

INSTITUT SUPERIEUR DE COMMERCE

Centre des Recherches Interdisciplinaires
de Gestion et Développement

« CRIGED »



Revue Congolaise de Gestion et le Développement
Volume n°22, Septembre 2021

DEVELOPPEMENT D'UN SYSTEME DE SECURITE DANS UNE ENTREPRISE BASE SUR LE PRINCIPE DU BRING YOUR OWN DEVICE (BYOD).

Par

IPASHA NGAPEMBE NYAMI Fortunat Fortus

Assistant 2/ ISP SUD-BANGA

Téléphone : +243 82 34 32 302 / 97 12 49 549

Email : ipashangapembenyami@gmail.com

Résumé

A l'ère de la mobilité, l'effectif moderne s'attend à pouvoir travailler n'importe où et en tout temps, en plus d'accéder aux ressources et aux données d'entreprise sur n'importe quelle plateforme depuis l'arrivée et le succès de l'Internet. Ce phénomène est baptisé BYOD pour Bring Your Own Device du français « apportez votre appareil personnel ». De nos jours, la plupart des grandes entreprises comprennent la valeur de ce modèle, mais sont préoccupées par la perte ou le vol de données de l'entreprise.

Pour réduire la menace à un niveau tolérable, les services informatiques d'entreprises devraient adopter une stratégie globale de « défense en profondeur ». Cette dernière touche l'utilisateur, l'appareil, le réseau, le serveur du centre de traitement des données et les piles d'applications qu'il utilise. Chacun des maillons de la chaîne présente un ensemble distinct de vulnérabilités qui requièrent des stratégies précises pour réduire la surface de menace.

Pour déployer un système de sécurité pour le BYOD, nous avons besoin de deux environnements nécessaires dont l'environnement matériel et logiciel. Dans l'environnement matériel, il est demandé à l'entreprise d'identifier les besoins de personnels pour l'entreprise tout en identifiant le nombre des équipements mobiles pour permettre sa bonne gestion. En ce qui concerne l'environnement logiciel, nous recommandons aux entreprises de choisir une solution de gestion de terminaux mobiles (de l'anglais Mobile Device Management, MDM) répondant à leurs exigences et recommandations pour être déployé.

La gestion des terminaux mobiles va permettre à une entreprise de développer un système de sécurité incluant les équipements mobiles personnels pour permettre à s'assurer le contrôle complet de son système d'information, la gestion des ses données et la situation sécuritaire de l'ensemble de son parc informatique.

0. Introduction

Depuis quelques décennies, les nouvelles technologies de l'information et de la communication ont un grand apport dans la croissance des entreprises. Les équipements mobiles, les applications et les formes d'accès transforment les modes d'interaction entre les entreprises et leurs clients, employés et partenaires. Partout dans le monde, elles utilisent des capacités mobiles de plus en plus étendues pour bénéficier de nouvelles opportunités et transformer leur business model tout en développant en parallèle les capacités existantes pour pouvoir y accéder partout et à tout moment. Le monde de l'entreprise a depuis longtemps misé sur ces technologies, mettant en œuvre des applications mobiles issues des besoins précis et significatifs. L'environnement professionnel est en train de changer chaque instant ; prendre place sur une chaise pour travailler a pris fin et le monde entier est devenu un lieu de travail. Maintenant les travailleurs peuvent collaborer à n'importe quel temps, travaillé à n'importe quel endroit tout en prenant d'énormes décisions.

Depuis l'arrivée de l'Internet et son succès, la nécessité de créer une continuité d'accès depuis des terminaux mobiles n'a fait que s'accroître, du fait de l'intérêt à disposer de tous types d'information depuis n'importe où, voire d'accéder à son propre système d'information sur n'importe quel périphérique. Aujourd'hui, il est pressenti par tout employé de vouloir utiliser son propre équipement ou son propre terminal mobile pour travailler dans l'environnement professionnel ; ce phénomène est baptisé BYOD pour Bring Your Own Device du français « apportez votre appareil personnel ». Cet outil fait bouger les lignes de la mobilité d'entreprise. Pour les entreprises, devenir mobile signifie cesser d'évoluer d'un modèle monolithique, centré sur le bureau et fournissant l'accès aux informations, vers un modèle de plus en plus décentralisé. Dans un environnement mobile, on doit garder à l'esprit que le fait de faciliter la mobilité des employés peut être un bon moyen pour améliorer la performance dans l'entreprise et la satisfaction de ces derniers au travail.

Cependant, si cela est mal aménagé, la mobilité de l'employé peut parfois engendrer un sentiment de mal être et créer une rupture entre l'employé, ses collègues et l'entreprise. C'est pourquoi le travail à distance ne devrait jamais se substituer complètement à celui du bureau mais doit plutôt au contraire, donner à l'employé la possibilité de travailler n'importe où et quand il le veut. Dans un modèle décentralisé, les employés doivent pouvoir accéder aux informations et aux ressources de l'entreprise n'importe où et à n'importe quel moment avec leurs propres équipements. Puisque les informations de l'entreprise sont accessibles à partir de n'importe quel endroit, à partir de

n'importe quel périphérique notamment dans les lieux publics, et stockées sur des périphériques se situant en dehors des limites du réseau de l'entreprise, le cœur de métier de la compagnie devient alors plus vulnérable.

Face à ces nouvelles problématiques, il est nécessaire de mener une réflexion dont l'objectif est de proposer des architectures nouvelles de gestion de systèmes d'information, mieux adaptées aux environnements mobiles dans une entreprise. Nous avons trouvé intérêt à entreprendre notre étude sur le développement d'un système de sécurité dans une entreprise basé sur le principe de Bring Your Own Device, du français « apportez votre appareil personnel ». Avec l'introduction des appareils mobiles personnels au sein du système d'information, comment l'entreprise arrivera-t-elle à gérer et à sécuriser son parc informatique ?

L'objectif général de cette étude est de permettre à une entreprise de développer un système de sécurité incluant les équipements mobiles personnels pour permettre à s'assurer le contrôle complet de son système d'information, la gestion des données et la situation sécuritaire de l'ensemble du parc informatique.

0.0. Méthodologie

Tout travail scientifique s'annonce en suivant des méthodes qui mettront son acheminement afin d'atteindre l'objectif fixé. Dans le cadre de notre travail, nous avons utilisé des méthodes d'analyse scientifique et descriptive complétées par une technique documentaire pour nous permettre de récolter les différentes données dans des articles, ouvrages, mémoires, Emission TV, site web et autres sources scientifiques susceptibles de nous fournir plus d'éléments jugés nécessaires. En outre de cela, nous nous sommes également servis de la technique d'interview pour compléter quelques informations se rapportant à notre travail.

1. Considérations générales sur le BYOD

1.1. Historique

En raison de la complexité de l'écosystème mobile d'entreprise, il s'avère essentiel de bien maîtriser cet environnement avant d'établir une approche complète en matière de sécurité. L'environnement mobile a pris de l'ampleur dans le monde actuel par l'introduction et l'envahissement du marché par des équipements mobiles dont notamment les ordinateurs portables, les tablettes, les smartphones, les téléphones mobiles, etc.

Le téléphone mobile est le résultat de différentes technologies qui existaient déjà, pour la plupart, dans les années 1940. Son invention est attribuée au docteur Martin Cooper, directeur de la recherche et du développement chez Motorola qui en a fait la démonstration dans les rues de New-York le 3 avril 1973. Le premier

téléphone mobile commercial, conçu par Motorola est lancé le 6 mars 1983 aux États-Unis : le Motorola DynaTac 800051.

L'usage du téléphone mobile s'est progressivement démocratisé, notamment vers la fin des années 1990. Le taux de pénétration du mobile dans le monde à cette époque est de 0,6 abonnements pour 100 habitants. La fin des années 2000 a été marquée par une hausse fulgurante de la popularité des smartphones dans l'entreprise, suivie par la tablette dès 2010. Aujourd'hui, les tablettes réussissent là où les Netbooks ont échoué, en offrant une alternative plus "mobile" aux ordinateurs portables. Depuis les années 2010, la majorité des téléphones mobiles dispose de nombreuses fonctions supplémentaires, rendues possibles grâce à l'intégration d'un système d'exploitation évolué dans le téléphone : ce sont les smartphones ou téléphones intelligents².

L'origine de l'expression est par analogie avec l'expression anglaise BYOB (Bring Your Own Bottle) des années 1950. Ce mot dit BYOD a été mentionné pour la première fois en 2005 dans un livre rédigé par Ballagas et al. A UBICOMP 2005. C'est en 2007 avec la sortie des iPhones d'Apple que le phénomène BYOD a eu de l'ampleur dans le milieu professionnel par le fait que les employés de l'entreprise pouvaient recevoir et consulter des emails à partir de leurs Smartphones. En 2009, le BYOD est définitivement vulgarisé avec l'autorisation d'Intel qui a remarqué une tendance croissante chez les employés à apporter leur appareil personnel pour travailler et ainsi se connecter au réseau d'entreprise. Ce mouvement a émergé maintenant sur les tablettes et les ordinateurs portables³.

1.2. Définitions de termes

- ✚ BYOD, « Bring Your Own Device » du français « apportez vos appareils personnels », est une tendance qui consiste à offrir aux utilisateurs finaux la liberté d'utiliser leurs propres outils pour accéder aux informations et communiquer au sein d'une entreprise, d'une université, école..⁴ ;
- ✚ Système(Entreprise) est un ensemble des moyens matériels, financiers, humains en interaction dynamique, structuré, organisé, poursuivant un but en fonction des objectifs prédéfinis.
- ✚ Smartphone ou téléphone intelligent, est un téléphone mobile évolué disposant des fonctions d'un assistant numérique personnel, et d'un ordinateur portable, il offre les fonctions d'accès Internet ;
- ✚ Tablette électronique est un petit appareil portatif doté d'une interface avec un écran tactile, qui offre de nombreuses possibilités de personnalisation, comprend

¹[https://fr.wikipedia.org/Telephone mobile—Wikipédia.html](https://fr.wikipedia.org/Telephone%20mobile). Consulté le 10 septembre 2015.

² Idem

³[https://fr.wikipedia.org/Bring_your_own_device.html](https://fr.wikipedia.org/Bring_your_own_device). Consulté le 03 septembre 2015.

⁴www.netacad.com/ccna1/explorateur du réseau.html. Consulté le 15 septembre 2015.

plusieurs applications et permet l'accès à l'internet, et dont les fonctionnalités se rapprochent souvent de l'ordinateur de bureau ;

- ✚ Internet mobile : accès à Internet sans fil via des moyens de communication comme le téléphone portable, le Smartphone ou la tablette numérique ;
- ✚ Terminal mobile petit appareil informatique ou de communication que l'on peut transporter avec soi dans ses déplacements et utiliser comme terminal donnant accès sans fil à un ou plusieurs réseaux ;
- ✚ PDA, assistant personnel numérique est un petit ordinateur de poche, principalement destiné à l'amélioration de la productivité personnelle ; gestion des contacts et de l'agenda, liste de tâches à faire, calculatrice ;
- ✚ MDM, Mobile Device Management du français Gestion des appareils mobiles, Solution basée sur le Cloud permettant à une entreprise d'étendre la protection de ses réseaux en prenant un contrôle actif et conséquent de la gestion des équipements mobiles ;
- ✚ Netbook : ordinateur portable, destiné principalement à la navigation sur Internet ;
- ✚ Télétravail : Mode de travail pratiqué à distance d'un lieu centralisateur, et dont la mise en œuvre nécessite des outils de télécommunication (fax, ordinateur connecté à un réseau, Smartphone, tablette, etc.)⁵.

2 : Système d'information et réseau informatique

Apparue dans les années 1970, l'entreprise était considérée comme un système donc un ensemble d'éléments en interaction dynamique, organisé en fonction d'un but. Les entreprises connaissent, depuis lors, la place déterminante de l'information et son rôle critique dans leur fonctionnement. Elles lui ont consacré, de manière plus ou moins explicite leur attention et des investissements croissants pour maîtriser sa gestion et sa sécurité. A mesure que les technologies informatiques se diversifient et se diffusent, en dehors de l'information, le système d'information est devenu pour les organisations, la préoccupation principale. Il y a trois grandes étapes qui ont marquées l'évolution du système d'information dont chacune d'elle indique l'importante extension de la transformation du concept⁶.

La Structure organisationnelle d'un système dans une entreprise est organisée en sous-systèmes dont le système pilotage dit système décisionnel, le système opérant exécutant les tâches selon le besoin des utilisateurs du système de

⁵https://fr.wikipedia.org/Nomadisme_numérique—Wikipédia.html. Consulté le 10 septembre 2015.

⁶Benci G., Foucaut O., Rolland C., *conception de système d'information. La méthode Rémora*, Éd Eyrolles, 1988, p.5.

pilotage et le système d'information constituant l'ensemble des informations internes et externes circulant dans l'entreprise⁷.

2.1. Système d'information

Un système d'information est l'ensemble des ressources (matériels, logiciels, données, procédures, humains, ...) structurés pour acquérir, traiter, mémoriser, transmettre et rendre disponible l'information (sous forme de données, textes, sons, images,...) dans et entre les organisations⁸.

Par système d'information d'une entreprise, on entend un ensemble organisé d'éléments qui permet de regrouper, classier, traiter et diffuser l'information au sein d'une entreprise. Ce dernier traverse toutes les couches de l'entreprise du niveau technique jusqu'aux données utilisateurs en passant par les métiers, les applications, les composants fonctionnels et les processus (employés). Il coordonne grâce à l'information les activités de l'organisation et lui permet ainsi d'atteindre ses objectifs grâce un ensemble d'éléments participant à la gestion, et au traitement de l'information à son sein.

Tout système d'information a son cycle de vie qui est caractérisé par les principales phases dont la conception, réalisation, d'exploitation-vieillessement, maintenance et la continuité du bon fonctionnement. Le cycle de vie d'un système d'information commence au moment où l'entreprise décide d'entreprendre le nouveau système.

Développer un système d'information, c'est mener un ensemble d'activités complexes et variées de décisions et de planifications, d'analyse de la réalité et de recueil de besoins informationnels, de conception et d'évaluation de système, de réalisation, de tests, de mise en orientation et des contrôles de qualité qui aboutissent à faire passer le système d'information d'une situation initiale de profit à une situation finale du système concret et opérationnel. Le travail du concepteur du système d'information est analogue au travail de l'architecte, il définit le futur système d'information et décide de la solution technologique avec préparation de tâches de réalisation.

Le processus de développement d'un système d'information s'organise globalement en deux phases, la première phase celle de conception qui aboutit à la spécification du système d'information sous la forme d'un schéma et une grande phase de réalisation, qui conduit à la fabrication effective du système d'information.

⁷ Foucaut O., & al, *Conception des SI et programmation événementielle*, Inter Editions, Paris, 1996, p.15.

⁸ Robert Reix, *Systèmes d'information et management des organisations*, Éditions Vuibert, Paris, 1995, p. 367

2.1.1. Méthodes de conception d'un système d'information

Pour mettre en place un bon système d'information, la méthode de conception s'avère nécessaire afin d'évaluer la complexité du problème à résoudre, entrer en relation d'échanges entre participants de la mise en place du système d'information, savoir si le système en place satisfait les besoins du gestionnaire et juger son efficacité sur le plan technique, augmenter le gain de productivité, réduire le coût et les qualités des activités du développement.

Aujourd'hui toutes les entreprises ont reconnu l'obligation d'utiliser la méthode de conception. Pour ce, le concepteur doit mettre en place les modèles statiques représentatifs du système d'information de l'entreprise. Ces derniers doivent décrire de façon formelle les données qui seront utilisées par le système d'information, avec un ensemble de règles et de signes utilisés pour élaborer un programme destinés à donner des ordres à l'ordinateur et les outils nécessaires (logiciels) qui permettront à effectuer le travail de conception, modélisation et la réalisation de la démarche. Les méthodes les plus utilisées sont MERISE et UML⁹.

2.1.2. Qualité et typologie d'un système d'information

Ayant pour rôle de traiter, de stocker, de diffuser, de communiquer les informations et de tenir compte des valeurs ajoutées à celles-ci, tout système d'information devra avoir la rapidité, la facilité d'accès, la fiabilité, l'intégrité, la pertinence, la sécurité et la confidentialité des informations en son sein¹⁰.

On distingue deux grandes familles de système d'information dont le système d'information de production dans lequel l'information est destinée au système opérant de l'entreprise et le système d'information opérationnel dont l'information de représentation et de coordination de l'activité du système opérant est destinée au sous-système de régulation dans le système de pilotage pour la prise de décision¹¹.

2.1.3. Evolution des systèmes d'information

Aujourd'hui on parle de systèmes d'information mobile par l'avènement de BYOD, de virtualisation des données et du Cloud computing. Avec toutes ces tendances, nous avons constatés un changement total dans la gestion et fonctionnement de système d'information. Au départ, ces derniers étaient physiques, statiques, mais actuellement ils deviennent mobiles et l'accès aux données peut se faire de n'importe où, à tout moment et sur n'importe quel périphérique grâce aux technologies mobiles. On est passé de l'automatisation des tâches administratives aux systèmes d'information d'aide à la décision, aux systèmes d'information de gestion de

⁹Benci G., Foucaut O. Rolland C, *Op. cit.*, p.12.

¹⁰ Idem

¹¹ MVIBUDULU K., *Méthode d'analyse informatique I*, G2 INFO/U.KA. 2007 - 2008

ressources humaines et aux systèmes d'information géographiques pour la récolte de données géographiques¹².

2.2. Réseau Informatique

Un réseau informatique peut être défini comme un ensemble d'équipements reliés entre eux pour échanger des informations. Un réseau en général est le résultat de la connexion de plusieurs machines entre elles, afin que les utilisateurs et les applications qui fonctionnent sur ces dernières puissent échanger des informations¹³.

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que des stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques et aujourd'hui il y a l'intégration de la parole téléphonique et de la vidéo dans les réseaux informatiques¹⁴.

2.2.1. Avantages de Réseaux Informatiques

Les avantages de la mise en réseau d'ordinateurs et d'autres périphériques incluent la réduction des coûts et une amélioration de la productivité. Dans un réseau, les ressources peuvent être partagées pour éviter d'endommager ou de dupliquer les données. Les principaux avantages d'un réseau informatique sont la diminution de périphériques, l'amélioration de fonctionnalités de communication, la non-duplication des données, la réduction de coût de licence, la protection et l'administration centralisée de données¹⁵.

2.2.2. Caractéristiques des réseaux informatiques

Les caractéristiques d'un bon réseau informatique sont l'extensibilité, la disponibilité, la facilité de gestion et la sécurité. Alors que les réseaux évoluent, nous découvrons que les architectures sous-jacentes doivent prendre en considération quatre caractéristiques de base si elles veulent répondre aux attentes des utilisateurs dont notamment la tolérance aux pannes, l'évolutivité, la qualité de service et la sécurité de l'infrastructure réseau et la protection des données¹⁶.

¹² <http://youtube.com/Panorama sur la sécurité des systèmes d'information>, Consulté le 20 Septembre 2015

¹³ X. Carcelle, *Réseaux CPL par la pratique : Avec trois études de cas : réseau domestique, réseau d'entreprise et réseau de desserte de collectivité locale*, Ed. Eyrolles, Paris Cedex, 2006, P.24.

¹⁴ http://netacad.com/course-assets/a_la_decouverte_du_reseau.html, Consulté le 10 septembre 2015

¹⁵ G. Pujolle, *Les Réseaux 5^e édition*, Ed. Eyrolles, Paris Cedex, 2006, P.7.

¹⁶ http://static-course-assets.s3.amazonaws.com/exploration_reseau.html, Consulté le 10 septembre 2015

2.2.3. Types de Réseau informatique

Tout le monde utilise les réseaux suivants dans la vie quotidienne dont notamment : le Réseau postal, Réseau téléphonique, Réseau de transports publics, Réseau informatique d'entreprise, Réseau social, Internet, etc. Les deux types les plus courants d'infrastructure réseau sont réseaux locaux et réseaux étendus.

Un réseau local, ou LAN (Local Area Network de l'anglais) est une infrastructure réseau qui couvre une zone peu étendue. Les réseaux locaux, correspondent par leur taille aux réseaux intra-entreprises. Ils servent au transport de toutes les informations numériques de l'entreprise.

Un réseau étendu, ou WAN (Wide Area Network de l'anglais) est une infrastructure réseau qui couvre une zone étendue. Les réseaux étendus sont généralement gérés par des fournisseurs de services ou des fournisseurs d'accès Internet. Ils sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise en ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellite¹⁷.

Bien qu'il existe des avantages à utiliser un réseau LAN ou WAN, la plupart des utilisateurs doivent communiquer avec des ressources situées sur un autre réseau, en dehors du réseau local du domicile, du campus ou de l'entreprise effectué via Internet. L'Internet est un ensemble mondial de réseaux interconnectés qui coopèrent pour échanger des informations en utilisant des normes courantes. Les files téléphoniques, fibres optiques, transmissions sans fil et liaisons satellites permettent aux utilisateurs d'Internet d'échanger des informations sous diverses formes¹⁸.

2.2.4. Architecture et composants d'un Réseau informatique

L'architecture d'un réseau informatique repose sur la manière dont les données sont stockées dans son infrastructure. Nous pouvons distinguer deux types d'architecture dont le Point à point et le client-serveur.

Dans un réseau point à point, il n'y a pas de serveur dédié entre les ordinateurs. Chaque périphérique possède des fonctionnalités et responsabilités équivalentes donc responsable de ses propres ressources et peut décider quelles données et quels périphériques partager ou installer. De ce fait, il n'existe aucun point central de contrôle ou d'administration du réseau. Ses inconvénients sont le manque d'administration centralisée, pas de sécurité centralisée, pas forcément de stockage

¹⁷ PUJOLLEG., *Op. cit.*, p.7.

¹⁸ Idem

commun et centralisé des données. La gestion des sauvegardes de données est séparée¹⁹.

Dans un réseau client-serveur, le client demande des informations ou des services au serveur et le serveur fournit les informations ou les services demandés par le client. Les serveurs de ce type de réseau réalisent généralement certaines tâches de traitement pour les postes clients. Les ressources sont contrôlées par une administration réseau centralisée²⁰.

L'infrastructure réseau comprend trois catégories de composants dont les périphériques, les supports de transmission (medias) et les services. Les périphériques et les supports sont les éléments physiques du réseau. Le matériel correspond souvent aux composants visibles de la plateforme réseau, par exemple un ordinateur portable, un ordinateur de bureau, un commutateur, un routeur, un point d'accès sans fil ou le câblage qui sert à relier les périphériques. Les composants réseau sont utilisés pour fournir des services et des processus et ceux-ci sont les programmes de communication appelés logiciels, qui sont exécutés sur les périphériques réseau²¹.

3 : Sécurité informatique dans une entreprise

Le système d'information est de nos jours au cœur de toutes les entreprises modernes. La sécurité informatique c'est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir et garantir la sécurité d'un système informatique²².

La mise en œuvre de la sécurité Informatique doit respecter quelques critères dont l'Intégrité, la confidentialité, la disponibilité, la non répudiation, et l'authentification à la base de données des personnes autorisées à avoir accès aux données par identification.

3.1. Enjeux et risques de la sécurité dans une entreprise

La sécurité informatique dans l'entreprise, c'est d'avoir la maîtrise parfaite de son SI tout en connaissant les aspects vu qu'un système d'information n'est jamais sécurisé dans toute sa globalité. Etant administrateur ou architecte du système d'information, on doit être capable de connaître ses faiblesses et les risques liés avec connaissance du système informatique.

¹⁹Carcelle X., *Op. cit.*, p.34.

²⁰PUJOLLE G., *Op. cit.*, p.764.

²¹Servin C., *Op. cit.*, P.30.

²²http://cybercrimactu.files.wordpress.com/concevoir_la_sécurité_informatique_en_entreprise.pdf. Consulté le 10 janvier 2016.

Nous pouvons classer les enjeux de la sécurité informatique dans l'entreprise en trois catégories dont notamment :

Les enjeux économiques

La nécessité de garantir sa sécurité, faire face à la concurrence et rester performante, pousse les entreprises à investir de plus en plus de moyens dans la sécurisation de leurs systèmes d'information et dans la qualité de service à fournir aux clients. La sécurité a un coût réel mais pour toute entreprise, il est recommandé d'investir dans le matériel, la formation sans faire pas en arrière parce qu'on peut perdre beaucoup plus que l'investissement qu'on aurait pu mettre au départ.

Les enjeux politiques

La plupart des systèmes d'information se référant aux documents officiels de sécurité élaborés par la plupart des Etats du monde, respectent et appliquent par toute structure engagée dans un processus de sécurisation du SI. Dans le cadre de cryptage ou chiffrement de données, chaque Etat définit des cadres et mesures d'utilisation des algorithmes de chiffrement et les recommande aux entreprises exerçant sur son territoire. Le non-respect de ces mesures et recommandations peut avoir des conséquences graves sur l'entreprise. A ce niveau, chaque Etat souhaite être capable de décrypter toutes les informations circulant dans son espace mais malheureusement que dans le cas de la RD Congo notre pays, il n'y a pas des règles de base en matière de sécurité de l'information établies par l'Etat²³.

Les enjeux juridiques

En cas d'incident informatique, la responsabilité civile et pénale de l'entreprise vis-à-vis d'autrui, des contractants, des clients, des partenaires, des autorités, des privés, etc., peut être engagée et peut avoir des répercussions très lourdes sur la vie de l'entreprise (paiement d'amendes, retrait d'autorisations, agréments, etc.). Des législations plus avancées en matière de cyber sécurité prévoient des sanctions très lourdes pour des entreprises dont le système mal sécurisé cause un préjudice aux utilisateurs de ses services²⁴.

Un risque permet de mesurer les possibilités à l'occurrence d'un événement, associé à une situation ou une activité. Dans le cas de la sécurité informatique en entreprise, il s'agit plutôt de ce que l'on peut perdre, en l'absence de moyens adéquats de sécurisation. Lorsque l'on évoque les risques susceptibles que peuvent engendrer un incident informatique sur le Système d'Information d'une

²³ [http://www.youtube.com/La protection des données personnelles.mp4](http://www.youtube.com/La%20protection%20des%20donn%C3%A9es%20personnelles.mp4). Consulté le 20 Septembre 2015.

²⁴ [http://cybercrimactu.files.wordpress.com/Concevoir la sécurité informatique en entreprise.pdf](http://cybercrimactu.files.wordpress.com/Concevoir_la_s%C3%A9curit%C3%A9_informatique_en_entreprise.pdf). Consulté le 10 janvier 2016.

entreprise, on distingue deux grandes catégories : les risques physiques et les risques logiques²⁵.

Les risques physiques

Les risques physiques sont toutes les atteintes physiques directes dont peut être victime un système d'information au cours de son cycle de vie. On les appelle également risques matériels, parce qu'ils ont trait à l'intégrité du matériel. Il s'agit entre autres d'événements tels que l'incendie, explosion, effondrement, dommages électriques, foudre, intempéries, vol, actes de vandalisme et la défaillance matérielle.

Les risques logiques

Avec le développement fulgurant de l'informatique distribuée et mobile par opposition à l'informatique centralisée, les données et les applications ont acquis une importance plus grande. En effet, l'on assiste à une migration progressive de la valeur du matériel vers la valeur des données et des applications. Le développement du Cloud Computing est l'une des illustrations les plus expressives de cette tendance. La question principale est de savoir comment évaluer et analyser la valeur de ce qui n'est pas physique, donc immatériel c'est-à-dire la donnée. C'est pour répondre à cette question que sont apparues les notions d'accident, d'erreur et de malveillance, directement issues des méthodes d'analyse des risques développées ces dernières années²⁶.

Les équipements mobiles sont le maillon faible de la chaîne de liaison et ses problématiques de sécurité font régulièrement la une des informations grand public. Les risques encourus par l'utilisation des terminaux personnels en entreprise sont révélateurs ²⁷:

- ✓ Perte ou vol d'informations : Le risque inhérent au facteur de forme de ces appareils est le vol ou la perte. En plus d'être le plus probable, c'est le plus dangereux. Le téléphone contient généralement tous les mails et les contacts de l'utilisateur, l'espace de stockage conserve les données sensibles et documents confidentiels, le terminal donne un accès privilégié au SI. La perte d'un appareil peut engendrer une réaction en chaîne dans les impacts de sécurité tombé entre de mauvaises mains, il peut avoir un effet dévastateur ;
- ✓ Défaillance et détérioration : Ces appareils sont relativement fragiles et, par conséquent, soumis à des défaillances techniques ou détériorations. En plus d'une immobilisation, voire d'un remplacement, qui peut être gênant, surtout pour un utilisateur VIP, le risque de perte de données existe. Il faut pouvoir retrouver

²⁵ <http://www.cgi.com/Assurer-la-securite-des-entreprises-mobiles-f.pdf>. Consulté le 10 Décembre 2015.

²⁶ [http://youtube.com/RSSIL- Introduction aux concepts de la sécurité informatique en entreprise.mp4](http://youtube.com/RSSIL-Introduction%20aux%20concepts%20de%20la%20s%C3%A9curit%C3%A9%20informatique%20en%20entreprise.mp4). Consulté le 20 Septembre 2015.

²⁷ Idem

et resynchroniser l'ensemble des données présentes (données stockées, configuration...);

- ✓ Utilisation illicite : L'ouverture des services de messagerie, de partage de documents et autres applications métiers habituellement cloisonnés sur internet incluent le risque d'accès illicite aux ressources et de divulgation d'informations. Le risque est d'autant plus grand qu'il est difficile de maîtriser la connectivité des terminaux ;
- ✓ Altération des données : Ce risque peut sembler anodin, mais il est fortement lié à la taille des terminaux et leur ergonomie. Les erreurs de saisie sur de petits claviers virtuels ou des erreurs de manipulation peuvent conduire à l'altération, voire la suppression de données sensibles de l'entreprise ;
- ✓ Intérêt des pirates : Chaque bond technologique est accompagné par les pirates et les cybercriminels ne tardent pas à s'y intéresser. La plupart des terminaux se connectent régulièrement avec un ordinateur classique pour synchroniser les contacts, effectuer une sauvegarde... Cette synchronisation est un vecteur de diffusion de malwares pour les pirates qui exploitent les faiblesses des terminaux ;
- ✓ Vers de nouveaux comportements : Avec l'apparition de Smartphone et la multitude des services qu'il présente, on voit apparaître de nouveaux comportements au près des employés. Les besoins des utilisateurs ayant changé, ils s'orientent massivement vers des appareils disposant de GPS, de multimédia. Ainsi, il devient de plus en plus difficile pour les responsables IT de résister aux sollicitations des employés.

3.2. Vulnérabilités & Menaces

Dans le monde de la sécurité IT, l'on croit trop souvent que les cybercriminels sont beaucoup plus ingénieux et savants que les professionnels assignés à la sécurisation des SI. Or, selon le célèbre hacker Kevin Mitnick¹², presque toutes les failles de haut niveau (critiques) sont le résultat d'une violation des processus métiers et/ou règles procédurales ou de l'ingénierie sociale, mais non le fait d'un savoir-faire technique exceptionnel²⁸.

L'être humain de par sa nature est vulnérable. La plupart des vulnérabilités humaines proviennent des erreurs (négligence, manque de compétences, surexploitation, etc.). Un système d'information étant composé des humains, convient d'assurer leur sécurité. Parmi les vulnérabilités, nous pouvons citer le stress au travail,

²⁸ [http://cksecurity.free.fr/hacking/securite hand-book.pdf](http://cksecurity.free.fr/hacking/securite%20hand-book.pdf). Consulté le 15 octobre 2014.

les conditions sociales, la santé physique, la fatigue, la non-satisfaction et d'autres événements de la vie, etc.

Avec la croissance exceptionnelle des outils informatiques dont notamment les équipements mobiles, les vulnérabilités technologiques sont découvertes tous les jours. Ces vulnérabilités sont dues au manque de contrôle l'employé sur les matériels, les processus et les applications composant le système d'information. Au niveau de l'organisation, les vulnérabilités sont dues à l'absence de charte à respecter, des procédures, et règles de base suffisamment détaillés pour faire face aux problèmes liés à la sécurité du système d'information. Actuellement, il existe plusieurs menaces à travers le monde provenant surtout de l'internet. Pour les entreprises, les menaces sont de deux sources de provenance dont à l'interne et l'externe. Selon les statistiques des experts, 80% de menaces proviennent de l'intérieur du système d'information alors que la plupart des entreprises investissent beaucoup moyens dans la sécurité interne.

La menace de l'intérieur est liée à l'utilisateur qui est l'employé. Avec la mobilité qui est devenue au fil du temps une véritable philosophie de vie dont notamment avec le phénomène BYOD faisant l'objet même de notre problématique, les employés peuvent avoir accès aux données de l'entreprise partout et à tout moment. Imaginons qu'un équipement d'un des employés infecté par un virus informatique qui prend le contrôle de son ordinateur ou équipement privé et ce dernier branché sur le serveur de l'entreprise infecte ce dernier et mettra les données de l'entreprise à la portée de pirates, hackers.

En considérant l'adoption massive des appareils mobiles, les entreprises font face à une grande variété de plateformes mobiles se connectant leurs ressources avec plus ou moins de contrôle. 60 % des entreprises déclarent ainsi accepter l'intégration des Smartphones personnels au sein de l'entreprise. Le Gain de productivité, amélioration de collaboration et plus grande rapidité des échanges, tels sont les arguments mis en avant par les entreprises pour faire accepter les Smartphones dans le monde professionnel. L'intégration des Smartphones au sein d'un système d'information menace pourtant directement la sécurité du système d'information.

Les Smartphones connectés au système d'information représentent un vecteur d'attaque supplémentaire utilisé par les cybercriminels et les pirates informatiques. La mobilité constitue pour les logiciels malveillants et la cybercriminalité un nouveau monde inexploré, objet de toutes les convoitises. Depuis cinq ans, le nombre total de virus informatiques visant les Smartphones est en forte augmentation suite au téléchargement des applications gratuites dans des boutiques en ligne telles que playstore de Google ou appstore de Apple.

A l'externe, la plupart des menaces sont des attaques effectuées au quotidien par des pirates informatiques, hackers, etc.... via internet par le web

notamment par la connexion au réseau de l'entreprise. Aujourd'hui par l'entremise des équipements mobiles tels que les smartphones, les tablettes, il est plus facile d'être attaquées.

3.3. Types d'attaques²⁹

De nombreuses menaces externes sur la sécurité réseau se diffusent via Internet. Il est également important de prendre en compte les menaces internes qui proviennent plus des utilisateurs. Avec l'adoption du BYOD, les cybercriminels effectuent leurs attaques sur les réseaux par l'entremise des équipements mobiles dont l'attaques zéro-day, l'attaque par déni de service, l'interception et vol de données, l'usurpation d'identité, l'attaque par botnet, l'attaque par logiciels espions et publicitaires(Spam), le social engineering, etc....

3.4. Principales mesures de sécurité

Pour se protéger des pirates, il faut connaître les possibilités d'attaques. Aussi, pour se défendre d'elles, il faut commencer par accepter le danger. La mise en place d'une politique (ou plan) de sécurité consiste en :

- ✚ L'identification des éléments à protéger (matériels, logiciels, données, personnes) ;
- ✚ L'identification des attaques éventuelles des pirates dont la dégradation qui consiste à perturber le réseau informatique via une panoplie de programmes malveillants ;
- ✚ L'altération des données qui s'effectue soit pendant la transmission des données sur un réseau, soit avant leur émission, soit pendant le passage sur un nœud du réseau ;
- ✚ L'écoute qui consiste à surveiller et à intercepter des données soit sur un poste (cheval de Troie), soit sur une ligne de communication, soit sur un smartphone.

Avec la croissance technologique actuelle, la sécurisation de son système d'information doit reposer sur quelques axes dont notamment l'aspect système (matériel, logiciel, réseau, web), humain et organisationnel³⁰.

Quand on parle de la sécurité du SI, c'est de rechercher d'aider, d'accompagner les entreprises ou les organismes à mettre en place un niveau de sécurité qui correspond à leur risques et à leurs enjeux. Aujourd'hui, il est impossible de produire sans son informatique c'est-à-dire les entreprises ne peuvent pas passer un

²⁹<http://cksecurity.free.fr/hacking/securite%20hand-book.pdf>. Consulté le 15 octobre 2014.

³⁰<http://cksecurity.free.fr/hacking/securite%20hand-book.pdf>. Consulté le 15 octobre 2014.

jour voir une heure au minimum sans que leur SI ne soit fonctionnel, fiable et que les informations ne soient confidentielles. Pour ce faire, l'entreprise a besoin de moyens provenant de la direction générale pour mettre en œuvre la sécurité de ses informations.

L'aspect humain est une étape très importante car certains pirates vont préférer s'attaquer à des systèmes en passant par les utilisateurs grâce à des techniques comme le social engineering. Sur ce, il est demandé à la hiérarchie de l'entreprise de procéder par la sensibilisation des utilisateurs en ce qui concerne les règles de base établies et de respecter la politique de sécurité définie. Pour le respect de tous ces aspects cités ci-hauts, la direction de système d'information doit mettre en place les règles de base incluant notamment la politique de sécurité englobant l'ensemble du système d'information. Pour cela, les mesures de sécurité doivent prendre en considération tous les aspects sécuritaires de l'entreprise³¹.

4. Développement du système de sécurité basé sur le principe BYOD dans une entreprise

Les équipements mobiles se multiplient de façon exponentielle dans les entreprises qu'ils soient dédiés à un usage personnel ou professionnel. Les responsables de parcs informatiques doivent maîtriser des parcs de systèmes hétérogènes et des matériels multiples (téléphones, tablettes...). Gérer ces terminaux de façon intensive et extensive est devenu une nécessité pour garantir la productivité des employés et la sécurité des données transportées en mobilité. Il est temps de mettre en place une véritable stratégie de gestion des équipements mobiles comme partie intégrante de la stratégie sécuritaire de l'entreprise.

4.1. Problématique du BYOD pour l'entreprise

Les enjeux de sécurité pour les ordinateurs, les utilisateurs, les applications et les données ont grandement évolué au cours des 20 dernières années. À l'ère de l'informatique mobile prônée par le phénomène BYOD, des services d'informatique en nuage dit Cloud computing et ainsi que l'univers des objets connectés, il est non seulement essentiel d'apporter des solutions ciblées, mais surtout de proposer une stratégie globale de « défense en profondeur » pour protéger tous les services de l'entreprise. Ces réalités ont toujours caractérisé la sécurité des technologies de l'information en entreprise, mais aujourd'hui, les enjeux sont plus importants que jamais puisque les utilisateurs peuvent accéder à l'information en tout temps, n'importe où, sur n'importe quel appareil et se connecter sur tous les types de réseaux.

Les avantages de ce phénomène BYOD se traduisent économiquement ; l'utilisation d'un appareil mobile personnel, performant presque partout, est un élément

³¹http://www.multimania.com/guide_du_hacker.pdf. Consulté le 03septembre 2014.

d'amélioration de la productivité individuelle de chaque employé. Selon une étude mondiale réalisée, Dell estime que 70 % des entreprises ayant mis en œuvre une stratégie BYOD a constaté une amélioration de la productivité de leur personnel et des temps de réponse aux clients, tandis que 59 % seraient moins compétitives sans cette pratique. L'accès mobile convivial et permanent aux applications business de l'entreprise génère de la croissance et de l'appétence pour tous les services et les produits offerts par la société. Dès lors, le succès d'une application mobile d'entreprise repose sur son intégration dans l'environnement informatique existant³².

Cette mutation de l'usage des terminaux personnels pour accéder au SI de l'entreprise, est perçue de façon différente par les employés et les discours divergent là où certains voient un outil qui leur simplifie la vie et d'autres perçoivent une contrainte supplémentaire qui les incite à étendre leur travail au-delà des heures de bureau. A l'heure où de nombreux témoignages rapportent que « l'hyper-connectivité » devient addictive, il est important que les départements de ressources humaines se positionnent sur plusieurs thèmes dont le temps de travail supplémentaire, stress induit par le fait d'être connecté en permanence via le télétravail.

Au cœur du BYOD se pose une problématique plus sociologique sur l'équilibre vie privée vie professionnelle ; comme pour le développement durable, le monde domestique, à travers le téléphone, pénètre le monde professionnel et inversement le monde professionnel peut s'imposer au monde domestique. Ceci peut créer des problèmes de domination, de pouvoir et de jeux d'acteurs, de négociations collectives et individuelles, de recherche de consensus, de justifications. Tous ces thèmes bien ancrés dans des cadres sociologiques apportent un éclairage critique sur le phénomène BYOD en entreprise, éclairage nécessaire pour un apprentissage pertinent.

4.2. Menaces éventuelles du BYOD

Tout comme les ordinateurs, les appareils mobiles sont cibles privilégiées d'attaques suite aux vulnérabilités qu'ils présentent. Dans l'écosystème mobile en entreprise, les vulnérabilités les plus courantes sont rencontrées dans les principaux sous-systèmes dont l'utilisateur final, l'appareil mobile, l'entreprise et le chemin d'accès réseau. Même si nous nous protégeons contre les menaces et vulnérabilités actuelles, nous devons demeurer à l'affût des technologies émergentes et des vulnérabilités potentielles qui y sont associées.

Par exemple, il semble évident que la communication en champ proche deviendra plus répandue sur les appareils mobiles au cours des prochaines années. En plus des vulnérabilités associées à ces transmissions, il faut s'attendre à ce que les assaillants s'en prennent à la plateforme mobile en espérant mettre la main sur des

³² Rapport de DELL 2011 sur le BYOD. Consulté le 18 septembre 2015.

données confidentielles telles que numéro de comptes bancaires, mots de passe, emails, etc. Bien que cette menace ne compromette pas nécessairement l'environnement informatique d'une entreprise, elle a poussé assurément les développeurs de maliciels à cibler davantage les plateformes mobiles. Le personnel IT des entreprises devra absolument tenir compte de la surface de menace des plateformes mobiles et aider les utilisateurs à protéger leurs appareils³³.

4.3. Impact du BYOD sur la sécurité de l'entreprise

Les équipements mobiles sont de plus en plus adoptés par les entreprises pour satisfaire les attentes des employés et gagner en productivité. La sécurisation de l'environnement du travail n'en devient que plus compliquée et nécessite le déploiement d'une stratégie de sécurité mobile adéquate. Les entreprises qui adoptent les technologies de mobilité et les pratiques BYOD pour que leur personnel ait systématiquement accès à leurs données professionnelles doivent veiller au respect des réglementations et normes de sécurité en vigueur.

C'est pourquoi on assiste à une unification des stratégies de sécurité des réseaux internes et des plates-formes mobiles. Ainsi, les utilisateurs sont libres d'interagir avec leurs collègues, leurs clients, les fournisseurs et partenaires, tout en minimisant l'exposition de l'entreprise à plus de risques. Mais parvenir au juste équilibre entre sécurité et mobilité relève souvent du défi, car la multitude des nouveaux équipements mobiles qui se connectent au réseau de l'entreprise sont autant de points d'accès supplémentaires aux données et aux applications professionnelles pour les utilisateurs malintentionnés et autres hackers³⁴.

Le BYOD figure d'ailleurs parmi les premières causes d'incidents de sécurité citées par les décideurs IT en réponse à une récente étude mondiale de Dell sur la sécurité. La démocratisation du BYOD constituera l'une des principales préoccupations de sécurité. Le fait est que les employés n'hésitent pas à contourner les règles du BYOD dès qu'ils les jugent trop contraignantes ou qu'elles risquent d'empiéter sur leur liberté personnelle. La connexion de nouveaux types d'équipements mobiles avec différents systèmes d'exploitation multiplie également les risques pour la sécurité de l'entreprise. La sécurisation de l'environnement du travail est une tâche ardue, que l'adoption des pratiques BYOD et de mobilité compliquent encore en créant des failles qui mettent en danger les données de l'organisation. Pour adopter les nouveaux types de périphériques, de plates-formes et de modes de travail favorables à la productivité des employés sans fragiliser les systèmes, ni mettre en péril les données de l'entreprise,

³³ http://www.ey.com/Bring_your_own_device.pdf. Consulté le 03 septembre 2015.

³⁴ <http://www.cgi.com/Assurer-la-securite-des-entreprises-mobiles-f.pdf>. Consulté le 10 Décembre 2015.

la meilleure stratégie consiste à appliquer des pratiques éprouvées en s'appuyant sur des solutions flexibles de gestion de mobilité qui ont fait preuve de leur efficacité³⁵.

4.4. Gestion du BYOD en entreprise

Les outils de gestion des postes mobiles permettent aux entreprises de surveiller l'état des appareils, c'est-à-dire de vérifier quelles applications y sont installées, quelles mesures de sécurité y sont appliquées, quels sites Web y sont autorisés, etc. L'une des plus importantes fonctionnalités offertes par de tels outils s'avère probablement la capacité d'effacer à distance le contenu d'un appareil perdu ou volé. Il n'est peut-être pas facile de convaincre les utilisateurs de laisser leur employeur installer ses logiciels sur leurs appareils personnels, mais l'élaboration de politiques de sécurité par l'entreprise peut contribuer à apaiser leurs craintes. Les entreprises qui fournissent des appareils mobiles à leurs employés devraient envisager la mise en œuvre d'une solution de gestion des postes mobiles dit MDM pour l'administration, le contrôle total et la sécurité de l'écosystème mobile au sein de l'organisation³⁶.

4.5. Mise en place d'un système de sécurité

Le principal enjeu pour le développement du BYOD est la sécurité et les entreprises doivent définir une politique de sécurité qui doit être respectée par les employés tout en définissant des profils de sécurité selon les postes de travail, classer les données selon la sécurité requise, sensibiliser et responsabiliser les employés.

Pour déployer un système de sécurité pour le BYOD, nous avons besoin de deux environnements nécessaires dont l'environnement matériel et logiciel. Dans l'environnement matériel, il est demandé à l'entreprise qui voudrait mettre en place le BYOD d'identifier les besoins de personnels pour l'entreprise tout en identifiant le nombre des équipements mobiles pour permettre sa bonne gestion. En ce qui concerne l'environnement logiciel, nous recommandons aux entreprises de choisir une solution de gestion de terminaux mobiles (de l'anglais Mobile Device Management, MDM) répondant à leurs exigences et recommandations pour être déployée.

4.5.1. Solutions logicielles MDM

Une application de gestion de terminaux mobiles est une solution informatique permettant de gérer un parc de terminaux mobiles. Le MDM a fait sa place en entreprise à cause des pressions d'adoption d'une politique de sécurité sur le BYOD et répond exclusivement à la notion de sécurité de ce dernier. Avec ses multiples

³⁵ http://www.atlab.fr/SSTIC09-article-Raboin-La_securite_des_smartphones.pdf. Consulté le 03 septembre 2015.

³⁶ Idem

avantages dont le renforcement réel du niveau de sécurité, le MDM présente quelques inconvénients dont le coût élevé pour son acquisition et la surveillance des utilisateurs.

Le MDM présente différentes fonctionnalités dont l'administration à distance, la propagation de politiques de sécurité, le chiffrement de données, la distribution d'application, la configuration de profil d'utilisateur, la gestion des services de télécommunication, le blocage ou effacement à distance, la performance et diagnostic, la sauvegarde et restauration de données puis la gestion du roaming et la géolocalisation de terminaux mobiles. Certains produits MDM permettent aux administrateurs de distribuer des applications à distance sur les périphériques mobiles des utilisateurs à l'aide de la technologie OTA³⁷.

Il existe deux types de MDM :

- ✚ MDM mono plateforme : ceux qui n'acceptent qu'un seul système d'exploitation (Microsoft avec son System Center MDM 2008) ;
- ✚ MDM multiplateforme : une approche dite agnostique puisqu'elle ne se limite pas à un système d'exploitation mais permet de gérer des mobiles fonctionnant avec les principaux systèmes d'exploitation mobiles.

Les fonctionnalités à risque pour l'entreprise dans l'adoption de MDM sont le partage et la diffusion de fichiers par Bluetooth et le téléchargement d'applications non qualifiées par la direction de système d'information dans des boutiques en ligne.

4.5.2. Sécurité du MDM

Le BYOD force l'entreprise à augmenter le nombre des appareils mobiles pour satisfaire ses employés car ces derniers ont des critères très élevés que le standard habituel. Pour arriver à mettre en place le BYOD dans son entreprise, on doit tenir compte de quelques critères dont la sécurité en première position. Des produits MDM sont commercialisés depuis des années, les entreprises ont désormais la possibilité d'acheter des solutions entièrement intégrées associant des fonctions de gestion des périphériques mobiles à des technologies de sécurité mobile.

Auparavant, les entreprises n'avaient pas d'autres choix que d'acheter séparément une solution MDM et une solution antivirus auprès de fournisseurs distincts. De nombreuses plateformes existent aujourd'hui qui proposent des solutions MDM avec les solutions sécuritaires incluses dont WindowsIntune, Symantec, BlackBerry RIM, MaaS360, Airwatch, BoxTone, ZENPRISE, GOOD, Kaspersky EndPoint, PushManager et tant d'autres.

³⁷ OTA : On The Air désigne les technologies permettant de distribuer et d'installer de nouvelles versions de [Firmware](#) dans un équipement mobile, téléphone, [smartphone](#) ou tablette.

Nous recommandons que chaque entreprise puisse développer sa propre plateforme MDM pour la meilleure gestion et sécurité de données de son parc informatique vues que celles-ci sont au cœur de tous les enjeux du monde.

5. Conclusion

Suite aux avancées technologiques et à l'ère de l'informatique mobile, des services d'informatique en nuage et des applications pour téléphones intelligents, permettent aux employés de pouvoir travailler n'importe où et en tout temps ainsi partager les ressources et les données sur n'importe quelle plateforme. Cette pratique est baptisée « Bring Your Own Device » du français « apportez vos appareils personnels ». Cela inclut les Smartphones, les tablettes tactiles, ordinateurs portables ainsi que les PDA, etc. La portabilité de ces équipements mobiles permet à l'utilisateur de rendre nomade ses pratiques de travail, d'échanges, de divertissement, de recherche d'information sur le web, de fréquentation des réseaux sociaux et de consommation de produits dans le monde professionnel.

Avec l'intégration de ces équipements mobiles dans l'écosystème de l'entreprise, aujourd'hui on parle de système d'information mobile ou de la mobilité professionnelle. Cette tendance a notamment apporté un changement total dans la gestion et fonctionnement de l'entreprise dont l'accès aux données peut se faire de n'importe où et à tout moment ce qui représente un danger potentiel en matière de sécurité. Avec une telle transformation croissante de la mobilité du système d'information, les organisations doivent développer les technologies mobiles qui leur permettront d'accroître la performance grâce aux gains de productivité tout en limitant le risque en matière de sécurité.

En effet, ces équipements mobiles collectent et traitent plusieurs informations sensibles dont l'accès doit être contrôlé afin de protéger la vie privée de l'utilisateur et la propriété intellectuelle de l'entreprise comme souligner ci-haut. L'unique stratégie valable consiste à remédier directement à l'ensemble des vulnérabilités tout en combinant technologie, formation des utilisateurs et processus dans un effort concerté visant à sécuriser les systèmes vulnérables, à réduire la surface exposée à des attaques potentielles et à limiter les dommages causés en cas d'attaque réussie.

Dans l'entreprise d'aujourd'hui, caractérisée par la mobilité, la sécurité est un catalyseur essentiel pour l'activité, en permettant aux collaborateurs de tirer partie en toute sécurité des avantages qu'apportent ces équipements mobiles et intelligents. Si les comportements, les vulnérabilités techniques et les menaces en perpétuelle évolution créent des défis, les entreprises peuvent se protéger et gagner en fiabilité en corrélant leurs dispositions en matière de sécurité et leurs priorités opérationnelles. Elles peuvent s'appuyer sur une solution abordable et facile à gérer en mettant en place une approche de gestion mobile structurée et progressive intégrant la sécurité mobile dans les technologies existantes et dans la culture de l'entreprise. Pour une entreprise qui

souhaite faire évoluer sa mobilité, les avantages doivent d'abord être bien compris et évalués.

Le challenge technologique consiste à identifier les différentes solutions de mobilité qui fonctionnent le mieux en dehors du réseau habituel de l'entreprise, qui garantit la meilleure sécurité, permettant à des informations confidentielles d'être stockées sur des dispositifs mobiles. La rapidité du retour sur investissement d'une société réside dans une intégration réussie des outils de mobilité et dans la compréhension de tous ses avantages par les employés mobiles et le management. Car, sans un personnel prêt à devenir mobile, les efforts de la société pour entreprendre un tel changement ne donneront que des résultats médiocres. En adoptant le BYOD, il est essentiel pour les entreprises de ne pas sous-estimer son impact à l'interne. Pour ce, il faut explorer toutes ces questions qui concernent les utilisateurs, les données et l'entreprise car le service IT aura des pressions de la part des utilisateurs.

Les entreprises doivent accepter l'hétérogénéité sur leur flotte mobile et faire le choix moins cher pour leur acquisition que les autres avec les propriétés distinctives et définir un standard concernant les applications à prendre en considération. Etablir un niveau de sécurité approprié tout en soutenant le travailleur mobile exige la prise en compte des vulnérabilités propres à tout le contexte des télécommunications mobiles et l'adoption en entier ou en partie de toutes les stratégies énoncées dans ce document.

Enfin, notre conviction est que la sécurité est une approche top to down donc mettre les directions en face de leur responsabilité par rapport aux risques majeurs que court l'entreprise. Il faut faire l'analyse de risques en triant, priorisant les mesures d'hygiène informatique qui vous protège d'un grand nombre de risques à partir desquels, il faut attribuer des responsabilités en terme de sécurité tout en élaborant une politique de sécurité, une charte déplorables, faire la traditionnelle de sauvegarde sur le Cloud et inclure les équipements mobiles dans la stratégie de sécurité de l'entreprise.

6. Bibliographie

B. Bouterin, Delaunay B., *Sécuriser un réseau Linux*, 3e édition. N°11960, 2007.

Benci G., Foucaut O., Rolland C., *Conception de système d'information. La méthode Rémora*, éd. Eyrolles, Paris 1988.

Carrez C., *Les systèmes Informatiques*, éd. Dunod ; Paris, 1990.

Cédric Llorens, Laurent Levier, Denis Valois, *Tableaux de bord de la sécurité réseau 2è Edition*, Editions Eyrolles, Paris, 2006.

Claude Servin, *Réseaux et Télécoms, cours et exercices corrigés*, Ed. Dunod, Paris, 2003.

Edward Evenson A., *The Telephone Patent Conspiracy of 1876: The Elisha Gray - Alexander Bell Controversy*, McFarland, North Carolina, 2000.

Foucaut O., *Conception des systèmes d'information et programmation événementielle*, Inter Editions ; Paris, 1996.

Guy PUJOLLE, *Les Réseaux 5è édition*, Ed. Eyrolles, Paris Cedex, 2006.

Jaulent P., *Génie logiciel : les méthodes*, éd. Armand Collin, Paris, 1992.

Laurent Bloch & Christophe Wolfhugel, *Sécurité informatique : Principes et méthodes*, Ed. Eyrolles, Paris Cedex, 2007.

Michèle Germain, *Du téléphone au smartphone*, Éditions du Puits Fleuri, Paris 2011.

Michèle Germain, *Les bases de la radio – Introduction à la radio*, Éditions du Puits Fleuri, Paris 2007.

Michèle Germain, *Les Réseaux de téléphonie mobile I : le GSM*, Éditions du Puits Fleuri, Paris, 2014.

Xavier Carcelle, *Réseaux CPL par la pratique : Avec trois études de cas : réseau domestique, réseau d'entreprise et réseau de desserte de collectivité locale*, Ed. Eyrolles, Paris Cedex, 2006.

Xavier Lagrange, Philippe Godlewski, Sami Tabbane Hermès, *Réseaux GSM-DCS*, Éditions du Puits Fleuri, Paris, 1999.