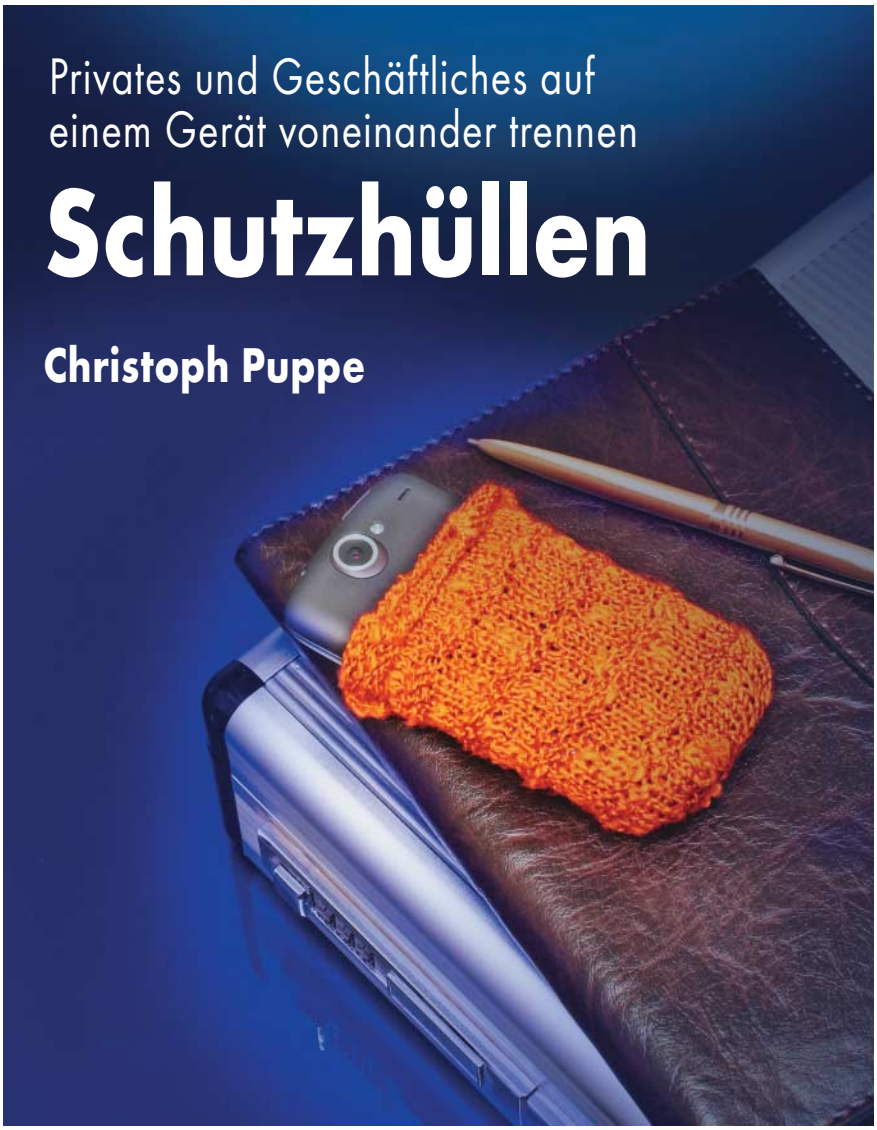
Privates und Geschäftliches auf einem Gerät voneinander trennen

Schutzhüllen

Christoph Puppe



Ansätze, geschäftliche von privaten Daten und Anwendungen zu trennen, sind teilweise das Beste aus zwei Welten und manchmal eine seltsame Mischung. Mitarbeiter haben nur den Wunsch, ihr eigenes Gerät ohne Einschränkungen nutzen zu können, während die IT alles Fremde lieber aussperren möchte. Drei Methoden versuchen den Widerspruch aufzulösen.

Niemand möchte mit zwei Telefonen herumlaufen, aber alle wollen auf alle Mails, Kontakte und Termine sowie andere Daten jederzeit zugreifen können. Der Zugang zu internen Webanwendungen der Firma soll genauso einfach sein wie das Surfen im Internet oder das Installieren von Spielen und beruflich bedingten Anwendungen.

Früher hatten Mitarbeiter ein Telefon und ein Notebook. Über das Telefon konnte man nichts anderes als Gespräche führen, und die IT hat das Firmen-Notebook den Sicherheitsvorschriften folgend konfiguriert. Glückliche Tage für die Systemadministration, in denen sie noch die volle Kontrolle über die Geräte hatte. Wer BlackBerrys an seine Mitarbeiter ausgegeben hatte, konnte sich ziemlich sicher sein, dass die Daten der Firma nicht in die falschen Hände gerieten.

Doch iPhone und spätestens das iPad haben das grundlegend verändert. Wie einst bei den BlackBerrys setzte zuerst die Leitungsebene im Betrieb den Wunsch nach der neuen Technik durch und erwartet inzwischen dieselben Funktionen von den mobilen Geräten ihrer Mitarbeiter. Der gravierende Unterschied besteht darin, dass dort die Administratoren kaum noch Kontrolle über die installierte Software haben, denn der Hersteller der Hardware kontrolliert das Betriebssystem, und die Benutzer können alle Apps installieren oder entfernen.

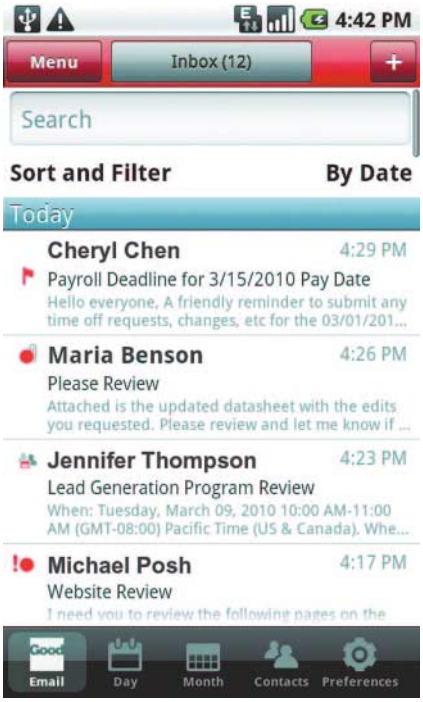
IT muss Kontrolle zurückerobern

Dem versuchen Fachleute mit einer Software zum Mobile Device Management (MDM) zu begegnen. Damit kann die IT in manchen Bereichen Kontrolle über die Geräte erlangen, allerdings kann der Benutzer sich ihr in einigen Fällen entziehen. Noch heikler wird es, wenn die Mitarbeiter ihre eigenen Geräte verwenden dürfen: „Bring Your Own Device“ (BYOD).

Ob mit oder ohne Management, sobald die Firmendaten auf einem mobilen Gerät gelandet sind, besteht ein erhebliches Sicherheitsrisiko. Trojaner, Drive-by-Downloads und Taschendiebe kommen schnell an sie ran; den Schutz davor kann kaum jemand garantieren. Erzwingt das Management des mobilen Geräts nennenswerte Absicherung, verliert es an Attraktivität für den Mitarbeiter. Wer will einen weiteren BlackBerry-Clone, auf dem nur die Firmendaten und freigegebene Apps verfügbar sind, der aber dennoch in keiner Weise so sicher ist wie das Original.

Der Wunsch nach Freiheit und die Notwendigkeit zur Absicherung sind also nur schlecht unter einen Hut zu bringen – und wenn einer nicht reicht, sollte es mit zweien einfacher sein, dachten sich in den letzten zwei Jahren einige Hersteller. Alle bieten Produkte an, die auf einem physischen Gerät getrennte Bereiche anbieten, in denen jeweils nur die zugehörigen Daten zugänglich sind.

Dazu gibt es unterschiedliche Methoden. Neben speziellen Kombinationen aus Smartphone und separat darauf laufender Thin-Client-Software existieren Angebote, Windows-Desktops plus Anwendungen auf handelsüblichen Tablets und Smartphones zu nutzen. Zu den Vorteilen zählt, dass die Verfahren Berufliches vom Privaten trennen können. Bei den serverzentrierten Konzepten speichern die mobilen Geräte keine Geschäftsdaten, die Remote-Desktop-



Zentral: Alle E-Mail-Kontakte laufen bei Good for Enterprise über einen Hub, der die Daten sammelt und sie an die Clients weiterleitet (Abb. 1).

Verbindung dient ausschließlich zum Anzeigen der Arbeitsoberfläche und Weiterleiten der Benutzeraktionen. Andere Anbieter wiederum statten die Geräte mit spezieller Hardware aus oder greifen zu virtuellen Maschinen, die auf einem Gerät laufen.

Firmen sind daran interessiert, die Daten des Personal Information Manager (PIM) mit dem Gerät zu synchronisieren, damit der Mitarbeiter unterwegs zumindest erreichbar bleibt, denn ohne Verbindung zum Internet ist er bei aus der Ferne gesteuerten Verfahren völlig isoliert.

Teilen, herrschen und synchronisieren

Wünschenswert ist oft eine Sicht auf alle PIM-Daten, etwa den Kalender, der Geschäfts- und Privattermine enthält, oder das E-Mail-Frontend, das zugleich die Kontakte anzeigt. Dazu kennen die auf den Smartphones installierten Clients Protokolle zum Synchronisieren, um Daten aus mehreren Quellen zu sammeln und in einer Sicht anzuzeigen. Verbreitet ist Microsofts Active Sync, für das selbst Lotus Notes einen Client anbietet, der auf dem Smartphone die Übersetzung zum Notes-eigenen Protokoll übernimmt.

In einer Firma mit geringem Anspruch an Sicherheit ist es üblich und auch nicht verkehrt, dass die Mitarbeiter die Daten des privaten und des Firmen-Accounts gemeinsam betrachten. Bei Unternehmen mit höherem Anspruch verbietet sich das, da jede Software, die auf E-Mails zugreifen darf, die Firmen-Mails erreichen kann. Eine unbedacht installierte Anwendung kann alle Kontakte, Kalendereinträge sowie E-Mails auslesen und an eine beliebige Stelle im Internet übertragen.

Eine Firewall muss eine strikte Trennung garantieren zwischen den Applikationen, die der Anwender installiert, und denen, die auf die Firmendaten zugreifen können. Im Umkehrschluss heißt das, dass eine gemeinsame Betrachtung nicht mehr möglich ist. Ein übliches Vorgehen ist es, Container zu definieren, die Firmendaten aufbewahren und die gegen Zugriffe aus privaten Anwendungen heraus geschützt sind.

Neben Fixmos „SafeZone“ und „DME Mobile Email & PIM“ von Excitor ist das bekannteste Beispiel für Container „Good for Enterprise“. Ehemalige Mitarbeiter von BlackBerry haben den früher existierenden Software-Client mitgenommen und weiterentwickelt. Damit sind Aufbau und Funktionen stark an BlackBerry angelehnt. Ein zentraler Hub sammelt die Daten von den in den Firmen installierten Servern und leitet sie an die mobilen Clients weiter. Dort speichert sie der Client in einem eigens verschlüsselten Datenbereich und zeigt die Informationen nur innerhalb der App an. Zudem baut er eine eigene VPN-Verbindung zum zentralen Hub auf, über die nur er und die dafür freigegebenen Apps Daten senden. Auf solchen Geräten darf der Anwender etwa einen zweiten Browser installieren, mit dem er auf das Intranet zugreifen kann, aber nicht auf das Internet. Good ist bei sicherheitsbewussten Firmen derzeit der Standard für Mitarbeiter, die keine BlackBerrys benötigen, auf ein Android oder

iX-TRACT

- Eine Trennung des privaten vom geschäftlichen Bereich ist selbst auf Smartphones möglich.
- Die Methoden unterscheiden sich vor allem im Sicherheitsniveau.
- Eine komplette Kontrolle über die Geräte durch Dritte dürfte heutzutage niemand mehr akzeptieren.

iPhone aus anderen Gründen angewiesen oder mit eigenen Geräten als Teil eines BYOD-Programms unterwegs sind.

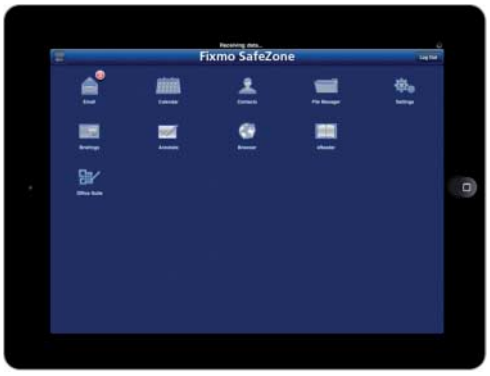
Reale Trennung durch Virtuelles

Mehr Trennung der Daten verspricht die Virtualisierung. Der Marktführer VMware in diesem Bereich präsentierte im August 2011 „Horizon Mobile“, das eine Weiterentwicklung des mit der Übernahme von Trango 2008 erworbenen Hypervisor ist. Zum Einsatz kommt eine Typ-2-Variante, die als Anwendung auf einem Betriebssystem läuft. Das Smartphone avanciert damit zum Wirt für Gäste, die auf einer immer gleichen, simulierten Hardware-Umgebung laufen. Damit können unterschiedliche Versionen von Android auf derselben Hardware parallel laufen. Außerdem hoffen die Betriebssystementwickler durch Virtualisierung schneller Updates bereitstellen zu können, weil sie die Software nicht mehr an unzählige Varianten der Hardware anpassen müssen.

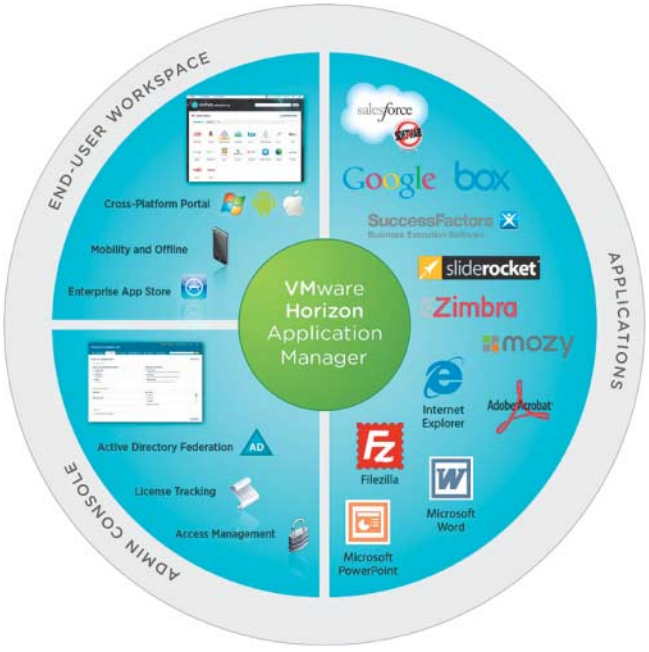
Der treibende Faktor ist die Trennung der beiden Welten – ein Janusköpfiges Android –, denn das Betriebssystem läuft zweimal auf demselben Smartphone, das eine für die private und das andere für die geschäftliche Nutzung. Beide sind vollständig gegeneinander abgeschottet, nur auf Wunsch gibt es Ausnahmen, die nur der Administrator einrichten kann: Cut & Paste etwa oder Benachrichtigungen, die in beiden Ansichten sichtbar sind. Wenn der Benutzer privat ein Video anschaut, erhält er dennoch die Nachricht, dass sein Chef ihm eine E-Mail geschickt hat, die aber nur im Mail-Programm auf dem „geschäftlichen“ Gast auftaucht.

Zwei Provider wollen auf Basis von Horizon mobile Produkte herausbringen: Verizon kündete 2011 an, auf dem US-amerikanischen Markt bald etwas anzubieten, und die spanische Telefónica hat auf dem diesjährigen Mobile World Congress (MWC) angekündigt, als erste solche Geräte in Europa anzubieten. Beide planen, eine SIM mit zwei Telefonnummern zu verwenden, sodass bei Anrufen zwischen privat und beruflich unterschieden wird. Abgesehen davon sind bei Verizon noch keine weiteren Details bekannt.

Telefónica will voraussichtlich in der zweiten Jahreshälfte 2012 die Geräte und den dazu gehörenden Service als „Dual Persona“ verkaufen. Ob das Paket in anderen Ländern als Spanien auf den Markt kommt, was stark zu erwarten ist, und zu welchen Preisen das Unternehmen anbieten will, ist bis dato nicht bekannt. Fest steht, dass es ein Onlinedienst sein wird, bei dem der Provider die volle Kontrolle über die Geräte behält und den Kunden eine



Isoliert: Die Umgebung bei Fixmos SafeZone ist serverzentriert und abgeschottet (Abb. 2).



Zwischenschicht: VMware schafft mit Horizon Mobile eine virtuelle Umgebung für Mobile Devices (Abb. 3).

BYOD auf der Mobile World Conference

Immer wieder kam das Thema „Bring Your Own Device“ auf dem Kongress der MWC zur Sprache. Firmen wie die SAP-Tochter Sybase und Symantec setzen auf Produkte für das Mobile Device Management (MDM), von denen sie auf der Veranstaltung neue Versionen präsentierten. Einen anderen Weg schlägt Telefónica ein, das mit dem Dienst „Dual Persona“ in Zusammenarbeit mit VMware ein virtuelles Business-Gerät auf dem privaten Android-Smartphone anbietet, das sich über die Cloud administrieren lässt.

Auch der israelische Anbieter Cellrox vertreibt mit Jade ein vergleichbares Produkt, das als Betaversion auf der MWC in Barcelona zu sehen war. Ähnliches bietet Enterproid mit Divide an, einer sicheren Plattform zum Content Sharing und zur Collaboration. Es stellt einen Dienst für Android bereit, den man per Dual Persona Cloud verwalten kann. Für Mitte des Jahres haben die Firmen vor, eine Unterstützung für iOS herauszubringen.

Microsoft kündigte während des MWC an, das Produkt „Good for Enterprise“ zusammen mit dem US-amerikanischen Hersteller Good Technology auf Windows-Phone-Geräte zu bringen. Es stellt eine FIPS-zertifizierte 192-Bit-Verschlüsselung per AES für mobiles Messaging bereit, die den sicheren Zugriff auf Unternehmensdaten wie E-Mail und Kontakte ermöglichen soll. Diese Daten legt die Good-Anwendung auf dem Smartphone verschlüsselt ab und erlaubt es dem Administrator, sie aus der Ferne per Remote Wipe zu löschen.

Citrix Receiver, das den sicheren Zugriff auf Unternehmensanwendungen von fast jedem mobilen Endgerät ermöglicht, bekam den Preis als beste Mobile App for Enterprise, und der Cloud-basierte Device-Management-Dienst Fiberlink MaaS360 wurde als bester Enterprise Mobile Service prämiert.

Nachdem sich lange Zeit lediglich BlackBerry speziell um die Bedürfnisse von Geschäftskunden gekümmert hatte, engagierten sich 2012 verstärkt andere Hersteller in dem Bereich. Letztendlich besteht das Ziel bei vielen vor allem darin, private Endgeräte mit in das Firmennetz zu integrieren, ohne dabei die Unternehmensdaten in Gefahr zu bringen. *Kay Glahn*

Zwei in eins: Telefónica will Smartphones mit zwei Telefonnummern auf einer SIM anbieten (Abb. 4).

Weboberfläche für die Konfiguration eigener Parameter und die Verwaltung der installierten Apps bereitstellt. Neumodisch nennt Telefónica das eine „cloudbasierte“ Verwaltung.

Bei der Hardwareauswahl hat sich Telefónica bereits entschieden: Es zeigte auf dem MWC ein SII von Samsung. Der Hersteller wiederum hat angekündigt, mit VMware zusammen alle seine Android-Smartphones auf Mobile Horizon anzupassen. LG hat unabhängig von Providern ähnliche Pläne und ebenfalls einen Prototyp gezeigt. Von der Bedienung her ist es ein überzeugendes Konzept: Der Wechsel zwischen den Gästen erfolgt über einen Klick auf eine Anwendung auf dem Desktop und geht auf dem SII fast blitzartig über die Bühne.

Darüber hinaus plant VMware, einen Hypervisor für das iPhone herauszubringen – Erfahrungen mit Mac OS X hat die Softwareschmiede dank Fusion auf Apple. Allerdings steckt das Projekt für iOS noch in den Kinderschuhen.

Gesichert im Sandkasten

Enterproid bietet mit „Divide“ ein weiteres Produkt, das die Virtualisierung zum Separieren nutzt. Allerdings ist die Software nicht so tief in der Firmware verankert wie Mobile Horizon. Man kann Divide auf einem beliebigen Android ab Version 2.2 als Anwendung einrichten. Sie startet eine virtuelle Maschine, in der ein abgespecktes Android läuft. Die Installation verlangt keine besonderen Rechte, und man braucht das Gerät nicht zu „rooten“. Allerdings muss man es der Routine erlauben, Pakete zu installieren, die nicht aus dem Market stammen. Außerdem beansprucht Divide fast alle von einer App zu beantragenden Rechte, inklusive der zum Administrieren. Nach wenigen Minuten ist die Sandbox eingerichtet und öffnet einen Onlinezugang zu einer Management-Plattform beim Hersteller.

Divide ist wie Horizon Mobile eine Mischform zwischen Virtualisierung und Container. Gegenüber den Containern hat der Anwender den Vorteil, dass die Administration innerhalb des Gastes weitere Anwendungen installieren kann. Es stehen wie auf einem regulären Android mehrere Screens zur Verfügung, und es gibt die bekannten Standardprogramme. Der Market fehlt allerdings, da nur die Management-Plattform Apps installieren darf.

Die Daten der Anwendung sind wie bei Horizon Mobile laut Auskunft des Herstellers mit 256 Bit AES Verschlüsselt. Wo der Schlüssel liegt und wie er geschützt ist, darüber gibt es bei beiden keine Angabe. Der Wechsel zwischen der Berufswelt und dem Privaten erfordert die Eingabe einer PIN oder eines Passwortes. Die Länge ist im Management einstellbar. Ob dies als Quelle für einen AES-Schlüssel ausreicht, ist sehr fraglich.

Was die weiteren Funktionen angeht, verhält sich Divide wie ein Container: Der Administrator kann nicht sämtliche Daten auf dem Gerät aus der Ferne löschen, sondern nur den Speicher der Anwendung. Die Onlineverwaltung ist übersichtlich und bietet zusätzlich eine Überwachung der Datenübertragung und des Gesprächsvolumens. Der Inhaber des Geräts kann sein Divide an die IT-Administration seiner Firma übergeben, muss es aber nicht. Dadurch genießt er etwas mehr Freiheiten als bei der stärker zentralisierten Verwaltung von Horizon Mobile.

Vom Kernel bis in die Domains

Einen komplett anderen Weg geht das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) in Darmstadt. Die Trennung der Bereiche erfolgt bei

Geschützt: Enterproid nutzt eine virtuelle Maschine, in der die geschäftlichen Apps geschützt sein sollen (Abb. 5).

„BizzTrust“ durch eine im Projekt „TrustDroid“ entstandene Erweiterung der Sicherheitsarchitektur von Android. Wenn SELinux innerhalb des Kernels arbeitet, ist TOMOYO-Linux eine Erweiterung, die die Schnittstelle zum Linux Security Modul (LSM) bedient und damit auf Kernel-Ebene die Ausführung der darüberliegenden Middleware samt den Apps kontrolliert. BizzTrust nutzt das Kernel-Modul und greift somit tief in Android ein – das SIT musste einiges im Code einbauen. Ein funktionierender Prototyp ist derzeit nur für das Nexus One verfügbar.

Für Linux und damit ebenso für Android ist es Standard, Zugriffe auf Objekte durch Discretionary Access Control (DAC) zu kontrollieren. Dabei hat jeder Prozess dieselben Rechte wie die Benutzer-ID, unter der er läuft, und gibt sie weiter, wenn er einen neuen Prozess startet. Das genügt für die meisten Anwendungsfälle, doch bietet das keinen fein granulierten Schutz der Daten, Ressourcen und Verbindungen (Netz und Inter Process Communication (IPC)), da die an die Benutzer-ID gebundenen Rechte nicht ausreichend das Verhalten eines Prozesses beschreiben können.

Wer eine differenziertere Rechtevergabe möchte, benutzt Mandatory Access Control (MAC). Dabei haben neben den agierenden Subjekten, den Prozessen, die zu verarbeitenden Daten und Netzwerkverbindungen, die Objekte, selbst Berechtigungen. Deren Verwaltung ist oftmals komplex, wenn man mit MAC ein Schutzziel erreichen will. Deswegen setzen es die Administratoren seltener ein, und es ist bis heute meist nur bei Anwendungen zu finden, bei denen es um Regierungsangelegenheiten und deren Geheimnisse geht. Der Vorteil besteht aber darin, dass damit Systeme realisierbar sind, die Daten unterschiedlicher Sensitivität verarbeiten dürfen. Und genau das ist das Ziel beim Separieren, daher passt der Ansatz trotz der damit verbundenen Komplexität.

Mobiles als Desktop

Ubuntu verfolgt das Ziel, Smartphones als Desktops einzusetzen. Neben der in Java geschriebenen Oberfläche richtet es auf dem Gerät eine Desktop-Umgebung ein. Es geht den Entwicklern mehr darum, mit Bildschirm und Tastatur einen vollständigen Arbeitsplatz zu schaffen, und weniger darum, das Notebook oder den Desktop zu ersetzen. Bei Ubuntu sollen alle Daten auf einem Gerät verfügbar und gleichzeitig nutzbar sein. Es vereint die Bereiche.

Einen ähnlichen Weg wie Ubuntu beschreitet Motorola mit Atrix. Die Docking-Station besteht aus Tastatur samt Display, sie erkennt das Smartphone beim Einstecken und präsentiert einen Remote-Desktop. Ebenso geht es darum, den Mitarbeitern nur ein Gerät zu geben, was Kosten und Arbeitsaufwand einsparen soll.

Anwender könnten einen Remote-Desktop ohne eine Docking-Station benutzen, was aber bei Smartphones und Tablets spitze Finger und Übung verlangt. Immerhin wären sie damit in der Lage, unterwegs Kleinigkeiten erledigen – zum Arbeiten empfiehlt es sich nicht.

Getrennt durch Rechte im Hintergrund

Für Anwender und Systemadministrator ist der Aufwand transparent; der Anwender bemerkt keinen Unterschied. Die Entwickler von BizzTrust haben zwei Domains definiert, die private und die geschäftliche. Beim Installieren einer App entscheidet das Zertifikat, das die Paket-Datei signiert hat, über die Zugehörigkeit zur Domain, in der der Kernel die App ausführen soll. BizzTrust bringt alle Einstellungen für beide Domains mit. Apps können nur innerhalb ihrer eigenen Umgebung Daten aus Kontakten auslesen, E-Mails versenden, Kanäle zur Inter Process Communication (IPC) öffnen und auf das Netz zugreifen. Außerdem sieht BizzTrust einen VPN-Kanal vor, der zum Unternehmen führt und in dem nur Apps aus der geschäftlichen Domain Daten senden dürfen.

Mit BizzTrust steht eine vollständige Umgebung samt Administrationsschicht für den sicheren Betrieb von Android-Geräten zur Verfügung, bei der das Management in der Firma die Systeme vollständig unter Kontrolle hat. Es ist damit das einzige Produkt am Markt, bei dem die Administratoren wieder die komplette Kontrolle über die eingesetzte Software erhalten. Externe Dienstleister sind nicht in den Betrieb mit einbezogen.

Fazit

Nur wenige Jahre nach dem Beginn der immer noch nicht abgeschlossenen 5. Revolution der IT-Landschaft stehen bereits mehrere Angebote zum sicheren Betrieb von Smartphones im Unternehmen zur Verfügung. Von der unsicheren, aber preiswerten Synchronisation per Active Sync über die verschlüsselten Container und die virtualisierten Umgebungen bis hin zur geheimdienstkompatiblen Trennung der Daten durch MAC auf eigens installierten ROMs ist für jedes Sicherheitsbedürfnis das Passende dabei. (rh)

CHRISTOPH PUPPE

ist seit 23 Jahren in der IT-Sicherheit aktiv und verantwortet derzeit die technischen Audits bei der HiSolutions AG in Berlin.

Literatur

[1] Jörg Riether; Mobile Computing; Zugriff zwischendurch; Administrationswerkzeuge für das iPad; *iX* 2/2012, S. 76

[2] Thomas Künneth; Mobile Computing; Kalt serviert; Neuerungen in Android 4; *iX* 1/2012, S. 72

[3] Christian Kirsch; Mobile Computing; Immer und überall; Smartphones für den Geschäftseinsatz; *iX* 7/2011, S. 78

Alle Links: www.ix.de/ix1204056