IBM Security
Livre blanc

Sécurité des données mobiles

Protéger les données confidentielles tout en préservant la productivité des utilisateurs

IBM

Sécurité des données mobiles : le juste équilibre

Les termes « prévention contre les fuites de données » et « conteneurisation » commencent à dominer les discussions sur la gestion de la mobilité. Au cours des dernières années, de grandes avancées ont été réalisées pour fournir des outils et des solutions incluant des fonctions de gestion et de sécurité dédiées aux dispositifs mobiles, aussi bien pour des appareils appartenant aux entreprises ou à leurs employés.

Même si ces solutions répondent généralement à des besoins de sécurité mobile, elles n'ont pas les fonctions sophistiquées habituellement installées sur les ordinateurs portables et les déploiements de réseaux distribués. Plus spécifiquement, elles sont dépourvues de contrôles de fuites de données, couramment intégrées aux solutions de gestion des ordinateurs portables.

Le principe de précaution exige que votre solution de gestion des applications mobiles (MDM) intègre des contrôles de sécurité supplémentaires plus solides, afin de sécuriser et de protéger les données sensibles contre la diffusion à des tiers non autorisés, de manière intentionnelle ou par inadvertance.

A vous de trouver l'équilibre entre des risques tolérables pour la sécurité des données confidentielles et fournir une expérience utilisateur simple et productive.

Définissez vos objectifs

Au cours de votre recherche de technologie, vous découvrirez différentes approches. Ces approches présentent toutes des avantages et des inconvénients, et il vous faut donc commencer par définir vos objectifs. Pour définir vos objectifs et votre approche, vous devez trouver un équilibre satisfaisant entre les risques tolérables pour la sécurité des données confidentielles et une expérience utilisateur simple et productive. N'oubliez pas de tenir compte des éléments suivants :

Bloquer l'utilisateur – Le mot de passe et le chiffrement de l'appareil ne peuvent pas empêcher un utilisateur autorisé de copier des données. Ce contrôle appartient à la politique de protection contre la fuite des données. Votre entreprise a peut-être déjà réalisé des investissements considérables pour contrôler la circulation des données confidentielles à l'extérieur des périmètres logiciels et matériels qui protègent les ordinateurs de bureau et portables. Si tel est le cas, optez pour des capacités qui étendent la protection contre la fuite des données à vos déploiements mobiles. Votre politique et vos objectifs doivent être cohérents pour tous les types d'appareils utilisés dans votre entreprise.

Bloquer l'utilisateur externe - La communauté des fournisseurs MDM a fait un travail exceptionnel en proposant des outils de protection des données pour appareils mobiles. La mise en place d'un mot de passe, le chiffrement et l'effacement des appareils représentent 90 % de la bataille. Toutefois, il reste des défis importants à relever, notamment en ce qui concerne l'application et la vérification systématiques et fiables de ces contrôles, et en particulier sur les nombreuses versions de la plateforme Android. La diversité des appareils et par conséquent la fragmentation de la solution implique que tous les appareils ne peuvent pas bénéficier d'un niveau de sécurité raisonnable.

Support élargi et flexible des programmes BYOD - La diversité des appareils est une contrainte énorme pour votre approche et votre stratégie. Après tout, le BYOD (Bring Your Own Device) signifie seulement : apporter votre dispositif personnel, et pas : *apporter votre dispositif personnel approuvé par le service informatique*, ce qui irait à l'encontre de l'esprit de tout programme BYOD. Même si un programme et un processus de certification des appareils pourraient apporter une certaine structure, une politique BYOD entièrement ouverte devrait être secondée par un support technologique capable de garantir la sécurité minimale des données.

L'administration de deux environnements utilisateur indépendants permet de séparer les données / utilisations professionnelles et personnelles sur un même appareil mobile.

Environnements indépendants - C'est ici que le débat limité aux seules questions de sécurité dévie pour se transformer en discussion sur la fonctionnalité et la volonté de mettre en place un programme BYOD flexible. De nombreuses entreprises ne voient pas la nécessité de mettre en place une politique de protection contre les fuites de données. Elles souhaitent simplement ne pas toucher aux données personnelles des utilisateurs et contrôler uniquement les données professionnelles. Lorsque vos objectifs sont définis, une solution basée sur deux environnements indépendants peut être la plus appropriée pour votre entreprise. Fondamentalement, des environnements indépendants permettent de séparer les deux dimensions professionnelles et privées sur un appareil mobile, d'isoler les données et leurs utilisations dans leur dimension respective.

Autres considérations - Ces solutions ne sont pas gratuites. Assurez-vous que votre programme BYOD sera en mesure d'évoluer, de rester fiable et de ne pas dépasser un certain plafond financier. Vous devez tenir compte de l'expérience utilisateur et implémenter une solution qui sera acceptée et adoptée par vos utilisateurs. La vieille autocratie informatique n'est plus et la démocratie fait aussi partie de notre vie technologique.

Choisissez votre approche

Vos objectifs étant définis, voyons les approches disponibles.

Conteneurisation - Le terme « conteneurisation » semble être le terme le plus utilisé pour décrire les solutions qui isolent les applications et les données professionnelles. Le terme « sandbox » (bac ou bac à sable) est aussi fréquemment utilisé. Vous pouvez aussi entendre parler « d'environnements indépendants » pour décrire ce type de solutions. Mais ils sont le résultat ou l'objectif de la solution, dans le sens où une solution de conteneurisation sert à mettre en œuvre des environnements indépendants.

Dans cette approche, une zone complètement séparée ou « bac à sable » est réservée à des activités spécifiques, où la circulation des données est strictement limitée au périmètre du bac. Etant donné que toutes les activités professionnelles sont effectuées dans un bac spécifique, l'utilisateur ne peut pas utiliser le client de messagerie natif, mais uniquement la messagerie, le calendrier et les contacts disponibles dans le conteneur. Ce dispositif peut entraîner certains mécontentements mais, lorsqu'il est implémenté correctement, il peut procurer une expérience utilisateur transparente. Il est important d'expliquer aux utilisateurs le rôle important de la solution au regard des objectifs de sécurité de l'entreprise.

Extraction - Cette solution intercepte le flux des courriers électroniques, extrait les contenus pertinents (pièces-jointes, texte, etc.) et les transfère dans une application séparée qui autorise une consultation / manipulation contrôlée des données. En ce qui concerne la messagerie, l'utilisateur se sert normalement du client natif jusqu'à ce qu'il ait besoin d'accéder à un élément qui a été extrait du flux des e-mails. Le contenu qui a été extrait peut être stocké sur le serveur d'extraction ou sur un terminal mobile configuré pour autoriser uniquement son ouverture dans une application sécurisée.

Une solution d'extraction peut procurer une expérience utilisateur disjointe. L'utilisateur reçoit un e-mail sans texte ni pièce jointe (c'est pourquoi de nombreuses solutions ne touchent pas au texte) et il doit ouvrir une autre application pour accéder aux éléments extraits de manière sécurisée.

Virtualisation - La virtualisation est une technologie qui permet à un logiciel appelé « hyperviseur » de créer une « machine virtuelle » logicielle sur un appareil mobile spécifique (au lieu d'un serveur distant). Dans cette solution, l'appareil virtuel est totalement contrôlé et géré par l'entreprise. Toutes les applications et les données de l'entreprise résident dans la machine virtuelle exécutée sur l'appareil mobile. La circulation des données entre cet appareil physique et la machine virtuelle est strictement contrôlée. Cette solution reproduit fondamentalement la même infrastructure de bureau virtuelle (VDI) exécutée sur des ordinateurs fixes et portables, et pose les mêmes défis de déploiement et de gestion.

Si votre entreprise souhaite empêcher que des utilisateurs autorisés puissent diffuser des données confidentielles à partir de dispositifs mobiles, chacune de ces solutions : conteneurisation, virtualisation ou extraction des pièces jointes leur apportera une bonne efficacité.

Cette technologie est prometteuse puisque toutes les fonctions matérielles et logicielles des dispositifs mobiles peuvent être virtualisées et contrôlées, incluant même la connectivité réseau et les fonctions matérielles. Par exemple, la carte SIM peut être virtualisée et reparamétrée virtuellement lors des changements de réseaux (ce qui ne serait pas du goût des opérateurs). Dans la pratique, tant que les appareils mobiles ne prennent pas en charge la virtualisation sur le matériel comme c'est le cas avec Intel VT et AMD-V sur des ordinateurs de bureau, l'adoption en masse de cette technologie semble encore lointaine, et sur iOS en particulier.

Aucun des éléments ci-dessus - Après réflexion, de nombreuses entreprises peuvent aboutir à cette conclusion. Si vous ne travaillez pas dans les secteurs de la santé ou des services financiers, que vous n'avez pas d'obligation de conformité PCI ou HIPAA, ou si vous avez défini vos besoins spécifiques en matière de sécurité et mis en œuvre une stratégie intelligente de gestion des applications et des dispositifs, augmenter les coûts et la complexité d'utilisation, pour vos utilisateurs et votre service informatique, n'est pas forcément justifiable.

Un choix basé sur les priorités

Hiérarchisons maintenant toutes ces informations en fonction de vos priorités.

Priorité – la menace interne : Si votre entreprise souhaite empêcher que des utilisateurs autorisés puissent diffuser des données confidentielles à partir de dispositifs mobiles, chacune de ces solutions : conteneurisation, virtualisation ou extraction des pièces jointes leur apportera une bonne efficacité. Toutes ces solutions sécurisent le texte et les pièces jointes, mais les expériences d'utilisation qu'elles procurent sont fondamentalement différentes, comme indiqué ci-dessus. (Pour l'extraction, prenez un produit capable d'extraire aussi bien les textes que les pièces jointes.) Si vous n'avez aucune flexibilité ou tolérance applicable aux fuites de données par e-mail, la conteneurisation a l'avantage d'améliorer l'expérience utilisateur et elle est relativement moins complexe à configurer et à gérer. En théorie, la virtualisation convient parfaitement à la lutte contre les menaces internes mais son implémentation et sa gestion peuvent s'avérer complexes.

Priorité – la menace extérieure : La menace extérieure est assez simple à endiguer en adoptant une approche raisonnable de la gestion des dispositifs autorisés à se connecter à la messagerie. Avec votre solution MDM, (en supposant que vous en avez une) vous pouvez limiter les connexions aux seuls appareils connus et approuvés, intégrés à une politique de mot de passe, protégés par chiffrement, et effacement des données à distance. Dans ce cas, les fuites de données et les dommages liés aux pertes ou vols de dispositifs seront limités, voire inexistants. Si la protection contre les menaces extérieures est votre priorité, vous pouvez ainsi éviter les coûts et la complexité supplémentaires des solutions dédiées à la fuite de données. En règle générale, éliminer les risques de fuite de données sur les dispositifs mobiles est seulement efficace si les autres vulnérabilités sont également corrigées.

Une solution de conteneurisation, qui permet de créer une zone sécurisée dédiée aux données de l'entreprise sur des dispositifs non sécurisés, peut être une alternative plus avantageuse que la mise à niveau des appareils non certifiés et non adaptés inscrits au programme par le personnel.

Priorité – support du programme BYOD : Pour mettre en œuvre un programme BYOD, la prudence vous invite à utiliser un processus de certification des appareils et à créer une liste des appareils autorisés capable de supporter un niveau minimal de sécurité. Si vous avec un tel programme, vous réaliserez rapidement qu'il existe de grandes différences de support des fonctions essentielles de sécurité entre les diverses versions d'Android. Dans le meilleur des mondes, le BYOD serait exactement calqué sur ce modèle et s'adapterait à un large éventail d'appareils.

Une solution de conteneurisation, qui permet de créer une zone sécurisée dédiée aux données de l'entreprise sur des dispositifs non sécurisés, peut être une alternative plus avantageuse que la mise à niveau des appareils non certifiés et non adaptés inscrits au programme par le personnel. Les solutions d'extraction offrent des avantages similaires, si elles sont configurées pour extraire et sécuriser le texte et les pièces jointes des courriers électroniques. La virtualisation ne permet pas de supporter un large éventail d'appareils BYOD car le nombre de dispositifs capables d'exécuter un hyperviseur est limité.

Priorité – les environnements indépendants : Une autre bonne raison pour choisir une solution de conteneurisation ou d'extraction ne concerne pas seulement la sécurité. Compte tenu de la prolifération des appareils personnels dans l'entreprise, il sera toujours inévitable que des données d'entreprise se mêlent à des données personnelles malgré tous les efforts pour l'éviter. Opter pour une approche plus douce de la gestion des données d'entreprise sur ces appareils constitue aussi une possibilité intéressante.

Plutôt que d'avertir les utilisateurs que leur appareil sera entièrement effacé s'il est perdu ou volé, ou s'ils quittent l'entreprise, vous pouvez leur proposer une solution d'extraction ou de conteneurisation. Ainsi, la suppression des informations se cantonnera aux données d'entreprise et n'affectera pas les données personnelles que l'utilisateur pourrait avoir enregistrées sur l'appareil. Dans ce cas de figure, la conteneurisation s'avère la plus efficace et, à choisir entre le bâton et la carotte, il pourrait bien s'agir de la meilleure carotte de la botte. Les utilisateurs se voient attribuer un profil professionnel et sont satisfaits car ils savent que le service informatique ne touchera pas à leurs données privées.

L'approche de l'extraction ne convient pas aussi bien à la mise en place d'environnements indépendants car elle n'implique pas une séparation assez nette entre les données d'entreprise et les données personnelles. En effet, le client de messagerie électronique est utilisé aussi bien pour les activités privées que pour les activités professionnelles.

La virtualisation est également prometteuse dans ce domaine. Toutefois, elle est limitée à un nombre tellement restreint d'appareils qu'aucune alternative pratique n'existe à ce niveau pour le BOYD.

Prenez vos précautions avant de vous lancer

Pour résumer, vous devez prendre vos précautions avant de vous lancer. Définissez des objectifs, écoutez vos utilisateurs, étudiez les technologies disponibles et leur impact potentiel sur votre environnement et sur les employés. Plus important encore, informez-vous avant d'écouter l'argumentaire du fournisseur. Lorsque vous communiquez avec des fournisseurs, et que vous évaluez leurs offres, recherchez des solutions capables de s'adapter à l'évolution rapide de l'environnement mobile et réévaluez régulièrement vos objectifs.

A propos d'IBM MaaS360

IBM MaaS360 est une plateforme de gestion de la mobilité d'entreprise qui soutient la productivité et assure la protection des données en fonction des habitudes de travail des utilisateurs. Des milliers d'entreprises font confiance au MaaS360 comme fondation de leurs initiatives mobiles. MaaS360 offre une gestion intégrale, avec de puissants contrôles de sécurité pour tous les utilisateurs, les appareils, les applis et les contenus afin de supporter tous les déploiements mobiles. Pour plus d'informations sur IBM MaaS360 et pour commencer un essai gratuit de 30 jours, rendez-vous sur www.ibm.com/maas360

A propos d'IBM Security

La plateforme de sécurité IBM fournit les données de sécurité nécessaires pour aider les entreprises à gérer leurs utilisateurs, leurs données, leurs applis et leur infrastructure de manière globale. IBM propose des solutions de gestion des identités et des accès, de gestion des données et des événements relatifs à la sécurité, la sécurité des bases de données, le développement d'applis, la gestion des risques, la gestion des terminaux, la protection de dernière génération contre les intrusions, etc. IBM possède l'un des plus grands services du monde en matière de recherche, de développement et de mise en œuvre de services de sécurité. Pour en savoir plus, visitez le site : www.ibm.com/security

Compagnie IBM France
17, avenue de l'Europe
92275 BOIS COLOMBES CEDEX

Produit aux Etats-Unis
Mars 2016

WGW03113-FRFR-01