ZEBRA

MISE EN PLACE D'UNE STRATÉGIE DE SÉCURITÉ MOBILE ROBUSTE : principaux risques et comment les éviter

La sécurité informatique de la mobilité d'entreprise est souvent comparée à une assurance. Vous devez la prendre en compte, car elle est incontournable. Cette vision est toutefois limitée et erronée. La sécurité ne se limite pas à vous protéger contre un événement spécifique. Elle vous donne également des garanties et permet à votre entreprise d'être opérationnelle et novatrice sans risque de faille de données.

Dans ce livre blanc, nous présentons les points essentiels à prendre en compte pour développer une stratégie de sécurité mobile robuste. Nous exposons les risques principaux et expliquons comment les contourner afin d'exploiter de nouvelles opportunités pour améliorer la productivité, l'efficacité et la précision de vos opérations.

Pas de solution universelle

Les avis divergent sur la valeur de la sécurité. Nous sommes toutefois unanimes à reconnaître qu'il s'agit d'un sujet complexe qui concerne de nombreux aspects de l'organisation. Il faut tenir compte des multiples cas d'utilisation de la mobilité, des méthodologies applicatives et des options de déploiement d'entreprises individuelles pour mieux comprendre la valeur globale de la sécurité, ainsi que sa complexité.

Dans un magasin de détail, les employés équipés de tablettes servent les clients rapidement. Ces clients exigent toutefois que les informations personnelles qu'ils communiquent via ces périphériques soient sécurisées. Dans le secteur de la fabrication, vous devez tenir compte de l'essor des technologies portatives. Cette évolution implique la protection du flux de données émanant de nombreux points de terminaison.

Les méthodologies applicatives varient également selon le cas d'utilisation et le type de périphérique. Des applications Web aux applications mobiles natives, ou même hybrides, l'entreprise doit appliquer une stratégie de sécurité adaptée à chaque cas.

Les options de déploiement mobile disponibles risquent de compliquer la tâche encore davantage. Si l'entreprise favorise les initiatives BYOD (Bring Your Own Device) ou utilise des technologies grand public, le service informatique devra sans doute allouer des ressources supplémentaires. Il sera amené à développer des solutions de sécurité personnalisées si les systèmes d'exploitation (SE) mobiles grand public n'assurent pas la sécurité requise. Il est également nécessaire de protéger l'activité du réseau, ainsi que la connectivité du réseau étendu ou du réseau local sans fil.

Les plateformes de mobilité doivent tenir compte de ces exigences individuelles en matière de sécurité tout en prenant en charge des solutions informatiques mobiles, à la demande des entreprises. L'objectif de toute entreprise doit être d'assurer la sécurité des données sans perturber les opérations quotidiennes. Quelles sont alors les principales menaces, et par conséquent, les composants essentiels d'une stratégie de sécurité mobile robuste ?

VOUS DEVEZ TENIR COMPTE DE L'ESSOR DES TECHNOLOGIES PORTATIVES.

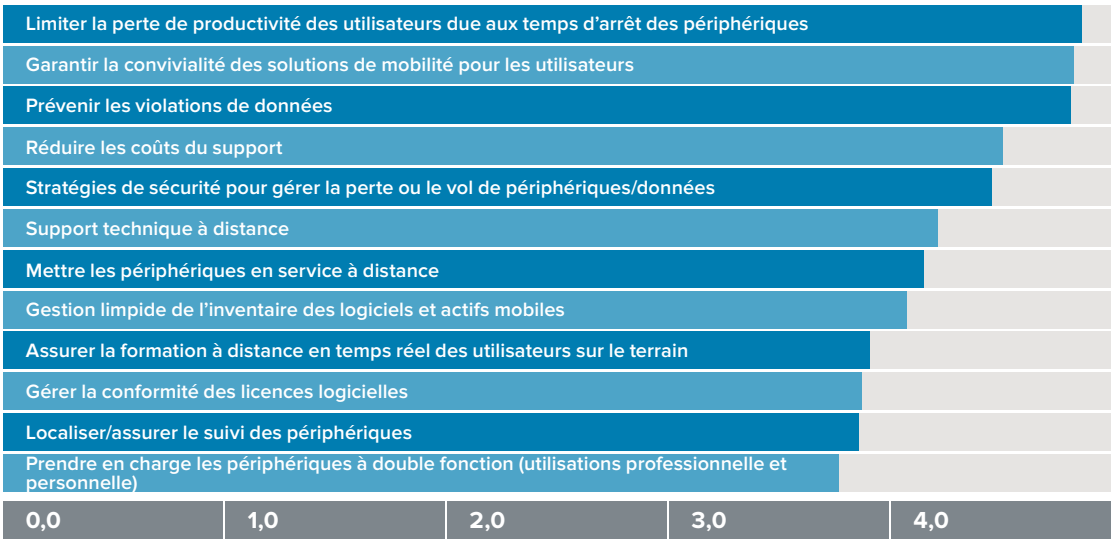
Cette évolution implique la sécurisation du flux de données émanant de nombreux points de terminaison.

Identification des risques

Exposés à un nombre bien supérieur de menaces de sécurité, les périphériques embarqués sont bien plus vulnérables que les ordinateurs de bureau. Portables et de taille inférieure, ils sont plus susceptibles d'être volés. S'ils ne sont pas correctement gérés, les applications et systèmes d'exploitation polyvalents peuvent présenter des failles que les cybercriminels peuvent exploiter. En outre, puisque les communications via des connexions cellulaires ou Wi-Fi ouvertes et non protégées menacent la sécurité des données des clients ou de l'entreprise, il est également nécessaire de prendre des mesures visant à contrôler l'accès aux réseaux non sécurisés.

D'après les analystes industriels VDC, sur les trois préoccupations principales des entreprises en matière d'investissement dans la mobilité, la violation des données occupe la troisième place. La mise en place de stratégies de sécurité pour gérer la perte ou le vol de périphériques et de données fait partie des 5 principales priorités, après les efforts visant à limiter les temps d'arrêt, à garantir une expérience utilisateur conviviale et à réduire les coûts de support. [1]

Classez les points suivants concernant la mobilité en fonction de leur importance pour votre entreprise
(1=sans aucune importance ; 6=extrêmement important)



[1] *« Total Cost of Ownership Models - Enterprise and Government Mobility Applications », VDC Research, Josh Martin, David Krebs*

Ces risques ne sont pas négligeables. Explorez les préoccupations essentielles concernant la sécurité et vous identifierez des menaces internes et externes. Les résultats de l'étude VDC sont confirmés par une enquête TechTarget SearchSecurity qui recense les cinq principaux problèmes que rencontrent les entreprises en matière de sécurité mobile.[1] Chacun des problèmes majeurs identifiés par les 487 participants concerne les données de l'entreprise.

1 Perte de périphériques : oubli d'une tablette ou d'un smartphone professionnel dans un taxi ou un restaurant, par exemple

2 Sécurité des applications : données communiquées aux développeurs d'applications mobiles gratuites, par exemple

3 Fuite de données provenant d'un périphérique : risque d'accès des cybercriminels aux applications professionnelles exécutées sur des périphériques personnels, par exemple

4 Attaques de logiciels malveillants : chevaux de Troie, outils de surveillance ou applications malveillantes, par exemple

5 Vol de périphériques : vulnérabilité des données après le vol d'un périphérique essentiel, par exemple

Ce sont la réputation et les revenus de l'entreprise qui sont menacés. Comme un article publié sur CIO.com l'indique,[2] *« Plus les employés et sous-traitants utilisent des périphériques embarqués pour accéder aux systèmes, applications et données de l'entreprise, plus cet accès doit être protégé. Il est également important d'empêcher les périphériques embarqués censés optimiser la productivité et les résultats financiers de présenter des failles favorisant un accès non autorisé aux informations et autres actifs de l'entreprise, ce qui les transformerait alors en une menace susceptible d'entraîner une perte de revenus. »*

La question est donc la suivante : quelles mesures spécifiques votre organisation peut-elle prendre pour faire face aux menaces constantes risquant de déstabiliser la sécurité mobile des entreprises ?

[1] *Top 5 enterprise mobile security issues, Tech Target, 2012*

[2] *http://www.cio.com/article/2378779/mobile-security/7-enterprise-mobile-security-best-practices.html*

Lutte contre la menace

Alors que les entreprises dépendent de plus en plus des technologies mobiles, elles doivent mieux se prémunir contre les problèmes de sécurité. Plusieurs analyses effectuées par Gartner, Forrester et Information Week recommandent certaines précautions que les services informatiques peuvent prendre pour éliminer les risques internes et externes.

Forrester recommande également les sept mesures suivantes pour assurer la sécurité mobile et la gestion des périphériques embarqués (MDM - Mobile Device Management) :

- Utilisation d'un code confidentiel (mots de passe difficiles à déchiffrer)
- Réinitialisation sélective (essentielle dans le cadre d'une stratégie BYOD)
- Détection de débridage/enracinement
- Cryptage des données
- Réseaux privés virtuels (VPN)
- Protection contre la fuite de données (pour empêcher les utilisateurs autorisés de transmettre des données accidentellement ou par malveillance)
- Restriction des périphériques via ActiveSync

Toutes ces mesures ne seront que des vœux pieux du service informatique si l'entreprise ne prend pas la sécurité mobile au sérieux. Ce sont les responsables qui mettent la sécurité à l'ordre du jour des réunions ou qui allouent des ressources pour combattre des menaces de plus en plus sophistiquées.

Pour y parvenir, il est essentiel de connaître la réglementation en vigueur et les meilleures pratiques internationales en matière de sécurité. Voici un résumé de ces normes qui met en évidence les mesures que chaque entreprise doit inclure dans sa stratégie de sécurité mobile :

- Protection contre le vol ou la perte de périphériques
- Protection des données en transit
- Protection des données entreposées
- Gestion des applications mobiles
- Conformité à la réglementation
- Contrôle, gestion et surveillance des périphériques
- Protection renforcée de la confidentialité des données
- Réduction des coûts administratifs pour la protection constante des plateformes
- Application de contrôles stricts d'accès/d'authentification
- Utilisation optimale de l'infrastructure informatique existante

L'entreprise doit alors proposer une stratégie mobile qui repose sur ces mesures de sécurité. Tout comme les scénarios d'utilisation, la sécurité doit être un facteur déterminant dans le choix des périphériques et systèmes d'exploitation.

FONCTIONS DE GESTION DE LA SÉCURITÉ[3]
Mise en service et inscription automatiques des périphériques
Mot de passe obligatoire
Réinitialisation des périphériques, verrouillage à distance
Fonctions d'audit des comptes utilisateur et applications
Détection du débridage
Fonctions de protection des données
Contrôles des applications
Contrôle d'accès au réseau (NAC) mobile
Antivirus, antispam, pare-feu de points de terminaison et système de détection des intrusions aux points de terminaison
Certificats basés sur les périphériques
Contrôle actif des protections ci-dessus
VPN d'entreprise
Gestion des clés et des certificats

[3]*Sources : Information Week report, novembre 2011 ; Forester report, Answers to top mobile security questions, 2011 ; Gartner Report, MCM_MQ, avril 2011.*

Conséquences du choix de solutions de mobilité inadaptées

« 277 millions de périphériques embarqués doivent intégrer des fonctions de sécurité d'ici à 2016. »

Compte tenu de la prolifération des risques de sécurité, les entreprises attirées par des prix bas doivent réfléchir avant d'acheter des périphériques grand public prêts à l'emploi. La plupart des systèmes d'exploitation grand public installés sur ces périphériques n'intègrent pas toutes les fonctions de sécurité dont les entreprises ont besoin. Des études indiquent que le coût total de possession de périphériques grand public pour une utilisation en entreprise peut être entre 40 et 78 % supérieur à celui des périphériques professionnels conçus sur mesure.[3] La sécurité contribue en grande partie à cet écart.

Les périphériques grand public utilisés à des fins professionnelles sont souvent exposés aux brèches de sécurité. Une étude sur la stratégie BYOD publiée par Decisive Analytics[4] révèle que presque la moitié (46,5 %) des entreprises interrogées signale une brèche de sécurité ou violation de données lorsqu'un périphérique appartenant à un employé accède au réseau de l'entreprise. Pour se protéger contre cette menace, les entreprises doivent investir lourdement. Toutefois, ces mesures de protection ne garantissent en aucun cas leur efficacité contre les nouvelles menaces.

En revanche, les périphériques robustes conçus sur mesure pour l'entreprise sont optimisés pour assurer et simplifier la conformité aux mandats réglementaires phare en matière de sécurité. La conformité en matière de sécurité peut s'appliquer à des domaines très généraux (formation des utilisateurs, par exemple), mais également très spécifiques (validation de l'intégrité des algorithmes cryptographiques, par exemple).

Les plateformes de SE mobiles ou les périphériques ne peuvent garantir à eux seuls la conformité à la réglementation. Toutefois, en choisissant des plateformes logicielles et des périphériques chez un fabricant soucieux du respect des mandats réglementaires sur la sécurité, vous favorisez le respect des règles de conformité et limitez les tâches administratives fastidieuses visant à la valider. Vous réduirez également ainsi les frais d'audit, éviterez potentiellement les amendes et les pénalités et n'aurez pas à signaler de brèche de sécurité, d'où une augmentation de vos résultats financiers.

3 « Total Cost of Ownership Models - Enterprise and Government Mobility Applications », Josh Martin & David Krebs, VDC Research ; « A 3 Year Cost Comparison of Consumer-grade vs. Durable Smart Devices », Jack Gold, Gold Associates

[4] http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf

Gros plan sur la sécurité des applications et des systèmes d'exploitation : Android

Les entreprises à la recherche de périphériques grand public peuvent choisir plusieurs acteurs phare du marché : Google, Apple et Microsoft. La plateforme Android de Google détient la part du lion (81 % du marché mondial en 2015)[5]. Son offre de sécurité intrinsèque attire également les entreprises qui envisagent d'utiliser des périphériques grand public. Elle se démarque surtout des autres plateformes de SE mobiles grand public. Le cloisonnement des applications, l'octroi d'autorisations d'accès aux ressources et le cryptage de données ne sont que quelques illustrations des fonctions de sécurité fiables d'Android.

La plupart des problèmes liés à la sécurité sur Android provient du fait qu'elle risque d'être menacée par d'éventuels logiciels malveillants provenant de GooglePlay, la galerie d'applications de la plateforme. En contrôlant strictement le processus de signature, Apple filtre étroitement les applications de son AppStore. Pourtant, le risque de sécurité que présente GooglePlay affecte toutes les galeries d'applications publiques. Elles sont toutes exposées aux logiciels malveillants et aux atteintes à la vie privée (même l'AppStore d'Apple).

Pour plus de sécurité, nous vous recommandons de permettre le verrouillage des applications et/ou d'utiliser une galerie d'applications d'entreprise fiable lorsque vous utilisez des périphériques dans l'entreprise. Le jeu de fonctionnalités Mobility Extensions (Mx) de Zebra vous offre une protection renforcée. En simplifiant la conformité aux exigences en matière de mobilité et à la réglementation en vigueur, les entreprises bénéficient d'une sécurité professionnelle sur des périphériques grand public.

Si vous utilisez une galerie d'applications d'entreprise, des extensions comprenant des listes blanches, des fonctions d'authentification AD/LDAP, de gestion des clés ou d'autres fonctions essentielles de sécurité, votre service informatique peut mettre des périphériques grand public en service dans l'entreprise en toute sécurité.

[5] http://www.idc.com/getdoc.jsp?containerId=prUS40664915

Il est évident que la sécurité mobile ne se limite pas à protéger l'intégrité de l'entreprise si vos données et périphériques sont menacés. Elle peut satisfaire aux exigences opérationnelles propres à la stratégie mobile globale et réduire le coût total de possession lors des déploiements de solutions mobiles d'entreprise. Avant tout, la sécurité mobile va continuer à évoluer et devra faire l'objet de révisions et mises à jour permanentes et scrupuleuses.

Alors que la mobilité d'entreprise a fait de formidables progrès en quelques années seulement, le paysage sécuritaire ne cesse d'évoluer, au point de devenir méconnaissable. Les défis sont complexes et les solutions très variées. Vous devez les étudier individuellement en les adaptant aux priorités de l'organisation. Une stratégie de sécurité stricte ne présente aucun intérêt si elle limite vos opérations et nuit à votre avantage concurrentiel, ainsi qu'à la productivité de vos employés. En revanche, en omettant la sécurité dans les efforts que vous déployez, vous vous exposez à des attaques. Les stratégies de sécurité mobile les plus robustes limiteront les risques auxquels vous êtes exposé tout en garantissant le bon déroulement de vos opérations et l'application d'initiatives novatrices.

Vous devez donc harmoniser les priorités de votre stratégie de sécurité mobile en satisfaisant aux principales exigences de votre entreprise et des utilisateurs, grâce à des stratégies secondaires adaptées à divers cas d'utilisation.

Liste de contrôle utile

Vu la complexité et la diversité des points à prendre en compte, la mise en place d'une stratégie de sécurité mobile pour votre personnel peut sembler particulièrement complexe. Cette liste de contrôle va vous permettre de choisir des solutions adaptées à votre entreprise et qui tiennent compte des besoins des utilisateurs, de l'entreprise et des exigences en matière de sécurité.

1 **Informez le personnel :**
Sensibilisez-le aux menaces sécuritaires et mettez en place des stratégies claires et compréhensibles.

2 **Modifiez régulièrement vos mots de passe :**
Nous recommandons une mise à jour mensuelle des mots de passe, éventuellement imposée par les applications, en spécifiant des niveaux de sécurité stricts.

3 **Assurez la visibilité totale de tous vos périphériques :**
Utilisez des outils de gestion des périphériques embarqués pour localiser instantanément les périphériques égarés ou volés et les désactiver ou effacer les données qu'ils contiennent. Utilisez des fonctions de surveillance et des alertes pour localiser chaque périphérique et en surveiller l'utilisation.

4 **Créez une liste blanche :**
Limitez l'accès des utilisateurs de périphériques aux sites Web figurant sur des listes blanches que vous approuvez.

5 **Protégez-vous contre les logiciels malveillants :**
En identifiant sur une liste blanche les applications internes et les sources d'applications autorisées sur vos périphériques, vous vous protégez contre les infections. En outre, en contrôlant le chargement latéral d'applications externes par les périphériques, via une connexion externe ou à partir d'une carte de stockage, vous les protégez contre les logiciels malveillants et toute autre application néfaste.

6 **Mettez à jour vos périphériques :**
Veillez à exécuter les logiciels les plus récents sur vos périphériques en contrôlant les mises à jour et/ou en les automatisant.

7 **Conteneurisez vos données :**
Configurez vos périphériques pour que les données soient conteneurisées dans des zones cryptées distinctes, qui en interdisent l'accès à toute personne malveillante.

8 **Appliquez un encryptage intégral :**
Vous pouvez crypter les données extrêmement confidentielles stockées sur des périphériques, ainsi que les données transmises via des réseaux sans fil.

9 **Utilisez une galerie d'applications d'entreprise :**
Évitez d'utiliser les galeries d'applications publiques et téléchargez les applications à partir d'une galerie d'applications d'entreprise fiable.

10 **Réévaluez régulièrement la sécurité :**
La sécurité mobile n'est pas une préoccupation ponctuelle, et vous devez continuellement mettre à jour vos stratégies et meilleures pratiques pour faire face aux menaces en constante évolution.

DÉCOUVREZ POURQUOI LA SÉCURITÉ N'EST QU'UN DES NOMBREUX POINTS À PRENDRE EN COMPTE LORSQUE VOUS CHOISISSEZ UN NOUVEAU SE MOBILE.

EXPLOREZ LES AUTRES POINTS ESSENTIELS À ÉTUDIER SUR
WWW.ZEBRA.COM/MOBILITYREVOLUTION

Siège social général et siège Amérique du Nord
+1 800 423 0442
inquiry4@zebra.com

Siège Asie-Pacifique
+65 6858 0722
contact.apac@zebra.com

Siège EMEA
zebra.com/locations
mseurope@zebra.com

Siège Amérique latine
+1 847 955 2283
la.contactme@zebra.com