 portieren. Die Aufgabe des Tools ist den Entwicklern zu zeigen, welche Funktionen kompatibel sind.

6.1.7 Fazit

Ein wirkliches Enterprise-Smartphone-OS wie das BlackBerry-Betriebssystem oder Windows Mobile ist Windows Phone nicht – will es wohl aber auch nicht sein. Unternehmen, die intensiv mit Microsoft-Lösungen arbeiten, insbesondere mit Exchange Server 2010, SharePoint 2010, Office 2010 oder auch Office 365, sollten sich Windows Phone 7 zumindest mal ansehen. Wenn mobile Anwender Besprechungsanfragen effizient beantworten und Termine verwalten wollen, kann Windows Phone 7 punkten.

Zwar lässt sich all das auch mehr oder minder mit iOS- und Android-Geräten lösen, dazu sind allerdings meist zusätzliche Apps erforderlich. In Windows Phone kann dies mit Bordmitteln realisiert werden. Apropos Apps: Zweifelsohne kann hier das Microsoft-OS nicht mit den Wetbewerbern konkurrieren.

Thomas Joos

6.2 Ratgeber: Windows Phone 7 für Admins

Administratoren, die entweder Windows Phone 7 verwalten müssen oder selbst einsetzen, werden schnell feststellen, dass die neue Mobile-Generation von Microsoft sehr endkundenorientiert ist und sich stark von den Vorgängerversionen unterscheidet. Windows Mobile 6.5 war noch anzumerken, dass eher Unternehmenskunden im Fokus standen, während Windows Phone 7 eindeutig zentral zunächst auf Privatanwender oder zumindest privat orientierte Anwender setzt.

Zwar ist die Anbindung an Exchange und SharePoint direkt integriert, und auch Exchange-ActiveSync-Richtlinien lassen sich umsetzen, allerdings ist generell der Unternehmenseinsatz von Windows Phone 7 für Administratoren eine komplexe Angelegenheit, da Microsoft im neuen System viele wichtigen Funktionen für Unternehmenskunden schlicht weggelassen hat.

Das fällt sofort auf, wenn Sie ein Windows-Phone-7-Gerät mit Windows 7 verbinden. Hier unterstützt das Gerät nicht das Synchronisierungscenter, sondern Sie müssen die Zune-Software installieren. Über die Software verwalten Sie die Musiktitel auf dem Gerät, ebenso die installierten Anwendungen. Die Telefone sind auch nicht als USB-Speicher sichtbar, sodass keine Daten mit dem Gerät synchronisiert werden können. Nur wenn Sie die Consumer-Software Zune nutzen, lassen sich Daten synchronisieren – und dann auch nur unvollständig.

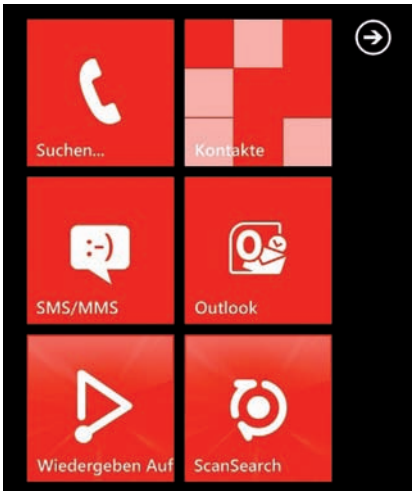
6.2.1 Oberflächliches

Das Erste, was Administratoren auffallen wird, die Windows Phone 7 verwalten, ist die komplett veränderte Oberfläche, die Microsoft stark abgespeckt hat. Im Gegensatz zu Android-Geräten, die sich in der Bedienung ganz ähnlich wie Apples iPhone präsentieren, glänzt Windows Phone 7 über eine neu entwickelte Oberfläche mit der Bezeichnung Metro.

Diese Technologie übernimmt Microsoft mittlerweile auch für seine Webseiten, und in Windows 8 soll Metro ebenfalls integriert sein und eine vereinfachte Bedienung ermöglichen. Viele Anwender kommen mit der Oberfläche schnell zurecht, da die Bedienung sehr intuitiv ist. Nutzer, die von Windows Mobile 6/6.1 oder 6.5 kommen, werden sich grundlegend umstellen müssen.

Der Homescreen von Windows Phone 7 zeigt die wichtigsten Programme als Kacheln an, und Anwender können den Bildschirm anpassen und zusätzliche Programme integrieren. Leider bietet Windows Phone 7 hier nicht genügend Möglichkeiten, die Benutzeroberfläche besser an die eigenen Wünsche anzupassen. Die 2-D-Animationen wirken in der ersten Version von Metro noch nicht so richtig ausgereift und flüssig. Pinnen Anwender mehr Programme, Kontakte oder Webseiten direkt an den Homescreen, muss man ordentlich scrollen, da eine bessere Anpassung fehlt. Beispielsweise lassen sich maximal zwei Kacheln nebeneinander anordnen, dies nutzt den Raum nicht gerade ideal aus. Hier wäre es besser, wenn

die Möglichkeit bestünde, die Größe der Kacheln anzupassen und damit mehr Programme zu integrieren oder einzelne Programme besser hervorzuheben.



Einfach anders: Die Oberfläche von Windows Phone 7 ist in Kacheln organisiert.

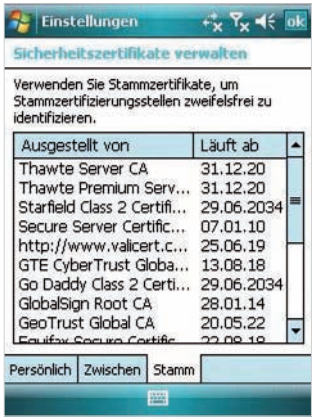
Vor allem Administratoren, die noch zusätzliche Apps installieren müssen, zum Beispiel für die Netzwerkverwaltung oder -tests, würden so einiges an Zeit sparen. Leider lassen sich die Farben einzelner Kacheln nicht anpassen, um zum Beispiel spezielle Anwendungen wie E-Mail oder SharePoint-Zugriff herauszustellen. Windows Phone 7 bietet nur die Möglichkeit, die Farben aller Kacheln über das entsprechende Theme zu ändern.

6.2.2 Synchronisation und Zertifikate

Dass es nicht möglich ist, Daten mit lokalen Rechnern auszutauschen, fällt schnell auf. ActiveSync gibt es nicht mehr, und auch die Verwaltung der Zertifikate auf dem System hat Microsoft stark eingedampft. Zwar lassen sich Zertifikate weiterhin installieren, aber nicht über ActiveSync übertragen oder zentral verwalten wie mit Windows Mobile 6.

In Vorgängerversionen von Windows Phone 7 hat Microsoft noch eine Konsole im Gerät unterstützt, über die sich Zertifikate verwalten lassen. Diese Konsole fehlt in Windows Phone 7. Daher können Zertifikate nur noch installiert werden, nicht mehr verwaltet. Die Installation muss über den Zugriff auf eine Webseite, eine Dateianlage per E-Mail oder einen Internetspeicher erfolgen (siehe auch Windows-Phone-7-Praxis: Exchange-Anbindung und Zertifikate, Webcode **2036585**). Ein Austausch des Zertifikats über eine SD-Karte oder ActiveSync ist nicht möglich.

Vergangenheit: Windows Mobile konnte noch mit Zertifikaten umgehen.



Die Synchronisierung mit dem lokalen Outlook ist nicht integriert. Anwender müssen einen Abgleich über das Internet durchführen, lokal ist das nicht möglich.

Zusammenspiel: Über Zune kann man etwa Mediendateien mit dem Smartphone synchronisieren.

Nicht einmal das Synchronisierungscenter in Windows 7 lässt sich nutzen, um Daten eines PCs auf Windows Phone 7 zu übertragen. Durch die Installation der Zune-Software auf einem Computer können Anwender aber Bilder, Musik und Videos synchronisieren und auf dem lokalen Speicher des Gerätes ablegen. Andere Dateien, Office-Dokumente oder Termine und Kontakte mit Outlook lassen sich dagegen nicht synchronisieren. Das ist für Unternehmenskunden sehr ineffizient.

6.2.3 Dateizugriff und Verschlüsselung

Viele Technologien in Windows Phone 7 sind optional, das heißt, es bleibt dem entsprechenden Gerätehersteller überlassen, ob er die entsprechende Technologie in seine Geräte einbaut. Zu den optionalen Funktionen gehören Wi-Fi (802.11g und 802.11n), Bluetooth, erweiterbarer Speicher und eine Hardwaretastatur. Setzen Unternehmen daher nicht zentral auf ein einzelnes Gerät, müssen sich Administratoren auf die Verwaltung einer Vielzahl von Geräten einstellen. Grundsätzlich unterstützt Windows Phone 7 MicroSD-Karten, allerdings lassen sich diese nicht austauschen. Eine Vergrößerung des Datenspeichers ist nicht möglich.

Ebenfalls problematisch ist der fehlende Datei-Explorer. Mit diesem konnten Anwender und Administratoren bis Windows Mobile 6.5 noch auf das Dateisystem des Smartphones zugreifen und Dateien verwalten. Diese Konsole gibt es nicht mehr, und auch der Zugriff auf das Dateisystem von Smartphones ist nicht mehr möglich. Leider ist es mit Windows Phone 7 auch nicht ohne Weiteres möglich, Screenshots für Anleitungen zu erstellen. Was in iPhones standardmäßig integriert und in Android-Geräten nachgerüstet werden kann, fehlt schlicht und ergreifend in Windows Phone 7. Dies lässt sich lediglich über nicht offizielle Funktionen bewerkstelligen, siehe auch Workshop – Versteckte Windows-Phone-7-Funktionen aktivieren (Webcode **2036340**).

Daten lassen sich in Windows Phone 7 nicht verschlüsseln. Das heißt, wenn Sie wichtige Daten auf dem System speichern, was vor allem bei Administratoren sehr oft der Fall ist, müssen Sie aufpassen, dass kein Unbefugter Zugriff auf das Gerät erhält. In der aktuellen Version werden keinerlei Daten in Windows Phone 7 unterstützt. Auch zusätzliche Apps die diese Funktion übernehmen, gibt es aktuell nicht. Unternehmen, die sichere Umgebungen einsetzen, sollten daher zunächst auf andere Systeme setzen.

Die aktuelle Version von Windows Phone 7 ist nicht Multitasking-fähig. Erst mit dem Mango-Update, das Microsoft Ende des Jahres veröffentlicht, integriert Microsoft diese Möglichkeit in Windows Phone. Aktuell basiert der Internet Explorer Mobile in Windows Phone 7 noch auf dem langsamen Internet Explorer 7. Erst mit dem Mango-Update erhält das System den neuen Browser Internet Explorer 9 inklusive einer Hardwarebeschleunigung.

6.2.4 Fehlende Exchange-ActiveSync-Richtlinien

Zwar können mit Windows Phone 7 problemlos Exchange ActiveSync-Richtlinien umgesetzt werden, aber es sind nicht alle Möglichkeiten von Exchange integriert. Im Gegensatz zu Android-Geräten lassen sich bei iPhones und Windows-Phone 7-Geräten die Richtlinien nicht aushebeln, dafür aber auch nicht alle Einstellungen setzen. Windows Phone 7 unterstützt die Exchange-ActiveSync-Richtlinien von Exchange Server 2003 SP2/2007/2010.

Folgende Einstellungen sind per Richtlinie auf die Geräte übertragbar:

- Password Required
- Minimum Password Length
- Idle Timeout Frequency Value
- Device Wipe Threshold
- Allow Simple Password
- Password Expiration
- Password History

Andere Richtlinien, die Exchange-Server unterstützt, geben bei Windows Phone 7 immer den Wert True zurück:

- Disable Removable Storage
- Disable IrDA
- Disable Desktop Sync
- Block Remote Desktop
- Block Internet Sharing

Alle anderen Einstellungen, die Exchange unterstützt, geben den Wert False zurück. In einem TechNet-Artikel (http://social.technet.microsoft.com/wiki/contents/articles/exchange-activesync-considerations-when-using-windows-phone-7-clients.aspx) erhalten Sie mehr Informationen zu diesem Thema.

6.2.5 Mehrere E-Mail-Konten – Vor- und Nachteile

Alle E-Mail-Konten erhalten eine eigene Kachel und eine eigene Oberfläche im Homescreen. Zwar lassen sich in Windows Phone 7 auch mehrere Exchange-Konten anbinden, allerdings ist die Verwaltung der Konten beispielsweise in iPhones besser gelöst. Im Gegensatz zu Apple bietet Microsoft nicht die Möglichkeit, alle eingehenden E-Mails auf Wunsch in einer gemeinsamen Oberfläche anzuzeigen.

Will ein Anwender alle seine E-Mails bearbeiten, muss er nach und nach die verschiedenen Posteingänge öffnen, eine zentrale Verwaltung der E-Mails fehlt. Das ist auf der einen Seite vor allem für Nutzer problematisch, die mehr als zwei Konten verwalten müssen, da hier ein ständiger Wechsel notwendig ist. Auf der anderen Seite sind in Windows Phone 7 vor allem Besprechungsanfragen wesentlich effizienter zu verwalten, da die Exchange-Anbindung konsistenter gelöst ist. Anwender können Besprechungsanfragen beantworten, Termine ändern und auf Wunsch die Besprechungsteilnehmer bei Verspätungen mit einem Klick informieren. Diese erweiterten Möglichkeiten sind in anderen Geräten nicht integriert.

6.2.6 Tethering und Aktualisierung

Tethering bezeichnet eine Funktion, die es ermöglicht, andere Geräte mit dem Smartphone zu verbinden, zum Beispiel andere Telefone oder Notebooks. Mit dieser Technologie kann zum Beispiel mit einem Notebook oder Tablet die Internetverbindung von Android-Geräten oder iPhones genutzt werden – damit werden diese Geräte zu kostenlosen UMTS-Modems. Leider ist diese Möglichkeit in Windows Phone 7 nicht integriert. Hier muss Microsoft nacharbeiten, denn für Unternehmensanwender ist eine solche Technologie nahezu unverzichtbar.

Für den Betrieb von Windows Phone 7 ist Zune auf dem Rechner nicht notwendig, die Anbindung an Exchange und SharePoint funktioniert auch so. Wollen Sie allerdings Anwendungen bequem installieren oder das Telefon aktualisieren, ist der beste Weg der über Zune. Sobald Sie das Gerät mit dem Computer verbinden und Zune installiert haben, überprüft die Software, ob eine Aktualisierung für das Telefon verfügbar ist. Anschließend lädt Zune die notwendigen Daten herunter und installiert diese auf dem Telefon. Der Vorteil bei der Verwendung der Zune-Technologie ist, dass auch Anwender schnell und einfach Updates auf dem Gerät installieren können. Über Zune lassen sich auch Anwendungen auf Windows-Phone-7-Geräten installieren und verwalten.

6.2.7 Apps für Administratoren

Über Windows-Phone-7-Geräte selbst oder über die Zune-Software lassen sich Apps auf den Geräten installieren. Zwar gibt es für Windows Phone 7 weit weniger Anwendungen als für Android oder iPhones, aber im Marketplace finden Sie einige interessante Tools.

Praktisch: Mit den Network-Tools können Sie unter Windows Phone 7 Webseiten testen.

Ein Beispiel sind die Network-Tools. Diese können Sie entweder eine Weile testen oder für 4,49 Euro kaufen. Die Tools enthalten Möglichkeiten zum Pingen von Rechnern im Netzwerk, zum Testen von Ports, einen HTTP(S)-Test und zum Testen von Webseiten und deren Verfügbarkeit.

Die App bietet den Windows-Phone-7-typischen Navigationsbereich, und die einzelnen Funktionen sind schnell erreichbar und leicht verständlich.

Administratoren, die unterwegs über den Remote-Desktop auf Server oder PCs eine Fernwartung starten wollen, finden mit der Anwendung Remote Desktop von Topperware im Marketplace einen passenden Client dazu. Die Anwendung ist für 11,49 Euro zu haben, und die Bedienung ist recht einfach. Die Anwendung speichert bereits aufgebaut Verbindungen, sodass sich diese schnell und einfach wieder öffnen lassen. Die Testversion bricht die Verbindung nach 60 Sekunden ab, bei der gekauften Version sind die Verbindungen unbegrenzt. Aktuell können Sie mit solchen Tools aber keine lokalen IP-Adressen verwenden. Hier verspricht erst das Mango-Update von Windows Phone 7 Abhilfe. In der aktuellen Version routet die Anwendung den Datenverkehr über einen Server beim Anbieter, der den Datenverkehr dann wiederum zum entsprechenden lokalen Server weiterleitet. Der lokale Server muss dazu im Internet verfügbar sein. Ist das nicht der Fall, können Sie die App nicht nutzen.

6.2.8 Fazit

Windows Phone 7 bietet einige Vorteile im Vergleich zur direkten Konkurrenz iPhone und Android, allerdings auch ein paar Einschränkungen. Die direkte Anbindung an Exchange und SharePoint ist mit Windows Phone 7 wesentlich besser möglich als mit anderen Systemen. Vor allem Besprechungsanfragen, Office-Dokumente und der Zugriff auf SharePoint-Bibliotheken funktionieren bereits mit Bordmitteln problemlos.

Negativ fallen Funktionen auf, die Unternehmenskunden einfach benötigen, sei es eine zentrale Verwaltung und Steuerung von Zertifikaten, eine effiziente Anpassung der Oberfläche, Umsetzung der Richtlinien, Zugriff auf das lokale Netzwerk, eine Verschlüsselung und vieles mehr. Sie sollten Windows Phone 7 ausgiebig in Ihrer Umgebung testen, um zu überprüfen, ob Sie Ihre Anforderungen damit erfüllen können.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

6.3 Praxis: Office Mobile in Windows Phone 7 nutzen

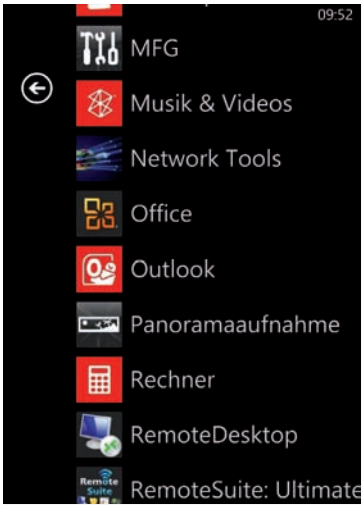
Zweifellos fehlen Windows Phone 7 einige elementare Eigenschaften zu einem vollständigen Smartphone-Betriebssystem für den Einsatz in Unternehmensumgebungen. Das integrierte Office Mobile hat aber für Anwender, die es mobil mit Office-Dokumenten zu tun haben, erhebliche Vorteile. Insbesondere im Vergleich zu den anderen Smartphone-Plattformen und deren diesbezüglichen Möglichkeiten bietet Windows Phone 7 hier mehr.

Mit Office Mobile lassen sich Dokumente nicht nur betrachten, sondern ebenso bearbeiten und anlegen. Neben den Mobile-Versionen von Word, Excel und PowerPoint können Windows-Phone-7-Geräte direkt mit SharePoint verbunden werden, auch über das Internet.

Office Mobile sowie der SharePoint-Zugriff sind direkt in das Betriebssystem integriert. Es ist nicht notwendig, etwas zu installieren oder tiefer gehend anzupassen. Sollen Dokumente in SharePoint gespeichert werden, müssen Sie nur die URL und die Authentifizierungsdaten für die Seite eingeben. Anschließend lassen sich Dokumente auch schnell und einfach in SharePoint speichern.

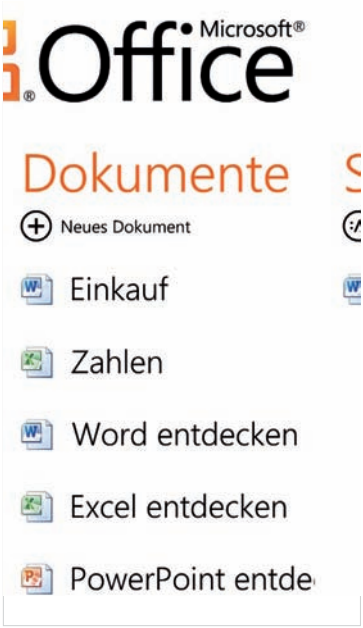
6.3.1 Dokumente mit Windows Phone 7 öffnen und erstellen

Neben der reinen Möglichkeit, Dokumente auf das Windows-Phone-7-Gerät herunterzuladen, können Sie auch Dokumente über die Office-Funktion anlegen.



Alles auf Anfang: Der Office-Hub ist der Einstiegspunkt zu Ihren Office-Dokumenten.

Um ein neues Dokument zu erstellen, öffnen Sie die Office-Programmgruppe, auch Office Hub genannt, auf der Anwendungsseite des Gerätes. Dieser Bereich ist immer der Einstiegspunkt für Office-Dokumente, die Sie in Windows Phone 7 nutzen wollen. Die Anbindung an SharePoint über SharePoint Workspace Mobile erfolgt gleichfalls in diesem Bereich. Wechseln Sie auf die Seite *Dokumente* und klicken auf *Neues Dokument*. Speichern Sie nach der Bearbeitung ein Dokument ab, erscheint es in diesem Bereich wie die Office-Mobile-Verknüpfungen. Auf diesem Weg können Sie das Dokument schnell und einfach wieder öffnen.



Neues Dokument anlegen: Über den gleichnamigen Punkt können Sie neue Word- oder Excel-Dateien anlegen.

Wollen Sie häufiger mit Office Mobile arbeiten, können Sie die Office-Verknüpfung direkt auf der Startseite von Windows Phone platzieren. Dazu klicken Sie auf der Seite der Anwendungen auf *Office* und halten die Verknüpfung fest. Wählen Sie aus dem erscheinenden Menü die Option *Auf Startseite* aus.

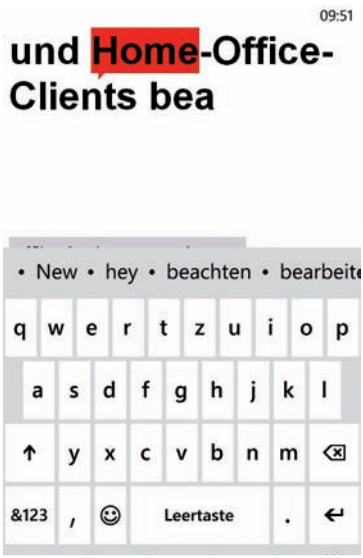
Haben Sie sich für ein neues Dokument entschieden, können Sie auswählen, ob Sie ein neues Word-Dokument oder eine neue Excel-Tabelle erstellen wollen. Sie können zwar in Windows Phone 7 Dokumente öffnen und bearbeiten, die in SharePoint-Bibliotheken gespeichert sind, und die Änderungen auch wieder direkt in die SharePoint-Bibliothek speichern. Sie haben aber keine Möglichkeit, ein neues Dokument in Office Mobile zu erstellen und zu einer SharePoint-Bibliothek hochzuladen. Dokumente müssen bereits in SharePoint vorhanden sein.

Typenwahl: Hier müssen Sie sich für den Dokumenttyp entscheiden.

Um Dokumente aus anderen Quellen in Windows Phone 7 zur Verfügung zu stellen, müssen Sie diese entweder per E-Mail versenden, die Sie mit Windows Phone 7 abrufen, oder Sie verwenden eine Verbindung mit Windows Live SkyDrive. Zum Herunterladen nutzen Sie dann den Internet Explorer Mobile, eine Synchronisierung mit Windows Live SkyDrive über den Office-Hub funktioniert nur mit OneNote. Eine direkte Übertragung von Office-Dokumenten über WLAN, USB oder Bluetooth ist in Windows Phone 7 nicht möglich.

6.3.2 Word-Dokumente bearbeiten

Wenn Sie beispielsweise ein neues Word-Dokument erstellen, beginnen Sie auf dem nächsten Fenster mit der Bearbeitung. Um ein geöffnetes Dokument zu bearbeiten, klicken Sie auf den kleinen Stift in der unteren Symbolleiste. Das funktioniert entsprechend in allen Programmen in Office Mobile.



Editieren: Dokumente können Sie mit Office Mobile auch bearbeiten.

Falls Sie Dokumente öffnen, die Formatierungen enthalten, die von Word Mobile nicht unterstützt werden, zeigt Word Mobile diese einfach nicht an. Das Dokument an sich lässt sich aber problemlos öffnen. Sie können im unteren Bereich über die Icons auch Formatierungen einfügen wie zum Beispiel Schriftgröße, Schriftformatierung oder Farbe. Folgende Formatierungen stehen zur Auswahl: Fett, Kursiv, Unterstrichen, Durchgestrichen, Vergrößern und Verkleinern.

Optik: Es sind begrenzte Formatierungsmöglichkeiten vorhanden.

Wollen Sie die Ansicht des Dokumentes vergrößern, können Sie mit den Fingern diese größer und kleiner ziehen, wie bei anderen Smartphone-Systemen auch. Geben Sie ein Wort ein, schlägt Word Mobile eine Vervollständigung auf. Tippen Sie diese an, übernimmt Word das vorgeschlagene Wort in das Dokument. Klicken Sie auf die drei Punkte in der unteren Symbolleiste, erscheint ein Menü, über das Sie das Dokument speichern oder Änderungen rückgängig machen. Auf diesem Weg nehmen Sie auch Formatierungen wieder zurück. Diese drei Punkte erscheinen an vielen Stellen in Office Mobile und ermöglichen erweiterte Funktionen.

Kommentare und Gliederungen in Word-Dokumenten

Besonders praktisch ist die Möglichkeit, in fertige Dokumente Kommentare einzufügen. Da Windows Phone 7 diese direkt in die Worddatei (.docx) einbindet, sind die Kommentare auch im normalen Word auf dem PC ersichtlich sowie in den SharePoint-Bibliotheken gespeichert. Das ermöglicht das Lesen und Korrigieren von Dokumenten von unterwegs. Andere Anwender im Unternehmen können das entsprechende Dokument dann öffnen und sehen den Kommentar so, als ob er in einem normalen Word erstellt wurde.

Die Bearbeitung von Dokumenten lässt sich abbrechen, und Sie können die vorgenommenen Änderungen einfach auf dem Gerät speichern. Sobald Sie das Dokument verlassen, fragt Sie Windows Phone 7, ob Sie speichern wollen. Anschließend ist das entsprechende Dokument direkt im Office-Hub verfügbar und lässt sich auf diesem Weg auch wieder öffnen. Sie können alternativ über das Menü im un-

teren Bereich, das Sie über die drei Punkte erreichen, ein Dokument speichern. Enthält ein Dokument eine Gliederung, können Sie durch Anklicken des Gliederungssymbols im unteren Bereich diese Gliederung anzeigen und durch Antippen des entsprechenden Bereiches direkt an die gewünschte Stelle im Dokument wechseln. Windows Phone 7 bietet die Möglichkeit, direkt in den Dokumenten zu suchen. Dazu klicken Sie einfach auf die Lupe im unteren Bereich und geben den gewünschten Suchbegriff ein. Mit der Weiter-Taste können Sie zwischen den gefundenen Ergebnissen wechseln.

6.3.3 Excel und Office Mobile

Excel-Tabellen erstellen Sie auf dem entsprechenden Weg wie Word-Dokumente über den Office-Hub auf der Seite der Anwendungen. Sie wählen zur Erstellung *Excel-Arbeitsmappe* aus. Anschließend können Sie die Arbeitsmappe bearbeiten. Klicken Sie im unteren Bereich auf die drei Punkte, öffnet sich ein Menü, das erweiterte Möglichkeiten bietet.

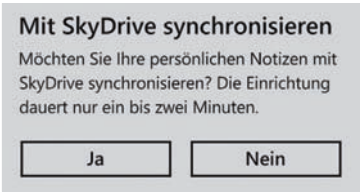
Zellstruktur: Sie können auch Excel-Tabellen in Office Mobile bearbeiten.

Excel Mobile unterstützt selbstredend nicht alle Funktionen der Office-Version von PCs. In entsprechenden Fällen zeigt Excel Mobile die jeweiligen Werte in den Zellen zwar an, lässt aber keine Änderung dieser Daten zu. Achten Sie daher beim Speichern von Änderungen darauf, nicht das Quelldokument zu überschreiben. Es kann sonst passieren, dass beim Speichern nicht unterstützte Daten und Formatierungen verloren gehen. Wie in Word, gibt es auch in Excel Mobile eine Gliederungsansicht. Mit dieser können Sie zwischen Arbeitsmappen und Diagrammen wechseln. Auch Kommentare lassen sich auf diesem Weg einfügen. Die generelle Bedienung ist in allen Programmen von Office Mobile nahezu identisch.

6.3.4 OneNote, Windows SkyDrive und PowerPoint

Neben Word und Excel können Sie in Windows Phone 7 auch Notizen mit OneNote erstellen und ebenso PowerPoint-Präsentationen nachträglich bearbeiten, ändern und Kommentare hinzufügen. Die Bedienung von PowerPoint entspricht der Bedienung anderer Office-Mobile-Programme. Sie haben die Möglichkeit, Präsentationen in Windows Phone 7 bearbeiten, nicht nur anzuzeigen. Die OneNote-Notizbücher können Sie wiederum mit OneNote synchronisieren und in Windows Live SkyDrive speichern. Synchronisieren Sie ein lokal installiertes OneNote mit SkyDrive, können Sie auf diesem Weg lokal und mobil mit den gleichen Notizen arbeiten. Hier lassen sich Notizbücher auch mit Office Web Apps bearbeiten und sind überall verfügbar. Sie können allerdings nur OneNote-Notizbücher mit Windows Live SkyDrive synchronisieren, keine anderen Dokumente.

SkyDrive: Sie können die Synchronisierung mit Windows Live SkyDrive konfigurieren.



Neben Notizen lassen sich mit OneNote auf dem Windows Phone 7 auch Sprach-Memos anfertigen. Bilder kann man als Notizen hinterlegen. Notizen erscheinen als Kacheln direkt im Office-Hub auf der OneNote-Seite. Jede Notiz kann Texte, Bilder und Sprach-Memos enthalten.

Achtung Aufnahme: Sie können in Office Mobile Sprachnotizen erstellen.

Klicken Sie in OneNote auf Alle, sehen Sie alle Notizen. Außerdem können Sie an dieser Stelle über die Synchronisierungsschaltfläche im unteren Bereich die Synchronisierung mit Windows SkyDrive konfigurieren und Synchronisierungen durchführen, wenn Sie ein kostenloses Konto eingerichtet haben. Diese Möglichkeit haben Sie nur mit OneNote in Office Mobile.

Ändern Sie den Namen der Einstellungen in OneNote und SkyDrive nicht ab, da ansonsten die Synchronisierung nicht korrekt funktioniert. Geöffnete Notizen können Sie bearbeiten und über die Bearbeitungsschaltflächen im unteren Bereich formatieren oder per E-Mail versenden.

Halten Sie eine Notiz gedrückt, können Sie diese direkt auf der Startseite von Windows Phone 7 verknüpfen. Neben der möglichen Synchronisierung mit SkyDrive können Notizbücher mit Notizen in SharePoint synchronisiert werden. Dazu verwenden Sie SharePoint Workspace Mobile.

6.3.5 Dokumente speichern – SharePoint Workspace Mobile

Der Austausch von Dokumenten ist über das Senden per E-Mail oder das Speichern in SharePoint möglich. Die Anbindung an SharePoint erfolgt über WLAN. SharePoint Workspace Mobile ist direkt in Windows Phone 7 integriert, Sie müssen keine App herunterladen und nichts lizenzieren. Sobald das Smartphone im WLAN angebunden ist, können Sie über SharePoint Workspace Mobile auf SharePoint zugreifen.

Zugriff: Über SharePoint Workspace Mobile können Sie auf SharePoint zugreifen.

Der Zugriff auf die Dokumente kann dann auch durch Office Web Apps erfolgen, also ebenfalls wieder online oder über SharePoint, wenn Sie Office Web Apps in Ihrer SharePoint-Farm installiert haben.

Um SharePoint und die integrierten Bibliotheken anzubinden, klicken Sie im Office-Hub auf der Seite *SharePoint* auf *URL öffnen*. Auf dieser Seite zeigt SharePoint Workspace Mobile auch Dokumente an, die Sie bereits über SharePoint geöffnet haben. Sie müssen diese Dokumente nur anklicken, um sie zu öffnen. Die Dokumente stehen ebenso offline zur Verfügung. Um eine SharePoint-Seite zu öffnen, geben Sie auf der Seite *URL öffnen* einfach die Adresse ein. Anschließend bindet Windows Phone 7 sie an. Sind für die Seite noch Authentifizierungsdaten notwendig, erscheint ein Fenster, in dem Sie den Benutzernamen, die Domäne und das Kennwort eingeben müssen, mit dem Sie sich an SharePoint anbinden wollen. Nach der erfolgreichen Authentifizierung öffnet sich die Anzeige der SharePoint-Seite mit allen Dokumenten, Listen, Bibliotheken und weiteren Inhalten. Die Seiten sind dazu speziell für Windows Phone 7 angepasst.

Übersicht: SharePoint-Seiten lassen sich so einfach anzeigen.

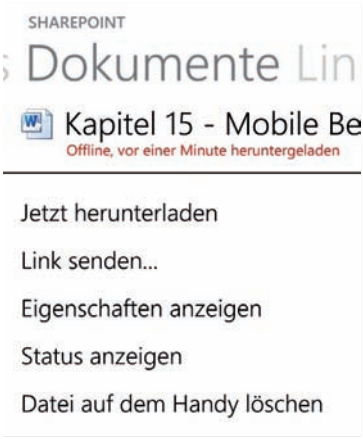
Sobald Sie ein Dokument geöffnet haben, erscheint es künftig auf der Startseite von SharePoint Workspace Mobile und ist im direkten Zugriff. Wenn Sie online mit dem SharePoint-Server verbunden sind, speichert Windows Phone 7 Änderungen im Dokument direkt im Original in der SharePoint-Bibliothek. Sie können aber auch offline weiterarbeiten, da SharePoint Workspace Mobile das Dokument auf dem Smartphone speichert. Sind Sie wieder mit SharePoint verbunden, können Sie das Dokument und Ihre Änderungen dann in der SharePoint-Bibliothek speichern. Die Speichervorgänge sind für Anwender sehr einfach, da diese das Dokument nur speichern und keine Bibliothek auswählen müssen. Die Anbindung ist auch problemlos an Small Business Server 2011 Standard beziehungsweise SharePoint Foundation 2010 möglich. Sie müssen also nicht auf einen vollwertigen SharePoint Server 2010 setzen, um Windows Phone 7 über SharePoint Workspace Mobile an SharePoint anzubinden.

6.3.6 SharePoint-Dokumente offline verwenden

Wenn Sie in Windows Phone 7 auf der Seite der Anwendungen auf Office klicken und dann zu SharePoint Workspace Mobile wechseln, sehen Sie nach der Verbindung zur SharePoint-Seite die bereits geöffneten Dokumente. Aus den Bibliotheken können Sie an dieser Stelle durch Anklicken neue Dokumente öffnen.

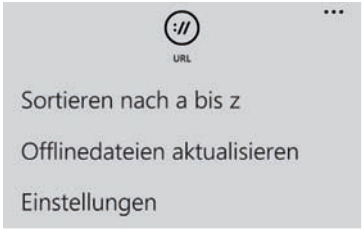
Klicken Sie auf *Alle* und dann auf die Seite *Dokumente*, um weitere Funktionen zu nutzen. Halten Sie den Finger über der Verknüpfung eines Dokuments an dieser Stelle fest, erscheint ein Menü, mit dem Sie das Dokument auf vielfältige Weise verwalten können.

- *Jetzt herunterladen* – Lädt das Dokument aus der SharePoint-Bibliothek auf das Smartphone. Auf diese Weise speichern Sie offline im Smartphone die aktuelle Version des Dokuments.



Heruntergeladen: So lassen sich Dokumente auch offline verwenden.

- *Immer Offline bleiben* – Lädt das Dokument aus der Bibliothek herunter und ermöglicht die Bearbeitung, auch wenn Sie nicht mit SharePoint verbunden sind. Auf diese Weise können Sie beliebige Dokumente aus SharePoint offline auf dem Gerät verwenden. Wollen Sie alle offline gespeicherten Dokumente auf dem Smartphone auf einmal aktualisieren, also aktuelle Versionen aus den SharePoint-Bibliotheken herunterladen, klicken Sie auf der SharePoint-Workspace-Mobile-Startseite auf Dokumente und dann auf die drei Punkte, um das erweiterte Menü aufzurufen. Anschließend können Sie durch Auswahl von Offline-Dateien aktualisieren alle Dokumente auf einmal neu herunterladen.



Hilfreich: Sie können Offline-Dateien erneut aktualisieren lassen.

- *Link senden* – Durch diese Auswahl erstellen Sie eine neue E-Mail oder eine SMS, die den direkten Link zum Dokument in der SharePoint-Datenbank

enthält. Auf diese Weise können Sie anderen Anwendern den Zugriff auf das Dokument schnell und einfach ermöglichen.

- *Eigenschaften anzeigen* – Zeigt den SharePoint-Inhaltstyp an, auf den das Dokument aufbaut, den Titel, den Namen der Datei, das Erstellungsdatum, den Autor, das Datum der letzten Änderung und ob das Dokument ausgecheckt ist. Auch die Version des Dokuments in SharePoint sehen Sie.
- *Status anzeigen* – Zeigt den Zeitpunkt der letzten erfolgreichen Aktualisierung vom SharePoint-Server aus an. Hier können Sie das Dokument auch manuell erneut von der entsprechenden SharePoint-Bibliothek herunterladen.
- *Datei auf dem Handy löschen* – Entfernt die Offline-Kopie der Datei auf dem Smartphone. Das Original in der SharePoint-Bibliothek bleibt erhalten.

6.3.7 Einstellungen in SharePoint Workspace Mobile

Klicken Sie in SharePoint Workspace Mobile auf den Link *Alle* auf der Seite, zeigt Ihnen das Tool die angebundenen Bibliotheken und Dokumente an, die Sie bereits geöffnet haben. Sie können in der Ansicht Alle zwischen den zwei Seiten *Dokumente* und *Links* wechseln. Auf der Seite Dokumente können Sie über das Menü, das Sie über die drei Punkte im unteren Bereich erreichen, die Sortierung ändern, die Dateien offline synchronisieren und Einstellungen ändern.

Verbindung: Sie können die Einstellungen für die SharePoint-Anbindung verändern.

Neben der Seite *Dokumente* in SharePoint Workspace Mobile steht noch die Seite Links zur Verfügung, zu der Sie ganz einfach umblättern können. Hier sehen Sie alle in der Vergangenheit geöffneten SharePoint-Links. Öffnen Sie eine Seite, steht

wiederum das erweiterte Menü über die drei Punkte zur Verfügung. In diesem Bereich können Sie dann die Ansicht aktualisieren oder ein Lesezeichen hinzufügen, um die Seite künftig sofort aufrufen zu können, und Sie haben die Möglichkeit, die Seite direkt im Internet Explorer Mobile zu öffnen. In den Einstellungen setzen Sie den Cache für die Verwendung der SharePoint-Dateien zurück und steuern die Anbindung an ein Unified Access Gateway (UAG) im Unternehmen. Hier regeln Sie auch die Konfliktlösung in SharePoint (siehe unten).

6.3.8 Zugriff mobiler Anwender auf SharePoint

SharePoint spielt seine Vorteile dann aus, wenn auch mobile Anwender über das Internet auf das System zugreifen können. Dazu ist es notwendig, die Dienste in SharePoint zu veröffentlichen. Neben dem Forefront Threat Management Gateway (TMG) 2010 bietet Microsoft noch das Forefront Unified Access Gateway (UAG) 2010 an. Hierbei handelt es sich um eine erweiterte Version des TMG, das besser für SharePoint geeignet ist. Das TMG 2010 ist der Nachfolger von ISA 2006, das UAG 2010 der Nachfolger des Intelligent Application Gateway (IAG) 2007.

Der Vorteil der größeren UAG-Version ist die Unterstützung von AAM (Alternative Access Mappings, alternative Zugriffszuordnungen). Mit dieser Funktion können Sie effizient URLs zu SharePoint frei definieren und zu den internen Webanwendungen umleiten. Dazu leiten Sie die externe Adresse zum UAG, zum Beispiel *https://www.contoso.com*. Das UAG leitet die Anfragen dann an die interne URL zu SharePoint weiter, beispielsweise *http://sps01.contoso.local*. Zusätzlich kann das UAG die Webanwendungen von SharePoint direkt unterstützen und in die Veröffentlichung einbinden. Das Veröffentlichungskonzept des UAG 2010 funktioniert etwas anders als beim TMG. Während Sie mit dem TMG einzelne Websites im Internet zu Verfügung stellen, bietet das UAG eine eigene Portalanwendung an. Seine Vorteile spielt das UAG 2010 aus, wenn Sie mehrere Websites, Dateifreigaben, Remote Desktops oder OWA anbinden wollen. Allerdings ist der Preis des Unified Access Gateway wesentlich höher als der des TMG 2010.

6.3.9 Konflikte beim Speichern in SharePoint-Bibliotheken lösen

Kommt es zu einem Konflikt beim Speichern, können Sie diesen auch direkt in Windows Phone 7 lösen. Ein Konflikt entsteht zum Beispiel, wenn Sie ein Dokument offline ändern, während es auch online in der SharePoint-Bibliothek durch einen anderen Anwender geändert wurde. In diesem Fall öffnen Sie den Office-Hub und wechseln auf *Alle\Dokumente*. Tippen Sie das Dokument an, halten Sie es fest und wählen *Status anzeigen*. An dieser Stelle steht die Konfliktlösung zur Verfügung. Hier können Sie entscheiden, welche Version des Dokuments Sie behalten wollen. Sie können auch beide Versionen behalten.

Lösungsansatz: Sie können sich bei Konflikten stets benachrichtigen lassen.

In diesem Fall wählen Sie bei der Bearbeitung des Dokuments *Speichern unter* und geben einen neuen Dateinamen an. Sie können das generelle Verhalten von Konflikten anpassen, wenn Sie im Office-Hub auf *SharePoint\Alle* und dann auf die drei Punkte klicken. Rufen Sie *Einstellungen* auf und gehen dann auf Konflikte.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

TecChannel-Links zum Thema	Webcode	Compact
Praxis: Office Mobile in Windows Phone 7 nutzen	2036626	S.268
Windows Phone 7 im Unternehmenseinsatz	2036115	S.255
Ratgeber: Windows Phone 7 für Admins	2036148	S.261
Windows-Phone-7-Praxis: Exchange-Anbindung und Zertifikate	2036585	S.280
Workshop – Versteckte Windows-Phone-7-Funktionen aktivieren	2036340	S.288
Praxis: Termine verwalten mit Windows Phone 7	2036685	S.295
Windows Phone 7 im Unternehmen bereitstellen	2036982	S.301

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

6.4 Windows-Phone-7-Praxis: Exchange-Anbindung und Zertifikate

Wer in seiner IT-Umgebung Smartphones mit Windows Phone 7 einsetzt, wird diese in den meisten Fällen auch an vorhandene Exchange- und SharePoint-Strukturen anbinden wollen. Dies funktioniert relativ problemlos und klappt dementsprechend auch, wenn Sie auf den Small Business Server 2011 von Microsoft setzen. Mit Outlook Mobile und dem Office Mobile-Client für SharePoint bietet Windows Phone 7 eine bessere Anbindung als die direkten Konkurrenten iPhone respektive iOS und Android. Da die zusätzliche Bereitstellung von Apps entfällt, können Anwender mit entsprechenden Anleitungen schnell und einfach selbst die Anbindung durchführen.

Im Gegensatz zur Anbindung von iPhones (siehe auch iPhone-Praxis: Anbindung an Exchange und SharePoint Server, Webcode **2032686**) müssen Administratoren aber die Anbindung von Windows Phone 7 an Exchange, SBS oder SharePoint vorbereiten. Die Anbindung ist nicht Out-of-the-Box möglich, wenn Sie eigene Zertifikate oder das selbstsignierte Zertifikat von Exchange oder SBS nutzen.

6.4.1 Zertifikate und Windows Phone 7

Bei der Anbindung an Exchange spielt in Windows Phone 7 die Konfiguration der Zertifikate eine zentrale Rolle. Ist das Zertifikat des Exchange-Servers auf dem Smartphone nicht bekannt, ist keine Anbindung möglich. Anwender können das Konto zwar einrichten, erhalten aber in den meisten Fällen eine Fehlermeldung, weil das Zertifikat nicht bekannt ist. Im Gegensatz zum iPhone oder zu Android-Geräten ermöglicht Windows Phone 7 dann keine Anbindung, sondern bricht die Synchronisierung mit einem Fehler ab. Das heißt, wenn Sie mit eigenen oder selbstsignierten Zertifikaten arbeiten, müssen Sie vor der Anbindung an Exchange das Zertifikat auf dem Smartphone installieren. Bei den Vorgängern von Windows Phone 7, zum Beispiel Windows Mobile 6 oder 6.5, konnten Sie das Zertifikat noch mit einer SD-Karte oder per Active Sync auf das Endgerät kopieren. Das ist mit Windows Phone 7 nicht mehr möglich.

6.4.2 Zertifikate auf dem Smartphone installieren

Um ein Zertifikat auf dem neuen System zu installieren, müssen Sie es beispielsweise über eine Webseite zur Verfügung stellen. Die Webseite rufen Sie mit dem Smartphone auf und installieren dann das Zertifikat. Eine andere Variante ist, dass Sie auf dem Smartphone ein weiteres (anderes) E-Mail-Konto einrichten und zu diesem die Zeritifikate-Datei senden. Den Anhang können Sie auf dem Smartphone dann anklicken und das Zertifikat installieren.

Die Installation können auch Anwender durchführen, da die Datei nur angeklickt werden muss. Anschließend lässt sich das Zertifikat schnell und einfach durch einen einfachen Klick installieren.

Zustellung: Sie können ein Zertifikat per E-Mail versenden.

Sie benötigen dazu das Zertifikat von Exchange, also das Webserver-Zertifikat, und das Zertifikat der Stammzertifizierungsstelle, wenn Sie mit einer eigenen Zertifizierungsstelle arbeiten, zum Beispiel auf Basis der Active-Directory-Zertifikatsdienste. Am besten exportieren Sie dazu auf dem Exchange-Server beide Zertifikate in eine Exportdatei und verschicken diese per E-Mail, zum Beispiel zu einem Windows Live-E-Mail-Konto. Das können Anwender teilweise auch selbst durchführen, zum Beispiel durch eine Verbindung zu Outlook Web App auf einem PC und anschließendem Export. Anschließend senden sie die Exportdatei an ein anderes E-Mail-Konto und führen die Anbindung durch.

6.4.3 Zertifikate per Outlook Web App exportieren

Liegt ein Problem mit dem Zertifikat vor, informiert der Internet Explorer oder Mozilla Firefox darüber, wenn Sie sich mit Outlook Web App verbinden. Lassen Sie in diesem Fall das Laden der Seite fortsetzen, um das Zertifikat zu übertragen.

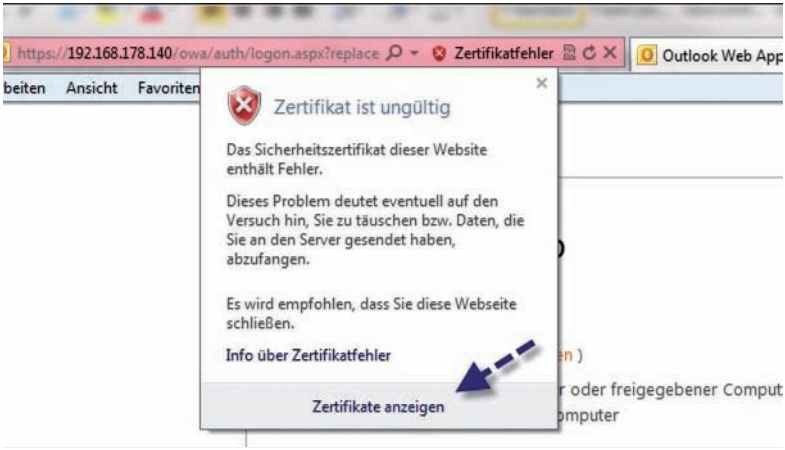
Sie müssen sich nicht an OWA anmelden, das Zertifikat wird bereits beim Aufrufen der OWA-Seite angezeigt. Anschließend können Sie das Zertifikat der Stammzertifizierungsstelle über OWA auf dem PC exportieren. Dieser Weg funktioniert allerdings nicht immer, da meistens nur das Webserver-Zertifikat übertragen wird, nicht zusätzlich noch das Zertifikat der Stammzertifizierungsstelle.

Wenn Sie beispielsweise mit einem selbstsignierten Zertifikat arbeiten, wie in Small Business Server 2008/2011, funktioniert der Export über OWA nicht.

Schritt-für-Schritt: Export per Outlook Web App

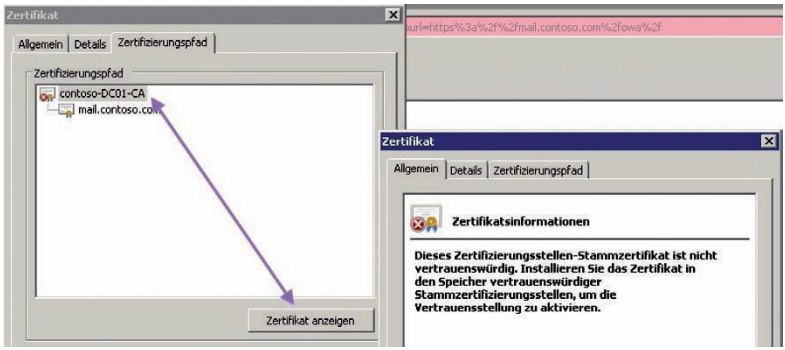
Arbeiten Sie aber mit einer internen Zertifizierungsstelle, können Sie über OWA beide Zertifikate exportieren. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie eine Verbindung zu Outlook Web App mit dem Internet Explorer auf einem Computer. Bei diesem Vorgang wird das Zertifikat übertragen.



Geht doch: Auch bei einer Fehlermeldung können Sie das übertragene Zertifikat öffnen.

2. Klicken Sie im Anschluss auf die Meldung *Zertifikatfehler* und dann *Zertifikate anzeigen*, wenn Sie das Laden der Seite fortgesetzt haben. Alternativ können Sie die geladenen Zertifikate auch auf der Seite anzeigen lassen.
3. Öffnen Sie die Registerkarte *Zertifizierungspfad*.
4. Markieren Sie das oberste Zertifikat im Pfad, da dieses das Zertifikat der Zertifizierungsstelle darstellt. Wird hier kein Zertifikat angezeigt, funktioniert dieser Weg nicht, das Zertifikat der Zertifizierungsstelle wird nicht übertragen. In diesem Fall müssen Sie das Zertifikat auf einen Rechner exportieren, der über das entsprechende Zertifikat verfügt, zum Beispiel den Exchange-Server selbst, oder einen Computer, der Mitglied in der gleichen Active-Directory-Gesamtstruktur des Exchange-Servers oder des SBS ist.



Details: Sie können sich das Zertifikat anzeigen lassen.

5. Klicken Sie im Anschluss auf *Zertifikat anzeigen*.
6. Klicken Sie im neuen Fenster auf die Registerkarte Details und dann auf die Schaltfläche *In Datei kopieren*, um das Zertifikat in eine Datei zu exportieren. Wurde das Zertifikat als nicht exportierbar markiert, ist die Schaltfläche für das Exportieren nicht aktiv.
7. Wenn Sie den geschützten Modus im Internet Explorer aktiviert haben, können Sie die Schaltfläche ebenfalls nicht auswählen. In diesem Fall können Sie versuchen, den geschützten Modus des Internet Explorers zeitweise zu deaktivieren. Klicken Sie dazu doppelt auf den Modus in der Statusleiste des Internet Explorers. Anschließend öffnet sich ein Fenster, und Sie können den geschützten Modus deaktivieren. Starten Sie den Internet Explorer neu und versuchen Sie den Export erneut. Die Schaltfläche In Datei kopieren sollte jetzt verfügbar sein.

Einfach: Installation eines Zertifikats unter Windows Phone 7.

8. Belassen Sie die Standardeinstellungen und exportieren das Zertifikat in eine Datei, die Sie zum Beispiel auf dem Desktop abspeichern.
9. Versenden Sie diese Datei an ein E-Mail-Konto, das Sie auf dem Smartphone eingerichtet haben. Klicken Sie dann auf dem Smartphone die Datei an und lassen das Zertifikat installieren. Anschließend können Sie die Exchange-Anbindung durchführen.

6.4.4 Zertifikat auf einem Mitglied der AD-Struktur des Servers exportieren

Zeigt Outlook Web App das Zertifikat der Stammzertifizierungsstelle nicht an, können Sie es auch direkt auf einem Computer exportieren der Mitglied in der gleichen Active-Directory-Gesamtstruktur des Servers ist. Die vertrauenswürdigen Zertifizierungsstellen finden Sie am besten über den Internet Explorer.

Rufen Sie nach dem Start über *Extras/Internetoptionen* die Registerkarte *Inhalte* und dann per Klick auf die Schaltfläche *Zertifikate* und Auswahl der Registerkarte *Vertrauenswürdige Stammzertifizierungsstellen* die Auflistung der Zertifizierungsstellen auf dem PC auf. Markieren Sie diese Zertifizierungsstelle und klicken Sie auf die Schaltfläche *Exportieren*. Unter Umständen tauchen an dieser Stelle mehrere Zertifikate Ihrer Stammzertifizierungsstelle auf. Erscheint beim Exportieren

eine Abfrage des privaten Schlüssels des Zertifikats, haben Sie das falsche erwischt. Verwenden Sie dann einfach das andere Zertifikat. Exportieren Sie auf dem Computer das Zertifikat in eine .cer-Datei. Diese Datei senden Sie per E-Mail an das Windows-Phone-7-Gerät über ein E-Mail-Konto, zum Beispiel Windows Live.

6.4.5 Zertifikat per Konsole auf dem Webserver exportieren

Um das Zertifikat des Webservers zu exportieren, können Sie auch direkt die Zertifikatekonsole des Computers verwenden:

1. Geben Sie *mmc* im Suchfeld des Startmenüs ein, um eine Managementkonsole zu öffnen.
2. Klicken Sie auf *Datei/Snap-In hinzufügen/entfernen*.
3. Wählen Sie *Zertifikate* aus und klicken auf *Hinzufügen*.
4. Wählen Sie als Speicher *Computerkonto* aus und klicken auf *Weiter*.
5. Wählen Sie das lokale Computerkonto aus und klicken auf *Fertig stellen* sowie anschließend auf *OK*.
6. Erweitern Sie in der Konsole den Knoten *Zertifikate/Eigene Zertifikate/Zertifikate*. Die Zertifikate der Stammzertifizierungsstellen finden Sie im Ordner *Vertrauenswürdige Stammzertifizierungsstellen\Zertifikate*.
7. Klicken Sie das Zertifikat mit der rechten Maustaste an und wählen *Alle Aufgaben/Exportieren*.
8. Gehen Sie die einzelnen Fenster des Assistenten durch. Den privaten Schlüssel müssen Sie nicht exportieren.
9. Belassen Sie als Format DER-codiert.
10. Wählen Sie den Namen und den Speicherort der Exportdatei aus.
11. Schließen Sie den Export ab.
12. Versenden Sie das Zertifikat zum Smartphone oder stellen Sie es auf einer Webseite zum Download zur Verfügung.

Haben Sie das Zertifikat auf dem Windows-Phone-7-Gerät installiert, müssen Sie das Gerät neu starten. Erst dann liest Windows Phone 7 das neue Zertifikat ein. Das gilt auch für die Anbindung an Small Business Server 2008/2011, die wir nachfolgend beschreiben.

6.4.6 Windows Phone 7 und SBS 2008/2011 – selbst signierte Zertifikate

Wollen Sie Windows Phone 7 an SBS 2008/2011 anbinden, können Sie das Zertifikat des SBS auch über bereits vorkonfigurierte Wege auf das Smartphone übertragen. Sie müssen in diesem Fall keinen komplexen Exportvorgang starten, wie vor-

hergehend besprochen. In SBS 2008 finden Sie die notwendigen Dateien über \\<*Name des Servers*>*public**downloads*. In SBS 2011 finden Sie die Zertifikatedatei über \\<*Name des Servers*>*public**Downloads**Certificate Distribution Package*. Sie benötigen nicht die .exe-Datei, sondern nur die .cer-Datei im Verzeichnis. Diese enthält das erforderliche Zertifikat.

Verschicken Sie diese Datei per E-Mail an das Smartphone oder stellen Sie diese über das Web zur Verfügung. Auch wenn Sie nicht mit SBS 2008/2011 arbeiten, sondern mit Exchange und selbst signierten Zertifikaten, müssen Sie dieses auf dem Smartphone installieren. Dazu exportieren Sie das selbst signierte Zertifikat wie in den vorangegangenen Schritten besprochen. Sie müssen zur Installation des Zertifikates auf dem Smartphone nur das Zertifikat anklicken.

Nach der Installation des Zertifikats richten Sie ein neues Exchange-E-Mail-Konto auf dem Windows-Phone-7-Gerät ein. Geben Sie dazu zunächst die E-Mail-Adresse und das Kennwort ein und lassen Sie sich dann verbinden. In den meisten Fällen erscheint noch eine Fehlermeldung, da Sie sich authentifizieren müssen. Achten Sie bei der Anbindung über das Internet darauf, dass Sie den Port 443 der externen Firewall zur internen IP-Adresse des SBS beziehungsweise des Client-Zugriff-Servers weiterleiten lassen. Anschließend baut das Smartphone die Verbindung auf. Findet das Gerät den Server nicht, erscheint eine erweiterte Einrichtungsoberfläche. In diese tragen Sie den Benutzernamen und die Domäne ein.

Verwenden Sie hier den internen Domänennamen zur Anmeldung. Kann das Gerät auf Basis des DNS-Namens Ihrer E-Mail-Adresse Ihren Server finden und durch die Port-Weiterleitung auf der Firewall eine Verbindung aufbauen, lassen sich E-Mails synchronisieren. Sie können über die Einstellungen des Kontos durch Anklicken der Schaltfläche *Synchronisierungseinstellungen* die Daten des Servers auch nachträglich ändern.

DynDNS einsetzen

Bei kleinen Netzwerken haben Sie hier die Möglichkeit, mit DynDNS zu arbeiten. Dazu tragen Sie Ihren DynDNS-Namen, der zur externen Schnittstelle der Firewall zeigt, als Servernamen ein. Haben Sie auf Ihrer Firewall eine Weiterleitung aktiviert, leitet diese die Anfrage des Windows-Phone-7-Gerätes an den Port 443 des SBS oder des Exchange weiter und baut die Verbindung auf.

Achten Sie aber darauf, dass Sie bei der Einrichtung des Assistenten für die Internetanbindung des SBS beziehungsweise bei der manuellen Zuteilung des Exchange-Zertifikats als gemeinsamen Namen des Zertifikats den Namen verwenden, den Sie auch für die Verbindung nutzen, im Falle von DynDNS also den DynDNS-Namen. Bei der ersten erfolgreichen Verbindung mit dem Server erhalten Sie auch Meldungen der zugewiesenen ActiveSync-Richtlinien und müssen diese umsetzen. Erst dann synchronisiert sich Windows Phone 7 erfolgreich mit dem Server. Kann das Gerät hingegen bereits die Richtlinien abrufen, können Sie davon ausgehen, dass die Verbindung funktioniert.

Alternative: Sie können ebenso mit DynDNS arbeiten. Geben Sie die Verbindungsdaten mit Exchange oder SBS ein.

6.4.7 Zertifikate über das Internet über eine Webseite veröffentlichen – SBS 2011

Zertifikate, die Ihnen als .cer-Datei vorliegen, können Sie über das Internet zur Verfügung stellen. Dazu müssen Sie im internen Netzwerk einen Webserver betreiben, zum Beispiel auf Basis des IIS.

Einrichtung: Das Zertifikat lässt sich über den Internet Explorer installieren.

Auf diese Weise können Sie zum Beispiel auch das Zertifikat von SBS 2008/2011 veröffentlichen. Der Weg dazu ist ganz leicht:

1. Sie kopieren die .cer-Datei in das Verzeichnis *C:\inetpub\wwwroot* auf dem SBS oder dem Webserver. Im Fall von SBS verwenden Sie einfach die bereits beschriebene Datei, die auf dem Server vorliegt.
2. Sie benennen die Datei um, damit diese die Endung .p7b hat. Dieser Schritt ist wichtig.
3. Sie richten eine Port-Weiterleitung auf Ihrer Firewall zum Port 80 des Webservers ein, im Fall von SBS der internen IP-Adresse des SBS.

4. Auf dem Windows-Phone-7-Gerät geben Sie die URL *http://<Externer Name des Servers>/<Name des Zertifikats>.p7b* im Internet Explorer Mobile ein. Sie können auch hier mit DynDNS-Namen arbeiten.
5. Anschließend öffnet sich auf dem Gerät ein Fenster, über das Sie das Zertifikat installieren können.

Haben Sie das Zertifikat installiert, richten Sie die E-Mail-Synchronisierung genauso ein wie mit anderen Konten.

6.4.8 SharePoint und Companyweb mit Windows Phone 7

Windows Phone 7 kann man auch relativ schnell und einfach an SharePoint anbinden. Im Gegensatz zu iPhones oder Android-Geräten, ist in Windows Phone 7 bereits über Office Mobile eine entsprechende App integriert. Sie müssen nur die URL des SharePoint-Servers eingeben, im Falle von SBS ist das beispielsweise *http://companyweb*. Anschließend geben Sie noch die Benutzeranmeldedaten ein und können problemlos auf SharePoint zugreifen.

Problemlos: Mit einem Windows-7-Smartphone können Sie einfach auf SharePoint, hier im Falle des Small Business Servers, auf das companyweb zugreifen.

Wenn Sie auf eine Liste oder eine Bibliothek klicken, können Sie direkt mit Office-Mobile auf die Dokumente zugreifen und diese bearbeiten. Haben Sie einmal auf eine Bibliothek oder Liste zugegriffen, speichert Office Mobile den Link ab und ermöglicht Ihnen den direkten Zugriff.

Natürlich können Sie sich auch mit mehreren SharePoint-Seiten verbinden. Dazu geben Sie in Office Mobile einfach die URL zu den entsprechenden Seiten ein. Der Umgang ist sehr intuitiv. Zum Aufbauen der Verbindung ist lediglich die URL notwendig, alles andere ist bereits in Windows Phone 7 integriert.

Thomas Joos

6.5 Workshop – Versteckte Windows-Phone-7-Funktionen aktivieren

Das Windows-Phone-7-Betriebssystem besitzt undokumentierte Optionen, die den Funktionsumfang der mobilen Geräte erweitern. So lassen sich per Registry-Hack und App-Funktionen wie Multitasking, Taskviewer oder Screenshots nutzen. Unser Workshop zeigt, wie Sie diese Dienste einrichten.

Windows Phone 7 unterstützt standardmäßig kein Multitasking. Das heißt, wenn Sie Anwendung A öffnen und dann eine andere Anwendung B öffnen, schließt sich Anwendung A. Rufen Sie erneut Anwendung A auf, dauert der Start sehr lange, weil das System die Anwendung erst öffnen und das Programm B schließen muss. Das ist vor allem dann ein Problem, wenn Sie in einer Anwendung etwas erledigen und gleichzeitig eine E-Mail, eine SMS oder ein Anruf ankommt. Wechseln Sie mit der „Hometaste", müssen Sie anschließend die Anwendung erst neu öffnen. Mit dem Mango-Update (Windows Phone 7.5), das im Herbst 2011 erscheinen soll, behebt Microsoft dieses Leistungs- und Bedienungsproblem. Anwender mit Windows-Phone-7-Geräten können Multitasking aber mit einem Registry-Hack bereits jetzt in Windows Phone 7 aktivieren und das System dadurch enorm beschleunigen. Auf diesem Weg ist es dann auch möglich, Screenshots zu erstellen und auch andere versteckte Funktionen und Systemeinstellungen zu aktivieren.

Achtung: Nehmen Sie Änderungen über die in diesem Beitrag erwähnten Funktionen an Ihrem Handy vor, besteht die Gefahr, Ihr Telefon dauerhaft zu beschädigen. Sie testen also auf eigenes Risiko.

6.5.1 Developer-Einstellungen im LG E900 Optimus 7 aktivieren

Damit Sie entsprechende Einstellungen in Windows Phone 7 vornehmen können, die über die Standardmöglichkeiten hinausgehen, zum Beispiel Multitasking, einen Taskviewer oder Screenshots aktivieren, müssen Sie das Telefon „unlocken" und ein erneutes Relocken durch Zune verhindern. Solche Konfigurationen sind aber auch gefährlich, da solche Änderungen das Telefon stark in Mitleidenschaft gezogen werden kann.

Eines der meistgenutzten Windows-Phone-7-Geräte ist das LG E900 Optimus 7. Sie haben bei diesem Handy die Möglichkeit, über wenige Handgriffe das interne Entwicklermenü zu aktivieren. Dieses bietet verschiedene Funktionen wie einen Registry-Editor, verschiedene Tests, ein Engineer-Menü mit Port-Einstellungen, Modem-Einstellungen und vieles mehr. Mit diesem Menü können Sie Ihr Gerät auch „unlocken", also bleibende Änderungen ab Gerät ermöglichen, die sich von den Herstellereinstellungen unterscheiden. Achten Sie aber darauf, dass diese Einstellungen ein Gerät durchaus auch beschädigen können, daher sollten nur experi-

mentierfreudige Anwender Änderungen vornehmen. Das Einblenden des Menüs ist aber noch nicht gefährlich, da Sie dabei keine Änderungen vornehmen.

- Um es einzublenden, wechseln Sie in die Telefonansicht und geben `##634#` ein.
- Anschließend finden Sie bei den Anwendungen die neue Anwendung „MFG". Wenn Sie diese aufrufen, wird ein Kennwort verlangt. Dieses lautet in den meisten Fällen standardmäßig `277634#*#` oder `APPMFG#*#`.

Haben Sie das Kennwort korrekt eingeben, stehen Ihnen jetzt die entsprechenden Anwendungen für weitere Zwecke zur Verfügung.

Zusatzfunktionen: Nach dem Aktivieren des Factory-Menü in Geräten mit Windows Phone 7 sind zusätzliche Optionen frei geschaltet.

Innerhalb des Menüs müssen Sie genau wissen was Sie tun, wenn Sie das Gerät nicht beschädigen wollen. Ein solches Menü gibt es auch für andere Windows Phone 7-Geräte. Etwas Suche mit Google bringt einiges zu Tage. Jedes Telefon lässt sich auf anderem Weg unlocken.

6.5.2 LG E900 Optimus 7 „unlocken"

Um die versteckten Funktionen im LG E900 Optimus 7 zu setzen, müssen Sie das Telefon „unlocken". Dazu aktivieren Sie das MFG (Developer)-Menü des Telefons und öffnen anschließend den Registry-Editor des MFG-Modus, um Änderungen in der Registry vorzunehmen:

1. Starten Sie das MFG-Menü (im Telefonmodus die Zeichenfolge `##634##` eingeben, als Kennwort benutzen Sie die folgende Eingabe: `277634#*#`, teilweise ist das Kennwort auch auf `APPMFG#*#` gesetzt).
2. Navigieren Sie zu *Engineer Menu/Other Setting/edit registry*.

Handarbeit: die erweiterten Einstellungen im LG E900 Optimus 7 aufrufen.

3. Wählen Sie bei *Select Root_Path* die Option *HKEY_LOCAL_MACHINE* aus.
4. Geben Sie bei *Input SUB_PATH* folgendes ein: *Comm\Security\LVMod*.
5. Geben Sie bei *Input Key and select data typ*: *DeveloperUnlockState* ein.
6. Wählen Sie als Datentyp *DWORD* aus.
7. Geben Sie bei *Input data 1* ein.
8. Wenn Sie auf *Query* klicken, sehen Sie den aktuellen Registry-Wert. Ist dieser bereits auf 1 gesetzt, müssen Sie keine Änderungen vornehmen. Hat er einen anderen Wert oder ist nicht vorhanden, klicken Sie auf Set. Anschließend sehen Sie den neuen Wert des Registry-Eintrags.

So geht's: LG E900 Optimus 7 „unlocken".

Mit diesen Schritten haben Sie das Gerät zwar „unlocked“, sobald Sie es aber mit Zune verbinden, ist es wieder gelockt und erlaubt keine Änderungen mehr. Wollen Sie auch das „Relocken“ verhindern, müssen Sie im Registry-Editor noch einen Wert ändern:

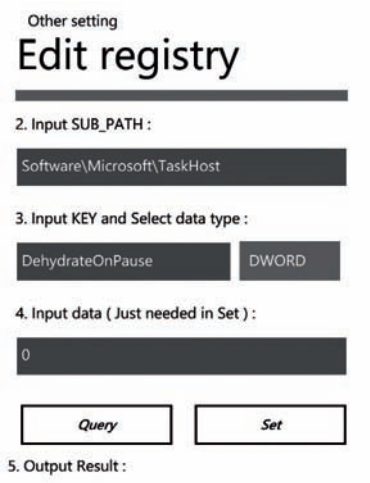
1. Wählen Sie bei *Select Root_Path* die Option *HKEY_LOCAL_MACHINE* aus.
2. Geben Sie bei Input *SUB_PATH* folgendes ein: *Software\Microsoft\DeviceReg*.
3. Geben Sie bei *Input Key and select data typ: PortalUrlProd* ein.
4. Wählen Sie als Datentyp *DWORD* aus.
5. Geben Sie bei *Input data* keinen Wert ein.
6. Wenn Sie auf *Query* klicken, sehen Sie den aktuellen Registry-Wert. Ist dieser bereits auf *0* gesetzt, müssen Sie keine Änderungen vornehmen. Hat er einen anderen Wert oder ist gar nicht vorhanden, klicken Sie auf Set. Anschließend sehen Sie den neuen Registry-Wert.

Starten Sie das Telefon neu. Ab dem Neustart ist das Telefon „unlocked“, und Zune kann es auch nicht mehr „relocken“. Das heißt: Änderungen, die Sie am Telefon vornehmen, bleiben bestehen.

6.5.3 Speed-Hack für Windows Phone 7 – Multitasking aktivieren

Den Speed-Hack für Windows Phone 7 können Sie mit nahezu jedem Windows-Phone-7-Gerät durchführen. Allerdings muss für diese Leistungsverbesserung die Registry bearbeitet werden. Aktivieren Sie dazu auf dem Gerät einen Registry-Editor (beim LG E900 Optimus 7 zum Beispiel über das MFG-Menü). Andere Registry-Editoren können Sie ebenfalls herunterladen (http://dotconn.de/Dateien/Homebrew/RegistryEditor.xap). XAP-Dateien installieren Sie über die Windows-Phone-Developer-Tools (www.microsoft.com/downloads/de-de/details.aspx?FamilyID=04704acf-a63a-4f97-952c-8b51b34b00ce). Am Beispiel des LG E900 Optimus 7 nehmen Sie den Registry-Hack wie angegeben vor. Bei anderen Handys geben Sie die Werte im entsprechenden Registry-Editor ein:

1. Wählen Sie bei *Select Root_Path* die Option *HKEY_LOCAL_MACHINE* aus.
2. Geben Sie bei *Input SUB_PATH* folgendes ein: *Software\Microsoft\TaskHost*
3. Geben Sie bei *Input Key and select data typ: DehydrateOnPause* ein.
4. Wählen Sie als Datentyp *DWORD* aus.
5. Geben Sie bei *Input data 0* ein.
6. Klicken Sie auf *Query*, sehen Sie den aktuellen Wert des Registry-Wertes. Ist dieser bereits auf 0 gesetzt, müssen Sie keine Änderungen vornehmen. Hat er einen anderen Wert (standardmäßig 3) oder ist nicht vorhanden, klicken Sie auf Set. Anschließend sehen Sie den neuen Registry-Wert.



Feinabstimmung: Dehydrate-Hacks in Windows Phone 7 durchführen.

Starten Sie Ihr Telefon neu. Wenn Sie nach dem Start zwischen zwei Anwendungen wechseln, schließt sich die erste Anwendung nicht, sondern bleibt aktiv und startet dadurch deutlich schneller. Die Einstellungen haben aber den Nachteil, dass die erste Anwendung im Speicher bleibt. Speicher- und Akku-Verbrauch erhöhen sich also, was in den meisten Fällen aber keine Probleme darstellt. Auf einigen Geräten gibt es nach dem Aktivieren dieser Funktion das Problem, dass die Kacheln des Homescreens teilweise nicht sauber dargestellt werden. Das kommt allerdings sehr selten vor. Wechseln Sie bei geöffneten Anwendungen über die Suchtaste oder die Hometaste die Ansicht, bleiben die entsprechenden Anwendungen aktiv. Sie können Anwendungen schließen, wenn Sie in der Anwendung die Zurücktaste betätigen. Das sollten Sie bei Anwendungen, die Sie nicht dauerhaft benötigen, auch tun, da ansonsten der Akku des Gerätes sehr schnell leer sein kann.

6.5.4 Taskviewer für Windows Phone 7

Haben Sie den Speed-Hack aktiviert, kann es sinnvoll sein zu überprüfen, welche Anwendungen aktuell im Gerät laufen. Auch die laufenden Systemprozesse in Windows Phone 7 sind oft interessant, lassen sich mit Bordmitteln aber nicht anzeigen. Mit der kostenlosen App WPH Task Viewer sehen Sie den Speicherverbrauch der einzelnen aktivierten Anwendungen und wie lange das Telefon bereits läuft. Zur Installation laden Sie sich die *.xap*-Datei herunter. Um diese auf dem Telefon zu installieren, müssen Sie das Telefon unlocken. Mit Windows Phone Developer Tools können Sie .XAP-Dateien in Windows Phone installieren. Sie benötigen dazu das Tool Application Deployment, das Sie in der Programmgruppe der Windows-Phone-7-Developer-Tools finden.

Anwendungsbereitstellung: Anwendungen auf Windows-Phone-7-Geräten installieren.

Sie wählen im Tool einfach die .xap-Datei sowie die Option Windows Phone 7 Device aus und klicken dann auf *Bereitstellen*. Das Telefon muss natürlich per USB verbunden sein und darf sich nicht im Sperrbildschirm befinden. Nach der Installation sollten Sie das Telefon neu starten, erst dann funktioniert die Anwendung. Zuweilen stürzt die Anwendung ab, wenn Anwendungen im Speicher nicht mit der App zusammen funktionieren.

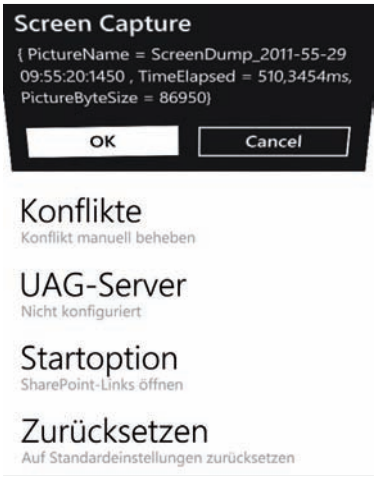
6.5.5 Screenshots mit Windows Phone 7 erstellen

Standardmäßig ist es nicht möglich, mit Windows Phone 7 Screenshots zu erstellen. Das kann vor allem für Entwickler oder Administratoren ärgerlich sein, die Screenshots für Anleitungen schreiben müssen. Bei diesem Problem hilft aber die kostenlose App ScreenCapture von der Seite xdadevelopers weiter (http://forum.xda-developers.com/showthread.php?t=1093169). Damit Sie das Programm nutzen können, müssen Sie das Telefon unlocken und das Relocken verhindern. Zusätzlich müssen Sie den Dehydrate-Hack ausführen, damit Windows Phone 7 Multitasking beherrscht.

Fertig und los: App zum Erstellen von Screenshots starten.

Laden Sie sich die .xap-Datei der aktuellen Version von der Seite herunter und installieren diese mit den Windows-Phone-7-Developer-Tools auf dem Windows

Phone 7-Gerät. Anschließend starten Sie das Telefon neu. In den Anwendungen finden Sie die neue App *CSharp_ScreenCapture*. Sobald Sie diese starten, prüft die Anwendung zunächst, ob der Dehydrate-Hack aktiv ist. Wenn das der Fall ist, sehen Sie einen Haken bei der entsprechenden Option



Final: Die App hat erfolgreich einen Screenshot erstellt.

Anschließend können Sie mit der Hometaste zu der Anwendung oder dem Fenster wechseln, in dem Sie den Screenshot erstellen wollen. Um den Screenshot zu erstellen, halten Sie kurz die Auslösetaste der Kamera gedrückt, wie wenn Sie ein Objekt mit der Kamera in den Fokus setzen wollen. Drücken Sie also den Knopf nicht ganz durch, da Sie ansonsten die Kamera auslösen. Damit Sie Screenshots erstellen können, müssen Sie möglicherweise auch noch die USB-Verbindung trennen. Ist der Screenshot erstellt, erhalten Sie eine Rückmeldung des Tools.

Das Foto speichert das Tool im Ordner der gespeicherten Fotos auf dem Telefon. Sie können die Fotos also problemlos vom Telefon herunterkopieren, zum Beispiel über Zune. Auf der Seite der Entwickler finden Sie auch eine Version, die Screenshots über die Suchen-Taste auslösen kann

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

6.6 Praxis: Termine verwalten mit Windows Phone 7

Die Verwaltung von Terminen gehört zweifelsohne zu den wichtigeren Aufgaben, die man mit einem Smartphone erledigen möchte. Dies beinhaltet neben den reinen Terminen natürlich auch die Synchronisation mit anderen Kalendern, in vielen Fällen wohl einem Exchange-Postfach. Insbesondere bei professionellen Anwendern ist zudem ein ordentlicher Umgang mit Besprechungsanfragen auf dem Smartphone ein wichtiger Gesichtspunkt. Genau das beherrscht Windows Phone 7 ganz ordentlich, verhalten diese sich doch mehr oder minder wie in Outlook.

6.6.1 Besprechungsanfragen nutzen

Wie bei Outlook, erscheinen Besprechungsanfragen auch in Windows Phone 7 im Kalender als Besprechungsanfrage. Diese Besprechungsanfragen lassen sich einfach beantworten und bearbeiten. Alle Informationen zum Termin sieht der Anwender direkt in der E-Mail und im Termin. Die Synchronisierung mit Exchange erfolgt innerhalb weniger Sekunden, sobald eine Netzwerk- oder Internetverbindung zur Verfügung steht. Natürlich lassen sich Besprechungsanfragen zu anderen Kontakten versenden, die nicht über Exchange angebunden sind.

Trefflich: Sie können Besprechungsanfragen in Windows Phone 7 bearbeiten.

Wenn Sie eine Besprechungsanfrage erhalten, können Sie einen anderen Termin vorschlagen. Diese Funktion ist ebenso in Outlook vorhanden. Das heißt, auf diesem Weg lassen sich nicht nur Besprechungen akzeptieren oder ablehnen, sondern auch aktiv ändern. Eingehende Besprechungsanfragen zeigt Windows Phone 7 bereits als vorläufig im Kalender an. Auch diese Funktion ist identisch mit Outlook, wenn Sie den Client in einer Exchange-Umgebung betreiben. Lehnen Sie eine Besprechungsanfrage ab, entfernt Windows Phone 7 diese aus dem Kalender. Bestätigen Sie die Besprechungsanfrage, nimmt das Gerät den Termin als gebucht an und integriert ihn fest in das Postfach. Da die Synchronisierung sehr schnell vonstatten geht, ist Ihr Postfach auch in der Ansicht anderer Anwender immer aktuell.

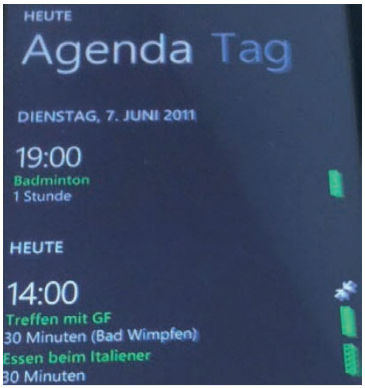
6.6.2 Termine verwalten

Windows Phone 7 hat standardmäßig drei verschiedene Kalenderansichten:

- **Tag** – Zeigt die Termine eines Tages in einer Leiste an. Sie sehen alle Details und können mit der Navigation zwischen den Tagen wechseln. Auch das Erstellen von Terminen ist möglich.
- **Agenda** – Zeigt alle Termine im Kalender übersichtlich an. Die verschiedenen Kalender kennzeichnet Windows Phone 7 farblich.
- **Monat** – Zeigt die Monate an, um schnell zwischen den Tagen zu wechseln. Gebuchte Termine sehen Sie an den einzelnen Tagen.

Um Termine anzuzeigen, öffnen Sie den Kalender im Homescreen. Im oberen Bereich können Sie zwischen der Tagesansicht und einer Agenda umschalten.

Wenn Sie die Agenda verwenden, sehen Sie alle Termine im Kalender und können sich einen Überblick verschaffen. Einzelne Termine lassen sich anklicken, und Sie sehen, zu welchem Kalender der Termin gehört. Auf diesem Weg können die nächsten Termine schnell und einfach angezeigt werden.



Übersicht: Alle Termine im Kalender auf einen Blick. Hier können Sie Termine erstellen und Ansichten ändern.

Bei der Tagesansicht sehen Sie die Termine eines Tages und können auch hier mit dem Display navigieren. Sind Sie am Ende des Tages angekommen, zeigt Windows Phone 7 automatisch die Tagesansicht des nächsten Tages an. In dieser Ansicht erstellen Sie schnell und einfach Termine. Generell zeigt Windows Phone 7 beim Öffnen die jeweils letzte verwendete Ansicht an.

6.6.3 Im Kalender navigieren und Termine erstellen

Im unteren Bereich des Kalenders befinden sich drei verschiedene Schaltflächen. Auf der ersten wird das aktuelle Datum angezeigt. Klicken Sie auf das Datum,

springt Windows Phone 7 zum aktuellen Datum, wenn Sie sich an einem anderen Tag in der Navigation befinden. Klicken Sie auf das Pluszeichen in der Mitte, können Sie einen neuen Termin erstellen. Es besteht aber auch die Möglichkeit, direkt in der Tagesansicht auf den Zeitpunkt zu klicken, an dem Sie einen Termin erstellen wollen. Es öffnet sich ein neues Fenster, in dem Sie den Termin dann eintragen. Auch hier kann ausgewählt werden, in welchem Kalender der Termin erscheinen soll. Über die Schaltfläche *Weitere Informationen* können Sie, neben den Standardeinträgen für einen Termin, auch Wiederholungen festlegen und weitere Teilnehmer einladen, also selbst Besprechungsanfragen erstellen.

Wie in Outlook, lassen sich an dieser Stelle erforderliche und optionale Teilnehmer hinzufügen. Nach der Auswahl zeigt Windows Phone 7 alle gespeicherten Kontakte an, und die Teilnehmer können ausgewählt werden. Erstellen Sie einen Termin, können Sie diesen natürlich jederzeit anpassen und auch löschen. Dazu rufen Sie den Termin einfach im Kalender auf. Mit der ganz rechten Schaltfläche wechseln Sie zur Monatsansicht. Dort sehen Sie an den verschiedenen Daten auch, wo bereits Termine eingetragen sind. Klicken Sie auf einen Tag, öffnet sich die entsprechende Agenda-Ansicht dieses Tages und alle Termine, die Sie zu diesem Datum festgelegt haben. Leider zeigt der Kalender in Windows Phone 7 keine Kalenderwochen mit Wochennummern an, was für Geschäftsanwender sehr ineffizient sein kann. Allerdings gibt es für diese Funktion im Marketplace die kostenlose App Weekfinder (siehe unten).

Mit den drei Punkten öffnen Sie ein erweitertes Menü. Hier können Sie Einstellungen für den Kalender anpassen, zum Beispiel die Farbe der verschiedenen Kalender. Außerdem steuern Sie hier, welche Kalender Windows Phone 7 in der Ansicht der Termine berücksichtigen soll. Generell zeigt das Smartphone immer alle Termine aller Kalender in der Ansicht an. Sie müssen für verschiedene Kalender also keine eigenen Ansichten aktivieren.

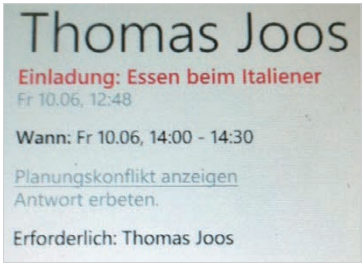
6.6.4 Mit mehreren Exchange-Konten arbeiten

Windows Phone 7 ermöglicht die Anbindung mehrerer Exchange-Konten, die sich über Exchange ActiveSync synchronisieren. Die Kontakte der verschiedenen Konten kann Windows Phone 7 zusammenfassen und gemeinsam bei den Kontakten anzeigen. Diese stehen über eine eigene Kachel zur Verfügung. Außerdem können Sie mehrere Kalender synchronisieren. An dieser Stelle ist es möglich, mehrere Exchange-Konten, aber auch Kalender anderer Anbieter zu synchronisieren. Die Termine zeigt Windows Phone 7 im Telefonkalender an, jeder synchronisierte Kalender erhält eine eigene Farbe. In der Agenda-Ansicht sehen Sie alle Termine von sämtlichen Kalendern, die im Gerät gespeichert sind. Im Display können Sie bequem zwischen den Terminen navigieren. Hinter jedem Termin sehen Sie die Farbe des Kalenders, in dem der Termin eingetragen ist. Die Farbe des Termins steuern Sie in den Kalendereinstellungen. Diese erreichen Sie über die drei Punkte im unteren Bereich. In den Kalendereinstellungen können Sie die Anzeige von ver-

schiedenen Kalendern auch deaktivieren, sodass diese nicht in der Agenda erscheinen. Im oberen Bereich sehen Sie immer das Datum, in dem Sie sich in der Ansicht befinden. Aktivierte Kalender zeigt Windows Phone 7 in allen Ansichten an. Befinden Sie sich in der Tagesansicht, zeigt das Telefon immer alle Termine sämtlicher Kalender an diesem Tag an. Die Unterscheidung der Kalender findet wiederum über die Farben statt, die Sie in den Kalendereinstellungen festlegen.

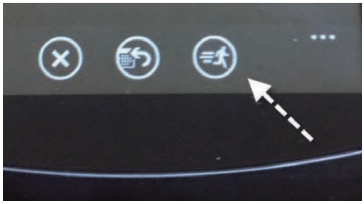
6.6.5 Planungskonflikte lösen

Erhalten Anwender mehrere Besprechungsanfragen, die sich gegenseitig blockieren, oder ist bereits ein anderer Termin im Kalender eingetragen, der sich mit Anfragen überschneidet, erscheint direkt in der Anfrage der E-Mail eine Information über den Konflikt. Auf diese Weise können Anwender den Konflikt lösen und bei Besprechungsanfragen andere Termine vorschlagen.



Planung: Outlook Mobile erkennt Planungskonflikte und kann diese lösen.

Termine, die Sie auf dem Windows-Phone-7-Gerät oder auch in Outlook erstellen, sind sehr schnell synchronisiert, wenn das Gerät eine Internetverbindung hat. Das heißt, Sie haben jederzeit konsistente Informationen über Ihre verschiedenen Termine in allen angebundenen Kalendern.



Informiert: Über eine eigene Schaltfläche informieren Sie Teilnehmer der Besprechung, dass Sie sich verspäten.

Neben dem Planungskonflikt sehen Sie an dieser Stelle auch die anderen Teilnehmer der Besprechung, den genauen Zeitpunkt und den Betreff. Ein Feature in Windows Phone 7 ist die Möglichkeit, andere Teilnehmer der Besprechung mit

einem Mausklick zu informieren. So können Sie im Kalender mit wenigen Klicks beispielsweise allen Teilnehmern einer Besprechung oder nur dem Organisator per E-Mail mitteilen, dass Sie zu spät kommen. Dazu steht in den Optionen des Termins im unteren Bereich eine eigene Schaltfläche zur Verfügung. Klicken Sie auf diese, können Sie sehr schnell eine E-Mail erstellen und die Teilnehmer mit wenigen Klicks über die Verspätung informieren. Eine weitere übersichtliche Funktion in Windows Phone 7 ist die Anzeige der nächsten Termine direkt auf dem Sperrbildschirm. Wenn Sie wissen wollen, wann der nächste Termin ansteht und wozu er dient, dürfen Sie das Gerät nicht entsperren.

6.6.6 Apps zur Terminverwaltung für Windows Phone 7

Der Kalender in Windows Phone 7 enthält schon sehr viele Funktionen und ist den Lösungen anderer Smartphone-Plattformen teils deutlich überlegen. Allerdings gibt es noch einige Erweiterungen, mit denen Sie die Terminverwaltung in Windows Phone 7 verbessern und die Übersichtlichkeit erhöhen können. Sie finden dazu im Marketplace verschiedene Apps.

Weekfinder – Kalenderwochen anzeigen

Die App *Weekfinder* behebt ein Manko in Windows Phone 7, das vor allem professionelle Anwender stört: fehlende Kalenderwochen und Wochennummern. Diese Anwendung steht kostenlos zur Verfügung. Leider kann auch diese App die Kalenderwochen nicht direkt im Kalender einblenden, sondern Sie müssen die Anwendung starten, ein Datum auswählen und sehen dann, in welcher Kalenderwoche sich das Datum befindet. Zusätzlich haben Sie die Möglichkeit, eine Wochennummer auszuwählen und zu schauen, welche Tage sich in der entsprechenden Woche befinden. In diesem Bereich gibt es zwar noch die App Kalenderwoche, allerdings unterstützt diese keine Vor- oder Rückschau und ist auch sonst nur bedingt brauchbar. Doch da die App kostenlos ist, spricht nichts gegen einen Test.

Ferien und Feiertage im Überblick

Mit der App *ferien+feiertage* bekommen Sie Feiertage und Ferien angezeigt, können diese aber nicht in den Windows-Phone-7-Kalender einbauen. Setzen Sie Windows Phone 7 zusammen mit Exchange ein, können Sie Feiertage auch mit Outlook in den Kalender integrieren. Da sich der Kalender in Windows Phone 7 mit Exchange synchronisiert, bekommen Sie auch auf diesem Weg die Termine in das Telefon. Eine Synchronisierung mit Outlook ist in Windows Phone 7 allerdings nicht integriert, Sie müssen entweder den Weg über Exchange gehen oder Outlook mit einem Google-Konto oder einem Windows Live-Konto synchronisieren. Im Kalender von Outlook lassen sich automatisch die deutschen Feiertage als ganztägige Ereignisse einfügen. Öffnen Sie dazu die Registerkarte *Datei* und klicken auf *Optionen/Kalender* und anschließend im Abschnitt *Kalenderoptionen* auf die Schaltfläche *Feiertage hinzufügen*. Anschließend können Sie auswählen, für

welches Land Sie Feiertage hinzufügen wollen. Leider steht keine Testversion zur Verfügung, Sie müssen die App für 0,99 Euro kaufen. Vor allem wenn Sie bei der Terminplanung auf Ferien Rücksicht nehmen müssen, ist die App extrem hilfreich. Zusätzlich gibt es noch die kostenlose App feiertage. Diese enthält allerdings keine Ferientermine, sondern nur die deutschen Feiertage. Leider sind auch diese derzeit nicht vollständig. Mit neuen Versionen ist aber zu erwarten, dass der Entwickler die noch fehlenden Feiertage (zum Beispiel Fronleichnam in Bayern und Hessen) noch nachträgt, sodass diese dann auch vollständig sind.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.

Das Blog von Thomas Joos finden Sie unter thomasjoos.wordpress.com.

TecChannel-Links zum Thema	Webcode	Compact
Praxis: Termine verwalten mit Windows Phone 7	2036685	S.295
Windows Phone 7 im Unternehmenseinsatz	2036115	S.255
Ratgeber: Windows Phone 7 für Admins	2036148	S.261
Praxis: Office Mobile in Windows Phone 7 nutzen	2036626	S.268
Windows-Phone-7-Praxis: Exchange-Anbindung und Zertifikate	2036585	S.280
Workshop – Versteckte Windows-Phone-7-Funktionen aktivieren	2036340	S.288
Windows Phone 7 im Unternehmen bereitstellen	2036982	S.301

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195.

6.7 Windows Phone 7 im Unternehmen bereitstellen

Wollen Unternehmen intern auf Windows Phone 7 setzen, gibt es mit Bordmitteln zunächst keine Möglichkeit, die Verteilung zu beschleunigen oder zu optimieren. Anders sieht es aus, wenn auch selbst entwickelte Anwendungen zur Verfügung gestellt werden sollen. Zwar sind auch in Windows Phone 7 durchaus Unternehmensfunktionen enthalten, allerdings lassen sich keine zentralen Images zur Verfügung stellen, wie zum Beispiel bei Windows 7. Verwaltungssoftware, mit der sich Smartphones auf Basis von Windows Phone 7 zentral im Unternehmen verwalten lassen, sucht man aktuell vergeblich.

Sehr gut gelungen sind bei Windows Phone 7 dafür die Anbindung an Exchange und der Office Hub mit Office Mobile. Da in den meisten Unternehmen die Anbindung an das E-Mail-System ausreicht, kann Windows Phone 7 im Vergleich mit der direkten Konkurrenz BlackBerry, Android und iPhone deutlich punkten.

6.7.1 Bereitstellung im Vergleich zu iOS und Android

Administratoren, die im Unternehmen iPhones verwalten müssen, finden bei Apple ausführliche Informationen zum Thema iPhone-Deployment im Unternehmen sowie den Download-Link zum iPhone-Konfigurationsprogramm und verschiedene Anleitungen (http://www.apple.com/de/support/iphone/enterprise/).

Hilfreich: iPhones lassen sich relativ einfach im Unternehmen zentral einrichten.

Mit dem Tool können Profile, die sich auf iPhones anwenden lassen, erstellt, verwaltet, verschlüsselt und bereitgestellt werden (siehe auch iPhone-Praxis: Einstellungen per Konfigurationsprogramm automatisieren, Webcode **2033060**). Diese

Profile enthalten verschiedene Einstellungen für iPhones. Ein solches Tool steht für Windows Phone 7 derzeit nicht zur Verfügung. Google bietet mit den kostenlosen Tool Google Apps Device Policy die Möglichkeit, Android-Handys mit Sicherheitsrichtlinien zu versorgen und Geräteadministratoren festzulegen. Google Apps Device Policy läuft dazu auf dem Endgerät als Systemdienst und tauscht sich mit einem Google-Server aus. Dort nehmen Administratoren die Einstellungen vor. Über den Server lassen sich Geräte bei Verlust auch löschen (Remote Wipe) – ein sehr wichtiges Feature für den Unternehmenseinsatz.

Praktisch: Android-Geräte lassen sich zentral mit Google Apps Device Policy verwalten.

Um Windows Phone 7 im Unternehmen bereitzustellen, steht kein spezielles Tool von Microsoft zur Verfügung. Idealerweise bereiten Sie die notwendigen Konfigurationsmaßnahmen vor der Verteilung der Geräte vor. Hier müssen Sie im Vorfeld beachten, auf welche Unternehmensressourcen Windows-Phone-7-Besitzer zugreifen sollen. Entsprechende Vorbereitungen sollten vor allem in den Bereichen Exchange, SharePoint oder auf anderen internen Webseiten getroffen werden. Mit der neuen Version des System Center Configuration Managers (SCCM) 2012 Beta 2 führt Microsoft einige wichtige Neuerungen in die Verwaltungssoftware ein. Neben Windows-Computern verwalten Administratoren jetzt auch Smartphones mit Windows Phone 7, iOS und Android. Allerdings ist die Beta-Version noch sehr im Funktionsumfang begrenzt. So können Sie Smartphones erst mit der endgültigen Version von SCCM 2012 oder sogar erst durch nachgereichte Patches verwalten. In der Betaversion fehlt diese Unterstützung. Es ist aber zu erwarten, dass Microsoft über die Systemverwaltungssoftware künftig auch Windows Phone 7 unterstützt.

6.7.2 Zertifikate für SSL-Verbindungen und für Exchange vorbereiten

Damit Windows-Phone 7-Anwender Zugriff auf verschlüsselte Webseiten und vor allem auf ihr Exchange-Postfach haben, sind einige Vorbereitungen zu treffen.

Ohne ein gültiges Zertifikat auf dem Smartphone ist eine Verbindung zu Exchange nicht möglich. Arbeiten Sie intern mit einer eigenen Zertifizierungsstelle oder einem selbst signierten Zertifikat von Exchange Server 2007/2010, müssen Sie einen Weg finden, dieses Zertifikat optimal an die Smartphones zu verteilen.

Simpel: So installieren Sie ein Zertifikat unter Windows Phone 7.

Im Gegensatz zu Windows Mobile 6 haben Sie in Windows Phone 7 keine Verwaltungskonsole mehr auf dem Smartphone, mit der Sie Zertifikate steuern können. Auch der Datenaustausch über eine SD-Karte oder ActiveSync mit dem lokalen Rechner ist nicht mehr möglich. Um Zertifikate auf den Smartphones mit Windows Phone 7 zu installieren, benötigen Anwender keine Administratorrechte. Es reicht aus, wenn diese Zugriff auf die Zertifikatedatei haben. Wird diese angeklickt, installiert Windows Phone 7 das Zertifikat automatisch. Der entscheidende Punkt ist, wie die entsprechenden Dateien auf die Endgeräte gelangen.

Hier gibt es grundsätzlich drei Möglichkeiten. Die erste besteht darin, dass Sie beispielsweise auf dem Windows-Phone-7-Gerät einfach ein E-Mail-Konto zu Windows Live einrichten. Schicken Sie an dieses Konto das Zertifikat, kann der Anwender die E-Mail herunterladen und die Datei mit dem Zertifikat einfach anklicken. Generell ist es, wie bei Android mit einem Google-Konto, in Windows Phone 7 notwendig, ein Windows Live-Konto einzurichten. Dabei muss nicht jeder Mitarbeiter sein eigenes Konto haben – er kann aber. Sie können auch ein Unternehmenskonto einrichten und auf allen Windows-Phone-7-Geräten zuweisen. Auf diese Weise können Sie schnell und einfach Dateien per E-Mail verteilen.

6.7.3 Exchange-Anbindung

Anschließend funktioniert die Anbindung an Exchange über die internen Assistenten in Windows Phone 7. Arbeiten Sie mit AutoDiscovery in Exchange Server 2007/2010, müssen Anwender nur noch ihre E-Mail-Adresse und ihr Kennwort eintragen. Den Rest findet das Smartphone automatisch.

Achten Sie aber darauf, dass Sie sowohl intern als auch über das Internet die AutoDiscovery-Funktion von Exchange einrichten müssen. Ohne AutoDiscovery müssen Anwender zusätzlich noch Servernamen und Domäne sowie den Anmeldenamen für die Domäne eintragen.

Mehr zum Hintergrund von AutoDiscovery finden Sie in Microsofts TechNet

(http://technet.microsoft.com/en-us/library/bb124251.aspx#works). Auf externen DNS-Servern sollte der Eintrag aus folgenden Daten bestehen:

- Service: *_autodiscover*
- Protocol: *_tcp*
- Port Number: *443*
- Host: <Externer DNS-Name, für den das Zertifikat gültig ist >

Wenn Windows Phone 7 einen Server finden will, sieht der Ablauf bei der Verbindung folgendermaßen aus – hier am Beispiel für die Domäne .contoso.com:

1. Autodiscover sucht nach *https://contoso.com/Autodiscover/Autodiscover.xml*.
2. Falls diese nicht gefunden wird, sucht Autodiscover nach *https://autodiscover.contoso.com/Autodiscover/Autodiscover.xml*.
3. Bleibt die Suche auch hier ergebnislos, stellt Autodiscover eine DNS-Abfrage nach dem SRV-Eintrag für *_autodiscover._tcp.contoso.com* und erhält die Antwort, auf welchem Server die Daten liegen.
4. Autodiscover lädt die Daten von *https://<Servername>/autodiscover/autodiscover.xml*.

Der zweite Weg, ein Zertifikat zu installieren, ist das Bereitstellen über eine Webseite. Diese muss der Anwender dann nur noch öffnen und kann das Zertifikat herunterladen. Dazu speichern Sie das Zertifikat am besten als .p7b-Datei im Webspace. Gibt der Anwender direkt die URL zur Zertifikatsdatei ein, erscheint in Windows Phone 7 bereits der Installationsassistent.

Die dritte Möglichkeit der Verteilung der Zertifikatdatei ist die Ablage in einem Online-Speicher wie Windows Live Sky Drive oder Dropbox. Anwender können dann über diesen Weg das Zertifikat auf das Smartphone herunterladen.

6.7.4 Exchange-ActiveSyc-Richtlinien konfigurieren

In Exchange sollten Sie darüber hinaus die Exchange-ActiveSync-Richtlinien für Windows Phone 7 optimieren. Diese rufen Endgeräte ab, wenn Sie sich mit dem Server verbinden.

Folgende Einstellungen lassen sich per Richtlinie auf die Geräte übertragen. Die Einstellungen müssen Sie direkt in der Exchange-Verwaltung vornehmen:

- Password Required
- Minimum Password Length
- Idle Timeout Frequency Value
- Device Wipe Threshold
- Allow Simple Password
- Password Expiration

- Password History

Andere Richtlinien, die Exchange-Server unterstützt, geben bei Windows Phone 7 immer den Wert True zurück:

- Disable Removable Storage
- Disable IrDA
- Disable Desktop Sync
- Block Remote Desktop
- Block Internet Sharing

Alle anderen Einstellungen die Exchange unterstützt geben den Wert False zurück. In einem TechNet-Artikel (http://social.technet.microsoft.com/wiki/contents/articles/exchange-activesync-considerations-when-using-windows-phone-7-clients.aspx) finden Sie ausführliche Informationen hierzu.

6.7.5 Office 365 und Windows Phone 7

Unternehmen, die auf Office 365 setzen, haben es relativ einfach, Windows Phone 7 anzubinden: Die Anwender müssen lediglich ihre E-Mail-Adresse und ihr Kennwort angeben; über AutoDiscovery findet Windows Phone 7 dann automatisch den Office-365-Server. Zertifikate müssen Sie ebenfalls nicht installieren, denn die verwendeten Zertifizierungsstellen sind in Windows Phone 7 bereits integriert. Mit dem kommenden Mango-Update von Windows Phone 7 wird die Zusammenarbeit mit Office 365 optimiert. Aktuell gibt es noch keine befriedigende Möglichkeit, die SharePoint-Seiten von Office 365 in den Office-Hub einzubinden. In der Testversion von Office 365 Enterprise lässt sich SharePoint über die Syntax *http://<Domänennamen>.sharepoint.com* anbinden, zum Beispiel *http://joos.sharepoint.com*. Allerdings funktioniert das aktuell in der Small Business-Version von Office 365 noch nicht; hier können Sie nur über den Browser zugreifen.

Generell fällt auf, dass Windows Phone 7 erst mit dem Mango-Update richtig fit gemacht wird für Unternehmen, denn erst mit diesem Update ist Multitasking für Apps möglich, und auch der Internet Explorer 9 und HTML5 halten erst mit dem Update Einzug in Windows Phone 7. Die direkten Konkurrenten können das schon lange. Wer allerdings intern auf Exchange und SharePoint setzt, findet in Windows Phone 7 ein gutes System für die E-Mail-Anbindung. Zwar können auch iPhones problemlos Termine aus Exchange abrufen, aber sie sind nicht in der Lage, diese zu bearbeiten oder gar Terminüberschneidungen aufzulösen. Wie bei Outlook, erscheinen Besprechungsanfragen auch in Windows Phone 7 im Kalender als Besprechungsanfrage, die sich einfach beantworten und bearbeiten lassen; außerdem können für Besprechungsanfragen andere Termine vorgeschlagen werden. Besprechungsanfragen zeigt das Smartphone bereits als vorläufig im Kalender an. Komplexe Kennwörter unterstützt Windows Phone 7 allerdings auch erst mit dem Mango-Update.

6.7.6 Eigene Apps zur Verfügung stellen

Unternehmen, die intern auf Windows Phone 7 setzen, wollen unter Umständen ihren Anwendern selbst entwickelte Apps zur Verfügung stellen, mit denen eine Datenverbindung zum internen Netzwerk aufgebaut werden kann.

Apps entwickeln Sie zum Beispiel mit dem kostenlosen Visual Studio 2010 Express for Windows Phone. Wer sich in das Thema Entwicklung von Anwendungen für Windows Phone 7 einarbeiten will, findet bei The Windows Club (www.thewindowsclub.com) ausführliche Anleitungen – auch für Anfänger. In verschiedenen Lektionen lesen Sie in diesem Tutorial, wie Sie Anwendungen für Windows Phone 7 erstellen und optimal verteilen (www.thewindowsclub.com/windows-phone-7-tutorial-series-building-deploying-wp7-apps).

Eine Übersicht zu den verschiedenen Tools und Ressourcen bietet Microsoft auf der Seite „In drei Schritten zur eigenen Windows Phone-Anwendung“ (http://msdn.microsoft.com/de-de/windowsphone/gg456294.aspx). Wer Code-Beispiele sucht, kann diese ebenfalls direkt bei Microsoft herunterladen (www.microsoft.com/download/en/details.aspx?id=11487). Ein wichtiger Anlaufpunkt für Entwickler ist der Entwickler-Blog (http://windowsteamblog.com/windows_phone/b/wpdev/) von Microsoft für Windows Phone 7.

6.7.7 Fazit

Zur Bereitstellung von Windows Phone 7 im Unternehmen bietet Microsoft aktuell noch keine Lösung an. Zwar soll diese mit dem neuen System Center Configuration Manager 2012 kommen, erfordert dann aber einiges an Investitionen. Allein für den Einsatz und die Verwaltung von Windows Phone 7 lohnt sich die Lizenzierung von SCCM 2012 nicht. Windows Phone 7 fehlen derzeit noch an zahlreichen Stellen Funktionen und Sicherheitseinstellungen, die die Wettbewerber mitbringen. Sollen die Anwender dagegen lediglich auf ihre E-Mails und unter Umständen noch auf SharePoint zugreifen, ist Windows Phone 7 der Konkurrenz durchaus gewachsen. Das gilt aber auch nur dann, wenn im Unternehmen Exchange und SharePoint in den aktuellen Versionen eingesetzt werden. In den meisten Unternehmen wird ohnehin eine heterogene Umgebung mit mehreren Smartphone-Plattformen existieren. Das liegt meistens daran, dass Anwender ihre private Smartphones auch an das Netzwerk einbinden wollen. Da die wichtigsten Geräte in diesem Bereich allesamt Exchange-ActiveSync-Richtlinien und Löschen über das Internet unterstützen – auch Windows Phone 7 –, lässt sich zumindest auf diesem Weg eine gewisse Sicherheit erreichen.

Windows-Phone-7-Geräte zentral verwalten und überprüfen, welche Apps die Anwender installieren – diese Aufgabe ist für Administratoren derzeit unlösbar.

Thomas Joos

7 iPad und iPad 2

Von Apples iPad, dem Wunder-Tablet, wurde nicht weniger erwartet, als dass es die Computerwelt revolutioniert und den Medienkonsum verändert. Bei so hohen Erwartungen sind für viele sogar die nur geringfügigen Verbesserungen der zweiten iPad-Generation gegenüber dem Ursprungsmodell zu verzeihen. In diesem Kapitel widmen wir uns ausführlich den Neuerungen des iPad 2.

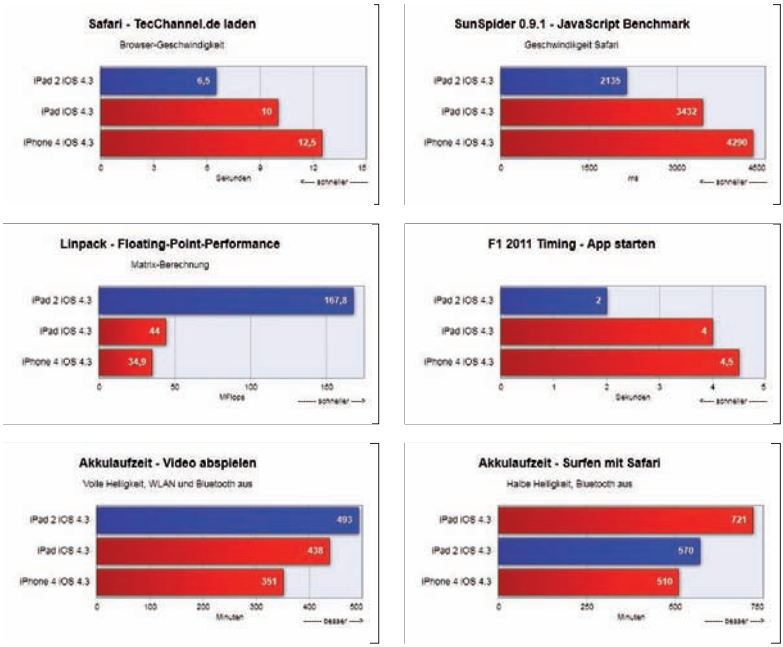
7.1 Test – Lohnt der Umstieg von Apple iPad auf iPad 2?

Seit 25. März 2011 ist das iPad 2 in Deutschland verfügbar. Der Ansturm war und ist ungebrochen hoch – lange Wartezeiten bei Bestellungen sind keine Seltenheit. Für viele Besitzer des bisherigen iPads ein Grund, schon deshalb erst einmal abzuwarten. Und viele iPad-Eigner stellen sich zudem die Frage, ob das neue iPad 2 für sie überhaupt Vorteile bringt. Und immerhin wären mindestens 479 Euro zu investieren. Die Frage, ob sich ein Umstieg lohnt, ist mehr als gerechtfertigt. Schließlich besitzen beide Tablets den gleichen Formfaktor. Das 9,7-Zoll-Display löst jeweils 1024 mal 768 Bildpunkte auf. Auch arbeiten iPad und iPad 2 mit dem identischen Betriebssystem iOS. Der auffälligste Unterschied in den Features sind die integrierten Kameras beim iPad 2.

Apple iPad 2: Die zweite Generation besitzt den gleichen Formfaktor mit 9,7-Zoll-Display wie das erste iPad. Wie die Apps auf dem Bildschirm zeigen, hat Apple im iPad 2 aber Kameras integriert.

Im Inneren des iPad 2 werkelt mit dem A5 mit 1 GHz Taktfrequenz und Dual-Core-Technologie allerdings ein leistungsfähigerer Prozessor als der einkernige 1-GHz-A4 des iPad. Zudem spendiert Apple der zweiten Tablet-Generation einen

auf 512 MByte verdoppelten Arbeitsspeicher. Damit steigt die gemessene Performance deutlich, wie die Messergebnisse zeigen:



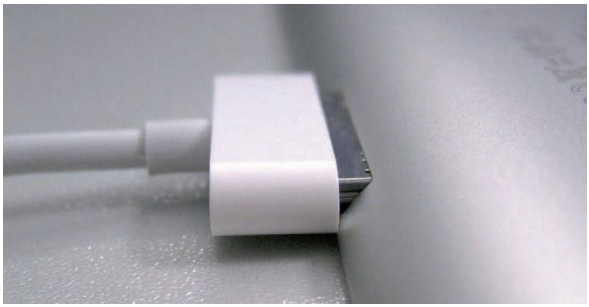
Der Unterschied in den Messergebnissen ist allerdings nur die eine Seite. Die andere Seite ist, dass bereits das erste iPad im Praxisbetrieb (Webcode **2027815**) wenig Anlass zu Klagen in Bezug auf die Geschwindigkeit gibt. Wir zeigen Ihnen, welche Vorteile der Umstieg auf das iPad 2 im täglichen Praxiseinsatz mit sich bringt.

7.1.1 Geänderte Haptik, Bedienelemente und Gewicht

Beim ersten Anfassen des iPad 2 fällt sofort auf, dass das Gerät angenehm in der Hand liegt. Denn harte Kanten sucht man beim iPad 2 vergeblich. Die seitlichen Gehäuseflächen sind jetzt schräg, und auch die „Kante" zum Display ist abgerundet. Dadurch schmeichelt das iPad 2 den Händen noch deutlich mehr als das iPad. Die Bedienelemente des iPad 2 entsprechen in Funktion und Anzahl dem Vorgänger. Jedoch fühlt sich der Home-Button beim Drücken mit leiserem Klick und etwas weicherem Anschlag angenehmer an. Durch die schrägen Außenflächen des Gehäuses sind die Wippe für die Lautstärke, der Sperrknopf sowie der Ein-/Ausschalter ein wenig „versteckt" angebracht.

Angenehm: Beim iPad 2 sind die Kanten im Gehäuse angenehmen Rundungen gewichen.

Dadurch lassen sie sich weniger gut erreichen als beim iPad. Natürlich handelt es sich hier um Meckern auf hohem Niveau, aber die Bedienbarkeit hat sich hier leicht verschlechtert. Insbesondere, wenn das iPad 2 auf dem Tisch liegt, sind die Tasten zu sehr versteckt. Auch der Stecker des Dockingkabels und der Kopfhörerstecker schließen nicht bündig mit den Buchsen am iPad 2 ab.



Hakelig: Der Stecker des Dockingkabels schließt nicht bündig mit der Buchse am iPad 2 ab. Das Einstecken ist deshalb oft schwierig.

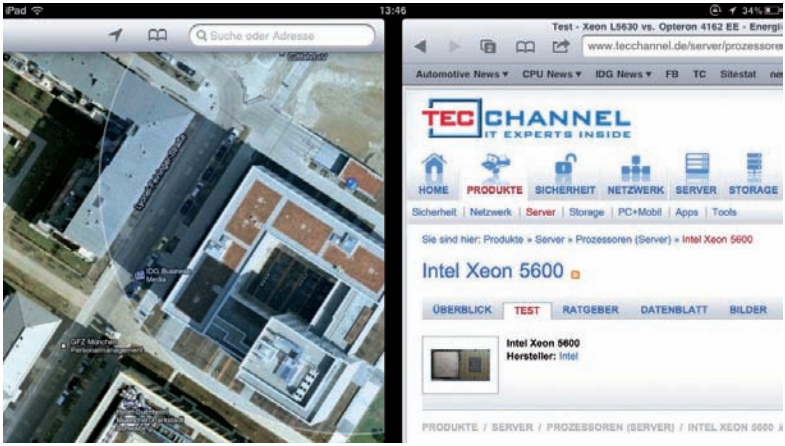
Apples iPad 2 wiegt mit 601 (Wi-Fi) beziehungsweise 613 Gramm (Wi-Fi + 3G) im Vergleich zum iPad 79 (Wi-Fi) oder 117 Gramm (Wi-Fi + 3G) weniger. Das geringere Gewicht klingt in der Theorie sehr wenig und als kaum bemerkbar. In der Praxis macht sich die Schlankheitskur des iPad 2 aber angenehm bemerkbar: Es fühlt sich deutlich leichter an und lässt sich besonders einhändig länger ohne Anstrengung halten.

Beim Einschalten des iPad 2 macht sich noch das hellere Display angenehm bemerkbar. Durch die hohe Leuchtkraft wirken die Farben noch intensiver und klarer als beim bereits guten iPad-Display. Mit gemessenen 350 cd/m² ist der iPad-2-Bildschirm um 27 Prozent heller als der des iPad mit ermittelten 275 cd/m².

7.1.2 Unterschiede: Geschwindigkeit und Akku-Laufzeit

Die Rechenleistung des iPad 2 ist durch den Dual-Core-Prozessor A5 mit seinen Architekturverbesserungen deutlich gestiegen, wie Sie in der Galerie mit den Testergebnissen auf der Seite 308 sehen können. Im typischen Praxisbetrieb entscheiden aber mehr die „gefühlte" Geschwindigkeit sowie die Reaktionszeiten beim Auslösen von Aktionen.

Während das iPad bereits sehr flink bei fast allen Aktionen agiert und wenig Anlass zu Kritik gibt, zeigt sich beim direkten Vergleich mit dem iPad 2 doch noch ein merklicher Unterschied. So starten die Apps meist deutlich flinker. Apples Numbers beispielsweise benötigt bis zum Anzeigen des Startbildschirms mit den verfügbaren Dokumenten zirka zwei Sekunden, beim iPad verstreichen rund drei Sekunden. Bei Pages ist ein ähnlicher Zeitunterschied festzustellen: Die F1 2011 Timing App startet auf dem iPad 2 nach zwei Sekunden, beim iPad dauert der Vorgang vier Sekunden. Auch der Aufruf von Videos, beispielsweise in einem eMagazin wie Jaguar Issue 1 / 2011, geht beim iPad 2 mit einer statt zwei Sekunden Verzögerung flinker vonstatten. Wird beispielsweise ein pdf in iBooks geschlossen, so erfolgt der Vorgang beim iPad 2 nahezu verzögerungsfrei, während es beim iPad meist eine kurze Wartezeit von einer guten Sekunde gibt.



Flinker: Beim Wechsel zwischen Apps agiert das iPad 2 ein wenig flotter. Inhalte werden durch den größeren Arbeitsspeicher weniger oft nachgeladen.

Die aufgezeigten Unterschiede werden vor allem dann sehr deutlich, wenn bei den Tablets schon sehr viele Apps seit dem letzten kompletten Neustart geöffnet wurden. Der Arbeitsspeicher ist dann überwiegend belegt – ein typisches Praxisszenario. Wird iOS auf iPad und iPad 2 neu gestartet, dann sind die Zeitunterschiede bei den ersten geöffneten Apps geringer.

Wird mit aktivierten Multitasking-Gesten (Webcode **2034903**) mit den Fingern durch die offenen Apps gewischt, so gibt es beim iPad 2 seltener ein „Hakeln“, und Inhalte stehen öfter sofort zur Verfügung. Beim Scrollen von aufwendigen langen Webseiten mit vielen Bildelementen in Safari ist das iPad 2 ebenfalls im Vorteil: Der Inhalt steht viel häufiger sofort zur Verfügung im Gegensatz zu den grauen Flächen, wo der Content erst nachgeladen wird.

Trotz der höheren Leistung und Displayhelligkeit müssen bei der Akku-Laufzeit – je nach Einsatz – keine Abstriche gemacht werden. Beim Abspielen von Videos mit maximaler Helligkeit (WLAN deaktiviert) hält das iPad 2 sehr gute 8,2 Stunden durch, Apples iPad schafft bei dunklerem Display „nur“ 7,3 Stunden. Konträr verhält es sich beim Surfen mit Safari via WLAN (Helligkeit auf 50 Prozent): Das iPad 2 hält erneut sehr gute 9,5 Stunden durch, der Vorgänger aber sogar 12 Stunden.

7.1.3 Smart Cover – geringer Praxisnutzen

Als Zubehör für das iPad 2 bietet Apple das Smart Cover an. Die Schutzklappe gibt es aus Kunststoff (39 Euro) oder Leder (69 Euro). Man klippt das Smart Cover per Magnet an das iPad-2-Gehäuse – für das iPad ist es nicht geeignet. Faltet man das Smart Cover, so dient es als Ständer fürs iPad 2. In den Einstellungen des iPad 2 findet sich der neue Eintrag „iPad-Hülle verriegeln / entriegeln“. Hier wird festgelegt, ob sich das iPad 2 beim Auflegen und Entfernen des Smart Covers automatisch aus- und einschaltet. Zu Beginn mutet das automatische Einschalten beim Aufklappen ganz praktisch an, doch es kann schnell nerven. Denn sehr oft rutscht während des Aufklappens der Daumen, der das iPad 2 festhält, auf das Display und kann ungewollte Aktionen auslösen. Im Testbetrieb wurde solch eine in Bearbeitung befindliche, noch unfertige E-Mail verschickt, weil der Daumen beim Öffnen des Smart Covers ungewollt den Sendeknopf berührte.

Automatisch: In den Einstellungen des iPad 2 findet sich der neue Eintrag „iPad-Hülle verriegeln / entriegeln“. Hier wird festgelegt, ob sich das iPad 2 beim Auflegen und Entfernen des Smart Covers automatisch aus- und einschaltet.

Ist das Smart Cover zum Arbeiten umgeklappt auf der Hinterseite des iPad 2, so lässt sich das Tablet unbequemer halten. Im Hochformat gehalten sticht das Metallgelenk des Smart Covers in die Handinnenseite. Wird das iPad 2 im Querformat benutzt, so nervt das von der Rückseite immer wieder wegklappende Smart Cover. Hier wäre ein ebenfalls magnetischer Effekt wünschenswert, damit es an der Rückseite „kleben" bleibt. Mit dem umgeklappten Smart Cover auf der Rückseite verschwindet auch der angenehme handschmeichelnde Effekt beim Halten des iPad 2.

Unangenehm: Ist das Smart Cover zum Arbeiten umgeklappt auf der Hinterseite des iPad 2, so lässt sich das Tablet weitaus weniger bequem halten. Im Hochformat sticht das Metallgelenk des Smart Covers in die Handinnenseite.

Ein Vorteil des Smartcovers ist dagegen der Reinigungseffekt beim Display, wenn das Cover geschlossen ist. Sobald das iPad 2 dann gehalten wird, bewegt sich die Cover-Innenseite leicht auf dem Glas des Displays. Dadurch wirkt der Bildschirm des iPad 2 nach dem Aufklappen sofort klarer und sauberer als beim iPad. Allerdings sammelt sich auch unter dem Smart Cover entlang der Biegestellen Staub.

Leider schützt das Smart Cover aber nur sehr bedingt vor Kratzern, denn eine Seite des Tablets ist immer ungeschützt. Wer sein iPad 2 viel in Aktentaschen, Rucksäcken oder Ähnlichem mitnimmt, sollte lieber eine richtige Schutzhülle verwenden.

7.1.4 Integrierte Kameras – eingeschränkte Funktionalität

Apple integriert beim iPad 2 auf der Gehäuserückseite eine Kamera für Schnappschüsse. Die 0,7-Megapixel-Kamera bietet eine Auflösung von 960 mal 720 Bildpunkten. Bei guten Lichtverhältnissen gelingen zwar brauchbare Aufnahmen, durch die geringe Auflösung sind die Bilder aber bereits beim Betrachten auf dem iPad 2 pixelig. Bei Kunstlicht oder geringem Umgebungslicht zeigen die Fotos ein starkes Rauschen und wirken unscharf. Jedes halbwegs aktuelle Smartphone eignet sich zum Fotografieren besser als die Kamera des iPad 2.

Nur für Schnappschüsse: Die 0,7-Megapixel-Kamera auf der Rückseite des iPad 2 bietet eine Auflösung von nur 960 mal 720 Bildpunkten. Schon in der Vorschau der Kamera-App zeigt sich die geringe Qualität der Kamera.

Ein wenig schärfer, aber ebenfalls mit einem deutlichen Hang zum Farbstich, fallen die Videos aus, die die Kamera mit 720p-Auflösung anfertigt. Für gelegentliche Videoaufnahmen ohne Anspruch reicht die Qualität, für mehr aber nicht. Für die Frontkamera mit 0,3 Megapixeln und 640 mal 480 Bildpunkten Auflösung muss der Qualitätsanspruch bei Bildern und Videos nochmals gesenkt werden.

Generell sollte man die integrierten Kameras des iPad 2 nur für Video-Chat via Facetime oder Skype verwenden. Hierfür reicht die Qualität einigermaßen aus.

7.1.5 Datenübernahme von iPad auf iPad 2

Wer bereits ein iPad besitzt und auf das iPad 2 wechseln will, dem stellt sich die Frage nach der Möglichkeit der Übernahme von Daten, Apps und Einstellungen auf das neue Gerät. iTunes bietet hierfür die entsprechende Möglichkeit. Bevor Sie aber das iPad 2 einrichten, sollten Sie von Ihrem bisherigen iPad ein Backup anlegen. Ein Backup lässt sich bei iTunes jederzeit manuell starten. Wählen Sie in der Medienspalte unter Geräte das angeschlossene iPad mit der rechten Maustaste aus und rufen im Kontextmenü „Sichern“ auf. Das Backup sichert neben den installierten Apps und deren Einstellungen die Konfiguration des iPad sowie die eigenen gesicherten Bilder. Auch die von installierten Apps gespeicherten Daten sowie die in den Freigabeordnern von iTunes abgelegten Inhalte werden gesichert.

Wird das neue iPad 2 erstmals an iTunes angeschlossen, so bietet das Programm die Wahl zwischen dem Einrichten als komplett neues Gerät oder der Datenübernahme vom iPad. Hier können Sie nun von den durchgeführten iPad-Backups das aktuelle auswählen. Nach dem Zurückspielen des iPad-Backups besitzt das iPad 2 aber auch den Namen des iPad. Über zwei Mausklicks in iTunes auf das iPad 2 in der Medienspalte lässt sich das neue Tablet aber wieder beliebig umbenennen. So-

wohl das iPad als auch das iPad 2 lassen sich nun unabhängig voneinander mit iTunes synchronisieren und sichern.

Ausgeschlossen von der Datenübernahme sind spezielle auf dem iPad installierte Konfigurationsprofile für Exchange oder Notes. Diese Profile werden meist für die Nutzung der Firmen-Accounts auf dem iPad benötigt. Beim iPad 2 müssen hier entsprechende Profile neu installiert werden.

7.1.6 Fazit

Nach umfangreichen Praxistests und wochenlangem parallelen Arbeiten mit iPad und iPad 2 fällt die Antwort auf die Frage, ob sich der Umstieg lohnt, eindeutig aus: Nein. Natürlich funktioniert das Arbeiten auf dem iPad 2 nochmals etwas flinker als mit dem iPad. Und ja, das neue Tablet schmeichelt den Händen noch mehr, und es ist etwas leichter. Doch man sollte sich bewusst sein, hier werden subtile Unterschiede auf hohem Niveau beschrieben.

Denn nach wie vor zählt das erste iPad zu den besten auf dem Markt erhältlichen Tablets. Die Geschwindigkeit und die flüssige Bedienung geben kaum Grund zum Nörgeln. Die Vorteile des iPad 2 in Gestalt des Dual-Core-Prozessors und des größeren Arbeitsspeichers fallen erst beim intensiven Arbeiten mit vielen Apps und beim direkten Vergleich mit dem iPad auf. Auch das noch hellere Display des iPad 2 wird erst im direkten Vergleich als besser eingeschätzt. Erfreulicherweise wird die höhere Leistung und Helligkeit des Displays beim iPad 2 nicht mit kürzeren Akku-Laufzeiten erkauft. Wer unbedingt Videotelefonie mit seinem iPad machen will, der muss auf die zweite Generation umsteigen. Allerdings sollten an die Kameraqualität keine hohen Ansprüche gestellt werden. Und Gimmicks wie das Smart Cover sollten Sie sich vor dem Kauf genau ansehen, ob es wirklich sinnvoll ist – aus unserer Sicht ist es das nicht.

Christian Vilsbeck

Christian Vilsbeck ist als Hardware-Redakteur bei TecChannel tätig. Der Dipl.-Ing. (FH) der Elektrotechnik, Fachrichtung Mikroelektronik, blickt auf längjährige Erfahrungen im Umgang mit Mikroprozessoren zurück. Außerdem betreut der vor seiner Fachredakteurslaufbahn als Laboringenieur tätige Experte das Themenfeld Storage und führt Tests von Festplatten und NAS-Systemen durch.

TecChannel-Links zum Thema	Webcode	Compact
Test – Lohnt der Umstieg von Apple iPad auf iPad 2?	2035275	S.307
Apple iPad 2 bringt neue Probleme	2034575	S.315

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195

7.2 Apple iPad 2 bringt neue Probleme

Viele IT-Chefs haben im Stillen vielleicht darauf gehofft, dass der Hype ums iPad endlich bald vorbei ist und sie sich wieder den wichtigen Dingen des Lebens widmen können. Aber der Tablet-PC von Apple beweist mehr Standvermögen, als ihm viele Analysten zugetraut haben. Es hilft nichts: Die Unternehmens-IT wird sich auch künftig mit den Dingen auseinandersetzen müssen, die Apple über die Welt ausschüttet: iPad, iPad 2, iPhone, Apps und vielleicht demnächst auch noch Macbooks und iMacs. Daher gibt es zurzeit keine Alternative: Managen Sie das iPad (2), bevor der Tablet-PC Sie verwaltet.

Aber was heißt das eigentlich nun genau? Charles Edge, Autor eines Enterprise-iPhone- und iPad-Guides, sieht zwei Probleme: die massenhafte Auslieferung von iPads und iPhones im Unternehmen sowie das Zuteilen von Unternehmensdaten an die richtige Person und wieder zurück in den Unternehmensserver.

7.2.1 Konfiguration aufwendiger

Das traditionelle Roll-out von Geräten und Anwendungen über vorkonfigurierte Images funktioniert bei den Apple-Geräten nun mal nicht so ohne Weiteres. Stattdessen müssen CIOs über das iPhone-Konfigurationsprogramm oder mit Tools von Drittanbietern einzeln für jedes Gerät spezifische Profile für unterschiedliche Nutzer erstellen. Aber, so Edge, dabei würden es viele Unternehmen an Verständnis für die Bedürfnisse der Mitarbeiter mangeln lassen.

Zudem interagiert das iPad anschließend nicht so mit den Unternehmensservern, wie man es von Laptops und Desktop-PCs gewohnt ist. Daher müssen sich die Admins auch damit beschäftigen, wie das iPad und seine Apps kommunizieren, wie man Inhalte aufs iPad bekommt und dort ändern kann, um sie anschließend mit dem Firmennetz zu synchronisieren.

7.2.2 Zu strikte Regeln könnten User-Revolte auslösen

Zu Beginn müssen IT-Abteilungen Policies für den Zugriff, die Authentifizierung und die Sicherheit der iPads definieren. Anschließend müssen diese Policies über den Roll-out der iPad in die Geräte implementiert werden. Als Administrator neigt man dazu, strikte Regeln für den Umgang mit dem Tablet-PC zu definieren, um Sicherheit und Integrität von Daten garantieren zu können. Aber hier ist Vorsicht geboten: Die Benutzer des iPad akzeptieren Einschränkungen ihrer gerade neu gewonnenen Freiheit nur schwer. So könnte es zum Beispiel unklug sein, den Zugang zum App-Store von Apple oder das Speichern von Daten in den Geräten zu beschränken. Im schlimmsten Falle provoziere man damit eine „User-Revolte", warnt Edge. Der Mobile-Experte widerspricht in diesem Zusammenhang den Sicherheitsbedenkenträgern: „Wir hatten bei den unterschiedlichen Typen von SSL-Zer-

tifikaten ein paar Hürden zu überwinden. Aber alles in allem war es kein Problem, die Sicherheitsstandards der meisten Unternehmen dort abzubilden."

Mit dem iPad 2 gibt es zudem ein neues Thema. Das superschnelle und ultraflache Tablet ist längst in den Apple-Läden zu kaufen und wird auf Dauer das Original-Pad ablösen. Das iPad 2 hat jeweils eine Kamera an Vorder- und Rückseite und ist mit der FaceTime-App uneingeschränkt für Videokonferenzen einsetzbar.

7.2.3 FaceTime schluckt Netzwerkkapazitäten

„FaceTime wird bei vielen Unternehmen Anklang finden, weil sie sehen, wie leicht es ist, in das Thema Videokonferenzen einzusteigen", meint Dan Hays von der Beratungsfirma PRTM. Das mag aus Sicht euphorisierter Chefs stimmen, aber IT-Abteilungen fürchten dabei sofort um ihre Netzwerkkapazitäten und Bandbreiten, die mit einem drastisch erhöhten Datendurchsatz umgehen müssen.

Videokonferenzen werden sie mit diesen Bedenken allerdings ebenso wenig stoppen können wie das iPad in Gänze. Die korrekte Antwort auf die Frage nach den Bandbreiten lautet daher: Das Netzwerk sollte dazu in der Lage sein.

Tom Kaneshige, Thomas Pelkmann

Der Artikel erschien zuerst bei unseren Kollegen von CIO.com und CIO.de.

TecChannel-Links zum Thema	Webcode	Compact
Ratgeber: Das iPad im professionellen Einsatz	2036988	S.329
Test – Lohnt der Umstieg von Apple iPad auf iPad 2?	2035275	S.307
Apple iPad 2 bringt neue Probleme	2034575	S.315
Workshop – Drucken mit iPhone und iPad	2036536	S.317
Workshop – Apple iPad sicher betreiben	2036859	S.321
Test: Apple iPad mit iOS 5	2036977	S.339

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195

7.3 Workshop – Drucken mit iPhone und iPad

Auch wenn Smartphones und Tablets-PCs wie iPhone, iPad, Windows Phone 7, Android-Geräte und Co. immer mehr Aufgaben von herkömmlichen Computern übernehmen, lassen sich nicht alle Funktionen genauso problemlos nutzen wie am Desktop. Ein häufiges Problem ist das Drucken von Dateien über das Smartphone. Während auf PCs einfach das Installieren eines Druckertreibers ausreicht, funktioniert dieser einfache Weg bei Smartphones nicht.

Drucker lassen sich per USB auch nicht so einfach an Smartphones anschließen, sodass Sie bei den verschiedenen Systemen zu Tricks greifen müssen, um zu drucken. Für iPhone und iPad gibt es seit iOS 4.2 die Funktion AirPrint. Diese erlaubt das Drucken über WLAN, offiziell aber nur auf ausgewählten HP-Druckern. Wir zeigen Ihnen, wie Sie diese Funktion trotzdem auch für andere Drucker nutzen können, und das vollkommen kostenlos. Die hier vorgestellten Möglichkeiten funktionieren für das iPhone 4 sowie das iPad und iPad 2.

7.3.1 Drucken mit iPhone und iPad – AirPrint offiziell nutzen

Apple hat ab iOS 4.2 die neue AirPrint-Funktion integriert, mit dem sich viele HP-Drucker direkt über iPhones und iPads ansprechen lassen. Um diese Funktion zu nutzen, ist keine Installation notwendig, und Sie brauchen den Drucker nicht mit den Endgeräten zu verbinden. Auch muss auf den iOS-Geräten nichts installiert werden. Wählen Sie ganz einfach die Weiterleiten-Funktion aus und starten den Druck. Anschließend scannt das iPhone/iPad das Netzwerk auf kompatible Drucker und bietet eine Druckerauswahl an. Den Druckauftrag sendet das Gerät über WLAN direkt an den Drucker. Sie benötigen dazu keine App und auch keinen Druckerserver, denn in den einzelnen HP-Druckern ist die Funktion direkt integriert. Alle Apps, die eine interne Druckfunktion haben, können AirPrint nutzen. Allerdings unterstützen ausschließlich HP-Drucker AirPrint, und auch hier nicht alle. Der Drucker muss WLAN unterstützen und per AirPrint erreichbar sein. Das sind aktuell folgende Drucker:

- HP Envy 100 eAll-in-One Drucker (D410a)
- HP Photosmart Plus e-AiO (B210a)
- HP Photosmart Premium e-AiO (C310a)
- HP Photosmart Premium Fax e-AiO (C410a)
- HP Photosmarte-AiO (B110)
- HP PhotosmarteStation (C510)
- HP LaserJet Pro M1536dnf Multifunktionsdrucker

- HP LaserJet Pro CM1415fn Multifunktions-Farbdrucker
- HP LaserJet Pro CM1415fnw Multifunktions-Farbdrucker
- HP LaserJet Pro CP1525n Farbdrucker
- HP LaserJet Pro CP1525nw Farbdrucker
- HP Officejet 6500A e-AiO
- HP Officejet 6500A Plus e-AiO
- HP Officejet 7500A Wide Format e-AiO
- HP Officejet Pro 8500A e-AiO
- HP Officejet Pro 8500A Premium e-AiO
- HP Officejet Pro 8500A Plus e-AiO

Beabsichtigen Sie also, mit Ihrem iPhone oder iPad zu drucken, sollten Sie sicherstellen, dass Ihr neuer Drucker diese Funktion beherrscht. Denn auf diesem Weg können Sie am einfachsten mit iPhone/iPad drucken, ohne irgendwas installieren und konfigurieren zu müssen. HP erweitert die Druckerversionen ständig, die AirPrint unterstützen. Einige Drucker erhalten zum Beispiel per Firmware-Update die AirPrint-Funktion. Überprüfen Sie daher bei HP, ob eine neue Firmware für Ihren Drucker zur Verfügung steht.

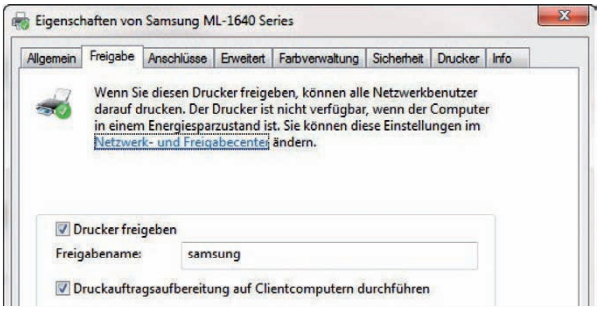
7.3.2 AirPrint für alle Drucker nutzen

Findige Programmierer haben ein Tool für Mac OS X und Windows entwickelt, mit dem Sie AirPrint auch für andere Drucker nutzen können. Dazu müssen Sie den Drucker auf dem Mac freigeben und iTunes gestartet haben. Zusätzlich installieren Sie auf dem Mac noch das Tool AirPrintActivator (http://netputing.com/airprintactivator). Das Tool steht auch für Windows zur Verfügung.

Damit Sie Drucker über AirPrint ansprechen können, müssen Sie das aktuelle iTunes auf dem PC installieren, sich zum Drucken mit einem Benutzerkonto authentifizieren und darauf achten, dem Benutzerkonto, mit dem Sie drucken wollen, ein Kennwort zuzuteilen. Das gilt für Mac OS X und für Windows gleichermaßen. Außerdem muss sich der PC im selben Netzwerk (Subnetz) befinden wie das iPhone/iPad. Hier reicht aber auch eine Verbindung mit LAN, der PC muss nicht per WLAN verbunden sein, das iPhone/iPad dagegen schon. Das iPhone/iPad muss daher mit WLAN verbunden sein und per DHCP eine IP-Adresse erhalten. Um AirPrint in Windows zu aktivieren, gehen Sie folgendermaßen vor:

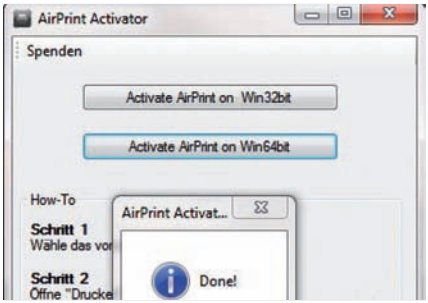
1. Klicken Sie auf *Start\Geräte* und *Drucker*.
2. Klicken Sie mit der rechten Maustaste auf den Drucker und wählen Sie *Druckereigenschaften*.
3. Wechseln Sie auf die Registerkarte *Freigabe*.
4. Stellen Sie sicher, dass die Option *Drucker freigeben* aktiviert und ein

Freigabename festgelegt ist. Sie müssen keine Änderungen vornehmen, wenn Sie den Drucker ohnehin freigegeben haben.



Drucken mit iPhone und iPad: Freigeben eines Druckers für AirPrint.

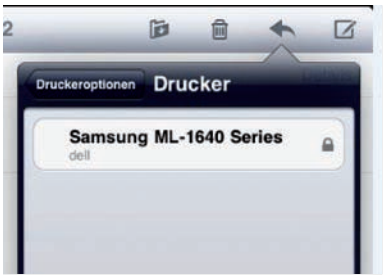
5. Klicken Sie mit der rechten Maustaste auf die heruntergeladene Datei *AirPrint_Activator.exe* und wählen *Als Administrator ausführen*.
6. Klicken Sie anschließend auf die Schaltfläche der Betriebssystemversion, die Sie installiert haben. Sie erhalten eine positive Rückmeldung der Installation.
7. Klicken Sie auf *Start\Systemsteuerung\System und Sicherheit\ Windows-Firewall*.
8. Klicken Sie auf der linken Seite auf *Ein Programm oder Feature durch die Windows-Firewall zulassen*.
9. Klicken Sie auf *Anderes Programm zulassen* und wählen Sie die Datei *Airprint.exe* im Verzeichnis *C:\Program Files (x86)\AirPrint* (64-Bit) oder *C:\ Program Files\AirPrint* (32-Bit) aus.



Drucken mit iPhone und iPad: AirPrintActivator starten.

10. Klicken Sie auf *OK*, damit das Programm im Netzwerk kommunizieren darf.
11. Wählen Sie die Druckfunktion in der App. Im E-Mail-Bereich wählen Sie zum Beispiel die *Weiterleiten-Funktion* und dann *Drucken*.

12. Wählen Sie *Drucker auswählen*.
13. Die freigegebenen Drucker müssten jetzt erscheinen.
14. Anschließend erscheint ein Authentifizierungsfenster, und Sie müssen sich am PC anmelden auf dem Sie ausdrucken wollen.
15. Anschließend können Sie die Optionen für den Druck auswählen und den Druck starten.



Drucken mit iPhone und iPad: Auswählen des Druckers auf dem iPhone/iPad.

16. Haben Sie den Druck gestartet, sendet das iPhone/iPad diesen an den PC, an dem Sie den Drucker freigegeben und iTunes gestartet haben.

7.3.3 Drucken mit Apps

Zusätzlich zu AirPrint bietet HP Apps an, die vor allem das Ausdrucken von Fotos deutlich verbessern. Eine solche App ist HP iPrintPhoto 3.0. Die App kann Fotos auch bearbeiten und ermöglicht verbesserte Druckoptionen. Aber auch hier muss der Drucker per WLAN mit dem Netzwerk verbunden sein. Für das iPad gibt es eine eigene Version. Setzen Sie das iPhone ein, stehen für HP-Drucker noch weitere Apps zur Verfügung.

Auch mit Tricks können Sie über AirPrint nur im lokalen Netzwerk drucken, nicht über das Internet. HP stellt aber noch die App HP ePrintservice zur Verfügung (http://itunes.apple.com/de/app/hp-eprint-service/id424306797), mit der einige ausgewählte Drucker auch über das Internet angesprochen werden können. Auch hier sollten Sie vor dem Kauf Informationen einholen, ob Ihr Drucker das kann. Eventuell gibt es hier ebenfalls Firmware-Updates.

Leider sind nicht alle Druckerhersteller so gründlich wie HP und bieten entsprechende Apps an. Samsung offeriert mit der App Samsung Mobile Print ebenfalls eine App (http://itunes.apple.com/de/app/samsung-mobile-print/id429611283), die verbessertes Drucken ermöglicht. Allerdings unterstützt diese nur die aktuellsten Top-Drucker.

Thomas Joos

7.4 Workshop – Apple iPad sicher betreiben

Tablets wie das iPad oder sein Nachfolger iPad 2 sind bei vielen bereits ein stetiger Begleiter. Die Gefahr, das Tablet unbeaufsichtigt liegen zu lassen oder zu verlieren, ist latent gegeben. Wenn die Daten dann in falsche Hände geraten, ist der Schaden schnell groß. Da auf dem Gerät oft auch sensible Zugangsdaten gespeichert sind, tut jeder Anwender gut daran, sich Gedanken über die Sicherheit zu machen. Durch die vielfältigen Apps und Standardmittel, die im Appstore zur Verfügung stehen, lassen sich auf iPads auch problemlos alle Arten von Daten im Netzwerk speichern, zum Beispiel komplette SharePoint-Bibliotheken, inklusive Offline-Versionen der Dokumente. Wenn ein iPad verloren geht, kann der Finder auf alle Daten des Gerätes zugreifen. Administratoren müssen daher auch die Anwender dafür sensibilisieren, das Gerät so sicher wie möglich zu betreiben.

7.4.1 Sicherheit mit Bordmitteln erhöhen: Code-Sperre aktivieren

Die Sicherheit beim Einsatz des iPads lässt sich schon mit Bordmitteln deutlich erhöhen, ohne dass irgendeine App installiert sein muss. Aus diesem Grund ist jedem Anwender anzuraten, sich bei der Anschaffung des iPads zunächst die Sicherheitseinstellungen anzusehen und optimal anzupassen.

In Unternehmen können auch Administratoren die Sicherheitseinstellungen vorgeben und durch ein Kennwort vor Änderungen schützen. Der erste Schritt besteht darin, Einstellungen\Allgemein aufzurufen. Hier finden sich drei wichtige Sicherheitseinstellungen, die besonderer Betrachtung bedürfen und standardmäßig nicht optimal eingestellt sind:

- Automatische Sperre
- Code-Sperre
- Einschränkungen

Bitte ändern: Die Voreinstellungen sind für die Sicherheit des iPads nicht optimal.

Wenn Sie das iPad nicht manuell sperren, bleibt es aktiv. Das heißt, wenn Sie das Gerät unbeaufsichtigt auf Ihrem Platz liegenlassen, hat jeder Zugriff auf alle Daten. Es ist auf jeden Fall empfehlenswert, die Einstellungen für Automatische Sperre zu aktivieren und so zu setzen, dass Sie bei der Arbeit nicht gestört werden, sich das Gerät nach gewisser Zeit aber automatisch sperrt und für das Entsperren einen Code verlangt.

7.4.2 Optionen der Code-Sperre

Auch wenn sich das iPad sperrt, lässt es sich problemlos wieder entsperren, solange Sie keinen Code festlegen. Aus diesem Grund sollten Sie auch auf *Einstellungen\Allgemein\Code-Sperre* aufrufen und entsprechende Einstellungen setzen. Im Fenster haben Sie verschiedene Einstellungsmöglichkeiten, mit denen Sie die Sicherheit deutlich erhöhen können:

- **Code aktivieren/deaktivieren** – Über diese Schaltfläche legen Sie einen Code für das iPad fest. Diesen Code müssen Sie eingeben, wenn Sie das iPad entsperren oder nach der Aktivierung erneut in die Konfiguration der Code-Sperre wechseln. Die Code-Sperre lässt sich auch über Exchange-ActiveSync-Richtlinien festlegen. Sobald sich das iPad das erste Mal mit dem entsprechend konfigurierten Exchange-Postfach verbindet, übernimmt es nach Bestätigung diese Einstellung. Akzeptiert der Anwender die Einstellungen nicht, lässt Exchange keinen Postfachzugriff durch das iPad zu.

Code-Sperre: Es gibt verschiedene Einstellungsmöglichkeiten.

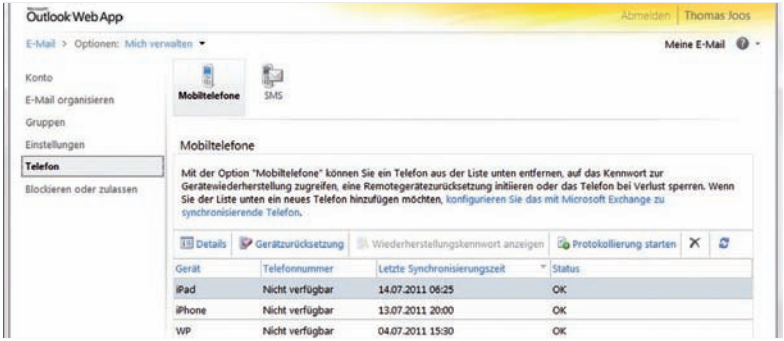
- **Code ändern** – Haben Sie einen Code gesetzt, können Sie Ihn an dieser Stelle ändern.
- **Code anfordern** – Hier legen Sie fest, wann das iPad den Code benötigt. In der Standardeinstellung Sofort muss der Code eingegeben werden, sobald Sie das iPad entsperren. Sie können die Eingabe aber auch verzögern und andere Einstellungen festlegen. Je kürzer der Zeitraum ist, umso sicherer ist die Einstellung. Mit Sofort haben Sie die beste Sicherheitseinstellung. Diese sollten Sie bei der beruflichen Verwendung des iPads auf jeden Fall aktivieren.
- **Einfacher Code** – Durch Aktivierung dieser Einstellung müssen Sie nur eine vierstellige Zahl zum Entsperren eingeben. Deaktivieren Sie diese Einstellung, können Sie einen längeren und sicheren Code verwenden. Auch hier sollten Sie einen Kompromiss zwischen Sicherheit und effizienter Bedienbarkeit eingehen.
- **Bilderrahmen** – Ist diese Option aktiviert, kann jeder Anwender, auch bei gesperrtem iPad, über die Bilderrahmen-Schaltfläche eine Diashow der auf dem iPad gespeicherten Bilder starten. Aus Sicherheitsgründen sollten Sie diese Option deaktivieren. In diesem Fall zeigt das iPad diese Schaltfläche auf dem Sperrbildschirm nicht mehr an.
- **Daten löschen** – Aktivieren Sie diese Option, löscht das iPad automatisch alle Daten vom Gerät, wenn jemand zehnmal den falschen Code in das iPad eingibt. Vor allem für iPads, die in Unternehmen eingesetzt werden, ist diese Einstellung fast Pflicht. Ist das iPad an Exchange angebunden, können Anwender und Administratoren das Gerät auch über das Internet löschen lassen. Dazu sendet der Exchange-Server ein Löschsignal an das iPad, sobald es sich das nächste Mal mit dem Server verbindet. Zusammen mit der Einschränkung, dass Anwender keine Einstellungen auf dem iPad bezüglich der E-Mail-Accounts ändern dürfen, kann niemand diesen Löschvorgang verhindern, sobald sich das iPad auf irgendeinem Weg mit dem Internet verbindet.

7.4.3 iPad mit Exchange und Office 365 betreiben

Viele der erwähnten Einstellungen lassen sich auch festlegen, wenn Sie im Unternehmen Exchange einsetzen. Hier können über Exchange-ActiveSync-Richtlinien folgende Einstellungen auf das iPad übertragen werden:

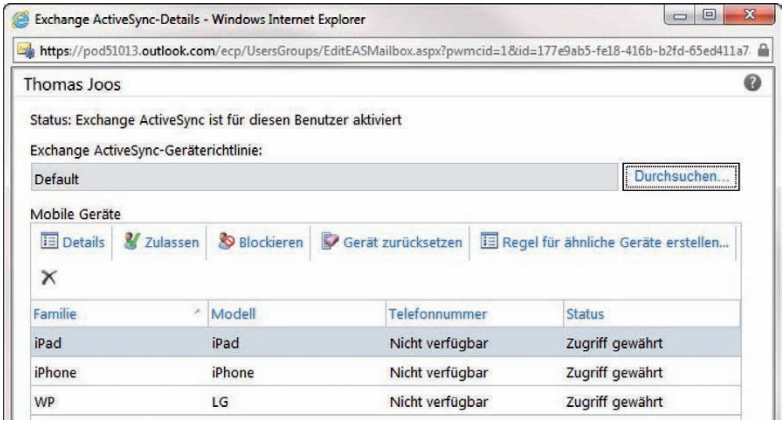
- Fernlöschen (Remote Wipe)
- Erzwingung eines Codes zum Sperren des Gerätes
- Mindestlänge für Kennwörter
- Mindestanzahl/Maximale Anzahl falscher Eingaben, bis sich das Gerät selbst löscht oder sperrt
- Kennwort muss Ziffern und Buchstaben erhalten
- Inaktivitätszeit

- Einfaches Kennwort zulassen
- Kennwortablauf und Kennwortverlauf
- Aktualisierungsintervall für Richtlinien
- Mindestanzahl komplexer Zeichen im Kennwort
- Kamera zulassen oder sperren



Im Zugriff: Endgeräte von Anwendern in Outlook Web App verwalten

Sobald Sie an OWA (Outlook Web Access) angemeldet sind, rufen Sie über den Menüpunkt rechts die Einstellungen Ihres Postfachs auf. Sie erreichen die Verwaltung Ihres Telefons über *Telefon\Mobiltelefone\<Name des Gerätes>*. Über *Wiederherstellungskennwort* lässt sich das Kennwort anzeigen, welches das iPad verlangt, wenn es aufgrund falscher Kennworteingaben gesperrt ist.



Unter Kontrolle: Einstellung für angebundene Smartphones der Anwender in Office 365 aufrufen.

Sie sehen alle mobilen Geräte, die sich per Exchange-ActiveSync mit dem Postfach synchronisieren, sowie ausführliche Details zu dieser Verbindung. Für die einzelnen Telefone können Sie sich auch die Details anzeigen lassen und kontrollieren, ob Richtlinien angewendet wurden beziehungsweise wann der letzte Synchronisierungsvorgang stattgefunden hat. Über die Schaltfläche *Geräterücksetzung* löschen Sie das Endgerät, sobald es sich das nächste Mal mit dem Exchange-Server verbindet. Diese Einstellungen stehen auch in den meisten gehosteten Exchange-Lösungen zur Verfügung, zum Beispiel in Office 365.

7.4.4 Admins können iPads löschen

Administratoren können die Endgeräte der Anwender ebenfalls löschen. Die Einstellungen dazu finden sich in der Exchange-Verwaltungskonsole im Kontextmenü des entsprechenden Benutzerpostfachs.

Haben Sie das iPad an Office 365 angebunden, können Administratoren auch die Geräte der Anwender steuern und löschen:

- Die Einstellungen dazu finden Sie über den Administratorbereich des Portals, wenn Sie auf *Allgemeine Einstellungen* im Bereich *Outlook* klicken.
- Markieren Sie einen Benutzer und klicken auf *Details*.
- Über *Telefon- und Sprachfeatures\Bearbeiten* sehen Sie die angebundenen Smartphones und können als Administrator die Löschung durchführen oder ein Wiederherstellungskennwort anfordern.

Für Admins: Einschränkungen auf dem iPad konfigurieren

Auch wenn Anwender ihr privates iPad oder iPhone im Unternehmen nutzen, haben Administratoren die Möglichkeit, das Endgerät zu löschen – mit allen darauf gespeicherten Daten. Dessen sollten sich Anwender bewusst sein, die ein privates Gerät an das Unternehmensnetzwerk anbinden.

7.4.5 Apps auf dem iPad sperren

Mit dem iPad haben Sie auch die Möglichkeit, bestimmte Apps für Anwender zu sperren. Setzen Sie als Administrator die Einstellungen, kann der Anwender diese später nicht rückgängig machen. Sie legen beim Aktivieren der Einschränkungen einen eigenen Code fest, der nur für die Konfiguration der Einschränkungen gesetzt ist und nichts mit der Code-Sperre zu tun hat.

Das heißt, iPads lassen sich von Administratoren effizient steuern, was die Bedienung der Apps angeht. Über *Einstellungen\Allgemein\Einschränkungen* aktivieren Sie zunächst die Einschränkungen auf dem iPad. Sie müssen noch einen Code eingeben, über den Sie nach dem Setzen der Einstellung die Einschränkungen wieder ändern können. Anschließend haben Sie weitreichende Möglichkeiten, den Umgang mit Apps zu steuern. Sie können Standard-Apps auf dem iPad ausblenden und die generelle Installation oder das Löschen von Apps verhindern. Auch die Einstellungen für Ortungsdienste oder die E-Mail-Accounts lassen sich an dieser Stelle vor Änderungen schützen. Die Spiele auf dem iPad können genauso effizient unter Kontrolle gebracht werden wie der Zugriff auf iTunes.

7.4.6 Achtung bei der Installation von Apps und Ortungsdienste

Auch wenn die Apps in Apples AppStore wesentlich besser vor Viren geschützt sind als bei anderen Systemen, besteht dennoch die Gefahr des Datenmissbrauchs. Installieren Sie eine App, müssen Sie in vielen Fällen bestätigen, dass diese auf die Ortungsdienste des iPads zugreift, also auch auf persönliche Daten.

Bevor Sie Apps installieren – vor allem kostenlose –, überprüfen Sie, auf welche Daten diese App zugreift. Vor allem wenn iPads gejailbreaked sind, also vollständigen Zugriff auf die komplette Umgebung gestatten, ist höchste Vorsicht geboten. Apps können problemlos selbst auf den AppStore zugreifen und Inhalte erwerben, wenn sie die entsprechende Genehmigung erhalten. Das kann zum Beispiel bei Zeitungsabonnements passieren.

Das Problem tritt besonders häufig bei kostenlosen Apps auf, da sich diese oft durch Werbung und den Verkauf von Benutzerdaten für den Entwickler bezahlt machen. Aus diesem Grund kann es für Administratoren sinnvoll sein, über die Einschränkungen des iPads die Installation von Apps komplett zu verhindern.

7.4.7 Sicherheitslücken beachten

Auch wenn iOS ein geschlossenes System ist, gibt es ständig Sicherheitslücken, die das iPad gefährden. So warnte im Sommer 2011 das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor einer Lücke im iOS, die es Angreifern ermöglicht, über PDF-Dateien auf die Daten des iPads/iPhones zuzugreifen. Betroffen sind auch die aktuellen Geräte iPhone 4 und iPad 2, da sie die gleichen iOS-Versionen verwenden. Angreifer können schon beim Aufrufen eines PDFs einen Virus auf dem iPad installieren, der alle Passwörter, Daten, Terminkalender, E-Mails und Kontakte abrufen kann, ohne Rückmeldung und ohne dass Anwender etwas davon bemerken. Auch der Zugriff auf die Kamera und die Ortungsdaten per GPS oder Internet sind möglich, genauso wie das Mithören von Telefongesprächen. Im Internet gibt es dazu bereits zahlreiche Hacker-Tools, die auch Skript-Kiddies leicht verwenden können, um iPad-Nutzer anzugreifen.

Über iTunes: regelmäßig Sicherheits-Updates auf dem iPad installieren.

Apple schließt solche Lücken durch Aktualisierung von iOS. Dies sollten Sie in regelmäßigen Abständen über iTunes durchführen. Ob sich das Gerät auf dem aktuellsten Stand befindet, erfahren Sie, wenn Sie es mit iTunes verbinden und auf das Gerät klicken sowie anschließend auf Updates suchen. Findet iTunes eine neue Version von iOS, sollten Sie diese möglichst schnell installieren, vor allem wenn dadurch Sicherheitslücken geschlossen werden.

Verlassen Sie sich auch nicht zu sehr auf die interne Verschlüsselung der Daten auf dem iPad oder die gesetzten Sicherheitskennwörter und Codes. Im Internet gibt es genügend Tools, die alle Daten von iPhones und iPads auslesen und kopieren können, auch wenn die Daten durch Kennwörter gesichert sind. Wie ein solcher Angriff ablaufen kann, zeigt das Fraunhofer-Institut.

7.4.8 Persönliche Daten vom iPad löschen

Wollen Sie das iPad an Kollegen oder Freunde weitergeben, ist es sehr empfehlenswert, alle persönlichen Daten vorher zu löschen. Dazu rufen Sie *Einstellungen\Allgemein* auf. Über *Zurücksetzen\Inhalte & Einstellungen löschen* können Sie zunächst im ersten Schritt alle gespeicherten Daten vom Gerät löschen.

Überlegt ausleihen: alle persönlichen Daten vom iPad löschen.

Damit die Löschung zuverlässig funktioniert, sollten Sie im nächsten Schritt das Gerät neu wieder aktivieren wie bei der ersten Inbetriebnahme. Anschließend ist es ratsam, die App iErase: Zero Free Space (http://itunes.apple.com/de/app/ierase-zero-free-space/id300428114) oder die noch bessere iErase: Government Edition (http://itunes.apple.com/de/app/ierase-government-edition/id419790063) zu installieren und das Gerät löschen lassen. Nach dieser Löschung starten Sie erneut eine Systemzurücksetzung. Anschließend sind keine wiederherstellbaren Daten mehr auf dem Gerät zu finden.

Thomas Joos

TecChannel-Links zum Thema	Webcode	Compact
Workshop – Apple iPad sicher betreiben	2036859	S.321
Workshop – Drucken mit iPhone und iPad	2036536	S.317
Ratgeber: Das iPad im professionellen Einsatz	2036988	S.329
Test: Apple iPad mit iOS 5	2036977	S.339

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195

7.5 Ratgeber: Das iPad im professionellen Einsatz

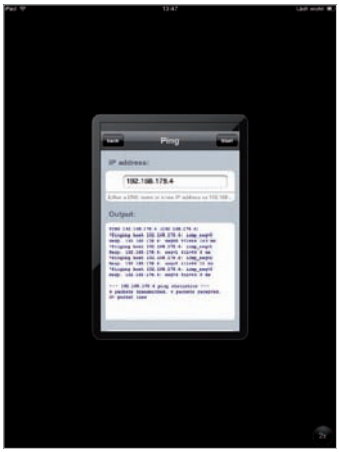
Mittlerweile gehören iPads in vielen Unternehmen zu den ständigen Begleitern professioneller Anwender. Daher stellt sich für Administratoren meist die Aufgabe, diese Anwender beziehungsweise deren Tablets so gut wie möglich einzubeziehen.

Meist wurden vor den iPads ja bereits iPhones im Unternehmen eingesetzt. Das ist insofern hilfreich, als beispielsweise in puncto Anbindung an Exchange und SharePoint die gleichen Regeln für iPad/iPad 2 und iPhone gelten. In Sachen Exchange-ActiveSync-Richtlinien bieten beide Gerätetypen die identischen Möglichkeiten, unterliegen aber auch den gleichen Einschränkungen. Die Anwendungen zur Verwaltung von E-Mails, Terminen und Kontakten sind identisch, nur die Ansicht ist größer. Das iPhone-Konfigurationsprogramm (Webcode **2033060**), das Sie zur Automatisierung der Konfiguration von iPhones verwenden, können Sie zusammen mit dem iPad 2 nicht einsetzen. Erstellte Konfigurationsprofile und Einstellungen lassen sich auf diesem Weg nicht übertragen.

7.5.1 iPhone-Apps auf dem iPad nutzen

Unternehmensanwender, die iPhone-Apps auf dem iPad nutzen wollen, stellen schnell fest, dass die meisten Apps nicht angepasst sind. Das äußert sich darin, dass die App in einem kleinen iPhone-Fenster dargestellt wird. Angepasste Apps für das iPad nutzen den ganzen Bildschirm. Sie können zwar das Fenster vergrößern, allerdings leidet darunter die Darstellung, sodass ein vernünftiges Arbeiten in vielen Fällen nicht möglich ist.

Darstellungsfragen: iPhone-Apps lassen sich auf dem iPad betreiben.



Sie können problemlos an dem Rechner, mit dem Sie ein iPhone verwalten, auch Ihr iPad anschließen. iTunes speichert den Status der verschiedenen Geräte, und Sie können für iPhone und iPad getrennt festlegen, welche Apps auf welchem Gerät zur Verfügung stehen sollen. Ist eine App nicht mit dem iPad kompatibel, überprüfen Sie, ob Sie kostenlos noch die iPad-Variante der App herunterladen können. In manchen Fällen bieten Entwickler auch optimierte Erweiterungen mit der Endung „HD“ an.

7.5.2 iPad-Internetzugang per iPhone

Generell spricht nichts dagegen, dass Anwender iPhones und parallel das iPad nutzen. Die Bedienung der beiden Geräte ist weitgehend identisch, wobei die tägliche Arbeit mit dem iPad natürlich wesentlich angenehmer ist. Die Anbindung an Exchange und SharePoint erfolgt entweder über Apps oder über den Safari Browser.

Voraussetzung: Der persönliche Hotspot muss aktiviert sein, damit andere Geräte die Internetverbindung nutzen können.

Besitzt ein Anwender ein iPhone mit aktiviertem persönlichem Hotspot, kann er mit seinem iPad über die UMTS-Verbindung des iPhones im Internet surfen oder E-Mails abrufen. Die Verbindung dazu steuern Sie am besten über WLAN. Diese als Tethering bezeichnete Technologie ermöglicht es, dass mehrere externe Geräte das iPhone und dessen Internetzugang nutzen können. Mit der neuen Technologie in iOS werden auch Anwender mit Notebooks oder iPads in die Lage versetzt, ohne Internetzugang zu surfen, indem sie sich mit dem iPhone verbinden. Bei der Anbindung über WLAN können drei Clients von außerhalb die Internetverbindung nutzen Fragen Sie vorher bei Ihrem Provider nach, ob Ihr Vertrag für Tethering freigeschaltet ist. Bei aktuellen Verträgen, die ab Oktober 2010 abgeschlossen wurden, ist das meistens der Fall, bei älteren Verträgen müssen Sie unter Umständen die Tethering-Funktion nachbuchen. Damit sich Computer oder andere Geräte an das iPhone anbinden können, ist diese Funktion erst in den Einstellungen zu akti-

vieren. Rufen Sie dazu auf dem iPhone *Einstellungen\Persönlicher Hotspot* auf. Sehen Sie den Menüpunkt nicht, muss unter Umständen diese Funktion auch noch aktiviert werden. Rufen Sie dazu *Einstellungen\Allgemein\Netzwerk* auf. Aktivieren Sie die Option *Mobile Daten*. Als Geschwindigkeit nutzt das iPhone 54 Mbit/s auf 2,4 GHz und WPA2 oder WPA als Sicherheitsprotokoll. Die SSID lässt sich nicht anpassen, hier verwendet das iPhone den Gerätenamen. Diesen können Sie nur in iTunes ändern, nicht im Gerät selbst.

Kontaktaufnahme: So verbinden Sie das iPad per WLAN mit dem iPhone.

Wollen Sie ein iPad mit dem iPhone über WLAN verbinden, um die schnelle Leitung des iPhone zu nutzen, sollten die iOS-Versionsstände der Geräte identisch sein (beispielsweise iOS 4.3.5). Setzen Sie verschiedene Versionen ein, gelingt die Verbindung nicht oder läuft nur sehr instabil. Aktualisieren Sie daher über iTunes möglichst immer beide Geräte auf einmal.

Haben Sie den persönlichen Hotspot aktiviert, können Sie auf dem iPad über *Einstellungen\Wi-Fi* nach dem neuen Netzwerk des iPhones suchen lassen und sich verbinden. Sie müssen noch das Kennwort für die Verbindung eingeben, das Sie auf dem iPhone konfiguriert haben. Anschließend verbindet sich das iPad und kann den Zugang des iPhones nutzen. Benötigen Sie die Verbindung nicht mehr, sollten Sie diese aus Sicherheitsgründen deaktivieren. Verbundene Geräte zeigt das iPhone auf dem Home- und dem Sperrbildschirm an.

7.5.3 iPad/iPad 2 und Exchange

Die Anbindung an Exchange über ActiveSync ist mit dem iPad genauso möglich wie die Anbindung von iPhones. Das bedeutet: Sie können iPads mit Exchange synchronisieren, ohne den Umweg über IMAP, POP3 oder Produkte von Drittherstellern gehen zu müssen. Mit Exchange ActiveSync (EAS) können Anwender ihr Postfach mit E-Mails, Kontakten und Kalendereinträgen über das Telefonnetz oder WLAN synchronisieren, E-Mails empfangen und E-Mails senden.

Auf dem iPad sind folgende Schritte notwendig, um eine Anbindung an Exchange durchzuführen:

1. Rufen Sie *Einstellungen* auf.
2. Wählen Sie in den Einstellungen die Option *Mail, Kontakte, Kalender*. Wollen Sie später Einstellungen ändern, nehmen Sie das in diesem Bereich wieder vor.
3. Wählen Sie im neuen Fenster *Account hinzufügen*. Einmal angebundene Accounts sind künftig hier zu sehen.
4. Hier sehen Sie alle Anbieter, die das iPad unterstützt.
5. Im neuen Fenster tragen Sie die Daten des Exchange-Kontos ein:

- *E-Mail* – Hier tragen Sie die E-Mail-Adresse ein, die Sie im iPhone einbinden wollen.
- *Domain* – Hier tragen Sie den Namen der Windows-Domäne ein, an der Sie sich authentifizieren wollen. Bei Anbindung an ein 1&1-Exchange-Postfach ist das zum Beispiel die Domäne exchange. In vielen Fällen müssen Sie hier nichts eintragen, da die Authentifizierung über die E-Mail-Adresse erfolgt, zum Beispiel bei der Anbindung an Office 365. Hier reicht die Eingabe der E-Mail-Adresse des Anwenders im Feld Benutzername.
- *Benutzername* – Hier geben Sie den Namen ein, mit dem Sie sich an der Domäne anmelden, zum Beispiel auch am lokalen Computer. Bei der Anbindung eines 1&1-Postfaches verwenden Sie hier den gleichen Namen wie in Outlook. Bei der Anbindung an Office 365 tragen Sie Ihre E-Mail-Adresse ein.
- *Kennwort* – Kennwort des Benutzerkontos.
- *Beschreibung* – Hier tragen Sie ein, was das iPad anzeigen soll, wenn Sie in die E-Mail-App gehen, um das E-Mail-Konto abzurufen.

6. Klicken Sie anschließend auf *Weiter*.
7. Im nächsten Schritt blendet das iPad das Feld Server ein, wenn keine automatische Anbindung möglich ist. Hier tragen Sie den Namen des Servers ein, mit dem Ihr Exchange-Server an das Internet angebunden ist. Beim Einsatz von 1&1 ist das zum Beispiel *profimailer.de*, bei Office 365 ein Server in der Domäne *outlook.com*. Diesen trägt die E-Mail-App aber automatisch ein, sobald Sie Ihre Office-365-E-Mail-Adresse und das Kennwort eingetragen haben. Eine Eingabe des Servernamens ist nicht notwendig.
8. Haben Sie den Namen eingegeben, klicken Sie wieder auf *Weiter*, um die Anbindung abzuschließen. Erhalten Sie eine Meldung, dass das iPad den Server nicht verifizieren kann, bestätigen Sie diese einfach. Das kann dann passieren, wenn das Sicherheitszertifikat nicht ordnungsgemäß funktioniert.
9. Im nächsten Schritt konfigurieren Sie noch einige Synchronisierungseinstellungen und klicken anschließend auf *Sichern*, um die Konfiguration zu speichern.

10. Erhalten Sie Meldungen, dass das iPad das Konto nicht überprüfen kann, bestätigen Sie diese und fahren mit dem Einrichten fort. In den meisten Fällen liegt es am Zertifikat des Servers, dessen Zertifizierungsstelle das iPad nicht vertraut. Sie können sich über Details das Zertifikat anzeigen lassen und es akzeptieren; im Fall von Office 365 ist es bereits hinterlegt.

7.5.4 Outlook Web App per Browser

Per Safari auf dem iPad ist natürlich auch ein Zugriff auf Outlook Web App möglich. Allerdings können Sie dann nur die eingeschränkte Light-Version von OWA nutzen. Über die Optionen in OWA ändern Sie zum Beispiel die Einstellungen für Ihr Exchange-Postfach, was in den E-Mail-Einstellungen des iPads nicht möglich ist. Auf diese Weise aktivieren Sie zum Beispiel den globalen Abwesenheitsassistenten für Ihr Postfach. In der Queransicht zeigt das iPad an der linken Seite den Posteingang mit Absender, Zeitpunkt, Betreff und den ersten zwei Zeilen ein. Auf der rechten Seite finden Sie den Text der E-Mail.

Reichen Ihnen die internen Möglichkeiten im iPad nicht aus, können Sie auch zusätzliche Apps installieren Die App Mailer kann erweiterte E-Mails an Gruppen und Rundmails an mehrere Anwender erstellen. Die kostenlose Lite-Version hängt am Ende der E-Mail noch die Signatur „Mailer“ an. Mit der App lassen sich E-Mails effizienter schreiben, wenn Sie auf dem iPad mehrere E-Mail-Konten einsetzen und Mails an zahlreiche Anwender versenden, auch mit Anhängen.

Sie müssen in Mailer aber einen eigenen E-Mail-Server eintragen; die App kann nicht die Konten verwenden, die Sie in der iPad-E-Mail-App eingetragen haben.

7.5.5 Apps für Terminverwaltung und Kalender

Im App-Store sind reichlich Apps verfügbar, die das Verwalten von Terminen erleichtern. Falls Sie bei der Terminplanung vor allem auf den Google-Kalender setzen, sollten Sie sich zum Beispiel die kostenpflichtige App CalenGoo ansehen. Sie lässt sich offline nutzen und synchronisiert sich automatisch bei der nächsten Internetverbindung. Sie können verschiedene Ansichten aktivieren und Farbeinstellungen anpassen. Die App kostet 5,49 Euro.

Wer eine schnelle Übersicht über ein ganzes Jahr erhalten will, ist mit der kostenlosen App PocketCal gut beraten. Es ist auch möglich, zum aktuellen Datum zu springen und mit einem einfachen Antippen des Monitors das Jahr zu wechseln. Die App kann aber keine Termine verwalten oder diese anzeigen, sondern dient nur der Übersicht über den Kalender. Die Ansicht lässt sich so anpassen, dass die App auch weniger Monate auf einer Seite darstellt.

Eine weitere App zur Terminverwaltung ist miCal HD. Sie erweitert die Funktionen des Standardkalenders. Sie können mit der App auch Ansichten wechseln und den Kalender in Quer-Ansicht betrachten. Mit dem Dashboard haben Sie alle

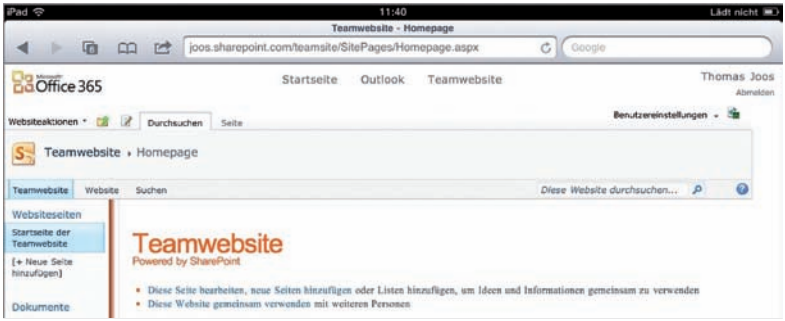
Termine des Tages in der Übersicht. Die App unterstützt alle Kalender, die Sie mit dem iPhone synchronisieren können, also unter anderem Outlook, Exchange, Google und Facebook.

Leider unterstützt das iPad keine Synchronisierung von Exchange-Aufgaben oder Notizen. Hier bietet es sich aber an, die App iMExchange 2 zu installieren – entweder als kostenlose Testversion oder als Vollversion im App-Store für knapp 6 Euro. Mit ihr können Sie Aufgaben und Notizen mit Exchange synchronisieren, auch über Exchange ActiveSync. Führen Sie einige Synchronisierungen kostenlos durch und entscheiden dann, ob Sie die App kaufen wollen. Für das iPad gibt es eine eigene Version, die den breiteren Bildschirm unterstützt. Verwenden Sie die App in der Queransicht, sehen Sie links die Aufgaben und rechts den Text zur Aufgabe.

Geht doch: Über Apps können Sie auch Aufgaben und Notizen synchronisieren.

4.5.6 iPad und SharePoint 2010

Mit dem iPad kann auch auf Daten von SharePoint-Servern zugegriffen werden.



Simpel: Der Zugriff auf Office 365 ist einfach per Browser möglich.

Dazu verwenden Sie entweder den integrierten Browser oder Apps. Über den Browser ist auch ein Zugriff auf Office 365 möglich. Als Adresse für SharePoint geben Sie die URL ein, mit der Sie auch über den Browser zugreifen. Arbeiten Sie mit Office 365, ist die Syntax *http:<Domänennamen>.sharepoint.com/teamsite*.

Es gibt mehrere Apps, die SharePoint unterstützen, zum Beispiel Moshare, eine kostenlose App für das iPhone, die auch die Anbindung an SharePoint 2010 problemlos unterstützt, oder Filamente SharePoint Client, eine App für SharePoint mit dem iPad. Sie kostet 10,49 Euro, es gibt aber auch eine kostenlose Version.

Wahlweise: Der Zugriff auf SharePoint kann auch per App erfolgen.

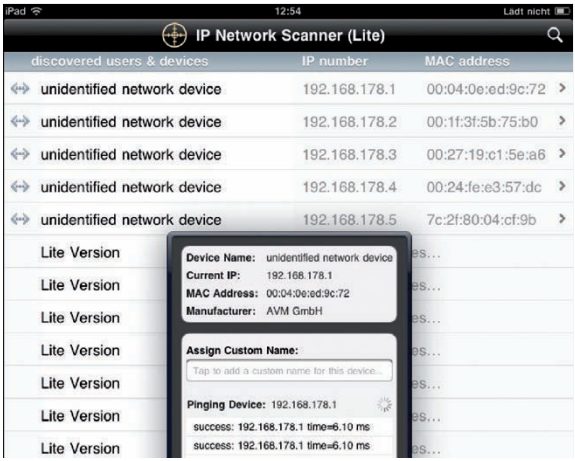
Ebenfalls kostenlos steht die App MoPrise SharePoint Documents for iPad zur Verfügung. SharePlus Office Mobile Clien kostet 11,99 Euro, eine kostenlose Testversion steht ebenfalls zur Verfügung. Die iPhone App SharePlus Lite Office Mobile Client und die kostenpflichtige Variante unterstütent sowohl das iPhone als auch das iPad. Nach der Anmeldung an SharePoint und dem Hinterlegen der Authentifizierung können Sie mit SharePoint und den Dokumenten arbeiten.

4.5.7 Apps für Admins

Administratoren, die im Netzwerk Windows-Server einsetzen, erhalten mit dem iPad umfangreiche Möglichkeiten, das Netzwerk auch von unterwegs aus im Auge zu behalten und einzelne Aufgaben durchzuführen. Mit der kostenlosen App Teamviewer HD können sich Admins mit Windows-Rechnern verbinden.

Die Freeware Teamviewer gibt es auch für Windows. Damit eine Fernwartung möglich ist, muss der Anwender auf dem Gast-PC die Freeware Teamviewer herunterladen und starten. Eine Installation der Software ist möglich, aber keine Voraussetzung für eine Fernwartung. Admins, die Teamviewer regelmäßig nutzen wollen, sollten sich die Pro-App kaufen. Administratoren in Windows-Netzwerken benötigen für die Fernwartung in den meisten Fällen das RDP-Protokoll. Hierfür sind ebenfalls zahlreiche Apps verfügbar.

Eine der bekanntesten ist iTAP RDP für 9,99 Euro. Sie können mit der App per RDP auf Rechner mit Windows XP/Vista und Windows 7 zugreifen und natürlich auch auf Server mit Windows Server 2000/2003/2008/2008 R2. Die App Remote Desktop Lite von Mocha ist kostenlos und funktioniert in den meisten Fällen ebenso problemlos.



Informativ: Admins können sich per App „IP Network Scanner Lite" mal eben die Geräte im Netzwerk anzeigen lassen.

Eine sehr wertvolle und kostenlose App ist auch der IP Network Scanner Lite. Dazu scannt die App das Netzwerk. Sie können den Geräten nach dem Scanvorgang ein Icon und eine Funktion zuweisen, sodass diese beim nächsten Scanvorgang berücksichtigt werden. Die kostenlose Lite-Version der Apps ist auf fünf Geräte limitiert. Für 3,99 Euro bekommen Sie die Vollversion, die keine Einschränkungen aufweist.

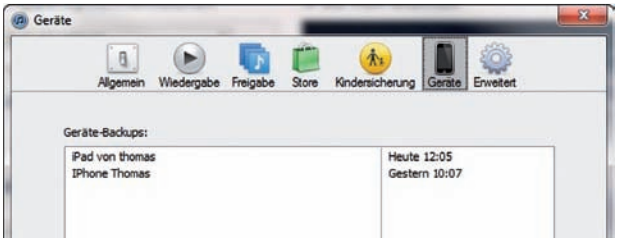
4.5.8 Datensicherung und Wiederherstellung

Das zentrale Instrument zur Datensicherung und Wiederherstellung von iPads und iPhones ist iTunes. Das Programm erstellt automatisch bei jeder Synchronisierung eine Datensicherung des Gerätes. Sie können auch mit Zusatz-Tools auf die Sicherungen zugreifen, manuell Sicherungen erstellen oder Sicherungen wiederherstellen, und auch die Mediathek kann gesichert werden.

Sobald Sie ein iPad mit dem PC verbinden, auf dem Sie iTunes installiert und mit dem entsprechenden Endgerät verbunden haben, startet automatisch eine Synchronisierung, bei der iTunes auch eine Datensicherung des Geräts anlegt, die immer zuerst startet, also bevor die eigentliche Synchronisierung beginnt. Den Stand des jeweils letzten Backups sehen Sie über *Bearbeiten\Einstellungen* auf der Regi-

sterkarte *Geräte*. iTunes sichert immer nur ein Backup für jedes Gerät. Das heißt, Sie sollten den Speicherort der iTunes-Sicherung in die Backup-Strategie Ihrer Daten einbinden. Geht das iPad verloren und ist die Datensicherung auf dem iTunes-PC nicht verfügbar, sind alle Daten weg.

Was bisher geschah: Sie können sich die letzten Backups der angeschlossenen Geräte anzeigen lassen.



Die Datensicherung des iPhones enthält vor allem die Daten, die Sie bei der Wiederherstellung der Werkseinstellungen wieder auf das iPhone übertragen können. Während der Datensicherung berücksichtigt iTunes folgende Daten auf dem iPhone/iPad:

- Adressbuch
- Daten für Programme aus dem App Store
- Programmeinstellungen
- Daten für das automatische Ausfüllen von Webseiten
- CalDAV und Kalenderabonnements
- Kalender-Accounts
- Kalendereereignisse
- Anrufverlauf
- Fotos, Screenshots, Bilder und Videos
- Kennwörter für E-Mail-Accounts und Wi-Fi-Kennwörter
- Liste der externen Synchronisierungsquellen (MobileMe, Exchange ActiveSync)
- Mail-Accounts und Microsoft-Exchange-Account-Konfigurationen
- Netzwerkeinstellungen
- Notizen
- Gekoppelte Bluetooth-Geräte
- Lesezeichen, Cookies, Verlauf, Offline-Daten und aktuell geöffnete Seiten in Safari
- SMS- und MMS-Nachrichten (Bilder und Videos)
- Hintergrundbilder

4.5.9 Datensicherung verschlüsseln

Sie haben die Möglichkeit, die Datensicherung von iPhones zu verschlüsseln, sodass sichergestellt ist, dass nur Sie diese Sicherungen verwenden können und kein unbefugter Benutzer an Ihre Daten kommt.

Klicken Sie dazu auf das Gerät, dessen Sicherungen Sie verschlüsseln wollen, und wählen Sie dann im oberen Bereich *Übersicht* aus. Aktivieren Sie im Bereich Optionen die Option *iPad-Backup verschlüsseln*. Anschließend müssen Sie ein Kennwort für diese Sicherung eingeben. Das Kennwort speichert iTunes, sodass Sie es nicht immer wieder neu eingeben müssen.

iTunes legt die Datensicherung des iPads auf dem lokalen PC ab. Der Speicherort unterscheidet sich je nach Betriebssystemen. Ein Backup besteht aus einem Ordner und zahlreichen Dateien, die sich standardmäßig nicht öffnen lassen.

Sie sollten mit der Datensicherung Ihres Computers auch regelmäßig die folgenden Ordner – je nachdem, welches Betriebssystem Sie einsetzen – mitsichern:

- Mac: *~/Library/Application Support/MobileSync/Backup/*
- Windows XP: *\Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Apple Computer\MobileSync\Backup*
- Windows Vista und Windows 7: *\Users\<Benutzername>\AppData\Roaming\Apple Computer\MobileSync\Backup*

Sie sehen die Ordner unter Windows erst, wenn Sie die versteckten Ordner im Windows-Explorer einblenden lassen.

Thomas Joos

TecChannel-Links zum Thema	Webcode	Compact
Apple iPad 2 bringt neue Probleme	2034575	S.315
Test – Lohnt der Umstieg von Apple iPad auf iPad 2?	2035275	S.307
Workshop – Drucken mit iPhone und iPad	2036536	S.317
Workshop – Apple iPad sicher betreiben	2036859	S.321
Ratgeber: Das iPad im professionellen Einsatz	2036988	S.329
Test: Apple iPad mit iOS 5	2036977	S.339

Mit den Webcodes gelangen Sie auf www.TecChannel.de direkt zum gewünschten Artikel. Geben Sie dazu den Code direkt hinter die URL www.TecChannel.de ein, etwa www.TecChannel.de/465195

7.6 Test: Apple iPad mit iOS 5

Mit den Tablet-Betriebssystemen Google Android Honeycomb, RIM PlayBook-OS QNX, WebOS von HP und dem künftigen Windows 8 von Microsoft wächst die Konkurrenz zu Apples iOS stetig. In puncto Funktionalität gerät das iOS 4.3 immer mehr in Bedrängnis, auch wenn der Bedienkomfort nach wie vor führend ist. Das neue iOS 5 bringt deshalb mehr als 200 neue Features mit sich. Im Herbst 2011 soll das neue Betriebssystem für das iPhone 3GS, iPhone 4, iPad und iPad 2 sowie den iPod touch der dritten und vierten Generation verfügbar sein. Mit der neuen Version 5 will Apple eigenen Angaben zufolge sein iOS auf ein ganz neues Level heben. Mit iOS 5 dürften sich auf jeden Fall einige Anbieter von Apps ärgern. So wandern nützliche Funktionen nun direkt in das Betriebssystem. Außerdem bohrt Apple den Safari-Browser deutlich in der Funktionalität und im Bedienkomfort auf. Während in iOS 4.3 häufig alternative Browser wie Atomic, iCab oder Opera Mini verwendet werden, könnten diese mit iOS 5 überflüssig werden.

TecChannel hat iOS 5 ausführlich auf dem Apple iPad getestet. Auf den folgenden Seiten stellen wir Ihnen die neuen Funktionen des Betriebssystems vor.

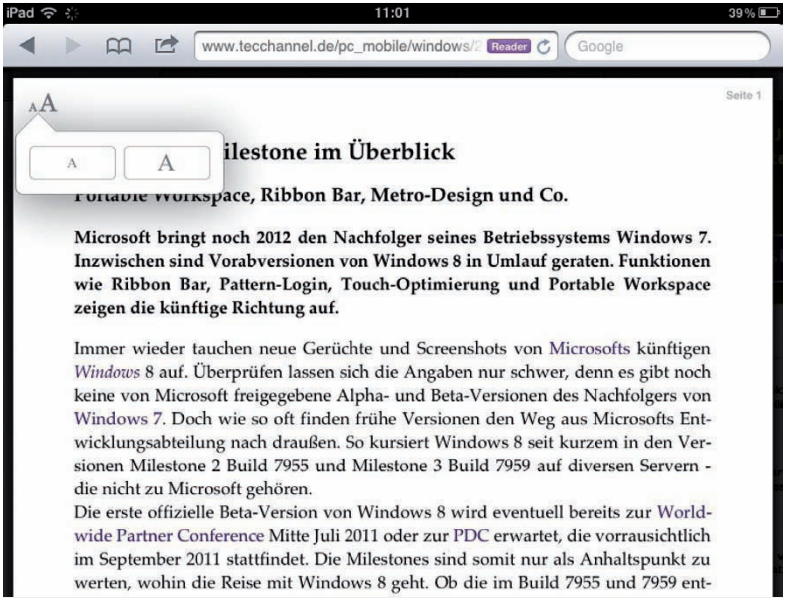
7.6.1 Safari: Tabbed Browsing und Reader

Apple führt beim Safari in iOS 5 das **Tabbed Browsing** ein. So lässt sich mit dem Finger schnell zwischen den offenen Tabs navigieren. Mit dem „+"-Zeichen wird ein neuer leerer Tab hinzugefügt. Maximal lässt Safari neun gleichzeitig geöffnete Tabs zu – bei der Anzahl hat sich somit nichts verändert.

Tabbed Browsing: Mit iOS 5 erlaubt der Safari nun Tabs wie bei Desktop-Browsern. Maximal lassen sich neun Tabs öffnen.

Eine weitere Neuerung ist die Möglichkeit, direkt auf Webseiten nach Begriffen zu suchen. Hierzu muss in das Suchfenster rechts oben getippt werden. Jetzt lässt sich in einem weiteren Suchfeld direkt über der eingeblendeten Tastatur der Suchbegriff eingeben. Treffer werden farblich hervorgehoben, mit Pfeiltasten kann durch die Treffer navigiert werden.

Apple integriert in den Browser den neuen **Safari Reader**. Die Funktion soll zum bequemeren und einfacheren Lesen von Artikeln auf Webseiten dienen. Bei Artikeln auf Webseiten blendet Safari automatisch nach dem Laden in der Adresszeile ein Icon Reader ein. Wird darauf getippt, so startet die Reader-Ansicht des Artikels. Selbst bei mehrseitigen Artikeln wird mit Safari Reader alles auf einer scrollbaren Seite angezeigt. Über das Symbol Weiterleiten können Artikel zu einer Leseliste hinzugefügt werden. Entsprechende Artikel werden dann in die **iCloud** synchronisiert. So lassen sich Artikel beispielsweise auf dem iPad weiterlesen, die auf dem iPhone geladen wurden.



Lesefreundlich: Der Safari Reader bereitet mehrseitige Artikel für ein bequemeres Lesen auf.

Auf der Webseite TecChannel.de funktioniert die Erkennung von Artikeln sehr gut. Wie in **iBooks** bei Büchern kann über das Schriftsymbol die Schrift vergrößert oder verkleinert werden. Gerade für mehrseitige Artikel erleichtert die Funktion das Lesen enorm, weil nur der Text und zugehörige Bilder zu sehen sind; alle übrigen Elemente der Webseite sind in der Reader-Ansicht verdeckt.

7.6.2 Notification Center löst Push-Nachrichten ab

Bei iOS 5 werden die bisherigen Push-Nachrichten durch ein neues Benachrichtigungssystem abgelöst. Die Einblendungen iOS 4.3 unterbrechen die Arbeit oder die App. In iOS 5 werden Nachrichten mit einer kleinen rotierenden Animation am oberen Bildschirmrand für ein paar Sekunden eingeblendet. Dabei wird die aktuelle App nicht unterbrochen. Wird während der Einblendung auf die Nachricht getippt, so öffnet iOS 5 die zugehörige App – beispielsweise den Mail-Client bei einer neuen E-Mail.

Nachrichten: Störende und die Arbeit unterbrechende Nachrichteneinblendungen haben bei iOS 5 ausgedient. Ein neues Benachrichtigungssystem bietet mehr Komfort.

Das **Notification Center** lässt sich jederzeit öffnen, wenn man mit einem Finger vom oberen Bildschirmrand nach unten zieht. Es zeigt beispielsweise neue ungelesene E-Mails oder Facebook-Updates an. In den Einstellungen unter Benachrichtigungen kann für jede einzelne App konfiguriert werden, ob und in welcher Form Hinweise eingeblendet werden sollen. So kann der Nutzer die Anzahl der Nachrichten konfigurieren und auch, ob die Neuigkeiten ebenfalls im Sperrbildschirm zu sehen sind. Wer weiterhin die Einblendungen wie bei iOS 4.3 bevorzugt, kann bei jeder App alternativ den Hinweisstil Meldungen statt Banner wählen. Dann wird die App allerdings wieder durch die Push-Nachricht unterbrochen. Im Benachrichtigungszentrum gibt es auch die Möglichkeit einzustellen, ob die Nachrichten nach Uhrzeit oder manuell sortiert darzustellen sind.

Wie erwähnt, lassen sich die Benachrichtigungen auch im Sperrbildschirm anzeigen. Um die Nachricht von hieraus direkt zu öffnen, muss das App-Symbol links neben der Nachricht mit dem Finger nach rechts gewischt werden. Auf diese Weise wird verhindert, dass beim einfachen Tipp darauf gleich das Gerät entsperrt wird. Kommt bei ausgeschaltetem Gerät (Stand-by) eine neue Nachricht an, so schaltet sich das Display für ein paar Sekunden ein, und man kann kurz die Meldung lesen.

7.6.3 iCloud: Dienste und Features

Mit iOS 5 stellt Apple jedem Nutzer einen 5 GByte fassenden Speicherplatz in iCloud zur Verfügung. **iCloud** löst im Prinzip den bisherigen Dienst **Mobile Me** ab, aber mit deutlich mehr Funktionalität. Über iCloud lassen sich die Apple-Dienste E-Mail mit Mobile-Me-Adresse, *Kontakte, Kalender, Erinnerungen, Lesezeichen* von Safari, *Notizen* sowie *Documents & Data* und *Bilder* synchronisieren. Bei den Bildern handelt es sich um das Album **Fotostream**, hier speichert iOS 5 alle selbst gemachten Fotos oder Screenshots ab (wenn es in den iCloud-Einstellungen aktiviert ist).

iCloud: Jedem Nutzer stellt Apple 5 GByte Speicherplatz kostenlos zur Verfügung.

Außerdem lässt sich in iOS 5 der iCloud-Dienst für ein Backup des Geräts nutzen. Beim Backup speichert iOS 5 neben den eigenen Fotos alle eingerichteten Accounts, Dokumente der Apps und die Einstellungen. iOS 5 bietet beim iCloud-Backup auch Optionen an, von welchen installierten Apps die Daten und Dokumente zu sichern sind. Praktischerweise wird bei jeder App der notwendige Speicherplatz angezeigt. So lassen sich bei Bedarf speicherfressende Apps vom Backup ausschließen. Wer will, kann für die 5 GByte fassende iCloud mehr Speicherkapazität einkaufen. Wer zusätzliche 10 GByte (insgesamt 15 GByte) haben will, muss pro Jahr 16 Euro zahlen. Zusätzliche 20 GByte kosten 32 Euro, 50 GByte schlagen mit 50 Euro pro Jahr zu Buche.

Bei neuen oder in den Werkszustand zurückgesetzten Geräten lässt sich somit nach der Anmeldung mit der Apple-ID das Backup direkt aus der iCloud drahtlos zurückspielen. Alternativ funktioniert aber auch noch der klassische Weg des Backups über iTunes.

7.6.4 Kabelos: Aktivierung und Updates

Neben dem iCloud-Dienst bietet iOS 5 weitere „kabellose" Funktionen an. Der Anwender ist mit iOS 5 nicht mehr gezwungen, sein neues Gerät über den PC oder Mac via iTunes und USB-Kabel zu aktivieren. Der Vorgang kann nun drahtlos erfolgen. Beim ersten Einschalten wird beim iPad – oder iPhone und iPod touch – nach der Sprach- und Landwahl ein verfügbares WLAN eingebunden – eine Internetverbindung ist für die kabellose Aktivierung Voraussetzung. Nach der Eingabe der Apple-ID ist das Gerät dann betriebsbereit.

Software-Updates erfolgen bei iOS 5 nun ebenfalls „over the Air". Dabei wird bei einem OS-Update nur geladen, was sich geändert hat – sogenannte Delta-Updates. Somit muss nicht stets ein komplett neues iOS-Image mit einer typischen Größe von zirka 600 bis 700 MByte heruntergeladen werden. Eine iTunes-Synchronisation ist nun auch über Wi-Fi möglich. Die Synchronisation kann automatisch erfolgen, sobald das iOS-Gerät an ein Netzteil zum Laden gesteckt wird.

7.6.5 Twitter-Integration in iOS 5

Apple integriert in iOS 5 den Social-Media-Dienst Twitter (www.twitter.com). So findet sich bei den Einstellungen des Betriebssystems jetzt der neue Eintrag Twitter. Von hier aus kann man zum einen die offizielle Twitter-App installieren. Zum anderen sorgt ein einmaliges Single-Sign-on in den Einstellungen für die Twitter-Integration in iOS 5. In der eigenständigen Twitter-App ist allerdings trotzdem nochmals eine – einmalige – Anmeldung notwendig.

Einfach twittern: iOS 5 ermöglicht durch die Twitter-Integration beispielsweise einen Tweet direkt aus dem Fotoalbum heraus.

Durch die Twitter-Integration ermöglicht iOS 5 ein direktes Twittern von Fotos aus dem Fotoalbum heraus. Beim Tippen auf das Symbol Weiterleiten bei einem Foto findet sich der zusätzliche Eintrag Tweet. Wird darauf getippt, so erscheint

ein Textfenster mit dem angehefteten Bild und einem Zeichenzähler. Außerdem lassen sich optional noch Geotagging-Infos einschalten. Im Safari-Browser ist die Twitter-Funktionalität ebenfalls integriert. Auch hier findet sich im Weiterleiten-Symbol der Tweet-Eintrag. Damit können Webseiten-Links direkt getwittert werden. Auch YouTube und Karten (Googlemaps) sind mit der direkten Tweet-Möglichkeit ausgestattet. Twitter ist in iOS 5 auch mit den Kontakten verbunden. Damit lassen sich Kontaktbilder automatisch aktualisieren, wenn die entsprechenden Kontakte mit Twitter verknüpft sind.

7.6.6 Verbessert: Mail, Kalender und Tastatur

In iOS 5 erhält der Mail-Client neue Funktionen. Einzelne Mails können nun wieder als ungelesen markiert oder mit einem Etikett zur Hervorhebung versehen werden. In jeder E-Mail findet sich der entsprechende Knopf *Markieren*, der beim Tipp darauf die beiden Optionen einblendet. Alternativ lassen sich im E-Mail-Eingangsfenster nach dem Tippen auf Bearbeiten auch mehrere E-Mails markieren und mit einem Etikett versehen.

Mail: Der Text in E-Mails lässt sich nun formatieren. Außerdem können einzelne E-Mails zum einfacheren Finden mit einem Etikett versehen werden.

In den *Einstellungen* bei Mail lässt sich nun eine Zitatebene aktivieren. Damit wird beim Antworten auf E-Mails der vorhandene Inhalt eingerückt und markiert dargestellt. Des Weiteren kann beim Verfassen von E-Mails Text Fett, Kursiv und Unterstrichen formatiert werden. Die Mail-App in iOS 5 erkennt jetzt auch Zertifikate und unterstützt S/MIME. Weiterhin erlaubt der E-Mail-Client nun direkt das Hinzufügen oder Entfernen von Ordner zu Accounts. Adressen lassen sich zudem beim Schreiben einer Mail zwischen den Feldern An:, Kopie: und Blindkopie: per Drag & Drop mit dem Finger verschieben.

Der Kalender hat in iOS 5 ebenfalls eine Auffrischung erhalten. Als neue Ansicht gibt es nun eine Jahresübersicht. Einzelne Termine können ebenfalls per Drag & Drop verschoben werden. Im Kalender lässt sich endlich auch per Fingerwisch zwischen den Tagen hin- und herblättern, ebenso bei den Ansichten *Monat* und

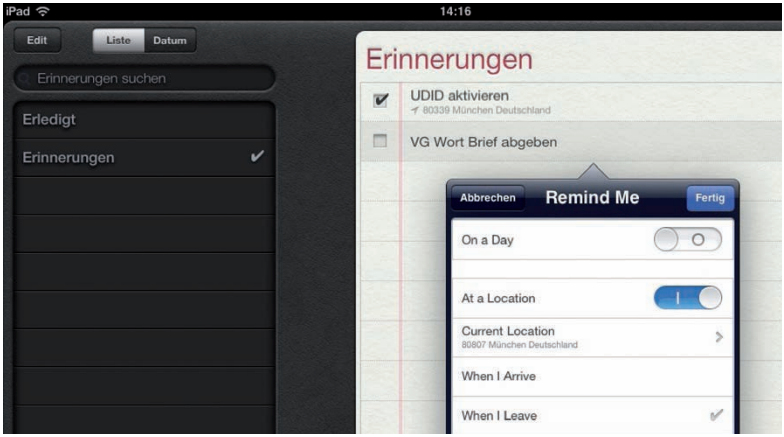
Jahr. Bisher musste mit dem Finger auf die kleinen Pfeile links und rechts unten getippt werden. Des Weiteren lassen sich direkt in der Kalender-App neue Kalender hinzufügen. In den *Einstellungen* beim Kalender können nun auch die Zeitpunkte für Standarderinnerungen definiert werden.

Kalender: Neben einer neuen Jahresübersicht ist nun auch das Blättern zwischen verschiedenen Jahren (oder Tagen, Wochen und Monaten) auch per Fingerwisch möglich.

Damit das Schreiben auf dem iPad besser funktioniert, lässt sich die Tastatur auf Wunsch teilen. Damit fällt insbesondere im Querformat das Schreiben mit den Daumen leichter. Wer will, kann die Tastatur in iOS 5 auch vertikal verschieben.

7.6.7 Neue Apps: Erinnerungen, Zeitungskiosk und iMessage

Apple spendiert iOS 5 die neue App **Erinnerungen** in der englischen Variante **Reminders**. Die App fungiert als Aufgabenliste mit Erinnerungsfunktion. Bei einer neu eingetragenen Aufgabe bietet die App zum einen eine wählbare Uhrzeit oder ein Datum, wann an die Erledigung erinnert werden soll. Zum anderen lässt sich aber auch Geotagging als Alarm verwenden. So wird ein Hinweis ausgelöst, wenn entweder der aktuelle Ort verlassen wird oder man an einem anderen wählbaren Ort ankommt.



Reminders: Die App erlaubt ortsbezogene Erinnerungen.

Als zweite neue App findet sich auf iOS 5 der **Newsstand** – bei gewählter deutscher Sprache wird sie als **Zeitungskiosk** bezeichnet. Die App sammelt zentral alle E-Magazine, die über ein Abo bezogen werden. Neue verfügbare Ausgaben werden automatisch geladen, sodass diese sofort im Newsstand sind. Aus der App heraus kann der Store zum Kauf und Abschluss neuer Abos gestartet werden.

Newsstand: Bei gewählter deutscher Sprache wird sie als Zeitungskiosk bezeichnet. Die App sammelt zentral alle E-Magazine, die über ein Abo bezogen werden. Neue verfügbare Ausgaben werden automatisch geladen, sodass diese sofort im Newsstand sind.

Die dritte neue App bei iOS 5 ist der Messaging-Service **iMessages**. In der deutschen Lokalisierung wird die App als **Nachrichten** angezeigt. Damit können iOS-5-Nutzer nicht nur Nachrichten, sondern auch Dateien, Fotos und Videos austauschen. Optional gibt es zudem Lese- und Empfangsbestätigungen. Der Messaging-Service läuft über Wi-Fi und 3G.

7.6.8 Weitere kleine Änderungen

Apple spricht bei iOS 5 von mehr als 200 neuen Features. Im Test auf dem iPad zeigen sich auch viele neue Detailfunktionen:

- **Benutzung:** Praktisch ist in den *Allgemeinen Einstellungen* der Eintrag *Benutzung*. Hier wird der belegte Speicherplatz jeder einzelnen App angezeigt.
- **Kurzbefehle:** In den *Allgemeinen Einstellungen* unter *Tastatur* findet sich der neue Eintrag *Kurzbefehl*. Hier lassen sich Kurzformen definieren. So wird beispielsweise „mfg“ beim Schreiben automatisch in „Mit freundlichen Grüßen“ umgewandelt.
- **Music:** In iOS 5 ist der Musik-Player *iPod* in *Music* umbenannt worden. Außerdem besitzt der Player ein neues Layout. Lieder können nun auch unmittelbar auf dem Gerät gelöscht werden.
- **Bilder:** iOS 5 erlaubt auf dem iPad das Löschen von Bildern aus Alben. Mit iOS 4.3 konnten nur Bilder aus dem Album „Gesicherte Fotos“ direkt auf dem Gerät gelöscht werden. In den Bildern lassen sich auch neue Alben anlegen. Außerdem ist das Kopieren von Bildern in andere Alben möglich.
- **Screenshots:** Wird mit iOS 5 auf dem iPad ein Screenshot durch das gleichzeitige Drücken von Power- und Home-Button erstellt, so ist dieser nicht mehr gedreht dargestellt wie in iOS 4.3.
- **Multitasking-Gesten:** Die Gesten zum Wischen zwischen offenen Apps mit vier oder fünf Fingern funktionieren bei iOS 5 nicht auf dem iPad. Apple behält die Funktion dem leistungsfähigeren iPad 2 vor.
- **Air Play Mirroring:** Beim iPad 2 lässt sich über Apple TV der Bildschirm direkt auf den TV-Screen übertragen.
- **Synchronisation:** Beim Synchronisieren über iTunes zeigt iOS 5 links oben in der Statusleiste einen rotierenden Kreis an.
- **Name:** In den *Allgemeinen Einstellungen* unter *Info* kann bei iOS 5 der Name des Geräts geändert werden. Bisher ist das nur mit iTunes möglich.

Christian Vilsbeck

8 Anhang: Die beliebtesten Artikel (QR-Codes)

Zum Thema dieses TecChannel-Buchs finden Sie hier die QR-Codes zu den meist geklickten Artikeln auf TecChannel.de. Mit einer entsprechenden App für Ihr Smartphone oder Tablet-PC gelangen Sie so schnell und ohne Tippen zu noch mehr Informationen.

Die beliebtesten Smartphones
(Webcode 2029356)

Die beliebtesten Tablet-PCs
(Webcode 2033311)

Test: Hewlett-Packard TouchPad
(Webcode 2037012)

Die besten Tipps und Tricks für Android
(Webcode 2031053)

So funktioniert das Blackberry-System
(Webcode 2029526)

Erster Test – HP webOS 2
(Webcode 2033737)

Samsung Bada im Test: Alternative zu Android?
(Webcode 2035009)

Lebensdauer von Smartphone-Akkus verlängern
(Webcode 2026668)

Kaufberatung: Das beste Smartphone
(Webcode 2024109)

Multitasking-Gesten auf dem iPad aktivieren
(Webcode 2034903)

Smartphones ins Firmennetz integrieren
(Webcode 2028107)

iPhone und iPad – Fit für Unternehmen?
(Webcode 2029059)

Die besten kostenlosen iPhone-Apps
(Webcode 2021220)

Die besten kostenlosen Apps für Android
(Webcode 2020642)

Die besten Bezahl-Apps für iPhone und iPad
(Webcode 2035091)

Die besten Symbian-Apps aus dem Ovi Store
(Webcode 2032526)

Nützliche Smartphone-Apps für private Zwecke
(Webcode 2035333)

Kurioses iPhone- und iPad-Zubehör
(Webcode 2030617)

Die beliebtesten Netbooks
(Webcode 2028410)

Die beliebtesten Notebooks
(Webcode 2028331)

Business-Notebooks 2011 – das sind die Trends
(Webcode 2033228)

Index

RATGEBER

Smartphones & Tablets im Unternehmen

SICHERHEIT, VERWALTUNG, INTEGRATION

Mobile Anwender sind für IT-Abteilungen seit jeher eine besondere Herausforderung. Bei Notebooks haben sich deshalb sehr schnell Zugriffsschutz, Verschlüsselung und Fernwartung etabliert. Smartphones und Tablets hingegen werden inzwischen in Unternehmen verwendet, als habe es nie ein Sicherheitskonzept oder einen relevanten Vorfall gegeben.

Die Integration von Smartphones und Tablets in die vorhandenen Strukturen ist daher eine der wichtigsten Aufgaben für IT-Abteilungen. Es stellt sich längst nicht mehr die Frage, ob, sondern nur, wie sie diese Geräte sauber und sicher integrieren. Schon seit geraumer Zeit können IT-Verantwortliche nicht mehr vorgeben, welche mobilen Geräte zum Einsatz kommen dürfen. Da heutzutage auch die privaten Smartphones und Tablets der Mitarbeiter mit E-Mail- und Netzwerkzugang ausgestattet werden, müssen für alle verfügbaren Plattformen Integrationsmöglichkeiten bestehen.

Dieser Ratgeber bietet das hierfür notwendige Basiswissen. Zahlreiche Workshops und Schritt-für-Schritt-Anleitungen helfen bei der Umsetzung in die Praxis.

TECCHANNEL
IT EXPERTS INSIDE

Auf ***TecChannel.de*** finden technische Entscheider alle wichtigen Informationen, die sie zu Planung, Betrieb und Optimierung der Unternehmens-EDV benötigen. Durch Tests, ausführliche Reportagen zu aktuellen Themen, Bugreports, Grundlagen und Workshops wird das gesamte redaktionelle IT-Spektrum abgedeckt.

ISBN 978-3-942922-07-4

9 783942 922074 03490

34,90 €