Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

CONTRÔLES DE CYBERSÉCURITÉ DE BASE POUR LES PETITES ET MOYENNES ORGANISATIONS

PETITES ET MOYENNES ORGANISATIONS

TLP:WHITE

Canada

AVANT-PROPOS

La publication *Contrôles de cybersécurité de base pour les petites et moyennes organisations* est non classifiée et est destinée aux petites et moyennes organisations du Canada qui souhaitent recevoir des recommandations pour améliorer leur résilience au moyen d'investissements en matière de cybersécurité. Ce document est destiné au public et comporte donc la mention TLP:WHITE, du protocole TLP (de l'anglais *Traffic Light Protocol*) [1][1].

HISTORIQUE DES MODIFICATIONS

Version	Modifications	Date
1	Première version.	Mars 2019

APERÇU

Ce document présente les contrôles de cybersécurité de base du Centre canadien pour la cybersécurité (CCC). Nous tentons d'y appliquer la règle 80/20 (c'est-à-dire l'atteinte de 80 % des bienfaits avec 20 % d'efforts) aux pratiques de cybersécurité des petites et moyennes organisations au Canada.

AVERTISSEMENT

Les conseils et les lignes directrices contenues dans le présent rapport ne sauraient être exhaustifs et complets, car c'est aux propriétaires de systèmes qu'il incombe ultimement d'assumer les risques de cybersécurité qui menacent leurs systèmes de technologie de l'information (TI).

[1] Les chiffres qui apparaissent dans les crochets indiquent la référence. La liste des références se trouve à la section Contenu supplémentaire.

TABLE DES MATIÈRES

1 Introduction 4
2 Contrôles organisationnels 5
2.1 Évaluation de la taille de l'organisation 5
2.2 Déterminer le type de technologie de l'information visée 5
2.3 Déterminer la valeur des biens et des systèmes d'information 5
2.4 Confirmer le niveau de la cybermenace 6
2.5 Confirmer les niveaux d'investissement dans la cybersécurité 6
3 Contrôles de base 7
3.1 Élaborer un plan d'intervention en cas d'incident 7
3.2 Appliquer automatiquement les correctifs aux systèmes d'exploitation et aux applications 7
3.3 Activer les logiciels de sécurité 8
3.4 Configurer les dispositifs pour assurer leur sécurité 8
3.5 Utiliser une authentification forte 8
3.6 Fournir de la formation pour sensibiliser les employés 9
3.7 Sauvegarde et chiffrement des données 9
3.8 Services mobiles sécurisés 10
3.9 Établir un périmètre de défense de base 11
3.10 Infonuagique sécurisée et services de TI externalisés 12
3.11 Sites web sécurisés 13
3.12 Mise en œuvre des contrôles d'accès et autorisation 13
3.13 Supports amovibles sécurisés 14
4 Résumé 15
5 Contenu complémentaire 16
5.1 Liste des abréviations 16
5.2 Glossaire 16
5.3 Références 17

LISTE DES ANNEXES

Annexe A Résumé des contrôles de base 18

1 INTRODUCTION

Ce document est destiné aux petites et moyennes organisations qui cherchent à améliorer leur résilience au moyen d'investissements en matière de cybersécurité. Il vise également à donner suite au besoin qui a été cerné dans la *Stratégie nationale de cybersécurité* [2] selon lequel le gouvernement du Canada doit soutenir les petites et moyennes organisations en mettant à leur disposition de l'information sur la cybersécurité.

Comme il est indiqué dans l'*Évaluation des cybermenaces nationales* [3], ce sont les petites et moyennes organisations qui sont les plus susceptibles d'être la cible de cybermenaces et de cybercriminalité entraînant des conséquences directes sur le plan financier ou de la vie privée. Les auteurs de cybermenaces ciblent les organisations canadiennes pour obtenir des données relatives à leurs clients, partenaires et fournisseurs; des données financières; des renseignements sur leurs systèmes de paiement; ainsi que de l'information exclusive. Les incidents de cybersécurité peuvent causer une atteinte à la réputation, une perte de productivité, le vol de propriété intellectuelle ou des perturbations en plus d'exiger des dépenses relatives à la reprise des activités.

Pour réduire les risques liés aux incidents de cybersécurité, nous recommandons aux organisations de prendre connaissance du profil 1 de l'annexe 4A, de l'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [4]. Ce profil est la spécification canadienne des contrôles qui équivaut aux contrôles du Cyber Security Framework [5] du NIST ou aux contrôles de l'ISO/IEC 27001:2013 [6]. Il convient toutefois de noter que la mise en œuvre de ce profil exige d'importantes ressources dont la majorité des petites et moyennes organisations du Canada pourraient ne pas disposer.

Nous estimons, toutefois, que les organisations peuvent atténuer la plupart des cybermenaces grâce à la sensibilisation et à l'adoption de pratiques exemplaires en matière de sécurité et de continuité des activités. Ainsi, nous croyons pouvoir appliquer avec succès la règle des 80/20 (c'est-à-dire l'atteinte de 80 % des bienfaits avec 20 % d'efforts) dans le domaine de la cybersécurité pour apporter des gains concrets sur le plan de la cybersécurité des Canadiens. Le présent document présente un résumé des avis, des conseils et des contrôles de sécurité qui permettront aux organisations peuvent de tirer le maximum de leurs investissements en matière de cybersécurité. C'est ce que nous appelons les contrôles de cybersécurité de base (ci-après « contrôles de base »).

Nous encourageons donc les organisations à mettre en œuvre le plus grand nombre de contrôles de base en fonction des ressources dont elles disposent. Si la majorité des organisations canadiennes mettent en œuvre ces contrôles, le Canada sera plus souple et jouira d'une meilleure cybersécurité. Pour obtenir des conseils et des avis supplémentaires, veuillez consulter le site cyber.gc.ca.

2 CONTRÔLES ORGANISATIONNELS

La cybersécurité dépend d'une multitude de facteurs. Elle est donc différente d'une organisation à l'autre. Le but de cette section est d'aider une organisation à déterminer si les contrôles de base sont indiqués dans les circonstances.

2.1 ÉVALUATION DE LA TAILLE DE L'ORGANISATION

Nous avons l'intention de mettre en place des contrôles de base pour les organisations qui répondent aux définitions d'Industrie, sciences et développement économique Canada pour les petites et moyennes organisations [7], à savoir les organisations qui comptent moins de 499 employés.

Les contrôles de base sont destinés aux organisations qui correspondent à la définition de « petite et moyenne organisations » [7], d'Industrie, sciences et développement économique Canada, à savoir les organisations qui comptent moins de 499 employés. Nous recommandons que les plus grandes organisations investissent dans des mesures de cybersécurité plus exhaustives.

Résumé :

CO.1 Les organisations qui utilisent des contrôles de base doivent compter moins de 499 employés.

2.2 DÉTERMINER LE TYPE DE TECHNOLOGIE DE L'INFORMATION VISÉE

Les organisations doivent déterminer quels éléments de leurs biens et systèmes d'information seront visés par les contrôles de base qu'elles souhaitent mettre en œuvre. En l'occurrence, les biens et systèmes d'information comprennent les ordinateurs, les serveurs, les dispositifs réseau, les appareils mobiles, les systèmes d'information, les applications, les services, les applications infonuagiques, etc., qu'une organisation utilise pour mener ses activités. Au reste, nous recommandons fortement aux organisations de veiller à ce que tous leurs biens et systèmes d'information (qu'elles en soient les propriétaires, que ces biens fassent l'objet d'un contrat ou qu'elles les utilisent de toute autre façon) soient visés par les contrôles de base.

Résumé :

CO.2 Les organisations doivent déterminer les éléments de leurs biens et systèmes d'information qui s'inscrivent dans la portée des contrôles de base qu'elles souhaitent mettre en œuvre.

2.3 DÉTERMINER LA VALEUR DES BIENS ET DES SYSTÈMES D'INFORMATION

Les organisations doivent connaître la valeur de leurs biens et de leurs systèmes d'information. Par exemple, il se peut que les informations sensibles ayant trait aux clients doivent être protégées. Il en va de même pour les informations privilégiées qui leur permettent de demeurer concurrentielles, notamment les renseignements sur la propriété intellectuelle.

Les organisations doivent évaluer le niveau de préjudice sur les plans de la confidentialité, de l'intégrité et de la disponibilité des systèmes d'information et des données :

- Sur le plan de la confidentialité, un préjudice pourrait se produire s'il y a une divulgation non autorisée de renseignements sensibles (p. ex., si une personne divulgue des renseignements de nature délicate au public ou à un concurrent).
- Sur le plan de l'intégrité, un préjudice pourrait se produire s'il y a une modification non autorisée de renseignements (par exemple, si quelqu'un modifie des renseignements de nature délicate qui deviennent alors inexacts).
- Sur le plan de la disponibilité, un préjudice pourrait se produire si l'information n'est pas disponible aux fins d'utilisation pendant un certain temps ou si elle est perdue de façon permanente (par exemple, si quelqu'un parvient à interrompre l'accès au site Web de l'organisation ou à supprimer des renseignements sensibles).

Les organisations doivent évaluer le niveau de préjudice lié à la confidentialité, à l'intégrité et à la disponibilité des biens et systèmes d'information au moyen de l'échelle suivante :

- Très faible – aucun préjudice

- Faible – préjudice probable (p. ex., certaines pertes financières)
- Moyen – préjudice probable et grave (p. ex. affaiblissement de la position concurrentielle, atteinte à la réputation)
- Élevé – préjudice probable et extrêmement grave (p. ex., compromission de la viabilité de l'organisation).

Les contrôles de sécurité de base sont prévus pour les situations où tous les préjudices sont à un niveau égal ou inférieur au niveau moyen. Nous recommandons que les organisations qui pourraient subir davantage de préjudices investissent dans des mesures de cybersécurité plus exhaustives.

Résumé :

CO.3 Les organisations doivent évaluer le niveau de préjudice sur le plan de la confidentialité, de l'intégrité et de la disponibilité de leurs biens et systèmes d'information.

2.4 CONFIRMER LE NIVEAU DE LA CYBERMENACE

Comme il est indiqué dans l'*Évaluation des cybermenaces nationales* [3], ce sont les petites et moyennes organisations qui sont les plus susceptibles d'être la cible de cybercriminalité. C'est dans cette optique que nous avons élaboré les contrôles de base qui permettent de contrer efficacement ce type de menace.

En outre, certaines cybermenaces ciblant les petites et moyennes organisations ont des répercussions qui vont bien au-delà de celles résultant du cybercrime. Par exemple, les organisations œuvrant dans les secteurs économiques stratégiques devraient consulter l'*Évaluation des cybermenaces nationales* [3] et décider si elles ont de la propriété intellectuelle ou d'autres renseignements de nature délicate qui les rendraient plus susceptibles d'être la cible d'espionnage industriel. Les organisations doivent également décider si les cyberincidents ciblant leurs biens et systèmes d'information sont susceptibles de compromettre la sécurité nationale ou la sécurité du public. Nous recommandons aux organisations qui font face à des niveaux de cybermenace plus élevés d'investir dans des mesures cybersécurité plus élaborées.

Résumé :

CO.4 Les organisations devraient cerner la menace qui les préoccupe le plus.

2.5 CONFIRMER LES NIVEAUX D'INVESTISSEMENT DANS LA CYBERSÉCURITÉ

Les organisations devraient nommer une personne occupant un poste de direction, au titre de responsable de la sécurité des TI. Nous recommandons que les plus grandes organisations considèrent l'embauche d'un responsable de la sécurité des systèmes d'information.

Les organisations devraient aborder la question des investissements en matière de cybersécurité en cernant le niveau de leurs dépenses en technologie de l'information et en sécurité des TI. Selon une analyse de l'industrie [8], les organisations peuvent consacrer jusqu'à 13 % de leur budget de TI à la cybersécurité, alors qu'il est conseillé de consacrer de 4 à 7 % du budget à la cybersécurité. Nous recommandons que les organisations évaluent leurs dépenses par rapport à ces chiffres, mais également qu'elles tiennent compte de leurs priorités à cet égard. En outre, nous recommandons aux organisations qui ont d'importantes dépenses en TI et en sécurité des TI d'investir dans des mesures de cybersécurité plus élaborées.

Veuillez noter que les niveaux de dépenses en TI et en sécurité des TI comprennent tous les coûts connexes, y compris les coûts liés à l'impartition.

Résumé :

CO.5.1 Les organisations devraient nommer une personne occupant un poste de direction au titre de responsable de la sécurité des TI.

CO.5.2 Les organisations devraient déterminer le niveau des dépenses qu'elles consacrent aux TI et aux investissements en sécurité des TI (chiffres bruts et pourcentages des dépenses totales).

CO.5.3 Les organisations devraient déterminer la part de leur effectif qui travaille en TI et en sécurité des TI (chiffres bruts et pourcentage de l'effectif).

3 CONTRÔLES DE BASE

Dans les sections qui suivent, nous présentons les contrôles de base dans le but d'aider les organisations à réduire les risques de cyberincidents ou d'atteinte à la protection des données. Ces contrôles mettent l'accent non seulement sur la réduction des risques, mais aussi sur la façon dont une organisation doit intervenir pour répondre aux incidents. En définitive, nous recommandons aux organisations de tenir pour acquis que des auteurs malveillants tenteront de porter atteinte à la protection de leurs données. Ainsi, elles seront mieux à même de détecter ces atteintes et d'intervenir adéquatement de façon à rétablir leurs activités.

3.1 ÉLABORER UN PLAN D'INTERVENTION EN CAS D'INCIDENT

Les organisations doivent envisager les incidents de cybersécurité comme étant inévitables et doivent disposer d'un plan d'intervention pour assurer la reprise de leurs activités. Ce plan devrait faire partie des plans de l'organisation sur la reprise des activités et la continuité des opérations en cas de sinistre.

Nous recommandons que les organisations mettent en œuvre des solutions permettant de détecter et surveiller les incidents et d'intervenir en conséquence, habituellement au moyen de systèmes de gestion des informations et des événements de sécurité. Toutefois, les petites organisations pourraient ne pas avoir les moyens d'effectuer de telles activités, ni en interne ni par le recours à des services externes. Malgré tout, les organisations devraient nommer une personne responsable d'intervenir en cas d'incident et définir les responsabilités qu'elle doit assumer. Au nombre de ces responsabilités, nous recommandons que les organisations prévoient leurs obligations légales relatives au signalement des incidents de cybersécurité. Les organisations qui ont besoin de soutien externe pour intervenir en cas d'incident devraient avoir un plan détaillé indiquant l'intervenant à embaucher et les types de services offerts par cet intervenant. Les organisations devraient envisager l'achat d'une police d'assurance en matière de cybersécurité qui comprend une couverture pour l'intervention et la reprise des activités en cas d'incident en plus de la responsabilité civile.

Résumé :

CB.1.1 Les organisations devraient avoir un plan de base faisant état des modes d'intervention en cas d'incidents en fonction des divers niveaux de gravité. Si une organisation n'est pas en mesure de gérer certains types d'incidents, elle devrait avoir un plan indiquant ce qu'elle compte faire.

CB.1.2 Les organisations devraient avoir un plan d'intervention officiel en cas d'incident qui précise les responsabilités relatives à la gestion des incidents; ce plan devrait comprendre les coordonnées des responsables concernés, de même que celles des parties externes, des intervenants et des organisations de réglementation. Les organisations devraient tenir à jour une copie papier de ce plan, au cas où une version numérique du plan ne serait pas accessible.

CB.1.3 Les organisations devraient envisager l'achat d'une police d'assurance en matière de cybersécurité qui comprend une couverture pour les activités liées à l'intervention en cas d'incident et pour assurer la reprise des activités.

CB.1.4 Les organisations devraient envisager la mise en œuvre d'une capacité de surveillance (p. ex., un système de gestion des informations et des événements de sécurité) ou consigner les informations expliquant leurs motifs de ne pas le faire.

3.2 APPLIQUER AUTOMATIQUEMENT LES CORRECTIFS AUX SYSTÈMES D'EXPLOITATION ET AUX APPLICATIONS

Les fournisseurs en TI diffusent régulièrement des mises à jour (correctifs) pour leurs logiciels et micrologiciels, de façon à corriger des défauts et des vulnérabilités en matière de sécurité. Faire un suivi manuel des vulnérabilités pour les divers produits du réseau est chronophage et coûteux. Pour les organisations plus grandes, il est avantageux, quoique coûteux, de faire la gestion des correctifs et des vulnérabilités pour réduire les risques en matière de cybersécurité.

Pour les petites et moyennes organisations, nous recommandons qu'elles activent les mises à jour automatiques pour tous leurs logiciels et tout le matériel, si une telle option est disponible – ou qu'elles envisagent de remplacer leurs logiciels et leur matériel par des produits qui offrent cette option. Il va de soi que cette recommandation s'applique aussi au remplacement des logiciels et du matériel pour lesquels le fournisseur a mis fin au soutien et n'envoie plus de mises à jour

(c.-à-d., les produits après la fin de leur vie utile). Ainsi, les petites et moyennes organisations pourront veiller à ce que les appareils autonomes, les systèmes d'exploitation, les applications et les logiciels de sécurité soient à jour et exempts de vulnérabilités connues.

***Nota* :** Ces recommandations diffèrent de celles qui visent les grandes organisations. Dans leur cas, nous préconisons la gestion complète des vulnérabilités et des correctifs. Il y a des risques inhérents à l'application automatique de correctifs, c'est-à-dire qu'il peut y avoir des répercussions imprévues. Nous croyons que les organisations plus petites peuvent obtenir le même résultat en matière de cybersécurité que les plus grandes organisations, lorsqu'elles acceptent tout simplement les risques de l'application des correctifs par défaut. Cette hypothèse sur le risque convient moins aux grandes organisations qui ont le personnel pour gérer et atténuer les risques. Les organisations doivent trouver un compromis au cas par cas.

Résumé :

CB.2.1 Les organisations devraient activer l'application automatique des correctifs pour tous les logiciels et tout le matériel OU mettre en place des solutions complètes de gestion des vulnérabilités des correctifs.

CB.2.2 Les organisations devraient mener des activités d'évaluation des risques pour déterminer si elles doivent remplacer ou non le matériel et les logiciels qui ne permettent pas l'application automatique des mises à jour. Si l'organisation choisit de conserver de tels appareils, elle doit avoir un processus opérationnel pour faire manuellement les mises à jour de façon régulière.

3.3 ACTIVER LES LOGICIELS DE SÉCURITÉ

Les organisations devraient se protéger contre la menace posée par les maliciels connus (p. ex. virus, vers, chevaux de Troie, rançongiciels, logiciels espions, etc.) en optant pour une configuration sécurisée de leurs appareils branchés et en activant les logiciels antivirus et anti-logiciel malveillant, si possible sur ces appareils. Conformément à ce qui est indiqué à la section 3.2, les organisations doivent activer les fonctions d'automatisation (mise à jour et de balayage) de leurs applications, et doivent envisager de remplacer tout produit qui n'est pas doté de ces caractéristiques.

Résumé :

CB.3.1 Les organisations devraient mettre en place des antimaliciels dotés de fonctions automatisées de mises à jour et de balayage.

3.4 CONFIGURER LES DISPOSITIFS POUR ASSURER LEUR SÉCURITÉ

Les mots de passe d'administration qui sont établis par défaut de même que les paramètres par défaut non sécurisés sur les dispositifs constituent un problème important sur les réseaux d'entreprise. Les fournisseurs et même les revendeurs configurent souvent les dispositifs avec des mots de passe d'administrateur établis par défaut. Il s'en faut peu pour que ces mots de passe soient connus du public.

Les organisations doivent s'assurer de changer tous les mots de passe d'administrateur sur leurs appareils. Ce faisant, elles devraient également examiner les paramètres sur leurs appareils (qui pourraient avoir été réglés par défaut et de façon non sécurisée) afin de désactiver toutes les fonctionnalités inutiles et activer toutes les caractéristiques de sécurité nécessaires. Les organisations devraient possiblement envisager d'utiliser des profils de configuration sécurisés sur leurs produits, comme l'indiquent les normes du Center for Internet Security [9] – ou mettre en place un contrat avec un fournisseur de services TI qui le fera à leur place.

Résumé :

CB.4.1 Les organisations devraient utiliser des configurations de sécurisation sur tous leurs appareils en changeant tous les mots de passe par défaut, en désactivant les caractéristiques inutiles et en activant toutes les caractéristiques de sécurité pertinentes.

3.5 UTILISER UNE AUTHENTIFICATION FORTE

Les organisations devraient avoir des politiques d'authentification des utilisateurs qui répondent aux besoins, tant sur le plan de la convivialité que celui de la sécurité. Dans la mesure du possible, utiliser une authentification à deux facteurs. Ces

méthodes combinent l'utilisation de quelque chose que l'utilisateur connaît (p. ex., un mot de passe) avec quelque chose que l'utilisateur a en sa possession (p. ex. un jeton physique, un code généré par une application, un appel téléphonique automatisé vers un numéro de téléphone préétabli). Les solutions à deux facteurs ne s'équivalent pas toutes, mais elles permettent d'améliorer globalement la posture de cybersécurité de l'organisation.

Nous recommandons de modifier les mots de passe seulement lorsqu'il y a des soupçons ou des éléments prouvant qu'il y a des problèmes de sécurité, comme la divulgation accidentelle d'un mot de passe ou des preuves qu'une personne a compromis un compte.

Les organisations devraient avoir des politiques claires sur la longueur des mots de passe, sur la réutilisation des mots de passe, sur l'utilisation de gestionnaires de mots de passe et sur les conditions qu'un utilisateur doit satisfaire pour pouvoir consigner son mot de passe et sur la façon de conserver ce mot de passe. Nous recommandons que les organisations suivent nos conseils relatifs à la sélection d'un mot de passe dans le *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* [10].

Résumé :

CB.5.1 Les organisations doivent mettre en œuvre une solution d'authentification à deux facteurs dans la mesure du possible et consigner tous les cas où elles prennent la décision de ne pas le faire. Les organisations devraient exiger une authentification à deux facteurs pour les comptes importants, tels que les comptes financiers, les administrateurs du système, les administrateurs du nuage, les utilisateurs privilégiés et les cadres supérieurs.

CB.5.2 Les organisations devraient uniquement obliger la modification d'un mot de passe lorsqu'elles soupçonnent qu'il y a eu compromission ou s'il existe des preuves de compromission.

CB.5.3 Les organisations devraient avoir des politiques claires sur la longueur des mots de passe, sur la réutilisation des mots de passe, sur l'utilisation de gestionnaires de mots de passe et sur les conditions auxquelles un utilisateur doit satisfaire pour consigner ou conserver son mot de passe en toute sécurité.

3.6 FOURNIR DE LA FORMATION POUR SENSIBILISER LES EMPLOYÉS

C'est l'erreur humaine qui demeure la cause trop fréquente d'incidents de cybersécurité pendant l'utilisation des systèmes d'information. Comme première ligne de défense, les organisations devraient donner de la formation à leurs employés sur les pratiques de sécurité de base. Les organisations devraient mettre l'accent sur les mesures pratiques et faciles à appliquer comme :

- l'utilisation de politiques efficaces sur les mots de passe (voir la section 3.5);
- la détection de courriels et de liens malveillants;
- l'utilisation de logiciels approuvés;
- l'utilisation adéquate de l'Internet;
- l'utilisation sécuritaire des médias sociaux.

Résumé :

CB.6.1 Les organisations devraient investir dans la formation pour sensibiliser leurs employés à la cybersécurité.

3.7 SAUVEGARDE ET CHIFFREMENT DES DONNÉES

Nous recommandons que les organisations sauvegardent régulièrement tous les renseignements commerciaux essentiels sur un support externe et sécurisé. La sauvegarde des données est un élément essentiel des efforts qui doivent être déployés pour assurer un rétablissement rapide non seulement à la suite d'un incident de cybersécurité, comme une attaque au rançongiciel ou une attaque perpétrée avec un maliciel, mais encore des suites d'une catastrophe naturelle, d'une panne d'équipement ou d'un vol.

Les organisations doivent cerner les renseignements commerciaux (y compris les renseignements de nature délicate) qui sont essentiels à leur fonctionnement et déterminer la fréquence à laquelle ces renseignements changent. Les organisations devraient déterminer au cas par cas les systèmes qui doivent faire l'objet d'une sauvegarde et la fréquence à laquelle la

sauvegarde doit être faite, car tous les systèmes auront différentes exigences en matière de sauvegarde et de récupération des données. Par exemple, les postes de travail essentiels et les serveurs peuvent nécessiter des sauvegardes incrémentielles quotidiennes, alors que les postes de travail de base peuvent être récupérés à partir d'une image commune.

Les organisations devraient avoir des procédures claires sur la façon de rétablir leurs activités à partir des sauvegardes et vérifier régulièrement le fonctionnement adéquat des mécanismes de sauvegarde et de restauration.

Les organisations doivent s'assurer qu'elles conservent leurs copies de sauvegarde chiffrées dans un endroit sécurisé. Seuls les responsables de la mise à l'essai ou de l'exécution des modalités de reprise devraient pouvoir accéder aux copies de sauvegarde. Les organisations doivent également envisager d'entreposer les copies de sauvegarde hors site (emplacement physique ou services d'infonuagique) pour varier les méthodes dans l'éventualité d'un sinistre (incendie, inondation, tremblement de terre ou incident de cybersécurité localisé).

Résumé :

CB.7.1 Les organisations doivent effectuer la sauvegarde des systèmes qui contiennent des renseignements commerciaux essentiels et s'assurer que des mécanismes de reprise puissent adéquatement restaurer ces systèmes à partir des sauvegardes. Les organisations devraient envisager d'entreposer les sauvegardes dans un endroit hors site sécurisé.

CB.7.2 Les organisations devraient entreposer dans un endroit sûr les sauvegardes chiffrées et limiter l'accès à ces sauvegardes aux responsables des mises à l'essai ou des activités de restauration des données.

3.8 SERVICES MOBILES SÉCURISÉS

Les appareils mobiles comme les téléphones cellulaires sont essentiels pour la plupart des organisations. Les organisations doivent opter pour le modèle de propriété qu'elles souhaitent adopter concernant les appareils mobiles. En général, les organisations fournissent des dispositifs selon le modèle « Voici votre appareil personnel (VAP) » ou permettent aux employés d'utiliser leurs propres appareils, selon le modèle « Prenez votre appareil personnel (PAP) ». Dans les deux cas, les organisations doivent prendre des mesures pour sécuriser les renseignements de nature délicate et l'accès à l'infrastructure TI d'entreprise à partir de ces dispositifs.

Que les appareils mobiles appartiennent à l'organisation ou aux employés, un principe directeur prime : il est impérieux d'avoir une séparation entre les données de nature professionnelle et les données personnelles sur ces appareils, y compris les applications, les comptes de courrier électronique, les contacts, etc. Il existe de nombreuses solutions pour séparer les espaces professionnels et personnels, notamment l'utilisation d'applications distinctes pour le travail et la vie personnelle ou l'utilisation de « dossiers sécurisés » natifs ou encore des « espaces de stockage » pour les renseignements commerciaux sensibles. Les organisations doivent déterminer la façon d'appliquer cette séparation de sorte à trouver un équilibre entre les activités de l'organisation et ses besoins en matière de sécurité. Les organisations devraient exiger que tous les appareils mobiles stockent tous les renseignements de nature délicate de façon sécurisée et chiffrée.

Nous recommandons aux organisations d'adopter les pratiques relatives à la configuration sécurisée de tous leurs appareils mobiles, lesquelles sont énoncées à la section 3.4.

Les applications améliorent grandement la capacité et la productivité des appareils mobiles, mais elles peuvent aussi présenter des risques. Pour minimiser ces risques, les organisations devraient exiger que les employés téléchargent seulement des applications de sources dignes de confiance, comme les boutiques d'applications bien connues. Si les organisations ne peuvent pas appliquer cette politique au moyen de contrôles techniques, elles devraient offrir une formation de sensibilisation à la sécurité à ce sujet (voir la section 3.6).

Les organisations qui ont une infrastructure TI et des processus opérationnels plus matures devraient opter pour une solution de gestion de la mobilité d'entreprise qui permet d'activer des fonctionnalités d'entreprise améliorées et qui permet de mieux administrer les appareils mobiles. Les solutions de gestion de la mobilité d'entreprise comportent diverses capacités, mais elles comprennent généralement les fonctions de gestion et de vérification et elles permettent d'encadrer l'utilisation des appareils mobiles en milieu de travail. Elles peuvent aussi inclure la capacité d'effacer à distance les données sur les appareils.

Pour la connectivité mobile, les organisations devraient demander aux utilisateurs de désactiver les connexions automatiques aux réseaux Wi-Fi ouverts et d'éviter les réseaux Wi-Fi inconnus; elles devraient aussi limiter Bluetooth et les autres protocoles de communication en champ proche pour la transmission de renseignements de nature délicate. Les organisations devraient aussi exiger des utilisateurs qu'ils sélectionnent l'option la plus sûre pour se connecter à Internet, par exemple en utilisant des données sur les réseaux cellulaires plutôt que les réseaux Wi-Fi publics.

Résumé :

CB.8.1 Les organisations devraient opter pour un modèle de propriété des appareils mobiles et consigner les motifs expliquant leurs décisions de même que les risques connexes.

CB.8.2 Les organisations doivent exiger qu'il y ait une séparation entre les données de nature professionnelle et les données personnelles sur les appareils mobiles qui accèdent aux ressources TI de l'entreprise. Les organisations doivent consigner les détails relatifs à cette séparation.

CB.8.3 Les organisations doivent veiller à ce que les employés téléchargent uniquement les applications pour appareils mobiles de la liste de sources dignes de confiance fournie par l'organisation.

CB.8.4 Les organisations devraient exiger que tous les appareils mobiles stockent tous les renseignements de nature délicate de façon sécurisée et chiffrée.

CB.8.5 Les organisations devraient mettre en œuvre une solution de gestion de la mobilité d'entreprise pour tous les appareils mobiles OU consigner les risques qu'elles assument, notamment sur le plan de la vérification, de la gestion et de la fonctionnalité de sécurité des appareils mobiles, en choisissant de ne pas mettre en œuvre une telle solution.

CB.8.6 Les organisations devraient encourager, voire contraindre les utilisateurs à suivre les consignes suivantes : (1) désactiver les connexions automatiques aux réseaux ouverts; 2) éviter la connexion aux réseaux Wi-Fi inconnus; (3) limiter l'utilisation de Bluetooth et des autres protocoles de communication en champ proche pour la transmission de renseignements de nature délicate; (4) utiliser le Wi-Fi de l'organisation ou le réseau cellulaire plutôt qu'un réseau Wi-Fi public.

3.9 ÉTABLIR UN PÉRIMÈTRE DE DÉFENSE DE BASE

Les réseaux connectés à Internet doivent être protégés contre les menaces en ligne au moyen de coupe-feu. Un coupe-feu est un logiciel ou un périphérique matériel qui surveille le flux de trafic et qui peut défendre un réseau interne contre les intrusions. Les organisations devraient mettre en œuvre des coupe-feux spécialisés à la frontière séparant les réseaux d'entreprise de l'Internet.

Les organisations doivent activer le logiciel coupe-feu intégré dans les systèmes d'exploitation sur tous les appareils à l'intérieur de leurs réseaux, à moins que l'organisation installe et configure une solution de rechange équivalente.

Les organisations devraient installer et configurer des coupe-feux dotés du système d'adressage par domaines (DNS) pour empêcher la connexion aux domaines malveillants connus. Des solutions sont disponibles pour protéger tous les dispositifs connectés à un réseau d'entreprise. Les organisations devraient également envisager une solution coupe-feu par DNS pour le filtrage de contenu, de façon à limiter l'accès à des sites Web à partir du réseau d'entreprise.

Les organisations devraient exiger l'utilisation d'une connexion sécurisée à tous ses services TI d'entreprise en ligne. Si une organisation permet aux employés de se connecter à son réseau local à partir d'Internet, elle devrait faire installer une passerelle vers un réseau privé virtuel (RPV) et exiger que les utilisateurs accèdent au réseau de l'organisation au moyen du RPV et d'un mécanisme d'authentification à deux facteurs (voir la section 3.5).

Les organisations qui ont un réseau Wi-Fi interne devraient utiliser le protocole de sécurité sans fil WPA2 ou un meilleur protocole. Dans la mesure du possible, les organisations devraient utiliser la version la plus forte (p. ex. WPA2-Enterprise), puisque cette version exige une authentification plus robuste des utilisateurs. Les organisations devraient consulter la documentation sur leurs produits pour savoir comment configurer ces protocoles. De plus, les organisations doivent isoler le réseau Wi-Fi au moyen d'un coupe-feu qui filtre le trafic entrant par le réseau sans fil en direction d'autres ressources du réseau.

De même, si une organisation choisit d'offrir des services de Wi-Fi public aux visiteurs et invités, elle ne devrait jamais relier ce réseau public à ses réseaux et à ses ressources internes, comme les imprimantes ou les systèmes audiovisuels.

Les organisations devraient suivre les normes de sécurité sur les données de l'industrie des cartes de paiement (PCI DSS) [11] pour tous les terminaux de point de vente et systèmes financiers. Les organisations devraient séparer les terminaux de point de vente et les systèmes financiers de façon à les isoler d'Internet en plus de les séparer des autres zones du réseau d'entreprise au moyen d'un coupe-feu. Les organisations devraient empêcher les systèmes de point de vente de naviguer sur Internet ou de balayer les services internes non liés aux opérations financières ou aux fonctions de contrôle des stocks.

Les organisations devraient filtrer les pourriels et les courriels qui contiennent des liens ou des pièces jointes malveillants. Pour réduire les risques de courriel frauduleux ou trompeur, les organisations doivent s'assurer que leur service de courrier électronique met en œuvre la spécification DMARC, de l'anglais *Domain-Based Message Authentication, Reporting and Conformance* [12].

Résumé :

CB.9.1 Les organisations devraient mettre en œuvre des coupe-feux spécialisés à la frontière des réseaux d'entreprise et de l'Internet.

CB.9.2 Les organisations devraient mettre en place un coupe-feu doté de DNS pour les requêtes DNS sortantes vers l'Internet.

CB.9.3 Les organisations doivent activer tout logiciel coupe-feu intégré dans les appareils sur leurs réseaux ou elles doivent consigner les mesures de rechange qui remplacent ces coupe-feux.

CB.9.4 Les organisations devraient exiger une connexion sécurisée à toutes les ressources TI d'entreprise en plus d'exiger la connexion à un RPV avec une authentification à deux facteurs pour tous les accès à distance aux réseaux d'entreprise.

CB.9.5 Les organisations devraient utiliser uniquement un Wi-Fi sécurisé, de préférence un WPA2-Enterprise.

CB.9.6 Les organisations ne devraient jamais permettre à des réseaux Wi-Fi publics de se connecter à leurs réseaux.

CB.9.7 Les organisations devraient suivre les normes de sécurité sur les données de l'industrie des cartes de paiement (PCI DSS) pour tous les terminaux de point de vente et les systèmes financiers. Elles devraient également isoler ces systèmes de l'Internet.

CB.9.8 Les organisations doivent mettre en œuvre la spécification DMARC sur tous les services de courrier électronique de l'organisation.

3.10 INFONUAGIQUE SÉCURISÉE ET SERVICES DE TI EXTERNALISÉS

Les organisations comptent habituellement sur des fournisseurs de services de TI externes pour répondre à leurs besoins en matière de traitement ou de stockage dans un nuage, de gestion ou d'hébergement de leur site Web et de gestion des systèmes de paiement en ligne. Les organisations devraient savoir dans quelle mesure elles connaissent et suivent les règlements en vigueur dans les territoires juridiques où leurs fournisseurs externes stockent ou utilisent leurs renseignements de nature délicate.

Les organisations devraient exiger que tous leurs fournisseurs de service infonuagique présentent un rapport SSAE 16 SOC 3 [13] indiquant qu'ils sont conformes aux principes des services Trust. Si un fournisseur ne peut pas fournir cette certification, l'organisation devrait envisager d'avoir recours aux services d'un autre fournisseur.

Les organisations devraient chiffrer toutes les informations sensibles stockées à l'extérieur des bureaux de l'organisation pour ainsi assurer un accès sécurisé aux données stockées dans les nuages (p. ex. au moyen de connexions du navigateur Web sécurisées).

Les organisations devraient également tenir compte de tous les éléments suivants en ce qui concerne leurs fournisseurs externes de services TI et de services d'infonuagiques :

- les politiques sur le traitement des données et la protection des renseignements personnels;

- les processus de notification lorsque les données privées sont accessibles sans autorisation préalable;
- les processus de destruction des données à la fin du contrat d'impartition;
- l'emplacement physique des centres de données externes et leur sécurité;
- l'emplacement physique des administrateurs externes.

Conformément à la section 3.5, les organisations devraient exiger que tous les comptes d'administration dans le nuage mettent en œuvre un mécanisme d'authentification à deux facteurs. De plus, les organisations devraient veiller à ce que tous les comptes de service dans le nuage aient des mots de passe différents (ou autres facteurs d'authentification) que ceux utilisés au sein de l'infrastructure TI de l'organisation.

Résumé :

CB.10.1 Les organisations devraient exiger que tous leurs fournisseurs de service infonuagique produisent un rapport SSAE 16 SOC 3 [13] indiquant qu'ils sont conformes aux principes des services Trust.

CB.10.2 Les organisations devraient établir dans quelle mesure elles sont au fait de la façon dont leurs fournisseurs TI externes traitent leurs renseignements de nature délicate et y accèdent.

CB.10.3 Les organisations devraient établir dans quelle mesure elles connaissent les règles qui régissent les territoires juridiques où leurs fournisseurs externes stockent ou utilisent leurs renseignements de nature délicate.

CB.10.4 Les organisations doivent s'assurer que leur infrastructure TI et leurs utilisateurs communiquent de façon sécurisée avec les services et les applications infonuagiques.

CB.10.5 Les organisations doivent s'assurer que les comptes d'administration des services infonuagiques s'appuient sur un mécanisme d'authentification à deux facteurs qui est différent des comptes d'administration internes.

3.11 SITES WEB SÉCURISÉS

Les organisations doivent veiller à ce que le traitement des renseignements délicats sur leur site Web soit sécurisé en appliquant les directives *Application Security Verification Standard* (ASVS) du Open Web Application Security Project (OWASP) [14]. Les organisations devraient inclure le respect de la norme ASVS dans les exigences contractuelles concernant les sites Web confiés à des fournisseurs externes, ou envisager d'investir dans des solutions permettant de répondre à ces exigences en matière de sécurité TI pour les sites web qu'elles développent et exploitent en interne.

Résumé :

CB.11.1 Les organisations doivent s'assurer que leurs sites Web respectent les directives ASVS OWASP.

3.12 MISE EN ŒUVRE DES CONTRÔLES D'ACCÈS ET AUTORISATION

Les organisations doivent respecter le principe des autorisations minimales, c'est-à-dire l'octroi d'autorisations aux utilisateurs pour qu'ils aient les fonctionnalités minimalement requises à l'exécution de leurs tâches. Les comptes d'administration devraient faire l'objet d'autres restrictions – ces comptes devraient permettre seulement la prise de mesures administratives et non pas les activités d'utilisateur comme la navigation Web ou l'accès à la messagerie électronique. Pour veiller à une imputabilité claire concernant les activités des utilisateurs, les organisations devraient fournir à tous les utilisateurs des comptes individuels et réduire au minimum ou éliminer l'utilisation de comptes partagés ou à vocations multiples. Les organisations devraient avoir un processus en place pour révoquer des comptes lorsque ces derniers ne sont plus nécessaires, par exemple lorsque les employés quittent l'organisation.

Les grandes organisations devraient mettre en place des systèmes de contrôle d'autorisation centralisée comme Lightweight Directory Access Protocol ou Active Directory.

Résumé :

CB.12.1 Les organisations devraient fournir des comptes avec les fonctionnalités minimalement requises à l'exécution des tâches. Elles devraient particulièrement restreindre les privilèges d'administrateur en fonction de leurs besoins. Les

organisations devraient supprimer les comptes et la fonctionnalité lorsque les employés n'en ont plus besoin pour réaliser leurs tâches.

CB.12.2 Les organisations devraient autoriser l'utilisation de comptes d'administration uniquement pour réaliser des activités de nature administrative (et non pas des activités typiques d'utilisateur, comme l'accès aux courriels ou la navigation sur le Web).

CB.12.3 Les organisations devraient envisager la mise en œuvre d'un système de contrôle des autorisations centralisé.

3.13 SUPPORTS AMOVIBLES SÉCURISÉS

Les supports portatifs comme les disques durs amovibles, les lecteurs flash USB et les cartes Secure Digital sont un moyen pratique de transférer des dossiers entre les appareils. Toutefois, compte tenu de leur taille et de la portabilité, ils sont sujets à la perte ou au vol de données, ce qui pourrait causer une atteinte à la protection des données. Comme il serait impensable d'interdire toute utilisation de ces supports portatifs, nous recommandons tout de même aux organisations de n'utiliser que leurs propres lecteurs commerciaux et chiffrés.

Nous recommandons le maintien d'un contrôle serré des biens pour tous les dispositifs de stockage, y compris les appareils portatifs. Ce contrôle devrait inclure l'élimination appropriée de ces supports. Les organisations doivent veiller à utiliser les fonctions d'effacement des données dont sont munis certains dispositifs (p. ex. les appareils mobiles et les tablettes) avant de les éliminer. En ce qui a trait aux appareils dépourvus de cette fonctionnalité, les organisations doivent avoir recours à un fournisseur de services afin de les éliminer.

Résumé :

CB.13.1 Les organisations devraient prescrire l'utilisation exclusive de supports amovibles sécurisés dont elles sont les propriétaires, avoir de solides contrôles des biens visant ces appareils et exiger l'utilisation de méthodes de chiffrement sur tous ces appareils.

CB.13.2 Les organisations devraient avoir des processus pour nettoyer les dispositifs portatifs ou effacer les données de ces dispositifs avant que ceux-ci soient éliminés.

4 RÉSUMÉ

Les contrôles de base visent à conseiller les petites et moyennes organisations qui souhaitent maximiser l'efficacité de leurs investissements en matière de cybersécurité. Les organisations qui cherchent à appliquer des contrôles plus approfondis devraient se tourner vers des mesures de cybersécurité plus complètes, telles que les contrôles du *Center for Internet Security* [15], le cadre de cybersécurité du NIST [5], la norme ISO/IEC 27001:2013 [6] et les recommandations du document du CCC, *La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie* [4].

5 CONTENU COMPLÉMENTAIRE

5.1 LISTE DES ABRÉVIATIONS

Terme	Définition
ASVS	Normes de vérification de sécurité des applications (*Application Security Verification Standard*)
CCC	Centre canadien pour la cybersécurité
CEI	Commission électrotechnique internationale
DMARC	Authentification des messages fondée sur le domaine, rapports et conformité (*Domain-Based Message Authentication, Reporting and Conformance*)
DNS	Système d'adressage par domaines (*Domain Name System*)
GME	Gestion de la mobilité d'entreprise
ISO	Organisation internationale de normalisation (*International Organization for Standardization*)
NIST	National Institute of Standards and Technology (NIST) des États-Unis
OWASP	Open Web Application Security Project
PAP	Prenez votre appareil personnel
PCI DSS	Normes de sécurité sur les données de l'industrie des cartes de paiement
PDV	Point de vente
RPV	Réseau privé virtuel
RSSI	Responsable de la sécurité des systèmes d'information
SD	Carte Secure Digital
TI	Technologie de l'information
TLP	Protocole TLP (*Traffic Light Protocol*)
USB	Bus série universel (*Universal Serial Bus*)
VAP	Voici votre appareil personnel
Wi-Fi	Réseau local sans fil (*Wireless Local Area Network*)
WPA2	Protocole WPA 2 (*Wi-Fi Protected Access 2*).

5.2 GLOSSAIRE

Terme	Définition
Application de correctifs	Acte d'appliquer des mises à jour au matériel informatique et aux logiciels.
Authentification	Processus ou mesure permettant de vérifier l'identité d'un utilisateur.
Authentification à deux facteurs	Authentification qui utilise une combinaison de deux différents facteurs d'authentification — quelque chose qu'un utilisateur connaît (p. ex., un mot de passe), qu'il possède (p. ex. un jeton physique) ou quelque chose de physique (p. ex. biométrie) — afin de vérifier l'identité de l'utilisateur.
Chiffrement	Procédure par laquelle une information est convertie d'une forme à une autre afin d'en dissimuler le contenu et d'en interdire l'accès aux entités non autorisées.
Compromission des données	Incident de cybersécurité, dans lequel une personne prend des renseignements de nature délicate sans l'autorisation du propriétaire.
Confidentialité	Caractéristique de l'information sensible protégée contre tout accès non autorisé.
Coupe-feu	Barrière de sécurité placée entre deux réseaux qui contrôle le volume et les types de trafic autorisés à passer d'un réseau à l'autre.
Cybercriminalité	Crime perpétré au moyen d'ordinateurs ou de réseaux informatiques.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin.
Espionnage industriel	Espionnage qui cible la propriété intellectuelle ou l'information sensible des organisations.

Terme	Définition
Gestion de la mobilité d'entreprise	Les systèmes qui gèrent des dispositifs informatiques mobiles ou des services pour le compte d'une organisation.
Incident de cybersécurité	Toute tentative non autorisée de consultation, de modification, de suppression ou de destruction qui est entreprise à l'endroit d'une ressource informatique ou d'un réseau.
Intégrité	Capacité à protéger l'information contre une modification ou une suppression non autorisée.
Maliciels	Logiciel malveillant conçu pour infiltrer ou endommager un système informatique sans le consentement du propriétaire.
Préjudice	Les préjudices que les organisations subissent à la suite d'une compromission de leurs systèmes d'information et de leurs biens de TI.
Rançongiciel	Type de maliciel qui empêche un utilisateur légitime d'accéder à des ressources (système ou données), et ce, jusqu'à ce qu'il ait payé une rançon.
Renseignements sensibles	L'information qui doit être protégée contre toute divulgation non autorisée.
Risque résiduel	Le degré de probabilité d'une menace et les répercussions potentielles qui subsistent après la mise en œuvre de contrôles de sécurité.

5.3 RÉFÉRENCES

Numéro	Référence
1	FIRST. *Traffic Light Protocol Definitions and Usage*, disponible sur : https://www.first.org/tlp.
2	Sécurité publique Canada. Stratégie nationale de cybersécurité, disponible sur : https://www.pulbicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.
3	Centre canadien pour la cybersécurité. Évaluation des cybermenaces nationales de 2018, disponible sur : https://cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2018.
4	Centre de la sécurité des télécommunications. ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014, disponible sur https://www.cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33.
5	NIST. *Cybersecurity Framework*, disponible sur https://www.nist.gov/cyberframework.
6	ISO/IEC. *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information* — ISO/IEC 27001:2013, disponible sur : https://www.iso.org/standard/54534.html
7	Industrie Canada. *Recherche et statistique sur la PME*, disponible sur : https://ic.gc.ca/smeresearch.
8	Gartner. « Gartner Says Many Organizations Falsely Equate IT Security Spending With Maturity » (décembre 2016) disponible sur : https://www.gartner.com/en/newsroom/press-releases/2016-12-09-gartner-says-many-organizations-falsely-equate-it-security-spending-with-maturity.
9	Center for Internet Security (CIS). *CIS Benchmarks*, disponibles sur https://www.cisecurity.org/cis-benchmarks.
10	Centre de la sécurité des télécommunications. *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information*, ITSP.30.031 V3, disponible sur : https://www.cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3.
11	Industrie des cartes de paiement. *Normes de sécurité sur les données de l'industrie des cartes de paiement* (PCI DSS, de l'anglais *Payment Card Industry Data Security Standard*) disponible sur : https://www.pcisecuritystandards.org/security_standards/documents.php.
12	Global Cyber Alliance. *Domain-Based Message Authentication* (DMARC), disponible sur : https://www.globalcyberalliance.org/dmarc.
13	SSAE 16. « Statement on Standards for Attestation Engagement (SSAE) », numéro 16, disponible sur : http://ssae16.com.
14	Open Web Application Security Project. *Normes de vérification de sécurité des applications*, disponible sur : https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf.
15	Center for Internet Security. *CIS Controls*, disponible sur : https://www.cisecurity.org/controls.

Annexe A Résumé des contrôles de base

Numéro	Contrôle
CO. 1	Les organisations qui utilisent des contrôles de base doivent compter moins de 499 employés.
CO.2	Les organisations doivent déterminer les éléments de leurs biens et de leurs systèmes d'information qui s'inscrivent dans la portée des contrôles de base qu'elles souhaitent mettre en œuvre.
CO.3	Les organisations doivent évaluer le niveau de préjudice sur le plan de la confidentialité, de l'intégrité et de la disponibilité de leurs systèmes d'information et de leurs biens.
CO.4	Les organisations devraient cerner la principale menace qui les préoccupe en fonction de leurs circonstances particulières.
CO.5.1	Les organisations devraient nommer une personne qui occupe un poste de direction et qui serait précisément responsable de la sécurité des TI.
CO.5.2	Les organisations devraient déterminer le niveau de leurs dépenses en TI et d'investissement en sécurité des TI (chiffres bruts et pourcentages des dépenses totales).
CO.5.3	Les organisations devraient déterminer la portion de leur effectif qui travaille en TI et en sécurité des TI (chiffres bruts et pourcentage de l'effectif).
CB.1.1	Les organisations devraient avoir un plan d'intervention de base en cas d'incidents dont les niveaux de gravité varient de faible à très grave. Si une organisation n'est pas en mesure de gérer certains types d'incidents, elle devrait avoir un plan indiquant ce qu'elle fera.
CB.1.2	Les organisations devraient avoir un plan d'intervention officiel en cas d'incident qui précise les responsabilités relatives à la gestion des incidents; ce plan devrait comprendre les coordonnées des responsables concernés, de même que celles des parties externes, des intervenants et des organisations de réglementation. Les organisations devraient tenir à jour une copie papier de ce plan, au cas où une version numérique du plan ne serait pas accessible.
CB.1.3	Les organisations devraient envisager l'achat d'une police d'assurance en matière de cybersécurité qui comprend une couverture pour les activités liées à l'intervention en cas d'incident et pour assurer la reprise des activités.
CB.1.4	Les organisations devraient envisager la mise en œuvre d'une capacité de surveillance (p. ex., un système de gestion des informations et des événements de sécurité) ou consigner les informations expliquant leurs motifs de ne pas le faire.
CB.2.1	Les organisations devraient activer l'application automatique des correctifs pour tous les logiciels et tout le matériel OU mettre en place des solutions complètes de gestion des vulnérabilités et des correctifs.
CB.2.2	Les organisations devraient mener des activités d'évaluation des risques pour déterminer si elles doivent remplacer ou non le matériel et les logiciels qui ne permettent pas l'application automatique des mises à jour. Si l'organisation choisit de conserver de tels appareils, elle doit avoir un processus opérationnel pour faire manuellement les mises à jour de façon régulière.
CB.3.1	Les organisations devraient activer des solutions anti-logiciel malveillant qui font des mises à jour et des analyses automatiquement.
CB.4.1	Les organisations devraient utiliser des configurations de sécurisation sur tous leurs appareils en changeant tous les mots de passe par défaut, en désactivant les caractéristiques inutiles et en activant toutes les caractéristiques de sécurité pertinentes.
CB.5.1	Les organisations doivent mettre en œuvre une solution d'authentification à deux facteurs dans la mesure du possible et consigner tous les cas où elles prennent la décision de ne pas le faire. Les organisations devraient exiger une authentification à deux facteurs pour les comptes importants, tels que les comptes financiers, les administrateurs du système, les administrateurs du nuage, les utilisateurs privilégiés et les cadres supérieurs.
CB.5.2	Les organisations devraient uniquement obliger la modification d'un mot de passe lorsqu'il y a des soupçons ou des preuves de compromission.
CB.5.3	Les organisations devraient avoir des politiques claires sur la longueur des mots de passe, sur la réutilisation des mots de passe, sur l'utilisation de gestionnaires de mots de passe et sur les conditions auxquelles un utilisateur doit satisfaire pour consigner ou conserver son mot de passe en toute sécurité.
CB.6.1	Les organisations devraient investir dans la formation pour sensibiliser leurs employés à la cybersécurité.
CB.7.1	Les organisations devraient effectuer la sauvegarde de leurs systèmes qui contiennent des renseignements commerciaux essentiels, et s'assurer que des mécanismes de reprise puissent restaurer avec efficacité et efficience ces systèmes à partir des sauvegardes. Les organisations devraient envisager d'entreposer les sauvegardes à un endroit hors site sécurisé.
CB.7.2	Les organisations devraient entreposer de façon sécuritaire les sauvegardes après les avoir chiffrées, et elles devraient limiter l'accès à ces sauvegardes aux responsables des mises à l'essai ou des activités de restauration.
CB.8.1	Les organisations devraient opter pour un modèle de propriété des appareils mobiles et consigner les motifs expliquant leurs décisions de même que les risques connexes.

Numéro	Contrôle
CB.8.2	Les organisations devraient exiger qu'il y ait une séparation entre les données de nature professionnelle et les données personnelles sur les appareils mobiles qui accèdent aux ressources TI de l'organisation. Elles doivent également consigner les détails relatifs à cette séparation.
CB.8.3	Les organisations doivent veiller à ce que les employés téléchargent uniquement les applications pour appareils mobiles de la liste de sources dignes de confiance fournie par l'organisation.
CB.8.4	Les organisations devraient exiger que tous les appareils mobiles stockent tous les renseignements de nature délicate de façon sécurisée, après les avoir chiffrés.
CB.8.5	Les organisations devraient mettre en œuvre une solution de gestion de la mobilité d'entreprise pour tous les appareils mobiles OU consigner les risques qu'elles assument en choisissant de ne pas mettre en œuvre une telle solution, notamment sur le plan de la vérification, de la gestion et de la fonctionnalité de sécurité des appareils mobiles.
CB.8.6	Les organisations devraient appliquer ou éduquer les utilisateurs à : (1) désactiver les connexions automatiques aux réseaux ouverts, 2) éviter la connexion aux réseaux Wi-Fi inconnus, (3) limiter l'utilisation de Bluetooth et de dispositifs de communication en champ proche pour la transmission de renseignements de nature délicate et (4) utiliser le Wi-Fi de l'organisation ou du réseau de données cellulaire plutôt qu'un réseau Wi-Fi public.
CB.9.1	Les organisations devraient mettre en œuvre des coupe-feux spécialisés à la frontière des réseaux d'entreprise et de l'Internet.
CB.9.2	Les organisations devraient mettre en place un coupe-feu DNS pour les demandes DNS sortantes vers l'Internet.
CB.9.3	Les organisations devraient activer tout logiciel coupe-feu intégré dans les appareils sur leurs réseaux ou elles devraient consigner les mesures de rechange qui remplacent ces coupe-feux.
CB.9.4	Les organisations doivent exiger une connexion sécurisée à toutes les ressources TI d'entreprise, et exiger la connexion à un RPV avec une authentification à deux facteurs pour tous les accès à distance aux réseaux d'entreprise.
CB.9.5	Les organisations devraient utiliser uniquement un Wi-Fi sécurisé, de préférence un WPA2-Enterprise.
CB.9.6	Les organisations ne devraient jamais permettre à des réseaux Wi-Fi publics de se connecter à leurs réseaux.
CB.9.7	Les organisations devraient suivre les normes de sécurité sur les données de l'industrie des cartes de paiement (PCI DSS) pour tous les terminaux de point de vente et les systèmes financiers. Elles devraient également isoler ces systèmes de l'Internet.
CB.9.8	Les organisations devraient mettre en œuvre la DMARC sur tous les services de courrier électronique de l'organisation.
CB.10.1	Les organisations devraient exiger que tous leurs fournisseurs de service infonuagique leur présentent un rapport SSAE 16 SOC 3 indiquant qu'ils sont conformes aux principes des services Trust.
CB.10.2	Les organisations devraient évaluer leur niveau de confort par rapport à la façon dont leurs fournisseurs TI externes traitent leurs renseignements de nature délicate et y accèdent.
CB.10.3	Les organisations devraient évaluer leur niveau de confort par rapport aux territoires juridiques où leurs fournisseurs externes stockent ou utiliser leurs renseignements de nature délicate.
CB.10.4	Les organisations devraient s'assurer que leur infrastructure TI et les utilisateurs communiquent de façon sécurisée avec tous les services et les applications dans le nuage.
CB.10.5	Les organisations devraient s'assurer que les comptes d'administration des services infonuagiques s'appuient sur un mécanisme d'authentification à deux facteurs qui est différent des comptes d'administration internes.
CB.11.1	Les organisations devraient s'assurer que leurs sites Web respectent les lignes directrices OWASP ASVS.
CB.12.1	Les organisations devraient fournir des comptes avec les fonctionnalités minimalement requises pour réaliser les tâches. Elles devraient particulièrement restreindre les privilèges d'administrateur en fonction des besoins. Les organisations devraient supprimer les comptes et les fonctionnalités lorsque les employés n'en ont plus besoin pour réaliser leurs tâches.
CB.12.2	Les organisations devraient uniquement permettre que les comptes d'administration servent à exécuter des activités de nature administrative (et non pas des activités typiques d'utilisateur, comme l'accès aux courriels ou la navigation sur le Web).
CB.12.3	Les organisations devraient envisager la mise en œuvre d'un système de contrôle des autorisations centralisé.
CB.13.1	Les organisations devraient prescrire l'utilisation exclusive dispositifs portatifs sécurisés dont elles sont les propriétaires, avoir de solides contrôles des biens visant ces appareils, et exiger l'utilisation de méthodes de chiffrement sur tous ces appareils.
CB.13.2	Les organisations devraient avoir des processus pour nettoyer les dispositifs portatifs et pour supprimer les données sur ces dispositifs avant de les éliminer.