Sécurisation de l'entreprise mobile

Contenu

Rapport de synthèse

La mobilité a toujours été un vecteur de transformation de nos activités professionnelles, de nos communications et de nos interactions sociales. A l'origine orientés consommateur, les avantages de la mobilité ont vite séduit les organisations, qui ont adopté ces solutions pour améliorer la productivité des employés et l'engagement des clients.

Mais ce processus ne s'est pas déroulé si simplement. Les employés ont forcé la main des départements informatiques, à commencer par les dirigeants, pour introduire des périphériques non gérés dans les réseaux d'entreprise. Les clients ont vite privilégié les applications mobiles pour accéder à leurs informations personnelles, médicales et bancaires. Les équipes de sécurité et de mobilité informatique ont dû se mettre à la page. Elles ont dû fournir les éléments nécessaires aux entreprises pour gérer un nouvel ensemble de menaces : la perte/le vol d'appareils, les programmes malveillants ciblant des applications vulnérables et les nouvelles tactiques d'ingénierie sociale augmentent les risques de failles de sécurité et d'utilisation d'appareils mobiles à des fins criminelles et frauduleuses.

La mise en place de contrôles des appareils personnels au niveau de l'entreprise était une première étape nécessaire. Il s'en est suivi une étape de sécurisation des données d'entreprise, car la perte de données constituait un énorme risque pour les entreprises. Au fur et à mesure que les entreprises découvraient comment les employés, partenaires et clients utilisaient les applications mobiles, de nouveaux processus ont dû être mis en place pour sécuriser ces applications contre les dangers. Enfin, il était nécessaire de gérer l'accès mobile aux ressources d'entreprise dans le cadre d'une stratégie de prévention globale contre les failles.

Les produits dédiés répondent à des besoins spécifiques en matière de sécurité mobile et doivent être intégrés ensemble au sein d'une solution cohérente. De nombreuses organisations informatiques font face à ce problème complexe et aux multiples facettes. Une solution globale, intégrée et évolutive devient donc nécessaire.

Ce livre blanc aborde les risques spécifiques associés aux appareils mobiles et les capacités que les entreprises doivent prendre en compte pour élaborer leur feuille de route vers une gestion sécurisée des appareils mobiles dans l'entreprise. Nous allons présenter l'infrastructure IBM Mobile Security Framework, une solution/stratégie complète répondant à toutes les exigences de sécurité mobile concernant les appareils, le contenu développé et transféré entre appareils mobiles, les applications mobiles, les transactions mobiles et les exigences relatives à l'identité mobile et à la gestion des accès. Basé sur la plateforme de veille sur les menaces unique d'IBM, Mobile Security Framework associe automatiquement la sensibilisation contextuelle et du risque dans chaque composant de sécurité mobile, afin d'optimiser la gestion de la mobilité et l'efficacité de la sécurité.

Opportunités et menaces pour l'entreprise mobile

La mobilité est un moteur de changement profond pour les consommateurs en termes d'interaction avec leurs cercles sociaux, d'achat et d'accès aux informations. Les organisations tirent profit de la mobilité dans leurs activités en permettant aux employés d'accéder à des ressources professionnelles telles que les e-mails, les calendriers et les contacts lorsqu'ils sont en déplacement. L'extension de l'accès mobile au contenu d'entreprise, aux applications et aux services améliore la productivité des employés, ce qui entraîne une augmentation de la compétitivité globale et une amélioration du service client. Les clients cherchent à approcher les entreprises via les solutions mobiles, car elles constituent un bon vecteur pour atteindre les objectifs définis. Par exemple, la banque mobile a connu un succès immédiat en offrant à ses clients un accès permanent aux données et transactions financières.

Les employés et les clients partagent une expérience utilisateur efficace et fluide. L'adoption de solutions mobiles par les clients a élevé le niveau d'utilisation des applications par les employés. Cette « consumérisation informatique » est devenue le moteur de l'émergence des programmes BYOD (Bring Your Own Device) et de la recherche d'une meilleure expérience utilisateur en termes d'applications d'entreprise[1].

La mobilité au travail constitue un nouveau modèle, qui ne se limite pas seulement à de nouveaux moyens d'accès aux informations. Voici ses caractéristiques :

- **Les appareils mobiles se déplacent facilement :** les appareils mobiles voyagent rapidement et sont toujours à portée de main[2]. Nous ne pouvons pas nous plier à des modèles rigides d'utilisation dépendant de la localisation ou de l'heure, comme c'était le cas avec les ordinateurs de bureau, voire les ordinateurs portables.
- **Les appareils mobiles ont un modèle d'utilisation flexible :** le cloisonnement traditionnel entre les appareils professionnels et personnels disparaît rapidement. Les utilisateurs veulent effectuer toutes leurs activités quotidiennes sur un seul appareil. Par exemple, les employés souhaitent pouvoir accéder à leurs applications sociales favorites et à leurs documents professionnels en même temps. Les clients souhaitent pouvoir utiliser un smartphone ou une tablette pour leurs opérations bancaires et de bourse en ligne, mais aussi pour prendre rendez-vous chez le médecin, pour jouer et pour consommer du contenu en ligne.
- **Les appareils mobiles sont difficiles à sécuriser :** les entreprises perdent de plus en plus le contrôle sur les terminaux mobiles. Les utilisateurs peuvent mettre en danger la sécurité des appareils en installant des applications malveillantes et en continuant d'utiliser leurs appareils pour effectuer des transactions métier sensibles. Cela est d'autant plus compliqué que les systèmes d'exploitation Android et iOS sont conçus et gérés de manière à minimiser la visibilité et le contrôle de l'état de l'appareil et des risques de sécurité.

Ces caractéristiques mettent les organisations face à des risques nouveaux et plus élevés :

- **Violation des données via des appareils compromis :** les utilisateurs peuvent compromettre la sécurité des appareils en déverrouillant ou en rootant un appareil. Ces appareils compromis deviennent exposés à des programmes malveillants avancés cachés dans des applications (jeux, sécurité, banque) à l'apparence inoffensive. Ces programmes malveillants peuvent falsifier les communications de vos appareils et permettent aux pirates d'y accéder à distance afin de les contrôler[3].
- **Perte de données via des appareils volés :** nombreux sont ceux qui, par expérience, savent à quel point il est facile de perdre ou de se faire voler un appareil mobile. Les photos de nos enfants sont importantes à nos yeux. Mais que dire de la perte d'informations sensibles sur nos clients, nos concurrents ou nos chiffres, qui exposent nos sociétés à des risques de marque, réglementaires et financiers ? Par exemple, la perte de dossiers médicaux stockés sur une tablette pendant des essais cliniques peut enfreindre la norme HIPPA d'un établissement de santé.
- **Fuite de données via un partage non autorisé ou involontaire :** avec le stockage des données sur les appareils mobiles, le partage n'a jamais été aussi facile. Toutefois, les organisations se préoccupent des données d'entreprise et s'investissent beaucoup pour contrôler l'utilisation des données sur les terminaux dédiés. En offrant un contrôle plus limité du partage des données, les appareils mobiles s'exposent à de nouveaux risques métier. Imaginez un employé partageant par erreur une ébauche de dossier AMF via un e-mail public ou postant des documents internes sur un réseau social suite à un conflit avec son employeur.
- **Perte de propriété intellectuelle et attaques au niveau des applications :** les applications mobiles constituent le principal canal de mise à disposition et de consommation de nouvelles fonctionnalités mobiles. Les entreprises investissent énormément pour développer ces applications et les proposer dans des magasins d'applications publics (clients) et professionnels (employés). Toutefois, certaines vulnérabilités logicielles les exposent aux programmes malveillants. Le reverse engineering permet d'extraire la propriété intellectuelle nécessaire à la redistribution d'applications contenant des programmes malveillants. Ces applications malveillantes sont proposées via des magasins d'applications tiers, intégrées à des programmes malveillants ou transmises aux victimes via des SMS[4]. Lors de leur installation, ces applications subtilisent les données d'identification et d'autres données pour prendre le contrôle des comptes.
- **Accès criminel et transactions frauduleuses :** les appareils mobiles prolongent le défi à long terme que constitue l'authentification des clients et des employés. Les criminels subtilisent des données d'identification via des techniques de phishing et des attaques malveillantes. Ils utilisent les appareils mobiles pour accéder à des applications sensibles, car il est plus difficile d'y appliquer des techniques de fingerprinting.[5]. Les entreprises doivent déterminer si l'utilisateur est un vrai employé, un partenaire, un client ou un criminel prétendant être l'une de ces personnes. En ce qui concerne les clients, et de plus en plus les employés, cette authentification doit être la plus discrète possible afin de préserver l'expérience utilisateur.

Le chapitre suivant abordera les capacités nécessaires à la résolution de ce nouvel ensemble de risques.

Approche globale de la sécurité mobile : capacités requises

Les risques liés à la sécurité mobile sont présents à tous les niveaux du cycle de vie de nos expériences mobiles. Ils couvrent les appareils mobiles, le contenu qui s'y trouve, les applications utilisées pour accéder à ce contenu, l'accès mobile au réseau d'entreprise et les transactions initiées depuis les appareils mobiles.

Une approche globale de la sécurité mobile doit permettre de supprimer tous ces risques et de résoudre les interdépendances uniques qui les relient (par exemple, comment les risques sur les appareils impactent les risques sur le contenu et les applications). Nous aborderons ci-dessous les principales capacités requises pour gérer et sécuriser les différents piliers de l'entreprise mobile.

Protection de l'appareil

Le premier impératif consiste à s'occuper de l'appareil mobile. Les entreprises doivent mettre en place des contrôles de base sur les appareils mobiles qui se connectent à leurs réseaux. Les appareils non conformes ne doivent pas accéder à tout ou partie des données et des services d'entreprise. Par exemple :

- **Enregistrement sécurisé des appareils :** permet de s'assurer que seuls les appareils à vocation professionnelle, authentifiés via des données d'identification de l'entreprise et attribués à un utilisateur valide peuvent utiliser le contenu et les services de l'entreprise (par exemple, e-mails).
- **Gestion optimale de la sécurité des appareils :** permet de s'assurer que la capacité à gérer la sécurité des appareils est conforme aux critères définis par l'entreprise. Par exemple, il peut s'agir d'un code d'accès complexe (ou authentification via empreinte digitale), de paramètres de sécurité et de confidentialité au niveau du système d'exploitation et d'un chiffrement des données de l'appareil.

Bien que ces étapes soient des solutions valides pour les appareils des employés, aucune d'entre elles n'est possible sur les appareils des clients. Voilà pourquoi d'autres impératifs (notamment au niveau des applications et des données de contrôle, de l'accès à la gestion et des fraudes) sont nécessaires pour résoudre les risques inhérents aux appareils des clients.

Contenu et collaboration sécurisés

Le deuxième impératif consiste à sécuriser le contenu d'entreprise stocké sur les appareils mobiles des employés. Ce contenu d'entreprise inclut les e-mails professionnels et les pièces jointes qui y sont associées. Il comprend également les données non structurées de référentiels de contenu d'entreprise tels que Sharepoint, Documentum et Filenet[6], ainsi que des services de stockage sur le cloud tels que Dropbox. Une fois disponible sur l'appareil, ce contenu doit être sécurisé contre les expositions non sollicitées.

La sécurité du contenu et de la collaboration s'articule autour des capacités suivantes :

- **Effacement sélectif du contenu d'entreprise :** si un appareil est perdu ou volé, il est essentiel que les entreprises puissent supprimer les paramètres de profil et de contenu professionnel sur ce périphérique. Cela nécessite de pouvoir isoler le contenu professionnel sur l'appareil *(conteneurisation)* afin que le contenu personnel ne soit pas affecté si l'appareil est retrouvé.
- **Partage limité du contenu d'entreprise :** les applications constituent le principal canal d'accès au contenu mobile. En fonction d'une analyse des risques spécifique à l'entreprise, des limitations doivent être appliquées au niveau du partage du contenu professionnel avec les applications extérieures à l'entreprise (messagerie personnelle, réseaux sociaux, etc.). Le contrôle du partage du contenu peut s'appliquer à toutes les données d'entreprise ou à un contexte spécifique.

Contrôle des applications et des données

Le troisième impératif consiste à contrôler les applications et les données mobiles. Pour les utilisateurs, les applications mobiles constituent la principale manière d'accéder au contenu et aux services d'entreprise. Les messageries, les contacts et les calendriers autorisent une communication basique, mais néanmoins sensible, avec les collègues, les partenaires et les clients. Les applications personnalisées et tierces gèrent l'accès aux systèmes CRM et ERP, ainsi que la collaboration sur le contenu à partir de systèmes de gestion des documents. Par conséquent, les applications mobiles représentent une cible de choix pour les criminels et les pirates.

La sécurité des applications comprend les capacités suivantes :

- **Codage sécurisé et détection des vulnérabilités :** comme pour toute application d'entreprise, les développeurs mobiles doivent suivre des méthodologies et des meilleures pratiques de codage[7]. Le code source des applications doit faire l'objet d'un contrôle des vulnérabilités[8], susceptibles d'étendre la surface d'attaque des programmes malveillants, pendant la phase de développement.
  Souvent disponibles uniquement sous forme de fichiers exécutables, les applications tierces doivent elles aussi être contrôlées. L'idéal consiste à résoudre les problèmes avant le passage en production.
- **Renforcement des applications :** les applications placées dans des magasins d'application publics (applications de banque et de commerce en ligne, par exemple) présentent des risques de reverse engineering. Les pirates peuvent extraire le code source de l'application, recompiler l'application avec un nouveau code conçu pour capturer les données d'identification et d'autres informations personnelles, puis redéployer l'application malveillante sur un magasin d'applications tiers. Ce problème est bien réel. Des applications populaires et iOS ont déjà été piratées[9].
  Les entreprises doivent renforcer les applications pour les protéger contre le reverse engineering et ainsi réduire leur exposition aux prises de contrôle de comptes.

Gestion des accès et des fraudes

Le quatrième impératif consiste à gérer l'accès mobile de l'appareil aux ressources d'entreprise, ainsi que la détection des fraudes. L'authentification mobile est une exigence essentielle qui doit permettre de maîtriser la nature volatile des appareils mobiles (localisation, durée d'accès) et de garantir un processus de connexion aussi fluide que possible. Au-delà de l'authentification, notamment pour les clients, l'activité transactionnelle doit être considérée en fonction de l'activité historique de l'utilisateur pour détecter les activités criminelles et frauduleuses.

Cet impératif comprend les capacités suivantes :

- **Authentification basée sur les risques :** l'authentification mobile doit tenir compte du contexte et des risques pour une meilleure fluidité. Des mesures d'authentification renforcées (telles que l'utilisation de mots de passe à usage unique) doivent être prises uniquement lorsque le contexte de l'accès (nouvel appareil, nouvel emplacement, heure de connexion inhabituelle, connexions multiples depuis des emplacements très distants) présente des risques élevés, afin de préserver l'expérience utilisateur.
- **Authentification unique sur les appareils mobiles :** les opérations de connexion sur appareils mobiles sont plus fastidieuses que sur un PC de bureau. Voilà pourquoi les utilisateurs n'auront qu'à se connecter une seule fois au service d'entreprise. Ils pourront ensuite accéder à tous les services pour lesquels ils sont autorisés.
- **Détection des risques de transaction frauduleuse :** dans le contexte d'un compte utilisateur spécifique, l'analyse de transactions entrantes par rapport à l'historique du compte et la présence d'indicateurs de risques de compte (programmes malveillants et phishing) permettent de détecter les accès criminels et de protéger les entreprises et leurs clients contre les prises de contrôle de comptes et les activités frauduleuses.

Une plateforme robuste pour une mobilité d'entreprise sécurisée

Dans les sections précédentes, nous avons présenté les quatre impératifs requis pour assurer une mobilité d'entreprise totalement sécurisée. Toutefois, pour une efficacité maximale et constante, ces impératifs doivent être accompagnés d'une sensibilisation au contexte et aux risques, ainsi que d'une sécurité globale et d'une veille sur la sécurité.

Intégration de la sensibilisation au contexte et aux risques dans l'infrastructure d'entreprise mobile

Il est essentiel d'évaluer le *risque des appareils sous-jacents* et de définir les contrôles appropriés pour les entreprises offrant aux employés un accès mobile au contenu et aux applications d'entreprise. Par exemple, les entreprises peuvent choisir d'interdire la distribution de contenu d'entreprise aux appareils qui présentent des risques élevés, de supprimer du contenu d'appareils devenus non conformes et de limiter l'accès aux ressources d'entreprise en fonction du profil de risque.

L'évaluation des risques d'un appareil repose sur les points suivants :

- **L'appareil a-t-il été déverrouillé ou rooté ?** Les utilisateurs qui souhaitent installer des applications non contrôlées par Apple ou Google peuvent avoir recours à un processus nommé Jailbreak (iOS) ou Rooting (Android) sur leurs appareils. Ce processus développé par les pirates est mis à jour à chaque nouvelle version du système d'exploitation. Il permet aux utilisateurs d'installer n'importe quelle application, mais désactive en même temps le modèle de sécurité de l'appareil et expose fortement ce dernier à des attaques de programmes malveillants. Nous conseillons vivement aux entreprises d'interdire l'accès de ces appareils à leur réseau.
- **L'appareil est-il infecté par un programme malveillant mobile ?** Un appareil est peut-être déjà infecté par un programme malveillant lorsqu'il demande d'accéder au réseau d'entreprise, ou peut le devenir ultérieurement. Les programmes malveillants peuvent falsifier des services critiques tels que les SMS, les contacts et les e-mails et capturer des informations personnelles telles que des données d'identification, les journaux d'appels et les photos. La détection en temps réel de la présence de programmes malveillants est essentielle pour évaluer les risques que présente un appareil et lui appliquer les stratégies d'entreprise appropriées.
- **L'appareil utilise-t-il la dernière version logicielle et tous les correctifs de sécurité ?** Comme sur les autres plateformes d'entreprise, les utilisateurs doivent disposer des derniers correctifs de sécurité (intégrés à la dernière version du système d'exploitation) sur leurs appareils. Pourtant, certains appareils (en particulier Android) ne sont jamais mis à jour ou présentent des vulnérabilités majeures non corrigées.
- **L'appareil est-il utilisé dans un contexte suspicieux ?** L'utilisation suspicieuse d'un appareil dépend du contexte dans lequel il est utilisé. Où et quand l'appareil a-t-il été utilisé ? S'agit-il d'un nouvel appareil ? S'agit-il d'un appareil déjà enregistré ? Par exemple, il peut s'agir d'un accès à un compte depuis l'étranger alors que les accès précédents ne se faisaient que depuis la France.

Une fois les risques détectés et analysés, plusieurs étapes de résolution peuvent être mises en œuvre. Par exemple, un système de gestion de la mobilité d'entreprise peut effacer le contenu d'entreprise des appareils compromis, empêcher la distribution de nouveau contenu et supprimer les applications malveillantes. L'accès aux ressources d'entreprise peut être limité jusqu'à la suppression des risques sur l'appareil. Les applications mobiles peuvent désactiver ou limiter l'accès aux fonctions sensibles en fonction des risques que présente un appareil. La couche de contrôle d'accès peut limiter l'accès aux périphériques vulnérables via une authentification basée sur les risques (l'authentification renforcée n'est utilisée que dans les situations présentant des risques élevés avérés).

En tenant compte du contexte et des risques dans l'infrastructure de sécurité mobile, les organisations peuvent adopter une meilleure approche de résolution des risques inhérents aux solutions mobiles.

Contrôle continu de la sécurité mobile caractérisé par une recherche de pointe et une veille sur les menaces

Les contrôles de sécurité doivent s'adapter constamment aux menaces émergentes. Il en est de même pour les contrôles de sécurité mobile. Par exemple, la logique de détection du jailbreak doit suivre l'évolution des *masqueurs de jailbreak*[10], destinés à dissimuler qu'un appareil est déverrouillé pour ne pas l'inclure dans la catégorie des appareils à risques élevés. De même, les contrôles de comportement et contextuels se démocratisant, les pirates cherchent à imiter au mieux les victimes pour échapper à toute détection.

En règle générale, la viabilité des contrôles de sécurité mobile nécessite des équipes de recherche dédiées et une source fiable de veille globale et en temps réel sur les menaces.

Intégration de la sécurité mobile dans l'environnement de sécurité d'entreprise élargi

Les appareils mobiles constituent un nouveau canal d'accès pour l'entreprise. Les événements de sécurité mobile doivent par conséquent être gérés dans le cadre global de la sécurité d'entreprise. En intégrant les événements de sécurité mobile dans un système de gestion des événements et des informations de sécurité d'entreprise (SIEM), les menaces et vecteurs d'attaques mobiles peuvent être incorporés dans les processus de réponses aux incidents d'entreprise.

IBM Mobile Security Framework

IBM Mobile Security Framework est une solution globale d'IBM qui répond à tous les impératifs de sécurisation de l'entreprise mobile.

Elle comprend des produits de pointe qui répondent spécifiquement aux besoins en matière de sécurité mobile et les intègre pour maximiser l'impact et réduire la rentabilisation.

Nous allons présenter les composants de l'infrastructure par le biais de deux initiatives de mobilité classiques.

Sécurisation de la main-d'œuvre mobile et mise en place d'un programme BYOD (B2E)

Les organisations souhaitent proposer à leurs employés un accès mobile sécurisé aux ressources de l'entreprise. Les programmes BYOD deviennent des éléments essentiels dans les projets de mobilité. Il est donc nécessaire de gérer et sécuriser les périphériques qui échappent au contrôle des départements informatiques. Outre le risque que présente un appareil, le mélange de données personnelles et professionnelles complique la tâche des équipes de mobilité et de sécurité informatique.

Sécurisation de l'appareil de l'employé et du contenu professionnel sensible

IBM Maas360 permet aux clients d'inscrire rapidement leurs appareils et de définir à distance des règles granulaires pour les appareils d'entreprise et les appareils personnels. Ces règles garantissent *un comportement et un enregistrement sécurisés des appareils*..

IBM MaaS360 utilise les technologies de *conteneurisation* et d'*encapsulation d'applications* pour isoler et contrôler les données d'entreprise sur les appareils mobiles. Cela permet un *effacement sélectif* des données d'entreprise sans impact sur les informations personnelles telles que les photos. Pour empêcher les fuites de contenu, MaaS360 propose un environnement de travail distinct composé d'*applications de productivité sécurisées* (e-mail, contacts, calendriers et éditeurs de contenu), ainsi que d'un navigateur et d'une passerelle garantissant une connectivité sécurisée aux réseaux d'entreprise. L'accès aux ressources des entreprises est ainsi contrôlé et le partage de contenu est limité en fonction des risques métier et des règles d'entreprise.

IBM MaaS360 Mobile Threat Management, qui repose sur IBM Security Trusteer, ajoute une fonction de prise en compte des risques unique et permet aux entreprises d'instaurer des règles de façon dynamique en fonction des risques inhérents à l'appareil. Cela est particulièrement important dans le cadre d'un programme BYOD, car les employés peuvent introduire des appareils vulnérables ou compromis dans l'environnement d'entreprise. Par exemple, les entreprises peuvent limiter l'accès des appareils infectés par des programmes malveillants aux applications Web internes ou aux référentiels de contenu afin de réduire les risques d'exposition aux données et de faille réseau.

Sécurisation des applications d'entreprise personnalisées

IBM MobileFirst Platform Foundation (ou Worklight) propose un environnement d'exécution et de développement intégré pour les applications mobiles hybrides et natives. IBM MobileFirst Platform comprend un moteur de sécurité capable de mettre en place des règles spécifiques à l'application pour contrôler son utilisation et des fonctionnalités basées sur les risques sous-jacents aux appareils et à d'autres paramètres de contexte. Cette fonctionnalité s'avère particulièrement utile lorsque les exigences de sécurité mobile sont liées à des applications spécifiques. Elle doit être pondérée en fonction d'une infrastructure plus complète que nous allons présenter dans ce livre blanc. **IBM MobileFirst Platform Application Scanning** apporte à cet environnement une fonctionnalité d'analyse de vulnérabilité du code source. La solution offre un cycle de vie de développement sécurisé et réduit les risques liés aux attaques de programmes malveillants. Les applications tierces sous forme de fichiers exécutables peuvent être analysées via **IBM Security Appscan Mobile Analyzer**, un service de sécurité des applications mobiles dans le cloud. Mobile Analyzer analyse les applications et signale les éventuelles vulnérabilités détectées au niveau du code, telles que les « cross-site scripting » et les cassages de chiffrement. La sécurité informatique peut autoriser ou interdire l'ajout d'applications mobiles sur des magasins d'applications interne en fonction des risques de sécurité

Les organisations peuvent également sensibiliser leurs applications aux risques grâce à Trusteer Mobile SDK Trusteer Mobile SDK est pré-intégré à IBM MobileFirst Platform Foundation et permet de mettre en place des règles de sécurité des applications lorsque les applications s'exécutent sur des appareils compromis ou vulnérables. La même sensibilisation aux risques peut également être intégrée directement à toute application mobile et s'appuyer sur les informations relatives aux risques de l'appareil pour adapter en conséquence la logique métier de l'application. Par exemple, une application d'ERP mobile peut désactiver les approbations de bons de commande sur les appareils présentant des risques élevés.

Contrôle de l'accès des employés aux ressources et au réseau de l'entreprise

Lorsque les employés se connectent aux ressources et au réseau de l'entreprise depuis un appareil mobile, **IBM Security Access Manager (ISAM)** analyse la demande de connexion. Cette solution analyse le contexte sur plusieurs domaines (heure d'accès, localisation de l'appareil, identification de l'appareil et facteurs de risque de l'appareil) pour appliquer des règles de contrôle d'accès à la connexion.

ISAM est intégré à IBM MobileFirst Platform, IBM MaaS360 et Trusteer Mobile Browser pour fournir à son moteur de règles des indications contextuelles et sur les risques spécifiques à l'appareil. Par exemple, il peut empêcher les appareils infectés par des programmes malveillants de se connecter au réseau, lancer l'utilisation de l'*authentification à deux facteurs* en cas d'accès via un nouvel appareil ou un nouvel emplacement ou activer l'utilisation d'un *navigateur sécurisé* pour accéder à des ressources spécifiques.

En outre, ISAM s'intègre à IBM MaaS360 pour offrir une *authentification unique* depuis les appareils mobiles dans les applications d'entreprise.

Sécurisation des transactions mobiles des clients et des partenaires (B2C et B2P)

La sécurisation des clients mobiles présente des défis autres que le simple traitement de la sécurité de la main-d'œuvre mobile. Les entreprises n'ont aucun contrôle sur les appareils des clients et des partenaires mobiles (« appareils non gérés ») et ces utilisateurs ne sont généralement pas enclins à autoriser un tel contrôle. Les entreprises doivent par conséquent partir du principe que les appareils non gérés peuvent être compromis et qu'aucun contenu d'entreprise sensible ne doit être déployé dessus. Les points clés à sécuriser sont les applications avec lesquelles le client interagit, ainsi que les informations de connexion et les transactions du client.

Sécurisation des applications externes

Les entreprises approchent leurs clients et partenaires via des applications mobiles disponibles publiquement. La vulnérabilité des applications mobiles doit être contrôlée, soit pendant le développement du code source, soit lors de leur déploiement sous forme de fichiers exécutables, comme précédemment abordé. Toutefois, ces applications étant disponibles publiquement, les entreprises doivent également tenir compte du renforcement des applications via des solutions telles qu'Arxan Application Protection for IBM Solutions. Le *renforcement des applications* empêche les pirates de procéder au reverse engineering des applications mobiles, d'y insérer du code malveillant et de les redéployer sur des magasins d'applications tiers pour leurrer les clients insouciants. Une fois installées et lancées, ces applications capturent les données d'identification des clients ou démarrent des opérations frauduleuses.

De plus, la sécurité des appareils non gérés étant souvent faible, les organisations peuvent intégrer Trusteer Mobile SDK dans leurs applications externes pour évaluer de façon dynamique les risques des appareils sous-jacents. Par exemple, les applications de banque mobile peuvent désactiver les transactions sur les appareils vulnérables.

Détection d'attaques sur différents canaux : accès criminel et transactions frauduleuses

Les clients utilisent des applications mobiles et des navigateurs pour accéder à des services tels que les banques et les commerces en ligne. Souvent, les données d'identification des clients sont exposées à des risques de phishing et d'attaques de programmes malveillants sur les appareils mobiles ou les ordinateurs personnels. Les criminels utilisent ces données d'identification pour prendre le contrôle des comptes des clients sur leurs appareils mobiles. Les équipes en charge de la sécurité et de la gestion des fraudes ont la lourde responsabilité d'identifier ce genre d'incidents. **IBM Security Trusteer Pinpoint Criminal Detection** met en corrélation de nombreux facteurs de risques associés aux connexions aux comptes et aux transactions pour repérer précisément les accès à risque élevé. Parmi les facteurs de risques, la solution tient compte de l'identification forte des appareils, des modèles d'usage des appareils et des précédentes attaques par programmes malveillants ou phishing sur le compte (via ordinateur de bureau, ordinateur portable ou appareil mobile). En se basant sur des données propriétaires, dynamiques et en temps réel sur les risques, elle répond rapidement aux activités criminelles et minimise les faux positifs.

Une base de sécurité mobile solide

Notre base pour la sécurité mobile améliore la puissance et l'efficacité de notre solution globale.

Prise en compte des risques : Trusteer Mobile SDK

Trusteer Mobile SDK détecte précisément les appareils compromis et vulnérables, y compris :

- **les appareils rootés et déverrouillés**, notamment ceux disposant d'un dispositif de masquage du déverrouillage
- **les appareils infectés par un programme malveillant**, menaces financières et menaces d'entreprise en générale
- **les systèmes d'exploitation mobiles obsolètes** et les correctifs de sécurité manquants

En outre, Trusteer Mobile SDK offre un ID d'*appareil fort* pour identifier spécifiquement chaque appareil.

Trusteer Mobile SDK est pré-intégré à plusieurs offres IBM pour évaluer les risques et informer de la mise en place de règles plus adaptées :

- **IBM MaaS360 Mobile Threat Management :** cette intégration permet aux organisations de mettre en place des actions de limitation spécifiques, telles que la suppression de contenu d'entreprise des appareils compromis par des programmes malveillants, jusqu'à l'élimination du risque inhérent à l'appareil.
- **IBM MobileFirst Platform (Worklight) :** l'intégration à la plateforme d'exécution et de développement des applications permet aux développeurs d'incorporer l'évaluation des risques directement dans leurs applications, sans aucun codage. Le moteur d'exécution des applications met en place des règles de sécurité pour restreindre l'utilisation des applications en fonction du type et de la portée des risques sous-jacents à l'appareil.
- **IBM Security Access Manager :** ISAM utilise les attributs de risques inhérents à l'appareil relayés par MobileFirst Platform, MaaS360 Mobile Threat Management et Trusteer Mobile Browser. Son moteur basé sur des règles permet de mettre en place un contrôle de l'accès aux ressources d'entreprise en fonction de ces attributs dynamiques en temps réel.

En plus de ces intégrations natives, les développeurs d'applications peuvent intégrer Trusteer Mobile SDK dans une application. En appelant SDK, les risques inhérents aux appareils sont détectés et retournés en temps réel au code de l'application. Par exemple, les applications de banque en ligne peuvent limiter les transferts d'argent en fonction des risques sous-jacents à l'appareil, tels qu'une infection par programme malveillant, puis associer un ID d'appareil fort à chaque transaction générée via l'application.

Veille globale sur les menaces : X-Force et Trusteer

Le nombre de menaces ne cesse de croître, car les criminels et les pirates recherchent de nouvelles manières de casser et déjouer les contrôles de sécurité. IBM utilise les opérations de recherche mondiale pour garder une trace du paysage des menaces et adapter les défenses de sécurité grâce aux dernières techniques et contre-mesures.

IBM suit l'évolution des programmes malveillants mobiles, les nouvelles techniques visant à rooter et déverrouiller les appareils et les nouvelles tactiques employées par les criminels pour pénétrer les comptes des clients et des employés. Les résultats de ces recherches donnent naissance à des règles et des améliorations du code sur les contrôles de sécurité mobile pour maintenir une détection et une prévention précises des menaces mobiles[11].

Informations sur la sécurité et gestion des événements : IBM Security QRADAR

Les différents produits de sécurité mobile sont intégrés, le cas échéant, à IBM Security QRADAR. IBM Security QRADAR consolide les événements liés à la sécurité et les met en corrélation dans toute l'entreprise. En intégrant les événements liés à la sécurité mobile, des mesures d'entreprise appropriées peuvent être définies pour répondre aux attaques sophistiquées lancées via le canal mobile.

Chemin vers une sécurité mobile solide : appel à l'action

Fin 2014, IBM a lancé une enquête visant à mettre en lumière les capacités mises en œuvre par les entreprises en fonction des impératifs d'IBM Security Framework. Nous avons également étudié les plans à court et moyen termes pour étendre ces capacités dans ce que nous appelons le « chemin vers une sécurité mobile solide ».

Nous en avons conclu que les entreprises étaient « à la moitié du chemin ». Naturellement, les entreprises se concentrent toujours sur l'impératif de base qu'est la sécurité du contenu et des appareils. Les entreprises sont toujours exposées à des risques de perte de données suite au vol d'un appareil. L'Enterprise Mobility Management (EMM) permet de répondre à ce cas de figure. Nous espérons que dans un avenir proche, pratiquement toutes les entreprises disposeront de cette solution pour s'assurer que les appareils mobiles soient conformes à leurs règles avant d'autoriser l'accès aux ressources de l'entreprise. De plus, le contenu d'entreprise peut être effacé de façon sélective ou protégé en cas de perte ou de vol d'appareil.

Le prochain grand défi des entreprises concerne le développement d'applications d'entreprise sécurisées. Le besoin d'établir un cycle de vie du développement d'application sécurisé puise ses origines dans le développement d'un Internet sécurisé.
Certaines personnes interrogées utilisent les outils d'analyse de vulnérabilité sur le code source de leur application, tandis que d'autres, moins nombreux, l'utilisent sur les fichiers binaires (applications tierces ou publiques). L'absence de vulnérabilités dans ces applications professionnelles est vitale pour toute entreprise souhaitant tirer profit de la mobilité tout en réduisant son exposition aux programmes malveillants et aux autres attaques.

Enfin, la gestion de l'accès et des risques liés aux transactions frauduleuses est une fonctionnalité émergente. Les risques de transaction frauduleuse concernent toutes les interactions entre les appareils mobiles et les systèmes : accès au réseau, connexion et accès aux données et services. Pour protéger efficacement les transactions, les entreprises devront tenir compte des risques sous-jacents aux appareils et des usages d'accès des utilisateurs pour déterminer l'exposition métier associée aux interactions et sessions spécifiques. Cela permet de détecter les prises de contrôle de comptes et les transactions frauduleuses avant que les données d'entreprise et les ressources des clients ne soient exposées.

IBM Mobile Security Framework propose une solution globale et une feuille de route complète de sécurisation de votre entreprise mobile. Vous pouvez maintenant aider vos employés et clients à tirer profit de la mobilité tout en réduisant les risques, les coûts et la complexité.

Pour plus d'informations

Pour en savoir plus sur la sécurisation de l'entreprise mobile, contactez votre représentant ou partenaire commercial IBM ou visitez le site Web suivant : http://www.ibm.com/mobilefirst/fr/fr/mobile-security.html

De plus, IBM Global Financing peut vous aider à financer l'acquisition des solutions informatiques nécessaires à votre société, de la façon la plus économique et stratégique possible. Pour les clients sérieux, nous pouvons personnaliser une solution de financement informatique adaptée à leurs objectifs métier, garantir une gestion financière efficace et améliorer leur coût total de propriété. IBM Global Financing est le choix à faire pour financer vos investissements informatiques stratégiques et faire progresser votre activité. Pour plus d'informations, consultez le site :

ibm.com/financing

Sécurité
17 avenue de l'Europe
92275 Bois Colombes Cedex

Imprimé en France
Mars 2016

Recyclable

[1] L'alliance IBM/Apple en termes d'entreprise mobile répond aux attentes élevées en matière de conception et de distribution des applications mobiles verticales.

[2] https://www.cmocouncil.org/facts-stats-categories.php?view=all&category=mobile-marketing

[3] https://www.lacoon.com/lacoon-discovers-xsser-mrat- first-advanced-ios-trojan/

[4] https://www.fireeye.com/blog/threat-research/2015/02/ios_masque_attackre.html

[5] http://securityintelligence.com/can-you-trust-it-mobile-authentication- must-become-context-and-risk-aware

[6] Pour plus d'informations sur les solutions de gestion de contenu d'entreprise IBM, consultez le site http://www-03.ibm.com/software/products/en/category/enterprise- content-management

[7] https://www.owasp.org/index.php/OWASP_Mobile_Security_ Project#tab=Home

[8] Gartner Hype Cycle for Enterprise Mobile Security 2014 mentionne ce qui suit : « …La démocratisation des appareils mobiles dans l'entreprise rend les tests de sécurité et la protection des applications mobiles et des données obligatoires contre les attaques »

[9] https://www.arxan.com/arxan-annual-report-state-of-mobile-app-security-reveals-an-increase-in-app-hacks-for-top-100-mobile-apps/

[10] http://lifehacker.com/5864300/xcon-unblocks-iphone-apps-with- jailbreak-detection

[11] IBM X-Force publie un rapport annuel résumant les développements clés dans le paysage mondial des cyber-menaces. Pour accéder au dernier rapport, consultez le site http://www-03.ibm.com/security/xforce/#quarterly

WGW03121-FRFR-00