MobileIron

WHITE PAPER

Docs@Work: Schutz vor Datenverlust und sicherer Zugriff auf Mobile Content

Einführung

Unternehmen nutzen zunehmend Mobilgeräte, insbesondere Smartphones und Tablets, als ihre primären Computing-Endgeräte. Benutzer von mobilen Geräten erwarten Zugriff auf ein breites Spektrum an Inhalten hinter der Firewall, von E-Mails bis unternehmenseigenen Speicherungssystemen wie Microsoft SharePoint. Diese Verschiebung zu mobilen Geräten bringt allerdings neue Herausforderungen mit sich, die das Risiko des Datenverlusts erhöhen:

- Mobilgeräte werden für die Benutzer konstruiert. Aus technischer Sicht ist ein ausführlicher Lockdown dieser Geräte, wie er bei Laptops vorgenommen wird, unmöglich. Lockdowns beeinträchtigen auch den Benutzerkomfort. Für die Zufriedenheit der Benutzer erlauben die meisten Unternehmen daher eine Mischung aus privaten und Unternehmens-Apps auf Mobilgeräten, wodurch erheblich weniger Einschränkungen entstehen.
- Mobilgeräte verfügen über sehr viel Speicherkapazität. Potenziell kann eine Vielzahl an Unternehmensdaten lokal auf einem Mobilgerät gespeichert werden.
- Mobilgeräte sind mit einer Cloud verbunden. Datendienste wie Dropbox haben das Verschieben von Daten von Mobilgeräten in die Cloud und damit außerhalb des Kontrollbereichs der Unternehmen erheblich vereinfacht.
- Mobilgeräte verfügen über Hyperkonnektivität. Mobilfunkverbindungen sind dauerhaft. Mobilgeräte versuchen, permanent auf verfügbare Netzwerke (Unternehmensnetzwerke, öffentliche Netzwerke oder Mobilfunk-Netzwerke) zuzugreifen, egal ob diese vom Unternehmen als vertrauenswürdig eingestuft werden.

MobileIron wurde speziell entwickelt, um diese Probleme zu beheben. Die MobileIron-Plattform bietet Unternehmen Sicherheit und Verwaltung von mobilen Apps, Inhalten und Geräten. MobileIron ist sowohl als standort- als auch Cloud-basierte Lösung erhältlich. In diesem Dokument liegt der Fokus auf Sicherheitslösungen für Inhalte und es bietet einen Überblick über das Docs@Work-Produkt von MobileIron für iOS-Geräte. Docs@Work bietet Endbenutzern eine intuitive Möglichkeit, auf Dokumente aus E-Mails und SharePoint zuzugreifen, diese zu speichern und anzuzeigen. Es ermöglicht mobilen IT-Administratoren den Aufbau von DLP-Kontrollen (Data Loss Prevention), um diese Dokumente vor nicht autorisierter Verbreitung zu schützen.

Die Vergangenheit: Umfassende Containerisierung von E-Mails

E-Mails sind die Primärquelle von Unternehmensdokumenten, die auf Mobilgeräte übertragen werden. Unternehmen fragen oft, wie sie E-Mails containerisieren

Sichere Inhalte

In vielen Organisationen sind E-Mails und SharePoint zwei der größten Speicherungssysteme für unternehmenseigene Dokumente. Benutzer von mobilen Geräten benötigen Zugriff auf diese Dokumente, aber Mobile weist einige Herausforderungen auf, die das Risiko des Datenverlusts erhöhen:

- Private und geschäftliche Verwendung
- Umfassende lokale Speicherung
- Cloud-Konnektivität
- Hyperkonnektivität

Mobile IT-Unternehmen müssen E-Mail-Anhänge und SharePoint-Dokumente in dieser Umgebung sicher machen und gleichzeitig den gewohnten Benutzerkomfort von Mobilgeräten und Betriebssystemen aufrechterhalten.

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

können. Ihr Ziel ist es, geschäftliche und private E-Mails zu trennen, damit die ersteren gesichert werden und die letzteren besonders in BYOD-Umgebungen unangetastet bleiben können. iOS bietet zwar bereits DLP-Kontrollen (Data Loss Prevention) für die Texte in E-Mails, allerdings nicht für Anhänge.

Die Herausforderung der mobilen IT liegt darin, den Benutzern auf ihren Mobilgeräten vollen Zugriff auf Unternehmens-E-Mails zu ermöglichen und gleichzeitig sicherzustellen, dass die Benutzer nicht in der Lage sind, geschäftliche E-Mail-Anhänge in Apps oder Cloud-basierten Speicherdiensten zu speichern, die sich außerhalb des Kontrollbereichs des Unternehmens befinden. Der Vor- und gleichzeitig Nachteil der Mobilität für Unternehmen ist, dass das Verteilen von Informationen vom Gerät an externe Cloud-Dienste einfach ist und häufig passiert, da nur ein Klick dafür notwendig ist. Ein geschäftlicher E-Mail-Anhang kann schnell ohne böswillige Absicht oder sogar Anstrengung des Benutzers in der Dropbox landen.

Deshalb waren einige regulierte Unternehmen wie z. B. Finanzdienstleister der Meinung, dass sie keine andere Wahl haben, als ein separates E-Mail-System auf den Geräten zu installieren, das einen lokalen E-Mail-Container zum Schutz der Anhänge enthält. Leider hat dieser Ansatz die Benutzer zu einer E-Mail-Anwendung gedrängt, die sie nicht mögen.

Benutzer haben ihre App Store-Bewertungen abgegeben. In fast allen Organisationen bevorzugen die Benutzer die systemeigene iOS-E-Mail-Anwendung und nicht die E-Mail-Container von Drittanbietern. Die Benutzer möchten integrierte Anwendungen, Push-Zustellung in Echtzeit, hohe Leistung und gute Nutzbarkeit. Und dies können ihnen nur systemeigene iOS-E-Mail-Anwendungen bieten. Allerdings wurden ihnen in der Vergangenheit von ihrer Organisation nur containerisierte E-Mail-Apps von Drittanbietern zur Verfügung gestellt.

Die Zukunft: Gezielte Containerisierung

MobileIron Docs@Work ermöglicht der mobilen IT den Schutz von E-Mail-Anhängen in systemeigenen iOS-E-Mail-Anwendungen mit Containerisierung, die ausdrücklich auf die Speicherung von Dokumenten ausgelegt ist. Die Benutzer können die E-Mail-Anwendung ihrer Wahl nutzen und die IT muss keine separaten Infrastrukturen verwalten, um die Sicherheit zu wahren. Dieselben Docs@Work-Kontrollen gelten auch für Dokumente aus SharePoint. Für zukünftige Veröffentlichungen sind auch noch andere Inhaltsspeicherungssysteme geplant.

Die sichere Inhaltsschnittstelle von Docs@Work ist ein Container für Dokumente auf dem Mobilgerät mit strengen Kontrollen, durch die mobile IT in der Lage ist, Zugriff zu gewähren und gespeicherte Daten zu schützen.

- Anzeige von Dokumenten
- Sichere Speicherung von Dokumenten auf dem Gerät
- Schutz von Daten durch Verschlüsselung auf Anwendungsniveau, z. B. iOS Data Protection auf iPhones und iPads

- Selektives Löschen von Dokumenten auf dem Gerät, wenn das Gerät gefährdet ist oder ein „Jailbreak“ vorliegt (sogar wenn das Gerät offline ist)
- Selektives Löschen von Dokumenten auf dem Gerät, wenn der MobileIron-Server aufgrund von Nichteinhaltung in Quarantäne steckt
- Sperren der Funktionen der Zwischenablage zum Ausschneiden/Kopieren/Einfügen von Informationen über sichere Dokumente an andere Apps
- Steuerung des Zugriffs externer Programme auf sichere Dokumente
- Vorbeugung der Verteilung sicherer Dokumente via E-Mail
- Nutzung bereits konfigurierter Richtlinien, Benutzer, Rollen, Gruppen und Berechtigungen der MobileIron-Plattform

Administratoren können ruhig schlafen, da sie wissen, dass sich ihre Unternehmensdokumente in einem sicheren Container und nicht in einer Anwendung oder einem Cloud-Dienst befinden, der außerhalb ihres Kontrollbereichs liegt.

Sicherheit für E-Mail-Anhänge

E-Mail-Anhänge sind die Primärquelle von mobilen Dokumenten. Die Sicherheit von E-Mail-Anhängen beginnt mit der intelligenten Übertragung der Anhänge vom ActiveSync-Server auf das Mobilgerät.

Docs@Work nutzt MobileIron Sentry, um E-Mails fortwährend nach Anhängen zu durchsuchen. Sentry ist das intelligente Gateway von MobileIron und dient als Inline Proxy für die ActiveSync E-Mail-Zugriffskontrolle. Wenn ein Anhang entdeckt wird, schützt Sentry diesen, damit er nur von Docs@Work geöffnet werden kann. Zudem kann Sentry AES-Verschlüsselung verwenden, um eine weitere Schutzschicht hinzuzufügen oder alle Anhänge zu entfernen, bevor sie auf das Mobilgerät gelangen.

Sentry ist intelligent: Wenn Benutzer Anhänge von ihrem geschäftlichen E-Mail-Konto an das Mobilgerät weiterleiten, wird der Dokumentenschutz entfernt, wenn der Anhang über Sentry zurück auf den E-Mail-Server des Unternehmens geleitet wird. Der Unternehmensserver leitet den korrekt formatierten Anhang anschließend an den entsprechenden Benutzer über die vom Unternehmen verwendeten DLP-Kontrollen weiter. Sentry schützt mobile Anhänge, aber beeinträchtigt dabei nicht die E-Mail-DLP-Kontrollen, die bereits vom Unternehmen eingesetzt werden.

Wenn Docs@Work einen E-Mail-Anhang auf einem Mobilgerät öffnet, kann es jetzt also das Dokument in der sicheren Inhaltsschnittstelle mit allen oben beschriebenen Schutzmaßnahmen speichern.

Die mobile IT kann Unternehmensdaten in E-Mail-Anhängen ausreichend schützen, ohne die systemeigenen iOS-E-Mail-Anwendungen zu beeinträchtigen. Und vor allem sind die Benutzer zufrieden, da sie jetzt die iOS-E-Mail-Anwendung für geschäftliche Kommunikation nutzen können, die sie gegenüber E-Mail-Apps von Drittanbietern bevorzugen.

Zugriff auf Unternehmensinhalte

Während mobile geschäftliche Kommunikation heutzutage primär über E-Mails abgewickelt wird, werden viele Unternehmensinhalte in Speicherungssystemen wie SharePoint gespeichert. Docs@Work ermöglicht zusätzlich, dass die Benutzer über WebDAV-Protokolle Zugriff auf Inhaltsspeicherungssysteme erhalten.

Administratoren können Docs@Work zentral konfigurieren. Benutzernamen und Serverinformationen können anhand von Active Directory oder LDAP-Gruppen automatisch angelegt werden. Da Docs@Work Teil des auf dem Gerät vorinstallierten MobileIron-Client ist, wird keine weitere Software benötigt. Daher kann Docs@Work schnell bedarfsgerecht eingesetzt werden, ohne dass der Endbenutzer aktiv werden muss.

Mit Docs@Work können die Benutzer die Netzwerk-Dateifreigabe navigieren, um Inhalte anzeigen zu lassen. Die Benutzer können Inhalte auch lokal auf ihrem Gerät speichern, um sie sich offline anzeigen zu lassen. Docs@Work aktualisiert diese Offline-Inhalte, wenn das Gerät verbunden und die Datei zur Ansicht geöffnet ist.

Alle Inhaltsschutzmechanismen für E-Mail-Anhänge, einschließlich Quarantäne von Unternehmensdaten und gesperrter Zugang zu Remote-Informationen, sind auch verfügbar, wenn über SharePoint auf die Netzwerk-Dateifreigabe zugegriffen wird.

MobileIron Sentry bietet Sicherheit für übertragene Daten

Mobilgeräte verfügen über Hyperkonnektivität und nutzen eine Vielzahl von Netzwerken, um Zugriff auf Unternehmensdaten zu erhalten. Leider sind nicht alle diese Netzwerke vertrauenswürdig. Daher ist Sitzungssicherheit von höchster Bedeutung.

Um das Risiko nicht vertrauenswürdiger Netzwerke zu mindern, nutzt MobileIron Sentry ein Authentifizierungsmodell mit zwei Phasen für den Zugriff auf geschäftliche E-Mails. Mit diesem Modell wird die Geräteidentität mit einem Zertifikat bestätigt. Dieses Zertifikat kann entweder von einer geschäftlichen Zertifizierungs-stelle (CA) oder vom MobileIron-Server, in den eine CA integriert ist, selbst ausgestellt werden. Für den letzteren Ansatz wird keine zusätzliche Infrastruktur benötigt. Wenn das Zertifikat auf dem Gerät installiert ist, muss es dem Sentry-Server angezeigt werden. Ohne das Zertifikat werden alle Versuche, auf E-Mails zuzugreifen, abgelehnt.

In der zweiten Phase der Authentifizierung werden der Benutzername und das Passwort benötigt. Sobald die Geräteidentität bestätigt wurde, wird die Benutzeridentität zurück an den geschäftlichen ActiveSync E-Mail-Server gesendet. Dadurch sind E-Mail-Administratoren in der Lage, Benutzeridentitäten zu bestätigen, ohne die E-Mail-Infrastruktur zu ändern (z. B. durch Konfiguration von Kerberos). Sentry unterstützt auch die einfache zertifikatbasierte Authentifizierung mit Kerberos.

Durch die zertifikatbasierten Identitäten können sich Unternehmen sicher sein, dass die Kommunikation vom Mobilgerät bis hin zum Sentry-Server sicher ist. Wenn sich ein Mobilgerät mit einem nicht vertrauenswürdigen Netzwerk verbindet, das

versucht, die Endnutzerkommunikation auszuspionieren, wird das Zertifikat von Sentry als ungültig eingestuft und über das Netzwerk kann keine Kommunikation stattfinden. Da MobileIron als CA Zertifikate ausstellen und Sentry diese verarbeiten kann, profitieren Organisationen von End-to-End-Sitzungssicherheit ohne zusätzliche Infrastruktur, selbst wenn sie über keinen Zugang zu einer CA verfügen.

Schlussfolgerungen

MobileIron Docs@Work deckt den gesamten Lebenszyklus von Mobile Content-Sicherheit ab:

- Schützt gespeicherte Daten mit einer sicheren Inhaltsschnittstelle oder einem Container auf dem Gerät
- Verhindert Datenverlust, indem es sicherstellt, dass E-Mail-Anhänge und andere Dokumente in der sicheren Inhaltsschnittstelle nicht von nicht vertrauenswürdigen Apps geöffnet werden
- Bewahrt systemeigene E-Mail-Anwendungen, indem es Anhänge sichert, ohne dass E-Mail-Apps von Drittanbietern benötigt werden
- Bietet einen sicheren Zugang zu SharePoint
- (Mit MobileIron Sentry) Sichert die E-Mail-Sitzung End-to-End mit zertifikatbasierten Identitäten, um zu verhindern, dass Unternehmensdaten in nicht vertrauenswürdigen Netzwerken auftauchen

Docs@Work bewältigt die wichtigen Inhaltsherausforderungen für mobile IT: Gewährleistung eines hervorragenden Benutzererlebnisses ohne Beeinträchtigung der Dokumentensicherheit. **MobileIron ist die einzige Mobile IT-Plattform, die sicheren Zugriff und DLP-Kontrollen inhaltsübergreifend für geschäftliche E-Mails und SharePoint bietet.**

Weitere Informationen zu den mobilen IT-Lösungen von MobileIron zur Sicherung und Verwaltung von mobilen Apps, Dokumenten und Geräten finden Sie unter http://www.mobileiron.com/