Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Facteurs à considérer lors de l'utilisation des médias sociaux dans votre organisation

GESTIONNAIRES

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

TLP:WHITE

Canada

AVANT-PROPOS

Le présent document non classifié est publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité.

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 3 janvier 2022.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Première diffusion.	3 janvier 2022

No de cat. D97-4/10-066-2022F-PDF
ISBN 978-0-660-41586-4

VUE D'ENSEMBLE

L'environnement des médias sociaux évolue rapidement et révèle de nouveaux risques et défis. Tous les intervenants devraient être informés du contexte de la menace en évolution et des mesures de sécurité nécessaires à la protection de leurs activités dans les médias sociaux.

Le présent document traite des menaces courantes dans les médias sociaux et des mesures de protection de la vie privée que votre organisation peut mettre en œuvre pour protéger les utilisateurs, les processus et les technologies qui contribuent à la création et à la publication de contenu en ligne.

TABLE DES MATIÈRES

1 Introduction 5

2 Menaces courantes dans les médias sociaux 6

3 Mesures de protection 8

3.1 Provisionnement sécurisé 8

3.1.1 Politique en matière de médias sociaux 8

3.1.2 Plateformes de médias sociaux 9

3.1.3 Gestion de l'accès 9

3.1.4 Applications et systèmes sécurisés 10

3.1.5 Considérations d'ordre juridique et en matière de confidentialité 10

3.2 Publication sécurisée 12

3.2.1 Procédures de publication 12

3.2.2 Accès de tiers 12

3.2.3 Éducation et formation 13

3.3 Intervention et reprise en cas d'incident 13

3.3.1 Plan d'intervention en cas d'incident 13

3.3.2 Surveillance 13

3.3.3 Vérification et journalisation 14

3.3.4 Partenariats 14

4 Résumé 15

4.1 Coordonnées 15

5 Contenu complémentaire 16

5.1 Liste des acronymes, abréviations et sigles 16

5.2 Glossaire 16

5.3 Références 17

1 INTRODUCTION

Le présent document recommande des mesures de sécurité que votre organisation peut mettre en œuvre pour protéger les utilisateurs, les processus et les technologies qui contribuent à la création et à la publication de contenu en ligne.

Les médias sociaux ont changé la façon dont les Canadiens communiquent, gardent contact et tissent de nouvelles relations. Les Canadiens passent plus de temps en ligne, et les organisations utilisent des outils de médias sociaux pour échanger avec leurs clients. Les entreprises travaillent de plus en plus avec des outils de gestion de marketing social pour exécuter leurs stratégies de marketing numérique. Les ministères du gouvernement du Canada (GC) utilisent aussi les médias sociaux pour établir des liens avec les Canadiens et promouvoir les programmes et services qu'offre le gouvernement.

Les auteurs malveillants ciblent les médias sociaux pour lancer des cyberattaques destructrices. Par exemple, des auteurs de menace parrainés par des États-nations se servent des médias sociaux comme outils de surveillance, et ils créent de faux profils pour influencer les débats publics. Il importe de porter attention aux risques liés à la sécurité qui sont associés aux applications de réseaux sociaux. Pour vous protéger et pour protéger les activités que mène votre organisation dans les médias sociaux, vous pourriez envisager une approche multidimensionnelle à la sécurité en mettant en œuvre divers contrôles de sécurité.

2 MENACES COURANTES DANS LES MÉDIAS SOCIAUX

Vos activités dans les médias sociaux peuvent exposer votre entreprise et vos utilisateurs à plusieurs types de menaces. Nous présentons ci-dessous quelques exemples de menaces types :

- **Attaques par hameçonnage :** Les auteurs de menace utilisent les attaques par hameçonnage de manière à inciter les utilisateurs à cliquer sur un lien malveillant, à télécharger un maliciel ou à divulguer de l'information sensible. Si les utilisateurs ne savent pas comment protéger leurs comptes de médias sociaux contre des attaques par hameçonnage, les auteurs de menace se servent de ces techniques pour voler les justificatifs d'accès et prendre le contrôle des comptes ciblés. Des comptes compromis peuvent être utilisés pour distribuer des pourriels malveillants ou commettre une fraude financière en ligne. Les auteurs de menace peuvent aussi publier des messages malveillants (réponses) dans le cadre d'attaques par hameçonnage pour cibler les propriétaires ou les abonnés de comptes.
  - **Harponnage :** Les auteurs de menace ciblent des personnes en particulier en envoyant des messages personnalisés qui peuvent contenir des détails comme leurs champs d'intérêt, leurs récentes activités en ligne ou leurs achats.
- **Attaques par maliciel :** Les auteurs de menace peuvent distribuer des programmes malveillants par le biais de publications dans les médias sociaux. Des comptes détournés de médias sociaux peuvent être utilisés pour infecter des utilisateurs peu méfiants avec un maliciel. Vos utilisateurs ou abonnés des médias sociaux pourraient cliquer sur des liens URL qui peuvent les rediriger vers des sites Web hébergeant un maliciel ou un rançongiciel.
  - **Rançongiciels :** Type de maliciel qui bloque l'accès aux fichiers ou aux systèmes jusqu'à ce que l'utilisateur verse une somme d'argent. Lorsqu'un rançongiciel infecte un appareil, il verrouille son écran ou chiffre les fichiers qu'il contient. Les rançongiciels peuvent aussi se servir d'un réseau pour infecter d'autres dispositifs connectés à l'appareil infecté.
- **Campagnes de désinformation :** Les campagnes de désinformation sont des diffusions d'informations délibérément fausses dans les médias sociaux. En ayant recours à des campagnes ciblées, les auteurs de menace peuvent diffuser de faux messages afin de véhiculer des messages particuliers dans le but d'obtenir des gains financiers ou d'atteindre les résultats souhaités.
- **Menace interne :** Des employés ou des contacts proches qui détiennent un accès autorisé aux systèmes de médias sociaux peuvent publier des messages pour nuire intentionnellement à une organisation. Les employés peuvent aussi causer des dommages accidentels au profil de médias sociaux de votre organisation.
- **Erreurs humaines :** Un employé pourrait divulguer par erreur des justificatifs d'accès à un compte de médias sociaux et causer des dommages importants à une organisation. Des messages publiés en ligne qui contiennent des erreurs typographiques peuvent aussi donner une mauvaise impression de la marque d'une organisation. Des profils de médias sociaux qui n'ont pas été correctement mis en œuvre peuvent aussi exposer des utilisateurs et des entreprises à des risques non intentionnels à la protection de la vie privée.
- **Usurpation de la marque et typosquattage :** L'usurpation de la marque peut se produire lorsqu'un auteur de menace crée de faux comptes pour imiter ou voler l'identité d'une organisation en ligne. Les attaques par typosquattage exploitent les erreurs de frappe que peuvent faire les utilisateurs lorsqu'ils tapent une adresse URL, et les redirigent vers de faux sites Web. Habituellement, ces attaques visent à frauder les utilisateurs ou à voler des renseignements.

Lors d'attaques plus sophistiquées, cette technique peut être accompagnée d'une attaque par piratage psychologique pour obtenir un accès privilégié à des ressources d'arrière-plan.

- **Vol d'identité ou attaques par piratage de compte :** Les hacktivistes ou les auteurs de menace peuvent prendre le contrôle de comptes de médias sociaux pour faire la promotion de leur plateforme ou distribuer des maliciels. Certaines campagnes récentes ont impliqué des pirates qui ont utilisé des applications malveillantes avec de faux messages pour arnaquer des utilisateurs et obtenir accès à leurs profils de médias sociaux.
- **Vulnérabilités dans des plateformes et des applications tierces :** Les vulnérabilités inconnues et connues dans des outils logiciels, des outils d'édition et des applications de fournisseurs peuvent exposer les comptes de médias sociaux à des risques supplémentaires. Les auteurs de menace peuvent profiter de ces failles pour lancer des attaques plus sophistiquées.
- **Attaques par reconnaissance :** Les auteurs de menace peuvent obtenir des renseignements sur les employés, les projets de l'entreprise et les outils institutionnels à partir de publications dans les médias sociaux, d'offres d'emploi, de nouvelles publications et d'autres activités en ligne. Les renseignements obtenus de ces sources peuvent procurer de précieuses informations et être utilisés pour lancer des attaques par intrusion hautement ciblées.
- **Attaques par inférence :** Les auteurs de menace peuvent déduire l'information sensible d'un utilisateur en recueillant les publications ou les activités en ligne de ce dernier. Les données ainsi déduites peuvent devenir une arme servant à cibler des utilisateurs.

3 MESURES DE PROTECTION

Afin de vous protéger contre les menaces en ligne et de réduire les risques qu'une activité malveillante puisse cibler les comptes de médias sociaux de votre organisation, nous vous recommandons de surveiller et d'évaluer continuellement les risques. Dans le cadre de vos activités de gestion des risques, vous devriez passer en revue les procédures relatives aux médias sociaux de votre organisation, identifier les risques et mettre en œuvre les mesures de sécurité appropriées pour s'attaquer à ces risques et protéger vos données.

Vous devez entre autres tenir compte des mesures de sécurité suivantes :

- provisionnement sécurisé;
- publication sécurisée;
- intervention et reprise en cas d'incident.

3.1 PROVISIONNEMENT SÉCURISÉ

Le provisionnement sécurisé fait référence aux activités de gouvernance et aux blocs fonctionnels essentiels que vous pouvez mettre en œuvre pour sécuriser les procédés liés à vos médias sociaux. Ces activités donnent le ton juste à vos employés et procurent un cadre sécurisé pour ce qui est de guider les étapes initiales de votre programme de médias sociaux.

3.1.1 POLITIQUE EN MATIÈRE DE MÉDIAS SOCIAUX

Votre politique en matière de médias sociaux établit les exigences et les normes d'utilisation des médias sociaux de votre organisation. Votre politique doit porter sur les aspects suivants :

- Donner des directives sur la façon dont votre organisation compte mener ses interactions en ligne;
- Établir les principes relatifs aux cas d'utilisation acceptable pour les interactions commerciales et du personnel;
- Définir les conséquences d'une utilisation abusive des médias sociaux au sein de votre organisation;
- Définir les types de classification des données d'entreprise qui peuvent (ou non) être partagées au moyen des médias sociaux;
- Obliger tous les employés à recevoir une formation officielle sur les comportements exigés par l'organisation et les détails stipulés dans la politique;
- Rendre obligatoire une formation régulière sur la sensibilisation, particulièrement pour les personnes qui prennent part directement à la publication du contenu dans les médias sociaux;
- Établir des normes de collaboration avec les fournisseurs de services externalisés comme les équipes chargées du marketing de contenu ou du marketing en ligne.

3.1.2 PLATEFORMES DE MÉDIAS SOCIAUX

Choisir une plateforme de médias sociaux et gérer les comptes connexes doit être un mécanisme d'évaluation continue des risques. Votre organisation doit évaluer ses objectifs à l'égard des médias sociaux et s'assurer que les plateformes permettent la réalisation de ces objectifs. Avant de choisir une plateforme de médias sociaux, passez en revue les caractéristiques de sécurité et de protection de la vie privée de cette plateforme. Les exemples suivants donnent certaines caractéristiques à rechercher :

- Elle doit prendre en charge des technologies de communications par réseau sécurisé, comme le protocole HTTPS (*Hypertext Transfer Protocol Secure*), le protocole TLS (*Transport Layer Security*) et le protocole SSH (*Secure Shell*), pour les applications de communications Web et mobiles;
  - Elle utilise des certificats signés d'autorité de certification (AC) valides, vérifiés et fiables;
  - Elle n'utilise aucun algorithme ou protocole obsolète (la plateforme prend en charge le protocole TLS 1.2 ou une version plus récente);
- Elle prend en charge des mécanismes d'authentification sécurisés comme l'utilisation de mots de passe robustes, l'authentification multifacteur (MFA pour *Multi-Factor Authentication*) et le test de sécurité CAPTCHA (*Completely Automated Public Turing tests to tell Computers and Humans Apart*);
- Elle prend en charge des comptes d'utilisateur distincts pour les comptes de médias sociaux de gestion à utilisateurs multiples;
- Elle prend en charge un modèle d'accès utilisateur basé sur les rôles pour gérer l'authentification de l'utilisateur et les autorisations;
- Elle détecte toute nouvelle activité d'authentification ou toute activité suspecte relative aux comptes d'utilisateur;
- Elle permet d'assurer le respect de la vie privée des utilisateurs et la personnalisation des paramètres de confidentialité;
- Elle compte sur un service d'assistance dédié ou une équipe de sécurité prête à intervenir en cas d'incident.

3.1.3 GESTION DE L'ACCÈS

Pour être en mesure de respecter les exigences de la politique et de vous protéger contre le vol d'identité, vous devez vous assurer de gérer adéquatement l'accès aux comptes de médias sociaux de votre organisation. Tous les comptes doivent respecter vos politiques en matière de comptes d'utilisateur et de gestion des justificatifs. Si cela est possible, nous recommandons l'utilisation de l'authentification multifacteur.

Vous devriez revoir régulièrement tous les droits relatifs aux accès et aux autorisations, et retirer l'accès aux employés ayant quitté l'organisation. Assurez-vous également de sécuriser et de passer en revue attentivement les autorisations tierces. Pour protéger l'accès et les données, votre organisation devrait mettre en œuvre une surveillance appropriée des mesures de protection.

Tenez compte des conseils suivants pour profiter d'une sécurité accrue :

- Utilisez des phrases de passe et des mots de passe forts et uniques pour chaque compte de médias sociaux;
- Évitez de partager les justificatifs;

  - Les utilisateurs doivent avoir des comptes individuels en fonction des autorisations qui leur sont accordées pour accomplir leurs tâches;
- Désactivez les services d'authentification qui ne sont pas utilisés, comme l'accès à une interface de programmation d'applications (IPA);
- Mettez hors service les comptes de médias sociaux qui ne sont plus utilisés et archivez les publications connexes.

Pour obtenir plus de conseils sur la gestion de l'accès, consultez les publications suivantes à ce sujet :

- *Gestion et contrôle des privilèges administratifs* (ITSAP.10.094) [1][1];
- *Sécurisez vos comptes et vos appareils avec une authentification multifacteur* (ITSAP.30.030) [2];
- *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* (ITSP.30.031) [3].

3.1.4 APPLICATIONS ET SYSTÈMES SÉCURISÉS

Vous pouvez mettre en application les recommandations suivantes pour vous assurer que les pratiques exemplaires appropriées en matière de cybersécurité sont adoptées pour les dispositifs et systèmes liés aux médias sociaux et pour toutes les applications logicielles utilisées pour la diffusion des publications dans les médias sociaux :

- Veillez à ce que seuls les dispositifs approuvés (p. ex. les dispositifs définis dans le modèle de déploiement de votre appareil mobile) soient utilisés pour les interactions dans les médias sociaux;
- Mettez à jour régulièrement les systèmes et les dispositifs et installez les correctifs dès qu'ils sont disponibles;
- Installez des solutions de prévention et de détection antimaliciels;
- Mettez en œuvre des contrôles de renforcement de la sécurité de dispositif de manière à resserrer les autorisations et à limiter l'accès aux systèmes essentiels de votre réseau d'entreprise depuis ces dispositifs;
- Assurez-vous que le personnel utilise un réseau privé virtuel (RPV) ou une technologie comparable pour accéder aux comptes de médias sociaux sur des réseaux Wi-Fi publics ou non fiables.

Pour obtenir de plus amples renseignements sur la façon de sécuriser les dispositifs sur les réseaux domestiques et d'entreprise, consultez les publications suivantes :

- *La cybersécurité à la maison et au bureau – Sécuriser vos dispositifs, vos ordinateurs et vos réseaux* (ITSAP.00.007) [4];
- *Application des mises à jour sur les dispositifs* (ITSAP.10.096) [5];
- *Utiliser le WI-FI sans compromettre la sécurité de votre organisation* (ITSAP.80.009) [6];
- *Les réseaux privés virtuels* (ITSAP.80.101) [7].

3.1.5 CONSIDÉRATIONS D'ORDRE JURIDIQUE ET EN MATIÈRE DE CONFIDENTIALITÉ

L'utilisation des médias sociaux expose votre organisation à des risques d'ordre juridique et liés à la confidentialité. Certains secteurs d'activités doivent respecter des exigences en matière de résidence des données. Avant d'utiliser les médias sociaux, vous devez vous assurer de bien comprendre les répercussions juridiques et les effets sur la protection des

[1] Les numéros entre crochets renvoient à des ressources figurant à la section Contenu complémentaire du présent document.

renseignements personnels qu'une telle utilisation pourrait avoir sur vos opérations. Par exemple, il faut savoir quelles sont les données stockées (publications, consultations, connexions, données suivies), à qui appartiennent les données dans votre compte, l'endroit où sont stockées les données (emplacement géographique des données, y compris les données transitoires ou les sauvegardes).

Le Canada possède des lois sur la protection de la vie privée comme la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)*, qui établit les règles entourant la collecte, l'utilisation et la divulgation des données des entreprises de médias sociaux, dans certaines circonstances. Toutefois, les utilisateurs peuvent donner à ces entreprises leur consentement pour collecter, utiliser ou partager leurs renseignements. Accordez une attention particulière aux conditions d'utilisation et aux avis sur la protection des renseignements personnels pour vous assurer de bien comprendre vos devoirs et obligations. Vous devriez vous familiariser avec les outils propres à la plateforme et les fonctions de confidentialité personnalisables que vous pouvez utiliser pour renforcer la protection de la confidentialité de votre compte. Enfin, passez régulièrement en revue ces services pour effectuer les mises à jour et profiter de nouveaux outils que vous pouvez utiliser pour réduire votre exposition aux risques.

3.2 PUBLICATION SÉCURISÉE

Cette section présente certaines pratiques exemplaires liées à la diffusion et à la protection de vos publications dans les médias sociaux.

3.2.1 PROCÉDURES DE PUBLICATION

Votre organisation pourrait disposer d'équipes spéciales chargées de l'engagement auprès de la communauté, du marketing de contenu et des relations publiques. Ces équipes peuvent être composées de plusieurs personnes ayant un accès direct aux comptes de médias sociaux de votre organisation. Il est essentiel de mettre en place des procédures permettant de s'assurer que tout le contenu est revu et autorisé avant sa publication.

Vous devriez tenir compte des mesures suivantes :

- Mettre en œuvre des procédures de travail visant à approuver les publications et à assurer l'uniformité du contenu publié;
- Passer en revue et approuver tout contenu mis à jour ainsi que les mises à jour;
- S'assurer d'avoir l'autorisation d'utiliser, de reproduire ou de publier du contenu tiers ou du contenu protégé;
- Impliquer le service juridique dans le processus d'approbation du contenu, comme il est prescrit;
- Activer les journaux d'accès et d'activités pour faire ressortir les détails du processus de révision;
- Épurer les documents, les images et le contenu vidéo pour supprimer les métadonnées connexes avant de les rendre disponibles au public.

3.2.2 ACCÈS DE TIERS

Souvent, les tiers jouent un rôle important dans la création et la publication de contenu pour les médias sociaux. Par exemple, vous pourriez collaborer avec une agence de commercialisation numérique pour assurer l'exécution de votre plan de marketing en ligne. Dans un tel scénario, les tiers obtiennent un accès administratif au compte de médias sociaux de l'organisation pour être en mesure de publier du contenu, selon les besoins. Une fois l'accès administratif ou l'accès privilégié accordé, vous devez vous assurer qu'il est étroitement contrôlé. Les attentes en matière de sécurité et de conduite des utilisateurs doivent être définies dans le cadre des conditions d'engagement du contrat. Les politiques en matière de mots de passe et de comportement qui s'appliquent aux employés internes doivent aussi être en vigueur pour l'agence afin d'assurer une cohérence. On sait que les auteurs de menace ciblent les maillons faibles de la chaîne d'approvisionnement. Même si votre organisation n'est pas la cible directe d'une cyberattaque, elle pourrait être touchée si l'un de ses fournisseurs est compromis.

Lorsque vous passez en revue les applications tierces, tenez compte de ce qui suit :

- Identifiez les applications tierces qui ont accès à vos données de médias sociaux;
- Validez les autorisations pour les applications qui doivent conserver l'accès;
- Supprimez ou enlevez les applications non désirées ou désactivez les autorisations que vous voulez révoquer;
- Mettez en place un programme de surveillance qui vous avertit dès qu'une application tierce accède à votre compte.

3.2.3 ÉDUCATION ET FORMATION

La formation constitue un élément essentiel pour tous les utilisateurs impliqués dans le processus de publication. Les utilisateurs doivent être informés des politiques d'utilisation acceptable et de leurs responsabilités. En ce qui a trait expressément aux systèmes ou aux comptes qui nécessitent un accès multi-utilisateur, les titulaires de comptes individuels doivent être informés des risques possibles. Votre organisation devrait tenir des séances de formation de routine (p. ex. sur une base annuelle) pour tous les employés. Formez les employés pour qu'ils soient en mesure d'utiliser les outils et les procédures permettant de supprimer les détails liés aux métadonnées comme les noms d'utilisateur, l'emplacement géographique, le modèle du dispositif et d'autres détails tirés des publications. Les utilisateurs devraient être obligés de signer une entente sur les modalités d'utilisation. De plus, en raison des fréquentes modifications apportées aux plateformes de médias sociaux, il vous faut passer en revue toutes les récentes mises à jour. Les nouvelles fonctions qui améliorent les paramètres de confidentialité désirés ou celles qui peuvent avoir une incidence sur le respect de la vie privée des utilisateurs sont des exemples de fonctions à surveiller.

3.3 INTERVENTION ET REPRISE EN CAS D'INCIDENT

Des incidents se produisent réellement. Dans le but de minimiser les répercussions que pourrait avoir un incident, il vous faut des plans d'intervention et de reprise pour guider le personnel sur la façon de traiter les problèmes.

3.3.1 PLAN D'INTERVENTION EN CAS D'INCIDENT

Précisez votre plan d'intervention en cas d'incident pour que celui-ci tienne compte des résultats possibles. On peut penser par exemple à quelqu'un qui publie un message non approuvé ou qui pirate un compte pour causer des préjudices. Le document doit présenter les mesures recommandées qu'il convient de prendre pour intervenir adéquatement en cas d'incidents différents. La plupart des plateformes de médias sociaux donnent les coordonnées du bureau d'enregistrement des cas d'abus sur leur site Web. Un non-respect de la LPRPDE, un accès délibéré ou accidentel non autorisé ou la divulgation de renseignements personnels lors de l'utilisation des médias sociaux pourrait être vu comme une atteinte à la vie privée, et devrait être signalé au service responsable de la protection de la vie privée de votre organisation et au Commissariat à la protection de la vie privée du Canada.

Lorsque vous prenez le temps de passer en revue, de tester et de mettre à jour votre plan d'intervention, vous pouvez garantir l'efficacité de vos plans et de vos procédures. Vous pouvez utiliser des exercices sur table basés sur un scénario pour analyser les étapes de votre plan d'intervention. Vous devriez appliquer les leçons tirées à partir de ces exercices sur table en mettant vos plans à jour.

3.3.2 SURVEILLANCE

Votre organisation peut mettre en place un programme de surveillance du flux des communications des médias sociaux pour détecter toute mention frauduleuse de la marque d'entreprise et corriger les éventuels incidents. La surveillance peut vous aider à détecter rapidement les menaces comme les attaques par usurpation d'identité ou celles liées à la désinformation.

Réussir à mettre en œuvre un programme de surveillance de marque peut s'avérer difficile en raison d'un taux plus élevé d'alertes faussement positives. Toutefois, avec des règles précises de détection et une bonne coordination entre les équipes

d'engagement auprès de la communauté, ce programme peut s'avérer très précieux. Beaucoup de plateformes offrent des fonctions de base pour le signalement d'abus, alors que d'autres permettent aux titulaires de compte d'administrateur de signaler des activités menées par des imposteurs afin qu'une intervention rapide soit faite.

Pour surveiller les attaques liées à l'authentification, vous pourriez envisager de configurer des notifications lors de l'authentification réussie de nouveaux dispositifs ou de changements apportés aux autorisations du compte. Pour ce qui est des cas d'utilisation avancés, un programme de surveillance peut être mis en place pour identifier les événements d'authentification fédérés réussis si un compte est utilisé pour se connecter à d'autres applications Web. Cela peut faciliter l'identification des violations des politiques du compte ou des incidents liés au vol d'identité.

3.3.3 VÉRIFICATION ET JOURNALISATION

La réussite du programme de surveillance dépend fortement des capacités de son infrastructure de vérification et de journalisation. La mise en œuvre de procédures pour saisir, stocker et fournir des journaux d'activités précis permet de voir les usages malveillants et vient appuyer les enquêtes sur les incidents. Par défaut, les plateformes de médias sociaux offrent pour la plupart aux utilisateurs des fonctions de vérification et de journalisation de base. Vous devez comprendre les capacités et les contraintes d'un paramétrage par défaut et déterminer s'il est suffisant pour répondre à vos besoins. Les politiques de conservation, les procédures de récupération et les délais d'intervention associés aux requêtes spéciales devraient faire l'objet d'une attention particulière. Pour les cas d'utilisation particuliers, vous pouvez profiter de la plateforme de médias sociaux pour explorer les possibilités liées aux capacités avancées de journalisation ou au soutien du stockage hors plateforme.

3.3.4 PARTENARIATS

Vous devriez établir des partenariats avec des intervenants pertinents avant que ne se produise un incident. Utilisez leurs coordonnées publiques pour les contacter et vous renseigner sur leur participation à vos exercices sur table. La plupart seraient prêts à vous aider. Lorsque vous traitez un incident, communiquez avec tous les organismes pertinents, selon vos besoins : médias sociaux, service de police local et agences spécialisées comme le Centre antifraude du Canada. Vous pouvez également signaler ces incidents à notre centre d'appel aux fins de suivi.

Votre organisation peut investir dans une police d'assurance en matière de cybersécurité si vous jugez que cela pourrait être bénéfique pour votre organisation. Votre police peut ajouter une couche de protection supplémentaire et elle peut également offrir à votre organisation une expertise en matière d'intervention en cas d'incident dans l'éventualité d'une attaque par rançongiciel.

Pour avoir de plus amples renseignements sur les mesures recommandées pour traiter un incident, reportez-vous à notre guide sur les *Faux comptes de médias sociaux* [8].

4 RÉSUMÉ

Le contexte de la menace dans les médias sociaux est en évolution. Les utilisateurs doivent demeurer informés des nouvelles menaces qui peuvent cibler leurs activités dans les médias sociaux en ligne. Votre organisation et les intervenants peuvent avoir recours à diverses mesures de protection et stratégies pour protéger vos plateformes de médias sociaux. Il est recommandé de mettre en œuvre des mesures de protection comme le provisionnement sécurisé de vos dispositifs et des techniques d'intervention et de reprise en cas d'incident. Les entreprises doivent porter une attention particulière au contexte de risque opérationnel changeant et s'assurer d'avoir en place les contrôles de sécurité nécessaires, comme ceux énumérés précédemment, pour combler les lacunes éventuelles.

4.1 COORDONNÉES

Pour de plus amples renseignements sur la mise en œuvre de cette ligne directrice, communiquez par téléphone ou par courriel avec le centre d'appel.

Centre d'appel
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

5 CONTENU COMPLÉMENTAIRE

5.1 LISTE DES ACRONYMES, ABRÉVIATIONS ET SIGLES

Terme	Définition
AC	Autorité de certification
CAPTCHA	Test de sécurité dont l'acronyme anglais est *Completely Automated Public Turing tests to tell Computers and Humans Apart*
GC	Gouvernement du Canada
HTTPS	Protocole HTTPS (*Hypertext Transfer Protocol Secure)*
IPA	Interface de programmation d'applications
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
MFA	Authentification multifacteur (*Multi-Factor Authentication*)
RPV	Réseau privé virtuel
SSH	Protocole SSH (*Secure Shell*)
StatsCan	Statistique Canada
TLS	Protocole TLS (*Transport Layer Security*)

5.2 GLOSSAIRE

Terme	Définition
Authentification	Processus de vérification de l'identité déclarée par ou pour une entité de système.
Authentification multifacteur (*Multi-Factor Authentication*)	Méthode d'authentification de l'utilisateur qui exige au moins deux moyens (facteurs) différents de vérifier l'identité déclarée. Les trois facteurs les plus répandus sont : (1) quelque chose que vous connaissez (p. ex. un mot de passe), (2) quelque chose que vous avez (p. ex. un jeton d'authentification physique) et (3) quelque chose qui vous caractérise (p. ex. une biométrie).
LPRPDE	La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) est la loi fédérale relative au respect de la vie privée qui touche les organisations du secteur privé.
Réseau privé virtuel	Réseau de communication privé généralement utilisé au sein d'une organisation ou entre plusieurs entreprises ou organisations diverses pour communiquer sur un réseau élargi. Les communications sur le RPV sont habituellement chiffrées ou codées pour protéger le trafic provenant des autres utilisateurs, qui est transmis sur le réseau public ayant recours au RPV.
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 en vue de compromettre les biens ou les activités d'une organisation.

5.3 RÉFÉRENCES

Numéro	Référence
1	Centre canadien pour la cybersécurité, *Gestion et contrôle des privilèges administratifs* (ITSAP.10.094), juillet 2020.
2	Centre canadien pour la cybersécurité, *Sécurisez vos comptes et vos appareils avec une authentification multifacteur* (ITSAP.30.030), juin 2020.
3	Centre canadien pour la cybersécurité. *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information* (ITSP.30.031 version 3), avril 2018.
4	Centre canadien pour la cybersécurité, *La cybersécurité à la maison et au bureau – Sécuriser vos dispositifs, vos ordinateurs et vos réseaux* (ITSAP.00.007), octobre 2020.
5	Centre canadien pour la cybersécurité, *Application des mises à jour sur les dispositifs* (ITSAP.10.096), février 2020.
6	Centre canadien pour la cybersécurité, *Utiliser le WI-FI sans compromettre la sécurité de votre organisation* (ITSAP.80.009), octobre 2020.
7	Centre canadien pour la cybersécurité, *Les réseaux privés virtuels* (ITSAP.80.101), octobre 2019.
8	Centre canadien pour la cybersécurité, *Faux comptes de médias sociaux.*