OUCH! | Février 2016

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...

- Votre réseau sans fil
- Vos équipements

Sécuriser votre réseau domestique

Vue d'ensemble

Il y'a plusieurs années, les réseaux domestiques étaient relativement simples et n'étaient rien de plus qu'un point d'accès sans fil et un ordinateur ou deux utilisés pour surfer sur Internet, faire des achats en ligne ou encore jouer à des jeux en ligne. Cependant les réseaux domestiques sont devenus de plus en plus complexes. Non seulement nous connectons de plus en plus d'équipements sur nos réseaux domestiques, mais nous en diversifions également notre utilisation. Dans cette édition, nous allons couvrir quelques étapes basiques liées à la création d'un réseau domestique plus sécurisé pour vous et votre famille.

Editeur invité

Cheryl Conley dirige l'équipe d'éducation et de sensibilisation à la sécurité chez Lockheed Martin, tirant parti de The I Campaign™ atteignant plus de 100.000 employés. Cela inclut des groupes de discussion qui se concentrent sur l'alliance et la défense au travers de l'entreprise en plus d'un programme de phishing mondial. Suivez Cheryl sur **@conleychera**.

Votre réseau sans fil

Presque tous les réseaux domestiques commencent par un réseau sans fil (parfois appelé un réseau Wi-Fi) ce qui vous permet de connecter sans fil tous vos appareils à Internet, des ordinateurs portables en passant par des tablettes jusqu'aux consoles de jeux et téléviseurs, sans aucun câble. La plupart des réseaux sans fil domestiques sont contrôlés par votre routeur Internet, qui est le dispositif de votre fournisseur de services Internet installé dans votre maison pour vous connecter à Internet. Cependant, dans certains cas, votre réseau sans fil peut être contrôlé par un système distinct appelé un point d'accès sans fil qui se connecte à votre routeur Internet. Peu importe quel réseau sans fil vous utilisez, ils travaillent tous les deux de la même manière en diffusant des signaux sans fil. Les différents appareils dans votre maison se connectent ainsi à votre réseau sans fil via ces signaux. De là, ces dispositifs peuvent alors se connecter à Internet ainsi que les autres périphériques de votre réseau domestique. Cela signifie que la sécurisation de votre réseau sans fil est un élément clé de la protection de votre maison. Nous vous recommandons de suivre les étapes suivantes pour le sécuriser.

- Changez le mot de passe administrateur par défaut de votre routeur Internet ou point d'accès sans fil, selon celui qui contrôle votre réseau sans fil. Le compte administrateur vous permet de configurer les paramètres de votre réseau sans fil. Le problème est que beaucoup de routeurs Internet ou points d'accès sans fil sont livrés avec un login admin et un mot de passe par défaut qui sont bien connus et souvent affichés sur Internet. En tant que tel, assurez-vous de changer le mot de passe admin en un mot de passe robuste et unique que vous seul connaissez.

Sécuriser votre réseau domestique

Pour protéger votre réseau domestique, sécurisez votre réseau sans fil et mettez à jour votre mot de passe afin de protéger tous les périphériques de votre réseau.

- Modifiez le nom par défaut de votre réseau sans fil (parfois appelé SSID). Il s'agit du nom visible par vos appareils lorsqu'ils rechercheront des réseaux locaux sans fil. Nommez votre réseau avec un identifiant unique et facilement reconnaissable tout en vous assurant qu'il ne contient aucune information personnelle. De plus, il y'a peu d'intérêt à configurer votre réseau en mode caché (ou non-diffusion). La plupart des outils de scan des réseaux sans fil ou tout attaquant un minimum expérimenté peuvent facilement découvrir les détails d'un réseau masqué.
- Veillez à ce que seules les personnes en qui vous avez confiance peuvent se connecter et utiliser votre réseau sans fil, et que ces connexions soient cryptées. Pour ce faire, vous devez activer une sécurité renforcée. Actuellement, la meilleure option est d'utiliser le mécanisme de sécurité appelée WPA2. Ainsi, un mot de passe est nécessaire pour que les gens puissent se connecter à votre réseau domestique, et une fois relié, leurs activités en ligne sont cryptées. Enfin, assurez-vous bien de ne pas utiliser des protocoles de sécurité obsolètes tels que WEP ou pire encore, aucune sécurité, ce qui est également appelé un réseau ouvert. Un réseau ouvert permet à n'importe qui de se connecter à votre réseau sans fil et ce, sans authentification.
- Assurez-vous que le mot de passe que les gens utiliseront pour se connecter à votre réseau sans fil est un mot de passe robuste, difficile à deviner et qu'il est différent du mot de passe administrateur. N'oubliez pas qu'en principe, vous n'avez à entrer le mot de passe qu'une seule fois pour chacun de vos équipements, car ces derniers stockent et se rappellent de votre mot de passe.
- De nombreux points d'accès sans fil supportent la notion de réseau invité. Un réseau invité permet aux visiteurs de se connecter à votre point d'accès sans fil ainsi que d'accéder à Internet tout en les empêchant de se connecter à tout périphérique de votre réseau domestique. Si vous ajoutez un réseau invité, veillez à activer le protocole WPA2 et d'y configurer un mot de passe différent dédié à ce réseau.
- Désactivez WiFi Protected Setup ou d'autres mécanismes qui permettent à un nouvel appareil de se connecter au réseau sans connaître les options de mot de passe et de configuration.
- Si vous avez du mal à vous souvenir de tous ces différents mots de passe, nous vous recommandons d'utiliser un gestionnaire de mot de passe afin de les stocker en toute sécurité.

Pas certain sur la manière d'aborder ces étapes? Demandez à votre fournisseur de services Internet, consultez la documentation fournie avec votre routeur Internet ou votre point d'accès sans fil, ou consultez leur site Web respectif.

Sécuriser votre réseau domestique

Vos équipements

L'étape suivante consiste à savoir ce qui est connecté à votre réseau domestique et veillez ainsi à ce que l'ensemble de ces dispositifs soient bien sécurisés. Cela pourrait s'avérer être simple si vous aviez seulement quelques équipements connectés. Cependant, de nos jours, presque tout peut se connecter à votre réseau domestique, y compris les téléviseurs, les consoles de jeux, les moniteurs de bébé, les haut-parleurs, votre thermostat, ou peut-être même votre voiture. Une façon simple de découvrir ce qui est sur votre réseau domestique est d'utiliser un scanner de réseau simple comme Fing. Ces applications, que vous pouvez installer sur votre ordinateur ou appareil mobile, scannent votre réseau sans fil et font un rapport pour chaque périphérique connecté. Une fois que vous avez identifié tous les périphériques de votre réseau domestique, vous devez vous assurer que chacun de ces dispositifs soit bien sécurisé. La meilleure façon de le faire est d'être certain qu'ils fonctionnent toujours avec la dernière version de leur système d'exploitation / logiciel. Assurez-vous d'avoir activé la mise à jour automatique si l'option est disponible. Si l'un de vos périphériques nécessite un mot de passe, utilisez toujours un mot de passe unique. Enfin, assurez-vous de visiter le site Web de votre fournisseur de services Internet, car ils peuvent fournir des outils gratuits pour vous aider à sécuriser votre réseau domestique.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients. Pour en savoir plus, veuillez vous référer aux liens suivants : http://www.answer.ch et http://answersecurity.com/

Sources

Phrases de passe :	https://securingthehuman.sans.org/ouch/2015#april2015
Gestionnaires de mots de passe :	https://securingthehuman.sans.org/ouch/2015#october2015
Sécuriser votre nouvelle tablette :	https://securingthehuman.sans.org/ouch/2016#january2016
Cartographie de votre réseau domestique :	http://l.rud.is/home-network-mapping

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Marilyn Combet