LA CYBERSÉCURITÉ ET VOTRE ENTREPRISE

Coût de la cybercriminalité et protection de vos données

SOMMAIRE

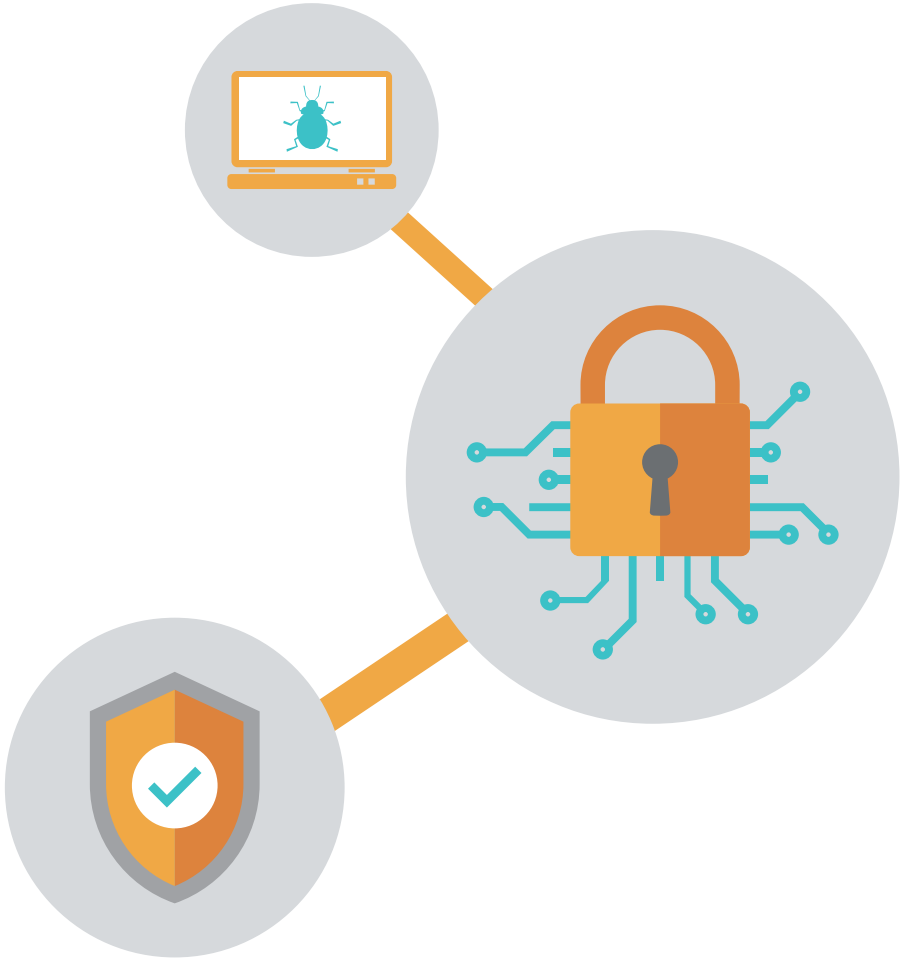
INTRODUCTION

« Beaucoup de cadres considèrent Internet comme le risque qui définit notre époque et notre génération. » – Dennis Chesley, spécialiste mondial en matière de gestion du risque, PwC[1]

La cybercriminalité n'est pas une menace nouvelle. Mais elle est en augmentation. Les pirates sont de plus en plus doués. Et ils disposent de toujours plus de moyens pour s'introduire dans un réseau. Notamment avec l'Internet des Objets qui multiplie le nombre de terminaux et par conséquent, le nombre de points d'accès. La taille des cibles augmente de façon exponentielle, en même temps que les perturbations occasionnées.

Le 21 octobre 2016, le fournisseur de services DNS américain Dyn a subi l'attaque par déni de service distribué (DDoS) la plus importante de l'histoire. Les sites web les plus importants du monde, dont Netflix,[2] Amazon et Twitter, se sont retrouvés hors ligne pendant des heures.

En janvier 2017, la Lloyds Bank a subi d'importantes interruptions de connexion. Les clients ne parvenaient pas à accéder à leurs comptes bancaires ni à effectuer de paiements. L'accès aux comptes via l'application mobile était également indisponible. Lloyds n'a rien confirmé, mais il y a de fortes présomptions qu'une attaque DDoS était à l'origine de la perturbation.[3]



Sources : [1] PwC : The Global State of Information Security Survey 2016 [2] http://thehackernews.com/2016/10/dyn-dns-ddos.html [3] https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

INTRODUCTION

De telles failles de sécurité sont la pire des publicités et sont coûteuses.

Dans le « 2016 Printer Security Survey Report » de Spiceworks (Rapport sur la sécurité des imprimantes 2016), 34 % des entreprises ont déclaré qu'une attaque déclenche un engorgement des centres d'appel et une augmentation du temps d'assistance, 29 % ont constaté une réduction de la productivité et de l'efficacité et 26 % ont signalé des problèmes générés par l'augmentation du temps d'arrêt du système.[4]

Près de 60 % des responsables de la sécurité interrogés pour un document d'évaluation IBM CSO ont indiqué que la sophistication des pirates dépassait celle de la défense de leur entreprise.[5]

Les DSI, inquiets, ont cité la cybersécurité comme l'un des 10 principaux problèmes de ces dix dernières années. Actuellement, elle occupe la deuxième place dans l'étude annuelle SIM Trends.[6]

Beaucoup des dommages causés sont évitables. Dans ce livre blanc, nous aborderons les idées reçues les plus répandues sur la cybersécurité, nous regarderons de plus près l'incidence de la cybercriminalité sur les entreprises et nous vous donnerons des clés pour mieux vous protéger contre ces attaques. Nous terminerons sur une prospective en abordant les menaces futures et comment nous y préparer.

Sources : [4] HP Printer Security Research 2016, Spiceworks [5] IBM CSO Assessment 2014 [6] SIM IT Trends Survey 2015

CINQ IDÉES REÇUES

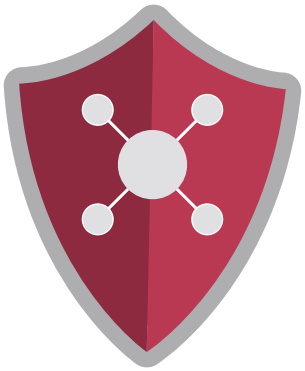
QUI PEUVENT EXPOSER LES ENTREPRISES À UN RISQUE DE CYBERCRIMINALITÉ

Des groupes d'entreprises très connues peuvent faire l'objet de piratage informatique, mais toutes sont exposées à ce risque. Voici cinq idées reçues sur la cybersécurité qui peuvent rendre les entreprises vulnérables aux pirates.

Violations de sécurité

Failles de sécurité

Pratiques de sécurité



Logiciel antivirus

Cyberattaques

1 LES ENTREPRISES PEUVENT SE REMETTRE RAPIDEMENT D'UNE VIOLATION

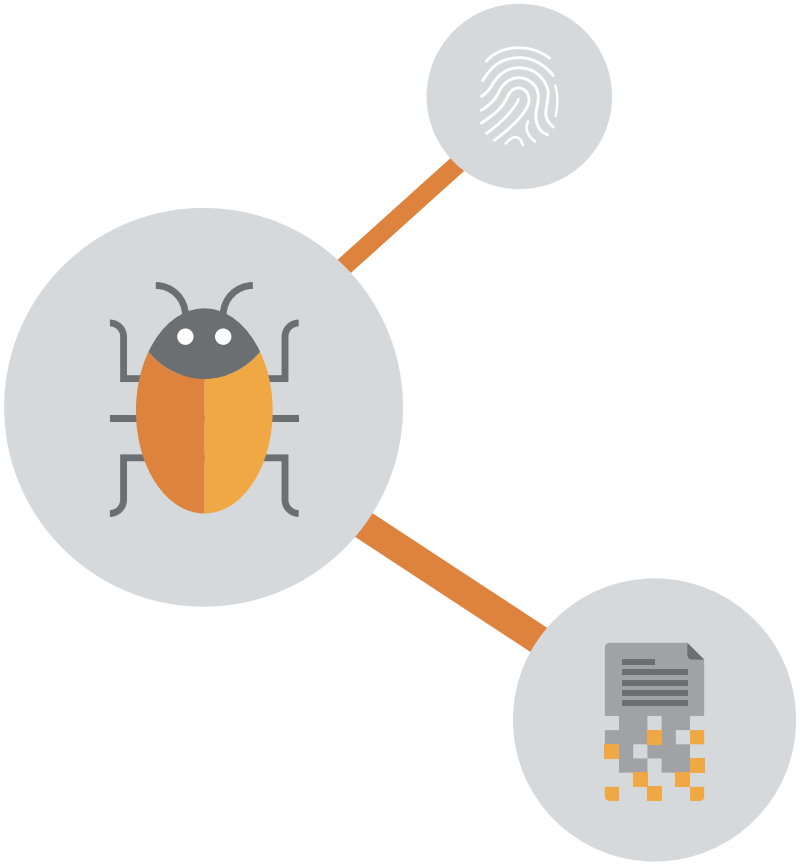
Il n'est jamais simple de mesurer le coût engendré par les violations de données pour les organisations commerciales. L'idée qu'une cyberattaque a pour effet visible la chute des valeurs boursières est couramment répandue.

Cependant, les valeurs boursières ne représentent qu'une partie, la première, de l'histoire. Les valeurs boursières peuvent remonter en quelques semaines, mais d'autres coûts peuvent s'accumuler à long terme. Nouveaux programmes de sécurité, personnel remplaçant, dépenses juridiques.

Tous ces facteurs peuvent profondément perturber une entreprise à long terme et bien des mois encore après une attaque. En outre, les coûts ne cessent d'augmenter. Une étude Ponemon récente indique que le coût annuel moyen d'un piratage est passé de **7,7 millions** de dollars en 2015 à **9,5 millions** en 2016.[7]

Source : [7] Ponemon Institute : Étude sur le coût de la cybercriminalité en 2016

2 LES FUITES DE SÉCURITÉ SE PRODUISENT RAREMENT ; UNE PROTECTION SOLIDE N'EST DONC PAS NÉCESSAIRE



L'institut IDC a déterminé[8] que la proportion des entreprises ayant subi une violation a atteint 99 % en 2016. En outre, le nombre de sociétés ayant indiqué avoir subi 6 à 10 violations par an a bondi de 9 % en 2014 à 18,9 % en 2016.[9]

Ces chiffres sont sans doute inférieurs à la réalité. Les intrusions ne sont souvent pas signalées, car les sociétés cherchent à éviter la mauvaise presse qui leur est associée.

L'autre aspect que cette idée reçue néglige est l'impact négatif qu'une fuite peut engendrer. Votre société ne subira peut-être qu'une fuite. Mais une fuite peut occasionner des difficultés majeures.

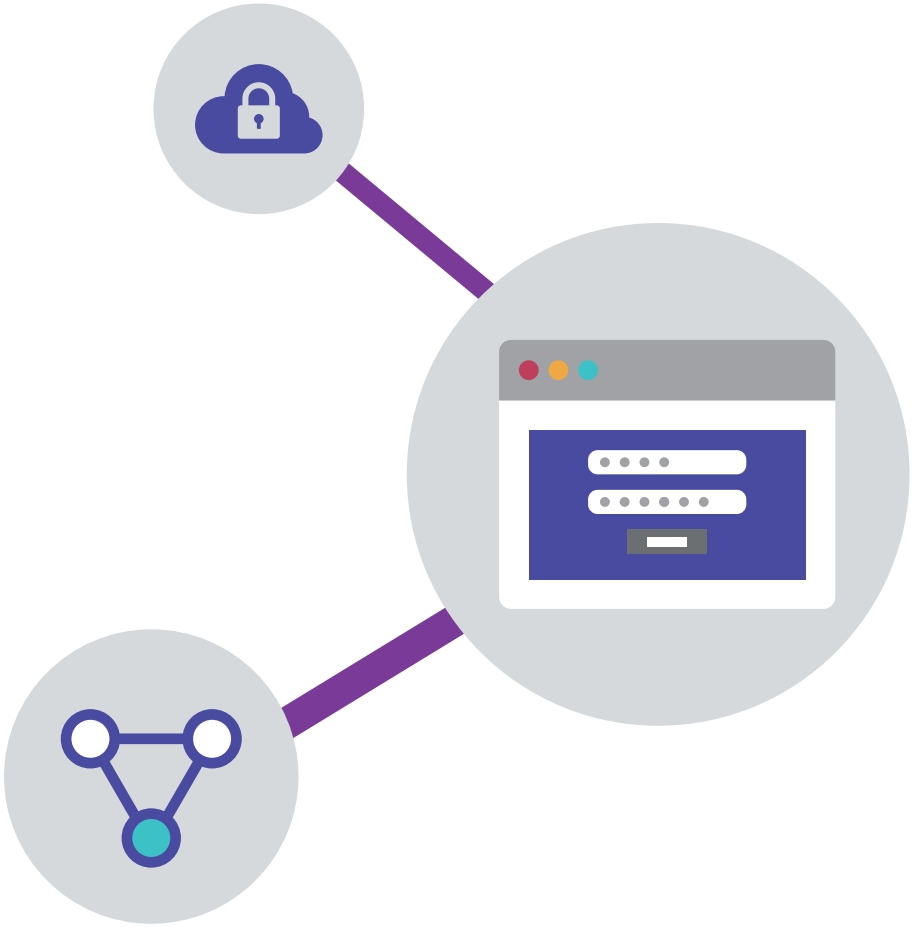
Sources : [8] IDC [9] Ponemon Institute : Étude sur le coût de la cybercriminalité en 2016

3 NOUS AVONS RECRUTÉ UN SPÉCIALISTE INFORMATIQUE POUR GÉRER LA SÉCURITÉ, LA QUESTION EST DONC RÉGLÉE POUR NOUS

Même si le recrutement d'un spécialiste est une bonne idée, chaque salarié de la société doit suivre une formation sur les bonnes pratiques en matière de cybersécurité.

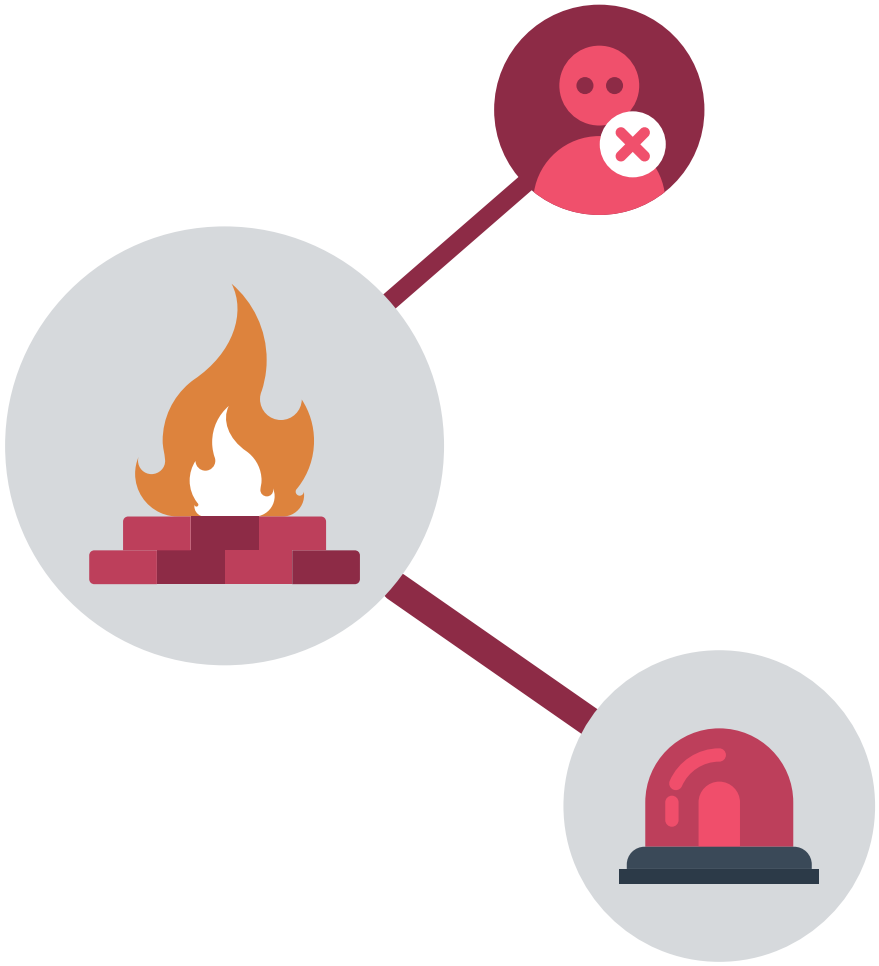
Pensez au collègue qui télécharge naïvement une pièce jointe d'un e-mail malveillant, un autre visite un site web dangereux, qui infecte le réseau de la société via un programme malveillant qui ralentit les ordinateurs ou qui envoie des informations sensibles à un cybercriminel.

Selon le rapport « 2016 Cyber Threat Report » de CyberEdge, les organisations ont signalé la « faible sensibilisation du personnel à la sécurité » comme étant le principal problème les empêchant de se protéger contre les menaces de sécurité. Ce facteur a été classé devant d'autres comme les « carences en budget » ou le « manque de personnel qualifié ».[10]



Source : [10] Ponemon Institute : Étude sur le coût de la cybercriminalité en 2016

4 TOUS NOS SYSTÈMES SONT ÉQUIPÉS D'UN TRÈS BON ANTIVIRUS, NOUS SOMMES DONC BIEN PROTÉGÉS



L'antivirus scanne les systèmes pour rechercher des programmes malveillants téléchargés à partir de sites web ou d'e-mails. Cependant, les pirates ont d'autres moyens de contourner cette protection.

Voici les cyberattaques qui ne peuvent pas être bloquées par l'antivirus : les attaques par déni de service distribué (DDoS), où un site web est inondé de trafic parasite qui le ralentit ou qui le met en panne ; les attaques Web, où les pirates injectent un code malveillant dans un site dans le but de voler des données ou d'espionner à distance ; l'accès des pirates via des appareils volés.

5 SI UN INTRUS S'INFILTRE DANS NOS SYSTÈMES, NOUS NOUS EN APERCEVONS TOUT DE SUITE

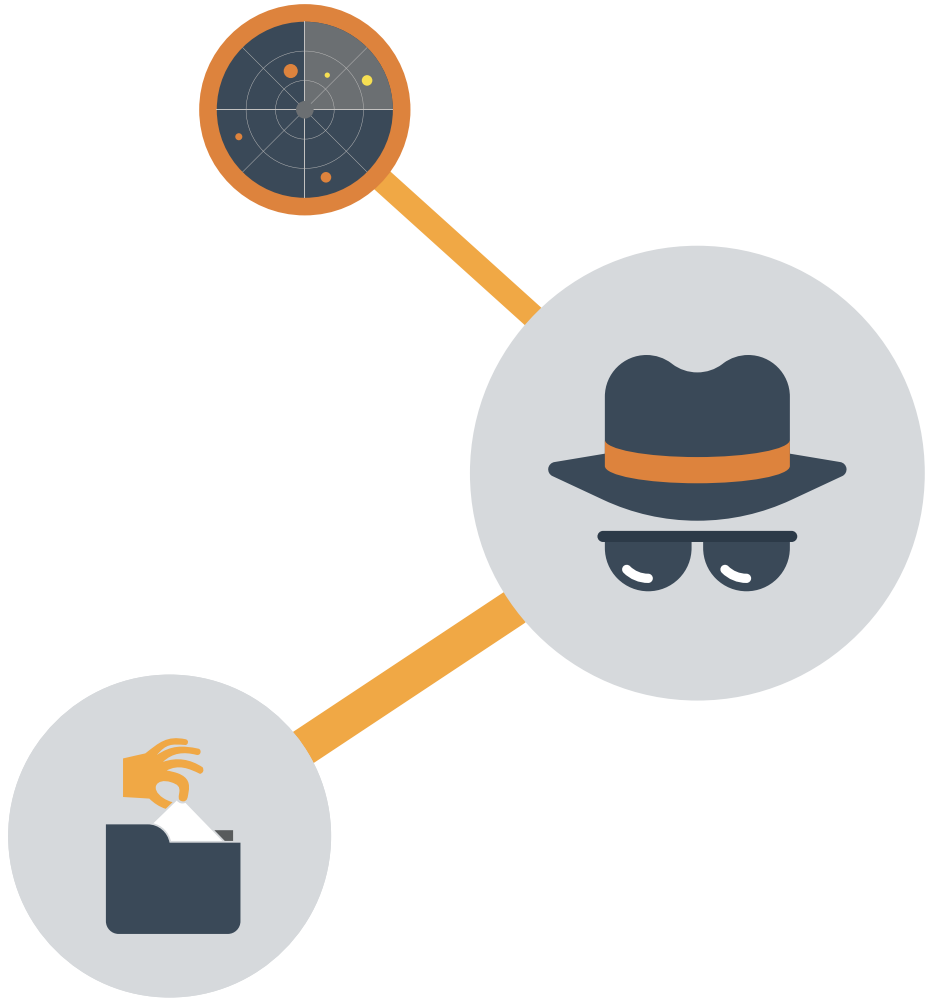
Il n'est pas facile de détecter une cyberattaque. Le programme malveillant qui pénètre dans un système peut ne pas interrompre les opérations immédiatement ; cependant, il peut espionner le système et fournir au pirate des informations lui permettant de mettre au point d'autres attaques plus ciblées, souvent pour accéder à l'ensemble du réseau.

Ces attaques sur des systèmes spécifiques sont considérées comme des menaces persistantes avancées (APT). Les attaques APT se caractérisent par une surveillance continue et une obtention de données à partir d'une infrastructure informatique particulière au fil du temps, qui passe souvent inaperçue.

Le Daisy Group, une société de conseil en informatique, estime que la moitié des entreprises britanniques pourraient être piratées en moins d'une heure.

CONSEIL :
la surveillance du trafic des données sortantes (s'il est supérieur au trafic normal) permet d'identifier un vol de données (il peut s'agir d'une attaque APT).

PASSER À L'ACTION :
sélectionnez un logiciel de sécurité avec protection de données tel que HP SureStart, qui permet de restaurer automatiquement le BIOS d'un ordinateur lorsqu'une attaque de programme malveillant est détectée et d'arrêter ainsi les violations avant de compromettre les données.



QUELLE EST L'ORIGINE DES MENACES ?

La protection de votre réseau commence par la prise de conscience de vos points faibles

Cause la plus probable des violations de données :[11]

1 = le plus probable
4 = le moins probable

Imprudence en interne — **1,67**

Agresseur externe — **2,89**

Action criminelle ou malveillante en interne — **2,45**

Combinaison d'attaques internes et externes — **3,49**

Types les plus fréquents de menaces externes :

- **30%** Hameçonnage
- **32%** Virus
- **38%** Malware

Causes des violations internes :[12]

- **21%** Utilisation d'un réseau domestique/public par les salariés
- **29%** Utilisation d'appareils personnels par les salariés
- **42%** Erreur humaine/de l'utilisateur

Sources : [11] http://www.kilpatricktownsend.com/_assets/Kilpatrick%20Townsend%20Report%20Final.pdf [12] Ponemon Institute : Étude sur le coût de la cybercriminalité en 2015

QUEL EST LE COÛT DE LA RÉPARATION DE LA CYBERCRIMINALITÉ ?

Types de cyberattaques les plus coûteuses :

25 %

1,7 millions d'€

Codes et programmes malveillants

Logiciels qui nuisent à un système en créant des failles de sécurité et qui endommagent des fichiers ou volent des données (notamment par des scripts, virus et vers)

24 %

1,1 millions d'€

Déni de service distribué

Les attaques « DDoS » consistent à inonder un réseau pour rendre indisponibles le site et les serveurs d'une société

16 %

760 000 €

Attaques par Internet

Attaques visant les visiteurs de votre site (par exemple, un code injecté qui redirige les navigateurs vers le chargement d'un programme malveillant)

13 %

620 000 €

Appareils volés

La disparition d'appareils à l'usage des employés permettant d'accéder aux comptes des salariés de la société peut être à l'origine de vols de données et d'usurpations d'identité

9 %

420 000 €

Hameçonnage et ingénierie sociale

E-mails ou fenêtre publicitaires se faisant passer pour des demandes de connexion légitimes

9 %

420 000 €

Personnes malveillantes internes à l'entreprise

Communication d'informations sensibles par des salariés

4 %

190 000 €

Botnets

Réseaux d'ordinateurs infectés et contrôlés pour une activité malveillante telle que l'envoi de virus

Source : [13] Ponemon Institute : Étude sur le coût de la cybercriminalité en 2015

L'INCIDENCE DE LA CYBERCRIMINALITÉ SUR LES ENTREPRISES

Le vrai coût de la cybercriminalité dépasse la simple réparation des dommages provoqués par une attaque

Les violations de la sécurité génèrent des coûts importants. D'une manière générale, une violation peut avoir une incidence sur les finances de votre société de trois façons.

Ressources de la société

Il vous faudra évidemment remettre de l'ordre. Cela représente beaucoup de temps et d'argent. Vous devrez peut-être mettre d'autres projets générateurs de recettes en suspens.

Amendes/pénalités

Vous pouvez écoper d'une amende en cas de non-conformité (p. ex., HIPAA). Une fois que le Règlement général sur la protection des données (RGPD) de l'UE sera entré en vigueur l'année prochaine, les sociétés considérées comme négligentes risquent une amende totale s'élevant à 4 % de leur chiffre d'affaires global. Vous pouvez même faire l'objet de poursuites judiciaires si la fuite donne lieu à une violation de la confidentialité du client.

Réputation ternie

Cela peut être l'une des incidences les plus graves d'une violation. Les clients, la presse et le grand public gardent très longtemps en mémoire les failles de sécurité. Regagner la confiance est un processus qui peut prendre beaucoup de temps.

ANATOMIE DE L'ATTAQUE IMPRÉVUE

Lorsque Sony Pictures a été piraté en 2014, les pirates sont tout simplement passés par la porte d'entrée.[14]

Selon « Lena » du groupe de pirates Guardians of Peace (GOP) – qui a revendiqué l'attaque – Sony « ne prend aucune mesure pour sa sécurité physique ». Pour accéder au réseau de Sony, ils se sont tout simplement introduits dans les locaux et ont volé les identifiants informatiques d'un administrateur système.

Les pirates ont en effet réussi à installer un programme malveillant qui s'emparait de fichiers privés, code source et mots de passe des bases de données Oracle et SQL. À partir de là, ils ont pu voler des calendriers de production de films, des e-mails, des documents financiers, etc., qui, pour beaucoup d'entre eux, ont été publiés sur Internet.

Les pirates ont menacé de publier d'autres informations sensibles et hautement confidentielles si la société ne retirait pas le film « L'Interview qui tue » des salles de cinéma.

Sony a finalement abandonné, en perdant au passage une quantité incalculable de recettes et en voyant sa réputation sérieusement ternie.

Sony a commis deux erreurs. La première, négliger la possibilité que des intrus puissent accéder physiquement aux données de la société, et la seconde, ne pas investir dans plusieurs niveaux de sécurité, ce qui aurait permis d'éviter l'accès aux informations sensibles après la première violation.

Après l'attaque, Bruce Schneier, expert de la sécurité, a écrit : « Tous les réseaux sont vulnérables face à des pirates suffisamment expérimentés, dotés de ressources financières et motivés. » L'astuce consiste à reconnaître les vulnérabilités de votre réseau. Il peut s'agir de la porte principale.

PASSER À L'ACTION :
Créer un plan de réponse aux violations pour chaque département, du service informatique au service client, pour réduire le temps de réparation.

CONSEIL :
Plusieurs types de programmes malveillants peuvent être envoyés sous forme de pièce jointe d'un e-mail. Formez le personnel à la reconnaissance des fichiers suspects (ces derniers sont conçus pour être assimilés à des documents légitimes).

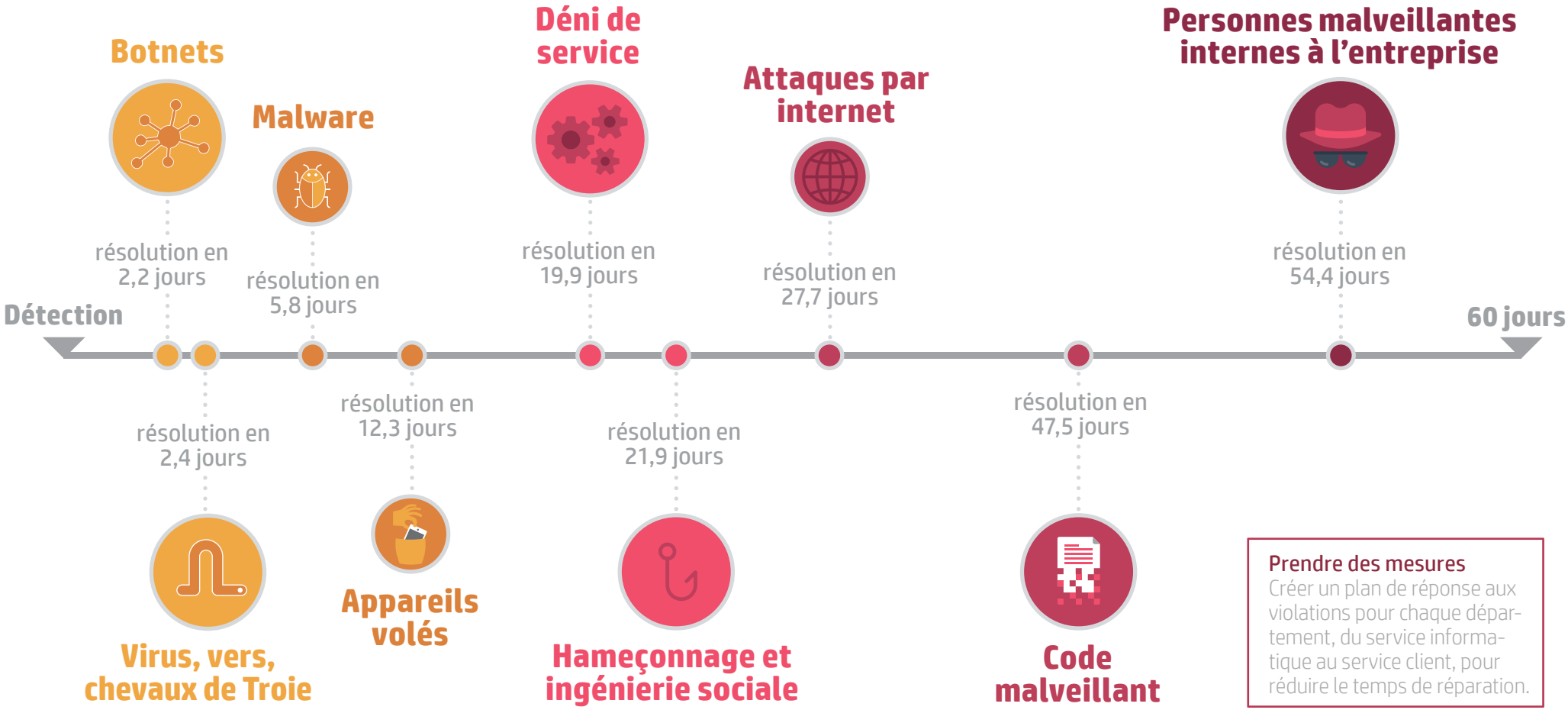
Selon une enquête menée en juin 2017 par l'Institut pour la criminologie de la KUL sur 300 entreprises belges

- Deux tiers des entreprises intérrogées ont été victimes d'au moins une forme de cybercriminalité l'année précédente.[15]
- La majorité des signalements concernent des tentatives de pénétrer dans certaines parties du système informatique de l'entreprise sans que les données n'aient été volées ou endommagées (50%) et les cyberattaques qui occasionnent des perturbations du système (46%)[15]
- 9% des sociétés visées par l'extorsion et le chantage ont subi des dégâts évalués à plus de 10 000 euros. Selon la nature de l'attaque, le chiffre d'affaires a baissé de plus de 50 000 euros dans 3% des cas.[15]

Sources : [14] https://www.rtbf.be/info/monde/detail_piratage-de-sony-de-la-cyberattaque-au-cyberterrorisme?id=8603146
[15] https://www.rtbf.be/info/economie/detail_deux-tiers-des-entreprises-belges-victimes-de-la-cybercriminalite?id=9647431

CYBERCRIMINALITÉ : TEMPS DE RÉPARATION

Combien de temps cela prend-il pour réparer les dommages causés par le piratage informatique ? L'institut Ponemon[16] indique une moyenne de 46 jours, ce qui représente un temps considérable pour les PME souhaitant être opérationnelles en continu.



Prendre des mesures
Créer un plan de réponse aux violations pour chaque département, du service informatique au service client, pour réduire le temps de réparation.

Source : [16] Ponemon Institute : Étude sur le coût de la cybercriminalité en 2015

COMMENT PROTÉGER VOTRE ENTREPRISE CONTRE LA CYBERCRIMINALITÉ

Conseils et stratégies essentiels pour la cybersécurité des entreprises

Voici six cibles fréquentes des pirates souhaitant violer les systèmes des entreprises (et ce que vous pouvez faire à l'heure actuelle pour vous protéger).

Bases de données clients

Services cloud

Smartphones et tablettes du personnel

Erreurs des employés

Internet des objets

Passerelles de réseau

À mesure que nous avançons vers un monde de plus en plus numérique où les données n'ont jamais été aussi précieuses, la cybercriminalité peut revêtir plusieurs formes. Les cybercriminels sont souvent à la recherche d'informations et, en raison du nombre grandissant d'appareils connectés utilisés sur le lieu de travail (des smartphones et tablettes aux imprimantes sans fil), le nombre de points d'accès potentiellement ciblés par les pirates est également de plus en plus important.

1 BASES DE DONNÉES DES CLIENTS

Les données financières ne sont pas la seule cible des pirates. Des informations telles que les noms et les adresses électroniques peuvent être utilisées pour les usurpations d'identité, le spam ou le piratage d'autres comptes.

Pour un bon pirate, le summum est de pirater les entreprises qui servent d'autres entreprises de plus grande taille. On peut voir cela comme l'équivalent numérique de la pénétration par effraction dans un magasin de matériel, dans le but d'avoir accès au mur du sous-sol, mur derrière lequel se trouve la salle des coffres d'une banque centrale.

Une fois que les pirates ont accédé au système plus petit, ils sont mieux placés pour accéder aux données des clients détenus par ses grandes sociétés clientes. Comment la base de données de votre client pourrait-elle être compromise ? Des virus, des vers et des chevaux de Troie (téléchargés à partir de sites ou d'e-mails malveillants) peuvent libérer le code nécessaire pour qu'un pirate pénètre dans une base de données et vole des informations.

Comment protéger les données de vos clients

- Utilisez un logiciel conçu pour les entreprises qui offre une protection du réseau, de la messagerie et du terminal.
- Mettez toujours votre logiciel de sécurité à jour afin de bloquer les programmes malveillants en constante évolution.
- Téléchargez les mises à jour logicielles pour vos programmes système car les anciens programmes peuvent contenir des failles susceptibles d'être exploitées par les pirates.

2 SERVICES CLOUD

Comment protéger les données de vos clients

- Chiffrez vos données les plus importantes à l'aide d'outils tels que la technologie Smartcrypt de PKWARE, qui utilise des politiques d'accès pour déterminer la complexité du chiffrement. De cette manière, les utilisateurs autorisés voient les données qu'ils sont censés voir, et les utilisateurs non autorisés ne voient rien.
- Créez un mot de passe fort pour votre compte cloud. De même, lors du paramétrage de votre compte cloud, définissez précisément les personnes autorisées à accéder à vos données et l'utilisation qu'elles peuvent en faire.
- Demandez une double authentification, comme un code Smartphone et un mot de passe, pour apporter des modifications aux données du cloud, telles que le téléchargement, la suppression ou le déplacement de fichiers.

Le recours au cloud computing dans les entreprises françaises s'accroit largement.

Selon l'étude sur le cloud computing de l'IDG de 2016[17], 70 % des entreprises ont au moins une infrastructure cloud. Tripwire, quant à lui, a révélé que 90 % utilisent le cloud comme infrastructure et/ou pour le stockage de données – y compris vitales.[18]

Même si la sécurité reste, bien sûr, un sujet de préoccupation, les données sont généralement plus en sécurité sur le cloud – stockées sur des serveurs extérieurs par une société dont la réputation repose sur sa capacité à les protéger.

C'est pourquoi 64 % des entreprises interrogées par Tripwire considèrent le cloud comme étant beaucoup plus sûr que les systèmes existants.

Heureusement, cette confiance est bien placée. Selon l'étude BIS de 2015,[19] seules 7 % des entreprises (grandes et petites) ont souffert d'une violation sérieuse de leurs services cloud, cela étant généralement dû aux droits d'accès ou à la protection insuffisante des mots de passe. Un cloud sûr nécessite encore une gouvernance solide de la sécurité interne. Pensez simplement à la porte d'entrée de Sony.

53 % des sites d'entreprises commerciales et de services publics belges ont recours à des applications Cloud. [20]

Sources :
[17] https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey
[18] https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/
[19] 2015 Small Business Survey. Ministère des Entreprises, de l'Innovation et des Talents
[20] https://www.computerprofile.com/fr/analytics-papers-fr/plus-de-la-moitie-des-sites-denterprises-belges-utilise-des-applications-cloud/

3 SMARTPHONES ET TABLETTES DU PERSONNEL

De nombreuses personnes utilisent leurs appareils personnels pour les tâches de bureau.

La politique BYOD (Apportez vos appareils personnels) des entreprises est un moyen efficace de rentabiliser les Smartphones que les employés possèdent déjà. Selon une étude HP consacrée à la mobilité a été réalisée auprès de 1 130 décideurs informatiques de huit pays européens en 2015, l'adoption des terminaux mobiles devrait augmenter au sein des entreprises d'ici 2020, les tablettes, smartphones, 2-en-1 et autres phablettes progressant de respectivement 17 %, 11 %, 12 % et 5 %.[21]

On estime qu'une application Android sur cinq contient une forme de programme malveillant invasif, susceptible d'être transmis aux fichiers et systèmes de l'entreprise pour surveiller les activités ou dérober des informations.

Dans une entreprise interrogée sur cinq, les failles de sécurité sont dues à l'utilisation de terminaux personnels dans un contexte professionnel. Ainsi, plus d'un tiers (36 %) des décideurs soucieux de la sécurité du BYOD déclarent que le transfert des logiciels malveillants et des virus à partir d'appareils personnels représente leur principale crainte.[21]

Les employés qui se font dérober leur téléphone peuvent involontairement ouvrir la porte aux pirates. Un voleur de téléphone peut revendre l'appareil à un acheteur sur le marché noir. Ce dernier peut alors en retirer les informations lui permettant d'accéder à l'entreprise de la victime ou de pénétrer dans les systèmes d'un plus gros client. Pourtant, moins de la moitié des décideurs informatiques (43 %) sont convaincus que les dispositifs BYOD sont correctement protégés. À titre de comparaison, 70 % estiment que les produits fournis aux employés par leur entreprise sont sécurisés.[21]

Comment sécuriser les appareils du personnel

- Installez un outil de détection des menaces tel que X-Ray pour Android de Duo afin de faciliter la détection des applications malveillantes et des codes suspects.
- Demandez aux employés d'activer l'effacement à distance (disponible gratuitement pour Android, iPhone et Windows Phone ; sur abonnement pour BlackBerry) afin que, en cas de perte, les données sensibles (professionnelles et personnelles) puissent être effacées.
- Demandez aux employés d'activer le chiffrement sur leurs Smartphones afin de protéger les données (cette option est activée par défaut sur les nouveaux téléphones iOS et Android).

Source : [21] http://www.infodsi.com/articles/153826/securite-est-obstacle-majeur-adoption-byod.html

4 ERREURS DES EMPLOYÉS

Comment aider votre personnel

- Expliquez à votre personnel les meilleures pratiques concernant la cybersécurité et organisez régulièrement des formations pour qu'ils soient informés des dernières menaces.
- Développez un protocole de sécurité adapté à votre entreprise et aux types de données qu'elle traite.
- Créez une équipe pour la communication de votre politique de cybersécurité aux employés ainsi qu'aux clients et partenaires commerciaux.

Le fondement de base de la cybersécurité est une bonne politique concernant les mots de passe. Et pourtant, 31 % des violations de sécurité les plus graves en 2015 étaient dues à un incident lié au personnel.

Qu'il s'agisse du piratage d'un mot de passe faible, du vol de documents envoyés par messagerie via une connexion non sécurisée ou de l'hameçonnage par e-mail d'un employé en particulier, les pirates exploitent souvent les erreurs humaines.

5 SE PRÉPARER À L'INTERNET DES OBJETS

Le cabinet de recherche IDC prévoit que le nombre de dispositifs connectés à Internet atteindra les 30 milliards en 2020, contre une estimation de 13 milliards actuellement.[22]

Alors que les ordinateurs de bureau sont sécurisés au moins par un mot de passe, et idéalement par un logiciel de sécurité, les files d'attente et travaux d'impression ne sont souvent pas protégés par ce type de protocole de sécurité.

Les imprimantes non sécurisées, ainsi que le matériel en réseau, peuvent être la proie de logiciels de « sniffing (reniflage) », capables d'enregistrer les documents en attente d'impression, le trafic sur le réseau, les noms et les mots de passe d'utilisateurs, le tout étant retransmis au serveur du cybercriminel.

Il est important de noter ici que l'attaque Dyn fortement médiatisée était liée à un réseau de caméras CCTV connectées à Internet et conçues par une seule entreprise, XiongMai Technologies. Selon la société de sécurité Flashpoint.

Cela indique que chaque appareil de votre réseau correspond à un point terminal et que votre réseau n'est pas plus solide que son appareil le moins sécurisé. Environ 97 % des entreprises disposent de pratiques de sécurité pour leurs ordinateurs de bureau/ordinateurs portables, 77 % pour leurs appareils mobiles, mais seulement 57 % appliquent des pratiques de sécurité à leurs imprimantes.[23] La seule façon de se protéger pour chaque entreprise est d'appliquer des pratiques de sécurité à chacun de ses terminaux.

Se préparer à l'Internet des Objets

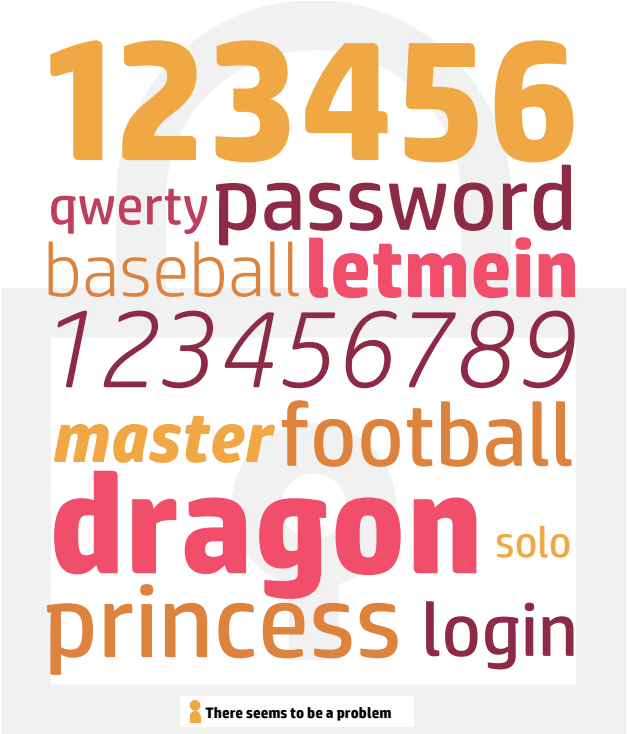
- Supprimez ou désactivez les fonctionnalités inutiles du matériel. Plus les fonctions sont nombreuses, plus le nombre de points de passage des pirates est élevé.

Sources : [22] PwC : The Global State of Information Security Survey 2016 [23] HPI Printer Security Research, Spiceworks 2016

MOTS DE PASSE ET RANSOMWARE

Les mots de passe les plus courants

Début 2013, un journaliste d'Ars Technica qui n'avait aucune expérience de la cybercriminalité ni de l'infiltration dans des systèmes protégés par mots de passe a réussi à déchiffrer 8 000 sur plus de 16 000 mots de passe chiffrés en une seule journée*. Alors quelles chances ont ces mots de passe extrêmement courants de résister à un pirate déterminé ?



Qu'est-ce qu'un ransomware ?

Les cybercriminels utilisent de plus en plus le ransomware, une forme de programme malveillant visant à prendre le contrôle des systèmes informatiques qui ne peuvent alors être débloqués qu'en échange d'une rançon sous forme de bitcoins. Voici une explication plus détaillée de la manière dont ces attaques fonctionnent.

1. Installation	Un code malveillant travaille seul dans votre ordinateur à la suite d'un téléchargement involontaire, via un e-mail ou un site Web malveillant.
2. Alerte envoyée au serveur de base	Le rançongiciel se connecte à l'aide de son serveur central pour créer une clé de chiffrement.
3. Chiffrement de vos fichiers	Le rançongiciel analyse les fichiers sur votre réseau et les chiffre, les rendant ainsi inaccessibles.
4. Extorsion	Un message apparaît généralement sur l'ordinateur de l'utilisateur indiquant le délai et le montant à payer pour déchiffrer les fichiers avant de les effacer.
5. Paiement	Le chef d'entreprise doit acheter de la monnaie virtuelle, comme les bitcoins, pour les transférer au pirate informatique, avec l'espoir qu'il déchiffre les fichiers.

* Splashdata

6 PASSERELLES DE RÉSEAU

Lorsque des pirates souhaitent pénétrer dans un réseau, ils peuvent déclencher une attaque DDoS ; des milliers de machines infectées par un programme malveillant s'unissent pour générer un trafic parasite tellement important que le réseau devient indisponible sous le poids de l'attaque.

Souvent, les pirates DDoS souhaitent détourner l'attention des administrateurs du site en gelant le système, pendant qu'ils dérobent des données ou installent des programmes malveillants pour planifier des vols ultérieurs de données. Certaines attaques DDoS sont le fait de « script kiddies », des pirates débutants qui souhaitent simplement prendre le contrôle d'un site Web car ils en ont la capacité. Même une interruption de quelques heures d'un site Web peut avoir un effet dévastateur sur les résultats et la réputation d'une entreprise.

CONSEIL :
investissez dans du matériel offrant une protection intégrée, comme l'authentification avancée et les outils de chiffrement.

Comment sécuriser votre réseau

- Construisez des systèmes capables de vérifier les données circulant sur votre réseau. Un pic d'activité soudain peut indiquer une attaque, alors qu'une activité constante mais inexpliquée peut indiquer qu'un cheval de Troie transmet des données à son vaisseau-mère.
- Filtrez tout le trafic afin de vous assurer que seul le trafic nécessaire à votre entreprise se retrouve sur votre réseau.
- Vérifiez que chaque routeur, commutateur ou appareil connecté fonctionne avec les mêmes fonctionnalités et logiciel de référence, et téléchargez toujours les mises à jour logicielles.

L'AVENIR DE LA CYBERSÉCURITÉ DES ENTREPRISES

Alors que les entreprises sont de plus en plus dépendantes d'Internet, il devient indispensable de créer des défenses et une cybersécurité solides.

Aujourd'hui, les employés apportent leurs propres appareils au travail. Les propriétaires utilisent des plates-formes de cloud computing et externalisent leurs services techniques principaux. Et plus de quatre millions de britanniques travaillent maintenant à leur domicile. La cybersécurité devient plus difficile lorsque ni l'appareil, ni l'infrastructure, ni le lieu de travail ne sont contrôlés.

De même, les smartphones nous ont appris qu'il est possible de travailler partout et n'importe quand. Dans un café aussi bien qu'au bureau, dans le train ou de chez soi. Nous utilisons les réseaux Wifi publics pour traiter d'importantes quantités de données professionnelles et personnelles, souvent via des smartphones peu sécurisés.

Ce changement n'échappe certainement pas à l'attention des criminels. La sécurité souffre lorsque nous ne prêtons pas attention à nos conditions de travail.

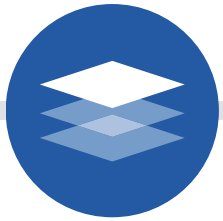
Dans les années à venir, il faudra bien plus qu'un simple ajout d'antivirus à nos appareils ou la modification de nos mots de passe tous les six mois. Les entreprises devront adopter des mesures de sécurité améliorées, fonctionnant aussi bien à distance que dans un bureau régi par un administrateur informatique.

Pour les organisations distribuées de demain, la cybersécurité repose sur une analyse sophistiquée capable d'isoler les comportements inhabituels et une sécurité en couches capable de protéger tous les points d'accès.

L'AVENIR DE LA CYBERSÉCURITÉ DES ENTREPRISES

Analyse : enquêteur de la cybersécurité

Même si votre site ne génère pas un trafic important, il disposera de modèles. L'utilisation d'outils d'analyse capables de mesurer et de noter l'activité peut faciliter la détection des problèmes. Ces outils fonctionnent en suivant et en décrivant le comportement normal dans un premier temps afin de détecter les anomalies dans un second temps. Après détection, les administrateurs peuvent passer à l'offensive et contrecarrer les attaques avant qu'elles ne déclenchent un cyber-chaos.



Organisation en couches : garder une longueur d'avance sur les pirates

Parfois appelée « défense en profondeur », la sécurité en couches protège chaque point d'accès de différentes manières. Les approches courantes comprennent les certificats SSL à validation étendue rendant difficile la falsification des identifiants nécessaires pour accéder à un réseau sécurisé. Renforcer cela avec une authentification multifactorielle qui contraindrait les pirates à casser plus qu'un simple mot de passe peut s'avérer utile.

Quelle que soit la technologie spécifique en œuvre, le principe qui sous-tend l'organisation en couches est que toutes les zones sensibles de votre réseau d'entreprise soient verrouillées d'une manière ou d'une autre. Vos utilisateurs et partenaires devront sans doute redoubler d'effort et avoir besoin de plus de temps pour accéder aux données importantes, mais tous ces inconvénients vous permettront de gagner en tranquillité d'esprit pour votre entreprise.

Passer à l'action maintenant

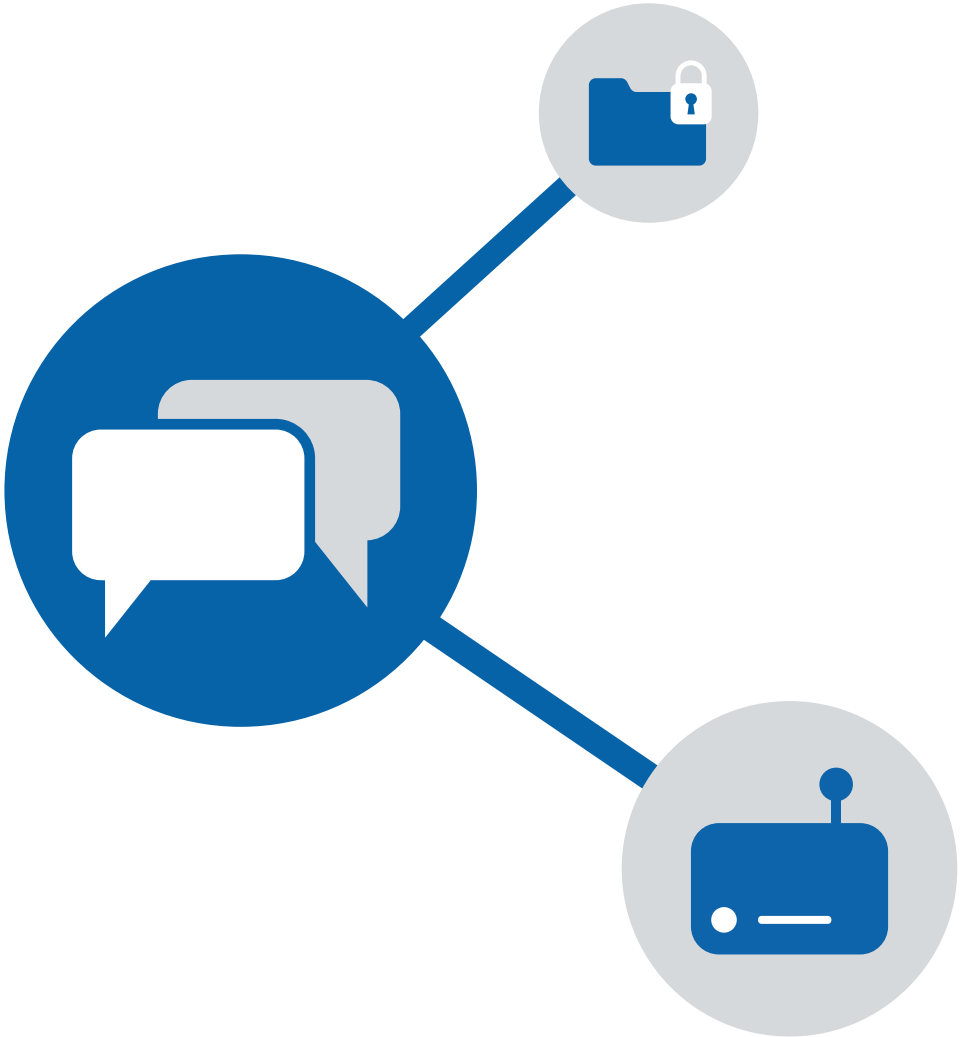
Investir dans un logiciel de cybersécurité et dans la formation constitue la meilleure défense. Commencez par réaliser un audit de vos systèmes et de votre infrastructure. Votre action est-elle suffisante ? Que pourriez-vous améliorer ?

Enfin, vous pouvez également faire appel à nos experts HP Inc. Notre base de connaissance collective est axée sur la conservation d'une longueur d'avance sur les menaces, et pas simplement sur les réponses à y apporter. Pour en savoir plus, rendez-vous sur le site HP.com.

CONSEIL :
Suivez et décrivez le comportement normal dans un premier temps afin de détecter les anomalies dans un deuxième temps.

CONSIDÉRATIONS CONCERNANT LA SÉCURITÉ DES TERMINAUX

Sécurisation de chaque dispositif de votre réseau



La recherche sur la sécurité réalisée par Spiceworks[24] a montré que les sources principales des menaces de sécurité auxquelles les entreprises doivent faire face sont les :

- Ordinateurs portables et ordinateurs de bureau : 81 % externes et 80 % internes
- appareils mobiles : 36 % externes et 38 % internes
- imprimantes : 16 % externes et 16 % internes

Laquelle de ces menaces nécessite des mesures de sécurité urgentes ? Réponse : elles sont toutes concernées. Cela semble tout simplement évident, mais un nombre inquiétant d'entreprises sélectionnent encore avec parcimonie les appareils à sécuriser.

Le point de vue de HP est que tous les appareils qui se connectent à votre réseau doivent être sécurisés. Pour dire les choses simplement, votre réseau n'est pas plus sécurisé que votre appareil le moins sécurisé.

La logique intuitive pourrait vous faire penser que la sécurisation d'une imprimante connectée n'est pas aussi importante que la sécurisation de votre parc d'ordinateurs portables. Mais le risque est le même. Les pirates sont réputés pour cibler les appareils tels que les imprimantes, ou n'importe quel appareil intelligent qui se connecte à votre réseau. Car ils savent que ces appareils sont généralement mal sécurisés, alors qu'ils offrent le même niveau d'accès à votre réseau.

Source : [24] Recherche HPI de 2016 sur la sécurité des imprimantes (Spiceworks)

HP : INNOVER DANS UN NOUVEAU PAYSAGE

La cybersécurité change. Nous disposons des outils pour vous aider à vous défendre.

Il n'existe pas de solutions rapides en matière de cybersécurité. Une défense solide nécessite une approche multidimensionnelle englobant les réseaux, les appareils et le personnel. Le choix de la technologie adaptée est un bon début.

Chez HP, la sécurité est la priorité. Notre gamme HP Elite propose des fonctions de sécurité de pointe disponibles nulle part ailleurs, comme HP SureStart (le premier BIOS à réparation automatique au monde).

HP équipe ses appareils des fonctions suivantes :

- **HP WorkWise :** lors de l'utilisation du Bluetooth, la machine se verrouille automatiquement lorsque vous vous absentez et se déverrouille lorsque vous revenez.
- **Sécurité biométrique :** la reconnaissance faciale et d'empreintes digitales permet l'accès aux utilisateurs authentifiés par contrôle biométrique uniquement.
- **Écrans HP SureView* :** l'écran assombri empêche les curieux de voir le contenu de votre écran, protégeant ainsi vos données confidentielles lorsque vous travaillez en déplacement.
- **BIOS à réparation automatique HP SureStart :** l'ordinateur HP Elite contrôle son BIOS toutes les 15 minutes. S'il détecte une anomalie, il réinitialise le PC à son état d'origine et éjecte tout intrus.**

Les appareils de la gamme Elite de HP ne protégeront pas votre entreprise à eux seuls. Mais ils constitueront une première ligne solide. Pour en savoir plus sur la gamme complète HP Elite, **cliquez ici**.

Pour accéder facilement à chaque appareil et service dont votre entreprise a besoin, consultez l'outil HP Device as a Service (DaaS). Vous pouvez choisir un appareil et un accessoire qui sont aussi uniques que vos besoins, le tout géré à distance, optimisé et maintenu par HP. Pour en savoir plus sur HP Device as a Service, **cliquez ici**.

* Modèles sélectionnés

** Selon les PC concurrents au 1er décembre 2016 avec plus d'un million d'unités par an équipés de la détection au niveau du BIOS à réparation automatique, de la détection des attaques dans la mémoire vive et de la protection de la configuration du BIOS et des polices

GLOSSAIRE ET SOURCES D'INFORMATIONS COMPLÉMENTAIRES

Accès aux outils de gouvernance

Attaques par web :
En général, une attaque par Internet qui consiste à rediriger un navigateur vers un site malveillant.

Botnet :
Renvoie généralement à un programme automatisé conçu pour accéder et contrôler les ordinateurs connectés à Internet sans que les propriétaires n'en soient conscients. Les ordinateurs sont souvent infectés par des programmes malveillants. Les pirates utilisent les botnets pour déclencher des **attaques de déni de service** sur un site Web.

Cheval de Troie :
Comparables aux virus et aux vers en termes d'incidences, les chevaux de Troie doivent être installés par l'utilisateur et, par conséquent, ils sont souvent très bien dissimulés. Les effets peuvent aller de la modification des paramètres de l'ordinateur à la suppression de fichiers en passant par la création d'une « porte dérobée » permettant au pirate de l'exploiter ultérieurement.

Gestion basée sur des stratégies :
En général, les outils de gestion des politiques définissent une norme pour établir ce que certains utilisateurs peuvent et ne peuvent pas afficher, puis appliquent ces politiques à un réseau entier. La cohérence garantit la sécurité (au moins, en théorie).

Hameçonnage :
Généralement effectué via e-mail, où un pirate demande des informations d'identification à renseigner dans une boîte de dialogue ayant un aspect légitime.

Ingénierie sociale :
Cas dans lequel un pirate essaie de forcer un utilisateur autorisé à fournir des informations confidentielles dans le but d'obtenir l'accès à un système.

Logiciel malveillant (Malware) :
Vaste catégorie de logiciels capables d'endommager, voire de désactiver, d'autres systèmes. Les virus, vers et chevaux de Troie sont des exemples de programmes malveillants. De même, pour répondre aux besoins de l'étude Ponemon citée tout au long de cet eBook, les programmes malveillants se distinguent des virus, car ils « sont présents dans le terminal mais n'ont pas encore infiltré le réseau ».

Outils de prévention de la perte de données :
Vaste catégorie de logiciels dont l'objectif est de surveiller les données sensibles et de bloquer les tentatives d'accès ou de copie par des personnes non autorisées. Différentes approches permettent la protection au point d'accès (c'est-à-dire le terminal), lors de la traversée du réseau, ou dans un système de fichiers. Selon Gartner, ce marché a **augmenté de 25 %** en 2013.

Outils GRC (Governance, Risk and Compliance) :
Ils concernent des initiatives importantes et coordonnées au sein d'une entreprise, qui visent à gérer et contrôler les opérations conformément aux réglementations et qui, par conséquent, permettent de réduire les risques.

Périmètre réseau :
Catégorie générale décrivant la cyberdéfense au point où l'Internet public ou un autre réseau public rencontre un réseau privé, géré localement. **Elle comprend généralement plusieurs couches d'appareils** de types différents.

GLOSSAIRE ET SOURCES D'INFORMATIONS COMPLÉMENTAIRES

Systèmes de renseignement de sécurité :
Un grand nombre de renseignements de sécurité permettent d'obtenir et de synthétiser les informations liées aux menaces. Les systèmes varient de la méthode de connexion des responsables aux systèmes pour détecter les anomalies du réseau.

Technologies de chiffrement :
Outils qui **rendent les données en elles-mêmes illisibles** sans un décodeur spécifique. Sous l'impulsion des dernières menaces terroristes en France, certaines voix au sein du gouvernement français ont plaidé en **faveur** d'une initiative européenne visant à la limitation du chiffrement. Plus récemment, le gouvernement a été contraint de **revenir sur sa position concernant la technologie de chiffrement** suite à de sévères critiques.

Technologies de pare-feu :
Un autre terme générique qui décrit un type de dispositif utilisant des algorithmes et d'autres technologies pour bloquer le trafic et empêcher les utilisateurs non autorisés à pénétrer sur le réseau. **Les versions de nouvelle génération** de ces dispositifs peuvent être efficaces car elles intègrent des fonctions qui auparavant étaient gérées par des dispositifs distincts. La détection des intrusions, par exemple. Elles ont également tendance à être compatibles avec l'application, et reconnaissent par conséquent la différence entre un trafic web provenant d'une mise en œuvre du service Salesforce.com et d'une page Facebook.

Vers :
À la différence des virus qui se propagent lorsqu'un fichier hébergé est partagé, les vers peuvent se reproduire quel que soit le fichier hébergé, par exemple un document Word ou une feuille de calcul Excel, et n'ont donc pas besoin d'une autre interaction humaine pour faire des ravages. Les systèmes de messagerie instantanée sont bien connus pour leur propagation des vers, comme l'a appris Skype a ses dépens en 2012.