LABS

GUIDE DE SÉCURITÉ ET CONFIDENTIALITÉ DU CONSOMMATEUR D'IDO

Protégez Vos actifs et vos données d'IdO d'un compromis

Sortie : Avril 2017

Ce guide est le résultat du Programme de Coopération de Cyber Sécurité (PCCS) de la santé publique du Canada. En utilisant nos techniques d'essai exclusive, TwelveDot Labs a été engagé pour faire des recherches sur les risques et l'impact sur les consommateurs canadiens et les entreprises qui utilisent des produits et services insécuritaire de l'IdO.

Ce guide présente les découvertes et recommandations de cette recherche. Nous espérons que vous trouverez le contenu utile, facile à comprendre et à mettre en place. Si vous trouvez que vous avez des questions sur le contenu, vous pouvez nous contacter de manière suivante.

Courriel	Twitter	LinkedIn
security@twelvedotlabs.com	TwelveDotSecurity	TwelveDot

Avec l'application rapide de la nouvelle technologie et la capacité à rapidement introduire les électroniques avec des applications mobiles, l'Internet des Objets (IdO) changera radicalement notre façon de vivre. De fournir plus de liberté aux personnes âgées, à permettre aux enfants handicapés de s'intégrer pleinement dans les écoles publiques, les possibilités sont grandes. Cependant, avec cette grande opportunité se présente également une grande exposition et un grand risque que les consommateurs doivent rapidement commencer à se renseigner sur.

Ce guide tente de fournir les détails nécessaires et les références qui doivent être utilisés lorsque l'on envisage l'achat de nouveaux produits et services de l'IdO. Notre objectif est de nous assurer que vous en savez assez pour poser les bonnes questions aux fournisseurs et vendeurs dans les magasins de détail avant d'acheter.

La compréhension des risques est aussi facile que la lecture de l'actualité. Un certain nombre de produits de l'IdO sont réellement conçus pour les situations les plus vulnérables et les personnes parmi nous. En tant que tel, les conséquences peuvent être très graves. Voici certaines des plus graves où il est facile de voir le besoin pour comprendre votre exposition et les risques avant l'achat d'une nouvelle solution. Il s'agit notamment de :

1. Moniteur pour bébé
2. Piratage de voiture
3. Moniteur de conditionnement physique avec SPG
4. Voiture connectée
5. Systèmes d'automatisation et systèmes sécuritaire pour maison

A un niveau élevé, gardez à l'esprit que, bien que ces technologies fournissent la liberté pour vous de garder un œil sur vos proches et vos biens personnels ou vous vous engagez avec des assistants personnels, le même est également vrai pour n'importe qui qui obtient l'accès à vos systèmes. Ils suivent vos déplacements et peut frapper (dans une forme ou une autre) à un moment où vous vous y attendez le moins et cela fonctionne le mieux à leur avantage. La surveillance se situe à plusieurs niveaux, notamment :

1. Votre location (géographique)
2. Votre adresse IP
3. Votre WIFI IDES et parfois mots de passe
4. Votre compte utilisateur
5. Vos habitudes d’utilisation d ‘application

Ensemble, tous ces aspects, en substance, forme vos habitudes. Une fois que quelqu'un sait vos habitudes, vous pouvez devenir une cible plus facile pour le cyber-crime. Gardez à l'esprit, la nature même de l'IdO franchis les frontières. Elle permet aux criminels dans les districts éloignés de cibler vous et votre famille. Leur

manque d'attachement affectif à un particulier, leur permet de négliger l'impact de leurs actes au niveau personnel. Ils cherchent des façons de faire de l'argent et n'ont pas vraiment de savoir qui est blessé dans le processus.

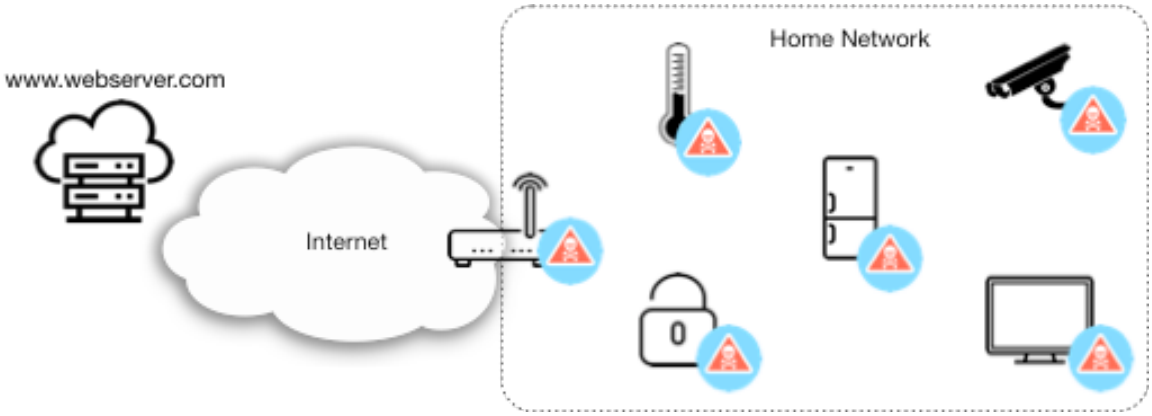

Figure 1: Zones de danger de l'IdO

La figure 1 indique le nombre de zones de danger pour les consommateurs de l'IdO. Les consommateurs ont besoin de comprendre ce sont les cibles d'attaque des pirates informatiques. Beaucoup de vendeurs, en raison de l'insuffisance des connaissances et des pratiques de sécurité, fourniront des produits et des solutions qui pourraient mettre vous et votre famille à risque. Gardez à l'esprit que les pirates informatiques tentent généralement d'attaquer le point faible, et puis pivotent pour quelque chose de plus intéressant pour les données et la surveillance. La section qui suit décrit ces risques.

Risques

1. Utiliser l'équipement ancien ou ne pas mettre à jour vos périphériques à la dernière version du logiciel ou micro logiciel permettent aux pirateurs de profiter des faiblesses connues
2. Utiliser des configurations par défaut sur les appareils, y compris les mots de passe prédéfinis qui sont bien connus
3. L'ouverture des trous dans votre pare-feu à l'accès à distance de vos appareils à domicile permettra aussi aux autres d'avoir accès à ces appareils
4. La non lecture des politiques de collecte de données des fournisseurs et des vendeurs permettra la collecte de données sans entrave de vous et votre famille. En général, ces données sont vendues pour des bénéfices à des spécialistes du marché.
5. Ne pas savoir comment vos appareils peuvent vous espionner, en particulier les périphériques avec les caméras et microphones. Être extrêmement vigilants lors de l'examen de ces dispositifs.

Avant d'acheter

Quelles questions devez-vous poser avant d'acheter un nouveau produit ou solution d'IdO ? Plusieurs de ces réponses peuvent être trouvées sur le site web des fournisseurs ou chez un détaillant. Les vendeurs ont généralement une page qui est dédiée à la sécurité et la confidentialité de leur(s) produit(s). S'ils ne le font pas, cela devrait être un avertissement que leur position sur la cybersécurité n'est peut-être pas suffisant. Au minimum, les vendeurs doivent être en mesure de fournir des détails sur les points suivants :

1. Vérifier les conditions d'utilisation, de sécurité et/ou à la politique de confidentialité du vendeur. Rechercher un libellé qui se réfère à ce qui suit :
    a. Quelles sont les données qu'ils recueillent et que font ils avec elles ?
    b. Vont ils vous prévenir en cas d'une violation de données ?
    c. Géographiquement, où dans le monde est ce que de vos données sont-elles stockées ?
    d. Est-ce qu'ils adhèrent aux lois canadiennes sur la protection des renseignements personnels ?
    e. Comment est-ce qu'ils vous alertent, le consommateur, des failles de sécurité et des risques spécifiques à leur produit ?
2. Quelles fonctionnalités de sécurité le produit a-t-il ? Recherchez les éléments qui pourraient indiquer que le produit peut être configuré pour fournir un niveau de sécurité plus élevé, si nécessaire. Cela peut inclure :
    a. Comptes utilisateur configurables
    b. Méthode pour mettre à jour le produit
    c. La connectivité PS ou PTSH du capteur au réseau du fournisseur
    d. Compte administrateur mot de passe peut-être modifié à partir de la valeur par défaut
    e. Le vendeur a t-il effectué une évaluation de sécurité lors du test de leur produit et/ou service ?
    f. Chercher le nom du vendeur et les expositions et Vulnérabilités Courantes (EVC) sur DuckDuckGo ou d'autres moteurs de recherche
3. Le vendeur livre blanc de la sécurité ou du document pareil qui décrit la manière dont il gère la sécurité ?
4. Quels sont les services offerts par les détaillants pour vous avertir des vulnérabilités dans les produits qu'ils vendent ?

Comment réduire considérablement votre exposition :

1. Changer les mots de passe par défaut à la suite de la configuration. Utiliser un outil pour générer des mots composés de 8 ou plusieurs caractères alphanumériques avec au moins un caractère spécial. S'assurer que ce mot de passe n'est pas utilisé n'importe où ailleurs. Ceci sont justes des minimums donc gardez cela en perspective.

2. Utiliser un RPV pour vous connecter à votre réseau domestique pour accéder aux périphériques. Ne pas ouvrir des ports du pare-feu pour autoriser l'accès à distance. Si votre pare-feu contient des fonctionnalités avancées, prévenez ces dispositifs de façon arbitraire d'avoir accès à l'Internet.
3. Utiliser un gestionnaire de mots de passe pour sauvegarder les différents mots de passe afin que vous pouvez conserver les mots de passe longs et aléatoires pour tous vos périphériques. Par exemple, LastPass fournit un seul mécanisme pour stocker et accéder à vos mots de passe. Certains systèmes d'exploitation offrent maintenant cette fonction aussi bien.
4. Mettre à jour la dernière version du micro logiciel lorsqu'un produit est nouveau et surveiller le site du vendeur pour les mises à jour au moins une fois par mois. De nombreux fournisseurs ont des listes de diffusion de sécurité servant de fournir des notifications au cas de failles de sécurité.
5. Endurcir votre installation de réseau Wifi. Cela inclut les fonctions intégrées à votre routeur :
    a. N'utilisez pas votre routeur sans fil comme votre seul moyen de défense. Obtenir un autre routeur ou pare-feu pour protéger vos données à caractère personnel et réseau.
    b. Utiliser un long mot de passe pour votre IDES. Ils ne doivent pas être simple ni facile à deviner. Voir le point 1 ci-dessus sur des suggestions de mots de passe plus forts.
    c. Désactiver la fonctionnalité WPS du routeur sans fil
    d. Désactiver la fonctionnalité réseau partagé s'il n'est pas utilisé. Si utilisé, assurez-vous que vous avez des mots de passe et de le changer au moins tous les mois.
    e. Utiliser l'épinglage Mac pour autoriser uniquement les périphériques connus de communiquer sur votre réseau sans fil
    f. Ne pas diffuser votre IDES. Bien que pas à toute épreuve de la protection des réseaux visibles sont plus facilement cibles d'attaque.
    g. Mise à jour à la dernière version du micro logiciel de votre appareil
    h. Ne pas autoriser l'accès distant à votre appareil
    i. Désactiver tous les services inutiles tels que l'UPnP, le VPN, etc.
    j. Éteignez votre appareil et Internet quand vous voyager pendant de longues périodes de temps
    k. Examiner les journaux du routeur pour voir ce qui est ciblé sur votre réseau.
    l. S'inscrire pour les notifications de sécurité des fournisseurs. Si et lorsque des correctifs sont disponibles, assurez-vous de mettre à jour

Résumé
A ce niveau, vous avez grandement réduit votre exposition par rapport à la majorité des consommateurs. Maintenez l'élevage de sécurité de vos appareils et posez toutes vos questions avant de dépenser votre argent durement gagner sur un risque de sécurité pour vous et votre famille.

Plus d'information sur la sécurité et les risques pour la vie privée peuvent être trouvés sur les sites suivants :

1. Commissariat à la protection de la vie privée du Canada
2. Les bureaux provinciaux de la vie privée
3. Sécurité Publique du Canada
4. Sites de sécurité du vendeur

Acronymes

EVC	Expositions et les Vulnérabilités Courantes
SPG	Système de Positionnement Global
PTSH	Protocol de Transport Sécuritaire Hypertext
IDES	Identificateur De l'Ensemble des Services
PS	Protocol Sécurisé
RPV	Réseau Privé Virtuel

Acronymes en anglais

CVE	Common Vulnerabilities and Exposures
GPS	Global Positioning System
HTTPS	Hypertext Transport Protocol Secure
SSID	Service Set Identifier
SSL	Secure Sockets Layer
VPN	Virtual Private Network