COMPUTERWOCHE

Link: http://www.computerwoche.de/a/mobile-plattformen-im-security-check,2544468

Android, iOS, BlackBerry, Windows Phone

Mobile Plattformen im Security-Check

Datum: 22.08.2013
Autor(en): Stefan Strobel, Christopher Dreher
URL: http://www.computerwoche.de/2544468

Jedes der vier mobilen Betriebssysteme weist Sicherheitslücken auf. Android und iOS sind vermeintlich anfälliger als BlackBerry und Windows Phone. Unternehmen müssen bei der Auswahl aber auch andere Aspekte berücksichtigen.

Mobile Geräte sorgen für Kopfschmerzen bei den Sicherheits-Verantwortlichen.
Foto: fotolia.com/Benicce

Smartphones und Tablets drängen immer stärker in die Unternehmen. Die Geräte wurden in der Regel aber nicht speziell für den beruflichen Einsatz entwickelt, sondern kommen aus dem Consumer-Bereich. iPhones und iPads, Smartphones und Tablets mit Googles Android oder die neuen Geräte mit Windows Phone 8 sind dabei am stärksten gefragt. **BlackBerry**[1] indes adressiert eher die Unternehmen, wenn auch erste Gehversuche in Richtung B2C-Market unverkennbar sind.

Die Anwenderunternehmen stehen damit vor der Herausforderung, die Geräte sinnvoll zu integrieren und dabei die neuen Bedrohungen und Sicherheitsaspekte angemessen zu berücksichtigen. Die Auswahl der Geräte und speziell deren Betriebssystem haben dabei einen wichtigen Einfluss auf die Sicherheit der Unternehmensdaten, die auf den Geräten gespeichert werden können oder von dort aus erreichbar sind.

Während die aktuellsten BlackBerrys ebenso wie die Windows-Phone-8-Smartphones noch recht neu sind und die Sicherheitsversprechen der Hersteller bisher kaum verifiziert oder widerlegt wurden, gibt es zu Googles Android und Apples iOS viele Untersuchungen und Veröffentlichungen. Die meisten sicherheitsrelevanten Eigenschaften oder Probleme von Android liegen demnach in seiner Offenheit und der früheren Trennung von Hardware-Lieferant und Betriebssystem-Hersteller begründet.

So gibt es außer von Google selbst kaum Geräte, die schon mit der neuesten Version von Android aufwarten können - die meisten laufen noch mit stark veralteten Versionen wie Android 2 oder 3. Ein nachträgliches Update des Betriebssystems ist zudem oft nicht möglich. Anwender müssen also mit bekannten Sicherheitsdefiziten leben, ohne etwas dagegen tun zu können. Für Unternehmen, die Patch-Management ernst nehmen, ist dies natürlich kein befriedigender Zustand.

Malware im Überfluss

Ähnlich sieht es mit der Viren-Problematik aus. Da Android als offene Plattform die **App-Stores**[2] verschiedener Anbieter erlaubt, hat die Plattform **ein ernstes Malware-Problem**[3]. Zwar ist Malware prinzipiell auch auf den drei anderen mobilen Betriebssystemen denkbar, aktuelle Fallzahlen belegen jedoch, dass der größte Teil bekannter Schädlinge für Smartphones und Tablets auf Android zielt. Bei Apples iOS geht es indes eher um prinzipielle Machbarkeitsbeweise (Proofs of Concept), dass Malware hier grundsätzlich funktionieren könnte. Ohne eine Manipulation der Geräte (Jailbreaking, Rooting) lassen sich auf Apple-Geräten schließlich nur Apps aus Apple-eigenen Quellen installieren - dank der dortigen restriktiven Prüfung ist das Risiko einer "Ansteckung" aber gering.

Andere Bedrohungen treffen Geräte mit iOS aber ebenso hart wie solche mit Android. Dazu gehört das Risiko eines Datenabflusses über Systemfunktionen, die beispielsweise GPS-Daten zwischenspeichern, Tastendrücke aufzeichnen oder Screenshots von laufenden Apps machen. Bei Apple-Geräten wird bei Druck auf die Home-Taste der Displayinhalt der zuletzt laufenden App in einer Animation verkleinernd dargestellt. Dafür macht das Betriebssystem zunächst einen Screenshot und animiert diesen dann. Der Screenshot ist für einen normalen Benutzer nicht sichtbar. Wer jedoch den gesamten Flashspeicher des Geräts ausliest, kann auf ihn zugreifen. Gleiches gilt für die Tastatureingaben, die bei beiden Plattformen für die Rechtschreibkorrektur oder die Komfortfunktionen zwischengespeichert werden.

Das Auslesen des kompletten Speichers inklusive der Systemdateien ist bei Android-Geräten meist über den Debug-Modus möglich. Bei älteren iPhones wie dem iPhone 3GS oder dem iPhone 4 ermöglicht ein Fehler im **Boot-ROM**[4] das Auslesen. Die Verschlüsselungsfunktionen des Betriebssystems und ein gesetzter PIN-Code schützen dabei nur E-Mails und die Keychain, in der Zertifikate und Schlüssel gespeichert sind. Die gespeicherten Screenshots, Tastatureingaben, GPS-Bewegungsdaten und die Daten der meisten Apps lassen snjch von Dieben oder unehrlichen Findern ohne Probleme auslesen.

[Hinweis auf Bildergalerie:] gal1

Jailbreaking

Diese exemplarische Code Injection bei der Passbook App auf einer gejailbreakten iPhone 4S sorgt nur für eine Warnmeldung. Im Ernstfall hätte der Angreifer Zugriff auf alle in der App hinterlegten Daten, wie beispielsweise Boardkarten für Flüge oder Eintrittskarten zu Veranstaltungen.
Foto: Cirosec

Ein weiteres Problem bei iOS- und Android-Hardware ist das sogenannte **Jailbreaking**[5] (iOS) respektive **Rooting**[6] (Android). Hierbei schalten Anwender die Schutzmechanismen der Geräte teilweise ab, um einen Zugang mit administrativen Rechten zum Betriebssystem zu bekommen. Typischerweise wird dabei ein SSH-Server installiert, über den sich der Anwender mit einem Terminalprogramm als Benutzer "root" anmelden kann und dann über alle Rechte auf dem System verfügt.

Auf einem gejailbreakten oder gerooteten System kann der Benutzer tief in das System hineinsehen, Systemdateien ändern und beliebige Software installieren. Der Code-Signing-Mechanismus, der auf Apple-Geräten die Installation von Nicht-Apple-Software verhindert, wird abgeschaltet, was auch bösartigen Malware-Programmen die Türen öffnet.

Die Motivation für einen Jailbreak oder ein Rooting können vielfältig sein. Manchen Anwendern geht es nur darum, die volle Kontrolle über ihr Gerät zu bekommen und deren interne Details sehen und vielleicht verstehen zu können. Andere wollen sich nicht vom Hersteller vorschreiben lassen, welche Apps installiert werden dürfen und welche nicht. Früher war ein Jailbreak teilweise notwendige Voraussetzung, um den so genannten "Net-Lock" abzuschalten, die Bindung des Geräts an einen bestimmten Mobilfunkprovider.

In jedem Fall schaltet ein Jailbreak bei iOS-Geräten ebenso wie das Rooting unter Android wichtige Sicherheitsfunktionen ab und macht die Geräte angreifbarer. Apps sind nicht mehr an die Grenzen einer Sandbox gebunden, sondern können selbst mit administrativen Rechten ablaufen. So entstehen Bedrohungen, bei denen eine Malware auf einem gejailbreakten iPhone oder iPad - und bei iOS ist Malware ohnehin nur auf gejailbreakten Systemen naheliegend - andere Apps und deren Daten angreifen kann.

Geräte mit vielen Unbekannten

Geräte mit Microsofts Windows Phone 8 und der aktuellen BlackBerry-Version 10 stehen hier auf den ersten Blick besser da. In beiden Fällen gibt es noch keine öffentlich bekannte Möglichkeit, den kompletten Speicher auszulesen. Telefone mit Windows Phone 8 werden mit einem **TPM-Chip**[7] ausgeliefert, der für einen sicheren Bootvorgang sorgt.

Das Dateisystem auf dem Flash-Speicher lässt sich zudem mit **BitLocker**[8] verschlüsseln, sofern ein MDM-System zum Einsatz kommt. Da bislang kein Jailbreak bekannt ist, können selbst Sicherheitsforscher nicht in die Details des Betriebssystems hineinsehen und prüfen, welche Daten möglicherweise zwischengespeichert werden oder wo sonstige Sicherheitslücken liegen könnten.

Ähnliches gilt für den neuen BlackBerry, über dessen proprietäre Plattform seit jeher kaum interne Details öffentlich wurden. Die Geheimhaltung sicherheitsrelevanter Interna muss jedoch nicht immer positiv sein. Erst Mitte Juli fanden Sicherheitsforscher heraus, dass die Einrichtung der POP-3- und Imap-Mailkonten auf BlackBerry-10-Geräten standardmäßig über einen Server der Herstellerfirma Research in Motion (RIM), der in Kanada lokalisiert ist, abläuft.

Eingebauter Schutz ist wackelig

Bei einem gejailbreakten iPhone 4 mit Fehler im Boot-ROM dauert das Bruteforcing des Passcodes bei vier Ziffern nur 15 Minuten. Bei neun Ziffern sind es immerhin 2,5 Jahre und bei sechs alphanumerischen Zeichen 5,5 Jahre.
Foto: Cirosec

Unternehmen, die Mobilgeräte einsetzen, legen Wert darauf, dass die bereits eingebauten Schutzfunktionen ihren Zweck auch erfüllen. In iOS sind Features wie die Dateisystemverschlüsselung und die sichere Ablage von Zertifikaten und Schlüsseln in der geschützten Keychain nur dann gewährleistet, wenn die entsprechenden Devices mit einem PIN-Code versehen sind (nicht zu verwechseln mit dem SIM-PIN, welcher zum Einbuchen der Geräte in die Mobilfunknetze benötigt wird).

Die Robustheit de Sicherheitsfunktionen ist demnach auch stark von der Komplexität des gewählten PIN-Codes abhängig. Durch die bereits erwähnte Schwachstelle innerhalb des Boot-ROMs bei allen iOS-Geräten, die vor dem iPhone 4S erschienen sind, können die vierstelligen PIN-Codes - wie sie etwa bei aktiviertem PIN-Schutz vorliegen - in durchschnittlich 20 Minuten geknackt werden. Will ein Anwender eine komplexere PIN setzen, so muss er explizit eine Zusatzoption in den Einstellungen seines Gerätes aktivieren.

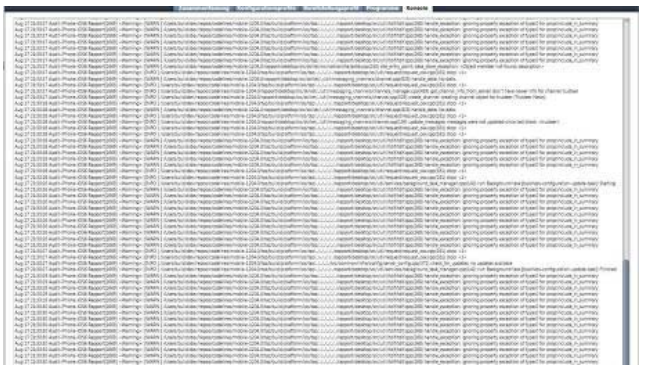
Was Android angeht, lässt sich in diesem Punkt keine allgemeinverbindliche Aussage treffen - dafür sind die Unterschiede zwischen den verfügbaren Geräten zu groß. So gibt es welche, die bereits hardwareseitig über ein Kryptomodul verfügen und dadurch - ähnlich wie bei Apple - eine robuste Verschlüsslung sensibler Daten ermöglichen, wenn ein komplexer PIN-Code gesetzt wurde. Beispielhaft hierfür sind die Referenzgeräte von Google selbst.

Die meisten erhältlichen Android-Devices können solch ein Kryptomodul jedoch noch nicht vorweisen und legen Daten in unverschlüsselter Form ab. Der PIN-Code schützt hier nur gegen unmittelbare Zugriffe. Durch die offengelegte Debug-Schnittstelle lassen sich die Daten auch ohne den korrekten PIN-Code auslesen.

Gegenmittel und Strategie

Unternehmen setzen meist eine Mobile-Device-Management-Lösung (MDM) ein, um mit allen betriebenen Geräten das gewünschte Sicherheitsniveau zu erreichen. Diese MDM-Lösungen dienen der Verwaltung von mobilen Endgeräten und ermöglichen eine plattformübergreifende Verteilung von Einstellungen und Restriktionen. Alle mobilen Betriebssystemplattformen bieten spezielle MDM-Schnittstellen zur Anpassung der Sicherheitsparameter an. Das kann die Mindestlänge des PIN-Codes sein, die Zulassung oder der Ausschluss bestimmter Apps oder das Auslösen eines "Remote Wipe" beim Verlust eines Gerätes.

Per MDM ebenfalls möglich ist die Verwaltung von Privatgeräten am Arbeitsplatz (ByoD). In Deutschland bringt der rechtliche Rahmen (Datenschutz, Mitbestimmung etc.) derartige Projekte jedoch meist zum Scheitern. Die verantwortlichen Unternehmensentscheider sollten deshalb über fundiertes Rechtswissen verfügen oder externe Beratung in Anspruch nehmen, bevor sie entsprechende Pläne in die Tat umsetzen.



Bei iOS-Geräten werden alle Ausgaben, welche über die NSLog-Funktion in der Applikation protokolliert werden, auf der Konsolenausgabe im iPhone-Konfigurationsprogramm für jedermann lesbar ausgegeben.
Foto: Cirosec

Ohne MDM-Lösung muss die Sicherung von Unternehmensdaten anders erreicht werden. Mehrere Hersteller bieten beispielsweise plattformübergreifende Container-Lösungen an. Diese Container-Apps verlassen sich nicht alleine auf die Sicherheitsmechanismen der Geräte, sondern bringen eigene Features und Policies mit. Sie kapseln die sensiblen Unternehmensdaten in eigenen verschlüsselten Bereichen und sorgen dafür, dass die Daten das Gerät nur auf vorher festgelegten Transportwegen verlassen. Die Gefahren liegen hier im technischen Detail.

Aufgrund der bereits erwähnten Sandbox-Mechanismen der verschiedenen Plattformen steht auch den Container-Apps nur eine begrenzte Anzahl an Mechanismen zur Verfügung, um das Sicherheitsniveau des jeweiligen Endgerätes festzustellen. In der Regel verweigern die Apps ihre Funktion, wenn sie feststellen, dass sie auf einem nicht vertrauenswürdigen Gerät, welches gejailbreaked oder gerooted wurde,

ausgeführt werden. Durch die begrenzten Mechanismen zur Überprüfung des Gerätezustandes gibt es jedoch prinzipiell immer die Möglichkeit, die Containter-Apps zu täuschen.

Ohne die Sicherheitsmechanismen der Betriebssystem-Sandbox lässt sich die App gezielt analysieren und dort vorhandene Security-Features aushebeln.

[Hinweis auf Bildergalerie:] gal2

Backup - der Anwender liebstes Kind

Die Auswahl eines mobilen Betriebssystems hat nicht nur Auswirkungen auf die Sicherheit der Daten auf dem Gerät selbst. Jedes Betriebssystem bringt auch unterschiedliche Backup-Mechanismen mit und kopiert damit potenziell vertrauliche Unternehmensdaten auf weitere IT-Systeme.

Wird zum Beispiel ein iOS-Gerät mit Apple iTunes gekoppelt, macht iTunes in der Standardkonfiguration zunächst ein lokales Backup, welches fast sämtliche Inhalte des mobilen Gerätes beinhaltet. Wenn auf dem mobilen Endgerät kein spezielles Sicherheitsprofil vorhanden ist, wird das lokale Backup möglicherweise sogar unverschlüsselt auf der Festplatte eines Privat-PCs abgelegt.

Die Sicherheit von Unternehmensdaten hängt dann von der Sicherheit der Privat-PCs der Mitarbeiter ab… Nicht weniger bedenklich ist eine Sicherung der Daten in der Cloud der jeweiligen Hersteller. Dass die amerikanischen Nachrichtendienste hierauf Zugriff nehmen, ist inzwischen hinlänglich bekannt. Aber auch unabhängig von Geheimdiensten werden immer wieder neue Sicherheitsdefizite und Datenverluste bei Cloud-Diensten bekannt.

Bei den Android-Geräten gibt es zum jetzigen Stand keine einheitliche Backup-Lösung. Viele der angebotenen herstellerübergreifenden Produkte erfordern Root-Privilegien, weil es schlichtweg noch keine Schnittstelle gibt, welche Google für diesen Zweck anbieten könnte. Aus diesem Grund haben einzelne Hersteller eigene Backup-Mechanismen für ihre Geräte in das Andoid-Betriebssystem eingebunden, welche jedoch ähnliche Gefahren wie Apples iOS aufweisen.

Was bringt iOS 7?

In den kommenden Tagen wird Apple mit **iOS 7**[9] vielversprechende Neuerungen für alle iOS-Geräte ab dem iPhone 4 bzw. iPad2 einführen. Gerade im Sicherheitsumfeld kann durch die neuen Funktionen ein höheres Schutzniveau erreicht werden. So ist es dann zum Beispiel möglich, für Apps, welche sensible Firmendaten verarbeiten und austauschen, den Transport der Daten über einen eigenständigen VPN-Tunnel abzusichern. Des Weiteren wird die Dateisystemverschlüsselung global für alle Apps aktiviert. Bisher mussten Entwickler selber dafür Sorge tragen, dass sensible Daten innerhalb der App mit der Dateisystemverschlüsselung (Apple Data Protection) abgesichert sind. (sh)

Mobile Betriebssysteme im Sicherheits-Vergleich

	iOS	**Android**	**Windows Phone 8**	**BlackBerry 10**
Jailbreak/Rooting	ja, bei iOS <6.1.3	ja	nein	nein
Dateisystemverschlüsselung	ja (in iOS 4.3 mit Passcode, in iOS 6.x mit Apple Data Protection innerhalb der Apps)	ja (ab 3.0 mit Unlock-Code, Verschlüsselung auf Dateisystemebene)	ja (per ActiveSync lässt sich BitLocker aktivieren, sofern ein MDM-System zum Einsatz kommt)	ja (mit BlackBerry Balance / Dateisystemtrennung privater und beruflicher Daten; erfordert BlackBerry Enterprise Server 10)
Sicherheit der Plattform	+	--	++	+
App-Verfügbarkeit	++	++	-	--
App-Sicherheit	++	--	++	+
Sideloading von Apps	nein	ja	ja	ja

Quelle: Cirosec

Links im Artikel:

[1] **http://www.computerwoche.de/k/blackberry,3469**
[2] **http://www.computerwoche.de/a/wie-sicher-sind-die-app-stores,2519593**
[3] **http://www.computerwoche.de/a/android-anwender-in-der-schusslinie,2537328**
[4] **http://de.wikipedia.org/wiki/Boot-ROM**
[5] **http://de.wikipedia.org/wiki/Jailbreak_(iOS)**
[6] **http://de.wikipedia.org/wiki/Softmod**
[7] **http://www.computerwoche.de/a/hardware-basierte-sicherheitskonzepte-in-windows-8,2533196**
[8] **http://de.wikipedia.org/wiki/BitLocker**
[9] **http://www.computerwoche.de/a/apple-zeigt-business-features-von-ios-7,2541390**