LISTE DE VÉRIFICATION

# Cyberattaques

## Comment se protéger contre les cyberattaques et quoi faire en cas d'attaque

*Voici les précautions à adopter pour empêcher les pirates informatiques d'attaquer votre organisation et une liste des mesures à prendre en cas d'attaque.*

Les cyberattaques constituent un problème de sécurité majeur, car les pirates informatiques savent exploiter toutes les faiblesses des systèmes de sécurité des petites entreprises, des sociétés du palmarès Fortune 500 de tous les secteurs.

La pandémie de COVID-19 a aggravé la situation, car davantage de travailleurs accèdent à des systèmes informatiques à distance (à l'aide d'appareils personnels). Il a été démontré qu'ils sont sujets à des attaques par hameçonnage lorsqu'ils reçoivent des courriels traitant de la COVID-19. Les pirates sont également plus motivés que jamais à attaquer les systèmes informatiques. En 2021, le total des dommages causés par la cybercriminalité devrait en effet atteindre 6 billions de dollars dans le monde[1].

Bien qu'il soit presque impossible de prévenir toutes les atteintes à la protection des données, les organisations qui se protègent contre les intrusions tout en établissant des protocoles post-attaques sont les mieux placées pour identifier une attaque et y réagir. Il est impossible de prévenir toutes les attaques, mais une organisation bien préparée est mieux équipée pour les contenir et réduire leurs répercussions au minimum.

Voici les listes de vérification destinées à la préparation et à l'intervention.

## Se préparer à une cyberattaque

- ❑ **PLANIFIER. Concevoir un plan d'intervention en cas d'incident et le tenir à jour.** Il faut établir un plan avant qu'une attaque ne survienne. Les éléments clés d'un plan d'intervention en cas de cyberincident comprennent une stratégie pour joindre les intervenants, ainsi que des instructions sur la façon d'enquêter sur le problème et de le transmettre à un échelon supérieur. Un bon plan d'intervention en cas d'incident repose souvent sur une politique sur les atteintes à la sécurité des données, qui fournit l'ensemble des principes directeurs de l'organisation.
- ❑ **PROTÉGER. Défendre l'infrastructure et former la main-d'œuvre.** Les contrôles techniques de cybersécurité, comme l'authentification multifactorielle, les sauvegardes de données régulières et les pare-feu sont essentiels. Puisque 90 % de toutes les atteintes sont causées par une erreur humaine et compte tenu de l'augmentation marquée du travail à domicile et des attaques d'hameçonnage liées à la COVID-19, les pare-feu humains sont également importants. Les employés doivent être formés (de façon continue) pour reconnaître et signaler les courriels d'hameçonnage et de maliciels au moyen d'un système de signalement à l'échelle de l'organisation. Pour assurer la sécurité de l'organisation, il incombe à chaque employé d'assurer la cybersécurité.

- **DÉTECTER. Soyez conscient de la menace.** L'utilisation d'un logiciel de protection évolutive des points de terminaison ainsi que d'outils de filtrage des courriels aidera à détecter une intrusion. L'évaluation périodique des vulnérabilités au moyen d'analyses antivirus du réseau ou de tests de pénétration est particulièrement cruciale pour les organisations ayant des emplacements multiples et des infrastructures de TI complexes.

## Intervention et rétablissement après une attaque

- **Documenter les faits et les actions.** Chaque cyberattaque ou atteinte à la sécurité des données est unique. Il est donc important de documenter les décisions clés et les actions prises. Au moment d'analyser la situation et de déterminer ce qui s'est passé, le suivi des dates, des heures et des détails aidera à préserver les preuves et à accélérer le rétablissement.

- **Contacter et valider.** Solliciter les TI constitue la première étape pour déterminer si vous avez subi une cyberattaque. Comprendre qui a été touché, si des données sensibles ont été compromises et les répercussions occasionnées contribuera à étayer les plans visant à contenir et à atténuer l'incident.

- **Aviser et tirer parti des ressources.** Un courtier d'assurance permettra de mieux orienter le processus de rétablissement et de réclamation. Il est essentiel d'aviser l'entreprise de cyberassurance au moyen de sa ligne téléphonique d'urgence afin de tirer parti des fournisseurs de solutions tiers qui vous aideront à éviter les problèmes de couverture de police à l'avenir. Le processus consiste habituellement à retenir les services d'un avocat spécialisé en protection de la vie privée, qui veillera à la conformité aux règlements fédéraux et d'état, fera appel à des fournisseurs de solutions et avisera les personnes touchées par une attaque.

- **Limiter et restreindre.** Si les fournisseurs de solutions ne sont pas immédiatement disponibles, conservez les preuves en débranchant ou en isolant les appareils touchés. Évitez de modifier l'état des systèmes en question. Si les systèmes sont en marche, laissez-les en marche, mais en les déconnectant du réseau. S'ils sont éteints, débranchez-les. Ne pas exécuter de programmes et d'utilitaires ni brancher de dispositifs de stockage ou de supports amovibles sans l'aide d'un expert.

- **Enquêter et réparer.** Les étapes concernant l'enquête en informatique judiciaire, la surveillance, la remise en état et le rétablissement sont souvent complexes et techniques. Elles devraient être dictées par un avocat spécialisé en protection de la vie privée ou un conseiller en matière d'atteinte à la vie privée. N'oubliez pas que le recours précoce à un avocat spécialisé en protection de la vie privée peut assurer le secret professionnel de l'avocat, ce qui aide à préserver la confidentialité des communications malgré les exigences juridiques qui y sont liées.

## Évitez d'être mis à rançon

Lorsque vous travaillez en partenariat avec HUB, vous êtes entouré d'une équipe d'experts qui peut vous aider à défendre et à protéger votre entreprise. HUB vous procure la tranquillité d'esprit et vous assure que vos actifs les plus importants sont en sécurité. Pour en savoir plus sur la façon de prévenir une cyberattaque et quoi faire en cas de cyberattaque, communiquez avec un spécialiste en cyberassurance de HUB.

[1] Magazine Cybercrime, « Global Cybercrime Damages Predicted To Reach 6 Trillion Annually By 2021 », 26 octobre 2020 [en anglais uniquement]