Les méthodes simples et rentables pour former votre équipe à la cybersécurité

Le risque de cyberattaque et de violation de données augmente. Les gérants d'entreprises doivent donc prendre le temps de protéger leur activité. Et pour cela, il convient d'abord de renforcer LE maillon faible des stratégies de cybersécurité : votre équipe.

La plupart des gérants d'entreprises n'enseignent pas les compétences en cybersécurité de base à leurs collaborateurs, principalement car des imprévus surviennent systématiquement et qu'ils ne trouvent pas le temps de le faire.

Malheureusement, cela peut être préjudiciable à long terme. Récemment, une étude britannique sur les violations de la cybersécurité a révélé que le coût annuel moyen du cybercrime est estimé à 15 300 £ par victime. Environ 95 % des problèmes de cybersécurité peuvent être imputés à une erreur humaine : en d'autres termes, vos collaborateurs.

Vous voulez aider votre équipe à prendre conscience des risques les plus courants et éviter que votre entreprise ne soit victime de cyberattaques ? Voici quelques méthodes simples et économiques pour former votre équipe.

Fournissez-lui les ressources appropriées

Pour former votre équipe à la cybersécurité, faites-la participer au processus d'intégration des nouvelles recrues. De cette manière, chacun comprendra dès le départ vos attentes, et votre entreprise sera moins vulnérable lorsque de nouveaux collaborateurs seront recrutés ou quand les systèmes numériques changeront de main.

Vous devez aussi fournir à votre équipe un accès simplifié aux programmes et ressources de formation à la cybersécurité. Beaucoup préfèrent apprendre quand ils le souhaitent et à leur rythme. Cela n'est pas un problème, mais vous devez alors vérifier que chaque collaborateur a bien suivi la formation.

Lorsque vous recherchez des ressources de formation, vous devez commencer par consulter le site Web du gouvernement ou vérifier si votre pays dispose d'une agence nationale dédiée à la cybersécurité. Dans le cas contraire, voici quelques programmes proposant des formations gratuites à la cybersécurité.

Cours

- Agence nationale de la sécurité des systèmes d'information (ANSSI) : l'ANSSI est l'autorité nationale en matière de cybersécurité et de cyberdéfense. Elle propose une formation en ligne sur la sécurité informatique gratuite et ouverte à tous.
- Hub Dell pour la formation à la cybersécurité : notre site comprend des ressources et informations gratuites sur des sujets comme les violations de données, les

rançongiciels et la sécurité des applications et infrastructures. Pour en savoir plus, consultez cette page.
- Capgemini : l'entreprise propose des cours sur la cybersécurité en abordant des thématiques comme la gestion des identités, les rançongiciels et la continuité informatique.

Podcasts (en anglais)

- Security Now : les experts Steve Gibson et Leo Laporte proposent chaque semaine un podcast sur la cybersécurité et les dernières actualités du numérique.
- CyberWireDaily : ce podcast est diffusé chaque jour et propose des actualités et une analyse de la cybersécurité.
- Malicious Life : Malicious Life par Cybereason raconte l'histoire méconnue de la cybersécurité, avec des commentaires et réflexions de véritables pirates, d'experts en sécurité, de journalistes et de personnalités politiques.

Autres ressources

- Ressources de cybersécurité de Cybercape pour les petites entreprises : Cybercape propose une gestion décentralisée de la cybersécurité. Son hub de ressources utiles propose des formations pour garantir la cybersécurité de votre entreprise.
- Cyber and Fraud Centre Scotland : le centre est basé en Écosse, mais propose des guides et ressources que tout le monde peut utiliser.
- TECH TALK : « AI for business: How to leverage the power of AI with Microsoft » (L'IA pour les entreprises : comment tirer parti de la puissance de l'IA avec Microsoft)
- TECH TALK : « Cyber security: Protect your business from hackers » (Cybersécurité : protégez votre entreprise des pirates)
- https://dwen.com/en-us/blog-how-to-avoid-cyber-attacks-coode-larson/
- https://dwen.com/en-us/blog-dr-amit-elazari-cybersecurity-for-small-business/

Former est une chose, mais il est aussi judicieux d'inciter votre équipe à user de prudence et à signaler toute menace potentielle. Même s'il s'agit d'une fausse alerte, il convient d'être attentif : il vaut mieux passer du temps à vérifier une fausse menace que d'avoir à gérer une véritable attaque qui aurait pu être repérée plus tôt.

Tenez-vous au courant de toute opportunité d'apprentissage potentielle

Les risques de cybersécurité évoluent constamment. Il est donc important de se tenir au courant des derniers développements. Par exemple, actuellement, les pirates sont susceptibles d'utiliser l'IA pour des cyberattaques plus sophistiquées.

Assurez-vous de vérifier régulièrement vos plans de cybersécurité, pour que votre entreprise soit protégée en permanence. De plus, veillez à ce que tous vos systèmes soient constamment à jour. En effet, les cibles les plus fréquentes des cyberattaques sont celles avec des systèmes obsolètes.

Pour vous sensibiliser aux risques de cybersécurité auxquels votre entreprise est confrontée, vous devez faire des tests. Le logiciel Cyber Coach de Mailinblack est un très bon outil qui vous permet de tester la résilience de votre entreprise face aux cyberattaques. Essayez l'outil ici.

Devez-vous utiliser des tests de sécurité contre le phishing ?

Lors des tests de sécurité contre le phishing, un employeur envoie de faux e-mails de phishing à ses collaborateurs. C'est une méthode très prisée pour tester le comportement en ligne des collaborateurs et évaluer leurs connaissances des attaques de phishing.

Gardez toutefois à l'esprit que, même si ces tests permettent de faire en sorte que vos collaborateurs restent vigilants, ils peuvent aussi constituer une forme de stress. Si vous prévoyez d'utiliser ces tests,veillez à vous y prendre de la bonne manière. Évitez de blâmer ou d'embarrasser tout collaborateur échouant à un test. Transformez cet échec en expérience plus positive en y apportant une touche ludique.

Mettez en place les bons outils et les bonnes pratiques

Disposer des outils, logiciels et pratiques appropriés peut aider à réduire le risque et l'impact négatif d'une cyberattaque.

Les collaborateurs suivront l'exemple qui leur est donné : veillez à mettre en œuvre des processus et à les appliquer. Cela inclut l'utilisation de mots de passe forts et uniques ainsi que la mise à jour de vos systèmes de sécurité.

Vous devez également vous assurer que tous vos appareils disposent d'une cyberprotection appropriée, qui peut être utilisée pour détecter et atténuer les menaces. Vous ne savez pas quoi utiliser ? Découvrez les services de sécurité proposés par Dell.