Réseau Wi-Fi Invité

AOÛT 2022

ITSAP.80.023

La configuration de réseaux Wi-Fi invités dans votre domicile et au sein de votre organisation contribue de façon importante à la protection de votre réseau principal. Un réseau invité est un point d'accès à Internet qui est distinct de votre réseau principal. Malgré leurs nombreux avantages, les réseaux invités peuvent également exposer votre domicile ou votre organisation à des vulnérabilités susceptibles d'être exploitées par les auteurs de menace. Le renforcement de votre posture de cybersécurité repose sur la mise en œuvre et la sécurisation d'un réseau invité.

Pourquoi devrait-on utiliser des réseaux invités?

Les réseaux Wi-Fi invités permettent aux invités et aux dispositifs d'accéder à Internet par l'entremise de points d'accès réseau distincts de votre réseau principal. Faciles à configurer et peu coûteux, ils permettent d'améliorer la cybersécurité de votre domicile et de votre organisation des façons suivantes :

At home:

- Permet aux invités d'accéder à Internet
- Évite d'avoir à communiquer ses mots de passe
- Isole les appareils intelligents et les dispositifs possiblement non corrigés du réseau principal
- Isole l'accès à distance aux réseaux et aux dispositifs d'entreprise

Organisation:

- Permet aux visiteurs d'accéder à Internet
- Réduit les risques que des attaquants accèdent aux dispositifs et à l'information sur le réseau principal (par exemple, pour propager des maliciels)
- Permet d'établir une séparation logique du réseau pour les dispositifs nouveaux et obsolètes, comme les logiciels non corrigés

Les réseaux locaux virtuels (VLAN pour Virtual Local Area Network) plus modernes permettent de créer plusieurs réseaux distincts afin que les utilisateurs principaux, les dispositifs et les invités puissent accéder à différentes parties de votre système. Plusieurs dispositifs, comme les appareils intelligents, exigent une connexion Internet pour fonctionner correctement, mais n'ont pas besoin d'avoir un accès direct à vos réseaux principaux. Les réseaux Wi-Fi invités réduisent les risques que des dispositifs compromis accèdent à de l'information sensible importante.

Menaces pesant sur vos réseaux invités

Les auteurs de menace ciblent souvent les réseaux Wi-Fi invités, puisqu'ils sont rarement sécurisés de façon appropriée. Il convient de tenir compte de certaines cybermenaces courantes si vous avez recours à un réseau invité :

- **Attaques par écoute clandestine:** Les auteurs de menace mènent des attaques par écoute clandestine pour tirer avantage d'un réseau Wi-Fi ouvert non sécurisé et compromettre l'information transmise par l'entremise du reseau.
- **Attaques par hameçonnage:** Tous les dispositifs connectés à votre réseau invité pourraient être compromis si un de ses utilisateurs est victime d'une attaque par hameçonnage avant d'établir une connexion ou pendant qu'il y est connecté.
- **Maliciels:** Après avoir infecté un dispositif, un maliciel se propagera aux autres dispositifs connectés au même réseau. Cette infection met également à risque l'ensemble des dispositifs et de l'information qui résident sur le réseau invité;
- **Attaques par déni de service (DoS):** Les auteurs de menace mènent des attaques par déni de service (DoS pour Denial of Service) pour submerger les réseaux ciblés. Une attaque par DoS peut surcharger le routeur et provoquer le mauvais fonctionnement des processus ou permettre aux auteurs de menace d'accéder à votre réseau principal.

La plupart de ces menaces illustrent pourquoi il peut être utile d'utiliser un réseau Wi-Fi invité pour protéger votre réseau principal (par exemple, empêcher les menaces d'accéder à l'information sensible). Afin d'assurer la sécurité de votre réseau principal et des dispositifs connectés à votre réseau Wi-Fi invité, il est impératif d'utiliser les outils de sécurité appropriés lors de la mise en œuvre et de la gestion de votre réseau Wi-Fi invité.

SÉRIE SENSIBILISATION

No de cat. D97-1/80-023-2022F-PDF
ISBN 978-0-660-44767-4

Comment puis-je sécuriser mes réseaux invités?

Bien qu'un réseau invité serve généralement à empêcher les dispositifs potentiellement non sécurisés d'accéder au réseau principal, il est important qu'il soit aussi sécurisé que possible. Atténuer les risques posés par votre réseau invité permettra d'assurer la sécurité des dispositifs qui doivent s'y connecter et de l'information qui doit y résider. Vous trouverez ci-dessous quelques mesures de sécurité que vous pourriez envisager de mettre en place.

Mots de passe distincts

L'accès à votre réseau Wi-Fi invité devrait être protégé par un mot de passe distinct des autres réseaux et comptes. Assurez-vous de changer le mot de passe par défaut et évitez de le communiquer à n'importe qui. Un invité en qui vous avez confiance pourrait ne pas divulguer le mot de passe, mais s'il utilise un dispositif compromis pour accéder à votre réseau invité, les autres dispositifs connectés pourraient également être compromis.

Mise à jour des logiciels

Appliquez les plus récentes mises à jour aux logiciels et aux micrologiciels sur votre routeur ou tous les dispositifs connectés au réseau invité. Vous pourrez ainsi corriger les vulnérabilités informatiques et réduire les risques que des maliciels se propagent sur votre réseau.

Isolation des réseaux

Assurez-vous que les paramètres de votre VLAN empêchent les invités et les dispositifs connectés aux réseaux invités d'interagir avec les dispositifs et l'information sur le réseau principal. Les pare-feux peuvent également fournir ces paramètres de sécurité avec une configuration avancée si votre organisation a les moyens financiers et techniques de les mettre en œuvre.

Surveillance des dispositifs connectés

Vérifiez quels sont les dispositifs connectés à votre réseau Wi-Fi invité. Limitez la période durant laquelle il est possible d'utiliser les mots de passe d'invités pour garantir que seuls les invités actuels peuvent accéder au réseau. Mettez en place une fonction de début et de fin d'accès pour les dispositifs tentant d'établir de nouvelles connexions.

Diffusion du réseau

Pour accroître la sécurité, vous pouvez désactiver la diffusion du réseau (par exemple, l'ID réseau ou l'identificateur SSID [*Service Set Identifier*]). Si votre réseau invité diffuse de l'information, n'importe qui peut tenter d'y accéder en recherchant les réseaux disponibles. Désactiver la diffusion du réseau fera en sorte que les utilisateurs devront saisir manuellement le nom du réseau pour s'y connecter.

Utilisation du protocole WPA2 ou WPA3

Utilisez les protocoles de sécurité WPA2 ou WPA3, le cas échéant, pour configurer votre réseau invité. Ces protocoles de sécurité proposent des mécanismes de chiffrement Wi-Fi avancés permettant d'assurer la sécurité de vos dispositifs et de votre information.

Filtrage Web

Utilisez le filtrage Web pour contrôler les sources accessibles par l'intermédiaire de votre réseau invité. Mettez en place des listes d'autorisation et d'exclusion pour gérer l'accès aux sites Web et aux applications. Vous pouvez également avoir recours à des mots -clés et à des filtres de contenu pour limiter l'accès aux sites Web comportant du contenu en particulier.

Vous pourriez également envisager de faire appel au filtrage des adresses de contrôle d'accès au support (MAC pour *Media Access Control*). Comme pour les listes d'autorisation et d'exclusion, le filtrage des adresses MAC permet de déterminer les dispositifs qui sont autorisés ou non à accéder à votre réseau.

Renseignements supplémentaires

Consultez notre site Web (cyber.gc.ca) pour accéder à une gamme de publications liées à la cybersécurité, notamment:

- *La sécurité du Wi-Fi (ITSP.80.002)*
- *Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation (ITSAP.80.009)*
- *Application des mises à jour sur les dispositifs (ITSAP.10.096)*
- *Ne mordez pas à l'hameçon: Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)*
- Protéger votre organisation contre les maliciels (ITSAP.00.057)
- *Protéger son organisation contre les attaques par déni de service (ITSAP.80.100)*
- *Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)*
- *Liste d'applications autorisées (ITSAP.10.095)*

Vous avez des questions ou vous avez besoin d'aide? Vous souhaitez être au fait des questions de cybersécurité ou en savoir plus sur le sujet? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.