Un livre blanc des TrendLabs

LE BYOD : ATOUT OU MENACE ?

5 RÉALITÉS SUR LA SÉCURITÉ DES ÉQUIPEMENTS MOBILES

L'équipement le plus compact peut représenter la faille la plus importante au sein d'une entreprise.

Comment ? L'avènement du BYOD (Bring Your Own Device), à savoir l'introduction et l'utilisation d'équipements personnels en entreprise, crée une passerelle pour les menaces qui s'immiscent via les failles du réseau, notamment lorsque les collaborateurs sont négligents. Le BYOD s'inscrit dans le cadre de la consumérisation des équipements informatiques, lorsque les technologies grand public sont utilisées dans un contexte professionnel.

Le BYOD est une tendance appellée à se renforcer. Aux PME d'identifier et de maîtriser les risques de sécurité liés au BYOD et à la mobilité.

43% des PME affirment êtres ouvertes à la mobilité, tandis que le support des dispositifs mobiles et des smartphones est perçu comme une priorité

Seuls **20%** des équipements sous *Android* ont une application de sécurité installée

1

Le BYOD est inévitable pour les PME.

La consumérisation est une pratique consistant en des collaborateurs qui utilisent des technologies grand public dans le cadre professionnel. Le BYOD est une forme de consumérisation, et fait référence aux collaborateurs qui amènent leurs propres dispositifs tels que smartphones, tablettes ou ordinateurs portables en entreprise, et les connectent généralement au réseau d'entreprise.[1]

Le BYOD est une tendance appelée à perdurer et se veut indispensable pour les PME qui veulent garder une longueur d'avance sur leurs concurrents.[2]

Certaines études révèlent que 43% des PME sont prêtes à accepter les équipements mobiles et font de leur support une priorité.[3] D'autre part, les chefs d'entreprise se servent aussi d'applications mobiles pour gagner du temps, encourager leur chiffre d'affaires et leur productivité, et maîtriser leurs coûts.[4]

1 http://consumerization.trendmicro.com/the-consumerization-university-day-1-consumerization-is-disruptive/
2 https://learningnetwork.cisco.com/blogs/vip-perspectives/2012/06/09/bring-your-own-devicebyod-fad-or-future
3 http://blogs.forrester.com/michele_pelino/10-09-24-mobility_momentum_intensifies_among_small_and_medium_size_businesses
4 http://www.sbecouncil.org/uploads/Mobile%20APP%20Final%20Report%20SBE%20Council.pdf

2

Les PME doivent s'attendre à des problèmes de sécurité liés au BYOD.

Les entreprises qui utilisent des équipements mobiles, quelle que soit leur taille, doivent se rendre compte qu'elles s'exposent à des risques de sécurité.

Avec plus de 900 millions de terminaux sous *Android* existants, la plateforme devient une cible particulièrement intéressante. D'autant que seuls 20% des équipements sous *Android* disposent d'une application de sécurité installée.[5]

Les entreprises qui s'adonnent au BYOD courent donc des risques et doivent réaliser que l'univers du BYOD dévoile certains dangers. Les cybercriminels sont particulièrement intéressés par les mobiles[6] et ciblent davantage les plateformes les plus populaires, compte tenu d'un nombre de victimes potentielles plus important.

5 http://fearlessweb.trendmicro.com/2012/misc/only-20-of-android-mobile-device-users-have-a-security-app-installed/
6 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_security_in_the_age_of_mobility.pdf

3 Un risque pour les données stockées dans les équipements mobiles.

Selon une étude menée par Ponemon Institute, les menaces sur les données d'entreprise proviennent des collaborateurs eux-mêmes. Ceux-ci s'exposent à la perte de leurs données, lorsque leur équipement est volé ou pas assez protégé contre les malwares qui détournent les données. La même étude démontre aussi que la négligence des collaborateurs est la principale cause des fuites de données. Les PME subissent de nombreuses fuites qui résultent de collaborateurs ou d'intervenants extérieurs négligents ou mal intentionnés.[7]

En outre, les équipements mobiles sont beaucoup plus exposés au vol. Les téléphones portables et les smartphones représentent 30 à 40% des vols dans les grandes villes des États-Unis, pour un chiffre de 27 000 vols par an.[8] Les PME doivent comprendre que les équipements mobiles doivent être tout aussi bien protégés que les ordinateurs de bureau, si ce n'est davantage. Tout comme un smartphone privé qui contient des informations personnelles est facilement exploitable, un smartphone d'entreprise infecté est une porte ouverte vers les données sensibles d'entreprise.

Les collaborateurs sont confrontés à de lourdes pertes de données professionnelles à partir de leur équipement mobile, et par les moyens suivants :

- Connexion à un réseau sans fil non sécurisé
- Téléchargement et installation d'applications non authentifiées
- Visiter des sites internet potentiellement malveillants
- Laisser l'équipement mobile sans surveillance

Ce sont de véritables risques pour les données d'entreprise, au-delà de la perte accidentelle du dispositif.

7 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf
8 http://www.fcc.gov/document/chairman-remarks-stolen-cell-phones-initiative

4 Les malwares orientés BYOD existent déjà.

Les cybercriminels multiplient leurs cibles. Au-delà des ordinateurs de bureau, La popularité et la diversité des équipements mobiles en font une cible particulièrement importante. Une fois les équipements infectés, les dommages pèsent sur les collaborateurs mais aussi sur leur entreprise.[9]

Les malwares mobiles peuvent causer des dommages importants à une entreprise. Ceux qui détournent des donnés comptent parmi les plus nombreux pour l'environnement *Android*, et peuvent lire et divulguer tout ce que le collaborateur fait avec son équipement mobile. Les appels entrants et sortants, les messages textes, les carnets d'adresses et les données de localisations fournies par GPS comptent parmi les types de données détournées. De tels malwares peuvent ainsi faciliter un acte de piratage de données au sein d'une entreprise.[10]

Le malware Rooter peut prendre le contrôle des équipements *Android* et de leurs fonctions dès qu'il y est installé. Il permet aux cybercriminels de contrôler à distance ces équipements. Il leur fournit également l'accès au réseau de l'entreprise une fois l'équipement connecté à celui-ci.

Les malwares qui détournent les informations sous *Android* sont parmi les plus nombreux

9 http://blog.trendmicro.com/beta-version-of-spytool-app-for-android-steals-sms-messages
10 http://blog.trendmicro.com/more-spying-tools-being-seen-in-application-markets

Le nombre des malwares *Android* a bondi de

350 000

au premier semestre 2013

Android : le système d'exploitation mobile le plus ciblé.

5

Les cybercriminels ont toujours pris pour cible les systèmes d'exploitation les plus utilisés, afin de frapper le plus large panel de victimes possible. Le nombre d'applications Android malveillantes et à haut risque a connu une croissance continue jusqu'en juin 2013. Il a fallu trois ans pour que le nombre d'applications malveillantes et à haut risque atteigne le palier de 350 000, chiffre ayant doublé en l'espace de six mois seulement (de janvier à juin 2013).[11]

Comment les PME doivent-elles réagir? Les équipements sous *Android* constituent une réponse fiable aux besoins de mobilité et les PME doivent se prémunir contre les nombreux malwares ciblant cette plateforme et donc, adopter des règles de sécurité adéquates.

11 http://www.trendmicro.fr/media/misc/2q-2013-trendlabs-security-roundup-fr.pdf

QUE FAIRE POUR TIRER AVANTAGE DE LA CONSUMÉRISATION?

Pour mieux protéger les données et les biens de votre entreprise contre les risques liés au BYOD, voici quelques conseils pertinents :

ÉTABLIR UN PLAN PROJET.

- Écarter les pratiques potentiellement dangereuses découlant de l'adoption du BYOD dans l'entreprise, et sur l'ensemble du périmètre d'entreprise.
- Sensibiliser vos collaborateurs et vos différents services.
- Observer les types d'équipements utilisés par les collaborateurs et les futurs choix en matière d'équipement.

INSTAURER DES RÈGLES.

- Déterminer les équipements privilégiés, ceux tolérés et ceux qui seront évités et donc bannis du réseau.
- Décider des critères d'autorisation du BYOD, suivant la fonction ou la localisation des utilisateurs.
- Prévoir des procédures en cas de perte, de vol ou de détérioration. Inciter à la franchise et à l'honnêteté.

DÉPLOYER DES OUTILS PERTINENTS.

- *Trend Micro™ Worry Free™ Business Security Services* gère la plateforme *Android* avec des fonctionnalités comme App Scanning (analyse des applications) et Web Reputation (réputation des sites Web). Ce logiciel intègre les équipements *Android* dans la liste des systèmes administrés depuis une console de gestion web centralisée.

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), spécialiste de la sécurité du cloud, sécurise les échanges numériques pour les entreprises et le grand public, grâce à ses solutions de sécurité des contenus Internet et de gestion des menaces. Pionnier de la sécurité des serveurs depuis plus de 20 ans, Trend Micro propose une offre complète de sécurité pour postes clients, serveurs et en mode Cloud, pour neutraliser les nouvelles menaces plus rapidement et protéger les données en environnements physiques, virtuels ou Cloud. Optimisés par l'infrastructure Trend Micro Smart Protection Network, les technologies, produits et services Trend Micro dédiés aux environnements Cloud neutralisent toutes les menaces à la source sur Internet et s'appuient sur un réseau mondial de plus d'un millier d'experts.

TRENDLABS℠

Les TrendLabs constituent l'infrastructure mondiale des centres de recherche, de développement et de support, dédiée, en 24x7, à la surveillance sur les menaces, la prévention des attaques et au bon fonctionnement des solutions de sécurité. Regroupant plus de 1 000 experts et ingénieurs supports, les Trend Labs sont disséminés aux quatre coins de la planète. Les Trend Labs permettent à Trend Micro d'assurer une veille permanente sur les menaces dans le monde, de fournir des données en temps réel pour détecter et neutraliser les menaces, d'étudier et analyser de nouvelles technologies pour déjouer les menaces, de répondre en temps réel aux menaces cibles et d'aider nos clients à minimiser les dommages, à alléger leurs coûts et à assurer la continuité de leur activité.

TREND MICRO™

Securing Your Journey to the Cloud

TrendLabs

©2012 by Trend Micro, Incorporated. Tous droits réservés. Trend Micro et le logo t-ball de Trend Micro sont la propriété de Trend Micro. Tous les autres noms de produits et d'entreprise mentionnés dans ce document appartiennent à leurs détenteurs respectifs.