Les bonnes pratiques de sécurité informatique pour les petites et moyennes entreprises

Que ce soit en raison de malveillances délibérées de la part de pirates informatiques ou de négligences en interne, le nombre d'incidents liés à la sécurité informatique n'a cessé d'augmenter ces dernières années. A titre d'exemple, en 2018, le nombre d'attaques cyber contre les entreprises par rançongiciel (ransomwares) a progressé de plus de 90%.*

Toutes les entreprises traitent au quotidien des données sensibles et peuvent donc être concernées par ces incidents de sécurité. Qu'elles soient à caractère personnel (données des collaborateurs et/ou clients), financières et stratégiques (résultats de l'entreprise, projets en cours, etc.) ou encore contractuelles (contrats, devis, etc.), ces données constituent un patrimoine informationnel qu'il convient de protéger au mieux.

Il est clé pour toutes les entreprises, de toutes tailles, de prendre conscience qu'elles peuvent être confrontées à la cybercriminalité. Celle-ci peut concerner **le vol de données, l'espionnage économique, des escroqueries, etc.** Les conséquences de ces attaques pour les PME peuvent être désastreuses entrainant par exemple une atteinte à son image de marque ou d'importantes pertes économiques et financières pouvant aller jusqu'à un dépôt de bilan.

Les cybercriminels n'ont pas tous recours à des techniques sophistiquées. Notamment lorsqu'il s'agit de toucher des PME, les failles de sécurité et vulnérabilités les plus basiques sont souvent les premières portes ouvertes. Sans pour autant garantir une protection contre tout type de cyberattaques, le respect des bonnes pratiques énoncées dans ce guide vise à aider à réduire de manière significative la probabilité pour votre entreprise d'être la prochaine victime de ces attaques informatiques.

Quelques bonnes pratiques à respecter

1. Choisir des mots de passe sécurisés

Choisissez des mots de passe différents pour chaque service, composés d'au moins 8 caractères différents, l'ANSSI en recommande 12 (incluant des minuscules, des majuscules, des caractères spéciaux et des chiffres) n'ayant aucun lien avec vous et ne figurant pas dans le dictionnaire. Assurez-vous enfin que les mots de passe par défaut soient changés systématiquement.

À noter qu'un mot de passe long, avec quelques caractères spéciaux sera toujours plus robuste qu'un mot de passe court et à première vue complexe. Par exemple, il est possible de modifier une courte phrase et y ajouter des chiffres et caractères spéciaux. « Au clair de la lune » devient par exemple: Aucl@air2laLune. Ce mot de passe est plus facile à retenir et moins rapidement déchiffrable par exemple que: $ » :B1_m!.

Il est également important de renouveler fréquemment son mot de passe.

2. Mettre à jour régulièrement les systèmes et outils

Les composants informatiques (systèmes d'exploitation, applications, logiciels) sont porteurs de vulnérabilités qu'il convient de traiter dès lors que les éditeurs proposent des correctifs. Définissez une politique de mise à jour de votre parc informatique, téléchargez et appliquez les correctifs de sécurité dès qu'ils sont disponibles et utilisez exclusivement les sites Internet officiels des éditeurs.

Suite

3. Réaliser des sauvegardes régulières

Pour se prémunir d'un risque de perte de données, il convient d'effectuer régulièrement (quotidiennement ou de manière hebdomadaire en fonction de la criticité des données) des sauvegardes de vos données sur des supports réservés à cet effet (disques durs externes, DVD ou clés usb, tout en s'assurant à la fois de la provenance et de la conservation sécurisée de ces supports). Dans la mesure du possible, ces supports devront être également stockés en dehors de l'entreprise et de manière sécurisée, afin de permettre une restauration des données en cas de sinistre sur le site de l'entreprise (incendie, inondations, etc.). Des tests de restauration pourront également être réalisés afin de s'assurer que les sauvegardes sont viables.

La sauvegarde sur des plateformes Internet (cloud) est également envisageable, tout en étant conscient de potentiels risques encourus. De ce fait, l'externalisation de la sauvegarde doit être encadrée et faire l'objet de règles de sécurité.

4. Sécuriser les réseaux sans fils

Afin de sécuriser les réseaux sans fils de votre entreprise, utilisez le protocole de chiffrement WPA2 (ne jamais utiliser le chiffrement WEP « cassable » en quelques minutes). Si besoin, n'hésitez pas à contacter le support technique de votre fournisseur afin qu'il vous guide dans la sécurisation de votre connexion wifi. Les paramètres de sécurité proposés (pare-feu par exemple) doivent être activés et les mots de passe d'accès modifiés (redéfinir la clé de connexion par défaut), distribués avec parcimonie et renouvelés si nécessaire.

5. Protéger les smartphones et tablettes

Dans la mesure où ils permettent souvent d'accéder aux mêmes données qu'un ordinateur « classique » (ex : mails), les smartphones et tablettes doivent faire l'objet d'une attention toute particulière, notamment en ce qui concerne les autorisations accordées aux applications installées.

6. Protéger ses données lors d'un déplacement

Voyager avec des appareils nomades engendre des menaces pour la protection des informations sensibles, notamment en cas de vol ou la simple observation des informations affichées sur les écrans des appareils. Lors de vos déplacements, ne vous séparez pas de vos appareils nomades et utilisez des filtres de confidentialité sur vos postes de travail.

S'assurer de la sécurité de la connexion Internet est également primordial lorsque l'on travaille en dehors du bureau. Les zones proposant un « wifi gratuit » ou prétendant avoir un wifi sécurisé peuvent être compromises et infectées. Avoir recours à un réseau privé virtuel (VPN) peut atténuer ces risques. Mais il est nécessaire de toujours rester attentif aux informations que vous souhaitez transmettre via une connexion non maîtrisée lorsque vous êtes en déplacement.

7. Etre prudent lors de l'utilisation de sa messagerie

Les messageries professionnelles et personnelles sont réputées être des vecteurs d'attaques privilégiés. Vérifiez systématiquement la cohérence entre l'expéditeur présumé et le contenu du message. En cas de doute, sollicitez votre service informatique ou tentez de contacter directement l'auteur du message. Soyez également vigilant avant de cliquer sur les liens fournis par mail, ils peuvent être à l'origine des attaques de type « phishing » (ou hameçonnage). Afin de ne

Suite

pas recevoir de sollicitations non désirées (SPAM) soyez vigilants lorsque vous communiquez votre adresse email sur internet.

8. Installer des logiciels ou applications sur ses équipements de manière sécurisée

Lorsque vous installez des logiciels sur votre poste de travail ou sur vos équipements nomades, assurez-vous de le faire depuis des sources vérifiées (site de l'éditeur par exemple). Il convient également de n'octroyer les droits d'administrateurs (droits en lecture et écriture sur l'intégralité de l'appareil) des postes qu'aux personnes en ayant réellement le besoin dans le cadre de leurs fonctions.

9. Etre vigilant lors d'un paiement sur internet

Afin de vous prémunir contre une interception des données bancaires de l'entreprise lors d'une transaction effectuée en ligne, vérifiez systématiquement la présence d'un cadenas dans la barre d'adresse de votre navigateur interne. Assurez-vous également que la mention https:// apparait au début de l'adresse du site. Enfin, soyez vigilants quant à l'exactitude du site, en contrôlant notamment la présence de fautes d'orthographe.

10. Séparer les usages professionnels et personnels

Les usages et mesures de sécurité sont différents sur les équipements personnels et professionnels. Ainsi, ne faites pas suivre vos messages professionnels sur un service de messagerie personnel. N'hébergez pas non plus de données professionnelles sur des équipements personnels. Enfin, de façon analogue évitez de connecter vos supports amovibles personnels sur des équipements professionnels.

11. Former et sensibiliser les employés de l'entreprise

La crédulité humaine étant considérée comme une des plus grandes menaces, sensibiliser les collaborateurs de l'entreprise aux règles de sécurité informatique est fondamentale et efficace pour limiter une grande partie des risques. Cela passe par exemple par des campagnes de sensibilisation ou des formations des collaborateurs sur les dangers réels de la cybercriminalité et les bonnes pratiques de sécurité (choix du mot de passe, sauvegardes régulières, prudence dans l'utilisation de sa messagerie, détection et signalisation d'une menace, etc.).

12. Mettre en place une politique de sécurité informatique

Face aux évolutions de la cybercriminalité et à l'usage des nouvelles technologies, il est recommandé que l'entreprise mette en place une politique de sécurité informatique ou à défaut une charte informatique intégrant certains éléments relatifs à la sécurité. Celle-ci permet de préciser clairement les responsabilités de chacun et les procédures prévues en cas d'attaque afin que l'activité de l'entreprise puisse reprendre le plus rapidement possible.

Suite

Quelques reflexes à adopter en cas d'attaque

Lorsqu'un incident survient et qu'une investigation est nécessaire, il convient de se comporter avec le système touché comme on se comporterait sur une scène de crime. Autrement dit, il est indispensable de limiter le plus possible ses actions pour ne pas modifier l'état du système. La moindre action peut potentiellement faire disparaître des traces ou des indices précieux.

En cas d'attaque cyber, votre premier réflexe :

Contacter le service d'assistance d'AIG, qui évaluera la situation et vous mettra en relation avec des experts informatiques et juridiques afin de gérer dans les plus brefs délais la situation.

Les coordonnées de votre service d'assistance sont indiquées sur votre contrat d'assurance.

Document réalisé en collaboration avec le cabinet Wavestone. Partenaire d'AIG, Wavestone met à disposition des assurés son expertise en cyber-sécurité : stratégie, évaluation des risques et gestion de crise, conformité numérique, identité numérique, fraude et service de confiance.

* Source : rapport Malwarebytes janvier 2018

Ce document est fourni à titre d'information et ne constitue pas un avis juridique ou technique sur vos risques Cyber. AIG ne peut être tenu pour responsable de tout manquement ou de tout préjudice subi suite à une attaque cyber.

DMC AIG – Cyber 008 – Juillet 2020