PAR
**ERIC FREUDENREICH**
CHARGÉ D'ENSEIGNEMENT, UNIVERSITÉ PARIS-DAUPHINE, MEMBRE DU CA DE L'INSTITUT DES DIPLÔMÉS D'EXPERTISE COMPTABLE EN ENTREPRISE (ECE)

PAR
**SARAH LETIZIA**
DIPLÔMÉE DU MASTER 2 CCA, UNIVERSITÉ PARIS-DAUPHINE, EXPERT-COMPTABLE STAGIAIRE

# Terminaux nomades **Dix leviers pour renforcer la securité**

Les ordinateurs portables, les smartphones et les tablettes permettent un gain de productivité grâce à une meilleure flexibilité du travail : les salariés peuvent accéder au réseau de l'entreprise pour travailler n'importe où, n'importe quand et grâce à n'importe quel outil. La multiplication de ces terminaux nomades impacte la sécurité des systèmes d'information (SI). Comment renforcer la sécurité face aux menaces cybercriminelles ?

Le « *blurring*[1] », la génération Y ou la multiplication des points d'accès expliquent l'inévitable développement de l'utilisation des terminaux mobiles dans l'entreprise organisée de trois manières : classique, *Byod* ou *Cope*.

## ÊTES-VOUS CLASSIQUE, *BYOD* OU *COPE* ?

Traditionnellement, l'entreprise fournit au salarié un équipement pour l'utiliser dans le cadre de son travail. Dans ce mode d'organisation classique, les outils, la sécurisation du terminal et les abonnements sont à la charge de l'entreprise.

À l'inverse, un nombre croissant d'employés utilise du matériel personnel dans le cadre professionnel. Ce phénomène est appelé « *Bring Your Own Device* » (*Byod*). Il en résulte une flotte tellement hétérogène que la responsabilité de la sécurisation du terminal est transférée au salarié, qui ignore souvent les problématiques de sécurité[2]. En outre, le *Byod* accroît forcément le « *blurring* », tout en rendant complexe l'appréciation du temps de travail. Enfin le *Byod* pose des questions de responsabilité et de propriété : quid des données professionnelles stockées sur le matériel personnel ou de la responsabilité en cas d'incident avec le terminal ?

Face à l'obsolescence de l'approche classique et aux risques liés au *Byod*, des entreprises adoptent le *Cope* (*Corporate Owned, Personnaly Enabled*). Le matériel est détenu par l'entreprise, mais le salarié est autorisé à l'utiliser et à télécharger des applications à titre personnel. L'entreprise peut déconnecter les périphériques du réseau de l'entreprise en cas d'intrusion. Au départ du salarié, l'équipement revient à l'entreprise et les données sont détruites. En revanche, le *Cope* inquiète parfois les salariés dans la mesure où leurs données sont accessibles pour l'entreprise.

## DES MENACES PLUS SPÉCIFIQUES AUX TERMINAUX NOMADES

Certaines menaces comme le *malware*, l'interception de données ou le vol, sont plus spécifiques aux terminaux mobiles.

Lors d'une connexion à distance via des réseaux publics et même privés, il y a un risque élevé d'interception des données. Par exemple, l'équipement « *WiFi Pineapple*[3] » peut détourner un réseau WiFi en empruntant son SSID (*Service Set Identifier*).

De par leur petite taille, les terminaux nomades sont aussi faciles à perdre qu'à voler. Leur disparition peut s'accompagner non seulement d'un vol des informations stockées, mais aussi être suivie d'une intrusion dans les SI de l'entreprise.

## LA GOUVERNANCE EN PRÉVENTION DES CYBER-ATTAQUES

Une recherche qualitative récente[4] fait ressortir que certains secteurs d'activités sont plus sensibles que d'autres[5] et que l'exposition des entreprises est proportionnelle à leur position sur un marché ainsi qu'à la concentration de celui-ci. Comme l'indique le « *Rapport sur les menaces à la sécurité mobile* » établi par Sophos en 2014, « *l'explosion des smartphones et des tablettes [...] a inévitablement abouti à une hausse de la cybercriminalité sur ce type d'équipement* ». D'après Olivier Buquen, « *la prévention est très importante, [car] elle permet d'éviter 80% des attaques*[6] ».

La sécurité du SI relevant de la gouvernance, nous préconiserons essentiellement des leviers organisationnels pour la renforcer autour de trois axes : la prise de conscience, la proactivité et la politique de mobilité.

## PRENDRE CONSCIENCE DES MENACES CYBERCRIMINELLES

### Les outils d'aide à la décision

Une représentation graphique de l'exposition au risque de cyber-espionnage (*cf. infra*) est un outil susceptible de favoriser une prise de conscience. Celle-ci s'accroit encore lorsque des failles de sécurité font l'objet d'une veille et que des fiches d'incident sont établies sans délai. Ces fiches communiquées aux dirigeants proposent des moyens préventifs pour faciliter et acter la prise de décision au plus haut niveau de l'entreprise.

### Rendre les utilisateurs acteurs de la sécurité

Une initiative consiste à donner aux utilisateurs les moyens d'alerter la DSI (Direction des SI), par email ou hotline, par exemple, en cas de fort ralentissement de la connexion susceptible d'être causé par une intrusion. Devenus acteurs de la sécurité, les utilisateurs sont plus enclin à respecter des règles préventives.

### Rendre les actions de sensibilisation interactives

Le marketing de la sécurité des SI passe par une sensibilisation interactive. L'attention sera portée sur des illustrations par analogie avec la vie privée et sur l'atteinte aux données personnelles. Une démonstration « choc » avec un Wifi *Pineapple* stimulera encore plus l'interactivité.

### Évaluer la performance des actions de sensibilisation

Il peut être intéressant pour l'entreprise de faire, quelques mois après une action de sensibilisation ayant porté sur ce thème, une analyse sur la force moyenne des mots de passe et d'en communiquer les résultats.

## LA PROACTIVITÉ

### Intégrer la sécurité au plus près des équipes métiers

Les RSSI (Responsables de la Sécurité des SI) sont généralement rattachés à la DSI. Pour mieux répondre aux besoins, la DSI doit se rapprocher des équipes métiers *via* un réseau de correspondants, par exemple.

### De la réactivité à la pro-activité

De manière proactive, la méthode d'intelligence économique, l'OSINT (*Open Source Intelligence*) peut être utilisée pour analyser les menaces et mieux les prévenir. Elle consiste à faire des recherches à partir de sources publiques et légales. Les informations obtenues sont sans intérêt jusqu'à leur compilation.

### Utiliser les bonnes pratiques

Au-delà des référentiels globaux ITIL ou CobiT et de la norme ISO 27000, les entreprises peuvent utiliser les méthodes ou supports (e-learning, fiches, jeux) mis à disposition dans le portail gouvernemental de la sécurité informatique[7].

## CADRER LA POLITIQUE DE MOBILITÉ

### Strictement encadrer le *Byod*

Même en perte de vitesse, le *Byod* doit être strictement encadré par des procédures d'agrément de matériel, de revue des problématiques d'accès et de compétences, ou de devoirs pour les utilisateurs.

### Utiliser un logiciel de gestion de la flotte

Le Management du Matériel Mobile (« *Mobile Device Management* ») est un outil de centralisation de la gestion de la flotte qui peut notamment bloquer un terminal et supprimer toutes ses données à distance.

Alors que les entreprises ne se sentent pas davantage exposées à la cybercriminalité par la diffusion des terminaux nomades, le catalogue d'applications professionnelles s'étoffe et la demande des utilisateurs qui apprécient leur convivialité et leur ergonomie est croissante. Ils contiennent des informations toujours plus sensibles (notamment financières ou commerciales) dont la fiabilité et l'intégrité sont susceptibles de ne plus être assurées. Il est temps d'actionner les leviers ! ●

**1.** Dans le M, le magazine du Monde de novembre 2013, Didier Pourquery dans le billet intitulé « *Juste un mot... Blurring*» cite l'étude menée mi-2013 par Pullman et IPSOS: «*Ce* blurring, *ou confusion progressive des activités professionnelles et personnelles, est un phénomène mondial, décrit et reconnu dans toutes les sociétés explorées.*»

**2.** Selon le rapport sur la cybercriminalité mené par Norton en 2012, 44% des interrogés ne savent pas qu'il existe des solutions pour sécuriser les mobiles.

**3.** Ndlr : peu onéreux, facile à obtenir et à utiliser.

**4.** Etude empirique réalisée par Sarah Letizia entre 2013 et 2014 dans le cadre de son mémoire de Master 2 Comptabilité Contrôle Audit, « *Cybersécurité et terminaux nomades : la sécurité du système d'information sous pression* » , sous le tutorat d'Eric Freudenreich et en lien avec le cours «Fraudes contrôle gouvernance - Fraud examination» associé à l'ACFE Higher Education Partnership. Le panel est composé de spécialistes d'ATOS, BSSI, EDF, Grant Thornton, KPMG, SANOFI, Schneider, SNCF, Thales, et Vallourec

**5.** Cf. Douze secteurs d'activités d'importance vitale : http://www.sgdsn.gouv.fr/site_rubrique70.html .

**6.** La légitime défense économique des entreprises, Sécurité & Stratégie, janvier/mai 2012.

**7** Lien : http://www.securite-informatique.gouv.fr/