UTILISER LE WI-FI SANS COMPROMETTRE LA SÉCURITÉ DE VOTRE ORGANISATION

Octobre 2020 **ITSAP.80.009**

Le Wi-Fi est souvent une technologie essentielle à la conduite des activités des organisations. En revanche, il peut également exposer ces dernières à des vulnérabilités susceptibles d'être exploitées par les auteurs de menace. Pour assurer votre sécurité en ligne, vous devez mettre en place les mesures de sécurité nécessaires pour protéger vos réseaux, vos systèmes et votre information.

EN QUOI CONSISTE LE Wi-Fi?

Il s'agit d'une 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. Le routeur met en réseau les dispositifs afin qu'ils puissent communiquer entre eux et échanger de l'information. Les utilisateurs peuvent accéder au Wi-Fi par l'entremise de réseaux qui sont propres à leur organisation ou accessibles publiquement.

COMMENT LES AUTEURS DE MENACE TIRENT-ILS AVANTAGE DU WI-FI?

Les auteurs de menace peuvent utiliser les réseaux Wi-Fi pour accéder à vos systèmes et à vos dispositifs, et les endommager. Ils peuvent également utiliser ces réseaux pour voler de l'information sensible. Les réseaux Wi-Fi publics sont particulièrement vulnérables, puisqu'ils ne demandent généralement pas aux utilisateurs de s'authentifier au moment de s'y connecter, et ils font souvent appel à des protocoles de chiffrement faciles à pirater. Une fois que l'auteur de menace s'est introduit dans le réseau, il peut accéder aux dispositifs non sécurisés qui y sont connectés.

MYSTIFICATION

Un auteur de menace crée un réseau frauduleux qui prend l'apparence d'un réseau légitime. Il peut, par exemple, créer un réseau portant le même nom que le réseau d'un aéroport, d'une bibliothèque ou d'un café afin de tromper les utilisateurs et de les inciter à s'y connecter. Si vos employés en télétravail se connectent à l'un de ces réseaux trafiqués, ils risquent qu'un auteur de menace intercepte les données personnelles et organisationnelles sensibles, et infecte leurs dispositifs avec un maliciel.

ATTAQUES DE L'INTERCEPTEUR OU ÉCOUTE ÉLECTRONIQUE

Un auteur de menace peut utiliser les réseaux Wi-Fi (particulièrement les réseaux non sécurisés) pour exploiter les failles de sécurité et intercepter les données qui sont envoyées par l'entremise du réseau. L'information qui transite par un réseau Wi-Fi public ou non sécurisé est particulièrement vulnérable à ce type d'attaque. Advenant une compromission, un auteur de menace sera en mesure de saisir et de lire l'information, comme les justificatifs d'ouverture de session et les numéros de carte de crédit.

BROUILLAGE DES SIGNAUX

Un auteur de menace peut surcharger un point d'accès sans fil dans le but de perturber le réseau et d'empêcher le trafic légitime de communiquer avec celui-ci. Le brouillage des signaux peut compromettre la disponibilité des services offerts par votre organisation.

Si le réseau physique de votre organisation n'est pas sécurisé, un auteur de menace pourrait tenter d'installer un point d'accès sans fil sur votre réseau, puis s'en servir pour se connecter aux dispositifs et lancer des attaques.

COMMENT PUIS-JE PROTÉGER MON ORGANISATION?

L'utilisation du Wi-Fi dans votre organisation ou dans des lieux publics soulève d'importantes préoccupations. Il convient donc de prendre les mesures suivantes pour protéger vos réseaux, vos systèmes et votre information.

CHANGER LE NOM DU RÉSEAU

Votre Wi-Fi comporte un identificateur SSID par défaut ou un nom de réseau. Donnez un nom unique à votre réseau et veillez à ce qu'il ne contienne aucune information personnelle et aucun renseignement susceptible de révéler le fabricant du routeur ou le point d'accès que vous utilisez.

UTILISER UNE PHRASE DE PASSE

Changez les mots de passe par défaut sur le réseau, ainsi que ceux du compte d'administrateur. Utilisez une phrase ou un mot de passe unique et complexe, tout en évitant les mots du dictionnaire ou les autres mots de passe faciles à deviner.

UTILISER UN RÉSEAU PRIVÉ VIRTUEL

La mise en place d'un réseau privé virtuel (RPV) sur votre réseau peut protéger l'information de votre organisation. Un RPV est un tunnel chiffré sécurisé par l'entremise duquel l'information est acheminée. Si vos employés travaillent à distance et doivent utiliser des réseaux publics ou non sécurisés, le recours à un RPV permettra à ces derniers d'établir une connexion sécurisée qui fait appel à l'authentification et assure la protection de vos données.

AVOIR RECOURS À DES OUTILS DE SÉCURITÉ POUR PROTÉGER VOTRE RÉSEAU

Installez un pare-feu sur votre réseau. Un pare-feu surveille le flux de trafic qui transite par votre réseau et filtre le trafic que l'on sait malveillant. Vous pouvez définir des règles pour contrôler le volume et le type du trafic autorisé à circuler d'un réseau à l'autre. Songez à activer le filtrage des adresses de contrôle d'accès au support (MAC pour *Media Access Control*) pour veiller à ce que seuls les dispositifs autorisés puissent se connecter à votre réseau.

Si vous disposez des ressources nécessaires, vous pourriez envisager d'investir dans un système de détection d'intrusions sans fil (WIDS pour *Wireless Intrusion Detection System*) ou un système de prévention d'intrusion sans fil (WIPS pour *Wireless Intrusion Prevention System*) afin de surveiller les anomalies sur votre réseau.

CONFIGURER UN RÉSEAU INVITÉ

Un réseau invité est un point d'accès distinct sur votre routeur sans fil qui permet aux dispositifs de se connecter à Internet, mais pas à votre réseau principal. Vous devriez envisager de connecter les dispositifs de l'Internet des objets (IdO) à un réseau invité pour diminuer le risque qu'un maliciel infecte votre réseau principal.

DÉSACTIVER LA DIFFUSION DU RÉSEAU

Vous pouvez également désactiver la diffusion du réseau. Si le nom de votre réseau est diffusé, il sera visible par tous les utilisateurs à la recherche d'un réseau auquel se connecter. La désactivation de la diffusion du réseau fera en sorte que les utilisateurs devront saisir manuellement le nom du réseau pour s'y connecter.

QUELS AUTRES FACTEURS DEVRIEZ-VOUS CONSIDÉRER?

Assurez-vous que tous les employés savent comment protéger votre organisation contre les cybermenaces. Offrez-leur de la formation en matière de cybersécurité et encouragez les employés qui font du télétravail à sécuriser leurs réseaux Wi-Fi domestiques en prenant les mesures mentionnées dans la présente. Il convient également d'adopter les pratiques exemplaires additionnelles suivantes :

- Ne vous connectez pas à des réseaux Wi-Fi publics lorsque vous travaillez à distance. Si vous devez utiliser un Wi-Fi public, utilisez un RPV pour assurer la protection de votre information;
- Évitez d'utiliser la fonction « Mémoriser mes informations » lorsque vous vous connectez à vos comptes et fermez toujours votre session lorsque vous
- Supprimez les réseaux enregistrés (« Oublier le réseau ») auxquels vous vous êtes connectés précédemment et que vous n'utilisez plus;
- Désactivez les fonctions de connexion automatique sur vos dispositifs mobiles pour éviter de vous connecter automatiquement à des réseaux non sécurisés;
- Désactivez le Wi-Fi et les connexions Bluetooth lorsque vous ne les utilisez pas;
- Appliquez régulièrement les mises à jour et les correctifs aux systèmes d'exploitation et aux applications;
- Mettez à jour régulièrement les logiciels et les micrologiciels sur les dispositifs de l'IdO, y compris les routeurs.

OÙ PUIS-JE EN APPRENDRE PLUS?

Pour de plus amples conseils en matière de sécurité, visitez le site Web du Centre canadien pour la cybersécurité à **cyber.gc.ca**. Vous y trouverez plusieurs publications sur le sujet.

- ITSAP.80.101, *Réseaux privés virtuels*
- ITSAP.10.016, *Conseils de sécurité pour les organisations dont les employés travaillent à distance*
- ITSAP.70.111, *Utiliser un poste de travail virtuel à la maison et au bureau*
- ITSAP.70.002, *Considérations de sécurité pour les modèles de déploiement de dispositifs mobiles*
- ITSAP.10.096. *Application des mises à jour sur les dispositifs*
- ITSAP.00.057, *Protéger l'organisme contre les maliciels*
- ITSAP.30.032, *Pratiques exemplaires de création de phrases de passe et de mots de passe*