Pratiques exemplaires en matière de cybersécurité pour les routeurs

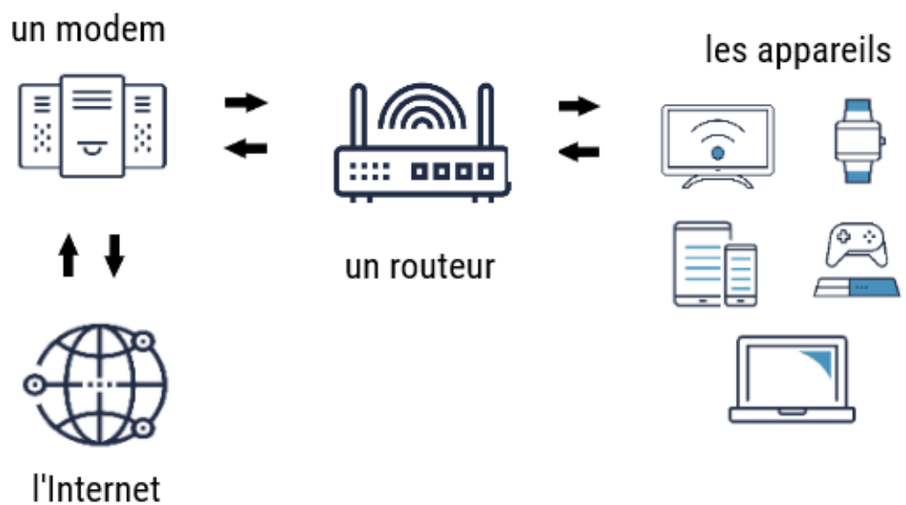
CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

OCTOBRE 2022 | ITSAP.80.019

Il est fort probable que votre lieu de travail et votre domicile soient dotés d'une vaste gamme d'appareils connectés à Internet, tels que des ordinateurs, des tablettes, des téléphones intelligents, des imprimantes, des téléviseurs intelligents et divers appareils de l'Internet des objets (IdO). Les routeurs permettent à de multiples appareils de se connecter à Internet en utilisant la même connexion. On utilise fréquemment un routeur sans connexion Internet pour connecter des appareils sans fil dans une zone locale afin d'accéder à des imprimantes réseau ou sans fil et à des fichiers partagés, ainsi que pour assurer la communication entre les appareils connectés. Malheureusement, les routeurs sont des cibles attrayantes pour les cybercriminels qui tentent d'infiltrer des réseaux pour mener des cyberattaques. Le présent document contient de l'information sur les pratiques exemplaires en matière de cybersécurité pour protéger vos routeurs contre les compromissions.

Qu'est-ce qu'un routeur?

Un routeur est un composant matériel qui sert à créer un réseau pour les appareils situés dans une zone locale, et un modem connecte ce réseau à Internet. Certains dispositifs combinent les deux fonctionnalités et sont souvent appelés des routeurs également. Les routeurs sont responsables d'acheminer les messages (paquets de données) d'un appareil à un autre au sein d'un réseau. Pour ce faire, le routeur attribue une adresse de protocole Internet (IP pour *Internet Protocol*) locale unique à chacun des appareils dans le réseau. Lorsqu'il reçoit un paquet de données à acheminer, le routeur lit l'adresse IP de destination, consulte sa table de routage pour déterminer le prochain saut et achemine le paquet en conséquence.



Quelles sont les **conséquences** de la compromission d'un routeur?

Les auteurs de menace ont recours à diverses techniques pour balayer automatiquement le matériel informatique (comme les routeurs) afin de déceler des vulnérabilités aux cyberattaques. Les routeurs sont vulnérables lorsqu'ils sont mal configurés. Si votre routeur est compromis, les auteurs de menace peuvent :

- voler des renseignements permettant d'identifier une personne (PII pour *Personally Identifiable Information*) stockés dans n'importe quel appareil connecté à votre réseau et les utiliser à des fins malveillantes.
- accéder aux justificatifs d'ouverture de session de comptes d'utilisateur et les utiliser pour obtenir un accès non autorisé aux réseaux et aux appareils. Pour ce faire, les auteurs de menace modifient la capacité de votre routeur à vous diriger vers des sites Web légitimes, pour plutôt vous rediriger vers des sites Web contenant des maliciels.
- surveiller, modifier et interdire le trafic entrant et sortant de votre organisation, ou encore établir un accès permanent à vos réseaux afin de réaliser de futures attaques.
- exploiter la propriété intellectuelle ou les données exposées en vue d'orchestrer des cyberattaques avancées, par exemple dans le but de faciliter l'espionnage.
- s'approprier votre routeur ou l'assimiler à un réseau d'appareils infectés pour créer un réseau de zombies. Les auteurs de menace utilisent les réseaux de zombies pour mener des attaques par déni de service distribué (DDoS pour Distributed Denial of Service). Ce type d'attaque submerge votre serveur de trafic Internet pour interrompre la conduite de vos activités opérationnelles essentielles et la prestation de vos services.

Les publications suivantes sont offertes sur notre site Web :

- Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation (ITSAP.80.009)
- Système d'adressage par domaine de protection (ITSAP.40.019)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Réseau Wi-Fi invité (ITSAP.80.023)
- La sécurité du Wi-Fi (ITSP.80.002)

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Pratiques exemplaires en matière de cybersécurité pour les routeurs

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

OCTOBRE 2022 | ITSAP.80.019

Mesures visant à empêcher la compromission de votre routeur

Vous pouvez prendre les mesures suivantes pour protéger votre routeur contre les cyberattaques, en commençant par les mesures de base, puis en mettant en œuvre les mesures supplémentaires progressivement.

Mesures de base

- **Changez tous les mots de passe par défaut** pour le réseau Wi-Fi et le routeur. Utilisez une phrase de passe, autant que possible, ou un mot de passe fort, unique et complexe. Les phrases de passe et mots de passe sont importants pour protéger votre routeur contre les attaques par force brute qui visent à percer les mots de passe.
- **Activez le protocole WPA (*Wi-Fi Protected Access*)** pour protéger le trafic Internet contre les accès non autorisés. Les protocoles WPA2 et WPA3 (plus récent) offrent un chiffrement robuste entre le routeur et vos appareils.
- **Désactivez la diffusion de l'identifiant de l'ensemble de services (SSID pour *Service Set Identifier*)** afin que les auteurs de menace qui balayent les réseaux à proximité ne puissent pas voir le nom de votre réseau sans fil.
- **Changez le nom de réseau sans fil (SSID) par défaut.** Cette mesure empêchera les auteurs de menace d'établir facilement la marque et le modèle de votre routeur afin de déterminer s'il présente des vulnérabilités.
- **Désactivez la fonction de configuration Wi-Fi protégée (WPS pour *Wi-Fi Protected Setup*).** Cette fonction est pratique puisqu'elle simplifie le processus de connexion des appareils à votre routeur Wi-Fi. Cependant, un auteur de menace à portée du routeur peut déjouer la méthode d'authentification par NIP à l'aide d'une attaque par force brute.
- **Tenez à jour le micrologiciel du routeur.** Cette mesure permet d'assurer que le correctif de sécurité le plus récent est installé sur le routeur pour éliminer les vulnérabilités connues. Activez la fonction de mise à jour automatique du micrologiciel si votre routeur l'offre.
- **Établissez un réseau invité** pour la connexion à Internet de vos invités et de vos appareils IdO. Cette mesure permet d'éviter le partage de mots de passe et de réduire le risque que des auteurs de menace accèdent aux appareils et à l'information sensible sur votre réseau principal.
- **Assurer la sécurité physique de vos appareils.** Limitez l'accès physique aux appareils et sécurisez l'accès aux points d'accès Wi-Fi.

Mesures supplémentaires

- **Planifiez des redémarrages courants** pour effacer la mémoire système et rafraîchir toutes les connexions. Le redémarrage du routeur peut déstabiliser un maliciel ayant été implanté.
- **Désactivez la gestion de l'accès à distance**, dans la mesure du possible, pour empêcher toute personne non autorisée d'accéder à votre routeur et de le trafiquer.
- **Désactivez le protocole de gestion de réseau simple (SNMP pour *Simple Network Management Protocol*)** pour réduire le risque que des auteurs de menace recueillent de l'information de base sur la configuration système de votre réseau.
- **Assurez-vous que chaque administrateur du routeur a son propre nom d'utilisateur et son propre mot de passe unique d'ouverture de session, de même que les privilèges appropriés.** Si la journalisation des événements est activée, l'information d'ouverture de session sera importante aux fins d'audit et d'enquête sur les incidents.
- **Utilisez le filtrage des adresses de contrôle d'accès au support (MAC pour *Media Access Control*)** pour choisir les appareils fiables qui peuvent se connecter à votre réseau.
- **Activez le filtrage des ports.** Par exemple, le SANS Institute recommande de bloquer le trafic sortant qui emprunte les ports suivants, afin d'éviter la diffusion de trafic indésirable sur Internet:
  - MS RPC – port TCP/UDP 135
  - NetBIOS/IP - ports TCP & UDP 137 à 139
  - SMB/IP - port TCP 445
  - Protocole TFTP (*Trivial File Transfer Protocol*) – port UDP 69
  - Syslog - port UDP 514
  - Protocole SNMP – ports UDP 161 et 162
  - IRC (*Internet Relay Chat*) – ports TCP 6660 à 6669
- **Activez la journalisation des événements et surveillez les activités régulièrement.** Vous pourrez ainsi détecter les types d'attaques lancées contre le routeur et mettre en œuvre des mesures d'atténuation proactives. Si vous utilisez un serveur syslog pour la surveillance, changez le port UDP 514 utilisé par défaut par un autre port, comme TCP 514 ou TCP 6514.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada