MobileIron

WHITE PAPER

Mobile Sicherheit:
Bedrohungen und Gegenmaßnahmen

Einführung

Mobilgeräte entwickeln sich schnell zur bevorzugten Endbenutzer-Computerplattform in Unternehmen. Die intuitive Benutzerumgebung, die robusten Computerfunktionen, eine breite Palette von Apps, die Möglichkeit der ständigen Vernetzung sowie die Portabilität machen Mobilgeräte zu einem sehr überzeugenden PC-Ersatz. Der Übergang zu Mobilgeräten ist jedoch ein echter Paradigmenwechsel gegenüber der PC-Ära, die Unternehmens-IT benötigt daher ein neues Konzept, um Firmendaten zu sichern und Risiken zu minimieren. Um Unternehmensdaten auf Mobilgeräten zu schützen, muss die IT neue Management-Tools und Sicherheitsstrategien einführen, da Mobilgeräte anders genutzt werden als PCs. Unternehmen, die auf Mobilgeräte setzen und die neuen Anforderungen berücksichtigen, profitieren letztendlich durch einen Wettbewerbsvorsprung und stärkere Innovation.

In diesem Dokument finden Sie eine Übersicht der grundlegenden, ergänzenden und Kompensationskontrollen, die mit MobileIron implementiert werden können, um das Risiko von Datenverlusten auf privaten und Unternehmens-Mobilgeräten zu verringern.

Wichtige Überlegungen vor dem Wechsel auf Mobilgeräte

Die IT-Abteilung benötigt vor allem aus zwei Gründen andere Strategien zum Schutz der Unternehmensdaten auf Mobilgeräten als bei PCs, wenn sie mit ihrer Strategie die Benutzerproduktivität erhöhen will.

- **Geringere Kontrolle der IT-Abteilung über Mobilgeräte:** In einer Ära, in der vorwiegend Mobilgeräte genutzt werden, dreht sich alles um den Endbenutzer. Der Endbenutzer wählt ein Mobilgerät, das seinem Geschmack am besten entspricht und erwartet, dass er das Gerät auch für geschäftliche Zwecke mit allen Apps und für jeden Content produktiv nutzen kann. Dies unterscheidet sich stark von der PC-Ära. Damals stellte die IT-Abteilung den Endbenutzern zertifizierte PCs mit einer Reihe vordefinierter Anwendungen zur Verfügung. Die Endbenutzer hatten kaum einen Einfluss darauf, auf welche Daten der PC zugreifen konnte, und die IT-Abteilung konnte jeden Aspekt der Firmengeräte kontrollieren, seien es die physischen Anschlüsse, die Software oder die Anwendungsversionen. In der mobilen Welt entscheiden die Endbenutzer über viele dieser Aspekte, die IT-Abteilung kann nur Geräte und Anwendungen empfehlen. Die IT-Abteilung kann kein Standardbetriebssystem, kein Gerät und keine bestimmte Anwendung für das gesamte Unternehmen vorschreiben. Je stärker die IT-Abteilung versucht, die Gerätefunktionalität zu begrenzen, umso mehr Endbenutzer versuchen, Richtlinien zu umgehen, so dass in der Praxis das Risiko für das Unternehmen steigt.

- **Alte Sicherheitsmodelle sind nicht mehr relevant**: Bei den PC-Betriebssystemen funktionierten agent-basierte Sicherheitsverfahren gut. Dabei wurde eine Software auf dem PC installiert, die den Prozess und die Daten anderer Anwendungen kontrollierte. Dieses agent-basierte Sicherheitsmodell kann leider zur Sicherung von Mobilgeräten nicht

MAKING ENTERPRISE MOBILE FIRST

MobileIron
415 East Middlefield Road
Mountain View, CA 94043 USA
Tel.: +1.650.919.8100
Fax: +1.650.919.8006
info@mobileiron.com

verwendet werden, da die Betriebssysteme sich in ihrer Architektur deutlich unterscheiden. Mobile Betriebssysteme arbeiten mit einer Sandbox-Architektur, welche die Isolierung der Apps und der zugehörigen Daten erlaubt. Eine Interaktion und gemeinsame Verwendung sind nur über gut definierte Mechanismen möglich. Dies ermöglicht eine höhere Sicherheit als bei den offenen, dateibasierten Systemen der PC-Betriebssysteme und erfordert neue Tools, die die vom Gerätehersteller selbst angebotenen spezifischen Sicherheitsfunktionen umfassend nutzen.

Mit der schnellen Akzeptanz der Mobilgeräte in Unternehmen eröffnen sich großartige Möglichkeiten für Wachstum und Innovation, aber es entstehen auch höhere Risiken. In diesem Dokument finden Sie eine Zusammenfassung der Hauptbedrohungen durch Mobilgeräte und Erläuterungen, wie die IT-Abteilungen mit Tools zum Enterprise-Mobility-Management das Risiko minimieren und Unternehmensdaten ohne Abstriche bei der Produktivität der Endbenutzer schützen können.

Bedrohungen durch Mobilgeräte

Die Verwendung von Mobilgeräten wird durch Trends wie "BYOD" ("jeder bringt sein eigenes Gerät mit") beschleunigt, welche die Produktivität im Unternehmen steigern. Gleichzeitig werden die Unternehmen damit diversen IT-Sicherheitsrisiken und -bedrohungen ausgesetzt. Bedrohungen durch Mobilgeräte lassen sich in drei Kategorien einteilen:

1) **Gerätespezifische Bedrohungen**
   Mit Mobilgeräten können Endbenutzer diverse unternehmensrelevante Aufgaben ausführen, beispielsweise E-Mails empfangen und auf Firmen-Content zugreifen, diesen bearbeiten und über diverse Produktivitäts-Apps teilen. Infolgedessen ist auf Mobilgeräten eine signifikante Menge sensitiver Daten gespeichert. Diese Daten können aus verschiedenen Gründen gefährdet sein:
   - Durch eine ständige Vernetzung, über die nicht autorisierte Dritte auf Unternehmensdaten zugreifen können.
   - Durch Software-Sicherheitslücken, mit denen ein "Jailbreak" oder "Rooting" der Geräte möglich ist und die Datensicherheit gefährdet wird.
   - Durch die geringe Größe und Portabilität können Geräte leicht gestohlen werden oder verloren gehen.

2) **Netzwerkabhängige Bedrohungen**
   Bei Betrieb im "Always-on-Modus" müssen die Mobilgeräte ständig mit dem Internet verbunden bleiben. Infolgedessen nutzen die Endbenutzer oft nicht vertrauenswürdige, öffentliche Netze, über die Kriminelle auf gesendete Daten zugreifen und Daten auf verschiedenen Wegen abfangen können:
   - durch schlecht konfigurierte Zugangspunkte
   - durch Wi-Fi Sniffing Tools
   - durch ausgeklügelte Man-in-the-Middle (MitM)-Angriffe

3) **Bedrohungen durch Benutzer**
   Durch Mobilität haben Endbenutzer mehr Möglichkeiten. Die große Auswahl ist zwar gut für die Benutzer, wohlmeinende Endbenutzer gewöhnen sich jedoch oft riskante Arbeitsweisen an, welche die Unternehmensdaten gefährden könnten. Beispiele für riskante Arbeitsweisen:
   - Verwendung von nicht genehmigten Cloud-Anwendungen zum Austausch und zur Synchronisation von Daten.
   - Verwendung von nicht genehmigten Apps zur Steigerung der Produktivität, die Kopien der Unternehmensdaten speichern.
   - Einsatz von Jail Breaking/Rooting-Geräten zur Umgehung von Sicherheitskontrollen
   - Verwendung von Anwendungen mit Schadfunktionen aus nicht zertifizierten App-Stores
   - Vorsätzliche Offenlegung von Geschäftsdaten, um dem Unternehmen zu schaden.

Man kann zwar argumentieren, dass die Liste der Bedrohungen durch Mobilgeräte sich nur wenig von den Bedrohungen durch Laptops und ähnliche, portable PCs unterscheidet, die fundamentalen Unterschiede zwischen den Betriebssystemen von PCs und Mobilgeräten zwingen die IT-Abteilung jedoch, spezifische Plattformen für die Unternehmensmobilität einzurichten, um Risiken durch Mobilgeräte zu minimieren.

Gegenmaßnahmen zur Vermeidung von Datenverlusten auf Mobilgeräten

Maßnahmen zur Verhinderung von Datenverlusten auf Mobilgeräten erfordern ein mehrstufiges Sicherheitskonzept. Dieses mehrstufige Sicherheitskonzept kann mit den im Folgenden aufgeführten Kontrollen implementiert werden:

1) Sichere Betriebssystemarchitektur
2) Authentifizierung
3) Fernlöschen
4) Verschlüsselung
5) Daten-Sharing
6) Netzwerksicherheit
7) Verwaltung des App-Lebenszyklus
8) Sicheres Browsen

Im Folgenden finden Sie Beschreibungen der Maßnahmen zur Vermeidung von Datenverlust und der spezifischen Kontrollen, die MobileIron unterstützt. Jede Klasse von Kontrollfunktionen kann grundlegende Kontrollen umfassen, die direkt auf die Anforderungen bezogen sind, sowie ergänzende Kontrollen zur Stärkung der grundlegenden Kontrollen und Kompensationsmechanismen, die dann Anwendung finden, wenn keine grundlegenden Kontrollen vorhanden sind. Gemeinsam verhindern diese mehrstufigen Sicherheitskontrollen einen Verlust von Daten auf Mobilgeräten.

1. Sichere Betriebssystemarchitektur

Anforderungen:

- Sandbox-Anwendungen zum Schutz vor dem Zugriff auf Anwendungsdaten durch Schadsoftware
- Bereitstellung eines sicheren Anwendungs-Ökosystems
- Schutz der Integrität des Betriebssystems
- Rasches Schließen von Sicherheitslücken im Betriebssystem

Grundlegende Kontrollmechanismen:

- *Sandbox*: Eine "Sandbox" ist ein isolierter Datensatz, der einer Anwendung ("App") auf dem Mobilgerät zugeordnet ist. Im Gegensatz zu PC-Betriebssystemen gestatten die Betriebssysteme von Mobilgeräten Anwendungen nur den Datenzugriff innerhalb der spezifischen Sandbox oder über wohldefinierte Kontrollen für die gemeinsame Datennutzung. Dadurch wird das Risiko von Schadsoftware begrenzt, da diese selbst nach dem Herunterladen auf das Gerät nicht auf das Dateisystem zugreifen kann, um Daten zu beschädigen oder zu stehlen.
- *App-Ökosystem*: App-Stores für Mobilgeräte wie Google Play oder der Apple App-Store werden genau überwacht, um die Wahrscheinlichkeit zu minimieren, dass sich in veröffentlichten Apps Malware befindet. Apple verbietet verborgene Zugänge und Mechanismen, über die beispielsweise neuer, ausführbarer Code in eine bereits genehmigte App eingebracht werden kann. Außerdem können Apps in den App-Stores sofort gesperrt werden, wenn später festgestellt wird, dass sie Richtlinien verletzen.
- *Betriebssystemintegrität*: Bei Mobilgeräten wird mit "Jailbreak" oder "Root" eine Gefährdung des Betriebssystems durch Entfernung integrierter Sicherheitsmechanismen bezeichnet. MobileIron sucht laufend in jedem registrierten Mobilgerät nach Jailbreak- oder Root-Funktionen, um sicherzustellen, dass das Betriebssystem nicht infiziert wurde. Wenn es infiziert wurde, löst MobileIron die entsprechende Sicherheitsfunktion in Abhängigkeit von der im Unternehmen definierten Richtlinie aus. Diese Sicherheitsfunktion kann online (oder offline, wenn das Gerät gestohlen wurde oder verloren ging und die Netzwerkverbindung nicht mehr besteht) ausgeführt werden.
- *Betriebssystem-Patching*: Weil Apple die globale Verteilung des iOS-Betriebssystems kontrolliert, wird traditionell jede Sicherheitslücke, die nach Ansicht von Apple relevant ist, schnell durch ein Patch geschlossen und die entstehende neue Version des iOS-Betriebssystems der globalen Benutzergemeinde zum Download angeboten. Die Bereitstellung von Betriebssystem-Patches für Android-Geräte hängt von den Geräteherstellern und Anbietern ab.

Ergänzende Kontrollmechanismen:

- *Durchsetzung von Aktualisierungen des Betriebssystems*: MobileIron überwacht die Betriebssystemversion aller Geräte, die das Unternehmen verwaltet. Wenn die Benutzer ihre Geräte nach einem Patch nicht aktualisieren, können diese Geräte in Quarantäne gestellt und Unternehmensdaten entfernt werden, bis das Problem beseitigt ist.

Durch die Sandboxfunktion des Betriebssystems werden Anwendungsdaten in separaten Containern isoliert, so dass es für Malware weniger Möglichkeiten gibt, Daten zu stehlen oder zu beschädigen.

MobileIron überwacht die Integrität und die Version des Betriebssystems, um seine Konformität und Konsistenz für das Unternehmen zu gewährleisten.

Kompensatorische Kontrollmechanismen:

- *Überwachung der Version des Betriebssystems*: Im Gegensatz zum Windows-Betriebssystem kontrolliert die IT-Abteilung die Verteilung von Vertriebssystem-Patches für iOS oder Android nicht. Das heißt, dass neue Patches für die Benutzer verfügbar sind, sobald die Gerätehersteller sie zur Verfügung gestellt haben, unabhängig davon, ob die IT-Abteilung der Verteilung zustimmt. Obwohl dadurch die Kontrolle durch die IT beschränkt wird, kann sie die Version des Betriebssystems über MobileIron auch weiterhin überwachen und einschreiten, falls der Benutzer zu früh oder überhaupt nicht aktualisiert hat.

2. Authentifizierung

Anforderungen:

- Fernkonfiguration der Passwortrichtlinien
- Automatisches Löschen des Geräts nach einer bestimmten Anzahl fehlgeschlagener Authentifizierungsversuche
- Kein Zugriff auf Unternehmensdienste ohne Eingabe der Identitätsdaten

Grundlegende Kontrollmechanismen:

- *Gerätepasswort:* MobileIron ermöglicht die Fernkonfiguration und die Durchsetzung von Passwortrichtlinien für das jeweilige Endgerät. Die IT-Abteilung kann folgende Passwort-Richtlinienvariablen über MobileIron konfigurieren:
  - Typ
  - Mindestlänge
  - Maximale Inaktivität bis zum Timeout
  - Minimale Anzahl komplexer Zeichen
  - Maximale Gültigkeitsdauer des Passworts
  - Maximale Anzahl an Fehlversuchen
  - Passwortverlauf
  - Nachfrist für Sperrung des Geräts
- *App-Passwort*: MobileIron AppConnect ist eine Containerisierungslösung zur Sicherung interner und öffentlicher Apps. Eine ihrer Funktionen ist die Authentifizierung des Zugriffs auf die Sammlung sicherer Apps auf dem Gerät.
- *Automatisches Löschen*: Eine übermäßig hohe Anzahl an Fehlversuchen gilt als Anzeichen, dass das Gerät gestohlen wurde, und führt zum automatischen Löschen der auf dem Gerät gespeicherten Daten.
- *Zertifikatsbasierte Identität*: MobileIron verwendet digitale Zertifikate, um den Zugriff auf Unternehmensdienste auf dem Gerät wie etwa E-Mail, WLAN und VPN zu sichern. Der Benutzerkomfort verbessert sich, weil die Benutzer nicht jedes Mal ihr Passwort eingeben müssen. Falls ein Gerät oder ein Benutzer nicht mehr konform mit den Richtlinien ist, wird durch das Löschen des Zertifikats auch der Zugriff auf den entsprechenden Dienst unterbunden.

iOS unterstützt neue biometrische Methoden, mit deren Hilfe sowohl die Authentifizierung als auch die Verschlüsselung sicherer gemacht werden können.

MobileIron stellt die Richtlinien-Engine zur Authentifizierung auf Geräte- und App-Ebene zur Verfügung, um den nicht autorisierten Zugriff auf Unternehmensdaten zu verhindern.

Ergänzende Kontrollmechanismen:

- *Biometrische Authentifizierung*: Mit Touch ID für das iPhone 5S hat Apple Ende 2013 sein erstes biometrisches Authentifizierungsverfahren herausgebracht. Mit Touch ID kann der Benutzer einen Fingerabdruck zur Authentifizierung auf Geräteebene verwenden, wodurch das Risiko gemindert wird, dass jemand bei der Eingabe unbemerkt das Passwort mitliest:
  - Falls bei der Authentifizierung mit dem Daumenabdruck eine bestimmte Anzahl an Versuchen fehlschlägt, wird der Benutzer gemäß der Passwort-Richtlinie von MobileIron zur Eingabe eines Passworts aufgefordert.
  - Vor der Verfügbarkeit von Touch ID mussten zur Authentifizierung stärkere Passwörter verwendet werden. Damit waren jedoch die Benutzer unzufrieden, weil sich solche Passwörter schwer merken

und eingeben lassen. Aus diesem Grund gestatteten die meisten Finanzdienstleistungsunternehmen ihren Mitarbeitern die Verwendung eines schwächeren Passworts. Durch das schwächere Passwort wurde außerdem die Stärke der Verschlüsselung verringert, wodurch Brute-Force-Angriffe auf ein Gerät einfacher wurden.

- Mit Hilfe von Touch ID kann die IT bei Bedarf jetzt jedoch wieder stärkere Passwörter verwenden, da der Benutzer das Passwort nur dann eingeben muss, wenn die Authentifizierung mit dem Fingerabdruck mehrfach fehlschlägt, was häufig ein Hinweis auf Diebstahl des Geräts ist.

3. Fernlöschen

Anforderungen:

- Fernlöschung aller auf dem Gerät gespeicherten Daten für unternehmenseigene Geräte
- Nur Fernlöschung aller auf dem Gerät gespeicherten Unternehmensdaten für Privatgeräte

Grundlegende Kontrollmechanismen:

- *Vollständiger Wipe*: MobileIron erlaubt es dem Administrator oder Benutzer, einen Remote-Befehl zur vollständigen Löschung an das Gerät zu senden; damit werden alle Daten auf dem Gerät gelöscht und das Gerät wird wieder auf die Werkstandardeinstellungen zurückgesetzt.
- *Selektiver Wipe*: MobileIron erlaubt es dem Administrator auch, nur die Unternehmensdaten von dem Gerät zu löschen. Dies schließt Folgendes ein:
    - Löschen des E-Mail-Kontos des Unternehmens auf dem Gerät, ohne das private E-Mail-Konto antasten zu müssen.
    - Löschen von Apps, die über den App-Store von MobileIron für Unternehmen installiert wurden, ohne die privaten Apps antasten zu müssen.
    - Löschen der digitalen Zertifikate auf dem Gerät, die eine Authentifizierung bei Unternehmensdiensten wie E-Mail, WLAN und VPN ermöglichen.
    - Entfernung von Unternehmensdaten, beispielsweise Dokumenten, Präsentationen, Arbeitsblättern usw.
    - Beenden der Durchsetzung von Unternehmensrichtlinien.

Die logische Trennung privater und geschäftlicher Daten auf dem Gerät ermöglicht der IT Maßnahmen zum Schutz der Unternehmenssicherheit, ohne die Privatsphäre der Mitarbeiter zu beeinträchtigen.

MobileIron verwaltet den Lebenszyklus von Unternehmensdiensten auf dem Gerät, einschließlich Verteilung, Konfiguration, Datenschutz und Löschung. Hierbei werden separate Richtlinien für Unternehmens- und Privatgeräte verwendet.

Ergänzende Kontrollmechanismen:

- *Privatsphäre*: Unternehmen machen sich Sorgen, dass die persönlichen Daten auf einem BYOD-Gerät von der IT durch menschliches Versagen, durch das Löschen eines verloren gegangenen Geräts oder durch andere Umstände (z. B. durch einen Gerichtsbeschluss, der dem Unternehmen keine andere Wahl lässt) gelöscht werden könnten. In solchen Fällen können die Benutzer wichtige private Daten verlieren, beispielsweise Familienfotos oder Textnachrichten.
    - MobileIron ermöglicht der IT das Festlegen einer Datenschutzrichtlinie nach Gerät oder nach Gruppe, damit die IT ausschließlich auf sicherheitsrelevante Informationen zugreifen kann.
    - Jedes BYOD-Programm bedarf einer klar definierten und kommunizierten Richtlinie rund um den Datenzugriff und das Löschen von Daten, die im Alltag auch glaubwürdig umgesetzt wird. Andernfalls kann die Akzeptanz von BYOD auf Seiten des Benutzers auf Grund falscher Annahmen bzgl. des Datenschutzes leiden.
    - Des Weiteren ist für jedes BYOD-Programm ein Endbenutzer-Lizenzvertrag erforderlich, um das Unternehmen rechtlich abzusichern, falls private Daten gelöscht werden, obwohl hiervon bei normaler Verwendung nicht auszugehen ist.

- Da es immer wieder Grenzfälle geben wird, müssen die Benutzer im Rahmen jedes BYOD-Programms darüber informiert werden, wie sie private Daten beispielsweise mit dem iCloud-Dienst von Apple sichern können. Auf diese Weise gehen die Daten selbst dann nicht verloren, wenn das Gerät vollständig gelöscht wird. Für den Endbenutzer hat sich das genauso bewährt wie das Sichern von Unternehmensdaten für die IT.

4. Verschlüsselung

Anforderungen:

- Verschlüsselung aller auf dem Gerät gespeicherten Unternehmensdaten
- Verschlüsselung aller vom und auf das Gerät übertragenen Unternehmensdaten
- Verschlüsselung aller Unternehmensdaten in sicheren Apps

Grundlegende Kontrollmechanismen:

- *Verschlüsselung von gespeicherten Daten integriert:* MobileIron kann Verwendung und Stärke des Gerätepassworts vorschreiben, damit eine Verschlüsselung auf Geräteebene möglich ist, und damit sicherstellen, dass diese für alle Apps zur Verfügung steht. Je stärker das Gerätepasswort ist, desto stärker ist auch die zweite Verschlüsselungsebene. Mit dem biometrischen Authentifizierungsverfahren Touch ID von Apple kann die IT ein starkes Passwort über MobileIron erzwingen, ohne den Anmeldekomfort des Benutzers zu beeinträchtigen.
- *Verschlüsselung für gespeicherte Daten – zusätzlich:* Die Containerisierungslösung AppConnect von MobileIron für Apps bietet verschiedene zusätzliche Sicherheitskontrollen, eine Verschlüsselung eingeschlossen. Das iOS-Betriebssystem und Android haben zwar integrierte Verschlüsselungsfunktionen, viele Unternehmen fordern jedoch diese zusätzliche Verschlüsselung für entsperrte Geräte.
- *Gespeicherte Daten*: Mobile Unternehmensdaten wie E-Mails, Apps, Dokumente und Internetseiten laufen über das intelligente Gateway MobileIron Sentry von MobileIron. Diese Daten sind gegen Man-in-the-Middle (MitM)-Angriffe und Mithören durch digitale Zertifikate und Verschlüsselung der Übertragungsebene geschützt.
- *Validierung nach FIPS 140-2*: Die Verwendung der Verschlüsselungsbibliotheken FIPS 140-2 durch MobileIron wurde durch ein anerkanntes Verschlüsselungs- und Sicherheitslabor (CST-Labor) in voller Übereinstimmung mit dem Kryptografiemodul-Bewertungsprogramm (CMVP) validiert. Die Validierungsbriefe sind hier zu finden.

Die MobileIron-Verschlüsselung für gespeicherte und übertragene Daten ist nach FIPS 140-2 validiert und ergänzt die integrierten Verschlüsselungsfunktionen des Betriebssystems.

5. Daten-Sharing

Anforderungen:

- Unternehmens-E-Mails in der nativen E-Mail-App:
  - Kein Öffnen von Anhängen in einer nicht autorisierten App
  - Kein Weiterleiten von E-Mails über ein privates E-Mail-Konto
  - Kein Kopieren/Einfügen, Drucken und keine Screenshots von E-Mail-Text
  - Keine Sicherung von E-Mails ohne Kontrolle durch die IT
- Für Apps des Unternehmens:
  - Kein Zugriff auf App-Daten durch nicht autorisierte Apps
  - Kein Kopieren/Einfügen, Drucken und keine Screenshots von App-Daten
  - Keine Sicherung von E-Mails ohne Kontrolle durch die IT

Daten auf Mobilgeräten gehen vor allem dann verloren, wenn wohlmeinende Benutzer Unternehmensdaten auf einer unsicheren App öffnen.

Grundlegende Kontrollmechanismen:

- Für Firmen-E-Mails in der nativen E-Mail-App:
  - *Anhänge*: Das intelligente Gateway MobileIron Sentry von MobileIron verschlüsselt alle E-Mail-Anhänge. Diese Anhänge können nur von MobileIron Docs@Work entschlüsselt werden. Die Anhänge werden in dem sicheren Docs@Work-Container des Geräts gespeichert. Nicht autorisierte Apps können nicht auf diese Anhänge zugreifen und sie auch nicht entschlüsseln. Bei Android werden alle Unternehmens-E-Mails in einem sicheren Workspace gespeichert, auf Anhänge können nur autorisierte Apps zugreifen.
  - *Weiterleitung*: MobileIron ermöglicht der IT das Deaktivieren der Weiterleitung von E-Mails von einem Konto über ein anderes Konto auf dem Gerät.
  - *Kopieren*: MobileIron kann die Screenshot-Funktion des Geräts deaktivieren. Der native E-Mail-Client von iOS unterstützt jedoch nicht das Deaktivieren der Funktionen zum Kopieren/Einfügen oder Drucken von Text. Im Abschnitt „*Kompensatorische Kontrollmechanismen*“ wird eine Methode beschrieben, um dieses Problem zu lösen.
  - *Datensicherung*: Das von MobileIron auf dem Gerät verwaltete Unternehmens-E-Mail-Konto wird niemals auf Diensten wie iCloud gesichert.
- Für Apps des Unternehmens:
  - *Teilen*: Mobile Betriebssysteme erlauben Anwendungen, Daten untereinander durch die "Open-In"-Funktion zu teilen. Mit MobileIron kann die IT-Abteilung festlegen, welche Apps diese Funktionen für den Zugriff auf Anwendungsdaten nutzen dürfen.
  - *Kopieren*: MobileIron AppConnect ist eine Containerisierungslösung, die eine zusätzliche Sicherheitsebene für Unternehmens-Apps bietet, inklusive der Möglichkeit, das Kopieren/Einfügen und das Drucken von App-Daten zu untersagen. Außerdem kann MobileIron die Screenshot-Funktion für das gesamte Gerät deaktivieren.
  - *Sicherung*: MobileIron kann die iCloud-Sicherung global für alle Apps deaktivieren, wobei die Benutzer iCloud dennoch weiterhin für

MobileIron AppConnect setzt beim Daten-Sharing verschiedene Kontrollen durch, damit Unternehmensdaten nur von autorisierten Apps aufgerufen werden können.

private Daten verwenden können. Für verwaltete Apps kann MobileIron die iCloud-Sicherung des Weiteren für ausgewählte Apps deaktivieren. Hierbei muss die IT jedoch sicherstellen, dass diese Apps nicht zusätzlich so codiert sind, dass sie auch iCloud zur Sicherung von Dokumenten oder Schlüssel-Wert-Paaren verwenden.

Kompensatorische Kontrollmechanismen:

- *E-Mail-Client*: Der native E-Mail-Client von iOS kann das Kopieren/Einfügen oder das Drucken nicht untersagen. Viele Unternehmen sind zu dem Schluss gekommen, dass diese Funktionen nur ein geringfügiges Risiko für Datenverluste darstellen, da der Benutzer mit Vorsatz handeln muss und es für Kriminelle verschiedene andere Möglichkeiten gibt, um Daten mechanisch (Stift) oder elektronisch (Foto) zu kopieren. Wenn das Risiko immer noch als zu hoch betrachtet wird, kann die IT-Abteilung MobileIron Divide installieren, einen nativen E-Mail-Client, der alle beschriebenen Kontrollen unterstützt.

6. Netzwerksicherheit

Anforderungen:

- Vermeidung von Datenverlusten bei der Übertragung von Unternehmensdaten über öffentliche Mobilfunknetze und WLAN-Netzwerke, die nicht von der IT kontrolliert werden.

Grundlegende Kontrollmechanismen:

- *App-Tunneling*: Mit MobileIron Sentry steht ein sicheres Tunneling auf Anwendungsebene für alle Unternehmensdaten einschließlich E-Mails, Apps, Dokumente und Webtraffic zur Verfügung. Auf diese Weise kann die IT-Abteilung die Unternehmensdaten (die über die Sentry in einem sicheren Kanal übertragen werden) von privaten Daten (die außerhalb Sentry über ein unsicheres Netzwerk übertragen werden) trennen.
- *VPN*: Für Unternehmen, die standardmäßig für alle Geräte VPN-Technologie von Anbietern wie Cisco und Juniper verwenden, konfiguriert MobileIron den VPN-Dienst so, dass ein sicherer Kanal für Daten bereitgestellt wird.
- *Architektur ohne NOC*: Bei einem Network Operations Center (NOC) handelt es sich um einen zentralen Standort zur Überwachung und Verwaltung eines Netzwerks. Bei der traditionellen BlackBerry-Architektur war das NOC der von BlackBerry überwachte externe Kontrollpunkt für das sichere Netzwerk, über den der E-Mail-Verkehr vom Unternehmen zum Gerät erfolgte. Das Problem bei solchen Architekturen liegt darin, dass das NOC einen potenziellen neuralgischen Punkt bildet und dadurch Datenverluste möglich sind, die sich der Kontrolle der IT entziehen. Glücklicherweise ist weder für das oben beschriebene App-Tunneling noch für die VPN-Modelle ein externes NOC erforderlich. BlackBerry musste mit einem NOC arbeiten, weil bei der Push-Zustellung die E-Mails vom Mailserver des Unternehmens abgerufen, an einem externen Speicherort (NOC) zwischengespeichert und dann von dort an das Gerät weitergeleitet werden mussten. Dieses Modell ist jedoch nicht erforderlich, da für E-Mail das ActiveSync-Protokoll verwendet wird. Ein Speichern/Weiterleiten der E-Mails und eine NOC-basierte Architektur sind damit überflüssig. Aus diesem Grund ist ActiveSync inzwischen auch das Standardprotokoll, das von den meisten integrierten bzw. Drittanbieter-E-Mail-Clients für die Push-Zustellung von E-Mails verwendet wird.

Das mobile Sicherheitsmodell muss davon ausgehen, dass alle Unternehmensdaten über öffentliche Netzwerke übertragen werden.

MobileIron Sentry ist das intelligente Gateway, das über jedes Netzwerk auf App-Ebene sicheres Tunneling für Unternehmensdaten bietet.

7. Verwaltung des App-Lebenszyklus

Anforderungen:

- Kein Herunterladen von unsauberen Apps auf das Gerät
- Blacklist für nicht autorisierte Apps
- Whitelist für autorisierte Apps
- Veröffentlichung und Verteilung von Unternehmens-Apps
- Aktualisierung von Unternehmens-Apps

Grundlegende Kontrollmechanismen:

- *Unsaubere Apps*: Die Risiken durch unsaubere Apps werden auf Mobilgeräten aus folgenden Gründen minimiert:
    - Die mobile Architektur isoliert Apps in unabhängigen Sandboxes voneinander, so dass eine unsaubere App einen Zugriff auf Daten einer Unternehmens-App nur über die Methoden zur gemeinsamen Verwendung von Daten haben kann, die durch MobileIron kontrolliert werden.
    - Öffentliche App-Stores werden genau überwacht, so dass Malware selten ist.
    - Apple verbietet das Herunterladen von ausführbarem Code durch Apps. Auf diese Weise wird verhindert, dass Schadcode in eine vorhandene App eingeschleppt wird.
    - Android gestattet es Benutzern, Apps von nicht zertifizierten App-Stores zu installieren oder aus anderen Quellen zu laden; die IT-Administratoren können jedoch Richtlinien definieren, die ein Laden der Apps aus anderen Quellen verbieten.
- *Blacklist/Whitelist*: Außerdem ermöglicht MobileIron das Erstellen von Blacklists und Whitelists mit Apps über Richtlinien, die entsprechende Benachrichtigungen senden oder Kontrollfunktionen aufrufen, falls ein Gerät nicht konform ist. MobileIron kann den App-Store komplett deaktivieren, wir empfehlen dies jedoch nicht, da Apps für das mobile Benutzererlebnis so wesentlich sind. Außerdem verwendet MobileIron Reputation Services für Apps von Drittanbietern, um das Vorhandensein potenziell gefährlicher Apps zu erkennen.
- *App-Store für Unternehmen*: MobileIron hat einen speziell abgesicherten App-Store für Unternehmen erfunden und patentieren lassen. Über diesen kann die IT interne und öffentliche Apps bereitstellen und sicher verteilen.
- *Aktualisierung von Apps*: MobileIron überwacht die Version der auf dem Gerät installierten Unternehmens-Apps, damit die IT den Benutzer auffordern kann, bei Verfügbarkeit die jeweils aktuelle Version der App zu installieren. Auf diese Weise ist im gesamten Unternehmen für Konformität gesorgt und Sicherheitslücken in der App können schnell geschlossen werden.

Ergänzende Kontrollmechanismen:

- *Gefiltertes App-Inventar*: Für BYOD ist Privatsphäre überaus wichtig. Die Benutzer möchten nicht, dass die IT das vollständige App-Inventar auf ihren Geräten sehen kann, da in einem solchen Fall die Privatsphäre nicht mehr geschützt wäre und beispielsweise Informationen zum Gesundheitszustand oder zur Konfession offen zugänglich wären. MobileIron gibt der IT-

Abteilung die Möglichkeit, Unternehmens-Apps und Apps von schwarzen Listen zu überwachen, ohne dass die auf den privaten Geräten installierten Apps offengelegt werden.

Kompensatorische Kontrollmechanismen:

- *Sperren unsauberer Apps*: Bei der normalen Installation kann die IT-Abteilung nicht verhindern, dass ein Benutzer eine App herunterlädt, weil der Benutzer entscheidet, welche Software auf dem Gerät installiert wird. Insbesondere bei BYOD werden die meisten Benutzer darauf bestehen, private Apps auf ihre Geräte herunterladen zu können, da sie dieses Arbeitsprinzip ansonsten womöglich ablehnen. Die Sicherheitsarchitektur von Mobilgeräten verringert zusammen mit der Blacklist-/Whitelist-Richtlinie von MobileIron jedoch das Risiko, dass eine unsaubere App auf dem Gerät installiert wird.

8. Sicheres Browsen

Anforderungen:

- Sicherer Zugriff auf Web-Apps des Unternehmens hinter der Firewall
- Vermeidung von Datenverlusten bei heruntergeladenen Dokumenten und gecachten Web-Inhalten
- Schutz vor Drive-by-Malware-Angriffen

Grundlegende Kontrollmechanismen

- *Zugriff*: MobileIron Web@Work ist ein sicherer Browser, mit dem die Benutzer Zugriff auf Webressourcen des Unternehmens erhalten. Web@Work benutzt native Webansichten, so dass die Benutzererfahrung die Gleiche ist wie bei nativen Browsern, beispielsweise Safari. Auf diese Weise wird die Akzeptanz durch den Benutzer gefördert, da er sich nicht mit zwei unterschiedlichen Benutzeroberflächen vertraut machen muss.
- *Dokumente und Web-Cache*: MobileIron ermöglicht der IT die Definition angemessener Daten-Sharing-Regeln für das Herunterladen von Inhalten und für das Sichern und Löschen der Daten in einem Cachespeicher durch Auslöser, die in den Richtlinien definiert sind. Beispielsweise können Daten nicht aus dem Cache abgesaugt und der Cache kann nicht durch einen Jailbreak oder einen anderen Auslöser gelöscht werden.
- *Whitelist zur Blockade von Drive-by-Angriffen*: MobileIron Web@Work kann so konfiguriert werden, dass bestimmte interne Seiten auf eine Whitelist gesetzt werden. Das bedeutet Folgendes: Wenn der Benutzer eine Seite aufruft, die versucht, einen verborgenen Frame (d. h. eine andere Seite) zu öffnen, wird diese neue Seite blockiert, bis sie ebenfalls in die Whitelist aufgenommen wurde. Mit dieser Kontrollfunktion kann der Browser-Zugriff ausschließlich auf zugelassene Websites beschränkt und so das Risiko von Drive-by-Angriffen gemindert werden.

Viele Unternehmensressourcen stehen in der Form von Web-Apps hinter der Firewall zur Verfügung, erfordern jedoch Sicherheitskontrollen für gespeicherte und übertragene Daten ähnlich wie bei nativen Apps.

MobileIron Web@Work ermöglicht sicheres Browsing mit nativer Safari-Erfahrung und auf Richtlinien basierender Containerisierung zum Schutz lokaler Daten.

Schlussfolgerungen

Für IT-Abteilungen entsteht immer wieder die Notwendigkeit, neue mobile Betriebssysteme zu unterstützen, weil Betriebssystem und Gerät jetzt vom Verbraucher bestimmt werden, nicht durch das Unternehmen, und der Verbraucher sie häufig wechseln kann. Mobilität ist eines der eindeutigsten Beispiele für die Verbraucherorientierung der IT, bei der das Kundenverhalten bestimmt, welche Technologien sich in Unternehmen durchsetzen.

Mobile Betriebssysteme wie Android und iOS und MobileIron als Plattform für Enterprise Mobility Management (EMM) sind so ausgereift, dass eine mehrstufige Sicherheitskontrolle zur Verfügung steht und das Unternehmen das Risiko von Datenverlusten auf unternehmenseigenen und privaten Geräten minimieren kann.

Durch diese Kontrollfunktionen können Unternehmen jetzt die neue Generation mobiler Betriebssysteme und Geräte nutzen, nach denen ihre Benutzer verlangen.

Weitere Informationen über MobileIron finden Sie unter www.mobileiron.com.

©2009-2014 MobileIron, Inc. Alle Rechte vorbehalten. MobileIron, MyPhone@Work und Connected Cloud sind eingetragene Markenzeichen von MobileIron. Alle anderen Produkt- oder Firmennamen können Markenzeichen und/oder eingetragene Markenzeichen ihrer jeweiligen Eigentümer sein. Obwohl jede Anstrengung unternommen wurde, um die Richtigkeit der in diesem Dokument aufgeführten Informationen sicherzustellen, übernimmt MobileIron keine Haftung für Fehler oder Irrtümer. Technische Daten und andere Informationen in diesem Dokument können jederzeit ohne vorherige Ankündigung geändert werden.