E-VISIBILITÉ – FICHE PRATIQUE N° 5

Comprendre les enjeux de cybersécurité pour mieux protéger votre entreprise

En matière de cyberattaques, aucune entreprise, petite ou grande, n'est épargnée. Depuis quelques années, ces actes malveillants ont tendance à s'intensifier et à toucher particulièrement les petites structures, dans tous les secteurs d'activité. Aussi, **pour protéger votre société et votre outil de travail, il est important de connaître les différents risques, ainsi que les bonnes pratiques visant à les prévenir ou à limiter les dégâts en cas d'attaque. On vous aide à faire le point.**

LES CHIFFRES À RETENIR

7e

La France, 7e pays le plus victime de cyberattaques en 2020 dans le monde avec 1 640 plaintes déposées[1].

4 x

plus de pertes financières liées aux cyberattaques en un an sur le territoire : un coût moyen de 35 000 euros en 2020, contre 9 000 euros en 2019[2].

+ 59 %

de TPE-PME ont été visées par une cyberattaque en 2019[3].

UNE CYBERATTAQUE, ÇA CONSISTE EN QUOI ?

Il s'agit d'une violation de la sécurité de votre système informatique. Elle se manifeste souvent par un dysfonctionnement de ce système (impossibilité de vous connecter, fichiers cryptés, arrêt d'un service…). Parfois invisible, elle peut avoir des conséquences graves, comme le vol de vos informations confidentielles. Ces attaques étant de plus en plus courantes, il est important de vous y préparer pour protéger votre activité, mais aussi vos clients et vos partenaires. C'est un bon moyen pour renforcer leur confiance ! Rassurez-vous, même si le risque zéro n'existe pas, chaque entreprise peut faire beaucoup pour sa propre sécurité en mettant en place quelques mesures simples mais essentielles pour une « cyber-hygiène » de base.

ÉTAPE 1

Connaître les différents types de cyberattaques

OBJECTIF : SAVOIR À QUOI VOUS AVEZ AFFAIRE POUR ANTICIPER LES RISQUES

COMMENT ?

En vous renseignant sur les principales menaces auxquelles vous pouvez vous retrouver confronté. Voici les cyberattaques qui touchent le plus les TPE-PME :

1. La cybercriminalité

Il s'agit d'actes de piratage malveillants qui ont pour but de voler vos informations confidentielles (identifiants, mots de passe, données bancaires…) afin de les utiliser ou de les revendre. Vous pouvez être victime de :

- **phishing (ou hameçonnage) :** c'est l'attaque la plus fréquente ! Le hacker (pirate informatique) se fait passer pour une institution ou un tiers de confiance et vous envoie un mail incluant un lien frauduleux. Si vous cliquez dessus, vous êtes renvoyé vers un faux site où le hacker récupère vos données ;
- **ransomware (ou rançongiciel) :** un logiciel malveillant chiffre vos données. Résultat, tous vos documents deviennent inaccessibles ou illisibles. Le hacker vous demande alors une rançon en échange d'une « clé » pour les déchiffrer ;
- **« arnaque au président » :** aussi très courante, cette attaque consiste à convaincre l'un de vos collaborateurs, en usurpant votre identité, d'effectuer en urgence un virement important à un tiers.

2. L'atteinte à l'image

Cette menace vise à nuire à votre image en remplaçant votre site web par de fausses informations et, en général, à demander une rançon :

- **l'attaque par déni de service (ou DDoS) :** votre serveur ou réseau informatique est mis hors service. Conséquence, vos clients n'ont plus accès à votre site e-commerce si vous vendez des produits en ligne, vous ne recevez plus vos mails, etc. ;
- **le défacement (ou défiguration) :** l'affichage de votre site web est modifié, souvent pour faire passer un message politique ou religieux.

3. L'espionnage

Ce genre d'attaque, souvent invisible, touche surtout les entreprises des secteurs sensibles (industrie, santé…) et a pour objectif de voler des informations stratégiques. Sans que vous vous en rendiez compte, le hacker infiltre vos ordinateurs après vous avoir envoyé un mail très personnalisé (technique du **spear-phishing**) ou en piégeant un site internet que vous avez consulté (**attaque par point d'eau ou watering hole**).

1. FBI, Internet Crime Complaint Center (IC3), Internet Crime Report 2020.
2. Hiscox, Rapport 2020 sur la gestion des cyber-risques.
3. Hiscox, Rapport 2019 sur la gestion des cyber-risques.

NOTRE CONSEIL +

Soyez attentif à vos points de vulnérabilité, à savoir vos mails (c'est le plus souvent par là que l'attaque arrive), votre réseau informatique, vos ordinateurs, les bornes wifi non sécurisées, les objets connectés, les clés USB inconnues, certaines bannières publicitaires… mais aussi l'humain. Il est facile pour les hackers de se montrer convaincants et d'abuser de votre confiance !

ÉTAPE 2

Comprendre les risques pour votre entreprise

OBJECTIF : VOUS PRÉPARER POUR RÉAGIR RAPIDEMENT, SANS ÊTRE PRIS AU DÉPOURVU

COMMENT ?

En gardant en tête les conséquences que peut avoir une cyberattaque sur votre entreprise, mais aussi sur vos clients et vos partenaires (fournisseurs, sous-traitants…). Cela peut notamment :

- **ralentir, voire bloquer votre activité** (indisponibilité de votre site internet ou de vos postes de travail, arrêt de la production…) : il faut compter en moyenne 9 semaines pour réparer les dégâts[1] ! ;
- **nuire à votre réputation** auprès de vos clients et de vos partenaires (retards de livraison, perte de confiance…) et parfois même les « **contaminer** » ;
- entraîner des **pertes financières** (frais de restauration, perte d'exploitation, sanctions réglementaires, dédommagement des clients, extorsion…) ;
- porter **atteinte à la disponibilité des données,** à leur confidentialité ou à leur intégrité.

LE RGPD, ÇA VOUS PARLE ?

C'est le règlement général sur la protection des données. Depuis le 25 mai 2018, toute entreprise européenne qui gère des données (sur internet ou sur papier) doit obligatoirement le respecter, sous peine d'une amende pouvant s'élever jusqu'à 4 % de son chiffre d'affaires annuel ou 20 millions d'euros. En clair, pour vous, cela implique de demander le consentement de vos clients et de vos partenaires quand vous collectez leurs données, de leur permettre de les effacer à tout moment, de les conserver en toute sécurité, et de prévenir la CNIL sous 72 h en cas de piratage.

1. NTT, Risk Value 2019, Destination standstill. Are you asleep at the wheel?, 2019.

ÉTAPE 3

Adopter les bons réflexes de sécurité

OBJECTIF : PRÉVENIR LES RISQUES ET LIMITER LES DÉGÂTS EN CAS D'ATTAQUE

COMMENT ?

En observant les bonnes pratiques suivantes, faciles à mettre en œuvre au sein d'une petite entreprise :

- **identifiez vos vulnérabilités** (équipements, services, logiciels…) pour définir les contrôles de sécurité à mettre en place et prévoyez de les vérifier régulièrement ;
- **choisissez des mots de passe robustes et différents** pour chaque service : au moins 12 caractères incluant des majuscules et des minuscules, des chiffres et des caractères spéciaux (surtout pas 123456 ou votre date de naissance). Pensez à les renouveler environ tous les 90 jours ;
- **effectuez des sauvegardes régulières de données** sur un disque dur externe ou un service en ligne (cloud) pour pouvoir les restaurer en cas d'attaque (dans ce cas, pensez bien à tester leur intégrité avant tout transfert !) ;
- **n'allez pas sur internet pour des usages personnels** et débranchez la connexion de vos bureaux le week-end ;
- **activez un pare-feu,** et mettez régulièrement à jour vos logiciels et antivirus ;
- **sécurisez votre messagerie** (analyse antivirus) et n'ouvrez pas les mails douteux. En cas de suspicion, vérifiez l'authenticité du message en téléphonant à l'émetteur avant de l'ouvrir ;
- **sensibilisez vos collaborateurs** aux risques cyber ;
- **prévoyez un plan de secours** en cas d'incident cyber et diffusez-le à vos équipes ;
- **sécurisez vos appareils mobiles** (codes d'accès, chiffrement, antivirus, appareil sous surveillance…) ;
- et surtout, **ne payez pas de rançon !**

VOTRE ATOUT SÉCURITÉ

Disposer d'une bonne assurance est essentiel, car le risque zéro n'existe pas ! Chez Aviva, nous vous proposons l'assurance Aviva Cyber Sécurité, qui vous garantit une assistance 24 h/24 et 7j/7 en cas d'attaque et prend en charge les dommages subis. N'hésitez pas à en parler avec votre Agent Général Aviva ou à consulter notre site, espace Professionnels, rubrique « Assurances entreprise ».

L'AVIS DE L'EXPERT AVIVA

Julien Nelkin, Agent Général Aviva à Mirepoix (Ariège - 09)

« Si vous vendez des produits sur internet, prenez certaines précautions : l'adresse web de votre site doit commencer par "https", vous devez confirmer le paiement de vos clients par un code reçu par SMS (dispositif 3D Secure), ne proposez pas l'enregistrement automatique des coordonnées bancaires… Vous pouvez aussi passer directement par une marketplace reconnue et fiable. »

Pour en savoir plus, consultez notre fiche n° 4 !

VOS RESSOURCES UTILES

- Les documents et supports de prévention de l'ANSSI
- Le site du gouvernement « RISQUES » sur la cybersécurité
- Le fil #CyberVigilant sur Twitter pour rester informé sur les menaces

RETROUVEZ TOUTES NOS FICHES THÉMATIQUES AUPRÈS DE VOTRE AGENT GÉNÉRAL AVIVA OU SUR NOTRE SITE INTERNET

https://www.aviva.fr/conseils-en-assurance/mon-activite-professionnelle.html

Document non contractuel à caractère publicitaire, à jour au 1er mars 2021.
Mod. 19127 A – 0321
Aviva France – Société anonyme au capital de 1 678 702 329 €
Siège social : 80 avenue de l'Europe – 92270 Bois-Colombes
331 309 120 RCS Nanterre