MobileIron

LIVRE BLANC

Sécurité mobile :
Menaces et mesures de prévention

Introduction

Les appareils mobiles sont en passe de devenir la principale plateforme informatique des utilisateurs finaux en entreprise. Outre une prise en main intuitive, ils offrent des fonctionnalités avancées, un catalogue d'applications étoffé, une connectivité permanente et une portabilité qui n'ont rien à envier aux ordinateurs. Toutefois, la transition du PC au mobile est un bouleversement majeur pour les entreprises, qui doivent envisager la sécurité de leurs données sous un nouvel angle pour réduire les risques. En effet, compte tenu des différences fonctionnelles entre les mobiles et les PC, les services informatiques doivent adopter de nouveaux outils de gestion et de nouvelles stratégies pour protéger les contenus d'entreprise. Cependant, ces entreprises qui passent au tout mobile et s'adaptent à l'évolution de leurs utilisateurs ne le regrettent pas, notamment car elles se démarquent de leurs concurrents et font preuve d'un grand esprit d'innovation.

Ce document résume les contrôles natifs, supplémentaires et complémentaires pouvant être mis en place avec MobileIron afin de limiter le risque de perte de données sur les appareils mobiles personnels et professionnels.

Points importants concernant le passage au Mobile First

Deux raisons principales obligent les services informatiques à adopter de nouvelles stratégies pour sécuriser les données d'entreprise lors du passage du PC au mobile, quand l'objectif est d'améliorer la productivité des utilisateurs.

- **Les mobiles échappent plus facilement au contrôle des services informatiques :** l'utilisateur final est l'acteur principal de l'ère Mobile First. C'est lui qui choisit la plateforme mobile qui lui convient le mieux. Il s'attend à ce que son appareil de prédilection fonctionne dans un contexte professionnel, et notamment à ce que l'ensemble des applications et des documents dont il a besoin pour être efficace soient disponibles. Cette situation est aux antipodes de celle de l'ère du PC, car jusqu'alors, le service informatique fournissait aux utilisateurs finaux un PC approuvé contenant un ensemble d'applications présélectionnées. Les utilisateurs n'avaient pas vraiment leur mot à dire sur les fonctionnalités disponibles sur leur PC et le service informatique contrôlait le moindre aspect de l'appareil d'entreprise, des ports physiques aux versions des applications et logiciels. Sur leur mobile, les utilisateurs reprennent le contrôle de plusieurs de ces paramètres et le service informatique se contente de recommander des appareils et des applications. Il n'a pas le pouvoir d'instaurer un système d'exploitation, un appareil ou une application standard pour l'ensemble de l'entreprise. Pire, plus le service informatique essaie de verrouiller les appareils, plus les utilisateurs tentent de contourner les règles imposées et font prendre des risques à l'organisation.

- **Les modèles de sécurité traditionnels ne sont plus efficaces :** sur les PC, la sécurité du système d'exploitation pouvait être assurée efficacement par un agent. Il suffisait d'installer un logiciel sur le PC pour qu'il contrôle les processus et données associés aux autres applications. Malheureusement, ces agents sont inefficaces sur les mobiles, car les systèmes d'exploitation ne sont pas conçus de la même façon. En effet, les systèmes d'exploitation pour mobiles reposent sur une architecture en bac à sable (« sandbox ») qui permet d'isoler les applications et les données associées, et de contrôler

MAKING ENTERPRISE MOBILE FIRST

MobileIron

415 East Middlefield Road
Mountain View, CA 94043 États-Unis
Tél. : +1 650 919 8100
Fax : +1 650 919 8006
info@mobileiron.com

les interactions et les partages de données de ces applications grâce à des mécanismes bien définis. Cette architecture est plus sécurisée que celle des PC et nécessite de nouveaux outils qui tirent parti des fonctions de sécurité proposées directement par le fabricant d'appareils.

L'adoption fulgurante des mobiles dans le milieu professionnel offre de grandes opportunités de croissance et d'innovation, mais expose également les entreprises à davantage de risques. Ce document récapitule les principales menaces introduites par les appareils mobiles et indique comment les services informatiques peuvent utiliser les outils de gestion de la mobilité en entreprise (EMM) pour diminuer les risques et protéger les données professionnelles sans compromettre la productivité des utilisateurs finaux.

Menaces introduites par les mobiles

À mesure que de nouvelles pratiques, telles que le BYOD, deviennent monnaie courante en entreprise et contribuent au développement rapide des appareils mobiles pour améliorer la productivité des employés, les données des entreprises sont exposées à de nombreux risques et font face à un nouveau genre de menaces. Ces menaces peuvent être regroupées en trois catégories :

1) **Menaces liées aux appareils**
   Les appareils mobiles permettent aux utilisateurs finaux de réaliser un grand nombre de tâches liées à leur travail, telles que consulter leurs e-mails, et accéder aux contenus d'entreprise, les modifier et les partager, par le biais d'applications axées sur la productivité. De ce fait, ils stockent de plus en plus de données sensibles, qui sont alors plus vulnérables en raison des facteurs suivants :
   - Les mobiles sont connectés en permanence et peuvent constituer une porte d'entrée pour des personnes non autorisées à accéder aux contenus d'entreprise.
   - Les logiciels sont plus fragiles et les appareils peuvent facilement être déverrouillés (« jailbreak » ou « root »), créant une faille de sécurité.
   - Le format compact des mobiles facilite les pertes et les vols.

2) **Menaces liées aux réseaux**
   Conformément au principe d'activité permanente, les appareils mobiles doivent constamment être connectés à Internet. Résultat : les utilisateurs finaux sont tentés de se connecter à des réseaux publics non sécurisés, que des personnes malveillantes peuvent utiliser pour accéder à l'appareil et intercepter les données transmises. Voici les méthodes les plus courantes :
   - Points d'accès malveillants
   - Outils de détection Wi-Fi (« reniflage »)
   - Attaques « man-in-the-middle » sophistiquées

3) **Menaces liées aux utilisateurs**
   L'informatique mobile donne le pouvoir aux utilisateurs finaux. Bien que cela constitue pour eux une avancée en matière de choix, des utilisateurs bienveillants peuvent s'engager dans des activités à risque qui compromettent la sécurité des contenus d'entreprise. Voici quelques exemples de comportements à risque :
   - Utiliser des applications cloud non autorisées pour partager et synchroniser des données
   - Utiliser des applications de productivité non autorisées qui conservent une copie des données d'entreprise
   - Déverrouiller (via jailbreak ou root) son appareil pour contourner les contrôles de sécurité
   - Utiliser des applications malveillantes provenant de boutiques d'applications non autorisées
   - Divulguer des données d'entreprise avec de mauvaises intentions

Certains peuvent penser que les menaces inhérentes aux appareils mobiles sont similaires à celles introduites par les ordinateurs portables et autres appareils informatiques portatifs. Cependant, les différences fondamentales entre les systèmes d'exploitation des PC et des mobiles obligent les services informatiques à adopter des plateformes de gestion de la mobilité en entreprise (EMM) pour réduire les risques liés à l'utilisation des mobiles.

Contremesures pour prévenir les pertes de données sur mobile

La prévention des pertes de données sur les appareils mobiles repose sur un modèle de sécurité multicouche. Ces couches de sécurité peuvent être implémentées via les contrôles répertoriés ci-dessous :

1) Architecture de système d'exploitation sécurisée
2) Authentification
3) Effacement à distance
4) Cryptage
5) Partage des données
6) Sécurité du réseau
7) Gestion du cycle de vie des applications
8) Sécurité de la navigation

Les pages suivantes décrivent les exigences en matière de prévention de la perte des données et les contrôles spécifiques pris en charge par MobileIron. Chacune des catégories de contrôle peut comprendre des contrôles natifs, qui répondent directement aux besoins, des contrôles supplémentaires, qui renforcent les contrôles disponible par nature, et des contrôles complémentaires, qui s'appliquent lorsqu'aucun contrôle natif n'est disponible. Ensemble, ces contrôles de sécurité multicouches constituent le modèle de prévention de perte des données sur mobile.

1. Architecture de système d'exploitation sécurisée

Exigences :

- Applications sandbox pour empêcher les programmes malveillants d'accéder aux données des applications
- Écosystème d'applications sécurisé
- Protection de l'intégrité du système d'exploitation
- Mise en place rapide de correctifs aux vulnérabilités du système d'exploitation

Contrôles natifs :

- *Sandbox* : une « sandbox » est un ensemble de données isolées et associées à une application sur un mobile. Contrairement aux systèmes d'exploitation sur PC, les systèmes d'exploitation pour mobiles ne permettent pas aux applications d'accéder aux données en dehors de leur sandbox spécifique, sauf en cas de contrôles de partage bien définis. Cela réduit le risque d'endommagement ou de vol des données par des programmes malveillants, car, même téléchargés sur l'appareil, ceux-ci ne pourront pas accéder au système de fichiers.
- *Écosystème d'applications* : les boutiques d'applications mobiles, telles que Google Play et l'App Store, sont conçues pour limiter la probabilité de programmes malveillants dans les applications publiées. Apple interdit certaines portes dérobées, comme le téléchargement d'un nouveau code exécutable dans une application déjà approuvée. Les boutiques d'applications peuvent par ailleurs retirer immédiatement les applications qui violent les règles.
- *Intégrité du système d'exploitation* : « jailbreak » (ou « root ») est le terme utilisé dans la communauté mobile pour définir un déverrouillage du système d'exploitation sous-jacent qui supprime les mécanismes de sécurité intégrés. MobileIron procède en permanence à des détections de jailbreak et de root sur chaque appareil mobile enregistré afin de s'assurer que le système d'exploitation n'a pas été compromis. Si c'est le cas, MobileIron déclenche l'action de sécurité appropriée en se basant sur la règle définie par l'organisation. Ce processus peut être réalisé en ligne ou hors connexion, quand l'appareil est perdu ou volé, et n'est plus connecté au réseau.
- *Correctifs du système d'exploitation* : Apple contrôlant la distribution globale du système d'exploitation iOS, toute vulnérabilité considérée comme importante est souvent corrigée rapidement et la nouvelle version d'iOS qui en résulte est rendue disponible au téléchargement pour la base d'utilisateurs. La disponibilité des correctifs du système d'exploitation Android dépend des fabricants d'appareils et des opérateurs mobiles.

Contrôles supplémentaires :

- *Application des mises à jour du système d'exploitation* : MobileIron surveille la version du système d'exploitation de tous les appareils gérés par son système. Ainsi, si des utilisateurs oublient de mettre à jour leurs appareils après la publication d'un correctif, ces appareils sont mis en quarantaine et les données d'entreprise peuvent être supprimées jusqu'à la résolution du problème.

Contrôles complémentaires :

- *Surveillance de la version du système d'exploitation* : contrairement aux systèmes Windows traditionnels, le service informatique ne contrôle pas la distribution des correctifs du système d'exploitation pour iOS ou Android. Cela signifie que les nouveaux correctifs sont disponibles pour les utilisateurs lorsque les fabricants d'appareils les publient, que le service informatique les ait approuvés ou non. Grâce à MobileIron, le service informatique a toujours la possibilité de surveiller les versions du système d'exploitation et de prendre les mesures qui s'imposent si les utilisateurs ont procédé trop rapidement ou trop tardivement à la mise à niveau.

L'architecture en bac à sable du système d'exploitation isole les données relatives aux applications dans des conteneurs distincts afin de limiter le risque qu'un programme malveillant endommage ou dérobe des données.

MobileIron surveille l'intégrité et les versions du système d'exploitation afin de garantir sa conformité et sa cohérence au sein de l'organisation.

2. Authentification

Exigences :

- Configuration à distance de la règle de mots de passe
- Effacement automatique des données de l'appareil après un certain nombre d'échecs d'authentification
- Application de l'identité pour les services d'entreprise

Contrôles natifs :

- *Mot de passe sur l'appareil :* MobileIron permet la configuration à distance et l'application en local d'une règle de mots de passe pour l'appareil. Le service informatique peut configurer les variables suivantes pour les règles de mot de passe via MobileIron :
  - Type
  - Longueur minimum
  - Délai maximum d'inactivité
  - Nombre minimum de caractères complexes
  - Durée de validité maximale du mot de passe
  - Nombre maximum d'échecs
  - Historique du mot de passe
  - Période de tolérance avant le verrouillage de l'appareil
- *Mot de passe pour l'application* : MobileIron AppConnect est une solution de compartimentation pour la sécurisation des applications internes et publiques. L'une de ses fonctionnalités est l'authentification pour l'accès à l'ensemble des applications sécurisées sur l'appareil.
- *Effacement automatique* : un nombre trop élevé d'échecs peut indiquer un vol et entraîner un effacement automatique des données de l'appareil.
- *Identité basée sur un certificat* : MobileIron utilise des certificats numériques pour sécuriser l'accès aux services de l'entreprise sur l'appareil, notamment la messagerie, le Wi-Fi et le VPN. L'expérience utilisateur s'en trouve améliorée, car l'utilisateur n'a pas besoin de saisir son mot de passe à chaque fois. Si un appareil ou un utilisateur s'avère non conforme, il suffit de supprimer le certificat de clé publique pour couper l'accès au service correspondant.

Contrôles supplémentaires :

- *Authentification biométrique* : Apple a publié son premier mécanisme d'authentification biométrique, Touch ID, avec l'iPhone 5S, fin 2013. Touch ID permet à l'utilisateur de s'authentifier sur son appareil grâce à son empreinte, ce qui réduit le risque de vol de mot de passe par-dessus l'épaule :
  - Après plusieurs échecs de l'authentification par empreinte, un écran de mot de passe est présenté à l'utilisateur, conformément à la règle de MobileIron.
  - Avant la diffusion de Touch ID, le principal désagrément de l'authentification était la nécessité de définir des mots de passe plus sûrs, et donc plus difficiles à mémoriser et à saisir. En conséquence, pour encourager l'adoption du système par mot de passe, de nombreuses sociétés de services financiers devaient autoriser un mot de passe plus faible que ce qui aurait été nécessaire. Un mot de passe avec un niveau de sécurité faible, c'est également un cryptage moins fiable et une augmentation du risque d'attaque de l'appareil par force brute.
  - En revanche, avec Touch ID comme entrée principale, le service informatique peut revenir à des mots de passe plus sûrs, car l'utilisateur n'aura à saisir son mot de passe que si son authentification par empreinte échoue à plusieurs reprises, ce qui représente un indicateur assez fort d'un potentiel vol.

De nouvelles méthodes biométriques prises en charge par iOS peuvent renforcer les contrôles d'authentification et de cryptage.

MobileIron fournit un moteur de règles pour l'authentification au niveau de l'appareil et au niveau de l'application afin d'empêcher tout accès non autorisé aux données d'entreprise.

3. Effacement à distance

Exigences :

- Pour les appareils détenus par l'entreprise, effacement à distance de toutes les données sur l'appareil
- Pour les appareils détenus par l'employé, effacement à distance des SEULES données de l'entreprise sur l'appareil

Contrôles natifs :

- *Effacement complet* : MobileIron permet à l'administrateur ou l'utilisateur d'envoyer une commande d'effacement à distance sur l'appareil. Toutes les données de l'appareil sont ainsi effacées et les paramètres par défaut sont restaurés.
- *Effacement sélectif* : MobileIron permet également à l'administrateur de supprimer uniquement les données de l'entreprise sur l'appareil, ce qui implique :
    - Supprimer le compte de messagerie professionnel sur l'appareil sans toucher au compte de messagerie personnel.
    - Supprimer sur l'appareil les applications qui ont été installées par le biais de l'App Store de l'entreprise MobileIron sans toucher aux applications personnelles.
    - Supprimer sur l'appareil les certificats numériques qui permettent l'authentification aux services d'entreprise tels que la messagerie, le Wi-Fi et le VPN.
    - Supprimer les contenus de l'entreprise, tels que les documents, présentations, feuilles de calcul, etc.
    - Interrompre l'application des règles de l'entreprise.

La séparation logique des données personnelles et des données professionnelles sur l'appareil permet au service informatique de prendre les mesures nécessaires pour préserver la sécurité de l'entreprise sans pour autant compromettre la confidentialité de chacun.

Contrôles supplémentaires :

- *Confidentialité* : les entreprises s'inquiètent du risque de suppression par le service informatique des données personnelles de l'utilisateur sur un appareil BYOD, suite à une erreur humaine, à l'effacement des données d'un appareil perdu, ou si l'entreprise n'a pas d'autre choix, comme dans le cas d'une procédure judiciaire. Dans une telle situation, l'utilisateur risque de perdre des données personnelles importantes, comme des photos de famille ou des SMS privés.
    - MobileIron permet au service informatique de définir une règle de confidentialité par appareil ou par groupe, de sorte que seules les informations affectant la sécurité puissent lui être accessibles.
    - Tout programme BYOD doit être accompagné d'une politique claire et correctement communiquée en ce qui concerne les pratiques raisonnables en matière d'accès aux données et de suppression des informations au cours du fonctionnement normal. Sans cela, l'adoption du BYOD sera restreinte par des suppositions erronées de la part d'utilisateurs inquiets pour leur confidentialité.
    - Les programmes BYOD doivent également être accompagnés d'un accord signé de l'utilisateur final qui protégera juridiquement l'organisation au cas où des données personnelles seraient supprimées, même s'il est peu probable que cela se produise lors d'une utilisation normale.
    - La possibilité d'une telle situation ne pouvant toutefois être totalement écartée, le programme BYOD devra enfin apprendre à ses utilisateurs à sauvegarder leurs données personnelles, par exemple avec le service iCloud d'Apple. De cette façon, même si les données de l'appareil sont effacées, les informations personnelles ne sont pas perdues. Il s'agit d'une bonne pratique pour l'utilisateur final, tout comme les sauvegardes de données d'entreprise sont une bonne pratique pour le service informatique.

MobileIron gère le cycle de vie des services d'entreprise sur l'appareil, notamment la distribution, la configuration, la protection des données et la suppression, avec des règles distinctes pour les appareils professionnels et les appareils personnels.

4. Cryptage

Exigences :

- Crypter toutes les data-at-rest d'entreprise sur l'appareil
- Crypter toutes les data-in-motion d'entreprise provenant et issues de l'appareil
- Crypter toutes les données d'entreprise dans les applications sécurisées

Contrôles natifs :

- *Cryptage des data-at-rest (intégré) :* MobileIron peut garantir la présence et la complexité du mot de passe de l'appareil afin d'assurer que ce niveau de cryptage est disponible pour toutes les applications. Plus le mot de passe de l'appareil est sûr, plus la deuxième couche de cryptage est fiable. La méthode d'authentification biométrique d'Apple, Touch ID, permet au service informatique d'appliquer un mot de passe sûr par le biais de MobileIron sans nuire à l'expérience de connexion de l'utilisateur.
- *Cryptage des data-at-rest (supplémentaire)* : la solution de compartimentation pour les applications MobileIron AppConnect offre différents contrôles de sécurité supplémentaires, et notamment le cryptage. Bien qu'iOS et Android intègrent déjà le cryptage, de nombreuses organisations recherchent ce niveau supplémentaire pour les appareils qui ne sont pas verrouillés.
- *Data-in-motion* : les données mobiles d'entreprise, notamment les e-mails, les applications, les documents et les pages Web, transitent par la plateforme intelligente de MobileIron, appelée MobileIron Sentry. Elles sont protégées des attaques dites « man-in-the-middle » et des interceptions grâce à l'utilisation de certificats numériques et d'un chiffrement Transport Layer Security (TLS).
- *Certification FIPS 140-2* : l'utilisation par MobileIron de bibliothèques cryptographiques FIPS 140-2 est désormais validée par un cabinet CST (Cryptographic and Security) agréé, conformément au programme Cryptographic Module Validation Program (CMVP). Les lettres de certification sont disponibles ici.

Le cryptage MobileIron pour les data-at-rest et les data-in-motion est certifié FIPS 140-2 et vient compléter les fonctionnalités de cryptage intégrées aux systèmes d'exploitation.

5. Partage des données

Exigences :

- Pour la messagerie professionnelle dans l'application de messagerie native :
  - Interdiction de l'ouverture des pièces jointes dans une application non autorisée
  - Interdiction du transfert via un compte de messagerie personnel
  - Interdiction du copier/coller, de l'impression ou de la capture d'écran du texte des e-mails
  - Interdiction de la sauvegarde des e-mails sans l'approbation du service informatique
- Pour les applications d'entreprise :
  - Interdiction de la lecture des données des applications par des applications non autorisées
  - Interdiction du copier/coller, de l'impression ou de la capture d'écran des données des applications
  - Interdiction de la sauvegarde des données des applications sans l'approbation du service informatique

Contrôles natifs :

- Pour la messagerie professionnelle dans l'application de messagerie native :
  - *Pièces jointes* : la passerelle intelligente de MobileIron, MobileIron Sentry, crypte toutes les pièces jointes aux e-mails. Seule la visionneuse MobileIron Docs@Work peut les déchiffrer. Les pièces jointes sont stockées dans le conteneur sécurisé Docs@Work sur l'appareil. Les applications non autorisées ne peuvent pas accéder à ces pièces jointes, ni les déchiffrer. Sous Android, tous les e-mails professionnels sont stockés dans un espace de travail sécurisé et seules les applications autorisées peuvent accéder aux pièces jointes.
  - *Transfert* : MobileIron permet au service informatique de désactiver le transfert des e-mails d'un compte à un autre sur l'appareil.
  - *Copie* : MobileIron peut désactiver la fonction de capture d'écran de l'appareil. Toutefois, le client de messagerie iOS natif n'accepte pas la désactivation des fonctions de copier/coller ou d'impression du texte. La section *Contrôles complémentaires* ci-dessous décrit une méthode pour contourner ce problème.
  - *Sauvegarde* : le compte de messagerie d'entreprise géré par MobileIron sur l'appareil n'est jamais sauvegardé dans des services tels qu'iCloud.
- Pour les applications d'entreprise :
  - *Partage* : les systèmes d'exploitation pour mobiles permettent aux applications de partager des données entre elles grâce à la fonction « Ouvrir dans ». MobileIron permet au service informatique de déterminer quelles applications peuvent utiliser cette fonction pour accéder aux données des applications.
  - *Copie* : MobileIron AppConnect est une solution de compartimentation qui offre une couche supplémentaire de sécurité pour les applications d'entreprise, notamment la possibilité de limiter le copier/coller et l'impression des données des applications. MobileIron peut également désactiver la fonction de capture d'écran pour tout l'appareil.
  - *Sauvegarde* : MobileIron a la possibilité de désactiver la sauvegarde iCloud pour toutes les applications de l'appareil, mais les utilisateurs peuvent souhaiter utiliser ce service pour leurs données personnelles. Dans ce cas, MobileIron peut désactiver la sauvegarde iCloud pour certaines applications gérées uniquement, mais le service informatique devra s'assurer que ces applications ne sont pas codées pour utiliser iCloud pour la persistance de la paire clé/valeur ou des documents.

La principale cause de perte des données sur mobile est à attribuer à un utilisateur bien intentionné qui ouvre des données d'entreprise dans une application qui n'est pas sécurisée.

MobileIron AppConnect applique plusieurs contrôles du partage des données pour garantir que les données d'entreprise ne sont lues que dans des applications autorisées.

Contrôles complémentaires :

- *Client de messagerie* : le client de messagerie iOS natif n'a pas la possibilité de limiter les actions de copier/coller ou d'impression. Beaucoup d'organisations ont déterminé que ces fonctions n'engendrent qu'un faible risque de perte des données, car les données concernées sont peu nombreuses et l'action doit être intentionnelle. Par ailleurs, il existe beaucoup d'autres techniques de copie des données mécanique (clé USB) ou électronique (photo) pour les initiés malveillants. Toutefois, si le risque est toujours trop élevé, le service informatique peut déployer MobileIron Divide, un client de messagerie natif qui prend en charge tous les contrôles décrits.

6. Sécurité du réseau

Exigences :

- Prévention de la perte des données, les données d'entreprise transitant par des réseaux Wi-Fi et cellulaires publics hors du contrôle du service informatique.

Contrôles natifs :

- *Tunneling d'applications* : MobileIron Sentry offre un tunneling sécurisé au niveau de l'application pour toutes les données d'entreprise, notamment la messagerie, les applications, les documents et le trafic Web. Ainsi, le service informatique peut séparer le flux des données professionnelles (qui transitent via Sentry sur un canal sécurisé) et les données personnelles (qui transitent sur le réseau non sécurisé, hors Sentry).
- *VPN* : pour les entreprises utilisant une technologie VPN standardisée de type Cisco ou Juniper sur tous leurs appareils, MobileIron configure le service VPN afin d'offrir un canal sécurisé pour les données.
- *Architecture sans NOC* : le centre des opérations réseau (NOC, Network Operations Center) est le centre névralgique de la surveillance et de la gestion d'un réseau. Dans l'architecture BlackBerry traditionnelle, le NOC était le point de contrôle externe pour le réseau sécurisé, contrôlé par BlackBerry et par lequel le trafic de messagerie était transféré de l'entreprise à l'appareil. Cependant, les architectures basées sur le NOC créent un point de défaillance et de perte des données potentiel hors du contrôle du service informatique. Par chance, ni les modèles de tunneling d'applications ni les modèles de VPN décrits ci-dessus ne nécessitent un NOC externe. BlackBerry avait besoin du centre NOC, car l'ancien modèle de push mail exigeait que la solution collecte les e-mails sur le serveur de messagerie d'entreprise, les stocke dans un emplacement externe (NOC), puis les transfère à l'appareil. Toutefois, ce modèle n'est pas nécessaire, car le protocole ActiveSync est utilisé pour le push mail. L'architecture NOC de type stockage/transfert n'est ainsi plus indispensable. C'est d'ailleurs l'une des raisons qui a fait d'ActiveSync un protocole standard utilisé pour le push mail par la plupart des clients de messagerie tiers et intégrés.

Le modèle de sécurité mobile doit partir du principe que toutes les données d'entreprise transiteront par des réseaux publics.

MobileIron Sentry est la plateforme intelligente qui offre une tunnellisation sécurisée pour les données d'entreprise au niveau de l'application sur n'importe quel réseau.

7. Gestion du cycle de vie des applications

Exigences :

- Interdiction de télécharger des applications malveillantes sur l'appareil
- Création d'une liste noire pour les applications non autorisées
- Création d'une liste blanche pour les applications autorisées
- Publication et distribution d'applications d'entreprise
- Mise à jour d'applications d'entreprise

Contrôles natifs :

- *Applications malveillantes* : la plupart des risques liés aux applications malveillantes sont limités sur mobile, car :
    - l'architecture mobile isole les applications les unes des autres dans des sandboxes, de sorte qu'une application malveillante ne puisse pas accéder aux données depuis une application d'entreprise, sauf par le biais de méthodes de partage des données contrôlées par MobileIron ;
    - les boutiques d'applications publiques sont très surveillées et les programmes malveillants sont rares ;
    - Apple n'autorise pas les applications à télécharger du code exécutable. Ainsi, aucun code malveillant ne risque d'être introduit dans une application existante ;
    - bien qu'Android autorise le chargement de versions test et l'installation d'applications provenant de boutiques d'applications non approuvées, les administrateurs peuvent appliquer des règles pour désactiver les applications de test.
- *Liste noire/blanche* : MobileIron permet la création de listes noires et de listes blanches pour les applications grâce à des règles qui déclenchent des actions de notification et de contrôle d'accès appropriées si un appareil s'avère non conforme. MobileIron peut désactiver totalement la boutique d'applications, mais cela n'est pas recommandé, car les applications occupent une place extrêmement centrale dans l'expérience mobile. MobileIron intègre également des services de réputation des applications tiers afin d'identifier l'éventuelle présence d'applications à risque.
- *App Store d'entreprise* : MobileIron a inventé et breveté l'App Store d'entreprise, qui permet au service informatique de publier et distribuer en toute sécurité des applications internes et publiques à l'intention de la communauté d'utilisateurs.
- *Mises à jour des applications* : MobileIron surveille les versions des applications d'entreprise installées sur l'appareil. Ainsi, le service informatique peut inviter l'utilisateur à procéder aux mises à jour vers la dernière version lorsque celle-ci est disponible. La conformité est ainsi assurée au sein de l'entreprise et les éventuelles vulnérabilités de l'application en termes de sécurité sont rapidement corrigées.

Les applications sont un élément central de l'expérience mobile et un des plus grands vecteurs de productivité dans l'entreprise.

MobileIron a inventé l'App Store d'entreprise qui distribue et gère de manière sécurisée les applications d'entreprise.

Contrôles supplémentaires :

- *Inventaire des applications filtré* : dans les déploiements BYOD, la confidentialité est un élément essentiel. Les utilisateurs ne souhaitent pas que le service informatique puisse consulter l'intégralité de l'inventaire des applications de leurs appareils, car cela pourrait lui offrir un aperçu de leurs vies personnelles, par exemple leur santé ou leur religion. MobileIron donne également au service informatique la possibilité de surveiller les applications d'entreprise et les applications sur liste noire sans accéder à l'inventaire des applications personnelles.

Contrôles complémentaires :

- *Blocage des applications malveillantes* : dans les déploiements standards, le service informatique n'a pas la possibilité d'empêcher un utilisateur de télécharger une application, car c'est l'utilisateur qui décide des logiciels qui sont installés sur son appareil. Particulièrement avec le BYOD, la plupart des utilisateurs exigeront la possibilité de télécharger des applications personnelles sur leurs appareils, faute de quoi ils seront moins favorables à l'informatique mobile. Toutefois, l'architecture de sécurité des appareils mobiles, associée à la règle de liste noire/blanche de MobileIron, réduit le risque de la présence d'une application malveillante sur l'appareil.

8. Sécurité de la navigation

Beaucoup de ressources d'entreprise prennent la forme d'applications Web situées derrière le pare-feu, tout en nécessitant des contrôles de sécurité pour les data-at-rest et les data-in-motion similaires à ceux des applications natives.

Exigences :

- Accès sécurisé aux applications Web d'entreprise situées derrière le pare-feu
- Prévention de la perte des données des documents téléchargés et du contenu Web en cache
- Protection contre les attaques par des logiciels malveillants « drive-by »

Contrôles natifs :

- *Accès* : MobileIron Web@Work est un navigateur sécurisé qui permet à l'utilisateur d'accéder aux ressources Web de l'entreprise. Web@Work utilise l'affichage Web natif de sorte que l'expérience visuelle soit identique à celle des navigateurs natifs, tels que Safari. La préservation de l'expérience utilisateur assure une adoption supérieure, car l'utilisateur n'a pas besoin de connaître deux interfaces de navigation différentes.
- *Documents et cache Web* : grâce à MobileIron, le service informatique peut définir des règles de partage de données adaptées pour le contenu téléchargé et pour la sécurisation et la suppression des données en cache en réaction à des déclencheurs. Par exemple, les données ne peuvent pas être détournées du cache et le cache peut-être purgé suite à un élément déclencheur, comme le jailbreak.
- *Liste blanche bloquant les attaques « drive-by »* : MobileIron Web@Work peut être configuré pour placer dans une liste blanche certains sites internes. Cela signifie que si l'utilisateur accède à un site qui tente d'ouvrir une page masquée (c'est-à-dire un autre site), ce nouveau site sera bloqué s'il ne figure pas également sur la liste blanche. Ce contrôle peut être utilisé pour limiter l'accès du navigateur aux sites Web approuvés et réduire ainsi le risque d'attaques « drive-by ».

MobileIron Web@Work offre une navigation sécurisée avec une expérience visuelle native et une compartimentation basée sur des règles qui protège les données locales.

Conclusion

La prise en charge des nouveaux systèmes d'exploitation pour mobiles sera un défi perpétuel pour les services informatiques, car le choix du système d'exploitation et de l'appareil revient désormais à l'utilisateur, et non à l'entreprise, et il est susceptible d'évoluer rapidement. Le mobile est l'un des meilleurs exemples de la consumérisation de l'informatique, car, dans ce domaine plus que dans tout autre, c'est le consommateur qui décide de l'adoption des technologies pour l'utilisation professionnelle.

Les systèmes d'exploitation, tels qu'Android et iOS, et MobileIron, la plateforme de gestion de la mobilité en entreprise, ont mûri et offrent aujourd'hui les contrôles de sécurité multicouches dont les entreprises ont besoin pour réduire le risque de perte des données, que ce soit sur les appareils de l'entreprise ou ceux détenus par les employés.

Grâce à ces contrôles, les organisations peuvent aujourd'hui prendre en charge la nouvelle génération de systèmes d'exploitation et d'appareils mobiles exigée par leurs utilisateurs.

Pour obtenir davantage d'informations sur MobileIron, consultez www.mobileiron.com.