OUCH ! Janvier 2025

Les apparents domestiques intelligents : sécurisez-les avant que les criminels ne tombent dessus

Un cauchemar digital : les cyber-criminels dans votre maison

Sarah et sa famille étaient ravis d'installer leur nouvel appareil connecté pour contrôler leurs lumières et leurs serrures grâce à quelques touches ou quelques commandes vocales. Cependant, leur excitation a été de courte de durée lorsque Sarah a remarqué son thermostat intelligent s'ajuster tout seul. Elle s'est d'abord dit que c'était un problème anodin, mais elle a commencé à s'inquiéter lorsque les lumières ont commencé à sauter mystérieusement. Elle s'est vraiment rendu compte du problème lorsque la voix d'un étranger est sortie de son baby phone, décrivant la pièce en détail. À ce moment-là, Sarah a compris que son sanctuaire avait été violé. Les cyber-criminels avaient pris le contrôle de ses appareils connectés, compromettant leur vie privée et leur sécurité. Sarah se sentait vulnérable et exposée à l'idée que des étrangers regardaient son bébé en train de dormir. Cette expérience extrêmement déstabilisante a accentué le besoin de Sarah de sécuriser ses appareils connectés pour assurer la sécurité et la tranquillité d'esprit de toute sa famille.

Que sont les appareils connectés ?

Les appareils domestiques intelligents sont des dispositifs et des appareils connectés à internet, tels que les thermostats, les caméras de sécurité, les serrures intelligentes, les lumières et parfois même des machines à laver, qui rendent nos maisons plus efficaces, plus confortables et parfois même plus sûres. Ces appareils sont contrôlés par des applications, des commandes vocales ou des systèmes automatisés, offrant une commodité sans précédent.

Cependant, la commodité qu'ils apportent comporte également des risques. Comme ces appareils sont connectés à internet, ils sont vulnérables s'ils ne sont pas correctement sécurisés. En cas de piratage, les intrus peuvent accéder à vos informations personnelles, espionner vos activités quotidiennes et même contrôler les appareils physiques à l'intérieur de votre maison.

Pourquoi est-il si important de sécuriser vos appareils connectés intelligents ?

La sécurisation des appareils domestiques intelligents ne consiste pas seulement à protéger les appareils eux-mêmes, mais aussi à protéger l'ensemble de votre foyer. Les cyber-attaquants recherchent souvent les dispositifs les plus faibles et commencent par ceux-là. Une fois compromis, un cyber-attaquant peut utiliser un appareil piraté pour accéder à d'autres appareils de votre réseau domestique, voler des données sensibles ou même déverrouiller vos portes. Dans un monde interconnecté, la sécurisation de vos appareils intelligents est essentielle pour préserver votre sécurité personnelle, votre vie privée et votre tranquillité d'esprit.

Cinq choses que vous pouvez faire pour sécuriser ces appareils

1. **Changez les mots de passe par défaut immédiatement** : de nombreux appareils intelligents sont dotés de mots de passe par défaut, définis en usine, qui sont connus ou faciles à deviner pour les cybercriminels. Changez-les immédiatement pour des mots de passe forts et uniques, et utilisez un gestionnaire de mots de passe pour en garder la trace.

2. **Activez l'authentification multifactorielle (MFA), parce qu'une seule ne suffit plus** : certains appareils domestiques intelligents nécessitent la création d'un compte en ligne pour accéder à l'appareil et le gérer. Protégez ces comptes avec la MFA, qui ajoute une couche supplémentaire de sécurité en exigeant à la fois un mot de passe et un code à usage unique envoyé sur votre téléphone. Les cybercriminels détestent la MFA parce qu'elle leur rend la tâche beaucoup plus difficile.

3. **Donnez à vos appareils intelligents leur propre réseau Wi-Fi** : créez un réseau dédié à vos appareils intelligents, distinct de vos appareils personnels ou professionnels. Sur de nombreux points d'accès ou routeurs Wi-Fi, ce réseau est souvent appelé réseau invité. Cela permet d'isoler les appareils et de limiter les dégâts si l'un d'entre eux est compromis.

4. **Mises à jour, mises à jour, mises à jour** : les fabricants publient régulièrement des mises à jour pour corriger les failles de sécurité. Veillez à ce que vos appareils disposent des dernières mises à jour des micrologiciels et des logiciels afin de rester protégés contre les nouvelles menaces. Le moyen le plus simple est d'activer la mise à jour automatique sur vos appareils. Envisagez fortement de remplacer tout appareil qui n'est plus pris en charge ou qui ne reçoit plus de mises à jour de sécurité de la part de son fabricant.

5. **Désactivez les fonctionnalités** : les appareils connectés ont de nombreuses fonctionnalités, dont beaucoup ne seront jamais utilisées. Plus vous avez des fonctionnalités actives, plus les cyber-criminels ont des manières de s'introduire chez vous. Désactivez les services qui ne sont pas nécessaires, comme les accès à distance ou la commande vocale, pour minimiser les points d'entrée qu'un cyber-attaquant pourrait exploiter.

Votre maison connectée ne doit pas devenir un terrain de jeu pour les cyber-criminels. Avec seulement quelques étapes, vous pouvez profiter de tout ce que la technologie a à offrir tout en dormant sur vos deux oreilles.

Rédacteur invité

Sai Sujitha Venkatesan est ingénieure principale en sécurité au sein de l'équipe de réponse aux incidents de sécurité des produits de Dell et membre du conseil d'administration de WiCyS (Women in CyberSecurity) Silicon Valley. Elle est passionnée par tout ce qui touche à la sécurité, y compris la diversité de la main-d'œuvre. LinkedIn : https://www.linkedin.com/in/saisujitha/

Ressources

Le pouvoir de la mise à jour : https://www.sans.org/newsletters/ouch/power-updating/
Le pouvoir des phrases de passe : https://www.sans.org/newsletters/ouch/power-passphrase/
Le pouvoir des gestionnaires de mots de passe : https://www.sans.org/newsletters/ouch/power-password-managers/

Traduit pour la communauté par : Juliette Busson