La cybersécurité et votre entreprise

Le guide incontournable pour protéger vos données

57% des PME françaises ont subi des attaques réseaux en 2015

Sommaire

Les grandes entreprises comme les PME paient plus cher que jamais pour se remettre des violations de leurs données.

Si l'on se fie aux gros titres des médias, on pourrait croire que les pirates ne ciblent que les grandes organisations.

Il y un an, TV5 Monde était touchée par une cyberattaque de grande ampleur. Selon France Info, le coût de cette attaque a été évalué entre 4,3 et 5 millions d'euros pour l'année 2015, et 11 millions d'euros pour les trois prochaines années. Sony Pictures a également fait parler d'elle lorsque des films inédits et des e-mails exposant certaines informations personnelles sur les plus grandes stars d'Hollywood ont été divulgués par des pirates.

Aux États-Unis, une violation des systèmes du gouvernement fédéral était en cours depuis plus d'un an au moment où elle a été découverte. Les pirates chinois avaient apparemment profité de ce laps de temps pour récolter des informations contenues dans les bases de données fédérales pour les utiliser ultérieurement.

La mauvaise publicité n'est pas la seule préoccupation pour ces organisations. Réalisée par le cabinet PwC, l'enquête Global economic crime survey 2016 révèle que les attaques dans le monde ne visent plus seulement les grandes entreprises, mais touchent aussi les PME. « On constate un quasi-doublement des fraudes identifiées au sein des entreprises de plus petite taille. » Selon le rapport 2016 de l'éditeur de logiciels Symantec, près de 10 millions d'attaques réseaux ont eu lieu en France en 2015. Les petites et moyennes entreprises (PME) subissent 57% de ces attaques, contre 29% pour les entreprises de plus de 1500 employés.

La bonne nouvelle, c'est qu'un grand nombre de ces dommages est évitable.

Dans les pages qui suivent, nous passerons en revue les idées reçues sur la cybersécurité et étudierons de manière plus détaillée l'impact de la cybercriminalité sur les PME et ce que vous pouvez faire pour mieux vous défendre contre ces attaques. Enfin, nous nous tournerons vers l'avenir et discuterons de ce qui nous attend, et comment nous y préparer.

Les mythes de la cybersécurité brisés

ASTUCE : Former votre personnel à la cybersécurité constitue un pas très important vers la prévention d'une infraction.

Six idées reçues qui peuvent exposer les PME à la cybercriminalité

Les grandes entreprises peuvent certes faire les gros titres en cas de violations de données, mais les petites et moyennes entreprises représentent souvent des cibles plus faciles. Voici six mythes sur la cybersécurité pouvant rendre les PME plus vulnérables face aux pirates.

MYTHE 1 Les grandes entreprises paient plus cher pour la violation de leurs données

Selon un rapport établi par la société française spécialisée dans la sécurité des systèmes d'information Kaspersky Lab, le budget moyen nécessaire pour se remettre d'une violation de sécurité atteint 504.000 euros pour les grandes entreprises et 34.750 euros pour les petites et moyennes entreprises. Les entreprises sont généralement amenées à dépenser encore entre 7.000 euros (PME) et 63.000 euros (grandes entreprises) en personnel, formations et mises à niveau des infrastructures. Ces données proviennent d'une enquête mondiale réalisée auprès de 5.500 entreprises en 2015, en collaboration avec B2B International.

MYTHE 2 Les cyberattaques se produisent rarement, donc une protection sérieuse n'est pas nécessaire

Une étude réalisée par la société d'analyse et de conseil Pierre Audoin Consultants (PAC) a établi que 67 % des entreprises ont rapporté une brèche de sécurité en 2015. De plus, selon l'étude The Global State of Information Security ® 2015 réalisée par PwC, les incidents concernant les PME, également en forte augmentation, seraient sous-estimés.

En effet, les PME prenant la peine de déclarer leurs sinistres en cas d'incident sont rares. Tout d'abord, parce qu'une partie des attaques n'est jamais détectée. Ensuite, parce que la déclaration de l'incident, hormis une perte de crédibilité, n'apporte rien à l'entreprise qui ne dispose généralement pas des ressources techniques suffisantes pour identifier et traiter le problème.

Figure 1. Quelles sont les sources des incidents de cybersécurité au sein des entreprises françaises ?

Activité criminelle	Erreur humaine	Systèmes de gestion (back-end)
		
48%	**24%**	**28%**
des entreprises Cyberattaques malveillantes	*des entreprises* Négligence d'un employé ou d'un contractant	*des entreprises* Défaillance du système informatique et du processus opérationnel

Source: Ponemon Institute, 2015 Cost of Data Breach Study: France

Le Groupe de Conseil informatique Daisy estime que la moitié des entreprises du Royaume-Uni pourrait être piratée en moins d'une heure.

MYTHE 3 Nous ne courrons aucun risque puisque nous n'acceptons pas les paiements en ligne

Les pirates ne sont pas nécessairement intéressés par les données bancaires ; ils peuvent être en quête de renseignements personnels utilisables dans la fraude d'identité, ou tout simplement vouloir pirater votre site et l'utiliser pour envoyer du spam.

Les données sont en général précieuses. Prendre en otage des données clés telles que les carnets de rendez-vous ou les coordonnées des clients permet aux pirates de contraindre leurs victimes à payer une rançon - et appliquer cette même escroquerie à des dizaines de sites Internet de PME leur permettrait de récolter une somme substantielle.

MYTHE 4 Nous avons embauché un spécialiste en informatique pour gérer la sécurité, donc nous n'avons pas besoin de savoir quoi que ce soit d'autre

Bien que l'embauche d'un expert soit une bonne idée, surtout pour une entreprise en pleine croissance, tous les employés de l'entreprise doivent également être formés aux bonnes pratiques en matière de cybersécurité. Pensez à ce collègue qui télécharge en toute bonne foi une pièce jointe malveillante ou se rend sur un site dangereux, infectant ainsi le réseau de l'entreprise avec des logiciels malveillants qui ralentissent les ordinateurs ou envoient des informations sensibles à un cybercriminel.

« Un des moyens les plus efficaces pour limiter le risque passe par la sensibilisation et la formation. Vous pouvez non seulement réduire le nombre de personnes victimes de phishing d'environ 5 %, mais aussi créer un réseau humain qui sera plus efficace pour détecter les attaques de phishing que pratiquement n'importe quelle technologie », explique Lance Spitzner, directeur de recherche du SANS Institute, au site Silicon.

Passez à l'action

Choisissez un logiciel de sécurité avec protection des données comme HP SureStart, qui restaure automatiquement le BIOS d'un ordinateur lorsqu'une attaque par un logiciel malveillant est détectée - stoppant celui-ci avant que les données ne soient compromises.

MYTHE 5 Nous avons doté nos systèmes d'un logiciel antivirus puissant, donc nous sommes bien protégés

Les logiciels antivirus scannent les systèmes à la recherche de logiciels malveillants téléchargés à partir de sites Internet ou de courriels. Mais les pirates informatiques ont d'autres moyens pour contourner cette protection. Parmi les cyberattaques que ne peut pas bloquer un logiciel antivirus, on compte les **attaques par déni de service distribué (DDoS)** où un site est inondé de trafic indésirable qui ralentit ou stoppe son fonctionnement ; les **attaques provenant du Web,** où les pirates tirent parti des vulnérabilités dans le codage du site Internet pour récupérer des données telles que les références bancaires ; les **codes malveillants**, injectés dans le codage d'un site à des fins telles que le vol de données ou l'espionnage à distance ; et des **pirates gagnant l'accès** aux données via des appareils volés.

ASTUCE : Une surveillance des données sortantes en cas de trafic plus élevé que d'habitude peut aider à identifier le vol de données souvent lié à des attaques APT.

MYTHE 6 Si un intrus pénètre dans nos systèmes, nous le remarquerons tout de suite

Il est difficile de détecter une cyberattaque, en particulier pour les PME qui n'ont pas un expert en informatique à portée de main. Il est possible qu'un logiciel malveillant qui s'introduit dans un système ne perturbe pas les opérations immédiatement. A la place, il espionnera le système, livrant au pirate des informations qui lui permettront de réaliser des attaques plus ciblées, souvent dans le but de gagner l'accès au réseau entier.

De telles attaques sur des systèmes spécifiques sont classées comme des menaces persistantes avancées (ou APT en anglais).

Selon un rapport de recherche FireEye, la France, l'Angleterre, la Suisse et l'Allemagne sont les quatre pays les plus attaqués en Europe et représentent à eux seuls 71 % des infections détectées sur le continent. La France est le pays européen où l'on compte le plus de secteurs touchés par les attaques avancées. Celles-ci se caractérisent par une surveillance continue et l'obtention de données à partir d'une infrastructure informatique sur la durée - passant généralement inaperçue.

Combien cela coûte-t-il de récupérer d'une attaque cybercriminelle ?

Les entreprises françaises dépensent environ 3,12 millions d'euros par an pour réparer les dommages causés par la cybercriminalité.

Voici les types de cyberattaques les plus coûteux :

Code & logiciel malveillants

Logiciel qui nuit à un système en créant des failles de sécurité, en endommageant les fichiers ou en volant les données (inclut scripts, virus et vers)

Déni de service distribué

Les « attaques DDOS » sont des saturations du trafic Web qui font s'effondrer le site d'une entreprise et ses serveurs

Attaques provenant du Web

Attaques ciblant les visiteurs de votre site, par injection d'un code qui redirige les navigateurs vers des sites regorgeant de logiciels malveillants

Appareils volés

Un appareil perdu par un employé contenant un accès aux identifiants de la société peuvent entraîner le vol de données et l'usurpation d'identité

Phishing et ingénierie sociale

E-mails ou pop-ups se présentant comme des demandes de connexions

Employés malveillants

Les employés qui révèlent des informations sensibles

Botnets

Réseaux d'ordinateurs infectés dont un pirate prend le contrôle pour exercer une activité malveillante comme l'envoi de spam

Source : Ponemon Institute, 2015 Cost of Data Breach Study : France [1]

Moyenne des pertes financières liées à des incidents de cybersécurité par entreprise en France, soit une augmentation de 28% par rapport à 2014 [3]

3,7M€

1 PME française sur 10 a déjà été victime d'une cyberattaque

L'impact de la cybercriminalité sur les PME

Le coût réel de la cybercriminalité va au-delà de la réparation des dégâts d'un piratage

« De nombreuses PME ont encore une approche blasée envers la cybersécurité et, à tort, ne se considèrent pas comme des cibles pour les cybercriminels », a déclaré George Scott, directeur de la cybersécurité pour KPMG en Écosse.

Cela signifie que les systèmes des PME sont des proies faciles pour les pirates. Nombre d'entre elles ont également des relations avec les grandes entreprises qui détiennent des informations précieuses.

En ciblant ces PME, les attaquants peuvent pirater des fichiers qui leur garantissent l'accès aux données les plus lucratives de leurs partenaires commerciaux - et nuire ainsi à la réputation des PME.

Les manquements à la sécurité peuvent affecter votre entreprise bien au-delà des coûts nécessaires pour réparer les dommages.

Voici comment.

- **En vous empêchant de faire de nouvelles affaires**

Dans un récent sondage auprès de directeurs d'achats, la société d'audit KPMG a constaté que la grande majorité d'entre eux y réfléchirait à deux fois avant d'initier de nouvelles affaires avec les PME ayant des pratiques de sécurité laxistes. Une constatation surprenante si l'on considère que, d'après une étude menée par Ipsos-Navista en 2015, les PME/PMI allouent seulement 50€ de leur budget à la sécurité informatique. Un investissement trop faible sachant que 11% des entreprises interrogées déclarent avoir été victimes d'actes de malveillance. En moyenne, une violation de données peut atteindre jusqu'à 11 millions d'euros de perte pour une organisation.

- **En empêchant les employés de travailler**

Pour revenir à l'exemple de TV5 Monde, en juillet 2015, soit trois mois et demi après la cyberattaque, les 400 salariés de TV5 Monde étaient toujours dans l'impossibilité de travailler normalement, selon le directeur général de la chaîne, Yves Bigot.

Pour une PME, un tel délai aurait pu être fatal.

Passez à l'action

Travaillant avec la CGPME (Confédération générale des petites et moyennes entreprises), l'Agence nationale de sécurité des systèmes d'information (ANSSI) apporte son expertise de terrain dans un guide des bonnes pratiques de l'informatique. Ce document compile 12 règles essentielles pour donner aux PME les moyens opérationnels de préserver leurs systèmes d'information des pirates.

ASTUCE : De nombreuses formes de logiciels malveillants sont transmises en pièces jointes. Formez votre personnel pour qu'il reconnaisse les fichiers suspects conçus pour ressembler à des documents légitimes.

• En érodant la confiance des clients

Les PME qui perdent les données de leurs clients souffrent souvent d'une atteinte à leur réputation qu'il est difficile de regagner - surtout si le vol concernait des données financières. Le logiciel bancaire malveillant Dridex continue de se répandre à travers l'Internet, infectant les appareils connectés et transmettant des informations sensibles, y compris les coordonnées bancaires, aux attaquants. Annoncé comme démantelé en octobre 2015, « il a généré des vocations (Shifu par exemple) et causé des pertes financières gigantesques dans de nombreuses entreprises », explique le site News Informatique. Selon Trend Micro, la France aurait été le 4ème pays le plus touché par le malware et certaines arnaques ont pu se chiffrer à plusieurs millions d'euros.

Anatomie du piratage inattendu

Comment une violation de sécurité peut en entraîner d'autres. Disons que vous êtes propriétaire d'un restaurant de fruits de mer qui prospère depuis des générations. Pour évoluer avec votre temps, vous passez à un système de réservation électronique qui permet aux clients de se créer un compte en utilisant leur adresse e-mail, puis de faire des réservations qui apparaissent ensuite sur votre calendrier numérique. Les affaires fleurissent et vous vous retrouvez à embaucher des serveurs pour la première fois en cinq ans.

A votre insu, ce maître d'hôtel que vous avez récemment embauché commence à s'approprier les adresses e-mail de vos clients pour les donner à son partenaire. Mais ce partenaire est un pirate informatique qui commence à craquer les mots de passe de messagerie de vos clients. Il y parvient en un rien de temps. Parmi les comptes craqués, 10 % ont des liens vers des portefeuilles électroniques contenant des données bancaires et de cartes de crédit.

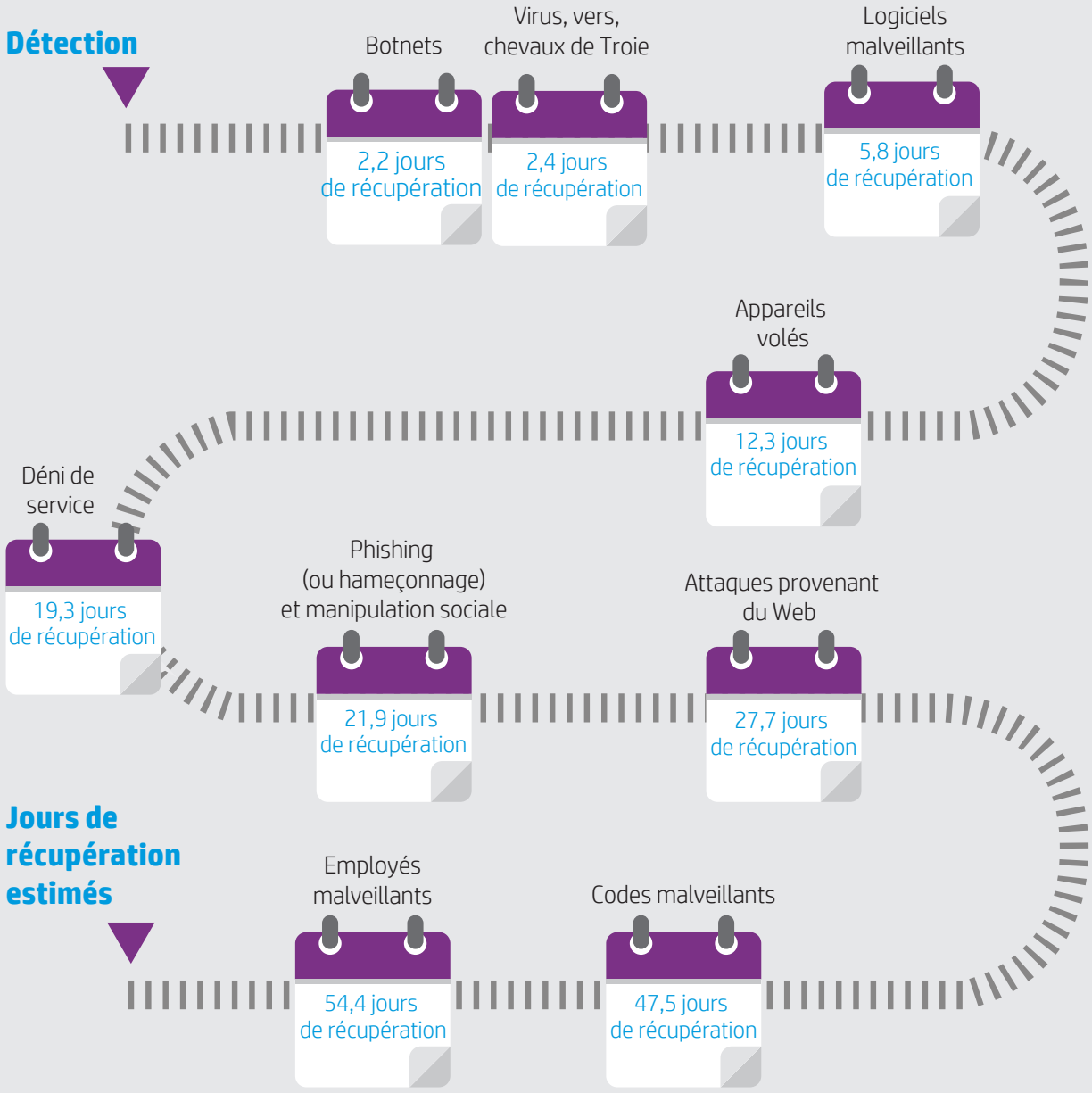
En utilisant les comptes de messagerie et les portefeuilles électroniques associés, les deux hommes se lancent dans 24 heures de dépenses frénétiques. Ils quittent la ville peu après, laissant derrière eux une douzaine de clients confus et en colère qui vont passer des mois à se remettre de l'usurpation de leur identité.

Ce qui rend les violations dangereuses, c'est que chacune d'elles peut en entraîner une autre. Ici, le maître d'hôtel qui s'est révélé être un « employé malveillant » pourrait laisser derrière lui une « porte dérobée » lui permettant d'espionner votre activité future. Ce point faible pourrait être découvert et utilisé par un autre pirate pour voler les données personnelles et financières de vos clients, même si vous mettez à jour vos systèmes.

Les cyberattaques étant de plus en plus sophistiquées, un plan de sécurité multicouche, pouvant aller des logiciels antivirus à la surveillance continue du système, est crucial pour protéger votre entreprise.

Cybercriminalité : durée de récupération

Combien de temps faut-il pour réparer les dégâts d'une violation de données ? L'Institut Ponemon [2] établit la moyenne à 46 jours, un chiffre potentiellement handicapant pour les PME qui misent sur un fonctionnement sans interruption.



Passez à l'action

Créez un plan d'intervention en cas de violation pour chaque service, de l'informatique au service client, afin de minimiser le temps de récupération.

Source: Ponemon Institute, 2015 Cost of Cyber Crime Study [2]

Comment protéger votre entreprise de la cybercriminalité

Conseils et stratégies essentiels pour la cybersécurité des PME

Tandis que nous évoluons vers un monde de plus en plus digital où les données ont plus que jamais de la valeur, la cybercriminalité peut prendre de nombreuses formes.

Les cybercriminels sont souvent en quête d'informations, et avec un nombre toujours plus élevé de dispositifs connectés dans notre lieu de travail - des smartphones et tablettes aux imprimantes Wi-Fi - les pirates disposent d'un nombre croissant de points d'accès.

Voici six cibles couramment visées par des pirates attaquant les systèmes d'une entreprise - et ce que vous pouvez faire pour les protéger aujourd'hui.

ASTUCE : Une détection rapide peut limiter les dégâts d'une attaque informatique. Choisissez donc un logiciel de sécurité qui surveille en permanence votre réseau afin de repérer tout comportement inhabituel.

1 Bases de données clients

Les données financières sont loin d'être les seules cibles des cybercriminels - des informations telles que les noms et les adresses électroniques peuvent être utilisées pour l'usurpation d'identité, le spamming, ou le piratage d'autres comptes.

Le gros lot pour les pirates est de pénétrer les systèmes des PME qui travaillent pour de grandes entreprises. Imaginez cela comme l'équivalent numérique d'un casse dans un magasin pour atteindre le mur du sous-sol, mitoyen avec la chambre forte d'une banque voisine. Une fois que les attaquants sont à l'intérieur du plus petit système, ils sont au meilleur endroit pour accéder aux données des clients des grandes entreprises elles-mêmes clientes des PME.

Comment votre base de données clients pourrait-elle être mise en danger ? Les virus, vers et chevaux de Troie - téléchargés à partir de sites ou d'e-mails malveillants - peuvent libérer un code nécessaire au pirate pour entrer dans un système et voler des données.

Comment protéger les données de vos clients

- Utilisez un logiciel de sécurité conçu pour les entreprises, qui offre une protection des réseaux, e-mails et postes de travail.
- Mettez toujours à jour votre logiciel de sécurité pour bloquer les évolutions de logiciels malveillants.
- Téléchargez les mises à jour des logiciels pour vos programmes système car les programmes plus anciens peuvent contenir des vulnérabilités exploitables par les attaquants.

55% des entreprises françaises utilisent le Cloud

2 Services en mode Cloud

Beaucoup de PME optent pour des services Cloud rentables tels que Microsoft Office 365 pour les tâches de bureau. Selon l'édition 2014 du Cloud Index PAC, ce sont ainsi 55% des entreprises françaises qui utilisent aujourd'hui l'informatique « dans le nuage ». Le besoin de flexibilité et la volonté de réduire les coûts sont les principales raisons du passage au Cloud (66%).

Les grandes entreprises européennes ont pourtant encore du mal à faire confiance au Cloud puisque, selon un rapport d'Eurostat datant de 2014, 57% d'entre elles ont déclaré le risque de piratage comme étant la principale raison réfrénant leurs ardeurs vis-à-vis du Cloud. Les PME, quant à elles, sont seulement 38%.

Les violations peuvent se produire en raison de protocoles de sécurité insuffisants - tels que des mots de passe et des permissions d'accès - sur les données hébergées dans le Cloud. Imaginez, en tant que propriétaire de notre restaurant de fruits de mer piraté, si vous aviez empêché le maître d'hôtel d'accéder à la base de données - ou, mieux encore, chiffré les informations afin que le pirate ne puisse pas les utiliser.

Comment protéger les informations du Cloud

- Cryptez vos informations les plus importantes en utilisant des outils tels que la technologie Smartcrypt de PKWARE qui utilise des stratégies d'accès pour déterminer la complexité du cryptage.

- De cette façon, les utilisateurs autorisés voient les données qu'ils sont censés voir - et les utilisateurs non autorisés ne voient rien.
- Créez un mot de passe pour votre compte Cloud. En outre, dans les paramètres de ce dernier, définissez précisément qui peut accéder à vos données et ce qu'ils peuvent en faire.
- Exigez une double authentification - comme un code pour votre smartphone en plus d'un mot de passe - pour modifier certaines données du Cloud, telles que le téléchargement, la suppression ou le déplacement de fichiers.

3 Smartphones et tablettes du personnel

Un grand nombre d'employés utilise leurs appareils personnels au bureau. Les politiques « Apportez votre propre matériel » sont pour les PME un moyen efficace de tirer parti des smartphones que les employés possèdent déjà - mais ces téléphones représentent une cible juteuse pour les pirates.

Environ 1 application Android sur 5 transporte un certain type de logiciel malveillant invasif, qui pourrait être transmis aux fichiers et aux systèmes de la société afin de surveiller son activité ou voler ses informations.

Les employés dont les téléphones sont volés peuvent aussi involontairement devenir une porte d'entrée pour les pirates. Un voleur de téléphone peut vendre un appareil à un acheteur sur le marché noir, qui a alors la possibilité de démonter le téléphone pour obtenir des informations et violer la sécurité de la société de la victime, ou pénétrer dans les systèmes d'un client plus important.

Comment sécuriser les appareils du personnel

- Installez un outil de détection de menace, comme X-Ray de Duo pour les appareils Android afin de faciliter la détection des applications malveillantes et des codes suspects.
- Demandez aux employés d'autoriser l'effacement à distance (disponible gratuitement pour Android, iPhone et Windows Phone, avec abonnement pour BlackBerry) de sorte qu'en cas de perte de l'appareil, les données sensibles à la fois professionnelles et personnelles puissent être effacées.
- Demandez aux employés d'activer le chiffrement de l'appareil sur leurs smartphones pour protéger les données (installé par défaut sur les nouveaux téléphones iOS et Android).

Qu'est-ce qu'un ransomware (ou rançongiciel) ?

Les cybercriminels sont de plus en plus orientés vers les ransomwares, une forme de logiciels malveillants qui prend les systèmes en otage. Ceux-ci sont débloqués une fois le paiement d'une rançon en Bitcoin effectué. Au mois de décembre passé, le ministère des Transports a été victime d'une série d'attaques au ransomware. Une étude récente de l'éditeur de sécurité Bitdefender affirme que les Français payeraient un montant de 190 euros pour débloquer leur ordinateur infecté par un ransomware. Voici un aperçu plus détaillé de la manière dont ces types d'attaques fonctionnent.

1. Installation	Le code malveillant s'immisce dans votre ordinateur après un téléchargement involontaire, par le biais d'un e-mail ou d'un site Web.
2. Il alerte son quartier général	Le ransomware se connecte à son serveur d'origine pour établir une clé de chiffrement.
3. Il crypte vos fichiers	Le ransomware scanne les fichiers sur votre réseau et les cryptent, les rendant ainsi inaccessibles.
4. Extorsion	Un message apparaît en général sur l'ordinateur de l'utilisateur affichant une limite de temps et le montant à payer pour que les fichiers soient décryptés avant d'être supprimés.
5. Paiement de la rançon	Le propriétaire d'une entreprise peut acheter une monnaie numérique comme le Bitcoin qu'il transférera au cybercriminel qui, espérons-le, décryptera les fichiers.

4 Erreurs du personnel

Le principe fondamental de la cybersécurité est une bonne politique de mot de passe au sein de l'entreprise. Selon une étude [3] réalisée par le cabinet PwC, la majorité (34,2%) des incidents de sécurité a pour origine un salarié de l'entreprise.

Du piratage des mots de passe peu sécurisés au vol de documents envoyés par courriel via une connexion non sécurisée, en passant par un courriel de phishing ciblant un employé en particulier, les cybercriminels exploitent souvent les failles humaines.

Comment aider votre personnel

- Formez votre personnel aux meilleures pratiques de la cybersécurité et offrez des formations régulières pour les tenir au courant des dernières menaces.
- Mettez en place un protocole de sécurité adapté à votre entreprise et aux types de données qu'elle traite.
- Créez une équipe qui communiquera votre politique de cybersécurité aux employés ainsi qu'à vos clients et partenaires commerciaux.

5 Imprimantes et autre matériel informatique en réseau

Votre imprimante pourrait être l'un des maillons les plus faibles de votre réseau de sécurité. Un pirate informatique entreprenant pourrait accéder à des contrats, des rapports financiers et d'autres données confidentielles puisque ces fichiers transitent des disques durs aux copies papier.

Tandis que les ordinateurs de bureau sont au moins protégés par des mots de passe et idéalement par un logiciel de sécurité, les files d'attente et les travaux d'impression ne sont souvent pas protégés par de tels protocoles de sécurité.

Ces imprimantes non-sécurisées - et tout autre matériel informatique en réseau - peuvent devenir la proie de « programmes renifleurs » capables de se connecter aux travaux d'impression, ainsi qu'au trafic du réseau, aux noms d'utilisateur et mots de passe, tous renvoyés directement à un serveur cybercriminel.

D'autres appareils suspects pouvant introduire des logiciels malveillants dans vos systèmes sont par exemple les lecteurs externes, utilisés sur plusieurs ordinateurs, et en particulier les clés USB, au format pratique pour partager des fichiers d'un ordinateur à un autre, éventuellement infecté.

Comment protéger les périphériques

- Téléchargez les mises à jour des logiciels pour l'ensemble du matériel informatique lorsqu'elles sont disponibles.
- Scannez les clefs USB et les disques durs à la recherche de logiciels malveillants lorsque vous les insérez.
- Investissez dans du matériel sécurisé par une protection intégrée, comme une imprimante capable de surveiller, détecter et agir contre un piratage en redémarrant et en effaçant la file d'attente d'impression de documents sensibles.
- Découvrez comment HP peut renforcer la sécurité de votre entreprise sur notre site dédié.

ASTUCE : Supprimez ou désactivez les fonctionnalités inutiles sur le matériel informatique, car un trop grand nombre de fonctions peut augmenter les passerelles permettant aux cybercriminels d'y avoir accès.

Passez à l'action

L'ANSSI précise que « la France dispose d'un réseau de CERT (Computer Emergency Response Team), organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ces CERT sont des centres d'alerte et de réaction aux attaques informatiques, destinés aux entreprises et/ou aux administrations, mais dont les informations sont généralement accessibles à tous.

Les mots de passe les plus communs

Début 2013, un journaliste d'Ars Technica, sans aucun passé cybercriminel ni expérience dans le craquage des systèmes protégés par mot de passe, parvint à craquer en un seul jour 8.000 mots de passe cryptés sur plus de 16.000. Alors quelle chance ont ces mots de passe extrêmement communs de résister à un pirate déterminé ?

Passez à l'action

Créez un mot de passe sécurisé

1. **Utilisez au moins 12 caractères**
2. **Évitez les expressions communes**
3. **Évitez votre date d'anniversaire et votre prénom**
4. **Ajoutez des numéros et des symboles**
5. **Ajoutez des lettres majuscules**

Bonus sécurité : Pensez à une phrase longue (facilement mémorisable) et créez un acronyme avec ses premières lettres - puis ajoutez des chiffres, des symboles et des majuscules.

Source: Splashdata

ASTUCE : Investissez dans du matériel qui offre une protection intégrée telle qu'une authentification avancée et des outils de chiffrement.

6 Passerelles de réseau

Lorsque les pirates veulent accéder à un réseau, ils peuvent déclencher une attaque par déni de service distribué (Distributed Denial of Service ou DDoS). Des milliers de machines infectées par des logiciels malveillants sont assemblées pour générer tant de trafic indésirable que le réseau s'effondre sous le poids de l'attaque. Souvent, les attaquants par DDoS cherchent à distraire les administrateurs du site en figeant le système pendant qu'ils volent des données ou installent des logiciels malveillants pour planifier de futurs vols. Certaines attaques DDoS sont aussi causées par des « script kiddies », des pirates débutants qui veulent simplement détruire un site Web parce qu'ils en ont les moyens. Malheureusement, à peine quelques heures d'arrêt du site d'une PME peuvent avoir un effet dévastateur sur ses résultats et sa réputation.

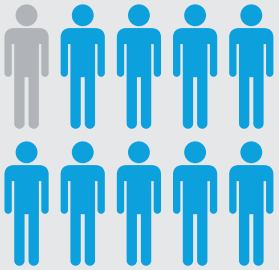
Comment sécuriser votre réseau

- Construisez des systèmes qui contrôlent le trafic entrant et sortant de votre réseau. Une hausse soudaine du trafic pourrait indiquer une attaque, tandis qu'une activité constante, mais inexplicable, pourrait indiquer qu'un cheval de Troie envoie les données à son site d'origine.
- Filtrez tout le trafic pour que seul le trafic nécessaire à votre entreprise arrive sur votre réseau.
- Assurez-vous que chaque routeur, commutateur ou autre périphérique réseau fonctionne avec le même logiciel et les mêmes fonctionnalités de base, et téléchargez toujours les mises à jour des logiciels.

Votre entreprise est-elle cybersécurisée ?

1 sur 2

Plus d'une PME sur deux ne prend aucune disposition pour se protéger des actes de malveillance



9 sur 10

9 PME sur 10 autorisent l'accès Internet aux sites Web potentiellement dangereux

7 sur 10

7 PME sur 10 échangent des documents avec leurs clients sans garantie de confidentialité

Source : Ipsos Navista, septembre 2014, Baromètre sur la sécurité informatique des PME

Votre checklist de la cybersécurité

- ☑ Installez un logiciel de sécurité avec une protection antivirus et une surveillance continue contre les intrusions
- ☑ Téléchargez toujours les mises à jour des programmes
- ☑ Cryptez vos fichiers les plus importants
- ☑ Scannez vos clefs USB et disques durs pour détecter les logiciels malveillants
- ☑ Formez votre personnel aux meilleures pratiques en matière de cybersécurité, de l'utilisation de mots de passe fiables à la reconnaissance de fichiers suspects
- ☑ Rédigez des directives pour la sécurisation des appareils du personnel et le travail à distance
- ☑ Créez un plan pour faire face aux cyberattaques
- ☑ Créez une équipe chargée de communiquer votre politique de cybersécurité aux employés
- ☑ Utilisez des imprimantes et des périphériques sécurisés par des fonctions anti-fraude et de cryptage
- ☑ Installez un logiciel pour surveiller tout trafic inhabituel sur votre réseau

Source : HP, Inc.

L’avenir de la cybersécurité des PME

Comme la présence des PME sur la toile croît à un rythme record, il devient crucial d’établir des mécanismes de cybersécurité solides

Aujourd’hui, les employés utilisent leurs propres appareils pour travailler. Les propriétaires d’entreprises utilisent des plates-formes de Cloud computing et sous-traitent les services techniques clés. Selon le site Net-iris, en 2015, plus de 4 millions d’actifs français travaillent au moins un jour par semaine hors des locaux de leur entreprise et 8,8 millions sont en télétravail au moins une fois par mois. La cybersécurité devient plus difficile à assurer lorsque vous ne contrôlez ni l’appareil, ni l’infrastructure, ni l’espace de travail.

Les smartphones nous ont appris que les affaires peuvent se faire partout et à tout moment. Un café est un endroit tout aussi propice au travail qu’un bureau. Nous utilisons les réseaux Wi-Fi publics pour traiter de grandes quantités de données commerciales et personnelles - souvent sur des smartphones qui sont faiblement sécurisés. Les criminels prennent certainement conscience de ce changement. La sécurité diminue lorsque nous ne tenons pas compte de nos conditions de travail.

Dans les années à venir, cela signifiera bien plus que l’installation d’un logiciel antivirus sur nos appareils ou la mise à jour de nos mots de passe tous les six mois. Les PME doivent plutôt adopter des mesures de sécurité renforcées qui fonctionnent tout aussi bien à distance que dans un bureau supervisé par un administrateur informatique.

Pour les organisations décentralisées de demain, la cybersécurité repose sur des analyses sophistiquées capables d’isoler un comportement inhabituel, et une sécurité par couches qui protège tous les points d’accès.

ASTUCE : Monitorez et documentez d’abord le comportement normal afin de détecter les anomalies dans un second temps.

Analytique : le détective de la cybersécurité
Même si votre site ne supporte pas de trafic lourd, il fonctionnera selon des schémas récurrents. En utilisant des outils d’analyse qui mesurent et enregistrent l’activité, il devient plus facile de diagnostiquer quand quelque chose ne va pas. Ces outils fonctionnent en suivant et en documentant le comportement normal dans un premier temps afin de détecter les anomalies plus tard. Une fois détectées, les administrateurs peuvent alors passer à l’offensive et supprimer les attaques avant qu’elles n’aient la chance de déclencher un cyberchaos.

Superposez les couches : gardez une longueur d’avance sur vos attaquants
Parfois qualifiée de « défense en profondeur », une sécurité par couches protège chaque point d’accès de multiples façons. Les approches les plus communes incluent des certificats SSL Extended Validation qui rendent difficiles à falsifier les informations d’identification nécessaires pour entrer dans un réseau sécurisé. Renforcez cela avec une authentification multifactorielle, qui oblige les envahisseurs à craquer plus qu’un simple mot de passe, peut également être utile. Quelle que soit la technologie spécifique appliquée, le principe sous-tendant la sécurité par couches est que tous les domaines sensibles du réseau de votre PME soient verrouillés d’une certaine façon. Vos utilisateurs et partenaires auront peut-être besoin de temps et de quelques efforts supplémentaires pour accéder aux données cruciales, mais ces inconvénients devraient plus que payer en tranquillité d’esprit pour votre entreprise.

Agissez dès maintenant
Investir dans un logiciel de cybersécurité et dans une formation est la meilleure des défenses. Commencez par faire un audit de vos systèmes et de votre infrastructure. En faites-vous assez ? Que pourriez-vous améliorer ?

Et enfin, vous pouvez également appeler nos experts ici chez HP. Notre base de connaissances collective vise à prévenir les menaces et pas seulement à y répondre. Pour en savoir plus, veuillez nous rendre visite sur notre site internet .

Notes

[1] Ponemon Institute, 2015 Cost of Data Breach Study: France

[2] Ponemon Institute, 2015 Cost of Cyber Crime study

[3] PwC, The Global State of Information Security® Survey 2016

Glossaire et lectures complémentaires

Accédez aux outils de gouvernance.

Botnet : Fait généralement référence à un type de programme automatisé conçu pour contrôler et accéder aux ordinateurs connectés à Internet à l'insu de leur propriétaire. Les ordinateurs sont souvent infectés par des malwares. Les pirates utilisent des botnets pour déclencher **une attaque par déni de service** sur un site Internet.

Outils de prévention de perte de données : Une vaste catégorie de logiciels dont l'objectif est de surveiller les données sensibles et de bloquer les tentatives d'accès ou de reproduction par du personnel non autorisé. Différentes approches permettent une protection au niveau du point d'accès (par ex. le poste de travail), tout en traversant un réseau, ou dans un système de fichiers. Gartner, une entreprise américaine de conseil et de recherche dans le domaine des techniques avancées, a fait croître ce marché **de 25 %** en 2013.

Technologies de chiffrement: Des outils qui rendent les données illisibles sans une sorte de décodeur. Lors de sa présentation de la stratégie du gouvernement en matière de cybersécurité le 16 octobre dernier, le premier ministre Manuel Valls a réaffirmé que « [son] gouvernement restait favorable à ce que les entreprises disposent de tous les moyens de cryptologie légale ». Devant la presse, Guillaume Poupard, le patron de l'Agence nationale de sécurité des systèmes d'information, a rappelé sa position :

« Le chiffrement est un outil indispensable à la sécurité. La question de l'autorisation du chiffrement s'est posée il y a 20 ans et on est arrivé à la conclusion que de telles démarches allaient freiner le développement du numérique et déranger les 99,9 % de gens honnêtes. »

Technologies de pare-feu : Un autre terme général qui décrit un style de dispositif recourant à des algorithmes et autres techniques pour bloquer le trafic non autorisé et empêcher des utilisateurs d'accéder à un réseau. En combinant des fonctions jusqu'ici traitées par des appareils distincts, comme la détection d'intrusion par exemple, la prochaine génération de ces dispositifs peut se révéler particulièrement puissante. Elle ne crée pas de conflit avec vos applications et fait ainsi la différence entre les différents types de trafic Web.

Outils en matière de gouvernance, de risque et de conformité (GRC) : Conçus pour faire référence à des initiatives larges et coordonnées dans une entreprise visant à gérer et régir des opérations d'une manière conforme à la réglementation, et qui, par conséquent, réduit les risques.

Logiciel malveillant : Une large catégorie de logiciels pouvant causer des dommages ou même désactiver d'autres systèmes. Les virus, les vers et les chevaux de Troie sont tous des exemples de logiciels malveillants. En outre, selon l'étude Ponemon [2] citée tout au long de ce livre électronique, les logiciels malveillants sont considérés comme distincts des virus, car « ils résident au point d'accès et n'ont pas encore infiltré un réseau ».

Contrôles de périmètre: Une catégorie générale décrivant la défense cybernétique à l'endroit où l'Internet public ou tout autre réseau public rencontre un réseau privé, détenu et géré localement. Des couches et des types multiples de dispositifs sont généralement impliqués.

Phishing (ou hameçonnage) : Habituellement réalisé via courrier électronique, dans lequel un attaquant demande des informations d'identification dans une boîte de dialogue d'aspect légitime.

Outils de gestion des règles de sécurité : D'une manière générale, les outils de gestion des règles de sécurité établissent une norme concernant ce que certains utilisateurs peuvent et ne peuvent pas voir, puis appliquent ces règles à travers un réseau entier. La cohérence (en théorie, du moins) garantit la sécurité.

Systèmes de renseignement de sécurité : Une multitude de renseignements de sécurité peut aider à rassembler et synthétiser les informations relatives aux menaces. Les systèmes varient des historiques d'activité aux systèmes de détection des anomalies du réseau.

Manipulation sociale : Méthode par laquelle un attaquant œuvre pour contraindre un utilisateur à livrer des informations alors qu'il ne devrait pas, octroyant ainsi l'accès à l'attaquant.

Cheval de Troie : D'impact similaire à un virus ou un ver, les chevaux de Troie doivent être installés par l'utilisateur, et pour cette raison, ont tendance à être astucieusement 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 « backdoor » ou porte dérobée que le pirate pourra exploiter plus tard.

Virus : Un code malveillant capable de se répliquer et de se diffuser à travers un réseau. Cette liste du Smithsonian de 2012 répertorie les virus les plus destructeurs de l'histoire. Le Monde Informatique reprend des informations plus spécifiques à la France.

Attaques provenant de pages Internet : Le plus souvent, une attaque provenant d'Internet consiste à rediriger un navigateur vers un site malveillant.

Vers : Contrairement aux virus qui se propagent lorsqu'un fichier hôte est partagé, les vers peuvent se répliquer indépendamment d'un fichier hôte tel qu'un document Word ou Excel, et ne nécessitent donc pas l'intervention humaine pour faire des ravages. Les systèmes de messagerie instantanée sont bien connus pour avoir propagé des vers. Skype a subi cette avanie en 2012.

Inscription pour les mises à jour
hp.com/go/getupdated

HP France SAS, société par actions simplifiée au capital de 72 010 928 €, RCS Evry 448 694 133, 1 Avenue du Canada 91947 Les Ulis Cedex.