



iPhone und iPad Security: The Good, the Bad and the Ugly

Apple ist derzeit eine der erfolgreichsten IT-Firmen; die Geräte mit dem iOS-Betriebssystem (iPhone und iPad) sind auf dem IT-Markt die größten Innovationen der letzten Jahre. Es kann nicht Aufgabe der Unternehmenssicherheit sein, diese Innovationen einfach abzulehnen. Vielmehr müssen sich die IT-Sicherheitsverantwortlichen mit den Geräten beschäftigen und innovative Lösungen finden, um diese sinnvoll in die Sicherheitsstruktur eines Unternehmens zu integrieren.



Florian Oelmaier leitet das Fachgebiet IT-Sicherheit und Computerkriminalität bei der Firma Corporate Trust – Business Risk & Crisis Management GmbH. Seine Spezialgebiete sind das Thema „mobile Security“ sowie aktuelle Angriffe auf Applikationen und Netzwerke, Sicherheitskonzeptionen in Softwareprojekten und ein sicherheitstechnisch und methodisch korrektes Vorgehen im Softwareentwicklungsprozess.

Dabei gibt es einen Aspekt, den sowohl Benutzer als auch IT-Sicherheitsverantwortliche an Apple schätzen: die Vorliebe für einfaches, simples Design. Anwender lieben diese Philosophie, weil sie nicht mit vielen (für sie oft unnötigen) Funktionen konfrontiert werden und IT-Sicherheitsexperten wissen, dass Komplexität der größte Feind der Sicherheit ist.

iOS-Security: The Good

Eine Plattform, auf der sich technisch nur Software installieren lässt, die vorher von Experten auf Herz und Nieren geprüft wurde? Bei der Software, die sich als schadhaft erweist, remote zurückgerufen und gelöscht werden kann? Auf der jedes Softwareprodukt in einem eigenen Container läuft und keinen Zugriff auf die Dateien des Betriebssystems oder anderer Softwareprodukte hat? Auf der Software nur mit einer klar definierten Anzahl von Funktionen auf die Hardware zugreifen darf?

Welcher IT-Sicherheitsverantwortliche hat noch nie von so einer Plattform geträumt? Die iOS-Plattform bietet das alles. Apple prüft jede Software, bevor sie in den App Store gelangt. Dabei werden sowohl einfache Sichtprüfungen (die App

funktioniert und stürzt bei oberflächlicher Benutzung nicht ab) als auch automatisierte Codeprüfungen (die App benutzt nur die freigegebenen API-Aufrufe des „Cocoa Touch Framework“, die App lädt keinen Code nach, etc.) eingesetzt. Da Apple dieses System regelmäßig und häufig benutzt, werden die Tools dafür ständig verbessert. Angesichts über 300.000 geprüfter Apps im App Store, von denen viele bereits in der zweiten, dritten oder vierten Version vorliegen, kann zu Recht von der größten Codereview-Aktion der Geschichte gesprochen werden.

Sowohl bei Android als auch in der herkömmlichen PC-Welt kann ungeprüfte Software aus dem Internet installiert werden. Und auch die Möglichkeit der Beschränkung auf digital signierte Software bringt nicht die Sicherheit, wie sie eine zentrale Softwareverteilung à la App Store bietet. Dazu kommt, dass maschinelle Codeprüfungen unter Windows kaum möglich sind – unzählige Programmiersprachen und viele Betriebssysteminterfaces (.NET, ATL/STL, MFC, WinAPI) erhöhen die Komplexität von Reviews immens.

Jede App wird in ein Unterverzeichnis installiert. Mit einem in der Unix-Welt altbekannten Verfahren („chroot“) wird der Zugriff jeder App auf Betriebssystemebene auf ihr eigenes Unterverzeichnis beschränkt. Es gibt keinen Teil der Applikation, der irgendwo außerhalb dieses Verzeichnisses landet (keinen Desktop, keine „eigene Dateien“, keine Registry, kein „\Windows\System32“, kein „\Programme\Gemeinsame Dateien“). Selbst die Menüapplikation (Springboard) muss alle Unterverzeichnisse durchsuchen, um die Icons der installierten ▶

[In diesem Beitrag lesen Sie:](#)

- warum das iOS-Betriebssystem eine sichere Plattform ist,
- wie gefährliche Jailbreaks wirklich sind,
- worauf Sie beim Kauf von iPhone und iPad für Ihre Firma achten müssen.



Programme „einzusammeln“. Dieser Paradigmenwechsel verhindert nicht nur viele Schadfunktionen (Welchen Spaß macht eine Schadfunktion, die nur die eigene Applikation schädigen kann?), sondern erlaubt auch das hundertprozentig rückstandsfreie Entfernen von Apps. Viele Windows-Benutzer vermissen eine solche Möglichkeit in ihrem System schmerzlich – und installieren deswegen regelmäßig den Rechner neu.

Apps können von zentraler Stelle aus remote zurückgerufen werden. Bei der nächsten Onlineverbindung wird die App dann vom Gerät gelöscht. Für Unternehmen bietet Apple mit dem „iOS Developer Enterprise Program“ die Möglichkeit, Teile dieser Infrastruktur selbst zu verwalten.

Wo sehen Sie die größten Bedrohungen für die Sicherheit Ihrer IT und Telekommunikation? (Mehrfachnennungen möglich)

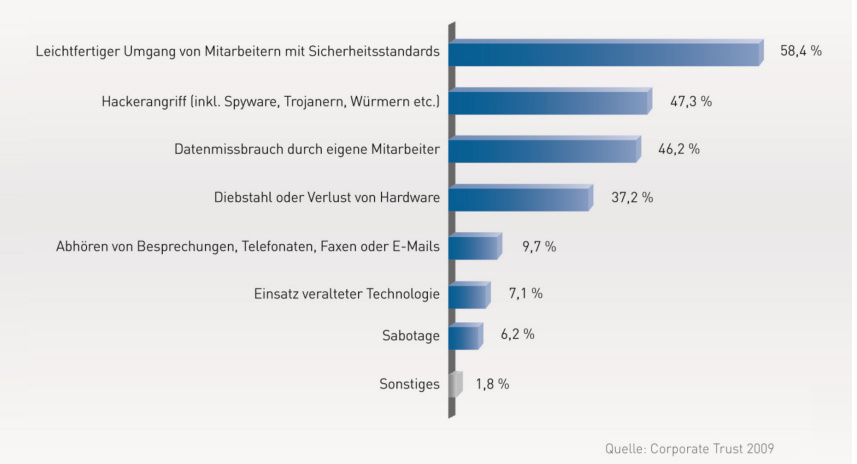


Bild 1 Gefahren für die IT-Sicherheit

iOS-Security: The Bad

So gut sich diese Möglichkeiten auch anhören, sie haben doch einen gravierenden Nachteil: Die Freiheit der Benutzer wird eingeschränkt. Während dies in der Unternehmens-IT völlig normal ist, sind Privatanutzer solche Vorgaben nicht gewohnt. Dementsprechend hat sich eine Community zusammgefunden, deren erklärtes Ziel es ist, ihre iPhones der Kontrolle durch Apple zu entziehen.

» Apple hat die iOS Geräte in erster Hinsicht für den Consumermarkt entworfen «

Das Verfahren, mit dem sie dies bewerkstelligen, wird „Jailbreak“ (Gefängnisausbruch) genannt. Wurde ein Gerät einem Jailbreak unterzogen, so kann man Software aus beliebigen Quellen installieren, die nicht von Apple kontrolliert wurde und damit auch ungewollte und undokumentierte iOS-Funktionen nutzen kann. Außerdem kann Software auch so installiert werden, dass sie nicht in der beschränkten Umgebung eines Verzeichnisses läuft, sondern Zugriff auf alle Dateien hat. Ein Jailbreak deaktiviert also die grundlegenden Sicherheitsfunktionen des iOS-Betriebssystems.

Sicherheitstechnisch müssen zwei Motivationen unterschieden werden, die im Unternehmensbereich relevant sind (siehe Bild 1):

- 1 Ein Mitarbeiter will sein Gerät von der Kontrolle durch Apple oder das Unternehmen befreien oder
- 2 ein Angreifer benutzt einen Jailbreak unbemerkt vom Besitzer des iOS-Geräts.

Es erübrigt sich, zu erwähnen, dass für den Fall 1 in jeder iOS-Sicherheitspolicy eines Unternehmens an prominenter

Stelle stehen muss: „Der Jailbreak von iOS-Geräten ist strikt verboten. Beim Betrieb von iOS-Geräten mit Jailbreak im Unternehmensnetzwerk muss mit arbeitsrechtlichen Konsequenzen gerechnet werden.“

Das löst aber das Problem nicht. Es gibt aktuell keine Software, die sicher per Remote einen Jailbreak detektieren kann. Gleichzeitig muss also eine regelmäßige, zumindest stichprobenartige Sichtkontrolle der iOS-Geräte durchgeführt werden. Dabei wird nach Applikationen gesucht, die auf einen Jailbreak hindeuten. Das sicherste Indiz hierfür ist die Installation der App „Cydia“, die die Installation von „freien“ Apps erlaubt. Für ein Unternehmen ist Fall 2 sehr viel problematischer. Das Durchführen eines Jailbreaks ist meist innerhalb von zehn bis fünfzehn Minuten erledigt – allerdings ist dazu (derzeit) der physische Zugriff auf das Gerät nötig, da dieses an einen präparierten Computer angeschlossen werden muss. Die Installation einer Spyware und das nachfolgende Löschen von Cydia und anderen erkennbaren Spuren kann nochmals fünf Minuten dauern. Wenn also ein Angreifer in den Besitz eines iPhones/iPads gelangt, ist ein umfassender Hackerangriff innerhalb von fünfzehn Minuten durchführbar. Eventuelle Passwörter oder Codes zum Entsperren von iPhone oder SIM-Karte erschweren den Angriff für normale Benutzer, werden aber von einem Experten nicht unbedingt benötigt.

Natürlich versucht Apple die Möglichkeit des Jailbreak mit jeder neuen Firmware wieder zu verhindern. Aktuell (19. Januar 2011) gilt folgender Status für Geräte mit der jeweils aktuellsten Firmware (3.1.3 für iPhone Classic/2G, 4.2.1 für iPhone 3G, 3GS und 4):

- iPhones der ersten (Classic/2G) und zweiten (3G) Generation können in jedem Fall einem Jailbreak unterzogen werden.



- iPhones der dritten Generation (3GS) können einem Jailbreak unterzogen werden, bei Geräten mit neuerem Produktionsdatum funktioniert danach aber kein Neustart mehr.
- iPhones der vierten Generation (4) und iPads können einem Jailbreak unterzogen werden, danach funktioniert aber kein Neustart mehr.

Gegen diese Art von Angriff existiert keine umfassende Gegenmaßnahme. Grundsätzlich werden folgende Schritte empfohlen:

- 1 Es wird sichergestellt, dass innerhalb von kurzer Zeit (zwei Wochen) nach Erscheinen einer neuen iOS-Version alle Geräte im Unternehmen versorgt sind.
- 2 iPhones der Generation Classic/2G, 3G sowie 3GS mit einem Produktionsdatum vor November 2009 werden im Unternehmenseinsatz nicht zugelassen.
- 3 Alle Mitarbeiter werden aufgefordert, ihre iPhones/iPads nicht unbeaufsichtigt in unsicherer Umgebung (außerhalb des Firmengeländes und der eigenen Wohnung) herumliegen zu lassen.
- 4 Alle Mitarbeiter werden aufgefordert, einen kompletten Reboot durchzuführen, falls Verdacht auf einen Jailbreak besteht oder das iOS-Gerät doch unbeaufsichtigt liegen gelassen wurde.

Diese Empfehlungen bieten natürlich keinen wasserdichten Schutz gegen solche Angriffe. Da ein Jailbreak derzeit der einzige Angriff gegen die iOS-Geräte ist, definiert das Risiko dieses Angriffs die Einsetzbarkeit der iOS-Geräte im eigenen Unternehmen. Um dieses Risiko zu bestimmen, hilft ein

Vergleich mit den firmeneigenen Laptops. Ein vergleichbarer Angriff auf ein Windows-Laptop ohne Festplattenverschlüsselung ist innerhalb von fünf bis zehn Minuten durchführbar. Hinzu kommt, dass Windows-Rechner mit der üblichen Software (Acrobat Reader, Flash etc.) ständig durch teilweise remote auszunutzende Lücken gefährdet sind – Festplattenverschlüsselung hin oder her. Generell gilt also: Wenn in der Firma Laptops ohne Festplattenverschlüsselung den Sicherheitsanforderungen genügen, dann gibt es keinen Grund, warum dies bei entsprechender Konfiguration nicht auch für neuere iOS-Geräte gelten sollte. Werden hingegen gesicherte Laptops verwendet (Festplattenverschlüsselung, Benutzer hat keine Adminrechte, Konfiguration nach den Vorgaben von Microsofts „Security Specialized Limited Functionality“-Profil), so sollte der iOS-Einsatz genau geprüft werden. Typischerweise sollten in solchen Umgebungen die Daten, die auf ein iPhone gelangen, beschränkt werden.

iOS-Security: The Ugly

Die hässliche Seite der iOS-Security zeigt sich in der obigen Forderung, binnen zwei Wochen alle Geräte im Unternehmen mit einer neuen Firmware auszustatten. Apple hat die iOS-Geräte in erster Linie für den Consumermarkt entworfen und scheint auch seine Strategie auf diesen Markt zu konzentrieren. Das Update auf eine neue iOS-Version ist derzeit remote nicht möglich. Für die Installation muss das Gerät zwischen dreißig Minuten und zwei Stunden mit iTunes verbunden bleiben. Neue Firmwareversionen erscheinen zwar durchschnittlich nur alle zwei bis drei Monate, dennoch ist der Aufwand im IT-Betrieb für den Rollout nicht zu unterschätzen. Firmen müssen hier also mit einem personellen Zusatzbedarf ▶

Ein kurzer (ironischer) Leitfaden für deutsche IT-Verantwortliche zum Thema Apple:

- 1 Grundsätzlich hat Apple-Technologie in einem Unternehmen nichts zu suchen. Wir hatten hier im Unternehmen schon immer nur PCs und das hat immer funktioniert. Zur Not vage und bedeutungsschwanger mit Sicherheitsbedenken argumentieren.
- 2 Mac OS X-Geräte dürfen ausnahmsweise in kleinen Stückzahlen für Marketing oder Kreativabteilungen angeschafft werden. Dabei ist ständig zu betonen, dass es die Adobe Creative Suite auch für PCs gibt.
- 3 iPhones sind im Unternehmen aus Sicherheitsgründen nicht zulässig und werden nicht gekauft. Ausnahmen gelten nur für hochrangige Manager, die sich von der IT-Sicherheit nichts vorschreiben lassen.
- 4 Private iPhones werden zur Not geduldet, es ist aber dafür zu sorgen, dass diese unternehmensfremden Geräte keinen Zugriff auf E-Mails oder ins Unternehmensnetzwerk bekommen. Mitarbeiter, die ihre E-Mails umleiten, müssen per organisatorischer Richtlinie kriminalisiert werden.
- 5 iPads sind Spielereien, die im Unternehmenseinsatz keinen Sinn haben. 7,3 Millionen verkaufte iPads im Jahr 2010 sind noch lange kein Grund für unser Unternehmen, sich mit Tablets auseinanderzusetzen.

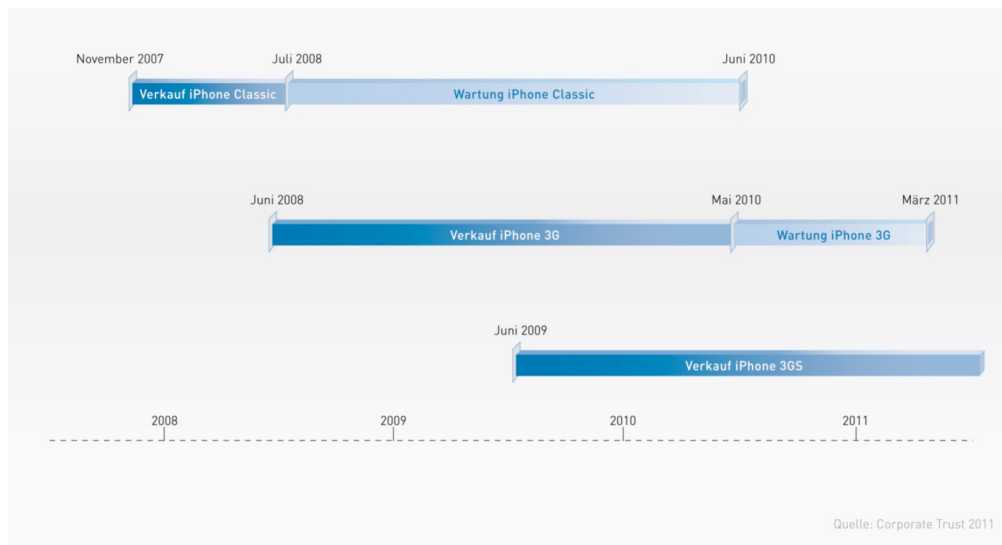


Bild 2 Release- und Wartungs-kalender des iPhones

rechnen, der momentan noch nicht automatisiert werden kann. Früher wurden solche Verfahren spöttisch „Turnschuh-Updates“ genannt, da die IT-Supportexperten durch die Firma laufen müssen, um die Geräte auf den neuesten Stand zu bringen.

Problematisch ist auch die Supportdauer – im Unternehmensbereich gilt es als Minimum, ein Software- oder Hardwareprodukt drei Jahre lang zu warten und mit Sicherheitsupdates zu versorgen. Das iPhone Classic/2G wurde im Juli 2008 das letzte Mal neu verkauft, seit Juni 2010 wird es nicht mehr mit Updates versorgt. Noch problematischer ist die Situation beim iPhone 3G. Bis Mai letzten Jahres wurde die 8GB-Version des iPhone 3G als low-cost-Alternative verkauft. Das neue Update auf 4.3 (erwartet für Februar/März) wird wohl keinen Support mehr für das iPhone 3G enthalten. Im Mobilfunkbereich ist es durchaus üblich, mit Softwareupdates für Geräte eher sparsam zu sein, sobald diese einmal verkauft sind und auch Android ist hier eher schlechter als besser. Dennoch bieten Hersteller wie RIM (Blackberry), die ihren Fokus auf Unternehmenskunden legen, für ihre Geräte einen wesentlich längeren Supportzeitraum.

Derzeit kann die Empfehlung für ein Unternehmen also nur lauten: immer die neueste Apple-Generation kaufen. Dann besteht die Hoffnung, dass der Support wenigstens knapp zwei Jahre lang gewährleistet ist.

Ausblick

Dieser Artikel konnte – zwangsläufig – nur einen kleinen Aspekt des Themas iOS-Sicherheit beleuchten. Durch die Konzentration auf grundlegende Themen wurden Gebiete wie E-Mail-Integration, Wifi-Authentifizierung, VPN-Zugang, Erstellung von Sicherheitsprofilen für iOS-Geräte mit dem iPhone-Konfigurationsprogramm oder Rechte-Einstellung von iTunes ebenso wenig angesprochen wie viele andere. Auch die fortschreitende Vermischung von privater und geschäftlicher Nutzung und neue Tendenzen wie BYOD („bring

your own device“) – also die Idee, dass Geräte der Mitarbeiter als Arbeitsgeräte in die Firmeninfrastruktur integriert werden – müssen sicherheitstechnisch betrachtet werden.

Die Erfahrung aus vielen Beratungsaufträgen rund um das Thema „mobile Security“ zeigt aber eines: Das Betriebssystem iOS von iPhone und iPad ist aus Designsicht sicherheitstechnisch für den Unternehmenseinsatz geeignet. Die Programme, Tools und Einstellungsmöglichkeiten, die Apple rund um das Thema Security bietet, sind vielfältig und für die meisten Schutzbedarfsanforderungen ausreichend. Der Einsatz von iPhones und iPads „out of the box“, ohne richtige Konfiguration und ohne Beschäftigung mit der Technologie, ist im Unternehmenskontext nicht empfehlenswert. Bei sorgfältiger Konzeption und richtiger Integration in die Sicherheitsstrukturen ist die Apple-Mobiltechnologie aber aus Sicherheitsicht für den Unternehmenseinsatz durchaus geeignet. ●

Schlüsselwörter

Jailbreak, iOS, Sicherheit

Literaturtip

Weitere Beiträge des Autors Florian Oelmaier finden Sie im Buch „Apple's iPad im Enterprise-Einsatz“, vorgestellt in unserer Literaturrecke auf Seite 34.

Kontakt

Corporate Trust – Business Risk & Crisis Management GmbH
 Florian Oelmaier
 Graf-zu-Castell-Straße 1
 81829 München
 Tel.: +49 (0) 89 / 599 88 75 80
 Fax: +49 (0) 89 / 599 88 75 820
 E-Mail: oelmaier@corporate-trust.de
 URL: www.corporate-trust.de