Die Kehrseiten unbegrenzter Mobility

Sicherheitsrisiko Smartphone

Der Siegeszug des Smartphones ist unaufhaltsam, die mobilen Alleskönner stellen im Jahrestakt neue Rekorde auf: Sechs Jahre nach der Markteinführung des ersten iPhones werden bereits über die Hälfte aller verkauften Handys „smart" sein (1), allein im Jahr 2012 wurden weltweit über 600 Millionen Geräte verkauft (2). Doch das mobile Büro ist Vision und Albtraum zugleich: Während der Endanwender sich über die neuen Möglichkeiten freut, Daten überall zu bearbeiten, muss das Unternehmen nun fürchten, dass wichtige, oft vertrauliche Daten unkontrollierbar in die Welt getragen werden: Wenn ein Mitarbeiter sein Tablet mit in den Urlaub nimmt, ist kaum davon auszugehen, dass er vorher die Geschäftsdaten löscht, die sich auf dem mobilen Gerät befinden und der Chef könnte sogar erwarten, dass der Angestellte diese im Notfall zur Hand hat. Im Folgenden werden wir einige der neuen Angriffsformen zeigen und entsprechende Gegenmaßnamen oder Handlungsempfehlungen vorstellen.

Der Reiz mobiler High-end-Geräte erschließt sich in einem Blick auf deren Funktionsvielfalt: Bereits ein Smartphone aus dem niedrigen Preissegment bietet eine hochauflösende Kamera, mehrere Gigabyte Speicherplatz, WLAN-, Bluetooth, NFC und einen GPS-Empfänger sowie Rechenleistung, die vor zehn Jahren noch einem high-end-Notebook vorbehalten war. Die mobilen Geräte sind einfach und schnell über Touchscreens zu bedienen. In diesen Wunderwerken der modernen Technik sind alle Funktionen aufeinander abgestimmt und der geringe Energiebedarf garantiert lange Standby-Zeiten. Und all das passt in jede Hosentasche.

Weiterhin ist allen Smartphones und Tablets gemein, dass der Benutzer über App-Stores Anwendungen herunterladen und auf dem Gerät installieren kann; auf diese

Weise lässt sich dessen Funktionsumfang noch einmal bedeutend erweitern. Neben der Funktion als Telefon, Navigationssystem, Kalender, MP3-Player und mobile Spielkonsole kann ein mobiles Gerät auch für besondere Anwendungsbereiche getrimmt werden. Ein aktuelles Beispiel ist der Medizin-/Gesundheitssektor: Blutdruck, Puls und weitere Daten werden über externe Sensoren an das Gerät versendet und dort ausgewertet. Bei kritischen Werten alarmieren die Smartphones auch gleich den betreuenden Arzt.

Der allzeit verfügbare Zugang zum Internet macht es möglich, E-Mails abzurufen, sich aktiv in sozialen Netzwerken zu beteiligen, News zu lesen oder einen Zugang zum Arbeitsplatz herzustellen. Unternehmen wie etwa jüngst Canonical mit Ubuntu propagieren eine Docking-Station, über die sich auch die Peripherie eines Desktop-Rechners mit dem Smartphone steuern lässt. Das PadPhone von Asus und Microsofts Surface-Tablet sind weitere Hinweise, dass mobile Geräte künftig verstärkt als direkte Konkurrenz zu Notebooks und Desktop-PCs positioniert werden.

Auf der Schattenseite kommen die mannigfaltigen Möglichkeiten, die ein Smartphone dem Anwender bietet, auch Angreifern entgegen: Der Zugriff auf Daten, die auf dem mobilen Gerät gespeichert sind, ist vergleichsweise einfach und Volumen sowie Wert der Daten nehmen zu. Gerade die erweiterten Möglichkeiten eines Tablets laden dazu ein, die Arbeit schon auf dem Weg zur Arbeit zu beginnen: Pendler und Geschäftsreisende können unterwegs E-Mails beantworten, Positionspapiere bearbeiten und Präsentationen erstellen. Auch hierdurch bieten sich Kriminellen neue Angriffspunkte. Doch betrachten wir die Gefahrendherde der Reihe nach.

Apps als Spionagesoftware

Moderne Smartphones sind mit einem komplexen Betriebssystem ausgestattet, das neben den grundlegenden Telefonfunktionen, Anrufe, SMS und Telefonbuch auch die Möglichkeit bietet, vom Benutzer installierte Anwendungen (Apps) zu verwalten und auszuführen. Um der täglichen Flut von über 800 neuen Apps, die im Store veröffentlicht werden wollen, Herr zu werden, gehen etwa Apple und Google unterschiedliche Wege: Während Apples App-Store über strenge Richtlinien versucht, schädliche Apps gar nicht erst in ihren Store herein zu lassen, setzt Google bei der Sicherheit auf den Benutzer: Neben automatisierten Kontrollen der Apps im Store wurde für Android ein neuartiges Sicherheitssystem vorgestellt: Will ein Benutzer eine App installieren – sei diese aus dem Store oder aus einer anderen Quelle heruntergeladen – wird zuerst eine Liste an Rechten eingeblendet, welche die App fordert. Diese Regeln den Zugriff auf Daten wie beispielsweise Kontakte, E-Mailsund Fotos aber auch die Verwendung von Hardware wie der Kamera, das Mikrofon oder der Bluetooth-Schnittstelle. Dieses Rechtesystem erlaubt die Installation von Apps, die nicht im Store gefunden werden können, ohne dabei zu viel der Sicherheit einzubüßen, die eine restriktive Kontrolle des App-Stores mit sich bringen würde. In der Praxis freilich verweigern Nutzer nur sehr selten aufgrund der Rechteliste die Installation – zu groß ist der Wunsch, die App zu nutzen. Einzelne Rechte vor der Installation auszuschließen ist nicht möglich.

Beide Vorgehensweisen haben ihre Vor- und Nachteile: Verfechter des geschlossenen App-Stores, wie Apple ihn betreibt, verweisen gerne auf das hohe Malware-Aufkommen für Android: So zielte nach einer Studie (3) Ende 2012 fast 80 Prozent aller Schadsoftware für mobile Geräte auf Android ab (zum Vergleich: 0,7 Prozent auf iOS); diese Zahlen stehen in keinem Verhältnis zum Marktanteil der Betriebssysteme. Es gibt aber auch andere Studien, die zeigen, dass reale Schadfunktionen der Malware auf den mobilen Geräten gleich verteilt sind.

Im Gegenzug erlaubt es der offene Play Store von Android, Apps einzustellen, ohne dass diese durch eine höhere Instanz überprüft und nach oft undurchsichtigen oder nicht nachvollziehbaren Kriterien abgelehnt werden. Des Weiteren können Android-Apps auch unabhängig vom Store heruntergeladen und installiert werden. Das hat für Endanwender durchaus Vorteile: Viele Apps, die Werbung unterdrücken oder bei unsachgemäßer Handhabe die Stabilität des Betriebssystems beeinträchtigen können, werden nicht im Play Store gelistet. Auf der anderen Seite lassen sich so – sehr zum Leidwesen der App-Entwickler – auch gecrackte Apps und illegale Kopien kostenpflichtiger Apps problemlos installieren.

Natürlich hat die offene Vertriebspolitik für Android-Apps auch Nachteile. Zwar kann ein erfahrener Benutzer über die geforderten Berechtigungen einschätzen, ob eine App vertrauenswürdig ist, allerdings prüfen die wenigsten Benutzer die Berechtigungen einer neuen App und hebeln so einen essenziellen Sicherheitsmechanismus von Android aus. Weiterhin kann ein kreativer Malware-Entwickler die geforderten Berechtigungen legitim erscheinen lassen: Eine App, die Sprachnotizen aufnimmt, braucht Zugriff auf das Mikrofon – ob sie zusätzlich als Wanze missbraucht wird, ist vom Benutzer nicht mehr zu erkennen.

Ein grundsätzliches Problem ist das vorherrschende Geschäftsmodell „Bezahlen mit persönlichen Daten". Zahlreiche Apps werden so kostenlos bereitgestellt, alles, was vom Benutzer verlangt wird, sind ein paar persönliche Daten als „Zahlungsmittel". Konkret bedeutet das: Die Finanzierung der App-Entwicklung erfolgt über die Vermarktung persönlicher Daten, die die Anbieter entweder weiter verkaufen oder nutzen, um personalisierte Werbung zu schalten.

Standortbasierte Dienste

Durch den eingebauten GPS-Empfänger kann ein Smartphone auf wenige Meter genau lokalisiert werden. Außerdem werden über die Basisstationen der Mobilfunkanbieter und mit der Hilfe von WLAN-Karten weitere Quellen verwendet, um schnell eine Standortbestimmung durchzuführen. Mit Wissen seines Standorts kann das mobile Gerät den Weg zeigen, Hotels, Restaurants und Kinos in der Nähe finden und Fahrpläne des öffentlichen Nahverkehrs durchstöbern. Da diese Dienste meist kostenlos angeboten werden, ist auch hier anzunehmen, dass die über die Weitergabe von persönlichen Daten an Werbetreibende finanziert werden.

Auch ist es möglich, mithilfe dieser Standortdaten ein Bewegungsprofil zu erstellen, das mehr verrät, als auf den ersten Blick ersichtlich: So kann ein längerer Aufenthalt im Büro einer konkurrierenden Firma ein Indikator für eine zukünftige Übernahme sein; der Aufenthalt des Chefs in der Wohnung der Sekretärin deutet auf eine Affäre hin. Die Beispiele ließen sich endlos fortsetzen.

Öffentliche Hotspots

Smartphones und Tablets werden zwar meist mit Verträgen über eine Internet-Flatrate verkauft. Diese umfasst aber nur ein begrenztes Transfervolumen, bevor die Verbindungsgeschwindigkeit drastisch herabgesetzt wird. Aus diesem Grund erfreuen sich öffentliche WLAN-Hotspots, an denen das Internet abseits dieser Grenzen benutzt werden kann, weiterhin großer Beliebtheit. Es ist sogar anzunehmen, dass durch die Verbreitung mobiler Geräte die Nutzung von Hotspots zunimmt. Das größte Sicherheitsproblem solcher Hotspots ist, dass es praktisch unmöglich ist, seinen Betreiber eindeutig zu identifizieren und die Vertrauenswürdigkeit zu bewerten: Ein Angreifer kann einen solchen Hotspot mit dem Namen „Free-Network" zum Beispiel in einem Café oder sonstigen öffentlichen Ort mimen und darauf warten, dass sich ein mobiles Gerät verbindet, um ins Internet zu kommunizieren. Diese Verbindung muss nicht in jedem Fall vom Opfer initiiert werden: Wurde in der Vergangenheit bereits ein WLAN mit demselben Namen (zum Beispiel „Free-Network") wie der Hotspot besucht, so verbinden sich viele mobile Geräte automatisch mit dem Hotspot des Angreifers. Der Angreifer kann aber auch Namen weit verbreiteter Hotspots wie „Telekom", „Vodafone" etc. nutzen, um Opfer in seinen Angriffs-Hotspot zu locken.

In jedem Fall kontrolliert der Angreifer alle über den Hotspot gesendeten Daten und kann die gesamte Kommunikation mitlesen. Stark besuchte Orte wie beispielsweise Flughäfen, Cafés etc., an denen Nutzer „nur mal eben E-Mails checken" wollen, werden so zu einer wahren Fundgrube von sensiblen Informationen und einer sehr großen Gefahr für den Nutzer, weil Zugangsdaten und weitere vertrauenswürdige Informationen mitgelesen werden können.

Parallele Nutzung von Geräten für Arbeit und Freizeit

Aus Kosten- oder Akzeptanzgründen erlauben oder tolerieren viele Firmen die Benutzung eines einzelnen privaten Geräts für die Arbeit. Dieser Trend, Consumerization oder BYOD (Bring Your Own Device) genannt, führt zu neuen Herausforderungen in der Unternehmenssicherheit. Nicht ohne Grund beäugen Sicherheitsexperten diese Entwicklung kritisch, da sie verschiedene neue Angriffe ermöglicht: Ein Angreifer kann über das mobile Internet des Smartphones die zentralen Sicherheitsmaßnamen des Firmen-Netzwerks umgehen und auf diesem Weg über das mobile Gerät das interne Firmen-Netzwerk angreifen. Aber auch ohne Zugang zum internen Firmennetz findet ein Angreifer oft eingespeicherte Passwörter, (firmeninterne) vertrauenswürdige oder datenschutzrelevante E-Mails und weitere Informationen auf dem mobilen Gerät, die ihm helfen, sein Ziel anzugreifen oder direkt zu schädigen.

Gerade Consumer-Smartphones verfügen nur über begrenzte Sicherheitsmaßnamen, um gespeicherte Daten zu schützen und die wenigsten Nutzer aktivieren diese auch. Die Geräteverschlüsselung, die verhindern kann, dass ein Angreifer Daten aus einem ausgeschalteten mobilen Gerät ausliest, ist meist standardmäßig deaktiviert. Statt einer PIN-Eingabe, um den Bildschirm zu entsperren, wird das allseits beliebte Wischmuster, bei welchem über eine Touch-Geste Punkte verbunden werden müssen, verwendet. Hier kann der Angreifer das Opfer entweder bei Eingabe der Geste beobachten oder anhand der Spuren auf dem Touchscreen, die das Wischen hinterlässt, das Muster rekonstruieren.

Verlust des Geräts

Ein Smartphone ist handlich und leicht – und deswegen praktisch immer dabei. In der Praxis ist es aber deswegen aber auch schon mal schnell verloren. Allein in Londoner Taxis werden pro Jahr über 60.000 Geräte liegen gelassen (4). Hinzu kommt gezielter Diebstahl, etwa durch Anheuern eines Taschendiebs. Wird das Smartphone für geschäftliche E-Mails oder Termine verwendet, ist ein gezielter Diebstahl ein beliebter und einfacher Weg, um Industriespionage zu betreiben.

Aber auch ein versehentlicher Verlust kann schwere Folgen haben: Eine Studie von Symantec (5) ergab, dass in 40 Prozent aller Fälle versucht wurde, die Firmen-E-Mails auf einem gefundenen Smartphone zu lesen und auf Bankdaten zuzugreifen.

Root-Exploits

Ein Root-Exploit ermöglicht praktisch die Übernahme des mobilen Geräts, indem ein Angreifer über eine Sicherheitslücke Administrator-Privilegien erhält. Dies kann geplant geschehen, wenn ein Benutzer sein Gerät rooten (Android) beziehungsweise jailbreaken (iPhone) will, um Einschränkungen des Betriebssystems zu umgehen oder Apps von alternativen Quellen zu installieren (iPhone).

Als Teil eines Angriffs ist dieser Vollzugriff ein mögliches Ziel für den Angreifer, da er so er sämtliche Sicherheitsmechanismen des mobilen Geräts umgehen kann: Er erlaubt ihm nicht nur, Daten auszulesen, sondern auch, Apps zu installieren, Ein-

stellungen zu ändern und Eingaben mitzulesen.

Wird ein solcher Root-Exploit bekannt, kann es oft mehrere Wochen bis Monate dauern, bis die Sicherheitslücke behoben wird (der Evasi0n-Jailbreak für iOS 6 von Apple war über einen Monat im Umlauf, bevor ein Update verfügbar war; ebenso der Exynos-Exploit für Samsung-Geräte) — genug Zeit für einen Angreifer, um ein mobiles Gerät zu kapern. Leider sind selbst die großen Firmen wie Apple und Samsung bei diesen kritischen Sicherheitslücken sehr langsam, wenn es darum geht, für Abhilfe zu sorgen. Durch den besonderen Erfolg von Samsung,wächst die Liste der Angriffe, die nur auf Samsung-Geräte exploiten können, zurzeit sehr stark. Insbesondere bei Apple, eine der wertvollsten Firmen der Welt, wäre eine höhere Verantwortung für die Sicherheit ihrer Kunden zu erwarten. Im Bereich IT-Sicherheit sollten die Kunden deutlich mehr Verantwortung von den Herstellern fordern.

Gegenmaßnamen

Um die neuen Unsicherheiten, die ein mobiles Gerät „by design" mit sich bringt, einzugrenzen, empfiehlt sich für Firmen die Nutzung einer Mobile Device Management (MDM)-Software. Sowohl Google als auch Apple stellen hierzu eine spezielle Administrationsschnittstelle bereit, die Administratoren verwenden können. Ein MDM kann Funktionen deaktivieren, Einstellungen verbergen oder forcieren und setzt so ganzheitliche Sicherheitsrichtlinien durch.

Ein neuer Trend, um eine höhere Sicherheit bei mobilen Geräten zu erzielen, ist die Nutzung von sogenannten Virtualisierungs- und Isolierungslösungen, bei denen auf einem mobilen Gerät zwei Instanzen des Betriebssystems parallel ausgeführt werden; sozusagen zwei „Smartphones" auf einem mobilen Gerät. Der Vorteil ist, dass eine Instanz für den privaten Gebrauch verwendet werden kann, in welche auch unsichere Apps wie Spiele installiert werden können. Die andere Instanz ist die „Business-Instanz", in der sicherheitsrelevante Apps und Daten wie zum Beispiel geschäftliche E-Mails und Firmenanwendungen residieren. Diese Trennung schützt vor Angriffen auf Firmendaten und -infrastrukturen aus einer unsicheren App heraus. Die Kommunikation in das Firmennetz ist nur aus der sicheren Business-Instanz heraus und über ein VPN möglich. Zusätzlich sind in diesen Isolations-Lösungen auch die Mobile Device Management-Funktionen integriert. Solche Lösungen werden beispielsweise von T-Systems unter dem Namen „SiMKo 3" oder von Sirrix unter „BizztrusT" (6) angeboten und bieten eine sehr gute Sicherheit.

MDM-Lösungen sowie Virtualisierungs- und Isolierungslösungen sind allerdings primär für Unternehmen ausgelegt und preislich sowie aufwandstechnisch entsprechend gestaltet. Die Komplexität, eine solche Business-Lösung zu managen, ist für Privatpersonen zu hoch, weshalb die folgenden einfachen Sicherheitsmaßnahmen auf jeden Fall ergriffen werden sollten:

Um die Angriffsfläche eines mobilen Geräts zu minimieren, empfiehlt es sich, das mobile Gerät, soweit es die Nutzung zulässt, einzuschränken: Deaktivieren Sie WLAN und GPS, solange diese nicht explizit verwendet werden müssen. Das mobile Datennetz ist deutlich schwieriger abzuhören als ein WLAN und die präzise Ortung des mobilen Geräts ist ohne WLAN schwieriger und langsamer. Vermeiden Sie die Installation unnötiger Apps! Gerade bei iOS-Geräten ist nicht ersichtlich, ob und welche Daten eine App ausliest und versendet. Da der Google Play-Store nicht den scharfen Kontrollen seines Apple-Pendants unterliegt, ist es extrem wichtig, vor der Installation einer Android-App die geforderten Berechtigungen genau zu prüfen sowie Bewertungen und Kommentare zur App zu lesen. Bei der Kontrolle der Berechtigungen sind diese auf Sinnhaftigkeit zu prüfen: Eine Taschenlampen-App, die das Adressbuch auslesen will, sollte ein absolutes No-Go sein.

Speziell für Android existieren verschiedene Programme wie AppGuard, LBE Privacy Guard oder SecDroid, die das mobile Gerät durch Kernel-Patches oder die Fähigkeit, Apps Berechtigungen zu entziehen, sicherer machen sollen. Allerdings können solche Lösungen die Stabilität des Systems gefährden und sollten nicht unbedacht eingesetzt werden.

Zusammenfassend lässt sich sagen, dass ein Smartphone — unbedacht eingesetzt — ein beträchtliches Risikopotenzial mitbringt. Dieses lässt sich durch geeignete Sicherheitsmaßnahmen reduzieren. Im privaten Umfeld sollte dies mindestens durch eine Reduzierung der Angriffsfläche geschehen. Ein Unternehmen kann durch die Verwendung eines MDM-Systems das Risiko weiter reduzieren und die Einhaltung von Sicherheitsrichtlinien forcieren. Durch die Verwendung von Virtualisierungs- und Isolierungslösungen ist eine deutliche sichere Nutzung von Smartphones möglich. ■

Michael Lamberty,
studentischer Mitarbeiter im Bereich „Mobile Security" am Institut für Internet-Sicherheit - if(is) an der Westfälischen Hochschule Gelsenkirchen

Norbert Pohlmann,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit - if(is) an der Westfälischen Hochschule Gelsenkirchen

(1) http://nydus.org/news/13907.html
(2) http://www.gartner.com/newsroom/id/2227215
(3) http://www.f-secure.com/static/doc/labs_global/Research/Mobile%20Threat%20Report%20Q4%202012.pdf
(4) http://news.bbc.co.uk/2/hi/7620569.stm
(5) http://edition.cnn.com/2012/03/20/tech/mobile/lost-smartphones-security