Stéphanie BRÉFORT
RISR 2013-2014
L3

# LE BYOD REMET-IL EN QUESTION LA SECURITE INFORMATIQUE DE L'ENTREPRISE ?

INSTITUT DE LA FILIÈRE NUMÉRIQUE

# SOMMAIRE

# Introduction

Dans le cadre de ma formation de responsable d'infrastructures systèmes et réseaux (**RISR**) au sein de l'école d'informatique l'IMIE, j'ai eu l'opportunité de mener à bien un projet de veille informatique.

J'ai articulé mes recherches autour de la problématique suivante : Le **BYOD** (Bring Your Own Devices) remet-il en question la sécurité de l'entreprise ?

Le cœur de cette problématique porte sur l'intégration de matériel informatique personnel tels que des smartphones, tablettes ou ordinateurs portables au sein des entreprises.

Comment doit réagir une entreprise face à ce phénomène et celui-ci remet-il en question la sécurité de ses infrastructures informatiques existantes et de ses données ?

Pour pouvoir répondre à ces questions j'ai dans un premier temps identifié les principaux risques posés par le BYOD, puis me suis penchée sur les solutions à mettre en place pour mitiger l'impact de ces risques.

Je suis arrivée à la conclusion que la mise en place d'une stratégie BYOD est actuellement un risque trop grand.

## Qu'est-ce-que le B.Y.O.D. ?

Le **BYOD,** ou bring your own devices, traduit de l'anglais par : « apportez vos propres appareils » est une pratique qui consiste à permettre aux salariés de travailler avec leur équipement personnel (téléphones intelligents, tablettes, ordinateurs portables...) au sein de leur entreprise. Ce matériel n'est alors pas pris en charge financièrement par l'entreprise.

Cette pratique a soulevé plusieurs questions sur les plans juridique, social et de la sécurité.

Dans ce dossier, je ne parlerais que de l'aspect sécurité de cette pratique.

## Jailbreaking et rooting

Ces termes font référence à la possibilité pour un utilisateur d'appareil mobile d'obtenir un **accès complet** à toutes les fonctionnalités de son système d'exploitation.

Le terme jailbreak est spécifiquement utilisé pour les appareils utilisant iOS. Pour les autres OS, le terme rooter est utilisé.

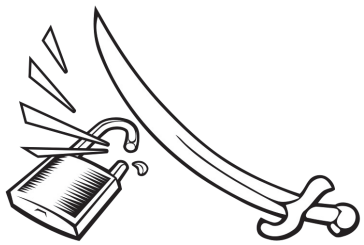
Cette pratique engendre comme principal risque la désactivation ou le contournement de nombreuses restrictions de sécurité mises en place par le constructeur.

Dans le cas d'iOS, les utilisateurs sont en mesure de télécharger des applications, des extensions ainsi que des thèmes non disponibles sur la boutique d'application officielle. L'utilisateur s'expose alors plus facilement à l'utilisation d'applications **non-sécurisées**.

Des virus existent et peuvent s'infiltrer en installant des applications tierces, non officielles, si elles ne proviennent pas de sources sûres. Ceux-ci peuvent alors endommager physiquement et logiciellement l'appareil ou bien altérer son fonctionnement pour détourner des données sensibles ou des informations d'authentification.

Concernant le rootage d'un équipement, celui permet à l'utilisateur et aux applications installées de **disposer des droits d'administrateur**.

Cette action est dangereuse car elle permet la suppression ou la modification de fichiers systèmes, la suppression des applications du constructeur, ou l'accès aux réglages système de l'appareil (le redémarrage, le contrôle des LED de notification ou le calibrage de l'écran tactile).



## Mises à jour de sécurité

Certaines personnes et certains virus exploitent les **failles de sécurité** des systèmes d'exploitation et des applications pour infecter le matériel.

Il est conseillé de maintenir régulièrement à jour le système d'exploitation et les applications car les mises à jour permettent de corriger ces failles.

Si l'utilisateur n'effectue pas les mises à jour de sécurités de son appareil, celui-ci devient alors **vulnérable aux différentes attaques**. ( prise de contrôle du matériel à l'insu de l'utilisateur, vol d'informations, dysfonctionnement ou arrêt de la machine, propagation d'un ver, installation de contenu illicite, etc...)

## Points d’accès WI-FI

Si une personne mal intentionné se connecte au même point d’accès, il peut à l'aide d'un analyseur de paquets (technique du sniffing), voir les pages web qu'est en train de consulter un salarié. Il peut aussi **intercepter les mails** envoyés et récupérer par la même occasion le nom d'utilisateur et le mot de passe si la connexion n'est pas chiffrée (technique du sidejacking).

De plus, le salarié peut se retrouver piégé s'il ce connecte directement sur un point d’accès pirate si le SSID de celui-ci semble correct. (technique du honeypot) De là, le pirate peut **intercepter toutes les données** qui transitent sur le réseau.

Ce problème peut être évité en mettant en place un système de **liaison VPN** depuis les outils utilisateurs vers le réseau de l'entreprise.

## Spyware et Adware

Un logiciel espion (spyware) est un logiciel malveillant (souvent inclus dans un logiciel gratuit) qui s'installe sur le matériel dans le but de **collecter** et **transférer des informations** sur l'environnement dans lequel il s'est installé. Les informations récoltées sont souvent les recherches de l'utilisateur ainsi que ses téléchargements.

Le logiciel malveillant adware est un logiciel (le plus souvent gratuit) qui affiche de la publicité. Ce type de logiciel inclut souvent un spyware dans le but d'injecter de la publicité ciblée dans l'application.

Le risque pour une entreprise est que le matériel du salarié contienne un spyware et que les informations contenues sur ce dernier soient alors compromises.

C'est pour ces raisons qu'il est indispensable que le matériel dispose d'un **anti-virus** à jour.

## Service Cloud

Certains appareils disposent d'un service cloud intégré, notamment les téléphones. Les salariés peuvent, sans se rendre compte de la gravité de leur action, y déposer des données professionnelles afin d'y avoir accès depuis d'autre appareils...

Les données concernées risquent alors d'être compromises ou même de tomber sous le coup des juridictions étrangères.

Il est aussi possible pour le système d'exploitation de détecter de nouvelles données sur l'appareil et les stocker **automatiquement dans le cloud** si le service est activé. Il est alors possible pour l'utilisateur de ne pas être conscient de l'utilisation du service.

La solution la plus simple est de désactiver ce type de service sur les appareils concernés. Mais cette solution prive aussi l'utilisateur de ce service pour ses données personnelles.

## Accès physique à l'équipement, Perte ou vol

L’accès physique à l'équipement est un risque potentiel pour la sécurité. En effet, rien ne sert de sensibiliser le salarié à la sécurité informatique si celui-ci laisse à la portée de tous son matériel.

Mettre un **mot de passe** ou **système de verrouillage** sur l'équipement peut-être une solution pour dissuader la plupart des personnes pouvant avoir accès physiquement au matériel. Mais cette solution n'est pas assez sûre si une personne mal intentionnée détient l'équipement concerné.

Il n'est pas nécessaire de connaître le mot de passe de l'équipement pour avoir accès aux données ; un simple accès à une carte SD ou à un disque dur est suffisant si ceux-ci ne sont pas **chiffrés**.

Il est tout aussi important de protéger les données par chiffrement que le matériel lui même.

## Le personnel

Le personnel lui-même est une faille de sécurité. En effet, si celui-ci n'est pas correctement informé et formé à la sensibilité des données de l'entreprise qu'il détient, il peut inconsciemment divulguer des informations.

De même un salarié peut décider de lui même de **divulguer des informations** concernant l'entreprise, qu'il en fasse encore partie ou non.

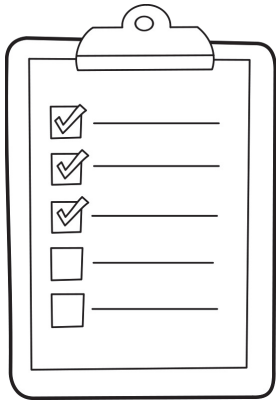
De plus, certaines entreprises mènent des activités d'**espionnage industriel**, et visent directement des membres du personnel. Un accès à des données confidentielles est alors plus facile si elles peuvent être compromises en dehors des heures de travail.

## Privilèges des applications

Lors de l'installation d'une application via les boutiques d'applications officielles, les applications peuvent demander certains **privilèges** à l'utilisateur.

Mais il est tout à fait possible que ces dernières demandent des privilèges beaucoup trop étendus compte tenu de l'utilisation qui en est prévue. Ces privilèges concernent par exemple les accès à la webcam, aux contacts, aux données de l'agenda, aux informations d'appels, aux périphériques de stockage...

Malheureusement, la plupart des **utilisateurs ne font pas attention** à ces demandes et valident toutes les demandes d'accès au mépris de la sécurité de leurs données.



## Charte informatique spécifique au BYOD

Pour limiter les risques liés au BYOD et se protéger vis-à-vis de la loi, l'entreprise se doit mettre en place une charte informatique dédiée au BYOD.

Celle-ci doit comporter de façon précise les différentes obligations et autorisations du salarié.

Il est nécessaire que cette charte comporte certains éléments, comme :

- des **conditions de sécurités** du matériel au salarié (antivirus, protection matérielle des terminaux contre le vol…) ;
- la **propriété des données** professionnelles contenues dans le matériel personnel (au cours de l'exécution du contrat de travail et à son terme.) ;
- d'établir précisément ce qui relève de la vie privée ou de la vie professionnelle du salarié ;
- de préciser les **modalités de contrôle** et les sanctions encourues.

## Virtualisation

Mettre en place un système de virtualisation, permettent de déployer des applications et des données **indépendamment** du système d'exploitation de l'appareil. Cela permet aussi d'**homogénéiser les OS** et d'être sûre de ne pas avoir de problèmes de **compatibilités** entre les différentes applications et les appareils .

Le fait de créer une machine virtuelle sur le matériel permet aussi de créer une «cloison » entre la partie personnelle et la partie professionnelle.

L'idéal serait de créer une machine virtuelle chiffrée.

## Conteneurs chiffrés

Les conteneurs se mettent en place sur des appareils tels que téléphones ou tablettes. L'avantage des conteneurs est de séparer nettement la partie privée de la partie professionnelle, ce qui permet d'effacer l'un sans toucher l'autre.

Cependant, si l'utilisateur à rooté ou jailbreaké son téléphone ou tablette alors le conteneur devient inutile : en effet, l'utilisateur peut transférer des documents professionnels sur sa partie privée.

## Mobile Device Management

Un Mobile Device Management (MDM) est un logiciel de gestion d'appareils mobiles. Il se compose d'une partie serveur et bien souvent d'une partie client (agent installé sur l'appareil à gérer).

Il permet de **configurer automatiquement** le matériel pour accéder aux différentes parties du réseau de l'entreprise.

Ce système **protège les données** du terminal pour éviter la perte, le vol ou la compromission des données et propose différentes solutions pour protéger les données :

- l'effacement des données à distance en cas de perte ou de vol du périphérique
- le chiffrement de la mémoire de masse
- des containers chiffrés
- un système d'échange de clé
- utilisation de certificats

# Conclusion

Le phénomène BYOD est devenu incontournable. Que l'entreprise adhère ou non à cette pratique, elle ne doit pas négliger la sécurité de son parc informatique.

Les risques encourus trouvent progressivement des solutions technologiques et organisationnelles, que celles-ci soient inclusent dans les appareils et systèmes d'exploitation ou fournies par des éditeurs tiers.

Cependant, il est évident qu'aujourd'hui une stratégie BYOD n'offre pas une sécurité aussi importante qu'une infrastructure normalisée et qu'il est plus judicieux pour une entreprise d'attendre que des solutions fiables et prouvées soient mises en place avec plus de recul.

De plus l'ANSSI (Agence Nationale de la Sécurité des Systèmes de l'Information) a encouragé les entreprises à ne pas mettre en place stratégies BYOD.

# Sources


INTERNET :

- ➔ www.openclipart.org/
- ➔ www.wikipedia.org/
- ➔ http://www.zdnet.com/five-security-risks-of-moving-data-in-byod-era-7000010665/ /
- ➔ http://www.businesszone.co.uk/blogs/scott-drayton/optimus-sourcing/advantages-and-disadvantages-byod /
- ➔ http://www.crn.com/slide-shows/security/240157796/top-10-byod-risks-facing-the-enterprise.htm /
- ➔ http://www.ey.com/GL/en/Services/Advisory/Bring-your-own-device---mobile-security-and-risk /
- ➔ http://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards /
- ➔ http://pro.01net.com/editorial/599687/mobiles-et-pc-perso-au-bureau-complique-mais-ineluctable/
- ➔ http://www.securite-informatique.gouv.fr/gp_article96.html
- ➔ http://www.lepoint.fr/high-tech-internet/pourquoi-il-est-dangereux-de-se-connecter-sur-les-reseaux-wi-fi-publics-18-07-2013-1706086_47.php//
- ➔ http://forums.cnetfrance.fr/topic/1205381-que-risque-t-on-a-se-connecter-au-wifi-public/

MAGAZINE :

- ➔ MISC n°66 Mars/Avril 2013