Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Stratégies pour protéger les systèmes d'application Web contre les attaques par bourrage d'identifiants

SÉRIE PRATICIEN

TLP:WHITE

Canada

AVANT-PROPOS

L'*ITSP.30.035 — Stratégies pour protéger les systèmes d'application Web contre les attaques par bourrage d'identifiants* est une publication NON CLASSIFIÉ émise sous l'autorité du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité).

Pour obtenir de plus amples renseignements, communiquez avec notre centre d'appel par téléphone ou par courriel :

Centre d'appel

Contact@cyber.gc.ca

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

DATE D'ENTRÉE EN VIGUEUR

Cette publication entre en vigueur le 17 janvier 2022.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1	Première version.	*17 janvier 2022*

ISBN 978-0-660-40253-6

CAT D97-3/30-035-2021F-PDF

APERÇU

Le présent document offre aux administrateurs de système d'application Web des recommandations en matière de sécurité qui visent à protéger leurs systèmes d'application Web contre des attaques par bourrage d'identifiants.

Les Canadiens comptent sur des applications Web pour obtenir des services essentiels. Des organisations publiques et privées en déploient d'ailleurs de plus en plus afin de fournir des plateformes de services en ligne qui sont sécurisées, flexibles et robustes. Il s'avère essentiel de sécuriser ces opérations contre des attaques relatives à l'authentification pour protéger la confidentialité et l'intégrité des systèmes et de l'information.

Le présent document contient ainsi des recommandations concernant des contrôles techniques et non techniques que vous pouvez appliquer pour protéger les services Web de votre organisation contre des attaques par bourrage d'identifiants. Bien que le présent document vise directement les systèmes du gouvernement du Canada (GC), les conseils y figurant s'appliquent également aux organisations non gouvernementales.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

1 INTRODUCTION

Le présent document porte sur les menaces usuelles découlant de l'authentification par mot de passe, mais vise principalement les attaques par bourrage d'identifiants. Il recommande des contrôles de sécurité techniques et non techniques que vous pouvez mettre en œuvre pour prévenir et atténuer les attaques par bourrage d'identifiants. Bien qu'ils visent les systèmes du GC, les conseils y figurant s'appliquent également aux organisations non gouvernementales.

Dans le monde branché dans lequel nous vivons, les applications Web offrent des infrastructures économiques et souples qui permettent rapidement de mettre en place et d'offrir des services. Les organisations comptent sur des applications pour offrir des services essentiels à leurs clientèles. Le besoin de créer un cadre d'authentification sûr et sécurisé est donc essentiel, surtout pour les déploiements complexes, comme les systèmes hautement sensibles ou critiques. Les ministères du GC misent par exemple sur des applications Web pour fournir différents services. Le personnel et les utilisateurs doivent alors souvent s'authentifier pour accéder à ces applications. Pour que les utilisateurs aient confiance envers le système, le cadre d'authentification doit correctement identifier les utilisateurs légitimes et bloquer les attaques par mot de passe des adversaires.

La hausse des cas signalés de violations de données au sein d'organisations a engendré une augmentation des cas d'attaque par bourrage d'identifiants. De fait, des millions d'attaques par bourrage d'identifiants ont lieu chaque jour, ciblant des systèmes d'application Web sur Internet. Pour ce faire, des auteurs de menace ciblent des comptes d'utilisateur en se servant de justificatifs d'identité obtenus à la suite de fuites ou de vols de données pour accéder à des comptes sans autorisation. Par conséquent, il vous incombe de vérifier l'architecture d'authentification de vos applications Web afin de les protéger des attaques associées aux mots de passe.

Nous vous recommandons de consulter les documents qui suivent pour savoir comment sécuriser les services offerts sur vos applications Web :

- *Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information (ITSP.30.031)* [1][1]
- *National Institute of Standards and Technology, NIST Special Publications, 800-63B - Computer Security. Authentication and Lifecycle Management* [2]
- *NIST SP 800-95 Guide to Secure Web Services* [3]
- *Open Web Application Security Project (OWASP) Application Security Verification Standard 4.0* [4]

1.1 PORTÉE

Le présent document porte sur la protection contre les attaques par bourrage d'identifiants au moyen de contrôles de sécurité. Bien que ce type d'attaque soit étroitement lié aux attaques par force brute ou par pulvérisation de mots de passe, ou à toute autre forme d'attaque relative aux mots de passe, les contrôles suggérés sont principalement conçus pour vous protéger contre les attaques par bourrage d'identifiants.

[1] Les chiffres entre crochets renvoient aux références présentées dans la section Contenu complémentaire du présent document.

Vous trouverez dans le présent document des conseils sur les applications Web qui contiennent des données dont le niveau de confidentialité est faible ou modéré; au GC, il s'agit de données Non classifié, Protégé A ou Protégé B. Il ne s'applique pas aux applications Web qui comportent des données hautement confidentielles (Protégé C) ni aux systèmes classifiés qui présentent des données hautement confidentielles ayant un intérêt national.

1.2 PROCESSUS D'AUTHENTIFICATION ET DE GESTION DES RISQUES LIÉS À LA SÉCURITÉ DES TI

L'intégrité des processus liés aux systèmes et aux données lors du développement et du déploiement d'applications Web sécurisées est fondamentale. Le besoin d'authentifier et d'autoriser correctement les demandes de service des utilisateurs est étroitement lié aux objectifs de confidentialité et d'intégrité du système. Vos processus de sécurité devraient donc être conformes aux cadres de gestion des risques liés à la sécurité des TI en place afin de préserver l'intégrité de votre système d'application Web. Les mécanismes d'identification et d'authentification permettent d'établir des procédures de sécurité visant à identifier les utilisateurs et à valider leur identité par rapport à ce qu'ils prétendent être.

L'ITSP.30.031 v3 [1] présente de l'information sur les contrôles de sécurité recommandés pour les systèmes d'application Web du GC. De plus, le National Institute of Standards and Technology (NIST) donne des conseils sur le développement et le déploiement d'architectures d'authentification sécurisées dans les publications suivantes :

- *NIST SP 800-63-3 Digital Identity Guidelines* [5]
- *NIST SP 800-63A Digital Identity Guidelines: Enrollment and Identity Proofing* [6]
- *NIST SP 800-63B* [2]
- *NIST SP 800-63C Digital Identity Guidelines: Federation and Assertions* [7]

1.2.1 IDENTIFICATION ET AUTHENTIFICATION

L'identification et l'authentification font référence à la famille des contrôles de sécurité qui permettent à un système d'information d'identifier et d'authentifier de manière unique les utilisateurs. On compte parmi ces contrôles les activités d'authentification relatives à l'orientation des politiques et des procédures, à l'identification des utilisateurs de manière unique, à la gestion des identifiants, à la gestion des authentifiants, à la gestion des messages de rétroaction, à la confirmation des identités et à la réauthentification.

Pour obtenir une description détaillée des activités de contrôle associées à l'identification et à l'authentification, consultez la section sur l'identification et l'authentification à l'annexe 3a de l'*ITSG-33 Une méthode axée sur le cycle de vie* (ITSG-33) [8].

1.2.2 CONFIRMATION DE L'IDENTITÉ

La confirmation de l'identité fait référence au processus de collecte, de validation et de vérification des renseignements sur l'identité d'un utilisateur de sorte à justifier l'accès à un système. Elle comprend des activités qui permettent de valider l'identité d'un utilisateur par rapport à ce qu'il prétend être. Les composantes du processus de confirmation de l'identité peuvent varier selon le profil de sécurité de l'application Web. Le document *NIST SP 800-63A* [6] décrit trois options

permettant de confirmer l'identité d'un utilisateur et d'inscrire l'utilisateur concerné. Chaque option présente des ensembles d'exigences différents basés sur le profil de risque du système concerné. Dans la plupart des systèmes d'application Web, ces activités comprennent les processus d'identification, d'inscription et de validation de l'utilisateur. Pour assurer l'intégrité d'une application Web, les propriétaires et administrateurs de système doivent mettre en place des exigences qui cadrent avec les profils de risque de leurs systèmes. Le choix d'un profil de risque pour une application Web dépasse la portée du présent document.

1.2.3 ATTAQUE PAR BOURRAGE D'IDENTIFIANTS

Il s'agit d'une attaque lors de laquelle des auteurs de menace se servent de justificatifs d'identité obtenus à la suite d'un vol ou d'une fuite de données pour accéder à des comptes d'utilisateur sur d'autres applications Web. Autrement dit, des auteurs de menace utilisent des justificatifs d'identité acquis ailleurs – une violation de données a habituellement eu lieu auparavant – et les entrent dans votre système pour se connecter comme le feraient des utilisateurs autorisés. Les pirates qui ont recours au bourrage d'identifiants tirent profit des habitudes qu'ont les utilisateurs d'opter pour les mêmes justificatifs d'identité pour différents comptes. Veuillez consulter la section 2.1.3 du présent document pour en savoir plus sur les attaques par bourrage d'identifiants.

1.3 AUTHENTIFICATION

La présente section traite des formes d'authentification et des facteurs d'authentification.

L'authentification numérique est un processus dans le cadre duquel un utilisateur présente une identité associée à des justificatifs d'identité particuliers et la revendique. Les systèmes d'authentification numérique reposent grandement sur les systèmes d'authentification axés sur les connaissances. Il s'agit souvent de noms d'utilisateur et de mots de passe. Or, un nombre croissant de plateformes en ligne mettent plutôt de l'avant l'authentification multifacteur, par exemple le recours à des jetons matériels. L'objectif du processus d'authentification consiste à valider les demandes légitimes et de rejeter toute tentative d'authentification malveillante.

1.3.1 FACTEURS D'AUTHENTIFICATION

Le facteur d'authentification fait référence à la propriété du paramètre servant à valider l'identité de l'utilisateur durant le processus d'authentification. Le tableau 1 décrit les différents facteurs d'authentification et leurs caractéristiques, et présente des exemples.

Tableau 1 : Facteurs d'authentification

Caractéristiques	Description	Exemples
Élément connu de l'utilisateur	Information que seul l'utilisateur légitime devrait savoir	Mot de passe, numéro d'identification personnel
Élément que possède un utilisateur	Objet physique que seul un utilisateur légitime traite et contrôle	Jeton matériel, téléphone cellulaire, signature numérique, clé privée, carte bancaire
Élément qui caractérise l'utilisateur	Attribut physique unique à chaque utilisateur	Empreinte digitale, rétine, visage, voix ou comportement, comme la vitesse de frappe

L'authentification multifacteur exige au moins deux facteurs d'authentification présentant des niveaux de caractéristique différents (p. ex. un élément connu de l'utilisateur et un élément qui caractérise l'utilisateur). De façon générale, l'authentification multifacteur améliore la sécurité du processus d'authentification. Bien que les codes d'authentification multifacteur distribués au moyen de technologies de téléphonie régulières (le service d'envoi de messages textes et les appels vocaux) soient encore largement utilisés, des auteurs de menace peuvent facilement les intercepter. En effet, pour accéder à un code d'authentification, ils peuvent recourir à des techniques d'attaque rudimentaires, par exemple en changeant le module d'identité d'abonné ou encore en lançant des attaques d'interception de communication de système de signalisation 7 (SS7) ou des attaques d'hameçonnage.

En fait, l'utilisation de facteurs d'authentification présentant des caractéristiques similaires ne constitue pas une authentification multifacteur. Par exemple, on considère qu'un mot de passe et une question de sécurité présentent une caractéristique similaire, étant donné qu'il s'agit de deux éléments connus de l'utilisateur. Deux facteurs présentant la même caractéristique peuvent être compromis de la même façon. Par exemple, un courriel d'hameçonnage ou un enregistreur de frappe peuvent aider un auteur de menace à trouver un mot de passe, une question de sécurité ou un numéro d'identification personnel. Pour voir une liste détaillée des types de jeton et leur description, consultez l'ITSP.30.031 v3 [1].

2 ATTAQUES LIÉES À L'AUTHENTIFICATION PAR MOT DE PASSE

Les attaques liées à l'authentification par mot de passe ont lieu lorsque des auteurs de menace tentent d'accéder en ligne ou hors ligne à un compte d'utilisateur au moyen de justificatifs d'identité légitimes sans toutefois détenir les autorisations requises. Lors d'attaques hors ligne, des auteurs de menace se servent d'outils pour percer des mots de passe, tandis que lors d'attaques en ligne, ils exploitent plutôt des contrôles d'authentification faibles sur des systèmes Web afin d'accéder sans autorisation à des comptes. Des auteurs de menace peuvent se servir de plusieurs mots de passe pour cibler un compte d'utilisateur ou employer un mot de passe pour cibler une base de données d'utilisateur complète.

De plus, sur les plateformes de nombreuses applications Web, on demande aux utilisateurs d'inscrire leurs adresses courriel comme noms d'utilisateur. Or, avec le temps, cette façon de faire peut pousser les utilisateurs a employé à répétition leurs noms d'utilisateur et leurs mots de passe sur différentes plateformes. En cas de compromission d'une paire de justificatifs d'identité employée sur une plateforme Web, des auteurs de menace peuvent y avoir recours sur d'autres plateformes.

2.1 MÉTHODES D'ATTAQUE DE MOT DE PASSE

Dans la présente section, nous passerons en revue des méthodes qu'emploient couramment des auteurs de menace dans le cadre d'attaques liées à l'authentification par mot de passe.

2.1.1 ATTAQUES PAR FORCE BRUTE

Lors d'une attaque par force brute, un auteur de menace essaie toutes les combinaisons de caractères possibles et tente de se connecter jusqu'à ce qu'il y parvienne. Des auteurs de menace peuvent lancer des attaques par force brute contre des systèmes hors ligne ou en ligne. Si une attaque vise une application en ligne, un auteur de menace cible un compte sur des systèmes Web qui ne limitent pas le nombre de requêtes ou qui n'offrent pas la protection par verrouillage de compte.

2.1.2 ATTAQUES PAR DICTIONNAIRE

Un auteur de menace a recours à une liste de mots de passe courants et tente de se connecter à un compte jusqu'à ce qu'il trouve une correspondance. Habituellement, des auteurs de menace essaient des mots de passe qui font partie des mots figurant dans les dictionnaires.

2.1.3 ATTAQUES PAR PULVÉRISATION DE MOTS DE PASSE

La pulvérisation de mots de passe est une variante d'une attaque par force brute menée en ligne. Durant ce type d'attaque, un auteur de menace essaie un petit nombre de mots de passe courants dans le but de se connecter à plusieurs comptes d'utilisateur. Il cible plusieurs comptes d'utilisateur afin d'éviter les contrôles de verrouillage de compte et les protections limitant le nombre de requêtes.

2.1.4 ATTAQUES PAR BOURRAGE D'IDENTIFIANTS

Une attaque par bourrage d'identifiants a lieu lorsque des auteurs de menace se basent sur une liste de combinaisons de noms d'utilisateur (souvent des adresses courriel) et de mots de passe pour s'authentifier sur une application Web. Autrement dit, des auteurs de menace utilisent des justificatifs d'identité acquis ailleurs et les entrent dans un système pour se connecter comme le feraient des utilisateurs autorisés.

Les pirates qui ont recours au bourrage d'identifiants tirent profit des habitudes qu'ont les utilisateurs d'opter pour les mêmes justificatifs d'identité pour différents comptes. Des pirates emploient des robots automatisés pour tenter de se connecter de manière consécutive à des comptes afin de valider une liste de justificatifs d'identité et relever les combinaisons qui fonctionnent. Des auteurs de menace peuvent en outre lancer des attaques par bourrage d'identifiants en faisant appel à des usines de piratage humain gérées par des groupes criminels dont l'objectif est d'imiter les comportements usuels des utilisateurs. En règle générale, des auteurs de menace utilisent des justificatifs d'identité obtenus dans le cadre de violations de données ou acquis de réseaux clandestins. Dans le cadre d'une attaque par bourrage d'identifiants avancée, des justificatifs d'identité sont jumelés à des données particulières sur un utilisateur, par exemple des renseignements sur sa naissance.

La protection contre une attaque par bourrage d'identifiants peut s'avérer très ardue. La vulnérabilité d'une application Web ne découle pas d'une violation de sécurité dans l'infrastructure de l'application en question; elle résulte plutôt de la réutilisation des mêmes justificatifs d'identité par les utilisateurs. Des administrateurs responsables de la sécurité des systèmes peuvent détecter une attaque en cours en surveillant les données relatives aux échecs d'authentification et en menant des analyses connexes. Dans la section 3, nous explorerons les mécanismes de contrôle de sécurité que vous pouvez adopter pour atténuer les attaques par bourrage d'identifiants et pour vous en protéger.

2.2 TYPES DE COMPTES COURAMMENT CIBLÉS

Les attaques par bourrage d'identifiants ciblent les types de comptes qui suivent :

- **Comptes d'utilisateur :** Il s'agit de comptes d'utilisateur auxquels on accède habituellement au moyen d'un nom d'utilisateur (souvent une adresse courriel) combiné à un mot de passe. La plupart des bases de données de justificatifs d'identité compromises consistent en des combinaisons d'adresses courriel et de mots de passe.
- **Comptes système :** Ces comptes sont associés à des processus, à des services ou à des dispositifs système. Le recours à des mots de passe faibles sur des dispositifs de l'Internet des objets (IdO) fait de ces dispositifs des cibles de choix. Des auteurs de menace prennent le contrôle de dispositifs IdO vulnérables qu'ils utilisent comme robots malveillants. Parmi les comptes système, on trouve aussi des comptes sur des dispositifs pare-feu ou réseau et des comptes associés à des services offerts sur des applications Web, comme des services de base de données.
- **Interface de programmation d'applications (API) :** La prolifération des services Web a conduit à l'augmentation de l'utilisation d'interfaces API. Des auteurs de menace ciblent des clés API, parce que les mécanismes de protection de compte, comme les jetons d'authentification multifacteur, sont habituellement désactivés.
- **Comptes d'identité fédérée :** Des auteurs de menace accordent une grande importance aux identités fédérées, comme les justificatifs d'identité à authentification unique, car elles permettent d'accéder facilement à plusieurs services. De nombreux déploiements infonuagiques s'effectuent sur des architectures hybrides et, afin de sécuriser

les communications entre ces systèmes, il est nécessaire de mettre en place une fédération d'identité. Des jetons d'authentification peuvent être partagés sur Internet lorsqu'une personne réussit à s'authentifier et que des demandes sont autorisées. Des auteurs de menace dotés de moyens sophistiqués peuvent alors recueillir des données de trafic réseau chiffrées et extraire les justificatifs d'identité du jeton au moyen de techniques cryptographiques avancées.

2.3 SOURCES COURANTES LIÉES À LA COMPROMISSION DE JUSTIFICATIFS D'IDENTITÉ

Des auteurs de menace comptent sur une variété de sources pour recueillir des justificatifs d'identité compromis. Ils peuvent se servir de données provenant des sources qui suivent :

- **Violation de données :** Lorsque des auteurs de menace réussissent à s'introduire dans des systèmes organisationnels, ils volent des bases de données comportant des justificatifs d'identité et affichent publiquement les données. Votre organisation peut surveiller les données qui ont fait l'objet d'une fuite de justificatifs d'identité et qui sont affichées publiquement. Elle pourra ainsi connaître les comptes qui ont été compromis sur sa plateforme. Elle doit toutefois confirmer auprès de son équipe juridique les possibles implications juridiques associées à ce genre d'opérations.
- **Internet clandestin :** Des auteurs de menace achètent des justificatifs d'identité compromis sur des marchés clandestins qui se spécialisent dans le domaine ou en acceptant des offres de vente à partir du réseau Tor. Certains de ces marchés exigent l'approbation de leur communauté avant qu'un utilisateur puisse y avoir accès. Votre organisation peut se prévaloir des services d'un fournisseur spécialisé en renseignement sur les menaces afin de détecter de façon proactive toute violation de justificatifs d'identité pouvant nuire à son personnel ou à sa clientèle.
- **Campagnes d'hameçonnage :** Des auteurs de menace mettent en œuvre des campagnes d'hameçonnage à grande échelle pour obtenir des justificatifs d'identité. Dans le cadre de ces campagnes, les pirates reproduisent votre image de marque et peuvent se servir de justificatifs d'identité compromis pour cibler vos systèmes. Vous pouvez par contre vous abonner à des services de protection de l'image afin de vous protéger contre les campagnes qui visent votre image de marque et avoir recours à des services de renseignement sur les menaces pour être au fait des campagnes d'hameçonnage actives qui visent votre marque ou votre secteur industriel.
- **Piratage psychologique :** Des auteurs de menace ont recours à des techniques de recherche de source ouverte afin de recueillir de l'information sur un compte d'utilisateur et de générer une liste de mots de passe. Des profils d'utilisateur publics (p. ex. des comptes de médias sociaux) peuvent révéler des noms d'utilisateur, des adresses courriel ou des renseignements personnels potentiels qui peuvent à leur tour donner des indices sur de possibles mots de passe.
- **Vulnérabilités sur des systèmes :** Des auteurs de menace peuvent exploiter des vulnérabilités sur des systèmes d'application Web afin d'accéder à des justificatifs d'identité.

3 PROTECTIONS CONTRE LES ATTAQUES PAR BOURRAGE D'IDENTIFIANTS

Il faut adopter une combinaison de mesures, notamment des approches fondées sur les risques et de défense en profondeur, pour se protéger contre des attaques par bourrage d'identifiants. Lorsqu'ils sont mis en place correctement, des mécanismes d'authentification multifacteur permettront de vous protéger contre des attaques par bourrage d'identifiants. Or, des auteurs de menace peuvent aussi exploiter d'autres vulnérabilités afin de contrer les protections découlant d'une authentification multifacteur. Nous vous recommandons ci-dessous des stratégies de contrôle de sécurité que votre organisation devrait envisager d'adopter pour se protéger contre ces attaques.

3.1 CONTRÔLES DE SÉCURITÉ PRINCIPAUX

La présente section décrit des contrôles de sécurité principaux. Nous recommandons à votre organisation de les appliquer afin qu'elle minimise les risques qu'elle court concernant les attaques liées à l'authentification par mot de passe. En fonction de l'environnement de votre organisation et des exigences en matière de sécurité, il se peut que vous deviez adapter ces contrôles et déterminer leur portée, ou penser à appliquer des contrôles de sécurité additionnels. Pour voir le catalogue complet des contrôles de sécurité, veuillez consulter l'annexe 3A de l'ITSG-33 [8].

3.1.1 MAINTIEN DE POLITIQUES DE SÉCURITÉ EFFICACES

Élaboration et mise en œuvre d'une politique en matière de mots de passe robustes

La politique en matière de mots de passe de votre organisation doit énoncer les principes régissant la création de mots de passe robustes que doivent suivre vos utilisateurs et vos développeurs d'applications Web. Cette politique doit inclure des exigences minimales en ce qui a trait à la composition et à la complexité des mots de passe des utilisateurs de votre système. Vous devez réviser régulièrement votre politique pour mettre à jour les directives; mettre en place des outils de système adaptés visant l'application de la politique; et remédier à toute violation de la politique. La politique doit en outre définir les exigences relatives aux contrôles de sécurité concernant le stockage et la gestion des mots de passe des utilisateurs. La liste présentée ci-dessous met de l'avant des éléments essentiels que votre organisation devrait inclure dans sa politique en matière de mots de passe :

- Autoriser l'utilisation de tous les types de caractère dans les mots de passe;
- Encourager l'authentification multifacteur, voire imposer son utilisation;
- Exiger l'utilisation d'un mot de passe unique pour chaque service;
- Vous assurer que les mots de passe sont conformes aux exigences liées à la composition et à la complexité des mots de passe, pour que les comptes ne soient pas compromis par des attaques;
- Encourager l'utilisation de phrases passe, car la longueur d'un mot de passe est possiblement plus importante que sa complexité;
- Empêcher l'utilisation de mots de passe courants sur votre plateforme;

- Conserver un dictionnaire hors ligne qui comporte un grand nombre de mots de passe courants et le configurer de sorte que les mots de passe en faisant partie soient rejetés;

- S'assurer régulièrement que les mots de passe des utilisateurs sont difficiles à deviner ou qu'ils ne sont pas compromis ni divulgués et, le cas échéant, aviser les utilisateurs concernés;
- Forcer un changement de mot de passe en cas de fuite ou d'activité malveillante;
- Décourager l'utilisation de renseignements associés à des adresses courriel comme noms d'utilisateur sur votre plateforme;
- Aviser les détenteurs de compte en cas de connexions ou d'événements de sécurité suspects ainsi que leur fournir la date et l'heure de leur dernière connexion;
- Activer la fonction de verrouillage de compte ou mettre en place des politiques visant à empêcher les tentatives de connexion automatique;
    - La politique de verrouillage devrait être expressément pour l'application Web, pas pour le compte Active Directory, car un auteur de menace pourrait verrouiller des comptes légitimes;
- Désactiver les comptes non utilisés ou les comptes d'invité, et renommer le compte administrateur par défaut pour qu'il soit difficile à deviner;
- Encourager le recours à des gestionnaires de mots de passe de bonne réputation visant la protection des mots de passe et la promotion d'une culture prônant les mots de passe complexes;
- S'assurer que les politiques en matière de mots de passe cadrent avec les dernières lignes directrices du GC, du Centre pour la cybersécurité et d'OWASP.

Activation des mécanismes d'authentification multifacteur

L'authentification multifacteur est l'une des mesures de protection les plus efficaces contre les attaques de compromission de mot de passe. Outre un mot de passe, les utilisateurs doivent fournir des facteurs d'authentification additionnels (p. ex. un élément qu'ils possèdent ou qui les caractérise). Ils peuvent par exemple présenter un jeton matériel, un certificat d'infrastructure à clé publique (ICP), une clé de sécurité numérique ou un élément biométrique, comme une empreinte digitale, comme deuxième facteur d'authentification.

L'authentification multifacteur offre une protection additionnelle si un auteur de menace connaît une combinaison valide de nom d'utilisateur et de mot de passe. Or, des attaques ciblées peuvent tout de même déjouer une authentification multifacteur, par exemple si la victime d'une attaque par hameçonnage donne tous les détails liés à son authentification dont a besoin un auteur de menace pour accéder à son compte. Pour se protéger contre ce type d'attaque, des propriétaires de système peuvent mettre en place des mécanismes de profilage de comportements à risque qui permettent de détecter des demandes de connexion malveillantes au moyen de justificatifs d'identité valides.

Autorisation donnée aux utilisateurs de créer et de modifier leurs noms de compte

L'utilisation d'adresses courriel comme noms d'utilisateur prévaut sur de nombreuses plateformes. Des auteurs de menace peuvent donc facilement trouver des justificatifs d'identité compromis qui sont affichés publiquement au moyen de ces

adresses courriel et de mots de passe potentiels. Le recours à des noms d'utilisateur uniques sur des plateformes Web offre des protections additionnelles contre des attaques par bourrage d'identifiants. Consultez les pratiques exemplaires présentées ci-dessous lorsque vous générez des identités d'utilisateur pour votre site Web :

- Permettre aux utilisateurs de créer des noms de compte uniques sur votre plateforme;
- Permettre aux utilisateurs de changer leurs noms de compte, au besoin;
- Permettre aux utilisateurs d'employer des caractères spéciaux dans leurs noms d'utilisateur;
- Générer des identifiants d'utilisateur uniques, si cette option est privilégiée.

Sensibilisation les utilisateurs et mise en place d'outils visant la prévention de pratiques risquées en matière de mots de passe

Vous devez sensibiliser les utilisateurs afin qu'ils créent des mots de passe complexes et qu'ils évitent leur réutilisation sur d'autres plateformes. De mauvaises pratiques en matière de mots de passe, comme leur réutilisation, accroissent en fait les risques liés aux attaques par bourrage d'identifiants. Vous devez aussi concevoir des outils à même votre système qui servent à détecter et à prévenir la réutilisation de mots de passe.

Même si votre application peut consigner les hachages d'anciens mots de passe aux fins de validation, il est à noter que ceci pourrait en fait accroître vos exigences de conformité et de protection des données. Vous devez donc mettre en œuvre les mesures de protection nécessaires pour sécuriser ces données.

Pour en savoir plus sur les pratiques exemplaires relatives à la génération de mots de passe sûrs, veuillez consulter ce qui suit :

- *ITSAP.30.032 Pratiques exemplaires de création de phrases de passe et de mots de passe* [10].

3.1.2 RENFORCEMENT DE VOS SYSTÈMES D'AUTHENTIFICATION

Renforcement de vos flux d'authentification et suppression d'algorithmes désuets

Vous devez sécuriser les voies d'authentification de votre application et détecter toute erreur de logique dans le flux d'authentification que peut exploiter un auteur de menace. Un problème courant est la divulgation d'informations sur l'état d'un compte dans des libellés de la rétroaction. Vous devez donc vous assurer que les messages d'erreur d'authentification ne révèlent pas l'existence ou l'inexistence d'un compte d'utilisateur. De plus, les délais de réponse d'exécution ne devraient pas différer et ne divulguer aucune information à l'utilisateur.

Si vous voulez renforcer votre flux d'authentification et supprimer tous les algorithmes désuets, vous devez vous servir de progiciels d'application de suivi dans votre système. Vous devriez également retirer tout progiciel vulnérable ou désuet. Vous ne devez jamais autoriser les utilisateurs à contourner une étape qui s'inscrit dans un processus d'authentification à plusieurs étapes. Vous devez en outre vous assurer de mettre en place des contrôles de gestion efficaces relatifs aux sessions.

Mise en œuvre de mesures visant la protection d'applications Web contre des exploits ciblant des vulnérabilités connus ou inconnus

Il est essentiel de protéger votre application Web contre des exploits connus ou inconnus. Des auteurs de menace peuvent lancer des exploits ciblés en se basant sur des vulnérabilités faisant partie de votre système, et ainsi accéder au répertoire de justificatifs d'identité de votre application. Des solutions comme des pare-feu pour applications Web et des mandataires d'applications Web peuvent atténuer les conséquences découlant de ce type d'attaque. Pour protéger les utilisateurs contre des attaques par injection, vous devez appliquer des techniques de validation d'entrée, en recourant par exemple à des requêtes paramétrées ou à des procédures stockées. Vous pouvez également envisager d'appliquer le mécanisme Strict Transport Security (HSTS) au protocole de transfert hypertexte (HTTP), afin d'obliger les navigateurs Web à accéder à votre application par l'intermédiaire du protocole HTTPS, plutôt que du protocole HTTP (texte en clair). L'application du mécanisme HSTS permet de se protéger contre des attaques par interception de session.

Mise en place de pratiques de gestion et de stockage sécurisées de justificatifs d'identité

Vous devez renforcer les protections associées aux coffres-forts de mots de passe afin de limiter les violations de données. Bien que des violations de données puissent se produire, votre organisation devrait concevoir ses systèmes d'application Web en y ajoutant des protections de sorte à empêcher les auteurs de menace d'accéder facilement à des justificatifs d'identité. Parmi les recommandations concernant la gestion sécurisée de votre coffre-fort de mots de passe, comptons les suivantes :

- Y conserver uniquement des copies de mot de passe chiffrées ou hachées; n'y consigner aucune donnée liée à des mots de passe en texte en clair;
- Utiliser du sel et poivre cryptographique pour sécuriser les mots de passe et accroître leur complexité;
- Recourir à des modules de sécurité matériel ou à des coffres-forts secrets pour conserver les clés de chiffrement en toute sécurité;
- Examiner régulièrement les applications pour y retirer les algorithmes de chiffrement faibles qui sont employés.

Nous vous recommandons de consulter le document *Application Security Verification Standard 4.0* [4] d'OWASP pour obtenir des détails sur la conception sécurisée de l'infrastructure d'authentification de votre application Web.

Déploiement de contrôles limitant le nombre de tentative de connexion, comme le test complètement automatisé de Turing qui permet aux ordinateurs de différencier les ordinateurs des humains (CAPTCHA)

Les mécanismes dynamiques visant à limiter le nombre de requêtes et à ralentir artificiellement le trafic sont efficaces pour prévenir les attaques d'authentification automatisées à grande échelle. Vous pouvez adopter des mécanismes de sécurité, comme le test CAPTCHA, la limitation dynamique du nombre de requêtes et un avertissement de l'expiration du délai prévu, pour réduire ou bloquer les attaques de script. Nous savons depuis longtemps que les contrôles CAPTCHA ont des répercussions négatives sur l'expérience des utilisateurs, mais les récentes avancées en technologie ont amélioré grandement les choses. L'intégration de fonctions d'analyse comportementale et la réalisation de tests CAPTCHA en arrière-plan sans qu'il y ait d'interaction humaine en sont des exemples. Dans la majorité des mises en œuvre, on suggère d'activer les contrôles CAPTCHA à la lumière des comportements observés (p. ex. des connexions suspectes, des hausses

vertigineuses des taux d'activités ou des comportements connus des robots). Des attaques sophistiquées peuvent toutefois contourner des contrôles CAPTCHA.

Vous pouvez songer à adopter des politiques de verrouillage pour empêcher toute attaque sérieuse. Sachez toutefois que des verrouillages peuvent involontairement engendrer des attaques par déni de service distribué ciblant des utilisateurs légitimes. Vous pouvez aussi penser à mettre en place des politiques de verrouillage de compte basées sur le risque ou le temps afin de réduire les conséquences sur les utilisateurs légitimes.

3.1.3 BLOCAGE DES INDICATEURS D'ATTAQUE CONNUS

Blocage des requêtes provenant de sources malveillantes connues

Vous devez bloquer les requêtes de service provenant de sources malveillantes déjà connues. Selon le cas d'utilisation, songez à bloquer de manière permanente les adresses de protocole Internet (IP) associées à des activités malveillantes. Déployez des solutions de gestion de robots automatisées pour qu'elles bloquent le trafic qui correspond aux signatures connues des robots.

Étant donné que les auteurs de menace changent souvent d'infrastructure, le recours à des sources de renseignement sur les menaces peut améliorer les contrôles que vous avez mis en place. Pour obtenir de l'information sur les utilisateurs qui visitent votre application, basez-vous sur la réputation des IP et faites appel aux services de renseignement sur les menaces. Pour certaines applications, pensez à mettre en place des listes de rejet qui bloqueront toute source suspecte pendant une période définie plutôt qu'en permanence. Vous pouvez aussi songer à mettre en place des contrôles de géoblocage des réseaux pour les applications Web qui ne présentent pas de cas d'utilisation en dehors d'une certaine région géographique et appliquer des blocages permanents pour le trafic associé à des régions qui sont connues pour réaliser des activités malveillantes. Les requêtes d'accès provenant de l'extérieur d'une région peuvent être gérées dans le cadre d'un processus d'autorisation.

Surveillance des violations de justificatifs d'identité visant la détection de justificatifs compromis

Vous devez adopter de façon proactive une solution de surveillance des violations de justificatifs d'identité qui vous permettra de détecter les justificatifs compromis qui sont employés sur votre plateforme. Pour ce faire, vous pouvez opter pour une solution interne ou vous prévaloir des services d'un fournisseur tiers. Chacun des deux modèles sélectionnés présente toutefois des risques. Le maintien d'ensembles de justificatifs d'identité additionnels à cette fin présente des exigences de conformité supplémentaires et pourrait rendre votre système attrayant pour les pirates. Les solutions provenant de fournisseurs tiers supposent la communication des données liées aux mots de passe (partiellement ou totalement), ce qui soulève des enjeux relatifs à la vie privée. Vous devriez verrouiller tous les comptes qui sont associés à des justificatifs d'identité compromis et demander à l'utilisateur touché de revérifier son compte et de configurer un nouveau mot de passe. Pour en savoir plus, veuillez consulter le document *NIST SP 800-63B* [2].

Suivi et blocage de comportements malveillants connus

Les auteurs de menace optent pour des navigateurs robotisés et des outils de script pour automatiser des connexions à grande échelle. Il vous est possible de repérer ces outils et de les relier aux activités de l'utilisateur. Vous pourrez ainsi prendre des décisions concernant le blocage d'activités en vous basant sur la dynamique. Votre application Web peut bloquer des requêtes suspectes provenant d'agents de navigateur malveillants. Vous pouvez en outre classer les comportements malveillants détectés sur votre plateforme pour créer des déclencheurs et bloquer à l'avenir les activités correspondantes.

Les solutions de gestion de robots constituent des options à évaluer lorsque vous songez à mettre en place une solution intégrée qui comprend une analyse dynamique et des protections actives contre les menaces. La gestion de robots est une stratégie vous permettant de filtrer les robots qui peuvent accéder à vos actifs Web. La gestion de robots est basée sur une variété de technologies de sécurité, d'apprentissage machine et de développement Web, et permet l'évaluation adéquate des robots et le blocage d'activités malveillantes tout en laissant les robots légitimes mener leurs activités.

Utilisation de technologies de détection d'anomalies permettant le blocage d'activités suspectes

Compte tenu de la sophistication et de la portée prises en charge par de nombreuses applications Web, le recours à des solutions de détection peut vous aider à repérer les connexions suspectes et à les bloquer. Vous pouvez attribuer des cotes de risque aux requêtes des utilisateurs au moyen de solutions d'analyse comportementale qui permettent de vérifier les mouvements des souris, les glissements sur les écrans et les habitudes de frappe. Les résultats relatifs aux cotes de risque qui ne s'inscrivent pas dans les comportements attendus déclencheront des contrôles de sécurité. Une activité malveillante est bloquée lorsque la cote qui lui a été attribuée dépasse le seuil fixé. Vous pouvez opter pour une analyse des statistiques ou de la fréquence afin de signaler et de prévenir l'utilisation de mots de passe faibles sur votre plateforme.

3.1.4 SERVICES D'AUTHENTIFICATION MODERNES

Services d'authentification fédérée en ligne

Grâce à des services Web d'authentification fédérée, comme Connexion Canada, la CléGC, OpenID Connect et d'autres services d'authentification similaires, des plateformes peuvent offrir des options vous permettant d'authentifier en toute sécurité vos utilisateurs. Les services de fédération permettent à votre application de recourir à un service d'authentification d'un fournisseur tiers grâce auquel vous pouvez identifier les utilisateurs sur votre plateforme. Vous pouvez ainsi réduire les coûts, les complexités et les restrictions associés à la gestion d'une solution d'authentification interne. La réalisation de plusieurs projets d'identité numérique est en cours au GC et au sein de gouvernements provinciaux canadiens. Ces projets visent à encourager l'emploi et l'acceptation d'une fédération et d'identités numériques de confiance.

Les services d'identités fédérées posent toutefois des risques de sécurité potentiels. Par exemple, un événement de sécurité touchant la plateforme d'un fournisseur de services pourrait avoir un effet domino sur votre application Web et empêcherait donc les utilisateurs d'accéder à votre application Web. De plus, les services fédérés pourraient exposer les utilisateurs concernés à des risques en matière de protection de la vie privée et de confidentialité des renseignements personnels. Dans le cadre de la plupart des mises en œuvre, ces services externes sont offerts à titre d'options d'authentification, et des mécanismes de substitution aux infrastructures d'authentification pris en charge à l'interne sont en place.

Solutions sans mot de passe

Le recours à des solutions sans mot de passe augmente. Des applications Web permettent à des utilisateurs de se connecter au moyen d'une solution d'authentification sans mot de passe qui est basée sur une combinaison de clés de sécurité physique, de données biométriques, de certificats cryptographiques et de caractéristiques de dispositif physique. À l'instar de la plupart des recommandations formulées, les solutions sans mot de passe ne s'appliquent pas à tous les cas d'utilisation. Cette solution peut être préférable pour les applications Web auxquelles on accède par l'intermédiaire d'un dispositif ou d'un réseau de confiance. Dans d'autres cas d'utilisation, cette solution peut être appliquée pour valider une requête d'un utilisateur en cas d'activité suspecte détectée. L'authentification Web W3C (WebAuthn) est un exemple d'une norme qui encourage l'emploi de solutions sans mot de passe dans les applications Web. Pour en savoir plus sur les spécifications de la WebAuthn, consultez le document *Web Authentication: An API for accessing Public Key Credentials Level 1 [11]*.

Lorsqu'une décision doit être prise concernant des solutions d'authentification, n'oubliez pas que certaines d'entre elles pourraient soulever des préoccupations importantes en matière de vie privée (p. ex. la biométrie) et exiger l'application de mesures additionnelles pour garantir la protection adéquate de la vie privée.

3.1.5 EXAMEN CONTINU DES LIENS DE CONFIANCE LIÉS À VOTRE APPLICATION

Mise en œuvre de mécanismes continus d'authentification et de cotes de risque liés aux activités

Vous devez structurer votre application en partant du principe que des compromissions de justificatifs d'identité auront lieu. Concevez votre application Web de sorte à pouvoir évaluer en continu les actions des utilisateurs sur le système et à exiger une réauthentification en cas d'événements présentant des risques élevés. Un auteur de menace peut tirer profit d'une attaque d'hameçonnage réussie pour obtenir un mot de passe et un code multifacteur permettant un accès initial. En exigeant une réauthentification lors de certaines actions effectuées dans l'application, votre application minimise les conséquences de cette attaque.

Vous pouvez en outre joindre une cote de risque pour chacune des actions d'un utilisateur. Si la cote de risque générale est inférieure au seuil prévu, des requêtes de réauthentification s'affichent. Parmi les scénarios pouvant faire l'objet d'une évaluation menant à une réauthentification, on trouve les suivants : première utilisation d'un dispositif, changements de l'état d'un dispositif, changements d'un profil utilisateur, changements du rôle et des droits d'utilisateur et opérations administratives.

Utilisation des attributs du dispositif visant l'authentification et l'autorisation d'actions

Vous pouvez vous servir des attributs du dispositif comme données additionnelles afin de sécuriser le processus de connexion et d'autoriser les requêtes des utilisateurs. Des attributs réseau, comme des données de géolocalisation, peuvent également se révéler utiles. Sachez toutefois que des attributs réseau peuvent facilement être trafiqués ou contournés au moyen de mandataires Web ou de réseaux privés virtuels. Les identifiants sur les dispositifs d'accès peuvent servir à valider l'authentification et à déterminer les services dont dispose l'utilisateur. Des flux de validation de sécurité additionnels peuvent être exigés lorsqu'un nouveau dispositif est détecté. Il est possible de connaître les empreintes d'un dispositif ou d'une source grâce à certaines mesures, notamment les suivantes :

- le recours à des fonctions de configuration ou à des dispositifs physiques (p. ex. la taille de l'écran, les paramètres liés à la langue, les paramètres liés aux fuseaux horaires);
- l'utilisation d'une chaîne d'agent utilisateur relatif à un navigateur Web ou d'informations sur des plugiciels installés;
- l'emploi d'informations liées à un dispositif réseau, comme l'adresse d'un contrôle d'accès au support ou l'identifiant d'un dispositif Bluetooth;
- l'utilisation de données liées à un système mondial de localisation découlant du dispositif local ou le recours à des services de renseignement de géolocalisation anti-mystification;
- la création d'un témoin persistant sur le dispositif aux fins de détection future;
- le recours aux services d'un fournisseur tiers responsable de valider l'état d'un dispositif.

En général, l'information découlant d'empreintes côté client n'est pas digne de confiance. Les utilisateurs peuvent déployer des outils pour prévenir la collecte d'informations ou trafiquer les données pour tromper l'application Web. Vous devriez tenir compte des résultats liés aux empreintes côté client et les déployer avec d'autres contrôles.

3.2 AUTRES CONSIDÉRATIONS

3.2.1 CONTEXTE JURIDIQUE

Choix des solutions en fonction du contexte juridique du lieu d'exploitation

Dans certains endroits, des solutions proposées pourraient malencontreusement aller à l'encontre de contraintes juridiques. Vous devriez ainsi évaluer les répercussions juridiques associées aux solutions choisies. Votre organisation devrait comprendre la manière dont les contrôles qu'elle pense appliquer pourraient influencer les utilisateurs, les exigences juridiques et les risques en matière de vie privée.

Les ministères et organismes du GC doivent consulter la *Loi sur la protection des renseignements personnels* [12] et mener une évaluation des facteurs relatifs à la vie privée avant de mettre en place des solutions ou des changements. Si votre organisation n'est pas un organisme fédéral, veuillez consulter la *Loi sur la protection des renseignements personnels et les documents électroniques* [13], qui régit les règles de base quant à la gestion des renseignements personnels par les organisations privées, ou les lois sur la protection de la vie privée provinciales qui s'appliquent, le cas échéant.

Dans certains cas, vous devez mener vos opérations en fonction des règles qui s'appliquent à d'autres endroits géographiques. Si votre service Web reçoit des données de citoyens européens, vous devez respecter le *Règlement général sur la protection des données* [14]. Discutez avec votre équipe juridique pour vous assurer de bien comprendre les effets de votre empreinte opérationnelle.

4 CONCLUSION

La mise en œuvre d'une authentification multifacteur permettra de contrer une grande majorité d'attaques par bourrage d'identifiants. Certains contrôles usuels, comme le filtrage de réseaux malveillants ou le blocage d'agents de navigateur malveillants, deviennent largement inefficaces contre les nouvelles techniques employées. Des méthodes d'authentification modernes offriront des options à prendre en considération. Pour protéger votre organisation contre des attaques par bourrage d'identifiants, veuillez penser à adopter les techniques suivantes :

- le renforcement de vos flux d'authentification;
- la suppression d'algorithmes désuets;
- le blocage de demandes provenant de sources malveillantes connues;
- la surveillance des violations de justificatifs d'identité visant la détection de justificatifs compromis;
- l'utilisation de technologies de détection d'anomalies permettant le blocage d'activités suspectes.

L'architecture et le besoin opérationnel de votre application Web seront essentiels à la sélection des solutions. Une approche polyvalente vous offrira une protection optimale.

5 CONTENU COMPLÉMENTAIRE

5.1 ABRÉVIATIONS, ACRONYMES ET SIGLES

Forme abrégée	Expression au long
API	Interface de programmation d'applications (*application protocol interface*)
CAPTCHA	Test de Turing complètement automatisé permettant aux ordinateurs de différencier les ordinateurs des humains *(completely automated public Turing test to tell computers and humans apart)*
DDoS	Attaques par déni de service distribué (*distributed denial of service*)
GC	Gouvernement du Canada
HSTS	*Hypertext Transfer Protocol Strict Transport Security*
HTTP	Protocole de transfert hypertexte (*hypertext transfer protocol*)
HTTPS	Protocole de transfert hypertexte sécurisé (*hypertext transport protocol secure*)
IdO	Internet des objets
IP	Protocole Internet (*Internet protocol*)
TI	Technologies de l'information
NIST	*National Institute of Standards and Technology*
OWASP	*Open Web Application Security Project*
ICP	Infrastructure à clé publique
SP	Publication spéciale (NIST) *(Special Publication [NIST])*
SS7	Système de signalisation 7
RPV	Réseau privé virtuel
WebAuthn	*W3C Web Authentication*

5.2 Glossaire

Termes	Définitions
Interfaces de programmation d'applications	Fonction de bibliothèque ou point d'accès du système présentant une syntaxe bien définie, qui est accessible à partir de programmes d'application ou d'un code utilisateur et qui permet d'obtenir une fonctionnalité bien définie.
Authentification	Processus ou mesure permettant de vérifier l'identité d'un utilisateur.
Limitation dynamique du nombre de requêtes	Contrôles dynamiques servant à limitant le nombre de requêtes envoyées ou reçues par un serveur Web.
Identité fédérée	Processus permettant l'acheminement de l'information sur l'identité et l'authentification entre les systèmes.
Hypertext Transfer Protocol Strict Transport Security (HSTS)	Politique d'accès à un site Web qui informe les agents utilisateurs qu'ils devraient uniquement accéder au site Web au moyen du protocole HTTPS. La politique aide à protéger les sites Web contre les attaques par écoute clandestine.
Confirmation de l'identité	Processus de collecte, de validation et de vérification de l'information sur l'identité d'un utilisateur visant l'établissement des justificatifs permettant l'accès à un système.
Authentification multifacteur	Processus visant à vérifier l'identité d'un utilisateur au moyen de différents mécanismes, dont un élément connu de l'utilisateur, un élément que l'utilisateur possède ou un élément qui caractérise l'utilisateur.
Hameçonnage	Procédé par lequel une tierce partie tente de solliciter de l'information confidentielle appartenant à une personne, à un groupe ou à une organisation en usurpant ou en imitant une certaine marque généralement bien connue dans le but d'obtenir habituellement des gains financiers. Les hameçonneurs incitent les utilisateurs à donner leurs renseignements personnels (numéros de cartes de crédit, données bancaires ou autres renseignements sensibles) afin de s'en servir pour commettre des actes frauduleux.
Texte en clair	Information non chiffrée.
Infrastructure à clé publique	Architecture, organisation, techniques, pratiques et procédures qui appuient collectivement l'exploitation d'un système cryptographique à clé publique fondé sur un certificat.
Système de signalisation 7 (SS7)	Système de signalisation international servant à gérer les transferts de données sur des dispositifs cellulaires.
Réseau privé virtuel (RPV)	Réseau de communication privé généralement utilisé au sein d'une entreprise 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 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, que pourrait exploiter un auteur de menace en vue de compromettre les biens ou les activités d'une organisation.

5.3 RÉFÉRENCES

Numéro	Référence
1	Centre canadien pour la cybersécurité. *ITSP.30.031 v3 – Guide sur l'authentification des utilisateurs dans les systèmes de technologie de l'information*.
2	National Institute of Standards and Technology. *NIST SP 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management*. Juin 2017.
3	National Institute of Standards and Technology. *NIST SP 800-95 Guide to Secure Web Services*. Août 2007.
4	*Open Web Application Security Project*. *OWASP Application Security Verification Standard 4.0.2*. Octobre 2020.
5	National Institute of Standards and Technology. *NIST SP 800-63-3 Digital Identity Guidelines*. Juin 2017.
6	National Institute of Standards and Technology. *NIST SP 800-63A Digital Identity Guidelines: Enrollment and Identity Proofing*. Juin 2017.
7	National Institute of Standards and Technology. *NIST SP 800-63C Digital Identity Guidelines: Federation and Assertions*. Juin 2017.
8	Centre canadien pour la cybersécurité. *La gestion des risques liés à la sécurité des TI : une méthode axée sur le cycle de vie (ITSG-33)*. Novembre 2012.
9	Janca, Tanya. *Alice and Bob Learn Application Security*. Novembre 2020. (Ressource papier).
10	Centre canadien pour la cybersécurité. *ITSAP.30.032 – Pratiques exemplaires de création de phrases de passe et de mots de passe*. Septembre 2019.
11	W3C. *Web Authentication: An API for Accessing Public Key Credentials Level 1*. Mars 2019.
12	Canada. Ministère de la Justice. *Loi sur la protection des renseignements personnels*.
13	Canada. Ministère de la Justice. *Loi sur la protection des renseignements personnels et les documents électroniques*.
14	Union européenne. *Règlement général sur la protection des données*.