Sensibilisation des utilisateurs : la première pierre de votre sécurité numérique

Antivirus, pare-feu, sauvegarde…, il existe différentes solutions de sécurité informatique. Et si la meilleure des protections restait la formation des salariés ? En étant capables de déjouer les pièges des cybercriminels, ils assurent la pérennité de votre activité.

L'être humain est souvent présenté comme le maillon faible de la sécurité numérique en entreprise, l'e-mail se révélant être son principal talon d'Achille : « Près de 90 % des clics sur des URL malveillantes ont lieu dans un délai de 24 heures après la remise de l'e-mail. 25 % de ces clics se produisent en seulement 10 minutes et près de 50 % en une heure ». Tirées du rapport annuel « Le facteur humain 2017 » de Proofpoint , une société spécialisée dans la sécurité informatique, ces statistiques témoignent du manque de vigilance des salariés et ainsi de l'importance de leur sensibilisation aux bonnes pratiques.

Quels sont les principaux risques ?

Le plus répandu actuellement est le **ransomware**. Il s'agit d'un virus caché dans une pièce jointe. Dès qu'on l'ouvre, il va chiffrer (ou crypter) tous les documents enregistrés sur le disque dur de l'ordinateur de l'utilisateur, mais aussi tous ceux qui sont partagés avec les autres collaborateurs via le serveur. En quelques secondes, l'activité de l'entreprise est au point mort.

L'autre menace est le **phishing** : un e-mail usurpant l'identité d'une banque ou d'un opérateur télécom vous demande de redonner vos identifiants sous différents prétextes. Les PME sont également ciblées avec de faux courriers d'une administration (impôt, URSSAF…) exigeant un virement pour effectuer une procédure quelconque.

Les cybercriminels profitent aussi de l'actualité professionnelle et notamment de l'instauration du RGPD. Fin novembre 2017, la Commission nationale de l'informatique et des libertés (CNIL) a ainsi publié une alerte sur de fausses mises en demeure administratives envoyées par fax et par téléphone à des entreprises. Comme pour le phishing, ce message insiste sur les sanctions financières encourues si les PME ne répondent pas très rapidement.

Face à ces différentes menaces, les outils de sécurité ne peuvent garantir une protection à 100 %. La cybersécurité n'est pas uniquement une affaire de logiciels ; elle repose aussi et avant tout sur la **sensibilisation des salariés**.

Quels sont les objectifs de cette sensibilisation ?

- Limiter les risques d'un piratage à cause d'une erreur humaine.
- Éviter les fuites ou les pertes de données volontaires ou involontaires.
- Réduire les tentatives d'usurpation d'identité de votre entreprise.

Les mesures élémentaires à mettre en place

Pour être en conformité avec le RGPD, différentes mesures doivent être prises :

- **première mesure : rédiger précisément votre charte informatique**
  Elle doit indiquer les droits et **les devoirs de chacun** en matière de protection des données personnelles (pour être en conformité avec le RGPD), de confidentialité des informations sensibles et d'usage des outils informatiques ;

- **deuxième mesure : mettre en place une politique de sensibilisation**
  Il existe toute une palette d'outils de **communication interne** : newsletter, affichage dans les bureaux et à la cafeteria, mémos...
  Cette politique passe également par des **sessions de formation** : intra-entreprise, e-learning mis à disposition par Generali, tutoriels vidéo… Quelle que soit la solution retenue, il s'agit de rappeler les règles de base en matière de sécurité informatique afin que tout le personnel (y compris la direction) acquière les bons automatismes.

Il faut par exemple que chaque collaborateur sache qu'en cas d'infiltration par un ransomware, le premier réflexe est de débrancher immédiatement le câble Ethernet et de couper la connexion Wi-Fi de l'ordinateur touché afin de limiter au plus vite la propagation du virus à tous les postes de travail ;

- **troisième mesure : organiser des formations spécifiques pour les services RH et comptabilité.**
  Des **formations spécifiques** aux services RH et comptabilité doivent être organisées, car ils sont de plus en plus la cible d'escrocs. Les premiers peuvent être touchés par un CV envoyé par e-mail et qui cache un code malveillant. Ils peuvent aussi être piégés par de faux profils sur les réseaux sociaux.
  Quant aux seconds, ils peuvent être victimes d'une « arnaque au faux Président ». Une personne usurpant l'identité du chef d'entreprise appelle son service comptable pour qu'il effectue immédiatement un virement afin de conclure par exemple un important marché.
  Cette escroquerie peut mettre en péril votre activité. En février 2016, une PME a ainsi été mise en liquidation judiciaire après deux arnaques au Président ayant entraîné le détournement d'environ 1,6 million d'euros.

Ce qu'il ne faut pas faire

Indépendamment de la taille ou du secteur d'activité de votre entreprise, ne restez surtout pas indifférent à sa sécurité numérique. **Toutes les PME peuvent être un jour ou l'autre victimes d'un piratage ou d'une perte de données.**

La sécurité informatique ne concerne pas uniquement les ordinateurs. **Les connexions via un smartphone peuvent aussi être à l'origine d'une attaque informatique.** Le rapport de Proofpoint révèle que 42 % des clics sur des URL frauduleuses ont été effectués depuis des terminaux mobiles.

Enfin, **ne pas faire de sauvegardes de ses données critiques est une erreur majeure.** C'est l'une des meilleures parades contre les ransomware. Payer la rançon exigée par le pirate ne garantit pas que vous pourrez récupérer vos fichiers pris en otage. Il est préférable de formater le disque dur du PC infecté et de faire une restauration de données.

Testez votre niveau de sécurité !

L'ANSSI (Agence nationale de la sécurité des systèmes d'information) a mis en place un MOOC (Massive Open Online Course). Il s'agit de cours en ligne, gratuits et accessibles à tous. Différents modules thématiques sont disponibles.

LEXIQUE

Les bons réflexes à faire passer

- Mettre à jour tous les ordinateurs et les appareils mobiles
- Utiliser des mots de passe « forts », c'est-à-dire comprenant au minimum 8 caractères, des majuscules, des chiffres et des caractères spéciaux, et dont le sens n'est pas transparent. Exemple de mot de passe « fort »: L54*45Rge.
- Contrôler les accès utilisateurs aux dossiers sensibles
- Sauvegarder ses informations confidentielles
- Multiplier les petites sessions de rappel aux bonnes pratiques en matière de sécurité informatique

Pour vous accompagner dans la formation de vos salariés, découvrez l'offre Generali Protection Numérique

https://www.generali.fr/professionnel/assurance-cyber-risques/

GAMP0002FC3A - Mars 2018