

iPhone-Security im Enterprise-Einsatz

Das iPhone findet sich immer häufiger in den Händen von Business Usern. Um Sicherheit zu gewährleisten, empfiehlt es sich, Daten in der Cloud aufzubewahren.

VON STEPHAN SUTTER

Das «S» des iPhone 3G S könnte angesichts der angekündigten Verbesserungen von Apple nicht nur für «Speed», sondern auch für «Security» stehen. Die Erwartungen an die Enterprise-Tauglichkeit sind hoch, da immer mehr iPhones professionell genutzt werden. Die Analysen von Sicherheitsexperten zeigen aber, dass Apple im Sicherheitsbereich ausser der Hardwareverschlüsselung keine Verbesserungen vorgenommen hat. Für das «Jailbreaking» kann nach wie vor dieselbe Schwachstelle zum Installieren von nicht von Apple autorisierten iApps ausgenutzt werden wie mit dem früheren Betriebssystem 2.0 und dem Modell 3G. Am 5. August dieses Jahres demonstrierten die beiden Researcher Collin Mulliner und Charlie Miller an der Black-at-Security-Konferenz, wie sie mit einer präparierten SMS die Kontrolle über ein iPhone mit dem OS 3.0 übernehmen und Daten stehlen konnten.

Wenig Schutz von Apple

Sind solche Meldungen für professionelle Anwender nun ein Grund zur Besorgnis, oder können sie sich darauf verlassen, dass Apple die Probleme rasch beseitigt?

Die SMS-Sicherheitslücke wurde mit dem Patch auf das iPhone OS 3.0.1 sechs Wochen nach der Meldung der Entdecker geschlossen. Zu «Jailbreaking» gibt es von Apple nur eine DMCA-Aussage (Digital Millennium Copyright Act), dass dieses Verfahren eine Copyright-Verletzung darstelle, die dazu führe, dass der Schutz, die Sicherheit und die Zuverlässigkeit des iPhones gefährdet sei und Tür und Tor für Piratensoftware geöffnet werde.

Weshalb ist «Jailbreaking» auf dem iPhone überhaupt ein Thema? Im Gegensatz zu anderen Smartphone-Herstellern hat Apple für das iPhone ein ganzes Geschäftsmodell entworfen und erfolgreich umgesetzt. Dieses Geschäftsmodell besteht aus der proprietären iPhone-Plattform, über die via iTunes-Store

Medien und Applikationen ganz einfach gekauft, installiert und genutzt werden können. Diese Applikationen unterliegen Einschränkungen, die den Entwicklern der Applikationen, den Netzbetreibern, Apple selbst sowie den Medienanbietern ein Einkommen sichern sollen.

Applikation in der Sandbox

Eine iApp kann Daten nur in ihrer eigenen Sandbox verwalten und nicht auf die Daten einer anderen Applikation zugreifen. Ein Beispiel: Eine iApp, die Worddateien bearbeiten kann, kann nicht einfach auf den Anhang einer E-Mail zugreifen, welche mit der iPhone-Mail-App empfangen wurde. Denn dazu würde die iApp ja die Sandbox verlassen. Also muss die Applikation den Anhang mit einem eigenen E-Mail-Client nochmals aus dem Mail-Account herunterladen, in ihrer Sandbox speichern, bearbeiten und dann wieder mit ihrem eigenen E-Mail-Client versenden.

Ein weiterer Schutzmechanismus ist die Tatsache, dass es keine Speicherkarte für das

iPhone gibt. Diese würde es nämlich wesentlich einfacher machen, mit einem PC oder Mac auf die darauf gesicherten Daten zuzugreifen.

Hürden überwinden als Gefahr

Die Hürden, mit denen das iPhone ausgestattet ist (eingeschränkte Applikationen, nur bestimmte Mobilfunkanbieter) hat jedoch auch zur Folge, dass Hacker angezogen werden, welche darauf aus sind, ebendiese Hürden zu beseitigen. So ist die «Jailbreak»-Software entstanden, welche dazu da ist, aus diesem «Gefängnis» auszubrechen. Dank «Jailbreak» wird es möglich, andere Mobilnetzanbieter zu nutzen, auf alle Daten des iPhones zuzugreifen oder von Apple nicht freigegebene Programme zu installieren. Natürlich birgt dies entsprechende Sicherheitsrisiken.

Die bereits angesprochene SMS-Sicherheitslücke, die mit iPhone OS 3.0.1 geschlossen wurde, nutzte solche nicht durch Apple autorisierten Programme aus dem «Jailbreak»-Umfeld. Das angegriffene iPhone installiert einen SSH-Server, der dem Angreifer Zugriff auf alle

IN KÜRZE

- Das iPhone ist auch im Unternehmens Einsatz äusserst beliebt.
- Apples geschlossenes System verführt zum «Jailbreaking», einem grossen Sicherheitsrisiko.
- Wertvolle Informationen sollten über Webanwendungen genutzt werden.
- Serveranwendungen sind einfacher zu schützen als iPhones.

WELCHE MASSNAHMEN STEHEN IPHONE-NUTZENDEN UNTERNEHMEN ZUR VERFÜGUNG?

- Mit dem «iPhone Configuration Utility» können Einstellungen zentral festgelegt werden. So beispielsweise VPN, Tethering, Sicherheitsvorschriften, E-Mail-Einstellungen und -Zertifikate usw.
- Für die Nutzung und Bewirtschaftung von vertraulichen Unternehmens-Informationen sind fürs iPhone optimierte, sichere Webapplikationen bereitzustellen.
- Die iPhone-User sind in den wichtigsten Sicherheitsmassnahmen zu schulen:
 - Einen Zugangscode festlegen und am besten auch «Löschen nach mehreren Versuchen» aktivieren.
 - Fernlöschen bei verlorenen oder gestohlenen iPhones sofort ausführen und die Zugangscode wechseln.
 - Vertrauliche Daten nur über Webapplikationen über HTTPS-Verbindungen bewirtschaften und nicht auf dem iPhone festhalten (Zugangscode im Safari-Browser, Notizen, E-Mails, Kalender, Kontakte, spezielle iApps usw.)
 - Das iPhone regelmässig mit iTunes sichern und vom Unternehmen geprüfte und freigegebene Updates installieren.
 - Keine unbekanntes W-Lan-Zugänge nutzen, lokales W-Lan wird von gewissen iApps als vertrauenswürdig angesehen.

Daten – und leider nicht nur diejenigen der Sandbox des SSH-Servers – ermöglichte.

Enterprisetauglich: Ja oder Nein?

Ist dies wie in Blogs diskutiert der Beweis dafür, dass das iPhone nicht enterprisetauglich ist? Smartphones sind schon seit ihrer ersten

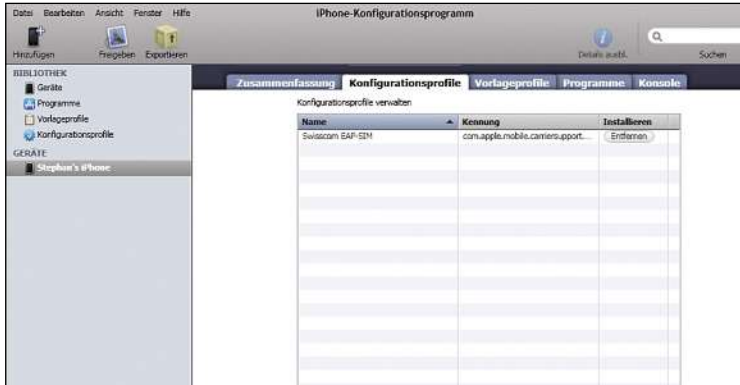
professionellen Nutzung ein Sicherheitsproblem, da sie häufig beispielsweise vertrauliche E-Mails mit Kundendaten enthalten. Wenn sie dann noch vermehrt als Terminal zu Unternehmensanwendungen genutzt werden, wird der Schaden bei Datendiebstahl noch grösser.

Deshalb drängt es sich auf, wertvolle Informationen in einer angemessenen Sicherheits-

zone aufzubewahren, und nur bekannte und berechnete Nutzer darauf zugreifen zu lassen. Das Zauberwort lautet Webanwendungen. Es ist einfacher, eine Server-Anwendung als ein iPhone oder ein anderes Smartphone gegen Angriffe zu schützen. Die sichersten Daten sind nicht mehr diejenigen in

unserer Hand, sondern die in geschützten Rechenzentren. Bei Webanwendungen haben Spezialisten üblicherweise jahrelange Erfahrung, sie gegen Angriffe zu schützen. Server werden physisch abgeschirmt und von einem dafür ausgebildeten Team betrieben und überwacht. Das Teamwork reduziert den Faktor der «Human Errors». Und Daten an mehreren Standorten konsistent und redundant für Ereignisfälle zu unterhalten, ist nur mit Server-Anwendungen möglich.

Deshalb lautet das Fazit: Mit sicheren Webapplikationen, die in einem Rechenzentrum von Spezialisten betrieben werden, ist Sicherheit günstiger zu erreichen als mit Smartphones. Gold ist in einem Tresorraum auch besser vor unberechtigtem Zugriff geschützt als in der Hosentasche.



Mit dem iPhone Configuration Utility können Einstellungen wie Sicherheitsvorschriften zentral festgelegt werden.

STEPHAN SUTTER IST PRINCIPAL BEI TECHNOLOGY INNOVATION, EINEM UNTERNEHMEN DER BUSINESS SOLUTION GROUP

Wo ist das nächste Standesamt?

Auf **map.search.ch** natürlich. Hier finden Sie neben Informationen zu öffentlichen Gebäuden auch Angaben zu Anfahrtswegen und Parkmöglichkeiten. www.map.search.ch - mehr als nur eine Karte.

[search.ch]
Immer ein Volltreffer.