OUCH! | Janvier 2014

La lettre d'information mensuelle pour la sensibilisation à la sécurité des utilisateurs informatiques

OUCH!

Dans ce numéro...

Sécuriser votre réseau domestique

Vue d'ensemble

Il y a maintenant 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 ou pour 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 notre utilisation. Dans cette édition, nous allons couvrir quelques étapes basiques liées à la création d'un réseau domestique plus sécurisé.

Rédacteur en chef invité

Kevin Johnson est le CEO de Secure Ideas, il administre **MySecurityScanner.com** et est instructeur senior au SANS Institute. Vous trouverez plus d'informations à **www.secureideas.com**.

Votre réseau sans fil

Presque tous les réseaux domestiques commencent par un réseau sans fil (parfois appelé un réseau Wi-Fi). C'est ce qui vous permet de connecter tous vos équipements à Internet, des ordinateurs portables en passant par les tablettes jusqu'aux consoles de jeux et téléviseurs, sans aucun câble. Pour ce faire, votre réseau sans fil a besoin de quelque chose appelé un point d'accès sans fil. Il s'agit d'un dispositif physique qui se connecte à votre routeur Internet (ou qui parfois peut y être intégré) et qui transmet un signal sans fil permettant à vos équipements de s'y connecter. Une fois que vos appareils se connectent au point d'accès, ils peuvent alors se connecter à d'autres périphériques de votre réseau domestique ainsi qu'à Internet. Par conséquent, votre point d'accès sans fil est l'un des éléments clés de votre réseau domestique, nous préconisons les mesures suivantes afin de le sécuriser.

- Pour la plupart des points d'accès sans fil, les identifiants par défaut du compte administrateur (login et mot de passe) sont bien connus et sont même très souvent postés sur Internet. Partant de ce constat, assurez-vous de modifier le login et le mot de passe par défaut du compte administrateur par quelque chose dont vous seul avez connaissance. Assurez-vous que c'est un mot de passe unique et qu'il n'est pas utilisé pour un autre de vos comptes.
- Un autre paramètre que vous devriez configurer est le nom de votre réseau sans fil (également 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-

Sécuriser votre réseau domestique

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.

- La prochaine étape est de s'assurer que seules les personnes de confiance et que vous connaissez peuvent se connecter et utiliser votre réseau sans fil, et que chacune de ces connexions est chiffrée. Nous voulons ainsi nous assurer qu'aucun voisin ou même étranger ne peut se connecter ou même surveiller votre réseau. Vous pouvez facilement mitiger ces risques en activant une sécurité renforcée sur votre point d'accès sans fil. Actuellement, la meilleure option est d'utiliser le mécanisme de sécurité WPA2. En activant celle-ci, vous imposez l'utilisation d'un mot de passe aux personnes qui souhaiteront se connecter à votre réseau domestique, et une fois authentifiées, leurs connexions seront chiffrées. 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.

Pour protéger votre réseau domestique, assurez-vous que vous avez un réseau sans fil sécurisé, que vous utilisez OpenDNS ou un service similaire, et que tous les périphériques de votre réseau domestique sont mis à jour.

- Assurez-vous que le mot de passe que les gens utiliseront pour se connecter à votre réseau sans fil est 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.
- Si vous ne pouvez pas vous rappeler de tous les différents mots de passe alors veillez à utiliser un gestionnaire de mot de passe afin de les stocker en toute sécurité.

OpenDNS

Une fois que vous avez configuré votre réseau sans fil, nous vous recommandons de configurer votre réseau domestique en utilisant OpenDNS en tant que vos serveurs DNS (ou un service similaire tel que Norton ConnectSafe for Home). Lorsque vous tapez un nom dans votre navigateur, le DNS permet à votre navigateur de déterminer auprès de quel serveur sur Internet il doit se connecter. Des services tels qu'OpenDNS identifient les sites Web

Sécuriser votre réseau domestique

infectés connus permettant ainsi à tout appareil connecté sur votre réseau domestique sans fil d'éviter de visiter accidentellement l'un de ces sites Web infectés. En outre, ces services vous donnent souvent la possibilité de filtrer et de bloquer les sites indésirables. Ce qui rend cette approche si efficace est qu'il n'y a aucun logiciel à installer sur vos équipements, vous avez juste un changement à effectuer au sein de votre point d'accès sans fil.

Vos équipements

L'étape suivante est de savoir ce qui est connecté à votre réseau domestique et de s'assurer que ces équipements sont bien sécurisés. Cela pourrait 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 thermomètre de maison, ou peut-être même votre voiture. Une fois tous les périphériques connectés à votre réseau domestique identifiés alors vous pourriez être surpris par leur nombre. La meilleure façon de conserver l'ensemble de ces dispositifs sécurisés est de s'assurer qu'ils fonctionnent toujours avec la dernière version de leur système d'exploitation. Assurez-vous d'avoir activé la mise à jour automatique si l'option est disponible. Si cela ne l'est pas, alors vérifiez mensuellement la disponibilité éventuelle de nouvelles mises à jour et appliquez les si disponible. En outre, n'oubliez pas de visiter le site Web de votre FAI car ce dernier peut fournir des outils et des services 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.answersolutions.ch et http://answersecurity.com/

Ressources

OpenDNS :
http://www.opendns.org
Norton ConnectSafe :
http://dns.norton.com/dnsweb/dnsForHome.do
Scanner de sécurité réseau :
http://www.sophos.com/fr-fr/products/free-tools/network-security-scan.aspx
Gestionnaires de mots de passe :
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_fr.pdf

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