Bblog | au plus près de votre business

Cybersécurité :
Méthode, outils et stratégies

ÉDITO

Face aux attaques informatiques d'ampleur internationale, on constate aujourd'hui une réelle prise de conscience des dangers encourus par nos entreprises. Les objets connectés, la RGPD ou bien encore le spectre d'une « Cyber-Guerre » sont des thèmes de plus en plus présents dans la presse, ce qui amène les entreprises de toutes tailles à repenser leurs politiques de sécurité.

Cela se traduit bien souvent par des évolutions majeures au niveau de l'organisation de l'entreprise, par des besoins en expertises mais également par l'acquisition (parfois sous ou surdimensionnée) de solutions informatiques de sécurité coûteuses.
Mais les outils ne suffisent pas pour garantir la sécurité des actifs d'une entreprise. La sécurité doit être pensée comme un ensemble de ressources et processus qui se complètent et se superposent afin de garantir une protection optimale contre les nombreuses attaques.

Le problème n'est plus « entre la chaise et le clavier » comme nous pouvons parfois encore l'entendre dans nos entreprises. Aujourd'hui, le collaborateur ne doit plus être considéré comme une vulnérabilité, mais bien comme un élément indispensable à notre sécurité.

C'est ce que nous tenterons d'expliquer dans ce dossier entièrement consacré à la sécurité des entreprises…

SOMMAIRE

4 ..... Le facteur HUMAIN

11 ..... Les leviers de l'ENTREPRISE

17 ..... La MÉTHODE pour aborder les enjeux de sécurité

21 ..... Les OUTILS de protection

26 ..... L'avis des DIRIGEANTS

31 ..... Le point de vue des EXPERTS

Le facteur **HUMAIN**

Le **COLLABORATEUR** comme premier antivirus

Piratage de systèmes, hacking de données, vol d'adresses… la menace informatique nous concerne tous. Or la première des protections reste la vigilance humaine. Voici nos 7 règles d'or pour sensibiliser au mieux vos équipes…

En matière de sécurité informatique, les bonnes pratiques sont clairement identifiées : opter pour des mots de passe d'au moins huit caractères alphanumériques, renouveler régulièrement ces précieux sésames, ne pas ouvrir de pièce jointe dont l'auteur n'est pas clairement identifié, ne pas utiliser de clés USB sans précaution… Ces préceptes semblent connus de tous… Et pourtant !

D'après une étude réalisée par OpinionWay pour le Club des experts de la sécurité de l'information et du numérique, 80 % des entreprises françaises ont été victimes d'une cyberattaque en 2015… Et les incidents de sécurité sont dus, dans 35 % des cas(1), à des maladresses de collaborateurs… La solution ? Bien sensibiliser et accompagner vos collaborateurs.

(1) Enquête sur 600 clients IDC, mars 2017

YVANNE DINGLI
Responsable SAV fixe et SCA
(Sécurité et Continuité d'Activité),
Bouygues Telecom Entreprises

ENCADRER

> « Il convient de fixer un cadre précis en établissant une charte informatique. »

La charte informatique est essentielle car elle fixe le cadre des pratiques autorisées, proscrites et / ou recommandées.

- **Peut-on utiliser une tablette tactile personnelle sur le réseau de l'entreprise ?**

- **Peut-on copier des données sur une clé USB pour les consulter de chez soi ?**

En établissant en quelque sorte une charte de sécurité informatique, l'entreprise ne se contente pas de faire de la pédagogie. Une fois ce cadre établi, les collaborateurs sont mis face à leurs responsabilités.

PROUVER

Comme tout règlement, la charte doit être perçue comme légitime par les collaborateurs, sous peine de ne pas être appliquée rigoureusement.

> Elle doit être intelligible et pragmatique car l'ensemble des collaborateurs doit pouvoir se l'approprier, et tous n'ont pas la même maturité technologique.

Pour ce faire, appuyer chaque recommandation par des exemples précis. Pour sensibiliser aux problématiques de phishing, on exposera le principe, et les moyens de détecter les messages suspects (des URLs ne correspondant pas au nom de domaine de l'émetteur du message, la présence de fautes d'orthographe dans le message, etc.)

FORMER

> La formation du management à l'ensemble des dangers et des moyens de s'en prémunir est certainement la priorité.

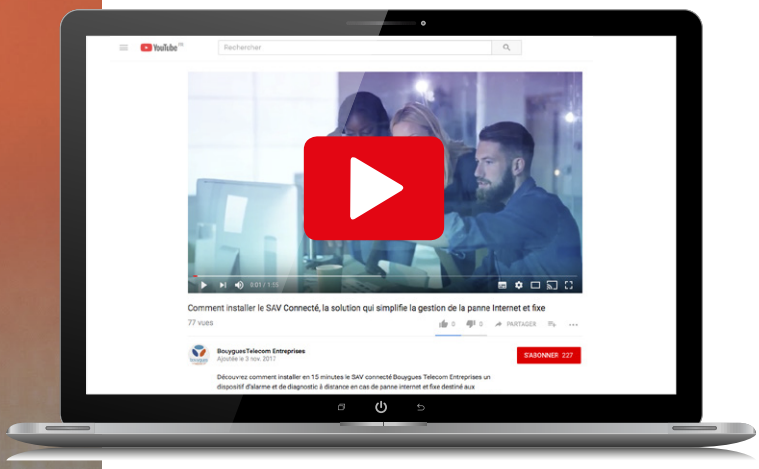
On peut d'ailleurs ajouter que la direction est une cible de choix car elle détient, de fait, des informations plus sensibles.

Le facteur **HUMAIN**

Plus le management de l'entreprise est au fait de ces questions de sécurité informatique, plus il est en mesure d'aider les collaborateurs à appliquer les bonnes pratiques, à remonter les incidents, mais aussi à s'assurer du respect des règles établies.

Par ailleurs, il est essentiel de ne pas pointer du doigt un utilisateur qui aurait ouvert une pièce jointe malveillante par exemple. Personne n'est à l'abris, il est donc nécessaire de bien accompagner ses équipes et valoriser la remontée d'informations post incidents afin d'accélérer le processus de réaction à une attaque.

COMMUNIQUER



Les discours techniques ou très théoriques peinent à toucher leurs cibles. Certains supports de communication, tels que les infographies par exemple, permettent de délivrer rapidement et simplement un discours clair et percutant. Les vidéos sont également un excellent moyen de sensibiliser les collaborateurs aux bonnes pratiques.

> "Nous avons relayé des vidéos explicatives disponibles sur Youtube. Elles sont très didactiques, abordent les problématiques les plus complexes avec humour et efficacité. "

Ces vidéos, ont rencontré un écho très favorable et permettent de sensibiliser efficacement les collaborateurs, en évitant les discours poncifs !

DÉMONTRER

Un vecteur de communication très efficace aujourd'hui reste la démonstration en direct de scénarios d'attaques et / ou de tests grandeur nature dans l'entreprise. Montrer concrètement comment un hacker est en mesure de prendre le contrôle d'un poste de travail ou de récupérer des données sensibles en quelques minutes à cause d'un mot de passe trop faible, d'une pièce jointe malveillante ou d'une erreur grossière de paramétrage est un formidable outil pédagogique.

De même, l'envoi d'un faux email de phishing permet à la fois « d'éduquer » les collaborateurs mais aussi d'établir des statistiques sur l'ensemble des employés suite au test. Sans pénaliser les utilisateurs ayant ouverts le mail et en n'utilisant que les statistiques anonymes, l'utilisateur au centre du processus prendra ainsi conscience des menaces potentielles.

VÉRIFIER

Parmi les initiatives qui présentent le double avantage de renforcer la sécurité tout en sensibilisant les collaborateurs, on retiendra la possibilité de déployer des bornes de décontamination de clés USB.

> « Nous avons réalisé ce type d'opération. Les collaborateurs sont invités à placer leurs clés USB dans ces bornes. Elles sont ainsi vérifiées et nettoyées en moins de trois minutes. Régulièrement des infections sont constatées, à la grande surprise des utilisateurs qui pensaient pourtant le contenu de leur clé irréprochable ! »

ET ENFIN, RÉPÉTER, RÉPÉTER, RÉPÉTER...

L'informatique est un outil du quotidien et si l'on relâche la pression sur les bonnes pratiques en matière de sécurité, si l'on ne martèle pas le message régulièrement, les mauvaises habitudes reviennent très vite !
Pour que l'accompagnement porte ses fruits sur le long terme, il faut considérer la formation et la sensibilisation comme des processus itératifs. N'oubliez pas non plus de prendre en compte le turn over des collaborateurs !

> Départs, arrivées, les effectifs d'une entreprise évoluent sans cesse.

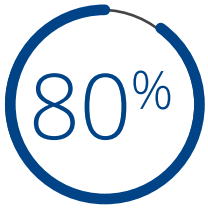
LE + DE L'EXPERT

Les effectifs d'une entreprise sont mouvants et les menaces évoluent. Pour maintenir un niveau de sécurité constant, il faut rester en veille et faire évoluer les processus en conséquence !

Les leviers de l'**ENTREPRISE**

Nos **10 COMMANDEMENTS** pour les PME

Pour une PME, les principales difficultés résident dans le peu de moyens financiers à leur disposition et le manque de ressources compétentes et disponibles. Toutefois, avec un peu de méthode et de rigueur, il est possible de se prémunir des principales menaces…



des entreprises ont subi
des attaques contre leurs systèmes (2)

LES TERMINAUX MOBILES
sont la cause d'importantes fuites
de données informatiques d'entreprise

(2) Étude réalisée par OpinionWay pour le Club des experts de la sécurité de l'information et du numérique

QUELQUES RÈGLES, VOUS FORMALISEREZ !

Couchez sur le papier les périmètres du système d'information à protéger. Établissez les responsabilités de chacun, les procédures à mettre en place pour réagir face à une menace informatique afin de ne pas réagir dans la précipitation et surtout, appuyez-vous sur une cartographie à jour de vos installations.

LES ACCÈS INTERNET, VOUS CONTRÔLEREZ !

Chaque point d'accès Internet de l'entreprise, constitue une brèche dans laquelle un pirate peut s'engouffrer pour accéder au système d'informations. Privilégiez une approche de réseau privé virtuel (VPN) avec un unique point d'échange sécurisé avec Internet pour l'ensemble de l'entreprise. Par ailleurs, effectuez régulièrement des tests de vulnérabilités sur chacun de ces accès afin d'anticiper une attaque.

LES ACCÈS WI-FI, VOUS VERROUILLEREZ !

Les bornes Wi-Fi déployées dans les locaux de l'entreprise doivent être placées sous haute surveillance. Des pirates installés dans le voisinage ou même dans un véhicule garé dans la rue ont de multiples outils à leur disposition pour décrypter les mots de passe Wi-Fi en quelques minutes. Contrôler ces accès doit faire partie de la politique de sécurité informatique de l'entreprise.

LES SOLUTIONS, VOUS STANDARDISEREZ !

L'une des priorités pour sécuriser un parc informatique consiste à contrôler et réduire le nombre de systèmes d'exploitation, les paramètres de sécurité et logiciels de protection différents installés sur chacun d'eux. Cela ne signifie pas n'avoir une seule configuration, qui en cas de faille rendrait l'ensemble du parc vulnérable, mais bien de contrôler le nombre et les configurations possibles et les adapter en fonction des usages et niveaux de protection nécessaire. Les solutions et configurations standardisées et centralisées réduisent considérablement le temps nécessaire au maintien d'un niveau de sécurité donné ainsi que les coûts et la complexité associé à la sécurité.

LES SITES WEB, VOUS FILTREREZ

Plusieurs niveaux de filtrage peuvent être appliqués. Un premier filtre Internet pour les sites dangereux, les sites liés au piratage d'applications, les sites de téléchargement illicites ou encore les sites pornographiques doit systématiquement être mis en place. Il peut ensuite être envisagé, selon l'entreprise, de réguler l'accès aux réseaux sociaux, aux sites de vidéos, etc. Une solution efficace consiste notamment à appliquer des « profils standards de filtrage » à vos utilisateurs et de les modifier à la marge si besoin par rapport aux usages spécifiques de vos collaborateurs.

LES CLOUD PERSONNELS, VOUS SURVEILLEREZ !

Le Cloud s'est démocratisé, y compris dans la vie privée des des collaborateurs, avec les outils de stockage, de traduction, de conversion de fichiers d'un format à un autre, les correcteurs orthographiques etc. Ces solutions librement accessibles via Internet

posent un problème de sécurité car les entreprises n'ont aucun contrôle sur les fichiers que le salarié fait transiter sur ces espaces, d'autant qu'elles sont souvent hébergées aux États-Unis, ce qui pose potentiellement un risque juridique s'il s'agit de données nominatives, notamment dans le cadre de la RGPD.

VOS VULNÉRABILITÉS, VOUS TESTEREZ !

80 % des entreprises ont subi des attaques contre leurs systèmes selon le baromètre CESIN(3) 2016. La menace des réseaux bots(4) informatiques est permanente et vous y serez nécessairement confronté. Pour les repousser, testez vos vulnérabilités, mettez en place sur le réseau de l'entreprise des dispositifs capables de filtrer les programmes malveillants, mais aussi déjouez les attaques les plus sophistiquées type 0-day(5) ou APT(6). Définissez les procédures qui permettront la détection et la gestion d'une attaque ainsi que la reprise de la production informatique si une attaque vous atteignait malgré tout.

VOTRE FLOTTE DE MOBILES, VOUS SÉCURISEREZ !

Les terminaux mobiles sont la cause d'importantes fuites de données informatiques d'entreprise. Il peuvent être piratés, mais également perdus ou volés. Avec une solution de Mobile Device Management (solution de gestion de flottes mobiles d'entreprise), vous pouvez activer / désactiver rapidement les accès à ces équipements, chiffrer ou effacer le contenu à distance, tout en appliquant des politiques de sécurité standard pour l'ensemble de votre flotte mobile.

(3) Club des experts de la sécurité de l'information et du numérique
(4) Robots informatiques
(5) Faille logicielle qui n'a pas encore été découverte par le fabriquant
(6) Advanced Persistent Threat - Menace persistante avancée

À JOUR, VOUS RESTEREZ !

La notion de sécurité informatique est par nature évolutive. Les menaces changent, les protections aussi ! Une seule parade : toujours tenir ses installations et l'ensemble de son parc applicatif à jour. Pour vous aider, des tests réguliers de vos vulnérabilités peuvent accélérer la détection de patchs, mise à jour ou évolution de configurations nécessaires. Le recours à une solution de sécurité managée peut être un moyen de simplifier cette problématique et faciliter une gestion centralisée de votre système de sécurité.

VOS COLLABORATEURS, VOUS IMPLIQUEREZ !

La sécurité informatique, c'est l'affaire de tous et de chacun ! Responsabilisez vos équipes en leur indiquant les bons comportements à tenir face aux menaces. Des règles de comportement simples permettent de déjouer ou réagir rapidement à bien des attaques.

LE + DE L'EXPERT

Les solutions de tests de vulnérabilités, les systèmes de sauvegardes, les outils de protections et de contrôles ainsi qu'un support opérationnel sont les piliers indispensables d'un dispositif de protection efficace.

La **MÉTHODE** pour aborder les enjeux de sécurité

Se **CHALLENGER** pour se protéger

Se protéger c'est bien, se tester c'est encore mieux. Avant de vous parer des solutions les plus complexes de cybersécurité, que diriez-vous de tester vos vulnérabilités ?

des entreprises subissent au minimum une attaque par semaine(7)

Certaines attaques informatiques récentes ont fait la une des médias grands publics telles que le virus Wanna Cry qui, en quelques heures avait déjà infecté plus de 300 000 ordinateurs dans près de 160 pays. Ces attaques prouvent que la sécurité n'est pas toujours qu'une affaire d'investissements coûteux.

Une entreprise pouvait se protéger de Wanna Cry par une simple mise à jour de Windows et l'application d'un patch qui était disponible depuis plusieurs semaines. La difficulté consistait donc à être informé de la présence de la vulnérabilité dans ses systèmes et de la nécessité d'appliquer le patch.

(7) Enquête sur 600 clients IDC, mars 2017

STÉPHANE LOUETTE
Chef de Produit
Sécurité Informatique,
Bouygues Telecom Entreprises

À VOS MARQUES ...

> Il n'est pas toujours si compliqué ni coûteux de maintenir son niveau de sécurité. Cela commence souvent par être bien informé, tester et auto-évaluer régulièrement son infrastructure informatique afin de connaître et mieux prioriser les corrections nécessaires.

S'il est difficile pour une entreprise de se protéger contre une attaque ciblée réalisée par un hacker chevronné, elle peut cependant relativement bien se protéger d'attaques de masse utilisant des failles largement répandues et connues.

Il n'est donc pas toujours pertinent d'acquérir les outils les plus complets et chers du marché si leur maintien opérationnel n'est pas assuré convenablement et si les vulnérabilités présentes dans vos systèmes référencés ne sont pas corrigées.

... ATTAQUEZ !

Beaucoup d'entreprises ne testent pas régulièrement leurs solutions de sécurité alors que deux tiers d'entre-elles subissent au minimum une attaque par semaine[8]. Il est temps d'y remédier !

Un test régulier des vulnérabilités permet donc de faire un état des lieux de la surface d'attaque de votre entreprise, de détecter un certain nombre d'erreurs de paramétrage ou mises à jour nécessaires à l'aide de scripts d'attaques. Les tests de vulnérabilités donnent également des informations sur les correctifs à appliquer ainsi que des indicateurs permettant de suivre votre vulnérabilité au cours du temps.

En un mot, pour mieux vous défendre, attaquez-vous !

LE + DE L'EXPERT

Pour bien préparer sa défense, il convient de bénéficier d'une source fiable d'informations sur les nouvelles vulnérabilités, de s'auto-diagnostiquer régulièrement et de maintenir (en les actualisant) les outils de sécurité adéquats.

(8) Enquête sur 600 clients IDC, mars 2017

Les **OUTILS** de protection

TESTER SA VULNÉRABILITÉ, de la théorie à la pratique

YOUNÈS ELMOUNTACIR
Sales Engineer,
Beyond Security

Les failles de sécurité sont partout : dans les systèmes d'exploitation, les applications, les machines virtuelles, les protocoles de transport de données…
Heureusement des tests existent pour vous évaluer.

Rencontre avec Younès Elmountacir, Sales Engineer chez Beyond Security qui nous dévoile les secrets d'une détection de vulnérabilités efficace et pertinente.

Comment élabore-t-on un test de vulnérabilité standard ?

Pour bien comprendre ce qu'est un test de vulnérabilité, il faut déjà définir ce que l'on désigne par ce terme. Une vulnérabilité n'est rien de moins qu'une brèche. Il peut s'agir d'un code de mauvaise qualité dans une application, d'une faiblesse dans un algorithme de chiffrement, d'une faille de sécurité dans un protocole de transport de données ou bien souvent d'une erreur humaine… Les vulnérabilités existent dans tous les systèmes d'exploitation, dans tous les logiciels.

Lors d'un test, on utilise un script de détection. Ce dernier exploite une base de données internationale qui recense toutes les vulnérabilités connues et identifiées à ce jour. Cette base évolue très fréquemment… à mesure que les vulnérabilités sont découvertes. La solution que nous avons développée et que nous avons baptisée AVDS (Automated Vulnerability Detection System) peut réaliser jusqu'à 50 000 tests différents sur un système connecté.

Comment se déroulent ces tests en pratique ?

Un test se déroule en plusieurs phases. La première est une phase de découverte qui permet de comprendre le système d'information, les machines utilisées, les OS, les applications et les usages. Cela permet de définir le périmètre du test. On effectue ensuite des tests de base portant sur les ports de communication ouverts ainsi que les services ouverts derrière chaque port. Peut venir en complément le Web Scan qui consiste à passer en revue l'intégralité d'une application Web de l'entreprise.

La deuxième phase consiste à appliquer des tests de détection sur les vulnérabilités fréquentes comme le SQL Injection par exemple. Nos scans de vulnérabilité ne sont pas intrusifs. Nos interventions s'effectuent à distance. En complément des tests classiques nous ajoutons une analyse comportementale qui nous permet d'affiner notre analyse et de réduire les faux positifs.
En effet, ce qui apparaît parfois comme une vulnérabilité n'en est pas une ! En règle générale on considère sur le marché que le taux de faux positifs atteint 5 %. Grâce à notre méthode, ce taux n'excède pas 0,1 % ! Les scans se déroulent sans perturbation des flux de la production et peuvent être exécutés sur les tranches horaires paramétrables (HNO(9), hors fenêtre de back-up, etc.). De plus, il est possible de définir le nombre d'actifs à scanner simultanément.

(9) Heures Non Ouvrables

Quels sont vos principaux critères d'évaluation ?

AVDS effectue une analyse interne et externe des réseaux quel que soit le nombre de serveurs, services, ports ou adresses IP.
Par ailleurs, les scans réseaux peuvent être authentifiés (Windows, Linux / Unix) pour améliorer la détection de vulnérabilités et comparer les configurations systèmes par rapports aux bonnes pratiques préconisées par les standards du marché ainsi que de vérifier les mises à jour de patchs de sécurité.

Chaque vulnérabilité est notée en fonction de sa sévérité.
L'algorithme ADVS interne croise ces informations pour délivrer un score sur l'infrastructure. Ce score est global, par zone choisie, par host, etc. Il est alors possible de visualiser en un coup d'œil le niveau de sécurité de l'infrastructure et de manager les différentes équipes, zones géographiques, responsabilités fonctionnelles quant au maintien de scores cibles au fil du temps.

À quels fréquence ces tests de vulnérabilité doivent-ils être menés ?

Chaque jour ou presque, de nouvelles vulnérabilités sont identifiées et viennent enrichir la base de données internationale que nous exploitons pour nos tests. S'il n'est pas conseillé d'effectuer des tests quotidiens (ce qui serait un non-sens car détecter ne suffit pas, il faut ensuite corriger le défaut), un test hebdomadaire est réellement efficace. Dans la réalité cependant, on peut considérer qu'un test mensuel, des rapports scrupuleusement analysés et des correctifs appliqués méthodiquement seront déjà une promesse de sécurité améliorée.
Les rapports que nous générons permettent aux entreprises de prioriser leurs actions. Nous précisons le degré de criticité des vulnérabilités détectées et depuis combien de temps celles-ci sont présentes sur le système d'information. À partir de ces deux informations, les DSI, RSSI peuvent définir les mesures à prendre prioritairement.

COMMENT ÇA MARCHE ?

Un test de vulnérabilité utilise un script de détection. Ce dernier exploite une base de données internationale qui recense toutes les vulnérabilités connues et identifiées à ce jour. La base évolue très fréquemment, à mesure que les vulnérabilités sont découvertes.

LE + DE L'EXPERT

Ne jamais oublier que « le numérique vient de la rue » comme le dit Hugues Meili, président de Bretagne Développement Innovation, PDG et cofondateur de Niji.

Les dispositifs de sécurité doivent avancer au rythme de l'évolution des usages. Ainsi, fournir un accès fluide aux données et aux outils de l'entreprise, quel que soit le lieu, le device et l'heure de la journée est aujourd'hui un pré-requis.

L'avis des **DIRIGEANTS**

Le rendez-vous des **DÉCIDEURS...**

PIERRE-ANTOINE THIEBAULT
Directeur Marketing Opérationnel,
Bouygues Telecom Entreprises

En mars dernier, nous assistions à la Rencontre d'Affaires Mobilité et Digital, voici ce qui nous avait alors marqué grâce au reportage de Pierre-Antoine Thiebault...

des employés effectuent des tâches professionnelles sur un appareil personnel(10)

des employés exercent des activités personnelles sur un appareil professionnel(10)

« Qu'est-ce qui fait basculer un Buzz Word comme la Transformation Digitale » dans la réalité quotidienne des entreprises ? Je vois deux exemples qui ne trompent pas : les vrais décideurs prennent le temps de se déplacer en masse et les points de « détails » de la mise en œuvre sont le sujet principal des discussions. C'est l'effet que j'ai ressenti lors de ma visite sur le Salon (Rencontres) ROOMn 2017 qui se tenait à Monaco les 7 et 8 Mars 2017.

(10) Étude Gartner et Ping Identity

Le thème principal était celui de la Transformation Digitale (que je nommerai Transformation Numérique car nous sommes en France). 400 décideurs IT des grandes entreprises (ETI et Grands Comptes) avaient fait le déplacement pour rencontrer en tête à tête les partenaires à même de répondre à leurs problèmes concrets d'implémentation. Pour le DSI, les deux dernières années ont été focalisées sur la Restructuration / Virtualisation de leur Système d'information mais c'est la mobilité qui porte et concrétise la transformation et les gains de productivité visibles par les utilisateurs. Les DSI se sont donc approprié ce sujet critique car il impacte la totalité de l'organisation, bien au delà de la DSI.

LA MOBILITÉ EST UN DROIT

La banalisation des smartphones s'accélère. 6 employés sur 10 (60 %) effectuent des tâches professionnelles sur un appareil personnel, et à l'inverse ils sont tout autant (55 %) à exercer des activités personnelles sur un appareil professionnel.(11) Cela place le DSI dans une situation intenable : comment passer à la phase concrète de mise en œuvre et de suivi de la transformation sans aucune maîtrise du terminal et donc de l'interface utilisateur ? Comment garantir le déploiement, la mise à jour et l'usage des Applications métier ? Les utilisateurs abandonnent très vite face à la moindre difficulté rencontrée.

LA SÉCURITÉ EST UN DEVOIR

J'ai trouvé les RSSI assez préoccupés... et il y'a de quoi ! En effet, la mobilité a fait voler en éclats la barrière rassurante de la protection périmétrique : quel que soit son degré d'efficacité, le Firewall

(11) Étude Gartner et Ping Identity

installé sur un lien fixe ne sécurise ni les utilisateurs Remote, ni l'accès aux applications Cloud ni, bien entendu, la passoire que représente le smartphone (qu'il soit fourni par l'entreprise ou bien privé).

Le BYOD[12] est une réalité massive.

L'ouverture d'Active Sync est un vrai plaisir pour les utilisateurs mais le cauchemar des DSI, en permettant à chacun d'accéder à ses mails sur tout smartphone ou tablette (et je ne parle pas de Mac personnel) et donc de disperser les données de l'entreprise sur une multitude de terminaux non sécurisés.

Le smartphone est une extension de soi.

Il est notre vie personnelle et, bien entendu, notre vie professionnelle. Comment séparer les deux vies sur un terminal unique ? C'est l'enjeu minimum mais majeur des DSI.

LA DONNÉE EST UN SECRET

Un dernier big bang dans la mare de la transformation numérique : la sécurisation des données utilisateurs. Il reste peu de temps avant la mise en œuvre effective de la RGPD[13].

Cette règle s'impose à tous : des TPE jusqu'aux grandes entreprises. Elle aura même un impact majeur sur les PME et ETI qui sont sous-traitants de grandes entreprises car celle-ci vont leur reporter leurs exigences de sécurité.

DÉCIDEURS : À L'ACTION !

Personne ne peut ignorer cette contrainte qui sera parfois lourde de la transformation numérique. Pour le PME et ETI, il faut prendre le temps de mettre en place des solutions simples, efficaces et rapides.

(12) Bring Your Own Device
(13) Règlement Général sur la Protection des Données

Manager sa flotte mobile avec une solution MDM(14).
Quelle que soit la provenance des terminaux (privés ou professionnels). Cela permettra également d'effacer simplement les données des terminaux perdus ou volés.

Sécuriser la partie professionnelle des Smartphones.
Comme le mail ou les applications métiers grâce à un container et offrir enfin aux utilisateurs un accès libre aux serveurs et applications internes (intranet, disques...).

Pour le PME et ETI, des solutions standardisées existent sous un format Cloud qui élimine toute notion d'investissement ou de serveurs additionnels à administrer. L'entreprise peut également faire le choix d'un service managé sans engagement et facturé à l'usage. Cela permet aux entreprises d'avancer à leur rythme.

Et enfin, un signe qui ne trompe pas : pour la première fois, j'ai rencontré un CDO sur le salon ROOMn. Non pas un Chief Digital Officer (la partie est gagnée par le DSI) mais un Chief DATA Officer. DSI ou CDO : à vous de jouer !

LE + DE L'EXPERT

Il est indispensable de penser global en terme de sécurité. Une solution isolée ne suffit pas. Les acteurs spécialisés proposent de plus en plus de solutions complètes et intégrées avec une gestion unifiée de type UTM (Unified Threat Management).

(14) Mobile Device Management

Le point de vue des **EXPERTS**

Parole
D'INGÉNIEUR

BRICE PINSART
Manager System Engineering,
Fortinet

Pourquoi faut-il repenser son dispositif de sécurité ?

Aujourd'hui, face aux menaces actuelles, les équipements de sécurité dissociés ne répondent plus aux défis de la cybersécurité. Une approche différente s'impose. Les entreprises ont besoin d'une offre de sécurité globale et intégrée pour couvrir l'ensemble des périmètres : des objets connectés jusqu'au Cloud, du poste de travail au data center. La visibilité étant la clef, les dirigeants d'entreprise doivent pouvoir piloter leur protection d'un seul et même tableau de bord.

C'est ainsi que la cohérence et la synergie entre les différents modules et fonctionnalités du dispositif doivent garantir plus de simplicité et élever le niveau global de sécurité.
Avec Security Fabric - un écosystème ouvert à nos partenaires - nous travaillons d'ailleurs sur des offres de sécurité intégrées, capables de contrer les menaces à chaque étape de leur cycle de vie.

Le point de vue des
EXPERTS

Face aux évolutions des usages, au décloisonnement des environnements privés et professionnels, à l'explosion de la mobilité et des services hébergés dans le Cloud, les entreprises sont confrontées à un besoin d'adaptation permanent de leurs outils et processus. Cette transformation impose à l'entreprise une cohérence globale de son système d'information et rend vitale la sécurisation des informations et des données échangées.

Bblog | au plus près de votre business

ACTUALITÉS, DÉCRYPTAGES, AVIS D'EXPERTS

Découvrez