souveraine MD
ASSURANCE

10 conseils pour renforcer la cybersécurité de votre entreprise

À la lumière de l'évolution croissante des activités commerciales en ligne, il devient de plus en plus important pour les petites et moyennes entreprises d'accorder la priorité à la cybersécurité. Voici dix conseils pour améliorer la cybersécurité de votre entreprise :

1. Faites le point sur vos actifs

Créez un inventaire de tous les actifs de l'entreprise à surveiller en cas d'incident de cybersécurité, tels que les appareils physiques (ordinateurs de bureau, ordinateurs portables, serveurs, appareils mobiles), les périphériques physiques (imprimantes, moniteurs, claviers), les appareils connectés (systèmes de point de vente, thermostats, systèmes de sécurité), les appareils de stockage physique (disques durs externes, clés USB) et les actifs numériques (comptes de médias sociaux, sites web, services en infonuagique).

2. Sécurisez vos comptes et vos appareils

Déterminez quels appareils ont accès aux données des clients, aux données financières de l'entreprise et aux données exclusives. Veillez à ce que l'accès aux programmes, aux logiciels et aux informations sensibles soit limité aux seules personnes qui en ont besoin pour des raisons professionnelles. Utilisez des mots de passe uniques pour chaque appareil et compte professionnel. Activez l'authentification multifactorielle (AMF) lorsque c'est possible. Pour assurer la sécurité des logiciels, utilisez des versions légitimes provenant de fournisseurs réputés. Si votre entreprise utilise un service d'hébergement pour son site Web, assurez-vous qu'il dispose d'un plan de sécurité et surveillez votre site Web régulièrement. Si vous utilisez un système de point de vente électronique, assurez-vous qu'il est protégé par un pare-feu, mettez en place un système de cryptage, utilisez un mot de passe unique, limitez l'accès aux employés autorisés et tenez à jour vos logiciels antivirus et anti-maliciel.

3. Sécurisez votre réseau

Les cybercriminels peuvent attaquer votre réseau pour voler des données et mener d'autres activités malveillantes. Protégez votre réseau à l'aide d'un pare-feu et d'un logiciel antivirus. Un réseau privé virtuel (RPV) peut contribuer à sécuriser les informations de votre entreprise entre vos appareils et l'Internet. Prenez des mesures pour sécuriser votre réseau Wi-Fi en créant un nom de réseau qui n'utilise pas d'informations personnelles, ainsi qu'un mot de passe unique. Évitez de vous connecter à des connexions Wi-Fi ouvertes et gratuites, à moins qu'elles ne soient sécurisées par un mot de passe et un cryptage.

4. Développez un système de sauvegarde

Si vous avez besoin de récupérer rapidement des données endommagées ou perdues à la suite d'une cyberattaque, vous devez sauvegarder vos données sur plusieurs systèmes. Pour stocker les sauvegardes de manière sûre et facile à récupérer, vous pouvez utiliser le stockage en infonuagique, les disques durs externes ou le stockage externe tel que la clé USB. Protégez votre système de sauvegarde à l'aide de mots de passe forts et d'un système de cryptage. N'oubliez pas de déconnecter les périphériques de stockage externes. Fixez-vous des rappels pour sauvegarder vos données chaque semaine.

5. Protégez les données des clients et les données sensibles

Une faille dans vos systèmes de cybersécurité pourrait signifier la perte des informations de vos clients, telles que les données clients et financières, les données des employés et les données exclusives. Sauvegardez les données clients et les données sensibles dans des bases de données en ligne ou sur vos dispositifs de sauvegarde, mais assurez-vous que l'endroit où vous stockez les données est crypté et sécurisé par un mot de passe fort. Si vous utilisez un service d'hébergement Web ou une plateforme de commerce électronique, choisissez le niveau de sécurité le plus élevé que vous puissiez vous permettre.

6. Activez les mises à jour automatiques

Une faille dans vos systèmes de cybersécurité pourrait signifier la perte des informations de vos clients, telles que les données clients et financières, les données des employés et les données exclusives. Sauvegardez les données clients et les données sensibles dans des bases de données en ligne ou sur vos dispositifs de sauvegarde, mais assurez-vous que l'endroit où vous stockez les données est crypté et sécurisé par un mot de passe fort. Si vous utilisez un service d'hébergement Web ou une plateforme de commerce électronique, choisissez le niveau de sécurité le plus élevé que vous puissiez vous permettre.

7. Activez les mises à jour automatiques

Mettez régulièrement à jour les systèmes d'exploitation et les applications de vos appareils et installez les correctifs de sécurité. Vous pouvez activer la mise à jour automatique de vos appareils et logiciels ou programmer les mises à jour à un moment où les systèmes ne sont pas utilisés de manière aussi active, par exemple pendant la nuit. Si les mises à jour automatiques ne sont pas disponibles, installez les mises à jour dès que vous y êtes invité.

8. Élaborez un plan de cybersécurité

Créez un plan de cybersécurité qui détaille les procédures à suivre au quotidien par les employés. Ce plan peut comprendre une politique d'utilisation de l'Internet, des règles de sécurité pour le courrier électronique et la messagerie, une politique relative aux médias sociaux, un plan de télétravail, un plan de départ pour les employés et un plan « Apportez votre propre appareil ». N'oubliez pas de mettre à jour le plan de cybersécurité en fonction des dernières menaces et informations.

9. Établissez un plan d'intervention en cas d'incident

Si un événement inattendu se produit, il est important d'établir un plan d'intervention en cas d'incident. Envisagez d'inclure les étapes suivantes lors de l'élaboration de votre plan de réponse aux incidents : détection, intervention et rétablissement. La section sur la détection peut comprendre des détails sur la manière dont les employés doivent signaler un problème de cybersécurité et à qui ils doivent s'adresser, sur les partenaires internes et externes que vous devez notifier et sur la manière dont vous pouvez communiquer l'incident publiquement. La section du plan consacrée à l'intervention peut comprendre des détails sur la déconnexion des appareils du réseau, la suspension temporaire de l'accès des employés pour résoudre le problème, la modification de tous les mots de passe concernés et l'activation de l'AMF, ainsi que la recherche de services professionnels pour résoudre le problème si nécessaire. La section consacrée au rétablissement peut contenir des informations sur la restauration de votre système à partir d'une sauvegarde, la mise à jour de tous les logiciels, anti-virus, pare-feu et micrologiciels une fois que votre système fonctionne à nouveau, l'exécution de logiciels anti-maliciel et anti-virus sur tous les appareils connectés et l'identification des failles dans votre plan de cybersécurité qui ont conduit à l'attaque et l'ajustement du plan. Testez votre plan d'intervention à l'aide de listes de contrôle, de simulations et de tests de système.

10. Restez informé

L'univers des cybermenaces évolue avec la découverte de nouvelles vulnérabilités et de nouvelles tactiques. Vous pouvez tenir votre organisation au courant des cybermenaces actuelles en suivant les nouvelles, les alertes et les ressources fournies par la campagne de sensibilisation Pensez cybersécurité.ca et le Centre canadien pour la cybersécurité.

La Source : « Dix mesures pour atténuer les risques ». Pensez cybersécurité - Gouvernement du Canada. Consulté le 3 octobre 2024. https://www.pensezcybersecurite.gc.ca/fr/ressources/guide-pensez-cybersecurite-petites-entreprises#C

souveraine MD
ASSURANCE