Choose a Centre de la sécurité des télécommunications Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

L'organisation bénévole et l'accès sécurisé

SÉRIE GESTIONNAIRES

TLP:WHITE

Canada

AVANT-PROPOS

La présente publication est un document non classifié publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, envoyez un courriel ou téléphonez à notre centre d'appel :

Centre d'appel

cyber.gc.ca

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 14 janvier 2022.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Première diffusion.	14 janvier 2022

ISBN 978-0-660-41546-8
CAT D97-4/30-010-2022F-PDF

VUE D'ENSEMBLE

Le présent document décrit les risques courants auxquels font face les organisations bénévoles et il recommande des mesures pour s'attaquer à ces risques en adaptant la manière de gérer les gens, les processus, l'information et les technologies. Le document s'adresse aux propriétaires et aux gestionnaires de programmes de sécurité, ainsi qu'aux praticiens de la cybersécurité.

L'accent sera mis dans cette publication sur les organisations qui font appel à un nombre élevé de bénévoles. Ces organisations peuvent comprendre des musées, des partis politiques et des organismes électoraux, ou toutes autres organisations qui comptent fortement sur des bénévoles. Cela représente des défis supplémentaires. Parmi ceux-ci, notons un taux de roulement excessif des bénévoles ou encore des bénévoles disposant d'accès privilégiés.

Si votre organisation repose sur une main-d'œuvre bénévole (en totalité ou en partie), vous pourriez être aux prises à des défis en matière de cybersécurité. Ces défis peuvent survenir si l'environnement dans lequel vous évoluez implique un roulement fréquent de personnel, des processus accélérés avec filtrage réduit des candidats, et des budgets limités pour trouver des solutions et avoir recours à des experts. Si la situation n'est pas corrigée, ces facteurs peuvent entraîner des risques qui pourraient rendre vos réseaux, vos systèmes et vos renseignements vulnérables aux cybermenaces.

TABLE DES MATIÈRES

1 Introduction 5

2 Gestion des gens et des comptes 6

2.1 Filtrage et vérification de la fiabilité 6

2.2 Formation en cybersécurité 7

2.3 Considérations légales 8

2.4 Menace interne 8

2.5 Gestion du cycle de vie des comptes 9

2.6 Authentification 10

2.7 Octroi et révocation d'un accès 11

3 Gestion des processus 12

3.1 Accueil et intégration des nouveaux bénévoles 12

3.2 Annulation de l'intégration 13

4 Gestion de la technologie 14

4.1 Équipements partagés 15

4.2 Prenez vos appareils personnels (PAP) 16

4.3 Surveillance 17

5 Gestion de l'information 18

5.1 Traitement de l'information 18

6 Contenu complémentaire 19

6.1 Liste des abréviations 19

6.2 Glossaire 19

6.3 Références 21

1 INTRODUCTION

Le présent document explique certains des facteurs qui augmentent les risques liés à la cybersécurité et auxquels les organisations bénévoles sont exposées. Pour vous permettre de réduire ces risques, nous proposons certaines mesures que votre organisation peut prendre pour gérer en toute sécurité les personnes, les comptes, les processus, les technologies et les renseignements.

En tant qu'organisation bénévole, vous êtes peut-être exposée à certains défis qui augmentent les risques liés à la cybersécurité. Voici les facteurs les plus couramment constatés :

- Vous avez un **budget des TI limité** : Compte tenu des contraintes d'un budget limité, il n'est pas raisonnable de s'attendre à ce que tous les risques soient atténués. Votre organisation devrait être dotée d'un registre des risques (p. ex. un outil de gestion des risques) pour établir l'ordre de priorité des risques. Suivez la règle du 80/20 pour réduire 80 % des risques en traitant 20 % des vulnérabilités connues.
- Vous pourriez éprouver des difficultés en ce qui a trait à la **gestion du cycle de vie des comptes** : Votre organisation doit passer en revue et confirmer que tous les comptes d'utilisateur actifs sont vraiment nécessaires et qu'ils sont associés à des bénévoles qui ont actuellement besoin d'y accéder. L'accès aux comptes doit être révoqué lorsqu'un bénévole ne travaille plus pour votre organisation.
- Vous devez **rapidement vous adapter à une augmentation ou à une diminution de la demande** dans votre équipe : Vous dépendez dans une large mesure de vos bénévoles, mais vous devez avoir la flexibilité d'accélérer ou de ralentir rapidement vos activités en fonction de votre effectif. Dans le contexte de la cybersécurité, cela peut signifier qu'il vous faut rapidement activer et désactiver les comptes, ce qui peut entraîner des risques causer par un provisionnement, une erreur humaine et une mauvaise gestion du cycle de vie des comptes.
- Vous pourriez présenter un risque plus élevé de **menaces internes** : Des taux de roulement de personnel élevés, et des processus de filtrage écourtés ou contournés peuvent accroître le risque de menaces internes étant donné qu'il peut s'avérer plus difficile de cerner les bénévoles ayant une intention malveillante. Si votre organisation traite de l'information très sensible, il pourrait s'avérer nécessaire de privilégier un processus de filtrage plus exhaustif (p. ex. une vérification des antécédents par la police).
- Vous permettez aux bénévoles de **travailler avec des dispositifs personnels ou des équipements partagés** : Il n'est peut-être pas rentable pour votre organisation de donner aux bénévoles des dispositifs appartenant à l'organisation ou de mettre l'équipement à la disposition de tous. Les utilisateurs peuvent partager des équipements ou utiliser des dispositifs personnels; toutefois, ces options peuvent présenter des risques additionnels, et votre organisation doit tenir compte de ceux-ci et les évaluer.

2 GESTION DES GENS ET DES COMPTES

Il existe toujours un certain niveau de risque lorsque vous accordez à quelqu'un (p. ex. un employé ou un bénévole) l'accès à vos réseaux, à vos systèmes et à vos renseignements, quelle que soit l'étendue du filtrage effectué. Lorsque vous disposez de ressources limitées (p. ex. en temps et en budget), vous aurez peut-être à accepter des risques additionnels pour prendre en compte votre effectif en constante évolution. Cette section aborde les pratiques exemplaires que votre organisation peut mettre en œuvre pour réduire les risques associés aux comptes d'utilisateur et à leur accès.

2.1 FILTRAGE ET VÉRIFICATION DE LA FIABILITÉ

Adaptez vos processus de filtrage des candidats en fonction du niveau d'accès requis pour chaque utilisateur. Par exemple, vous devriez effectuer un filtrage plus approfondi et rigoureux pour un utilisateur qui a accès à de l'information sensible ou qui a un accès privilégié aux systèmes. Différentes techniques de filtrage offrent différents niveaux d'assurance de la sécurité, et leurs coûts varient (tant sur le plan monétaire que sur le plan du temps d'exécution).

Le processus de filtrage de vos candidats peut comprendre les aspects suivants :

1. Une **vérification du curriculum vitæ** peut vous aider à identifier les écarts d'emplois ou les questions relatives à l'emploi (p. ex. un licenciement) qui pourraient entraîner des risques.
2. Une **vérification des antécédents criminels** peut se faire rapidement et être traitée par un partenaire externe. La vérification des antécédents criminels permet de recueillir de précieux renseignements à un coût minime.
3. La **vérification des références** est une étape que l'on retrouve souvent dans les processus de sélection des candidats et qui peut vous aider à recueillir des commentaires d'anciens gestionnaires ou collègues du candidat. Faites preuve de prudence au moment de valider les références, car les candidats ne donnent habituellement pas de références qui pourraient formuler des commentaires négatifs à leur endroit.
4. Il est possible d'effectuer une **entrevue de cybersécurité** pour savoir jusqu'à quel point le candidat est à l'aise avec les pratiques exemplaires en matière de cybersécurité. Cette étape peut s'avérer utile si le candidat doit recevoir un accès privilégié.
5. Une **entrevue de sécurité ou de fiabilité** réalisée par un officier de sécurité permet de mieux comprendre les risques liés à un candidat. Ces entrevues peuvent se révéler longues et coûteuses. Une telle entrevue est habituellement nécessaire pour une collaboration avec une organisation du secteur public.

2.2 FORMATION EN CYBERSÉCURITÉ

Tous les bénévoles doivent recevoir une formation, indépendamment de la durée de leur collaboration au sein de votre organisation. Une formation favorise la sensibilisation à la sécurité et permet de réduire les risques associés au comportement de l'utilisateur. Votre organisation devrait intégrer les pratiques suivantes dans le cadre de son programme de formation en cybersécurité :

- Donnez une formation obligatoire en faisant l'accueil et l'intégration des nouveaux bénévoles, et lorsque des modifications sont apportées à vos politiques et procédures :
  - Abordez les menaces courantes auxquelles fait face votre organisation, les politiques et les processus liés à la cybersécurité, le comportement auquel il faut s'attendre de l'utilisateur et les processus d'intervention en cas d'incident;
  - Intégrez des exercices qui aident les utilisateurs à identifier les menaces courantes comme les attaques par hameçonnage et par piratage psychologique. Consultez l'*ITSAP.00.101 – Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage* [1] pour obtenir de plus amples renseignements;
  - Informez vos bénévoles de la politique de l'organisation en matière de mots de passe et donnez-leur des conseils sur la création de phrases passe ou de mots de passe complexes. Consultez l'*ITSAP.30.032 – Pratiques exemplaires de création de phrases de passe et de mots de passe* [2] pour obtenir de plus amples renseignements;
- Offrez périodiquement des cours de perfectionnement (p. ex. une fois par année) pour que les bénévoles demeurent au courant de vos pratiques actuelles de sécurité;
- Adaptez votre formation de façon à aborder le contexte de menace et les stratégies d'atténuation de votre organisation.
  - Précisez les menaces qui sont spécifiques à votre organisation pour aider les bénévoles à comprendre pourquoi certains contrôles ont été mis en place. Consultez l'*ITSM.10.093, Les 10 mesures de sécurité des TI : Nº 6, Miser sur une formation sur mesure en matière de cybersécurité* [3] pour obtenir de plus amples renseignements.

2.3 CONSIDÉRATIONS LÉGALES

Avant de donner l'accès aux systèmes de votre organisation, tous les bénévoles doivent recevoir, lire et reconnaître leur assentiment aux politiques standards de l'organisation (p. ex. le code de conduite). Votre organisation devrait également mettre en œuvre une politique d'utilisation acceptable en matière de gestion de l'information (GI) et de TI qui explique comment se fait la surveillance des dispositifs et l'usage approprié des biens et des renseignements de l'organisation.

Tous les bénévoles doivent recevoir un accord qu'ils doivent signer pour en accuser réception au moment de l'embauche. Cet accord doit préciser la façon de traiter les renseignements de l'organisation et les conséquences de la communication non autorisée de ces renseignements.

Votre organisation doit également évaluer le coût et les avantages de se prévaloir d'une assurance cybersécurité pour protéger les systèmes et les renseignements. Il est important de comprendre les politiques qui sous-tendent votre assurance cybersécurité en tenant compte des attaques possibles qui pourraient ne pas être couvertes en vertu des conditions (p. ex. une menace parrainée par un État).

2.4 MENACE INTERNE

On entend par menace interne toute personne qui connaît l'infrastructure ou l'information de votre organisation, ou qui y a accès, et qui utilise ses connaissances ou son accès d'une façon malveillante ou involontaire pour nuire à l'organisation. Les menaces internes peuvent poser des risques contre vos bénévoles, vos clients, vos actifs, votre réputation et vos intérêts.

Une personne pourrait involontairement faire du tort à l'organisation en agissant de la façon suivante :

- Perdre un dispositif mobile ou un support amovible;
- Donner l'accès à d'autres personnes à de l'information sensible;
- Gérer de façon inadéquate de l'information sensible

Une personne ayant une intention malveillante pourrait mettre à exécution les actions suivantes :

- Exproprier de l'information et de la documentation;
- Modifier ou supprimer du contenu;
- Modifier des comptes pour en accorder l'accès à des utilisateurs non vérifiés;
- Modifier la sensibilité d'un document pour le rendre accessible à plus de gens;
- Mener une attaque par rançongiciel en chiffrant des documents et en demandant le versement d'un paiement en échange des documents déchiffrés.

Des entrevues, des autorisations de sécurité, des contrôles des antécédents et des vérifications de références sont des étapes qui aident à confirmer la loyauté des bénévoles. Lorsque vous devez accélérer le processus d'embauche, il est possible que vous n'ayez pas le temps de passer par des processus d'examen approfondi. Votre organisation aura peut-être à accepter les risques associés à une vérification partielle ou les conséquences de ne faire aucune vérification. Pour obtenir de plus amples renseignements sur les menaces internes, consultez l'*ITSAP.10.003 – Comment protéger votre organisation contre les menaces internes* [6].

2.5 GESTION DU CYCLE DE VIE DES COMPTES

Votre organisation pourrait avoir besoin de bénévoles à court terme et à long terme. Les embauches à court terme peuvent constituer un défi; la surcharge des TI augmente, les risques de mauvaise gestion d'un compte sont plus élevés, et les processus d'examen, d'accueil et d'intégration des nouveaux bénévoles doivent être simplifiés.

Vos processus d'intégration et d'annulation de l'intégration doivent comprendre les mesures de sécurité suivantes :

- Mettez en pratique le principe du droit d'accès minimal pour vous assurer que les utilisateurs ne disposent que des accès aux systèmes et à l'information dont ils ont besoin dans le cadre de leurs fonctions;
- Désactivez les comptes lorsqu'ils ne sont plus nécessaires;
- Mettez en œuvre et imposez une politique en matière de mots de passe robustes;
  - Consultez l'*ITSAP.30.032* [2] pour avoir plus de renseignements;
- Utilisez, lors de la création de nouveaux comptes, des modèles de création de comptes dans lesquels sont appliquées les bonnes politiques de sécurité;
  - Établissez des dates d'expiration pour les comptes en fonction de la fréquence des examens d'accès;
  - Envisagez le recours à l'automatisation pour faciliter la gestion de la création de comptes groupés;
- Établissez des dates d'expiration pour désactiver des comptes en fonction des horaires des bénévoles;
- Limitez les heures de connexion aux comptes des utilisateurs en fonction des horaires des bénévoles;
- Passez les comptes en revue de façon périodique et obtenez l'approbation du gestionnaire (p. ex. le gestionnaire responsable confirme la validité des comptes et il indique les comptes à modifier ou à désactiver;
- Choisissez un fournisseur situé au Canada pour la gestion infonuagique des comptes et familiarisez-vous avec leurs politiques d'accès conditionnel.

2.6 AUTHENTIFICATION

Afin de sécuriser les comptes et les dispositifs, il est important d'utiliser des méthodes d'authentification pour assurer la sécurité de l'information sensible. La mise en œuvre des pratiques exemplaires suivantes aidera à atténuer les risques associés aux mots de passe.

- Établissez une politique en matière de mots de passe qui comporte les aspects suivants :
  - Les mots de passe doivent avoir au moins 12 caractères;
  - L'utilisation de phrases passe d'au moins 15 caractères est à privilégier;
  - Un mot de passe doit appliquer un niveau minimum de complexité (p. ex. des caractères spéciaux, des chiffres et des lettres);
- Utilisez des comptes partagés **seulement si** aucune autre option n'est disponible;
- Permettez l'authentification multifacteur pour tous les comptes (p. ex. les comptes d'utilisateur général, les comptes administratifs et les comptes à accès privilégié) pour ajouter des mesures de sécurité supplémentaires, le cas échéant;
- Mettez en place une politique de blocage de compte.
  - Bloquez les comptes après 3 à 5 tentatives.
  - Permettez uniquement à l'administration la possibilité de débloquer les comptes.

Consultez les documents *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031)* [4] et *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031* v3) [5] pour obtenir de plus amples renseignements.

2.7 OCTROI ET RÉVOCATION D'UN ACCÈS

Sécuriser l'accès à l'information est important pour garder en toute sécurité les données sensibles de votre organisation. Si plusieurs utilisateurs partagent des rôles similaires et ont besoin des mêmes accès, il peut s'avérer plus facile de gérer ces accès en faisant ce qui suit :

- Créez des groupes en fonction des besoins de sécurité et des exigences d'accès de votre organisation;
  - Les utilisateurs avec un accès limité et un accès en lecture seule;
  - Les utilisateurs avec des exigences prévues pour un accès supplémentaire (p. ex. modifier, déplacer);
  - Le personnel des TI avec des exigences incluant le soutien à l'effectif de l'organisation;
  - Les utilisateurs ayant un accès spécial avec des exigences permettant l'accès à des documents pour public limité;
- Optimisez les structures de dossiers qui correspondent aux besoins de sécurité de divers groupes d'utilisateurs en fonction du niveau d'accès requis;
- Accordez un accès aux groupes requis (plutôt que de le faire individuellement) lors de la configuration d'un accès;
- Ajoutez des utilisateurs à des groupes qui correspondent au rôle de chaque personne et à chaque niveau d'accès lors de l'intégration du personnel;
- Retirez les comptes des groupes lors de l'annulation de l'intégration pour révoquer tous les accès;
- Restreignez aux utilisateurs de comptes privilégiés la capacité d'afficher les membres, et d'ajouter et de retirer des utilisateurs de groupes;
- Réservez la possibilité de changer les autorisations d'accès aux groupes à un petit groupe d'administrateurs;
- Utilisez un courtier de sécurité d'accès au nuage (CASB pour *Cloud Access Security Broker*) pour faire la prévention des pertes de données et la gestion de l'information (GI) pour assurer l'intégrité des données.

3 GESTION DES PROCESSUS

La présente section recommande des pratiques exemplaires pour l'atténuation des risques associés à vos processus d'intégration et d'annulation de l'intégration. Votre organisation doit bénéficier de suffisamment de souplesse pour être en mesure d'offrir rapidement et efficacement les ressources nécessaires aux bénévoles. Toutefois, cette transition rapide peut entraîner des erreurs humaines, des erreurs typographiques, des étapes oubliées ou des erreurs liées au contrôle d'accès. Voici quelques recommandations pour aider à atténuer les risques associés aux processus.

3.1 ACCUEIL ET INTÉGRATION DES NOUVEAUX BÉNÉVOLES

Le processus d'accueil et d'intégration des nouveaux bénévoles peut s'avérer très long. Les organisations bénévoles se doivent de simplifier ce processus. Votre processus d'accueil et d'intégration devrait idéalement permettre la création par lots de comptes lorsque vous devez embaucher un nombre élevé de bénévoles sur une courte période. Pour réduire le plus possible le risque, tout en respectant cette exigence, tenez compte des mesures suivantes :

- Utilisez des outils automatisés ou la rédaction de scripts pour accélérer les tâches répétitives;
- Utilisez des modèles ayant des politiques et des paramètres de sécurité testés pour répondre aux exigences en matière de sécurité des nouveaux comptes;
  - Les modifications (ou les tentatives de modification) de ce modèle doivent être limitées et documentées pour réduire tout accès inutile aux nouveaux utilisateurs;
- Transmettez en toute sécurité les mots de passe par défaut aux utilisateurs (p. ex. en communiquant en personne, au téléphone ou par messagerie protégée) et demandez que le mot de passe soit changé à la première connexion;
- Formez les nouveaux bénévoles aussitôt que possible (p. ex. en classe, par une formation en ligne ou à l'aide de documents écrits).
  - Le recours à une formation en ligne avec exercice de contrôle permet de s'assurer que les éléments clés de la formation ont été retenus.

3.2 ANNULATION DE L'INTÉGRATION

L'annulation de l'intégration est un processus complexe. Vous devez tenir compte de plusieurs aspects de ce processus, comme l'authentification décentralisée, des sessions considérées authentifiées avec des jetons non expirés, des comptes sur place (p. ex. Active Directory [AD]), des comptes dans le nuage (p. ex. Office 365, Azure AD), des comptes fédérés (p. ex. AD Federation Services [ADFS]) et des comptes de tiers (p. ex. le logiciel comme service [SaaS] avec authentification distincte).

Un bon processus d'annulation de l'intégration doit minimiser le risque d'erreur humaine et permettre que l'accès puisse être entièrement révoqué si une étape n'a pas été effectuée correctement.

Un processus d'annulation de l'intégration recommandé doit inclure les éléments suivants :

- Des processus automatisés, dans la mesure du possible;
- La désactivation des comptes;
- La révocation des certificats et des jetons des comptes;
- La révocation des jetons d'authentification des services infonuagiques;
- La désactivation de l'accès aux dispositifs qui ont accès aux capacités du mode de fonctionnement « prenez vos appareils personnels (PAP) »;
- La suppression des données de l'organisation se trouvant dans les dispositifs PAP.

4 GESTION DE LA TECHNOLOGIE

Cette section recommande les pratiques exemplaires que vous pouvez appliquer pour atténuer les risques associés à votre technologie. L'utilisation de dispositifs appartenant à l'organisation vous permet d'avoir plus de contrôle sur la sécurité de l'équipement et des dispositifs. Bien qu'il soit préférable de fournir à toutes les personnes de l'organisation des dispositifs qui lui appartiennent, il n'est pas toujours possible de le faire. Offrir des équipements partagés ou des capacités PAP, et travailler au moyen de services infonuagiques seraient plus facile à gérer, mais vous devez vous assurer de prendre les mesures nécessaires pour atténuer les risques associés à ces options. Il est possible d'offrir des capacités PAP à certains utilisateurs ou groupes spécifiques sans avoir à les donner à l'ensemble des utilisateurs.

Au moment de déployer des appareils mobiles et des équipements dans votre organisation, vous devriez tenir compte de différents modèles de déploiement. Avec cette technologie, la gestion des risques dépend en partie de la collaboration du bénévole (c.-à-d. sa volonté de permettre à l'organisation d'établir des restrictions d'utilisation ainsi que des modalités de surveillance et d'accès de sécurité) et en partie des risques et des vulnérabilités liés aux types de dispositifs offerts. Afin de choisir un modèle de déploiement qui équilibre le mieux ces éléments pour votre organisation, considérez l'expérience utilisateur, la confidentialité et les exigences de sécurité. Pour obtenir de plus amples renseignements, consultez l'*ITSAP.70.002, Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles* [7].

Utilisez la gestion des appareils mobiles (MDM pour *mobile device managemen*t) par le biais d'un fournisseur de confiance pour gérer l'administration et la surveillance des dispositifs. Cette gestion est utilisée pour mettre en œuvre une liste de vérification des mesures de sécurité automatiques parmi lesquelles peuvent se trouver des processus d'intégration et d'annulation de l'intégration relatifs à tous les équipements des bénévoles.

4.1 ÉQUIPEMENTS PARTAGÉS

Le partage des équipements peut s'avérer pratique et il peut aider à réduire les coûts, mais cette façon de faire entraîne un risque additionnel. Lorsqu'un utilisateur clique sur un courriel malveillant et infecte l'ordinateur, cela peut avoir des répercussions sur tous les utilisateurs qui partagent cet ordinateur. Certaines solutions de stockage dans le nuage vont, par exemple, donner accès à des fichiers hors ligne en copiant ces fichiers sur le disque dur local. Si plusieurs utilisateurs se servent du même ordinateur et ont également des copies hors ligne de leurs fichiers, les fichiers de chaque utilisateur risqueraient d'être infectés.

Si les bénévoles partagent des dispositifs, les mesures de sécurité supplémentaires suivantes doivent être appliquées aux dispositifs :

- Installez et mettez régulièrement à jour le logiciel antivirus et l'antimaliciel;
- Désactivez les droits administratifs des comptes et des dispositifs des utilisateurs s'ils ne sont pas nécessaires;
- Permettez l'accès à des comptes distincts par le biais de dispositifs partagés;
- Surveillez et limitez la navigation Internet si cette utilisation est nécessaire, et si elle ne l'est pas, bloquez la navigation;
- Dans la mesure du possible, utilisez l'infrastructure de bureau virtuel (VDI pour *virtual desktop infrastructure*) pour atténuer les risques associés aux bénévoles qui utilisent des ordinateurs de bureau.
    - Consultez l'*ITSAP.70.111 – Utiliser un poste de travail virtuel à la maison et au bureau* [8] pour obtenir plus de détails sur l'infrastructure de bureau virtuel.

4.2 PRENEZ VOS APPAREILS PERSONNELS (PAP)

Fournir des capacités PAP peut être extrêmement avantageux pour une organisation. Le fait de ne pas avoir à fournir et à faire l'entretien de dispositifs réduit les coûts. De telles capacités permettent aux utilisateurs de se servir d'ordinateurs, de tablettes ou de dispositifs mobiles qui leur appartiennent pour accéder aux données de l'organisation. Votre organisation peut mettre en œuvre des politiques pour protéger la plus grande quantité possible de vos données qui se trouvent sur des dispositifs personnels, mais les dispositifs en soi doivent être gérés par leurs propriétaires.

La commodité et les économies de coûts associées à de telles capacités peuvent l'emporter sur les risques. Cela peut placer les services des TI dans une situation qui n'est pas de savoir « si » la mise en œuvre des capacités doit se faire, mais plutôt « comment » la faire de manière sécuritaire.

Lorsque vous envisagez l'option PAP, tenez compte des mesures de sécurité suivantes :

- **Politique de protection des applications**
  - Empêchez que des applications non protégées par une politique de protection des applications puissent accéder aux contacts de l'organisation;
  - N'autorisez que l'installation d'applications provenant de sources de confiance;
  - Isolez les dispositifs PAP sur un différent réseau ou sous-réseau s'ils doivent être connectés au réseau d'affaires. Optimiser les coupe-feux de façon à filtrer les connexions qui sont permises vers et depuis le réseau PAP permettra de réduire le risque associé aux dispositifs personnels connectés à un réseau d'affaires.
- **Processus d'annulation**
  - Intégrez toutes les étapes nécessaires à la déconnexion des dispositifs PAP, révoquez les jetons d'authentification, et supprimez les données de l'organisation de dispositifs dans le cadre de l'annulation de l'intégration.
- **Contrôles de journalisation et de vérification**
  - Journalisez toutes les actions effectuées par les dispositifs PAP;
  - Utilisez un CASB pour enregistrer et surveiller les dispositifs.
- **Conformité des dispositifs**
  - Mettez en place une politique d'accès conditionnel, avant d'accorder un accès, pour vous assurer que les dispositifs personnels ne sont pas compromis;
  - Assurez-vous que les dispositifs sont connectés avec des comptes d'utilisateur et des certificats émis;
  - Vérifiez que le dispositif n'a pas été débridé (iOS), n'a pas été associé à une racine (Android) ou n'a pas été compromis;
  - Configurez une politique de protection des applications pour les dispositifs PAP afin d'appliquer des exigences de sécurité supplémentaires avant de pouvoir accéder aux données de l'organisation (p. ex. un NIP, un mot de passe, une marque biométrique);
  - N'autorisez l'accès qu'aux dispositifs qui répondent aux exigences de conformité (p. ex. un dispositif non associé à une racine ni débridé, un dispositif exécutant une version récente du système d'exploitation, un fabricant de dispositifs approuvés).

4.3 SURVEILLANCE

La surveillance et la journalisation sont nécessaires pour signaler des incidents et intervenir efficacement. La journalisation des éléments suivants est essentielle et doit être conservée, dans la mesure du possible, au moins 90 jours :

- Les connexions de l'utilisateur (p. ex. réussite ou échec);
- Les modifications de l'utilisateur (p. ex. créer, supprimer, désactiver, changer un mot de passe);
- Les documents consultés et interventions (p. ex. création, copie, déplacement, téléchargement, suppression);
- Les modifications des groupes de sécurité (p. ex. les utilisateurs ajoutés et supprimés);
  - L'ajout d'un utilisateur à un groupe et l'ajout d'un groupe à un groupe peuvent être consignés différemment (p. ex. un identifiant d'événement différent);
- Les connexions et les déconnexions à des accès privilégiés;
  - Tous changements appliqués pendant une session privilégiée;
- Les sauvegardes effectuées (p. ex. les erreurs signalées).

Les journaux de votre organisation doivent afficher des marques précises d'horodatage et les utilisateurs. Les journaux doivent également être surveillés. Si possible, utilisez un système de gestion des informations et des événements de sécurité (GIES) ou faites appel au Centre des opérations de sécurité (COS) pour surveiller les journaux et les événements 24 heures sur 24.

5 GESTION DE L'INFORMATION

5.1 TRAITEMENT DE L'INFORMATION

Afin d'assurer la sécurité des données de votre organisation lorsque celles-ci sont traitées par des bénévoles et des technologies, tous les documents doivent indiquer le niveau de sensibilité qui leur est associé. Vous devriez exiger et imposer le marquage de renseignements. Pour faciliter ce processus, élaborez des lignes directrices simples et claires pour veiller à ce que tous les bénévoles sachent comment noter adéquatement l'information.

Un exemple de modèle de diffusion est le protocole TLP, qui est un modèle créé par le National Infrastructure Security Coordination Centre du gouvernement du Royaume-Uni. Vous pouvez utiliser ce modèle pour identifier l'information sensible et la marquer avec des désignations garantissant que cette information est échangée adéquatement lorsque le partage est nécessaire. Le protocole TLP comporte quatre désignations :

- **White** : La diffusion n'est pas restreinte, et l'information peut être communiquée à quiconque;
- **Green** : La diffusion reste à l'intérieur de l'organisation;
- **Amber** : La diffusion reste à l'intérieur de l'organisation et n'est autorisée qu'en fonction du besoin de savoir;
- **Red** : La diffusion est limitée aux participants aux réunions et aux participants aux réunions.

Pour obtenir plus de renseignements sur le protocole TLP, consultez le document *Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance* [9].

Une fois l'information marquée, la technologie peut être mise à profit pour s'assurer que l'information ne franchit pas certaines limites établies par l'organisation. Des pare-feu, une technologie de prévention des pertes de données, un courtier de sécurité d'accès au nuage, ainsi que d'autres technologies peuvent servir à empêcher une mauvaise gestion de l'information (accidentelle ou intentionnelle). Le fait de marquer l'information contribue à rendre la solution technologique plus efficace.

6 CONTENU COMPLÉMENTAIRE

6.1 LISTE DES ABRÉVIATIONS

Terme	Définition
AD	Système d'exploitation Active Directory
ADFS	Services de fédération Active Directory (Active Directory Federation Services)
PAP	Prenez votre appareil personnel
CASB	Courtier de sécurité d'accès au nuage (Cloud Access Security Broker)
iOS	Systèmes d'exploitation pour l'iPhone (iPhone Operating System)
TI	Technologies de l'information
MFA	Authentification multifacteur (Multi-Factor Authentication)
NIP	Numéro d'identification personnel
SaaS	Logiciel en tant que service (*Software as a Service*)
GIES	Gestion des informations et des événements de sécurité
COS	Centre des opérations de sécurité
TLP	Protocole TLP (*Traffic Light Protocol*)
VDI	Infrastructure de bureau virtuel (*Virtual Desktop Infrastructure*)

6.2 GLOSSAIRE

Terme	Définition
Privilèges administratifs	Autorisations qui permettent à un utilisateur d'exécuter certaines fonctions sur un système ou un réseau, comme l'installation d'un logiciel et la modification de paramètres de configuration.
Biométrie	La biométrie désigne la mesure et l'usage de caractéristiques corporelles uniques (comme les empreintes digitales, la rétine, la structure faciale, les caractéristiques linguistiques et les réseaux veineux).
PAP	Les employés utilisent leurs dispositifs à des fins opérationnelles, et les organisations peuvent décider de rembourser certains coûts associés aux dispositifs. Toutefois, puisque le dispositif n'appartient pas à votre organisation, vous avez peu d'emprise sur les contrôles de sécurité mis en place sur le dispositif.
CASB	Un courtier de sécurité d'accès au nuage (CASB pour *Cloud Access Security Broker*) est un logiciel dans le nuage qui surveille les activités et met en application des mesures de sécurité entre les comptes et les applications.
Information classifiée	Toute information liée à l'intérêt national et qui pourrait faire l'objet d'une exception ou d'une exclusion, mais dont la compromission, selon toute vraisemblance, porterait atteinte à l'intérêt national (p. ex. la défense nationale, les relations avec d'autres pays, des intérêts économiques).
Chiffrement	Transformation de données d'un format vers un autre pour cacher leur contenu et empêcher un accès non autorisé.
Menace interne	Toute personne qui connaît l'infrastructure ou l'information d'une organisation, ou qui y a accès, et qui utilise ses connaissances ou son accès d'une façon malveillante ou involontaire pour nuire à cette organisation.

Terme	Définition
Débridage	Le processus qui consiste à exploiter un dispositif de façon à enlever les restrictions imposées par le fabricant. Ce processus est aussi appelé routage sur les dispositifs Android qui exécutent le système d'exploitation Android.
Droit d'accès minimal	Principe selon lequel il convient de n'accorder aux utilisateurs que les autorisations d'accès dont ils ont besoin pour accomplir les tâches qui leur ont été dûment attribuées. Ce principe permet de limiter les dommages pouvant résulter d'une utilisation non autorisée – abusive ou accidentelle – d'un système d'information.
Hameçonnage	Procédé par lequel une tierce partie tente de solliciter de l'information confidentielle appartenant à un individu, à un groupe ou à une organisation en les usurpant ou en imitant une marque commerciale connue, souvent dans le but de réaliser des gains financiers. Les hameçonneurs incitent les utilisateurs à partager leurs renseignements personnels (numéros de cartes de crédit, données bancaires ou autres renseignements sensibles) afin de s'en servir pour commettre des actes frauduleux.
Rançongiciels	Type de maliciel qui empêche un utilisateur légitime d'accéder à des ressources (système ou données) jusqu'à ce qu'il ait payé une rançon.
Risque	Dans le contexte de la cybersécurité, la probabilité qu'un auteur de menace se serve d'une vulnérabilité pour accéder aux biens et l'incidence de la menace.
GIES	La GIES est un produit ou un service qui réunit de grandes quantités de journaux de sécurité et effectue une agrégation automatisée, une normalisation, un signalement d'incidents, une gestion des incidents et d'autres fonctionnalités de sécurité. L'analyse du comportement de l'utilisateur peut aussi être une fonctionnalité offerte par un GIES.
COS	Un COS se compose habituellement d'une équipe d'analystes de la sécurité chargée de passer en revue les journaux et les incidents 24 heures sur 24. L'équipe réalise une évaluation des incidents en temps réel, elle explore en profondeur selon les besoins et elle fait le signalement des incidents et des interventions.
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice aux actifs et à l'information de TI.
VDI	L'infrastructure de bureau virtuel utilise des solutions technologiques pour héberger des environnements de bureaux virtuels sur des dispositifs appartenant à l'organisation ou à l'employé. Cette technologie permet aux utilisateurs d'avoir accès à leurs postes de travail au moyen d'une session virtuelle connectée à leur dispositif.
Vulnérabilité	Défectuosité ou lacune inhérente à la conception ou à la mise en œuvre d'un système d'information ou à son environnement, qui pourrait être exploitée par un auteur de menace en vue de compromettre les biens ou les activités d'une organisation.

6.3 RÉFÉRENCES

Numéro	Référence
1	Centre canadien pour la cybersécurité, *ITSAP.00.101 – Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage*, avril 2020.
2	Centre canadien pour la cybersécurité, *ITSAP.30.032 – Pratiques exemplaires de création de phrases de passe et de mots de passe*, septembre 2019.
3	Centre canadien pour la cybersécurité, *ITSM.10.093 – Les 10 mesures de sécurité des TI : No 6, Miser sur une formation sur mesure en matière de cybersécurité*, février 2020.
4	Centre canadien pour la cybersécurité, *ITSAP.30.030 – Sécurisez vos comptes avec une authentification multifacteur*, juin 2020.
5	Centre canadien pour la cybersécurité, *ITSP.30.031 v3 – Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information*, avril 2018.
6	Centre canadien pour la cybersécurité, *ITSAP.10.003 – Comment protéger votre organisation contre les menaces internes*, février 2020.
7	Centre canadien pour la cybersécurité, *ITSAP.70.002 – Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles*, juin 2020.
8	Centre canadien pour la cybersécurité, *ITSAP.70.111 – Utiliser un poste de travail virtuel à la maison et au bureau*, août 2020.
9	FIRST. *Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance v.1*.