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

OUCH!

Dans ce numéro...

Internet des Objets

Qu'est-ce que l'Internet des Objets

Editeur invité

James Lyne (**@jameslyne**) est le responsable mondial de la recherche sur la sécurité au sein de la société de sécurité Sophos. « Grand geek » auto-proclamé, son expertise technique couvre une variété de domaines de sécurité. Il est instructeur certifié à l'institut SANS et participe souvent à des conférences dans l'industrie en tant qu'intervenant majeur.

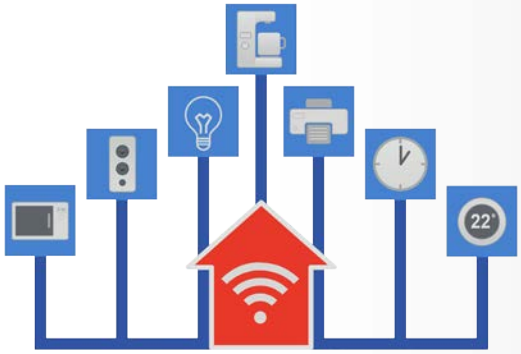
Dans le passé, la technologie était relativement simple, vous deviez simplement connecter votre ordinateur à internet et l'utiliser pour vos activités quotidiennes. Et puis la technologie a évolué avec l'arrivée dans vos vies des terminaux mobiles tels que les smartphones ou les tablettes. Ces terminaux permettent de mettre toute la puissance de calcul de vos ordinateurs de bureau dans votre poche. Beaucoup plus mobiles, ces terminaux posent de nouveaux problèmes de sécurité qui leur sont propres. Désormais, ce sont les objets connectés qui sont la nouvelle grande avancée technologique. Les objets connectés représentent tous les objets du quotidien que l'on peut connecter à internet, cela va de vos sonnettes, en passant par les ampoules, les poupées ou encore les thermostats. Ces objets connectés peuvent rendre votre vie beaucoup plus simple - par exemple vos ampoules peuvent s'allumer automatiquement dès que votre téléphone détecte que vous arrivez proche de chez vous. Le marché de l'internet des objets évolue à un rythme impressionnant avec des nouveaux produits connectés apparaissant chaque semaine. Cependant, comme les terminaux mobiles, les objets connectés représentent un nouveau défi du point de vue de la sécurité. Dans ce numéro, nous allons vous aider à comprendre quels sont ces risques et ce que vous pouvez faire pour sécuriser vos différents objets connectés, votre domicile et bien évidement votre famille.

Les problématiques relatives à l'Internet des Objets

La puissance des objets connectés réside dans leur simplicité. Par exemple, vous pouvez simplement brancher votre machine à café et elle vous demandera automatiquement de se connecter au réseau wifi de votre domicile. Par contre, cette simplicité a un coût. Le problème majeur des objets connectés réside dans le fait que les sociétés qui les produisent n'ont pas d'expérience en sécurité, leur expertise réside dans la conception d'équipements électroménagers. Il y'a également des startups qui essayent de développer un produit le plus efficacement et le plus rapidement possible, comme on le voit sur Kickstarter. Ces sociétés ne sont préoccupées que par les profits et pas du tout par la sécurité. Il en résulte que beaucoup des objets connectés achetés aujourd'hui ne sont construits qu'avec peu ou pas de sécurité interne. Par exemple, certains ont des mots de passes par défaut connus de tous, voire même postés sur internet et qui ne peuvent pas être changés. De plus, beaucoup de ces objets ne

Internet des Objets

peuvent pas être configurés d'un point de vue sécurité et vous devez vous contenter de ce qui vous a été livré. Encore pire, beaucoup de ces objets sont difficiles à mettre à jour, voire tout bonnement impossible pour certains d'entre eux. En conséquence, nombre d'objets connectés que vous utilisez peuvent rapidement devenir désuets, avec des vulnérabilités qui ne peuvent être corrigées. Ce qui vous laisse vulnérable en permanence.



Identifiez les objets connectés qui sont sur votre réseau, isolez-les lorsque cela est possible, gardez-les à jour et protégez-les avec des mots de passe forts.

Comment protéger vos Objets connectés

Finalement, que pouvez-vous faire ? Nous souhaitons réellement que vous puissiez utilisez vos objets connectés de façon fiable et sécurisée. Ces objets proposent des options fantastiques qui rendent la vie beaucoup plus simple, en vous aidant à économiser de l'argent ou en améliorant la sécurité physique de votre domicile. De surcroit, avec l'augmentation croissante de ces objets vous n'aurez probablement pas d'autres choix que de vous équiper. Voici les différentes étapes que vous pouvez prendre en considération afin de sécuriser vos objets connectés.

- **Ne connectez que ce dont vous avez besoin**: Le moyen le plus simple de sécuriser un objet connecté est de ne pas le connecter à internet. Si cet objet n'a pas besoin d'être en ligne, ne le connectez pas à votre réseau wifi.
- **Créez des réseaux wifi séparés**: Si vous avez réellement besoin que votre objet connecté soit en ligne, n'hésitez pas à créer un second réseau, un réseau invité par exemple. Une autre option serait d'acheter un deuxième point d'accès wifi, uniquement pour ces objets. Cela permettra de les garder isolés de votre réseau, ainsi ils ne pourront pas être utilisés pour pénétrer votre réseau principal sur lequel se trouve vos ordinateurs et vos téléphones (qui reste la cible privilégiée des pirates).
- **Faites les mises à jour dès que possible**: Comme pour votre ordinateur ou vos terminaux mobiles, il faut garder les objets connectés à jour. Si votre objet à une option permettant la mise à jour automatique, activez-la.
- **Utilisez un mot de passe fort**: Changez tous les mots de passe de votre objet connecté en un mot de passe fort. Vous n'arrivez pas à vous souvenir de tous vos mots de passe ? Pas d'inquiétude nous non plus. C'est pourquoi n'hésitez pas à utiliser un gestionnaire de mots de passe pour les sauvegarder tous de façon sécurisée.

Internet des Objets

- **Les options de confidentialité**: Si votre objet connecté vous permet de modifier les options de confidentialité, limitez au maximum les informations qui sont partagées. Une méthode serait de désactiver complétement la possibilité de partager des informations.
- **Envisagez le remplacement**: A un moment donné, vous remplacerez votre objet connecté, notamment quand celui que vous avez présentera trop de vulnérabilités qui ne pourront être corrigées ou alors qu'un remplaçant plus sécurisé sera disponible.

Il n'y a pas de règles miracles pour sécuriser tous les objets connectés, c'est important de vérifier les bonnes pratiques et les publications de chaque objet sur la manière de les sécuriser. Malheureusement la plupart des objets connectés n'ont pas été développés avec la sécurité à l'esprit et beaucoup de constructeurs ne proposent pas de solutions de sécurisation. Mais à mesure que la sensibilisation envers la sécurité augmente, nous espérons voir de plus en plus de constructeurs d'objets connectés intégrer nativement la sécurité dans leurs produits et fournir en plus des informations afin de les protéger et de les mettre à jour.

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
Les gestionnaires de mots de passe :	https://securingthehuman.sans.org/ouch/2015#october2015
Sécuriser votre nouvelle tablette :	https://securingthehuman.sans.org/ouch/2016#january2016
Sécuriser votre réseau domestique :	https://securingthehuman.sans.org/ouch/2016#february2016

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traduit par : Marilyn Combet