Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

La sécurité du Wi-Fi

PRATICIEN

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 31 mars 2022.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1.	Première version.	31 mars 2022

ISBN 978-0-660-42810-9
CAT D97-3/80-002-2022F-PDF

VUE D'ENSEMBLE

Le Wi-Fi est partout : dans votre café du coin, dans votre domicile et au travail. Alors que les organisations dépendent de plus en plus du Wi-Fi, il convient de porter davantage attention au contexte de la sécurité des réseaux sans fil afin de réduire les risques posés par les cybermenaces. Le présent document est destiné aux organisations des secteurs public et privé de toutes tailles qui utilisent le Wi-Fi.

La présente vise à sensibiliser les lecteurs aux vulnérabilités qui se trouvent dans les réseaux qui utilisent ou aspirent à utiliser le Wi-Fi. Il est important de tenir compte de la sécurité du Wi-Fi comme partie intégrante de la sécurité du réseau et de l'infrastructure, puisqu'elle permet d'effectuer des tâches essentielles qui comprennent souvent de l'information sensible et confidentielle (p. ex. des secrets commerciaux, de l'information nominative [PII] et du matériel assujetti au droit d'auteur). La sécurité d'un réseau est équivalente à son maillon le plus faible et le Wi-Fi est une cible facile dont les auteurs de menace peuvent tirer avantage.

La présente comporte des sections correspondant aux stratégies, aux contrôles techniques et aux mesures de sécurité recommandés par le Centre pour la cybersécurité, ainsi que de plus amples points à considérer pour assurer la sécurité dans l'ensemble du réseau.

TABLE DES MATIÈRES

1. SENSIBILISATION AUX MENACES QUI PÈSENT SUR LE WI-FI

Les premières étapes à suivre pour sécuriser votre réseau consistent à vous sensibiliser aux menaces, à identifier les risques et à corriger les vulnérabilités connues qui sont associées à un réseau mal sécurisé. La présente section aborde les risques courants qui pèsent sur les réseaux sans fil et fournit de l'information sur la façon de reconnaître les changements organisationnels qu'il est possible d'apporter pour réduire les risques.

1.1 SENSIBILISATION AUX ATTAQUES RÉSEAU

Au moment de sécuriser le Wi-Fi, il est important de reconnaître les menaces qui pèsent sur votre réseau sans fil et les mesures à prendre pour les atténuer.

Micrologiciels non corrigés : Les micrologiciels non corrigés peuvent rendre votre réseau sans fil vulnérable aux brèches de sécurité. Les auteurs de menace peuvent tirer avantage des micrologiciels auxquels les plus récentes versions n'ont pas été appliquées. Assurez-vous que votre organisation a mis en place une stratégie d'application des correctifs qui prévoit la mise à jour régulière de tous les micrologiciels de dispositifs, y compris les points d'accès et les contrôleurs.

Paramètres par défaut non sécurisés : Plusieurs dispositifs sans fil sont livrés avec des paramètres par défaut non sécurisés, comme des noms d'utilisateurs et des mots de passe connus, des ponts reliant des ports réseau ou des réseaux locaux virtuels (VLAN pour *Virtual Local Area Network*), des règles de pare-feu qui autorisent tout le trafic et la désactivation de l'isolation des clients sur les points d'accès. Pour corriger les faiblesses, il est très important de changer les noms d'utilisateur et les mots de passe par défaut sur votre réseau Wi-Fi pour des clés robustes et uniques. Vous pourrez ainsi renforcer la sécurité de tous les paramètres des dispositifs réseau.

Réseaux partagés : La répartition des tâches ou des rôles (p. ex. invités et employés) sur le réseau devrait donner lieu à une séparation des espaces réseau au moyen de mesures d'isolation des clients, de VLAN, de commutateurs et de règles de pare-feu. Segmentez votre réseau en zones de sécurité afin d'atténuer ces risques et de réduire la surface d'attaque pour les auteurs de menace.

Après avoir séparé vos utilisateurs en des zones de sécurité de réseau différentes, vous devriez également séparer les réseaux câblés et sans fil en des segments distincts pour chaque division. Il sera ainsi possible de prévenir les attaques sur votre réseau sans fil et d'empêcher les auteurs de menace d'obtenir un accès direct aux dispositifs et aux clients câblés dans la mesure où votre pare-feu et votre matériel réseau sont configurés de manière à bloquer un tel accès. Par exemple, si votre réseau invité et votre réseau d'employés sont séparés l'un de l'autre, vous devriez diviser chacune de ces zones en réseaux câblés et sans fil. Cela mènera à la mise en place de quatre zones : deux zones Wi-Fi et deux zones câblées.

Dispositifs de l'Internet des objets (IdO) : Les dispositifs de l'IdO sont souvent utilisés dans les petites entreprises et bureaux à domicile (SOHO pour *Small Office Home Office*) et dans les petites et moyennes entreprises (PME). Ces dispositifs posent d'importants risques à la sécurité en raison d'une mauvaise conception de la sécurité et de l'absence de mises à jour logicielles et micrologicielles. Dans la mesure du possible, il conviendra d'éviter de tels dispositifs ou de les mettre en œuvre dans un réseau séparé.

Piratage Wi-Fi (*wardriving*) ou attaque menée depuis le parc de stationnement (*parking lot attack*) : Le piratage Wi-Fi est une pratique qui consiste à créer un centre de reconnaissance mobile (et parfois, un centre d'attaque). Il peut s'agir d'une

camionnette équipée d'outils d'analyse sans fil (p. ex. un analyseur de spectre, des antennes de réception puissantes et hautement directionnelles, de l'équipement informatique mobile) ou d'un simple portable, téléphone cellulaire ou tablette. Le piratage Wi-Fi n'est pas toujours utilisé à des fins malveillantes, mais plutôt comme moyen de relever les facteurs de risques courants pour les utilisateurs et les organisations. Les attaques menées depuis le parc de stationnement (en anglais, *parking lot attack*) sont plus ciblées et concernent généralement davantage qu'une simple écoute des signaux sans fil. La zone d'attaque ciblée peut se trouver à l'extérieur des contrôles de sécurité conventionnels, comme des barrières, des portes sécurisées ou des systèmes de caméras de sécurité. La force du signal devrait être limitée de manière à éviter à ce que les auteurs de menace puissent mener des attaques sans fil sur votre réseau alors qu'ils conduisent, marchent ou sont assis à proximité de vos installations.

Vol d'appareils : L'utilisation des dispositifs ou des modules Wi-Fi n'est pas toujours limitée à un lieu, puisque ces derniers sont conçus pour être mobiles et faciles à manipuler. Cela pose des risques additionnels, puisque le vol devient dès lors une possibilité. Par exemple, on retrouve souvent des ampoules intelligentes dans des lieux publics et celles-ci peuvent contenir les informations d'accès au réseau sans fil. Des auteurs de menace pourraient attaquer ces ampoules pour ensuite se connecter au réseau sans fil au moyen de ces informations d'accès. Certains dispositifs, comme les téléphones ou les tablettes, peuvent contenir des données sensibles (p. ex. des renseignements personnels sensibles) et sont plus faciles à voler qu'un ordinateur portable. Aucun dispositif facile à dérober contenant de l'information sensible ou des informations d'accès ne devrait être laissé sans surveillance dans un lieu non approuvé sans être verrouillé ou sécurisé.

Points d'accès indésirables : On retrouve fréquemment ces dispositifs dans les environnements Wi-Fi publics comme les cafés, les restaurants et les aires publiques avec Wi-Fi. Les attaquants mettront souvent en place des dispositifs tentant de se faire passer pour un réseau fiable. Lorsque vous cherchez les réseaux disponibles (ou que votre dispositif le fait automatiquement), vous pourriez vous authentifier sur un point d'accès sans fil indésirable malveillant. Vous devez toujours vous assurer de vous connecter au bon réseau Wi-Fi et d'utiliser des techniques de communication chiffrées.

Une autre tactique consiste à mystifier des réseaux Wi-Fi d'entreprise. Un invité ayant accès à l'organisation peut faire appel à la mystification pour déployer un point d'accès malveillant dans une zone environnante.

Ces attaques peuvent donner lieu à des fuites de données et à des accès non autorisés.

Authentification faible : Il n'est pas recommandé aux organisations d'utiliser des clés prépartagées (PSK pour *Pre-Shared Key*), puisqu'elles ne permettent pas d'authentifier les utilisateurs étant donné qu'ils utilisent tous la même phrase de passe. Il est donc impossible de déterminer qui a utilisé la phrase de passe ou s'il s'agit d'un accès légitime. Il est très important de mettre en place une stratégie de mot de passe avec l'utilisation de la norme WPA-Entreprise (*Wi-Fi Protected Access*), puisqu'elle permet de veiller à ce que les mots de passe soient suffisamment longs et complexes pour éviter qu'ils ne soient facilement compromis.

Algorithmes de chiffrement faibles : L'utilisation d'algorithmes de chiffrement faibles ou désuets peut fournir aux auteurs de menace des moyens de compromettre votre réseau sans fil. L'attaquant peut employer différents outils sans fil pour compromettre le système sans avoir à se connecter physiquement aux périphériques du réseau pour l'exploiter. Prière de consulter l'ITSP.40.062, *Conseils sur la configuration sécurisée des protocoles réseau* [1] et l'ITSP.40.111, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* [2] pour les algorithmes qu'il convient d'utiliser.

1.2 EXEMPLES D'INTRUSIONS

En 2015, une menace du jour zéro (c.-à-d., une vulnérabilité matérielle ou logicielle sans correctif disponible) touchant les routeurs ANTLabs InnGate a été découverte (CVE-2015-0932). Bien que la vulnérabilité ait été corrigée rapidement après sa découverte, elle a donné lieu à une intrusion dans 277 hôtels, centres des congrès et centres de données différents. Ce routeur était généralement déployé sur les réseaux utilisés par plusieurs hôtels ou autres réseaux offrant un accès invité.

Cette menace du jour zéro permettait aux attaquants de prendre le contrôle du routeur et d'installer un maliciel afin de lancer des attaques sur les systèmes connectés et de contrôler l'ensemble des réseaux câblés et sans fil auxquels se connectent les invités.

Un autre exemple d'intrusion a eu lieu en 2015. WeWork, une société immobilière commerciale, a vu son réseau Wi-Fi compromis en raison de la sécurité inadéquate des autres locataires de l'édifice. N'importe qui pouvait payer 25 $ pour accéder à une salle de conférence et au réseau Wi-Fi, procéder au balayage du réseau et obtenir de l'information sensible sur les nombreuses entreprises utilisant le réseau. Ce problème n'était pas limité à ce seul édifice, puisque plusieurs édifices de WeWork utilisaient la même PSK. Il en a résulté un important incident de sécurité ayant touché des dossiers personnels, comme des permis de conduire, des passeports, des demandes d'emploi, des justificatifs d'identité de comptes bancaires, des dossiers de santé d'entrepreneurs, etc. [3]

Entre janvier et juin 2021, Kaspersky a fait rapport de 1,51 milliard d'intrusions visant des dispositifs de l'IdO, une augmentation par rapport aux 639 millions d'incidents signalés en 2020. En règle générale, ces attaques faisaient appel au protocole Telnet qui autorise l'administration à distance des dispositifs à partir de l'interface de ligne de commande. Elles ont été perpétrées dans le but de mener des attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*) et du cryptominage, ou d'atteindre d'autres cibles plus prisées sur le réseau. La pandémie mondiale a été marquée par une plus grande utilisation des dispositifs d'IdO, les rendant plus attrayants pour les auteurs de menace. [4]

Dans le cas d'Eduroam, un réseau Wi-Fi gratuit utilisé par plusieurs universités européennes, on a relevé une mauvaise configuration du protocole EAP (*Extensible Authentication Protocol*) susceptible de mener à une attaque par hameçonnage au point d'accès dans le cadre de laquelle les attaquants simulent le réseau de manière à tromper les dispositifs et les pousser à se connecter au moyen réseau. Comme certains systèmes d'exploitation (SE) ne valident pas le certificat au moment de se connecter à un système, cette situation aurait pu mener au vol des informations d'identification utilisées pour se connecter au Wi-Fi. Selon cette configuration, on aurait dû utiliser la version 2 du protocole d'authentification par défi-réponse (MSCHAPV2 pour *Challenge Handshake Authentication Protocol version 2*) plutôt que le protocole d'authentification PAP (*Password Authentication Protocol).* [5]

2 PRATIQUES EXEMPLAIRES

2.1 STRUCTURES DE DONNÉES

Les approches structurelles à la sécurité permettent de s'assurer que les ressources sont configurées de manière à faciliter l'approvisionnement, la maintenance et l'adoption de la sécurité tout en veillant à ce que les utilisateurs puissent accéder aux données sensibles dont ils ont besoin. Sans structure, vos données peuvent être placées n'importe où et il n'y a aucune distinction entre les données contenant de l'information sensible et les données publiques.

2.1.1 LIMITATION DE L'INFORMATION DISPONIBLE

L'information sensible (p. ex. les données classifiées, confidentielles, personnelles ou exclusives à l'entreprise) ne devrait pas être transmise par l'intermédiaire de réseaux ouverts sans la mise en place de contrôles de chiffrement additionnels. Les auteurs de menace peuvent s'asseoir à proximité et intercepter les communications sur le réseau. Il est important de mettre en place le droit d'accès minimal pour veiller à ce que chaque utilisateur de l'organisation ne puisse accéder qu'aux fichiers et aux ressources dont il a besoin dans le cadre de son travail.

Pour de plus amples renseignements sur la limitation de l'information sensible, prière de consulter l'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) [6].

2.1.2 STRUCTURATION DES CLASSES DE DONNÉES

Structurer les classes de données permet de veiller à ce que les données sensibles ne sortent jamais de la zone mise en place pour assurer leur protection et de limiter les dommages advenant une fuite de données ou une atteinte à la vie privée. Les données devraient être structurées de manière à répondre aux besoins de l'organisation en matière de sécurité et de protection de la vie privée et à assurer la sécurité des renseignements personnels et confidentiels. Vous trouverez ci-dessous un exemple de méthode de structuration de ces classes.

Classe 1 : Données publiques

Cette classe de données est utilisée pour définir les données accessibles au public. Le traitement de ces données en interne ou en externe ne porte pas atteinte à l'entreprise, aux clients, au personnel ou aux fournisseurs. Parmi les exemples de données publiques, on retrouve les pages Web publiques, les brochures et les cartes professionnelles de l'organisation.

Classe 2 : Données réservées à une utilisation interne

Ce type de données ne doit être utilisé qu'au sein de l'organisation par le personnel autorisé. Les données réservées à une utilisation interne contiennent de l'information légèrement sensible au sujet des opérations de l'organisation, ses politiques et ses plans d'activités. Les notes de service et les courriels de nature professionnelle en sont des exemples. La divulgation de ces données à des personnes non autorisées poserait un risque minimal pour l'entreprise.

Classe 3 : Données confidentielles

Ces données, qui se limitent à un groupe particulier au sein de l'organisation, exigent un niveau d'habilitation spécial ou des autorisations claires pour ce qui est de leur utilisation et de leur accès. Les données confidentielles peuvent contenir de

l'information nominative qui risque de causer des dommages considérables pour l'organisation, les employés et les parties concernées advenant sa compromission. En règle générale, ces données sont protégées en vertu des dispositions stipulées dans les lois régissant le respect de la vie privée dans les secteurs privé et public (c.-à-d., la *Loi sur la protection des renseignements personnels et les documents électroniques* [LPRPDE]) et les Normes de sécurité des données de l'industrie des cartes de paiement (PCI-DSS pour *Payment Card Industry Data Security Standard)*. Elles pourraient également être régies par l'Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM) ou l'Association canadienne des courtiers de fonds mutuels (MFDA pour *Mutual Fund Dealers Association*) du Canada. Parmi les exemples de données confidentielles, on retrouve les données commerciales exclusives, les données de recherche, le code source d'un logiciel et l'information nominative.

2.1.3 STRUCTURATION DE VOS RÉSEAUX WI-FI ET CÂBLÉS

Les dispositifs Wi-Fi vous permettent de configurer plusieurs identificateurs SSID (*Service Set Identifier*). Chaque identificateur SSID devrait avoir son propre VLAN pour limiter l'accès aux zones internes du réseau et des mesures de sécurité avancées (p. ex. la structuration du réseau) devraient être mises en place. Méfiez-vous des paramètres par défaut qui permettent à tout le trafic de transiter entre les identificateurs SSID ou les VLAN. Pour de plus amples renseignements à ce sujet, prière de consulter la sous-section 2.3.2 sur les contrôles techniques associés aux identificateurs SSID et aux VLAN.

Si votre organisation permet à ses visiteurs d'accéder à un réseau Wi-Fi invité lorsqu'ils se trouvent dans votre édifice, limitez la période durant laquelle ils pourront utiliser le mot de passe d'invité (p. ex. expiration quotidienne du mot de passe ou remise de laissez-passer d'invités) pour garantir que seuls les invités sur place peuvent accéder au réseau.

Pour de plus amples renseignements sur l'établissement de zones dans les réseaux, prière de consulter l'ITSG-38, *Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones* [7].

2.2 PRATIQUES EXEMPLAIRES AXÉES SUR LES STRATÉGIES ET LES POLITIQUES

Les politiques et stratégies écrites doivent refléter entièrement votre position sur la sécurité et la protection des renseignements personnels. Les contrôles techniques mettent en œuvre ce qui a été publié dans la politique ou stratégie écrite. Les contrôles techniques qui ne sont pas associés à une politique ou stratégie écrite ne sauraient résister aux contestations judiciaires. Vous trouverez aux sections suivantes différentes politiques et stratégies qui ont une influence sur la sécurité de votre réseau Wi-Fi et vos activités.

2.2.1 POLITIQUE D'UTILISATION ACCEPTABLE

Ce type de politique permet de clarifier de quelle façon il est possible d'utiliser un service, un réseau, un système ou un site Web. Elle a pour objet de limiter la responsabilité juridique de l'organisation et d'offrir aux utilisateurs une bonne compréhension de ce qui est une bonne ou mauvaise utilisation. Cette politique devrait comprendre les classes d'accès Web autorisées. Certaines catégories de sites Web peuvent attirer l'attention sur votre organisation et accroître le risque global. Cette politique devrait être combinée à des contrôles techniques qui permettent de faciliter son application (p. ex. un service de filtrage Web sur un pare-feu).

2.2.2 STRATÉGIE PRENEZ VOS APPAREILS PERSONNELS (PAP)

Si votre organisation autorise le modèle Prenez vos appareils personnels (PAP), on recommande de mettre en place une stratégie PAP. Celle-ci devrait appliquer des restrictions additionnelles aux dispositifs utilisés dans un environnement PAP. Elle doit également être applicable et vérifiable. Tout ce qui ne peut être appliqué ou vérifié au moyen des contrôles techniques devrait être considéré comme des risques qui pèsent sur l'organisation. La stratégie PAP devrait définir ce qui suit :

- le processus de validation des autorisations pour les applications et les données;
- les précautions de sécurité minimales qu'il convient de prendre;
- les classes de données stockées sur un dispositif;
- l'intention d'offrir ce mode de connexion au sein de l'organisation;
- la bonne façon de rejeter, de copier et de synchroniser les données;
- les exigences relatives au type de dispositif ou au chiffrement des applications;
- les pratiques exemplaires qu'il convient d'adopter pour sécuriser les opérations.

2.2.3 STRATÉGIE DE CHIFFREMENT ET DE SÉCURITÉ DES DONNÉES

La stratégie de chiffrement et de sécurité des données devrait déterminer les données qu'il convient de chiffrer, les algorithmes de chiffrement acceptables et les paramètres que l'organisation considère comme étant « sécurisés ». Elle devrait aborder le chiffrement des supports amovibles, les données au repos et les données en transit. Cette stratégie devrait également définir la norme à adopter selon la classe de données en question.

2.2.4 STRATÉGIE DE GOUVERNANCE DES DONNÉES

La stratégie de gouvernance des données devrait définir la procédure de conservation des données, les méthodes de destruction acceptables et le cycle de vie général des données selon leur classe. Elle devrait également établir les exigences en matière de résidence des données et les contrôles à mettre en place.

2.2.5 STRATÉGIE DE MOT DE PASSE

Une stratégie de mot de passe devrait définir les exigences liées à la sécurisation des mots de passe et leur utilisation au sein de l'organisation. Dans les environnements à faible sensibilité, il convient de considérer l'adoption de pratiques exemplaires minimales. Dans les environnements à sensibilité élevée (p. ex. les secteurs des finances et de la santé), les exigences devraient inclure des mesures à sécurité élevée. Cette stratégie devrait également déterminer qui peut réinitialiser ou changer les mots de passe et comment les justificatifs d'identité seront stockés en toute sécurité. En règle générale, le Centre pour la cybersécurité ne recommande pas d'utiliser la fonction d'expiration et de réutilisation des mots de passe.

Pour de plus amples renseignements sur les pratiques exemplaires en matière de mots de passe et de phrases de passe, prière de consulter l'ITSAP.30.032, *Pratiques exemplaires de création de phrases de passe et de mots de passe* [8].

2.2.6 STRATÉGIE D'APPLICATION DES CORRECTIFS

La stratégie d'application des correctifs définit l'équipement qui fera l'objet de correctifs et la fréquence à laquelle les correctifs seront appliqués dans l'environnement. Parmi les exemples de systèmes qui devraient être régis par la stratégie d'application des correctifs, on retrouve les dispositifs mobiles, les systèmes d'exploitation (SE) des ordinateurs, les applications, les antimaliciels, les logiciels antihameçonnage et l'équipement réseau. La stratégie d'application des correctifs devrait comprendre les calendriers relatifs aux mises à jour régulières à appliquer sur les micrologiciels de tous les dispositifs, les points d'accès et les contrôleurs. Elle devrait définir qui est le personnel autorisé à procéder à l'application des correctifs, le plan de restauration à mettre en œuvre advenant l'échec des mises à jour et qui doit être informé d'un tel échec (dans les délais impartis).

2.2.7 STRATÉGIE DU WI-FI PUBLIC

La stratégie du Wi-Fi public devrait être une stratégie dédiée ou une mention dans une autre stratégie (p. ex. une stratégie sur les communications réseau et TI) qui définit l'utilisation appropriée des réseaux Wi-Fi publics (p. ex. un café, un hôtel ou un réseau non géré). Cette stratégie pourrait exiger que l'organisation chiffre toutes les données en transit, limite l'accès aux classes de données confidentielles ou prenne les précautions nécessaires pour éviter que des auteurs de menace accèdent à ses données sensibles.

2.3 PRATIQUES EXEMPLAIRES AXÉES SUR LES CONTRÔLES TECHNIQUES

Des contrôles techniques devraient être mis en place pour prévenir les incidents de sécurité et assurer l'intégrité des données en misant sur un accès sûr et sécurisé. Sans contrôle technique, les données qui se trouvent sur les dispositifs des utilisateurs peuvent être interceptées, falsifiées ou compromises de façon involontaire ou malveillante.

2.3.1 CHIFFREMENT DU WI-FI ET PSK PAR RAPPORT AU PROTOCOLE EAP

Chiffrement

Au moment de choisir une méthode de chiffrement du Wi-Fi, il convient de faire appel à une méthode compatible avec tous vos dispositifs et votre équipement réseau.

Protocole WEP (Wired Equivalent Privacy) : Le protocole WEP peut facilement être compromis. Il a recours à l'algorithme de chiffrement RC4 (Rivest Cipher 4) (c.-à-d., un algorithme de chiffrement en continu) pour assurer la confidentialité et à un contrôle de redondance cyclique (CRC32) (c.-à-d., un algorithme de somme de contrôle) pour assurer l'intégrité.

WPA1 : Forme de chiffrement relativement robuste qui utilise l'algorithme RC4 avec le protocole TKIP (*Temporal Key Integrity Protocol*) (c.-à-d., un protocole de chiffrement). On considère que la norme WPA1 n'est pas une méthode de chiffrement suffisamment sécurisée pour le traitement de l'information sensible d'entreprise. Par conséquent, son utilisation n'est pas recommandée.

WPA2 : Forme de chiffrement robuste du Wi-Fi qui est largement utilisée sur les réseaux. Il convient d'éviter la norme WPS (*Wi-Fi Protected Setup*) si on utilise la norme WPA2 pour accroître la sécurité. La norme WPA2 fait appel à la norme de

chiffrement avancée (AES pour *Advanced Encryption Standard*) de 128 bits pour le chiffrement et au protocole CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) pour accroître le niveau de protection.

WPA3 : Nouvelle forme plus sécurisée de chiffrement du Wi-Fi qui fait appel à la norme AES de 192 bits en mode Entreprise et de 128 bits en mode Personnel. Le cas échéant, ce protocole devrait être utilisé pour tous les nouveaux déploiements.

PSK par rapport au protocole EAP

La PSK est l'un des moyens les plus souvent utilisés pour sécuriser les réseaux Wi-Fi personnels ou des PME. Toutefois, bien qu'il soit facile de la mettre en œuvre, la PSK n'est pas recommandée dans un environnement d'entreprise en raison de ses fonctionnalités limitées en matière de gestion de l'identité et d'audit. La PSK utilise une phrase de passe pour sécuriser le réseau sans fil et chiffrer le trafic. Cette méthode propose une grande utilisabilité et peut être configurée avec un minimum de soutien. Par contre, une fois que l'on donne le mot de passe à quelqu'un, la seule façon de l'empêcher de se connecter est de changer la PSK, ce qui a une incidence sur la connectivité des utilisateurs jusqu'à la saisie d'une nouvelle phrase de passe. Il faut alors mettre à jour tous les dispositifs, y compris ceux des non-utilisateurs comme les imprimantes sans fil, afin d'appliquer le nouveau mot de passe ou la nouvelle phrase de passe. Les petites entreprises peuvent se tourner vers le protocole LEAP (*Lightweight Extensible Authentication Protocol*) et le protocole d'authentification par défi-réponse de Microsoft PEAP-MS-CHAP (*Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol*). Dans le cas des grandes entreprises, le protocole EAP-TLS (*Extensible Authentication Protocol Transport Layer Security*) est le protocole le plus sécurisé qu'il est possible de mettre en œuvre. S'il est impératif d'utiliser la PSK, il conviendra alors de séparer les invités, le personnel, l'équipement informatique et les dispositifs de l'IdO en différents identificateurs SSID et d'utiliser des phrases de passe uniques pour chaque VLAN et segment de réseau.

Le protocole EAP est souvent utilisé dans les moyennes et grandes entreprises pour assurer la connectivité sans fil. Cette méthode permet d'utiliser un nom d'utilisateur et un mot de passe pour authentifier chaque dispositif, en plus de certificats basés sur le protocole de sécurité de la couche transport (TLS pour *Transport Layer Security).* La pratique la plus sécurisée serait d'utiliser des certificats TLS avec le protocole EAP. Il serait ainsi possible de désactiver l'accès de chaque dispositif pour une plus grande visibilité des utilisateurs connectés au réseau Wi-Fi. Cette méthode fait en sorte qu'il est plus difficile pour les attaquants de s'introduire sur le réseau. Combiner l'authentification unique (SSO pour *Single Sign-On*) au protocole PEAP-MS-CHAPV2 rend le processus plus facile, puisqu'il est possible de s'authentifier à partir d'un répertoire et de réduire le nombre de justificatifs d'identité dont les utilisateurs doivent se souvenir. Le PEAP-MSCHAPV2 est un protocole PEAP qui permet aux utilisateurs de saisir des justificatifs d'identité qui sont alors validés par le serveur du Service d'usager commuté à authentification distante (RADIUS pour *Remote Authentication Dial-In User Service)* par l'entremise d'un tunnel chiffré au moyen du protocole EAP.

2.3.2 VLAN ET IDENTIFICATEURS SSID

L'identificateur SSID est parfois appelé « nom de réseau Wi-Fi » ou « nom de réseau ». Il vous permet de voir et d'identifier le réseau Wi-Fi auquel vous voulez vous connecter. N'ajoutez jamais d'information nominative ou de données confidentielles dans le nom ou la description d'un identificateur SSID. Sur des réseaux personnels ou de petites entreprises, on utilise souvent un ou deux identificateurs SSID (p. ex. un réseau pour les employés et un pour les invités).

Les VLAN permettent d'intégrer des réseaux virtuels dans la même infrastructure physique. La plupart des commutateurs et pare-feux gérés prennent en charge l'établissement et l'utilisation de VLAN. Vous devriez également combiner les VLAN à des identificateurs SSID pour créer des zones de sécurité distinctes au sein de votre réseau.

Séparez le trafic sans fil du trafic câblé en utilisant un VLAN distinct de tout le trafic câblé, puis configurez l'identificateur SSID en conséquence. L'accès des utilisateurs invités devrait être séparé du VLAN restreint. Tous les points d'accès et les identificateurs SSID devraient permettre d'activer l'isolation des clients afin d'éviter qu'ils échangent les uns avec les autres. D'autres dispositifs, comme les imprimantes et les dispositifs de l'IdO, peuvent ne pas prendre en charge le protocole WPA-EAP en raison de contraintes de coûts. Ils devraient être placés sur un réseau sécurisé distinct qui est isolé des réseaux des employés et des invités. Ne permettez pas aux utilisateurs d'accéder à ces réseaux et assurez-vous de les verrouiller avec un mot de passe très robuste.

2.3.3 RADIUS

RADIUS fait appel au protocole EAP pour créer un système d'authentification sécurisé permettant d'utiliser un serveur RADIUS à partir d'un point d'accès ou du contrôleur d'un point d'accès. Vous devez vous assurer que le serveur RADIUS exige que l'authentification et la connexion des dispositifs s'effectuent au moyen d'un secret sécurisé. Le secret est équivalent à une phrase de passe. Les mises à jour doivent être appliquées aux logiciels installés sur les points d'accès, le contrôleur des points d'accès et le serveur RADIUS. De plus, les comptes doivent être gérés attentivement.

Plusieurs serveurs RADIUS se connectent également à un répertoire aux fins de l'authentification SSO (généralement à Active Directory [AD] ou à un service d'annuaire en nuage).

2.3.4 SÉCURITÉ DE RÉPERTOIRE

Les points d'accès sans fil, le contrôleur et le serveur RADIUS sont importants, mais les justificatifs d'identité sont validés par le répertoire. Il est important d'utiliser un contrôle d'accès basé sur les rôles (RBAC pour *Role-Based Access Control*) et de veiller à ce que les stratégies de sécurité physiques et de cybersécurité nécessaires soient en place pour sécuriser le service d'annuaire. En règle générale, on utilise AD comme répertoire pour authentifier les utilisateurs qui utilisent la SSO. Le serveur d'annuaire doit être sécurisé dans son intégralité, y compris le SE, les applications, les services, les comptes, les autorisations, les micrologiciels et le matériel.

2.3.5 RÉSEAUX PRIVÉS VIRTUELS (RPV)

RPV publics : On les utilise généralement pour protéger la vie privée des personnes ou masquer le point d'origine dans un réseau Wi-Fi public. Ils ne devraient jamais être utilisés pour des connexions d'entreprise. Il peut être difficile de savoir à quel fournisseur on peut se fier, puisque vous pourriez ne pas avoir les ressources nécessaires pour vérifier la sécurité ou l'infrastructure d'un service public, et ces services s'exécutent souvent sur des serveurs situés dans des pays qui ne sont pas régis par des lois strictes en matière de protection des données et de la vie privée. Les fournisseurs de RPV publics peuvent également ne pas vérifier les antécédents du personnel technique qui a accès aux données non chiffrées, ainsi qu'aux coordonnées et à l'information de paiement des clients.

RPV d'entreprise : On recommande de mettre en place un RPV d'entreprise lorsqu'il est nécessaire de se connecter à des ressources organisationnelles par l'entremise d'un réseau non géré (p. ex. un réseau d'invité ou un Wi-Fi public). Les RPV d'entreprise permettent à votre dispositif de créer un tunnel chiffré vers le réseau de l'entreprise et de sécuriser les données en transit. Même si un attaquant écoute sur le réseau, il ne sera pas en mesure de comprendre les données qui le traversent, puisqu'elles sont transmises dans un tunnel chiffré.

2.3.6 NORME WPS

La norme WPS permet de se connecter facilement à un réseau. En règle générale, cette fonction est offerte sur l'équipement SOHO. Elle permet de se connecter à un point d'accès sans fil en appuyant sur un bouton, sans avoir à taper de mot de passe. On la retrouve sur les réseaux chiffrés avec la norme WPA uniquement. Les versions modernes de cette fonction exigent la saisie d'un NIP de six chiffres, ce qui permet de contourner la nécessité d'entrer un mot de passe pour se connecter au réseau sans fil. Dans un environnement d'entreprise, il convient de désactiver cette fonction sur tout l'équipement sans fil, puisqu'elle n'est pas sécurisée.

2.3.7 SÉCURITÉ DES POINTS TERMINAUX

Tout point d'entrée à un réseau sans fil est un potentiel vecteur d'attaque. S'assurer que tous les points terminaux sont sécurisés permet d'atténuer les risques. Des logiciels de gestion des appareils mobiles (MDM pour *Mobiles Device Management*) peuvent être utilisés comme contrôle pour identifier les utilisateurs des appareils mobiles et faciliter la configuration et le déploiement du Wi-Fi, du RPV et des configurations des jetons d'authentification sur les dispositifs.

Pour de plus amples renseignements sur la sécurité générale des points terminaux, prière de consulter l'ITSP.70.012, *Conseils sur le renforcement de la sécurité de Microsoft Windows 10 Enterprise* [9].

Pour de plus amples renseignements sur la sécurité générale des dispositifs mobiles, prière de consulter l'ITSAP.00.001, *Utiliser son dispositif mobile en toute sécurité* [10].

Pour assurer la sécurité de votre Wi-Fi, il convient de sécuriser vos dispositifs PAP pour toute utilisation au sein de l'organisation et de mettre en place des stratégies et des contrôles techniques.

2.3.8 SÉCURITÉ PHYSIQUE

La sécurité physique est tout aussi importante que la cybersécurité. Elle réduit les risques qu'une personne arrive à réinitialiser physiquement les dispositifs pour s'y connecter au moyen des justificatifs d'identité par défaut, à se connecter au réseau câblé d'un dispositif sans fil ou à se connecter à de l'équipement sans fil pour voler les justificatifs d'identité. Si un dispositif fait l'objet d'une réinitialisation aux paramètres d'usine, il peut exposer l'ensemble de votre sous-réseau (qui est configuré pour assurer la jonction des dispositifs ou contrôleurs sans fil) à quiconque se connecte au réseau par défaut.

Un attaquant peut également installer un dispositif d'écoute clandestine entre le réseau et le dispositif câblé ou sans fil. Ces produits sont offerts en ligne et permettent aux attaquants d'accéder au trafic réseau afin de mener une attaque de l'intercepteur (PiTMA pour *Person-in-the-Middle Attack)*. Ces dispositifs peuvent également être utilisés pour injecter du code malveillant dans le trafic en transit ou offrir aux attaquants un accès à distance au moyen d'un tunnel RPV inversé.

La sécurité des infrastructures sans fil doit avoir pour objectif de prévenir l'accès physique aux composants sans fil (p. ex. les ampoules de l'IdO connectées au Wi-Fi) et aux composants qui permettent d'établir une connexion par le biais du réseau câblé.

2.3.9 SYSTÈME DE DÉTECTION D'INTRUSION SANS FIL (WIDS)

Les systèmes de détection d'intrusion sans fil (WIDS pour *Wireless Intrusion Detention System*) et les systèmes de prévention d'intrusion sans fil (WIPS pour *Wireless Intrusion Prevention System*) sont conçus pour détecter et possiblement atténuer les attaques actives qui sont menées en exploitant les radiofréquences (RF) émises. Combinés aux outils et aux mesures de protection mis en place sur le réseau câblé, les outils de surveillance sans fil peuvent aider à sécuriser votre infrastructure sans fil en surveillant les radiofréquences. Les points d'accès indésirables sont un cas d'utilisation où le WIDS et le WIPS peuvent faciliter la localisation et la désactivation des points d'accès non autorisés qui sont connectés au réseau câblé. Par points d'accès indésirables, on entend les points d'accès connectés au réseau d'une organisation qui ne sont pas autorisés et fournis par celle-ci. Ils peuvent causer des problèmes sur le plan de la sécurité, puisqu'ils peuvent employer des techniques de chiffrement et d'authentification inadéquates (voire aucune) et empêcher l'organisation de savoir quels dispositifs sont connectés au réseau et où ils le sont.

La mise en œuvre d'un WIDS ou d'un WIPS peut aider à écourter le temps de connexion de ces dispositifs au réseau dans la mesure où ils pourraient passer inaperçus indéfiniment en l'absence de tels systèmes. Certains WIDS et WIPS sont intégrés aux points d'accès et utilisent les radiofréquences de deux façons : ils peuvent servir de clients et écouter le trafic généré par les RF ou encore faire office de capteurs et fonctionner en mode de surveillance. Souvent, ces applications à double usage réduisent le temps de disponibilité ou la bande passante pour les utilisateurs du point d'accès, puisque le système ne peut utiliser qu'un seul mode à la fois (le mode de surveillance ou celui permettant d'envoyer et de recevoir les points d'accès).

2.4 PRATIQUES EXEMPLAIRES AXÉES SUR LA FORMATION

La formation doit être obligatoire pour tous les employés, nouveaux et actuels. Il est ainsi possible de veiller à ce qu'ils soient au courant des nouvelles menaces et des changements apportés aux politiques. Toute personne qui se connecte à vos réseaux sans fil devrait savoir comment reconnaître les réseaux sans fil mystifiés, comprendre la distinction entre les différents réseaux Wi-Fi déployés par votre organisation et la raison pour laquelle ils ont été déployés, connaître les types d'utilisations qui sont autorisés sur chaque identificateur SSID et segment du VLAN et savoir comment se connecter correctement à chacun des réseaux sans fil. Les utilisateurs devraient également être au courant des processus à suivre pour signaler les incidents de sécurité associés au sans-fil, des personnes-ressources à qui communiquer de tels signalements et de la façon d'obtenir du soutien en la matière.

2.4.1 FORMATION GÉNÉRALE SUR LES TI

La formation générale sur les TI pose les bases de la sécurité des dispositifs sans fil. Elle permet d'améliorer le travail dans le domaine de la cybersécurité et de sensibiliser les membres du personnel sur la cybersécurité personnelle qu'ils sont tenus d'assurer lorsqu'ils utilisent des dispositifs sans fil. D'importants sujets devraient être abordés, notamment les systèmes

disponibles, les classes de données gérées, le cycle de vie des données, les autorisations accordées aux utilisateurs finaux et les politiques relatives à l'utilisation du Wi-Fi et des ressources réseau.

Les utilisateurs devraient avoir accès aux guides opérationnels et aux procédures sur la meilleure façon d'interagir avec les systèmes et les données en toute sécurité. Ces procédures devraient être passées en revue et mises à jour régulièrement pour tenir compte des révisions logicielles et des changements apportés à la structure.

2.4.2 UTILISATION DE DISPOSITIFS

L'organisation devrait offrir de la formation sur les normes du sans-fil et l'utilisation des dispositifs. Former les utilisateurs sur la façon de sécuriser leurs propres dispositifs peut avoir une incidence positive sur la culture et la sécurité de l'organisation. Organiser des séances d'information pour démontrer les changements apportés aux paramètres en adoptant une approche pratique permettra d'ajouter de la variété et de retenir l'attention des apprenants plus visuels.

2.4.3 COURS SUR LA SÉCURITÉ DU WI-FI

Plusieurs cours sur la sécurité sont offerts en ligne et peuvent vous aider à parfaire vos connaissances générales en matière de sécurité du Wi-Fi. Misez sur les cours destinés aux utilisateurs moyens. Cette formation devrait aborder des sujets comme les pratiques exemplaires à adopter pour les réseaux Wi-Fi non chiffrés et publics, les RPV et les dispositifs mobiles. Elle devrait également traiter de l'importance qu'il convient d'accorder aux signes de compromission des dispositifs et des étapes à suivre pour remédier à la situation.

3 AUTRES FACTEURS À CONSIDÉRER

3.1 RÉPERCUSSIONS SUR LE PLAN JURIDIQUE

Tenez-compte des répercussions de vos politiques et de vos exigences sur le plan juridique avant de les mettre en œuvre. Il importe de mentionner qu'il ne s'agit pas d'un avis juridique. Veuillez vous adresser à un avocat pour vous assurer que vous respectez bien toutes les lois canadiennes.

L'utilisation d'équipement personnel (p. ex. des appareils PAP ou domestiques) pourrait avoir des répercussions sur le plan juridique. Avant d'autoriser un testeur de pénétration à effectuer des tests sur votre réseau, veillez à établir des limites claires, à limiter la portée des tests à des zones en particulier et à vous assurer qu'il est digne de confiance en vérifiant ses références et sa réputation au sein de l'industrie.

3.2 SOUTIEN TECHNIQUE ACCRU

La mise en place des contrôles techniques illustrés dans le présent document exigera du soutien technique additionnel. Les utilisateurs pourraient rencontrer des obstacles qui les empêchent d'effectuer leurs tâches comme ils ont l'habitude de le faire. Avant de mettre en place de plus amples contrôles de sécurité, il pourrait être nécessaire d'apporter des changements à la configuration de certains dispositifs et d'effectuer des étapes supplémentaires. Il est essentiel de protéger vos données et de veiller à ce que vous ayez les ressources nécessaires pour répondre aux questions plus techniques.

3.3 DISPONIBILITÉ

La disponibilité est un facteur important dont il faut tenir compte. Sans l'authentification ou la disponibilité de l'infrastructure réseau, les utilisateurs ne peuvent pas accéder aux ressources dont ils ont besoin. Dans le cas des infrastructures essentielles, il convient d'envisager la possibilité d'offrir une disponibilité élevée et la reprise après sinistre. Plusieurs points d'accès peuvent être déployés dans des zones avoisinantes pour fournir une couverture par échelon advenant une panne.

Les signaux sans fil sont susceptibles de faire l'objet d'attaques par brouillage et on ne peut garantir leur disponibilité. Il est important de considérer l'utilisation d'une infrastructure de réseau câblé robuste à laquelle pourront se connecter les dispositifs essentiels, ainsi que la séparation des réseaux câblés et sans fil. Cette configuration permet de s'assurer qu'il est possible d'isoler les attaques visant les réseaux sans fil et de déconnecter la source de ces attaques du réseau câblé au besoin.

4 RÉSUMÉ

Il est essentiel de mettre en place les politiques appropriées en matière de réseaux Wi-Fi, d'implémenter les contrôles techniques nécessaires pour appliquer vos politiques et stratégies, et de fournir la formation adéquate à votre personnel.

Le portrait du sans-fil évolue constamment alors que s'ajoutent des dispositifs intelligents avec Wi-Fi intégré. Le contexte des cybermenaces n'a jamais été aussi vaste. Sécuriser votre réseau et rester à l'affût des menaces permettra de protéger l'environnement de votre organisation pour les années à venir.

5 CONTENU COMPLÉMENTAIRE

5.1 LISTE DES ABRÉVIATIONS

Terme	Définition
AD	Active Directory
AES	Norme de chiffrement avancée (*Advanced Encryption Standard*)
API	Interface de programmation d'applications (Application Programming Interface)
CCMP	Protocole CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*)
DDoS	Attaque par déni de service distribué (*Distributed Denial of Service*)
EAP	Protocole EAP (*Extensible Authentication Protocol*)
IdO	Internet des objets
LEAP	Protocole LEAP (*Lightweight Extensible Authentication Protocol*)
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
MDM	Gestion des appareils mobiles (*Mobile Device Management*)
MFDA	Association canadienne des courtiers de fonds mutuels (*Mutual Fund Dealers Association*)
MSCHAPV2	Protocole d'authentification par défi-réponse version 2 de Microsoft (*Microsoft Challenge Handshake Authentication Protocol version 2*)
NIP	Numéro d'identification personnel
OCRCVM	Organisme canadien de réglementation du commerce des valeurs mobilières
PAP	Prenez vos appareils personnels
PAP	Protocole d'authentification PAP (*Password Authentication Protocol*)
PCI DSS	Normes de sécurité sur les données de l'industrie des cartes de paiement (*Payment Card Industry Data Security Standard)*
PEAP	Protocole PEAP (*Protected Extensible Authentication Protocol*)
PEAP-MS-CHAP	Protocole d'authentification par défi-réponse PEAP de Microsoft (*PEAP Microsoft Challenge Handshake Authentication Protocol*)
PII	Information nominative (*Personally Identifiable Information*)
PiTMA	Attaque de l'intercepteur (*Person-in-the-Middle-Attack*)
PME	Petites et moyennes entreprises
PSK	Clé prépartagée (*Pre-Shared Key*)
RADIUS	Service d'usager commuté à authentification distante (*Remote Authentication Dial-In User Service*)
RBAC	Contrôle d'accès basé sur les rôles (*Role-Based Access Control*)
RC4	Algorithme de chiffrement RC4 (*Rivest Cipher 4*)
RF	Radiofréquences
RPV	Réseau privé virtuel
SE	Système d'exploitation
SOHO	Petite entreprise et bureau à domicile (*Small Office Home Office*)
SSID	Identificateur SSID (*Service Set Identifier*)

Terme	Définition
SSO	Authentification unique (*Single Sign-On*)
STI	Sécurité des technologies de l'information
TKIP	Protocole TKIP (*Temporal Key Integrity Protocol*)
TLS	Protocole TLS (*Transport Layer Security*)
VLAN	Réseau local virtuel (*Virtual Local Area Network*)
WEP	Protocole WEP (*Wired Equivalent Privacy*)
WIDS	Système de détection d'intrusion sans fil (*Wireless Intrusion Detection System*)
Wi-Fi	Technologie Wi-Fi (*Wireless Fidelity*)
WIPS	Système de prévention d'intrusion sans fil (*Wireless Intrusion Prevention System*)
WPA	Norme WPA (*Wi-Fi Protected Access*)
WPS	Norme WPS (*Wi-Fi Protected Setup*)

5.2 GLOSSAIRE

Terme	Définition
Attaque par déni de service distribué (DDoS)	Attaque dans le cadre de laquelle plusieurs systèmes compromis sont utilisés pour attaquer une cible en particulier. Le flux de messages envoyés est tel qu'il provoque une panne du système ciblé, ce qui empêche les utilisateurs légitimes d'y accéder.
Authentification	Processus ou mesure permettant de vérifier l'identité d'un utilisateur.
Chiffrement	Transformation de données d'un format vers un autre pour cacher leur contenu et empêcher un accès non autorisé.
Confidentialité	Aptitude à protéger de l'information sensible pour en empêcher l'accès à des personnes non autorisées.
Droit d'accès minimal	Principe selon lequel on n'accorde à l'utilisateur que les autorisations d'accès dont il a besoin pour accomplir les tâches autorisées. Ce principe limite les dommages pouvant résulter d'une utilisation non autorisée, incorrecte ou accidentelle d'un système d'information.
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).
Information nominative (PII)	Toute information permettant d'identifier une personne qui est consignée dans un formulaire.
Intégrité	Aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles et inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. Elle s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Internet des objets (IdO)	Réseau de dispositifs Web courants capables de se connecter les uns aux autres et d'échanger de l'information.
Menace	Événement ou acte délibéré, accidentel ou naturel pouvant éventuellement porter préjudice aux actifs et à l'information de TI.
Prenez vos appareils personnels (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 l'organisation, elle a peu d'emprise sur les contrôles de sécurité mis en place sur le 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.

Terme	Définition
Wi-Fi	Technologie sans fil qui permet de connecter des dispositifs, comme des portables et des téléphones intelligents, à Internet. Le Wi-Fi utilise les ondes radio et un routeur sans fil plutôt qu'une connexion câblée physique.

5.3 RÉFÉRENCES

Numéro	Référence
1.	*Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062) – https://cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062
2.	*Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* (ITSP.40.111) – https://cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-pour-linformation-non-classifie-protege-et-protege-b
3.	*WeWork's weak Wi-Fi security leaves sensitive documents exposed* (en anglais) – https://www.cnet.com/tech/services-and-software/weworks-weak-wi-fi-security-leaves-sensitive-documents-exposed/
4.	*IoT Cyberattacks Escalate in 2021, According to Kaspersky* (en anglais) – https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/
5.	*Thousands of university Wi-Fi networks expose log-in credentials* (en anglais) – https://threatpost.com/misconfiguration-university-wifi-login-credentials/175157/
6.	*La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33) – https://cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie
7.	*Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones* (ITSG-38) – https://www.cyber.gc.ca/fr/orientation/considerations-de-conception-relatives-au-positionnement-des-services-dans-les-zones
8.	*Pratiques exemplaires de création de phrases de passe et de mots de passe* (ITSAP.30.032) – https://cyber.gc.ca/fr/orientation/pratiques-exemplaires-de-creation-de-phrases-de-passe-et-de-mots-de-passeitsap30032
9.	*Conseils sur le renforcement de la sécurité de Microsoft Windows 10 Enterprise* (ITSP.70.012) – https://cyber.gc.ca/fr/orientation/conseils-sur-le-renforcement-de-la-securite-de-microsoft-windows-10-enterprise
10.	*Utiliser son dispositif mobile en toute sécurité* (ITSAP.00.001) – https://cyber.gc.ca/fr/orientation/utiliser-son-dispositif-mobile-en-toute-securite-itsap00001