Mesures de cybersécurité de base à l'intention des petites organisations

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mai 2023 | ITSAP.10.300

Les petites et moyennes organisations (PMO) sont de plus en plus exposées à des problèmes de cybersécurité, comme les attaques par hameçonnage et rançongiciel, qui peuvent compromettre l'information sensible et entraîner des pertes financières ou de données. Dans cette publication, nous résumons les mesures de sécurité de base que vous pouvez prendre pour commencer à renforcer votre résilience en matière de cybersécurité. Ces mesures constituent un ensemble minimal de pratiques que vous pouvez mettre en œuvre au fil du temps. Vous y trouverez aussi des recommandations sur les mesures de sécurité que vous pouvez mettre en œuvre en fonction de l'augmentation des ressources et des capacités organisationnelles.

Utilisez des mots de passe robustes et l'authentification multifacteur

Utilisez une phrase de passe complexe et différente pour chaque appareil et compte. Les auteurs de menace savent que les gens réutilisent les mêmes mots de passe dans différents comptes. Si les auteurs de menace peuvent accéder à vos appareils et à vos comptes, ils peuvent les prendre en charge, les verrouiller et voler des renseignements de nature sensible. Au lieu de vous fier uniquement à votre mot de passe pour vous protéger, vous devez également utiliser l'authentification multifacteur. Lorsque l'authentification multifacteur est activée, l'utilisateur doit prouver son identité de multiples façons pour ouvrir une session, ce qui offre une protection supplémentaire et du temps pour réagir, même si un auteur de menace connaît le mot de passe. Pour en apprendre davantage, reportez-vous aux publications Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032) et Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030).

- ☐ Utilisez-vous différents mots de passe complexes d'au moins 12 caractères pour chaque compte?
- ☐ Utilisez-vous un gestionnaire de mots de passe ou avez-vous un processus pour consigner et stocker physiquement les mots de passe en toute sécurité?
- ☐ Avez-vous configuré l'authentification multifacteur sur les appareils et les comptes?
- ☐ Modifiez-vous les mots de passe en cas de compromission présumée ou réelle des appareils ou des comptes?
- ☐ Modifiez-vous tous les mots de passe par défaut générés par le fournisseur?
- ☐ Avez-vous une politique sur les mots de passe pour orienter les utilisateurs?

Appliquer automatiquement les mises à jour aux systèmes d'exploitation et aux applications

Les mises à jour et les correctifs permettent de remédier aux failles de sécurité connues, de corriger les bogues et d'améliorer la convivialité et les performances des applications et des systèmes d'exploitation. Le fait de reporter ou d'ignorer les mises à jour et les correctifs rend votre système d'exploitation et vos applications vulnérables aux cybermenaces. Les auteurs de la menace cherchent des vulnérabilités connues, les portes dérobées et autres moyens d'accéder à vos réseaux, systèmes et informations. Pour en apprendre davantage, reportez-vous à la publication Application des mises à jour sur les dispositifs (ITSAP.10.096)

- ☐ Appliquez-vous des correctifs de sécurité sur les logiciels et le matériel lorsque les fournisseurs les publient?
- ☐ Avez-vous activé les mises à jour automatiques?
- ☐ Faites-vous le suivi des applications et des systèmes d'exploitation que vous utilisez?
- ☐ Utilisez-vous des systèmes non pris en charge ou des anciens systèmes qui ne peuvent plus être mis à jour? Si oui, avez-vous un plan pour remplacer ces systèmes?

Outre la liste des mesures recommandées, nous vous recommandons d'effectuer régulièrement l'inventaire de vos biens pour déterminer ceux qui ont une grande valeur et qui doivent être protégés. Cela vous aidera à adapter et à améliorer vos pratiques de sécurité au fil du temps. Voici une liste potentielle des biens que votre organisation pourrait posséder:

- Appareils de bureau et mobiles (ordinateurs, ordinateurs portatifs, tablettes et téléphones)
- Dispositifs de stockage (disques durs et clés USB)
- Périphériques (imprimantes, numériseurs, écrans, claviers, souris et stations d'accueil)
- Appareils connectés à Internet (appareils de point de vente, systèmes de sécurité intelligents, haut-parleurs intelligents, autres appareils de l'Internet des objets)
- Biens et services numériques (comptes de médias sociaux, sites Web, services de tenue de livres en nuage et en ligne)

Données de sauvegarde

Si vos réseaux, vos systèmes ou vos renseignements sont compromis par une menace, comme un rançongiciel, ou endommagés par une catastrophe naturelle, une sauvegarde permet de minimiser le risque de perte de données, de réduire le temps d'arrêt et de rétablir les services essentiels. Pour en apprendre davantage, reportez-vous à la publication Sauvegarder et récupérer vos données (ITSAP.40.002).

- ☐ Avez-vous déterminé quels renseignements organisationnels et quels logiciels sont essentiels à la continuité des activités et au fonctionnement de l'organisation?
- ☐ Avez-vous déterminé à quelle fréquence vous sauvegarderez vos renseignements et vos systèmes?
- ☐ Avez-vous sauvegardé vos systèmes qui contiennent des renseignements organisationnels essentiels?
- ☐ Avez-vous testé vos sauvegardes et votre processus de récupération?
- ☐ Vos sauvegardes sont-elles stockées de façon sécurisée (p. ex., dans un emplacement hors site, hors ligne et non connecté à vos systèmes) et accessibles uniquement aux personnes autorisées?

Centre de la sécurité des télécommunications
Communications Security Establishment

© Gouvernement du Canada | Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production ou publication, en tout ou en partie, est stritement interdite sans l'autorisation expresse du CST. No de cat.D97-1/10-300-2023F-PDF ISBN 978-0-660-48635-2

Canada

Mesures de cybersécurité de base à l'intention des petites organisations

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mai 2023 | ITSAP.10.300

Installer des outils de sécurité préventive

Installez un logiciel de sécurité sur vos réseaux et vos appareils pour ajouter une couche de protection. Les logiciels de sécurité, comme les logiciels antivirus, analysent les systèmes et les fichiers pour détecter les maliciels, les bloquent pour empêcher le téléchargement et détectent les anomalies ou les comportements malveillants. Un réseau privé virtuel (RPV) agit comme un tunnel qui permet aux données chiffrées de passer par Internet en toute sécurité à l'abri des personnes malveillantes. Assurez-vous qu'un logiciel de sécurité soit installé sur les réseaux et appareils organisationnels. Envisagez un service DNS de protection pour protéger vos employés contre la consultation involontaire de domaines potentiellement malveillants sur Internet. Pour en apprendre davantage, reportez-vous aux publications Les outils de sécurité préventive (ITSAP.00.058) et Système d'adressage par domaine de protection (ITSAP.40.019).

- ☐ Avez-vous installé un logiciel antivirus ou antimaliciel?
- ☐ Avez-vous activé les mises à jour automatiques sur tous les logiciels de sécurité?
- ☐ Utilisez-vous un réseau privé virtuel?
- ☐ Un coupe-feu est-il installé entre votre réseau organisationnel et l'Internet?
- ☐ Utilisez-vous un service DNS de protection, comme le bouclier canadien, qui est offert gratuitement par l'Autorité canadienne pour les enregistrements Internet?

Donner de la formation au personnel sur les pratiques de cybersécurité de base

La formation adéquate constitue l'un des principaux moyens de défense contre les cybermenaces. Elle permet de s'assurer que les employés comprennent les risques de sécurité associés à leurs actions et la façon de détecter les cyberattaques par courriel ou sur le Web. Pour en apprendre davantage, reportez-vous aux publications Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093) et Ne mordez pas à l'hameçon: reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101).

- ☐ Vos employés savent-ils comment repérer les liens ou les pièces jointes aux courriels qui sont suspects?
- ☐ Vos employés savent-ils comment répondre aux appels téléphoniques, aux messages texte ou aux courriels non sollicités?
- ☐ Avez-vous un programme de sensibilisation à l'hameçonnage?
- ☐ Avez-vous une politique sur l'utilisation sécuritaire et appropriée du réseau, des logiciels et appareils et d'Internet (p. ex., interdiction d'utiliser des dispositifs USB non autorisés et des cartes mémoires externes, interdiction de télécharger des applications de sources non approuvées)?
- ☐ Offrez-vous une formation en cybersécurité à tous les employés?

Ressources utiles pour vous aider à sécuriser vos appareils mobiles:

- Utiliser son dispositif mobile en toute sécurité (ITSAP.00.001)
- Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles (ITSAP.70.002)

Élaborer un plan d'intervention en cas d'incident

Les cybermenaces, les catastrophes naturelles et les pannes imprévues entraînent des répercussions sur votre réseau, vos systèmes et vos dispositifs. Vous pensez peut-être que votre organisation ne subira pas d'incidents, mais de nombreuses entreprises canadiennes sont exposées à des menaces accrues et subissent des répercussions concrètes de la cybercriminalité. Grâce à un plan d'intervention en cas d'incident, votre organisation sera prête à intervenir et à se rétablir en cas d'incident. Pour en apprendre davantage, reportez-vous à la publication Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003). Un modèle de plan d'intervention en cas d'incident gratuit est disponible sur le site Web Cybersécuritaire Canada d'Innovation, Sciences et Développement économique.

- ☐ Avez-vous élaboré un plan d'intervention organisationnel en cas d'incident qui décrit l'intervention en fonction d'incidents de divers niveaux de gravité?
- ☐ Savez-vous qui est responsable de gérer les incidents (p. ex., équipes internes, fournisseurs de services gérés, équipe de soutien externe)?
- ☐ Avez-vous un document papier qui indique les coordonnées de vos contacts (p. ex., partenaires, fournisseurs et intervenants dans le domaine des TI) et qui est accessible même si vos systèmes et appareils sont inaccessibles?
- ☐ Avez-vous mis à l'essai votre plan d'intervention en cas d'incident et l'avez-vous mis à jour en fonction des leçons apprises?

Ces mesures de sécurité de base aideront votre organisation à commencer à renforcer sa résilience en matière de cybersécurité. Toutefois, un risque résiduel demeure. Si votre organisation a la capacité de mettre en œuvre d'autres mesures de sécurité, considérez les mesures ci-dessous:

- **Externalisation de la sécurité à un fournisseur de services gérés ou à un fournisseur de services infonuagiques** Ces fournisseurs peuvent gérer ou héberger à distance entièrement ou partiellement l'infrastructure de TI de votre organisation, surveiller les systèmes et dispositifs de sécurité, appliquer les correctifs et prendre des mesures pour éviter la compromission de vos systèmes TI. Ils offrent des services sur demande, de sorte que les coûts et la complexité sont adaptables selon les besoins et les ressources de votre organisation. Pour en apprendre davantage, reportez-vous à la publication Choisir la meilleure solution de cybersécurité pour votre organisation (ITSM.10.023).
- **Configuration d'un poste de travail administratif sécurisé** qui est isolé du réseau et dont la navigation Web et la messagerie électronique sont désactivées. Il s'agit d'un poste de travail minimal sans droit d'installation d'autres logiciels.

Vous pouvez également vous renseigner sur le programme de certification de Cybersécuritaire Canada qui aide les petites et moyennes organisations à mettre en œuvre les contrôles de sécurité conformes aux normes nationales (CAN/CIOSC 104:2021,Contrôles de base de la cybersécurité pour les petites et moyennes organisations). Le programme comporte une série de cours en ligne gratuits pour aider les organisations à apprendre comment mettre en œuvre les contrôles.

Centre de la sécurité des télécommunications
Communications Security Establishment

© Gouvernement du Canada | Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production ou publication, en tout ou en partie, est stritement interdite sans l'autorisation expresse du CST. No de cat.D97-1/10-300-2023F-PDF ISBN 978-0-660-48635-2

Canada