Facile et pas chère

Sécurité informatique, le b.a.ba

Se poser les bonnes questions pour mettre en place les bonnes pratiques, simples et peu coûteuses

21 % des PME ont été victimes d'une cyberattaque entre novembre 2017 et novembre 2018, selon l'étude Ifop réalisée auprès de 702 répondants pour Kaspersky Lab. 14 % des répondants admettent que les attaques leur ont coûté plus de 51 000 euros. Se protéger du piratage est donc devenu un enjeu primordial. La gestion de ce risque passe tout autant par la sensibilisation des salariés à des mesures simples qu'à la mise en place de systèmes de protection.

par Anne Thiriet

Les spécialistes en conviennent : le mail reste l'un des principaux points d'entrée des cyberattaques. Une première mesure de sécurité consiste déjà à utiliser des mots de passe difficilement décryptables : ils doivent contenir au moins 12 caractères sous différentes formes

En poursuivant votre navigation sur notre site, vous acceptez l'utilisation de cookies pour vous proposer une navigation optimale et nous permettre de réaliser des statistiques de visites.
En savoir plus sur les cookies
Fermer X

en permanence pour des accès divers et variés (comptes mails, de sites marchands, de compte bancaire, etc.). Ces outils, sous forme de logiciels ou d'extension dans le navigateur, conservent en un seul endroit l'ensemble des mots de passe dont un internaute peut avoir besoin pour différents comptes. Il suffit de mémoriser celui qui donne accès au lieu de stockage.

Le mail, courrier piégé

Le danger vient également de ce qui est reçu. Attention aux pièces jointes envoyées dans des mails ! Un premier niveau de protection peut être donné par les pare-feu et les routeurs installés par le service informatique. Le virus peut en effet être dissimulé dans une pièce jointe adressée par mail. "Les ransomwares, ces logiciels qui cryptent et bloquent les données en échange de rançons, proviennent les trois quarts du temps de pièces jointes. Le mail peut contenir un lien dirigeant vers une page à l'aspect sécurisé ou provenir d'un client dont le compte a été piraté, explique Jayson Bruhammer, responsable du pôle cybersécurité d'Actecil. En cas de doute, il faut télécharger la pièce jointe dans un dossier temporaire, la scanner et demander son avis au service informatique. Il vaut mieux lui faire perdre une heure que prendre le risque de rester bloqué pendant trois jours."

> "Les ransomwares, ces logiciels qui cryptent et bloquent les données en échange de rançons, proviennent les trois quarts du temps de pièces jointes"

Les faux mails, de plus en plus sophistiqués, reposent sur un mélange de stratégie cyber et de facteurs humains. "Ces méthodes d'ingénierie sociale visent à tromper des personnes peu méfiantes. La fraude au pdg est la plus classique. En l'absence de ce dernier, en déplacement, le hacker usurpe l'identité du responsable et envoie un mail demandant le virement urgent d'argent sur un compte bancaire. Il peut aussi prendre l'identité d'un client auprès du support client pour récupérer ses mots de passe", indique Pierre Lorcy.

Autre technique qui se développe : le spear-phishing qui consiste à cibler un nombre restreint de personnes. "Les hackers cherchent des informations personnelles sur leur victime, au travers d'Internet et des réseaux sociaux. Grâce à ces informations, les destinataires ont du mal à distinguer un vrai mail d'un faux, observe Thierry Gourdin, chef des préventes B2B chez Kaspersky Lab. La réponse consiste à protéger les serveurs de sa messagerie avec des antivirus et des antispams."

Les transferts de fichiers doivent également tenir compte de quelques impératifs. "Il faut essayer de bannir les solutions d'échange d'informations personnelles comme Google Drive ou Microsoft Drive car il n'existe aucun moyen de contrôle sur les fichiers déposés par les utilisateurs, souligne Thierry Gourdin. Dans le cadre d'informations confidentielles, il est nécessaire d'utiliser le chiffrement. On peut créer un container chiffré, comme un zip, et transmettre le mot de passe au destinataire par SMS." Il faut aussi penser à mettre à jour régulièrement les logiciels utilisés : l'intérêt réside dans la correction de failles de sécurité, parfois connues et exploitées par des cybercriminels.

Des réflexes simples

En poursuivant votre navigation sur notre site, vous acceptez l'utilisation de cookies pour vous proposer une navigation optimale et nous permettre de réaliser des statistiques de visites.
Fermer X
En savoir plus sur les cookies

nationale de la sécurité des systèmes d'information), qui ont réalisé un guide. Téléchargeable gratuitement en version PDF, il recense 12 règles essentielles pour sécuriser ses équipements numériques.

"Le premier rempart aux menaces reste l'utilisateur. Nous proposons des tutoriels en ligne aux personnes non familiarisées sur la plate-forme de formation Kaspersky Automated Security Awareness Platform, avec la possibilité d'organiser de fausses campagnes de phishing pour évaluer le niveau de maîtrise des salariés et proposer éventuellement des modules complémentaires", précise Thierry Gourdin.

> "La CPME et l'Anssi ont réalisé un guide. Téléchargeable gratuitement en version PDF, il recense 12 règles essentielles pour sécuriser ses équipements numériques"

Autre outil de sensibilisation, la politique de sécurité du système d'information (PSSI). "Ce document permet d'indiquer un certain nombre de règles aux salariés : quels outils utiliser pour le transfert de documents, quels logiciels sont autorisés, qui est en charge des outils, à qui donner l'accès à telle ou telle information, documenter les prestataires qui entrent dans l'entreprise..., détaille Jayson Bruhammer. L'objectif est de documenter l'existant pour que les salariés soient informés. Cette PSSI peut être régulièrement mise à jour sous la forme d'une foire aux questions. Pour inciter les entreprises à la mettre en place, je leur propose d'établir un fichier Excel avec les questions récurrentes des employés et tous les cas connus de tentatives de piratage. Je conseille de réaliser en priorité un fichier sur le traitement des données personnelles au sein de l'entreprise car ce sont les données les plus contrôlées."

Guillaume de Lavallade, directeur général de Hub One, qui insiste sur la prise de conscience des dirigeants de l'entreprise de l'importance de la sécurité numérique, souligne l'intérêt du RGPD (Règlement général sur la protection des données), en application depuis mai 2018. "L'aspect protection des données personnelles du RGPD est connu des entreprises mais le règlement est plus complet : il impose la sécurité par architecture (security by design), c'est-à-dire l'obligation de compartimenter tout leur système d'information. Chaque fois qu'une base de données peut contenir des données personnelles, business ou autres, il faut, par la construction, faire en sorte qu'elle soit isolée et que ses connexions soient bien identifiées. C'est important car le revers de la digitalisation, qui traverse toutes les entreprises, est la tendance à tout interconnecter. Or on peut ainsi augmenter sa surface d'exposition au risque."

Vigilance avec le cloud

Externaliser des données, via le cloud par exemple, peut aussi être un facteur de risques. "Il apporte bien des avantages, comme une solution de messagerie externalisée qui propose une gestion tarifaire efficace, sans avoir besoin d'acheter de licence, et une mise à jour de logiciel qui évite les problèmes de virus, souligne Pierre Lorcy. C'est un nouvel outil qu'il faut apprendre à utiliser et à sécuriser."

> "Le premier risque du cloud est la mauvaise utilisation ou un mauvais paramétrage"

En poursuivant votre navigation sur notre site, vous acceptez l'utilisation de cookies pour vous proposer une navigation optimale et nous permettre de réaliser des statistiques de visites.
Fermer X
En savoir plus sur les cookies

utilisation ou un mauvais paramétrage. “Il faut mettre en place une bonne politique de gestion des mots de passe. Si vous disposez de comptes utilisateurs et administrateur, il est nécessaire de différencier les deux et de bien définir sa politique d’attribution des droits, poursuit Jayson Bruhammer. Deuxième risque, les gens ne connaissent pas les règlements internationaux concernant la gouvernance de données. Dans certains pays, le chiffrement des données que vous stockez est interdit. Il faut vérifier les certificats du fournisseur de cloud, demander un hébergement en Europe voire en France.” En cas de cyberattaque, le site cybermalveillance.gouv.fr, lancé par l’Anssi, indique la marche à suivre aux victimes (particuliers, TPE/PME) pour bénéficier d’une assistance.

Le wifi public, gratuit mais pas sûr

Avec le développement du travail à distance et la multiplication des équipements mobiles, les entreprises échangent de plus en plus de données avec leurs salariés et leurs partenaires. Dans des lieux de passage (aéroports, mais aussi lieux de coworking), il est impératif de penser à la sécurité. Le réseau de wifi public est une aubaine pour le cybercriminel.
Il existe plusieurs risques si le wifi n’est pas sécurisé. N’importe qui peut intercepter le mail. Le point d’accès peut aussi être usurpé avec la mise en place d’une fausse borne, un phénomène particulièrement développé aux États-Unis.

Les hôtels ne sont pas non plus à l’abri : depuis plusieurs années, un groupe de hackers du nom de code Darkhotel s’attaque aux réseaux disponibles dans les chambres des établissements de luxe. Objectif : voler les données sensibles de hauts responsables, PDG, directeurs des ventes et du marketing ou chercheurs, en installant le logiciel malveillant sur leur ordinateur.
Une des parades à ces intrusions consiste à utiliser un VPN (réseau privé virtuel). Ce système permet d’envoyer ou de recevoir des données à travers une connexion privée, tout en utilisant un réseau internet. Les données échangées sont cryptées, assurant la sécurité des données de l’utilisateur, ce qui permet aux employés d’accéder en toute confidentialité aux serveurs de l’entreprise à distance. Un VPN peut être installé sur n’importe quel ordinateur ou tablette, PC ou Mac. Des versions gratuites existent mas il est préférable d’opter pour un VPN payant, souvent proposé sous forme d’abonnement mensuel. Il existe également des VPN d’entreprise, avec un serveur IP dédié, ce qui évite les surcharges et les ralentissements.

Un rempart contre le piratage visuel

Le développement du travail mobile multiplie les surfaces d’exposition au piratage. “Mettre en place des pare-feu et des solutions sécurisées ne servira à rien si vous laissez sur l’écran des données visibles par la personne assise à côté de vous dans les transports ou dans un open space. Lutter contre ce piratage visuel est la dernière pierre d’un [illegible]

En poursuivant votre navigation sur notre site, vous acceptez l'utilisation de cookies pour vous proposer une navigation optimale et nous permettre de réaliser des statistiques de visites.
Fermer X
En savoir plus sur les cookies

La part prise par ce type de vol est importante. Pour le démontrer, 3M a fait appel en 2016 à Ponemon Institute qui s'est chargée d'envoyer un hacker dans des entreprises de huit pays différents dans le cadre d'une visite. L'objectif était d'obtenir des informations sensibles ou confidentielles, en utilisant uniquement des moyens visuels. Résultat : moins de 15 minutes ont suffi pour que près de la moitié des attaques visuelles atteignent leur but. 52 % des informations sensibles dérobées ont pu être consultées sur des écrans. 27 % des informations volées étaient des mots de passe, des informations financières, ainsi que des documents confidentiels.

3M propose donc des filtres de confidentialité à appliquer sur l'écran. La visibilité est claire et nette avec une vision frontale. En décalé, le filtre forme un volet opaque qui dissimule l'écran. La société travaille avec des fabricants pour intégrer ces filtres directement dans les ordinateurs. Une offre est déjà disponible sur le marché mais pour l'utiliser, il faut acheter des ordinateurs neufs alors que le parc des ordinateurs d'entreprise se renouvelle lentement. "L'offre doit encore être améliorée mais nous pensons que c'est en partie l'avenir pour la sécurisation des données, en tout cas sur les ordinateurs neufs", ajoute le responsable. Des filtres pour les téléphones portables sont aussi disponibles.

Les e-mails frauduleux viennent en tête (à 52 %) des risques informatiques qui inquiètent les responsables de PME, suivis du piratage des données (51 %).

64 % des PME font de l'amélioration de la cybersécurité une priorité.

Moins d'une PME sur 2 (43 %) est assurée, et 51 % forment leurs équipes.

Source : étude Ifop 2018 pour Kaspersky Lab

A lire également

Cybersécurité : "Le collaborateur sert de porte d'entrée à la tentative de piratage"
Protection des systèmes d'information, mode d'emploi
La gestion des risques 4.0
Les audits externes de sécurité informatique
Le marché de la cyber-assurance se développe à une vitesse grand V

Publié le 21/02/2019

Catégories :
Marketing & Technologie / Digital & internet /

L'article ne possède pas encore de commentaires.

En poursuivant votre navigation sur notre site, vous acceptez l'utilisation de cookies pour vous proposer une navigation optimale et nous permettre de réaliser des statistiques de visites.
Fermer X
En savoir plus sur les cookies

Ce site utilise Akismet pour réduire les indésirables. En savoir plus sur comment les données de vos commentaires sont utilisées.

Affaires publiques

International
Economie
Economie durable
Politique
Social & Sociétal
Agriculture
Industrie
Services
Sciences & Technologies
Culture & Société

International

Afrique
Amériques
Asie
Europe
Moyen-Orient

Finance & Juridique

Banques & assurances
Droit des affaires
Finance et gestion
Marchés financiers

Management & RH

Création d'entreprise
Gestion d'entreprise
Management d'entreprise

Marketing & Technologies

Digital & internet
Informatique & technologies
Marketing & commercial
Medias & entertainment

Art de Vivre

Art & Culture
Gestion privée & Patrimoine
Style de vie

Innovation & Stratégie

Financial Times
The Economist

Grand Paris
Grandes Ecoles

Qui sommes nous ?

Le nouvel Economiste © 2007 - 2019 - Tous droits réservés - Mentions légales - CGV - CGU - Cookies - Nous Contacter - Publicité - Les salons partenaires

En poursuivant votre navigation sur notre site, vous acceptez l'utilisation de cookies pour vous proposer une navigation optimale et nous permettre de réaliser des statistiques de visites.
En savoir plus sur les cookies

Fermer X