LES MEILLEURES MESURES POUR RENFORCER LA CYBERSÉCURITÉ DES PETITES ET MOYENNES ENTREPRISES

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

JUIN 2021 | ITSAP.10.035

Cherchez-vous des façons de protéger les réseaux et l'information de votre entreprise des cybermenaces? Le présent document résume les **13** catégories de contrôle de sécurité qui figurent dans le rapport *Contrôles de base de la cybersécurité pour les petites et moyennes entreprises* et qui constituent le fondement du programme de certification **CyberSécuritaire Canada**. Grâce à ces contrôles, vous réduirez votre exposition aux risques et serez plus apte à intervenir en cas d'incident de sécurité. **Vous n'avez pas nécessairement besoin d'instaurer tous les contrôles, mais nous vous encourageons à en adopter le plus grand nombre possible pour optimiser votre cybersécurité.**

ÉLABORER UN PLAN D'INTERVENTION EN CAS D'INCIDENT

Un plan vous permettra de réagir rapidement en cas d'incident, de restaurer les données et les systèmes essentiels et de minimiser les interruptions de service et les pertes de données. Il doit comprendre des stratégies de sauvegarde de vos données.

- *Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004)*

UTILISER UNE AUTHENTIFICATION ROBUSTE

Établissez des politiques d'authentification des utilisateurs qui répondent aux besoins, tant sur le plan de la convivialité que celui de la sécurité. Assurez-vous que les dispositifs authentifient les utilisateurs avant de leur donner accès aux systèmes. Dans la mesure du possible, recourez à l'authentification à deux facteurs ou à l'authentification

- *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)*
- *Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)*
- *Repensez vos habitudes en regard de vos mots de passe de manière à protéger vos comptes des pirates informatiques (ITSAP.30.036)*

ACTIVER LES LOGICIELS DE SÉCURITÉ

Activez les pare-feu et installez sur vos dispositifs des antivirus et des antimaliciels qui bloquent les attaques malveillantes et protègent contre les maliciels. Assurez-vous de télécharger le logiciel en question d'un fournisseur de bonne réputation. Installez un filtre de système d'adressage par domaines (DNS) sur vos appareils mobiles pour bloquer les sites Web malveillants et filtrer le contenu dangereux.

- *Les outils de sécurité préventive (ITSAP.00.058)*

APPLIQUER DES CORRECTIFS AUX APPLICATIONS ET AUX SYSTÈMES D'EXPLOITATION

Dès qu'un problème ou une vulnérabilité est détecté dans un logiciel, le fabricant diffuse un correctif qui corrige les bogues, colmate les vulnérabilités connues et améliore la convivialité et le rendement. Si possible, activez l'application automatique des correctifs et des mises à jour pour tous les logiciels et le matériel de sorte à empêcher les auteurs de menace d'exploiter les faiblesses ou les vulnérabilités.

- *Application des mises à jour sur les dispositifs (ITSAP.10.096)*

SAUVEGARDER ET CHIFFRER LES DONNÉES

Copiez votre information et vos applications essentielles sur au moins un autre endroit protégé, comme le nuage ou un disque dur externe. En cas d'incident de sécurité informatique ou de catastrophe naturelle, ces copies vous aideront à poursuivre vos activités et à prévenir la perte de données. Vos données peuvent être sauvegardées en ligne ou hors ligne de trois façons : sauvegarde complète, sauvegarde différentielle et sauvegarde incrémentielle. Testez vos sauvegardes

- *Sauvegarder et récupérer vos données (ITSAP.40.002)*

FORMER LES EMPLOYÉS

Adaptez vos programmes de formation à vos protocoles, politiques et procédures de cybersécurité. Un effectif bien formé peut faire diminuer le risque d'incident de sécurité informatique.

- *Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093)*

APPLIQUER LES CONTRÔLES

Les contrôles présentés ne sont pas des solutions universelles de cybersécurité. Ils peuvent servir à orienter la création de votre propre cadre de cybersécurité.

Vous devriez les adapter aux exigences et aux besoins de votre entreprise. Adoptez-en le plus possible pour renforcer votre posture de cybersécurité et minimiser le risque de cyberattaques. Vous pouvez commencer à améliorer la sécurité de votre entreprise en adoptant les quatre contrôles suivants :

1. Élaborer un plan d'intervention en cas d'incident
2. Appliquer les correctifs aux applications et aux systèmes d'exploitation.
3. Utiliser une authentification robuste.
4. Faire des copies de sauvegarde et chiffrer les données

Avant d'adopter ces contrôles, tenez compte des conseils suivants :

- Déterminez à quels biens et systèmes d'information essentiels vous allez appliquer les contrôles.
- Cernez les principales menaces qui pèsent sur votre entreprise.
- Relevez vos données et vos systèmes de grande valeur et appliquez les plans de gestion du risque de sorte à améliorer votre posture de sécurité.
- Appliquez une partie ou l'ensemble des contrôles et vous allez constater que votre entreprise sera beaucoup plus résiliente et mieux protégée contre les cybermenaces. .

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

LES MEILLEURES MESURES POUR RENFORCER LA CYBERSÉCURITÉ DES PETITES ET MOYENNES ENTREPRISES

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
OCTOBRE 2020 | ITSAP.XX.XXX

SÉCURISER LES SERVICES INFONUAGIQUES ET LES

Familiarisez-vous avec un fournisseur avant de retenir ses services. Assurez-vous qu'il a pris des mesures pour satisfaire à vos exigences et besoins en matière de sécurité.

Informez-vous sur l'emplacement des centres de données du fournisseur. Les lois sur la protection de la vie privée et les exigences de protection des données varient d'un pays à

- *Avantages et risques liés à l'adoption des services fondés sur l'infonuagique par votre entreprise (ITSE.50.060)*
- *Modèles de l'infonuagique (ITSAP.50.111)*
- *Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030)*

SÉCURISER LES DISPOSITIFS MOBILES

Adoptez un modèle de déploiement des dispositifs mobiles. Est-ce que votre entreprise fournira des appareils de travail aux employés ou est-ce qu'elle permettra aux employés d'utiliser leurs appareils personnels pour le travail?

Assurez-vous que les employés puissent seulement utiliser que

- *Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles (ITSAP.70.002)*

ÉTABLIR UN PÉRIMÈTRE DE DÉFENSE DE BASE

Protégez vos réseaux des cybermenaces. Par exemple, installez un pare-feu pour protéger vos réseaux des intrusions en surveillant le trafic entrant et sortant et en filtrant les sources malveillantes.

Utilisez un réseau privé virtuel (RPV) lorsque des employés font du télétravail afin de sécuriser la connexion et protéger l'information sensible.

- *Les réseaux privés virtuels (ITSAP.80.101)*

SÉCURISER LES SUPPORTS AMOVIBLES

Les supports portatifs, comme les clés USB, sont un moyen pratique et économique de stocker et de transférer des données, mais il est possible de les perdre ou de se les faire voler. Maintenez un registre de tous vos biens.

Utilisez des supports portatifs chiffrés, si possible, et nettoyez les

- *Conseils de sécurité pour les dispositifs périphériques (ITSAP.70.015)*
- *Nettoyage et élimination d'appareils électroniques (ITSAP.40.006)*

SÉCURISER LES SITES WEB

Protégez votre site Web et l'information sensible qu'il sert à recueillir. Chiffrez les données sensibles, assurez-vous que les certificats sont à jour, utilisez des mots de passe ou des phrases de passe robustes en arrière-plan et utilisez le protocole HTTPS.

Si vous avez externalisé la gestion de votre site Web, assurez-

- *Défiguration de site Web (ITSAP.00.060)*

METTRE EN ŒUVRE DES CONTRÔLES D'ACCÈS ET

Appliquez le principe du droit d'accès minimal pour prévenir les accès non autorisés et la compromission de données. Veillez à ce que les employés aient accès seulement aux informations dont ils ont besoin pour accomplir leurs tâches. Chaque utilisateur doit avoir ses propres justificatifs d'identité et les administrateurs devaient avoir deux comptes : un compte

- *Gestion et contrôle des privilèges administratifs (ITSAP.10.094)*

CONFIGURER LES DISPOSITIFS

Examinez les réglages par défaut et faites les modifications nécessaires. Nous vous recommandons à tout le moins de changer les mots de passe par défaut (surtout les mots de passe administratifs) et de désactiver la géolocalisation et les fonctions non nécessaires.

- *La cybersécurité à la maison et au bureau – Sécuriser vos dispositifs, vos ordinateurs et vos réseaux (ITSAP.00.007)*

POUR EN SAVOIR PLUS

Le présent document contient des liens vers quelques-unes de nos publications. Pour consulter l'ensemble de nos parutions, rendez-vous au **cyber.gc.ca**.

Les contrôles de cybersécurité de base servent aussi de fondement au programme de certification **CyberSécuritaire Canada**. Le programme aide les petites et moyennes entreprises à renforcer leur cybersécurité et à démontrer qu'elles prennent des mesures de cybersécurité adéquates. Le fait de répondre aux exigences de certification vous aidera à protéger votre entreprise, ses clients et ses partenaires des cyberattaques.

Pourquoi obtenir la certification?

- Renforcez votre avantage concurrentiel en rassurant vos clients, vos partenaires, vos investisseurs et vos fournisseurs en leur garantissant que les précieuses données qu'ils vous transmettront seront sécurisées.
- Limitez les répercussions directes et indirectes des cyberattaques sur votre entreprise, notamment les pertes financières, l'atteinte à votre réputation, les dommages à l'infrastructure essentielle, les litiges, les pertes d'emplois et une hausse des prix à la consommation.
- Assurez-vous que votre entreprise a le droit de concurrencer et de profiter des occasions d'affaires qui exigent une certification en cybersécurité.

Centre de la sécurité des télécommunications
Communications Security Establishment

 No de cat.D97-1/10-035-2021F-PDF ISBN 978-0-660-39076-5

Canada