Sécurité IBM
Livre blanc

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

IBM

Introduction

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

Dans ce volume, vous découvrirez comment concevoir une stratégie des applis orientée entreprise qui vise les objectifs métier sans exposer les données et le réseau à des risques.

L'applification de l'entreprise englobe les concepts de découverte, d'évolutivité, de durabilité et de sécurité.

Les quatre éléments d'une solide stratégie pour applis mobiles

Comme évoqué dans le *Volume I, L'applification de l'entreprise*[1], les applis mobiles transforment fondamentalement les relations entre les entreprises, les employés et les clients, ainsi que la façon de mener les affaires en général. Le développement d'une stratégie efficace détermine la capacité des applis à générer des avantages réels pour l'entreprise et assurer la protection des données et du réseau. Pour réussir, l'applification doit englober la découverte, l'évolutivité, la durabilité et, bien sûr, la sécurité.

Concevoir des applis répondant aux besoins de vos utilisateurs

D'après une enquête menée par l'EME (Enterprise Mobility Exchange) auprès de 300 professionnels séniors de la mobilité d'entreprise [2], les investissements en mobilité des entreprises sont principalement consacrés à des applis mobiles conçues pour améliorer la productivité de leurs employés.

Cela ressemble à une histoire trop connue, avec une plateforme différente. La direction souhaite augmenter la productivité des employés, améliorer son engagement auprès des clients et se faciliter la vie. Le service informatique veut s'assurer que les employés ne ravagent pas le réseau et n'exposent pas l'entreprise à des risques de sécurité inconsidérés (et donc à des coûts). Cependant, la mise en place d'activités basées sur les applis n'est pas censée se transformer en affrontement entre le service informatique et le reste de l'entreprise. En réalité, il est essentiel que ces deux pôles participent ensemble au développement de la stratégie.

En premier lieu, le service informatique doit connaître les objectifs stratégiques à l'origine de toutes les initiatives basées sur des applis. Ensuite, il doit consacrer suffisamment de temps avec les directeurs et les utilisateurs pour comprendre comment les clients et les employés utilisent leurs appareils pour communiquer et obtenir les informations qu'ils recherchent. Le service informatique doit connaître la nature des données qu'ils consomment et partagent, et les problèmes susceptibles de faire obstacle. Il est essentiel que ce processus soit appliqué dans toutes les unités et tous les cas d'utilisation, même pour le développement d'une seule appli, afin d'éviter toute lacune ou incohérence dans le produit fini. Au cours de ses échanges avec le reste de l'entreprise, le service informatique doit répondre aux questions suivantes :

- Que feront-ils avec l'appli ? L'appli sera-t-elle utilisée pour un engagement direct auprès des clients ?
- Quelles sont les fonctions les plus importantes ?
- Quelle est la fonctionnalité qui concrétisera cet objectif ?
- Quels systèmes seront sollicités ?
- Quels sont les risques de sécurité engendrés par l'appli ? Quelles peuvent être les conséquences d'un accès par un utilisateur non-autorisé ?
- Est-ce que certaines réglementations sur les données sont à prendre en compte ?
- Quelle valeur ajoutée cette appli doit-elle apporter ?

Prête à évoluer dans la minute

Une fois cette première analyse terminée, le service informatique peut élaborer un plan de développement et de déploiement de l'appli. Quelle que soit l'ampleur de l'utilisation prévue, il est important de créer une appli mobile capable d'évoluer pour utiliser de plus importants volumes de données et d'offrir une expérience remarquable. Lors du choix des technologies qui supporteront vos applis, posez-vous les questions suivantes pour définir l'infrastructure finale :

- Comment puis-je être sûr que mon appli proposera une expérience utilisateur stable sur tous les appareils et systèmes d'exploitation ?
- Est-ce que l'architecture de mon appli est capable de s'adapter à la demande à la fluctuation du nombre d'utilisateurs ?
- Que se passera-t-il sur notre réseau lorsque les interfaces back-end seront simultanément reliées à des systèmes et/ou à des bases de données supplémentaires ?
- Notre réseau est-il assez solide pour supporter l'augmentation du nombre d'appareils simultanément connectés ?
- Comment puis-je contrôler les goulots d'étranglement pendant la conception, le déploiement et l'utilisation ?

Le changement est inévitable

Vous devez réfléchir sur le long terme car, avec le temps, les applis devront être mises à jour. Contrairement aux applis Web qui sont hébergées sur un serveur, les applis mobiles dépendent seulement de leur dispositif hôte. Cela signifie qu'il est impossible d'effectuer des modifications rapides et régulières. Que ce soit pour s'adapter aux fluctuations de la demande des utilisateurs ou aux mises à jour des systèmes d'exploitation, il sera nécessaire d'apporter des modifications. Ainsi, pour s'assurer de la viabilité de ses applis, le service informatique doit se poser les questions suivantes :

- La fonctionnalité de l'appli front-end est-elle suffisamment adaptable pour intégrer de nouvelles fonctions demandées par les utilisateurs ?
- Serons-nous prêts à lancer des mises à jour rapides pour nous adapter immédiatement lorsque des utilisateurs mettront à jour leur système d'exploitation ?
- Quel est notre processus de collaboration et de découverte concernant les applis utilisateurs ?
- Sommes-nous prêts à réagir aux commentaires des utilisateurs et à assurer une conception et un développement continus ?

La sécurité intégrée à chaque étape. . . et non pas une addition tardive !

Dans notre prochain volume, *Se protéger contre les dangers de l'application*, nous aborderons les dernières (mais pas des moindres) considérations sur l'application de la sécurité de l'entreprise.[3] Les applis mobiles constituent des sources grandissantes de vulnérabilité pour les entreprises, pour diverses raisons incluant : gestion inadéquate du stockage des données, logiciels malveillants, accès non autorisés, absence de chiffrement et fuites de données.

Gartner prévoit que 75 % des applis mobiles échoueront aux tests de sécurité de base en 2015 et pourront laisser ouvert un accès à des pirates sur leur réseau.[4] La dernière version de Masque Attack[5] fonctionne en remplaçant l'appli d'entreprise officielle par une appli malveillante. Elle est généralement non détectable sur l'appareil de l'utilisateur car elle se fait passer pour l'appli d'origine.

Les menaces pesant sur les données et le réseau des entreprises augmentent proportionnellement à l'extension de l'application. Ainsi, il est essentiel de formuler et d'appliquer des mesures de sécurité à chaque étape du développement et du déploiement.

En conjonction avec d'autres solutions du portefeuille IBM® MaaS360® , MaaS360 vous permet d'élaborer une stratégie d'applis mobiles capable de faire progresser l'entreprise tout en offrant des garanties d'évolutivité, de durabilité et de sécurité. Contactez IBM dès aujourd'hui pour découvrir comment tirer le meilleur parti de l'environnement d'applis mobiles de votre entreprise.

Prêt pour l'application de votre entreprise ? Consultez les autres volets de cette série :

- **Volume I :** ***L'application de l'entreprise.*** Explorez l'application 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 III :** ***Se protéger contre les dangers de l'application.*** 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.

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]
- Quatre conseils pour protéger l'entreprise contre les menaces liées aux applis mobiles
- Meilleures pratiques pour la gestion du cycle de vie des applis mobiles[8]
- Webinaire : Concevoir, développer et déployer des applis mobiles
- IBM® MaaS360® Mobile Application Management

A propos d'IBM MaaS360

L'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 s'appuient en toute confiance sur MaaS360 pour leurs programmes mobiles. MaaS360 offre une gestion intégrale, avec des contrôles de sécurité avancés pour tous les utilisateurs, les appareils, les applis et les contenus afin de supporter l'ensemble des déploiements mobiles. Pour plus d'informations sur l'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

Pensez à recycler

WGW03106-FRFR-01

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

2 Westacott, Robbie, *Rapport sur l'état mondial de la mobilité d'entreprise, 2014/2015*, Enterprise Mobility Exchange, 3 décembre 2014, http://www.enterprisemobilityexchange.com/the-global-state-of-enterprise-mobility-report

3 IBM Security, *Lorsque l'entreprise se centre sur l'appli, l'appli est l'entreprise*, *Volume III : Se protéger contre les dangers de l'application*, 2015, http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03107USEN&attachment=WGW03107USEN.PDF

4 « Gartner affirme que 75 % des applis mobiles échoueront aux tests de sécurité de base en 2015 », Gartner, 14 septembre 2014, http://www.gartner.com/newsroom/id/2846017

5 IBM Security Intelligence, Quatre conseils pour protéger l'entreprise contre les menaces liées aux applis mobiles, 11 février 2015, https://securityintelligence.com/four-tips-for-protecting-the-enterprise-against-mobile-app-threats/

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 », article Forrester mandaté par IBM, IBM MobileFirst, 2014, http://www.ibm.com/mobilefirst/us/en/good-apps-bad-apps.html

8 IBM Security, *Meilleures pratiques pour la gestion du cycle de vie des applis mobiles*, 2015, http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=WGW03110USEN&attachment=WGW03110USEN.PDF