Sécurité IBM
Livre blanc

Lorsque l'entreprise se centre sur l'appli, l'appli est l'entreprise

Volume III : Se protéger contre les dangers de l'application

IBM

Introduction

Leader de l'EMM (Enterprise Mobile Management), IBM Security présente le Volume III d'une série en trois parties qui étudie l'application de l'entreprise et le rôle clé que joue le service informatique à ce niveau.

Dans ce volume, vous découvrirez les principales menaces de sécurité induites par la mobilité dans l'entreprise et vous apprendrez comment les éliminer de vos activités basées sur des applis.

Découvrez les implications techniques et pratiques à prendre en compte pour soutenir et protéger correctement votre entreprise lorsque vous élaborez et implémentez des activités centrées sur des applis.

Se protéger contre les dangers de l'application

Comme abordé dans les Volumes I et II (notes 4 et 5) de cette série, les applis mobiles transforment profondément le fonctionnement des entreprises. Pour tirer pleinement profit de l'application, le service informatique doit élaborer une stratégie efficace qui englobe la découverte, l'évolutivité, la durabilité et bien sûr la sécurité.

Les applis sont de formidables outils pour améliorer la productivité et engager les clients, mais le service informatique est confronté à un travail colossal pour sécuriser les activités basées sur les applis. IDC prévoit que le nombre d'applis d'entreprise optimisées pour la mobilité quadruplera d'ici 2016, poussé par la compétitivité et l'évolution rapide des technologies qui supportent l'accélération et la sécurisation de l'« application ».[1] La sécurité n'est pas uniquement une étape applicable lorsqu'une appli est prête à être déployée : il s'agit d'un point qui doit être pris en compte et implémenté à chaque étape de l'application.

Dans leur site de stockage ou en mouvement, les données liées aux applis sont constamment menacées

Les applis d'entreprise sont particulièrement exposées aux fuites de données sensibles car elles sont directement connectées aux systèmes et fichiers de la société. Dans leur espace de stockage ou en mouvement, les données des applis doivent être sécurisées dès les étapes de conception et de développement.

Comme indiqué en détails dans le livre blanc « *Meilleures pratiques pour la gestion du cycle de vie des applis mobiles* »,[2] le service informatique doit supporter chaque étape de la planification et du développement des applis afin de s'assurer qu'elles seront sécurisées tout au long de leur cycle de vie. Voici un aperçu rapide des « indispensables » :

Pour les données dans leur espace de stockage :

• **Authentification :** Outre l'authentification des appareils mobiles, vous devez également intégrer l'authentification dans les applis. En effet, l'accès à certaines applis et à leurs données doit aussi être limité aux seuls utilisateurs autorisés, en cas de diffusion accidentelle à un utilisateur non autorisé.

- **Authentification unique :** Lors de la conception des applis, le service informatique peut permettre aux utilisateurs d'accéder à toutes leurs applis d'entreprise autorisées grâce un mot de passe individuel unique (une fonction souhaitée et attendue par la plupart des utilisateurs). Cette fonction supporte une approche mieux centrée sur l'utilisateur et intégrée à la conception des applis mobiles sur une plateforme de développement.
- **Protection contre la perte des données (DLP) avec deux environnements indépendants :** Les développeurs et les administrateurs MDM peuvent utiliser un conteneur protégé tel que IBM® MaaS360® Trusted Workplace, pour éviter les fuites d'informations, le mélange de données d'entreprise et personnelles, pour mieux protéger la vie privée des employés. IBM MaaS360 Trusted WorkPlace permet de désactiver le copier/coller des données à l'extérieur du conteneur (et d'avertir le service informatique lorsqu'une telle manœuvre est tentée). Grâce aux contrôles d'ouverture, les utilisateurs ne peuvent utiliser aucune appli en dehors des applis sécurisées de l'entreprise et situées dans le conteneur pour ouvrir des documents et des fichiers.

Pour les données en mouvement :

La protection des données en mouvement réduit considérablement les risques d'attaque de l'homme du milieu (HDM) lorsque des informations transitent entre des serveurs d'entreprise et un dispositif mobile. Si vous utilisez IBM® MaaS360® Gateway Suite, cette opération peut être réalisée indépendamment de toute infrastructure VPN. Les développeurs d'applis peuvent également définir des politiques pour bloquer l'ouverture d'une appli sur un appareil non conforme aux fonctions de surveillance automatique.

Ces mesures de sécurité semblent très efficaces, mais ne compliqueront-elles pas le processus de développement ?

Au sein de la communauté de la sécurité mobile, les discussions vont bon train sur la meilleure solution à adopter : encapsulation ou conteneurisation des applis. Chaque approche induit une expérience développeur, administrateur et utilisateur différente. L'encapsulation d'applis ne nécessite aucune modification du code, contrairement à la conteneurisation basée sur le code, évidemment. Toutefois, la conteneurisation offre un contrôle plus granulaire que l'encapsulation. Une récente étude de Forrester[3] indique que l'encapsulation d'applis constitue un choix légèrement plus judicieux, mais la meilleure technologie à adopter dépend surtout des priorités et des ressources de chaque entreprise. « IBM® MaaS360® Productivity Suite propose les deux options aux développeurs et aux administrateurs de la mobilité :

- **Encapsulation d'applis :** Intégrée à la plateforme Mobile Application Management, IBM® MaaS360® Mobile Application Security affiche les workflows dans une fenêtre unique et vo us permet de cocher des cases pour activer automatiquement des contrôles de sécurité lorsque vous chargez et déployez vos applis.
- **Conteneurisation :** Le kit de développement logiciel (SDK) MaaS360 Mobile Application Security permet aux développeurs d'intégrer une sécurité de niveau entreprise directement dans le code de l'appli. Grâce à ce kit, ils peuvent également ajouter rapidement des fonctions des conteneurisation aussi bien sur les applis privées que publiques.

Jusqu'au déploiement… et après

Maintenant que votre appli a été développée avec toute la sécurité nécessaire, elle est prête à être déployée sur les appareils des utilisateurs. L'une des méthodes les plus simples et les plus sécurisées de distribution et de contrôle est d'utiliser un magasin d'applis d'entreprise. Le catalogue IBM® MaaS360 permet aux administrateurs de gérer aussi bien les applis publiques que les applis d'entreprise internes.

La sécurisation des applis ne s'arrête pas au déploiement. Les meilleures pratiques « passives » de sécurisation des applis vous permettent d'assurer la gestion et la protection (avec un effort très limité de votre part) via :

- La mise sur listes blanche et noire des applis
- La configuration de la sécurité et des restrictions
- La mise en œuvre automatique des actions en cas de non conformité (avertissement, blocage de l'appareil, effacement sélectif ou complet de l'appareil)
- La surveillance automatique des dispositifs débridés, ancrés et non conformes
- Visibilité continue du statut de conformité pour tous les appareils
- Historique de la sécurité et de la conformité

L'applification de votre entreprise

Comme abordé dans les Volumes I et II (notes 4 et 5), les entreprises ne peuvent tout simplement pas se permettre d'ignorer la sécurité lors de leur applification. Et vous êtes à la tête de cet effort. L'entreprise a les yeux rivés sur vous en attendant que vous lui proposiez une stratégie et un programme qui améliorent la productivité des employés, l'engagement auprès des clients et le chiffre d'affaires, tout en les préservant des logiciels malveillants, des fuites de données et des autres menaces importantes.

Cependant, vous n'avez pas à le faire seul. En conjonction avec d'autres solutions du portefeuille IBM MobileFirst, MaaS360 peut guider et supporter votre applification. Contactez IBM dès aujourd'hui pour découvrir comment tirer le meilleur parti de l'environnement d'applis mobiles de votre entreprise.

Prêt pour l'applification de votre entreprise ? Consultez les autres parties de cette série :

- **Volume I : L'applification de l'entreprise.**[4] Explorez l'applification de l'entreprise et le rôle crucial du service informatique pour améliorer la productivité et la collaboration des employés, l'engagement client et la croissance de l'entreprise grâce à des applis pertinentes.
- **Volume II : Les quatre éléments d'une solide stratégie pour applis mobiles.**[5] Collaborez avec vos utilisateurs pour développer une stratégie d'applis adaptée à votre entreprise.

Ressources connexes

- Mobilisez vos applis et contenus d'entreprise[6]
- Bonnes et mauvaises applis : le retour sur investissement induit par des expériences mobiles exceptionnelles[7]
- Logiciels malveillants, masques et autres : protéger les utilisateurs contre leurs applis (MaaS360)
- Webinaire : Concevoir, développer et déployer des applis mobiles (MaaS360)
- MaaS360 Mobile Application Security
- MaaS360 Mobile Application Management

A propos de 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 individuelles. 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 de la sécurité IBM

La plateforme de sécurité IBM fournit les données de sécurité nécessaire 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, consultez le site : www.ibm.com/security

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

Produit aux Etats-Unis
Mars 2016

Pensez à recycler

WGW03107-FRFR-01

1 « *IDC révèle ses prévisions concernant les applis mobiles et les solutions d'entreprise mondiales pour 2015*, » BusinessWire, 18 décembre 2014 », http://www.businesswire.com/news/home/20141218006258/en/IDC-Reveals-Worldwide-Mobile-Enterprise-ApplicationsSolutions#.VSfAlig0qVh

2 IBM Security, « *Meilleures pratiques pour la gestion du cycle de vie des applis mobiles* », http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03110USEN&attachment=WGW03110USEN.PDF

3 Shields, T., *Sécurité des applis mobiles : les résultats du conflit* Forrester Research, Inc. Blog, 7 juillet 2014, http://blogs.forrester.com/category/application_wrapping/

4 IBM Security, *Lorsque l'entreprise se centre sur l'appli, l'appli est l'entreprise*, *Volume I : L'applification de l'entreprise*, 2015, http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03105USEN&attachment=WGW03105USEN.PDF

5 IBM Security, *Lorsque l'entreprise se centre sur l'appli, l'appli est l'entreprise*, *Volume II : Les quatre éléments d'une solide stratégie pour applis mobiles*, 2015, http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03106USEN&attachment=WGW03106USEN.PDF

6 IBM Security, *Mobilisez vos applis et contenus d'entreprise*, 2015, http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03111USEN&attachment=WGW03111USEN.PDF

7 « *Bonnes et mauvaises applis : le retour sur investissement induit par des expériences mobiles exceptionnelles* », étude mandatée par IBM et réalisée par Forrester, IBM MobileFirst, 2014, http://www.ibm.com/mobilefirst/us/en/good-apps-bad-apps.html