STRATÉGIES D'ATTÉNUATION DES CYBERRISQUES RECOMMANDÉES PAR BEAZLEY

1 Sauvegarder régulièrement les données critiques dans un endroit séparé qui ne sera pas affecté par un problème survenant dans votre environnement réel, et faire des tests pour s'assurer que ces sauvegardes sont restaurables.

Toutes les organisations devraient effectuer des sauvegardes régulières de leurs données critiques/importantes et doivent s'assurer que ces sauvegardes sont récentes et restaurables. Ainsi, vous pouvez garantir que votre organisation continuera à fonctionner après une cyberattaque, une suppression accidentelle, un dommage matériel ou un vol de données. En outre, si vous disposez de sauvegardes de vos données que vous pouvez récupérer rapidement, les tentatives de chantage des auteurs d'attaques par rançongiciel ont beaucoup moins de chances de réussir.

Plus la mise à jour des fichiers et des données essentiels à votre activité est fréquente, plus vous devez effectuer de sauvegardes. Vous devriez envisager de faire des sauvegardes quotidiennes si vous effectuez des modifications tous les jours, ou des sauvegardes mensuelles si vos mises à jour sont moins fréquentes, par exemple. De nombreuses plateformes sont dotées d'une fonctionnalité de sauvegarde intégrée; il se peut donc que vous disposiez déjà de plusieurs options de sauvegarde. Vous pouvez également opter pour une méthode de sauvegarde tierce (comme les plateformes de sauvegarde dans le nuage) ou effectuer vos propres sauvegardes sur des disques externes que vous gardez en sécurité et déconnectés de votre environnement réel.

2 Utiliser l'authentification multifacteur (AMF) pour accéder aux services infonuagiques et pour accéder à distance à votre réseau.

Les mots de passe n'offrent plus suffisamment de sécurité, en particulier lorsqu'il s'agit des services offerts dans le nuage (Microsoft 365, Google Workspace, etc.). Il arrive que les utilisateurs créent des mots de passe faciles à deviner, et les humains sont susceptibles de communiquer accidentellement leur mot de passe par piratage psychologique. L'AMF est importante car elle complique considérablement le vol des informations de votre organisation pour le criminel moyen. L'AMF n'élimine pas la nécessité d'utiliser des noms d'utilisateur ou des mots de passe, mais il ajoute une couche de protection à la procédure d'ouverture de session. Lorsqu'ils accèdent à des comptes ou à des applications, les utilisateurs fournissent une vérification d'identité supplémentaire, par exemple en numérisant une empreinte digitale ou en saisissant un code reçu par téléphone ou par application mobile. L'AMF est intégrée à la plupart des services infonuagiques/Internet. Veillez donc à l'activer. Sinon, il existe des fournisseurs tiers qui proposent des services d'AMF utilisant des codes SMS, des codes uniques et même des jetons matériels. Veuillez noter que l'AMF n'est pas nécessaire si vous ou votre entreprise utilisez Jane, Clinicmaster, Owl Practice ou Practiceperfect.

3 Ne pas autoriser l'accès à distance à votre environnement sans un réseau privé virtuel (RPV).

Les auteurs d'attaques informatiques procèdent régulièrement à du balayage de ports sur l'ensemble du réseau Internet à la recherche de services d'accès à distance visibles, tels que le protocole RDP (Remote Desktop Protocol) de Microsoft. Tout service ouvert utilisant le protocole RDP sera constamment scruté pour détecter les faiblesses. Le fait de dissimuler vos services d'accès à distance derrière un RPV vous offrira un bon niveau de protection contre ces attaques. Comme c'est le cas de l'AMF, il existe de nombreux fournisseurs tiers qui offrent des services de RPV, et votre propre infrastructure réseau (p. ex., les routeurs) peut également intégrer cette fonctionnalité, qui doit alors être activée. Cette exigence ne concerne que l'accès à distance aux services sur site.

4 Dispenser régulièrement (au moins une fois par année) de la formation sur la cybersécurité, y compris en matière d'antihameçonnage, à toutes les personnes qui ont accès au réseau ou aux données confidentielles/personnelles de votre organisation.

Votre personnel est la première ligne de votre organisation. Vos employés sont constamment exposés à des communications électroniques avec des tiers qui peuvent les rendre vulnérables à des attaques. Même si les mesures de sécurité techniques peuvent offrir un certain degré de protection – pensez aux passerelles de courrier électronique, aux logiciels de détection et réponse aux terminaux (EDR, Endpoint Detection and Response) – il demeure essentiel que le personnel soit conscient des risques. La formation aidera les employés à détecter les cyberrisques et, en retour, à les empêcher de nuire à votre organisation. Le National Cyber Security Centre (NCSC) offre une formation gratuite sur la cybersécurité à l'intention du personnel, qui comprend un module sur l'antihameçonnage. Vous pouvez visiter le site getcybersafe.gc.ca pour obtenir des informations et des ressources gratuites.

Pour en savoir plus, ou si vous avez d'autres questions sur les solutions d'assurance responsabilité professionnelle et d'assurance des entreprises, communiquez avec un courtier chez BMS – nous sommes là pour vous aider.

Sans frais: 1-855-318-6558 **Courriel:** info.canada@bmsgroup.com