Votre bulletin mensuel sur la sensibilisation à la sécurité

Sécuriser votre Wi-Fi chez vous

Aperçu

Pour créer un réseau local sécurisé, vous devez commencer par protéger votre point d'accès Wi-Fi (aussi appelé parfois un routeur Wi-Fi). C'est l'appareil qui contrôle qui ou quoi peut se connecter à votre réseau local. Voici cinq étapes simples pour sécuriser la Wi-Fi de chez vous afin de créer un réseau local bien plus fiable pour vous et votre famille.

Concentrons-nous sur les bases

Souvent, le moyen le plus facile de se connecter et configurer votre appareil Wi-Fi est quand il est connecté à votre réseau local. Ouvrez votre navigateur et tapez l'adresse IP indiquée dans le manuel de votre appareil (par exemple, vous pouvez trouver quelque chose comme https://192.168.1.1), ou bien, utilisez un fournisseur ou une application mobile fournis par le vendeur de votre routeur Wi-Fi.

1. **Changez le mot de passe administrateur** : Votre point d'accès Wi-Fi vous a probablement été envoyé avec un mot de passe par défaut pour le compte administrateur qui vous permet de changer la configuration de votre appareil. Souvent, ces mots de passe sont connus du public et peuvent être même postés sur internet. Assurez-vous de bien changer le mot de passe de l'administrateur en un mot de passe unique et fiable pour que seul vous ayez accès à ce mot de passe. Si votre appareil le permet, changez aussi le nom d'utilisateur de l'administrateur.
2. **Créez un mot de passe de réseau** : Configurez votre réseau Wi-Fi afin d'également paramétrer un mot de passe unique et fiable (assurez-vous qu'il soit différent du mot de passe administrateur). De ce fait, seuls les personnes et appareils en qui vous avez confiance peuvent rejoindre votre réseau local. Envisagez la possibilité d'utiliser un gestionnaire de mots de passe qui peut choisir pour vous un mot de passe fiable et peut vous permettre de lister tous vos mots de passe.
3. **Les mises à jour firmware** : Activez les mises à jour automatiques du système d'exploitation de votre réseau local Wi-Fi, souvent appelé firmware. De cette manière, vous vous assurez que votre appareil est aussi sécurisé que possible, équipé des dernière options de sécurité. Si les mises à jour automatiques ne sont pas disponibles sur votre point d'accès, connectez-vous régulièrement et vérifiez qu'il n'y ait pas de mises à jour disponibles. Si votre appareil n'est plus financé par le vendeur, envisagez la possibilité d'en acheter un nouveau que pouvez mettre à jour avec les dernières caractéristiques de sécurité.

4. **Utilisez un réseau invité** : Un réseau invité est un réseau virtuel indépendant que votre point d'accès Wi-Fi peut créer. Cela signifie que votre point d'accès Wi-Fi a en réalité deux réseaux. Le réseau *principal* est celui auquel vos appareils fiables se connectent, tels que votre ordinateur, vos téléphones ou tablettes. Le *réseau invité* est celui auquel vos appareils non-fiables se connectent, tels que des invités qui viennent chez vous ou peut-être certains de vos dispositifs personnels intelligents. Quand quelque chose se connecte à votre réseau invité, il ne peut voir aucun de vos appareils personnels fiables connectés à votre réseau principal, ni communiquer avec lui.
5. **Utilisez un DNS sécurisé filtrant :** DNS est un service internet vaste qui convertit les noms des sites en adresses numériques. C'est ce qui vous aide à vous assurer que votre ordinateur peut se connecter à un site quand vous tapez le nom du site. Les point d'accès Wi-Fi utilisent habituellement le serveur DNS par défaut fourni par votre fournisseur de services internet, mais des alternatives plus sécurisées sont disponibles gratuitement avec des services tels que OpenDNS, CloudFlare for Families, ou bien Quad9 qui peut fournir une sécurité supplémentaire en bloquant des sites malveillants ou indésirables. Connectez-vous sur votre point d'accès Wi-Fi et changez l'adresse du serveur DNS par une alternative plus sécurisée.

Sécuriser votre point d'accès Wi-Fi est la première étape et la plus importante durant la création d'un réseau local sécurisé. Pour plus d'informations sur la sécurisation de votre point d'accès Wi-Fi, référez-vous au manuel de l'appareil, ou si votre fournisseur de services internet vous a fourni votre appareil, contactez-le pour plus d'informations sur les options de sécurité.

Rédacteur Invité

Joshua Wright (Twitter @joswr1ght) est un directeur expérimenté à Counter Hack Challenges, LLC, dirigeant la coordination et le développement des défis lancés par des cybercriminels pour NetWard et Holiday Hack Challenge. Vous pouvez retrouver Josh sur LinkedIn ici : https://linkedin.com/in/joswr1ght.

Ressources

Simplifier les mots de passe : https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Gestionnaire de mots de passe : https://www.sans.org/security-awareness-training/resources/password-managers-0
Attaques personnalisées : https://www.sans.org/security-awareness-training/resources/power-updating
Guide d'installation de OpenDNS : https://www.opendns.com/setupguide/#familyshield

Traduit pour la communauté par : Juliette Busson