LABS

GUIDE DE SÉCURITÉ ET DE CONFIDENTIALITÉ DES ENTREPRISES IDO

Protégez vos consommateurs et vos donnés d'IdO d'un compromis

Sortie : Avril 2017
Traduit : Juin 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

L’Internet des Objets (IdO) a été aux alentours pendant des décennies, mais maintenant avec les progrès réalisés dans la fabrication microélectronique, il permet à une multitude de capteurs et actionneurs d’être accédé et de supporter via l'Internet.

Les 3 clés de la sécurité de l'information, la confidentialité, l'intégrité et l'authenticité s'appliquent toujours à l'IdO, toutefois, selon la façon dont ils sont appliqués, ils peuvent devenir un problème de sécurité. La sécurité est généralement considérée dans le secteur industriel, mais avec les soins de santé, l'agriculture, et les autres secteurs, un capteur défectueux peut causer des dommages aux humains.

Les entreprises doivent pouvoir quantifier les risques de leurs systèmes IdO, leurs fournisseurs de services, leurs fournisseurs de composants et leurs équipes de support sur le terrain. Le risque prendra plusieurs formes et les gestionnaires devront être vigilants pour quantifier et évaluer le le risque en utilisant une approche de système de système pour la gestion des risques. La capacité de qualifier ce risque fournira la diligence raisonnable nécessaire pour déterminer la responsabilité après le compromis.

Ce guide décrit les systèmes qui doivent être considérés et quantifiés quand une évaluation des risques est menée. Les systèmes d'IdO peuvent être complexes et seront composés de plusieurs fournisseurs, systèmes, composants, et même le personnel.

En ce moment, plusieurs appareils qui sont compromis sur un réseau d'IdO sont utilisés comme un point de pivot pour attaquer d'autres services sur le réseau ou sont utilisés comme arme pour attaquer des sites tiers et même des gouvernements étrangers. Avoir de solides pratiques de gestion du risque qui assurent que tous les risques sont identifiés et atténués au minimum requis est la clé à votre succès.

Une approche à la compréhension de l'IdO à partir d'une perspective de sécurité et de risque est le concept de "système de systèmes". Dans ce contexte, vous devez d'abord évaluer chaque système indépendamment et ensuite regarder chaque lien d’un point de vue processus et logique entre chaque système jusqu'à ce que tous les autres liens sont identifiés. En ce moment, et seulement en ce moment, vous pouvez vraiment traiter un modèle et comprendre les risques du système d'IdO.

En utilisant le système des systèmes un évaluateur devrait considérer ce qui suit comme un minimum lors de l'évaluation d'une solution, d’un produit ou d’un service d'un fournisseur de l'IdO :

1. Une pratique de la gestion du risque qui fait partie d'un des Systèmes de Gestion de la Sécurité de l'Information (SGSI) ou d'autres processus formels d'atténuation des risques de sécurité au sein de l'ensemble de

l'organisation. Il devrait commencer par les cadres supérieurs et retomber sur les membres du personnel les plus bas qui ont accès à des renseignements confidentiels de l'entreprise.

2. Le Cycle de Développement du Logiciel (CDL) du vendeur devrait avoir des aspects de sécurité et de confidentialité construit dans leur CDL. C'est facilement validé avec l'évaluation des risques, évaluation des facteurs relatifs à la vie privée, et de la documentation de produit.
3. Gestion de la menace et de la vulnérabilité de processus et de procédures
4. Politiques et pratiques des ressources humaines
5. Gestion des incidents
6. Gestion de l'actif et de l'opérationnel
7. La gestion de la chaîne d'approvisionnement
8. Gestion des fournisseurs tiers
9. Adhésion aux mises à jour de la législation LPRPDÉ au Canada.

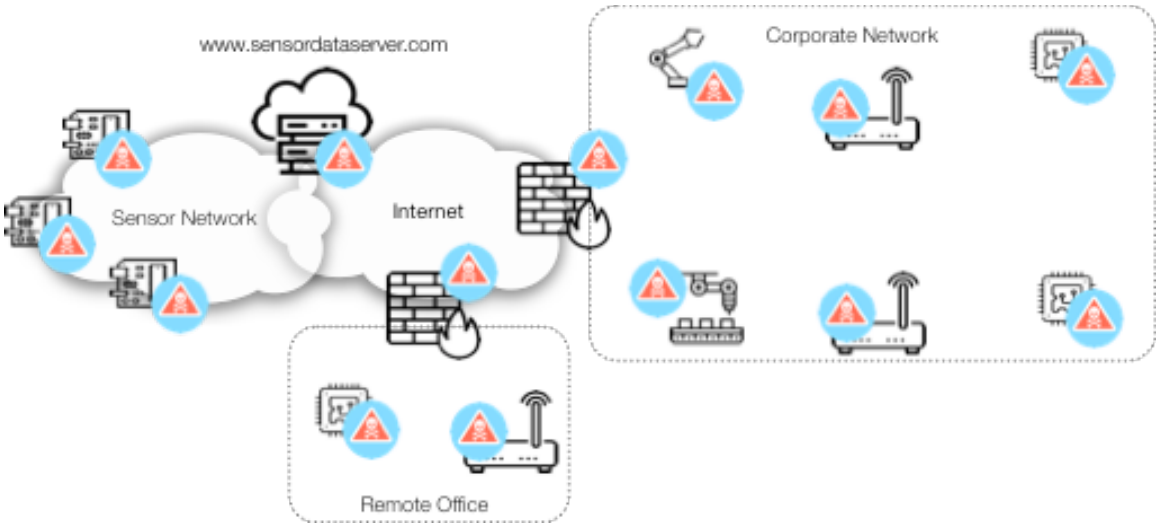

Figure 1: Zones de danger d'IdO

La figure 1 identifie plusieurs zones de danger de l'IdO des entreprises. Les entreprises ont besoin de mieux quantifier leurs risques à travers tous les systèmes qui compromettent leurs réseaux d'entreprise et leurs réseaux d'IdO. Comme beaucoup d'entreprises utilisent maintenant les d'aspects des édifices intelligents pour surveiller les installations, la qualité de l'air et le contrôle climatique, connaitre les risques pour les capteurs et actionneurs devient critique.

Risques

Le plus gros risque d'une entreprise est la violation de ses données ou le compromis des données de l'IdO. En cas de la violation de données les aspects suivants doivent être considérés :

1. Perte de confiance en le vendeur et le fournisseur
2. Perte de réputation du vendeur
3. Éventuel procès pour négligence ou autre manque de protection ou de notification des utilisateurs au cours d'une violation de données
4. Défaut de signaler une violation de données en vertu de la LPRPDE
5. TI escroc qui sauvegarde des données confidentielles stockées sur les serveurs connus, généralement sur un sol étranger
6. L'armement de votre réseau d'IdO pour attaquer votre réseau d'entreprise ou d'autres sites tiers

Préparation de votre organisation pour des risques d'IdO

Avant d'acheter n'importe quelle solution, composant ou service, vous devez d'abord déterminer les données à risque pour votre solution d'IdO. Une fois que vous connaissez les données que vous allez collecter, le traitement et le stockage, vous serez en meilleure position pour comprendre les commandes qui seront nécessaires pour protéger ces données et le danger que ces données soient compromises.

1. Mettre en place un SGSI pour mieux comprendre vos données en danger et la meilleure façon d'atténuer les risques propres à votre organisation. Ces systèmes aident grandement les employés et les actionnaires à mieux comprendre l'importance de la sécurité et de la confidentialité des renseignements personnels à votre organisation.
2. Mettre en place une pratique de gestion des risques de sécurité qui permettront d'identifier les cyber-risque pour tous les projets qui ont une composante technologique.
3. Quelles sont les données importantes qui seront recueillies, traitées et stockées par votre produit/solution de l'IdO envisagé pour le déploiement ? En général, ceci est déterminé lorsque l'Évaluation de la Menace et des Risques (EMR) et Évaluation de l'Impact de la Vie Privée (EIVP) ont été effectuées.
4. Créer l'ensemble de règles et de procédures qui feront clairement que les employés, les partenaires et fournisseurs tiers comprendront vos exigences en matière de sécurité pour les implémentations de l'IdO.
5. Assurez-vous de bien comprendre la LPRPDÉ et comment il influe sur votre organisation.

Évaluer les fournisseurs et les produits tiers et services pour des risques

Maintenant que vous comprenez comment mieux protéger votre entreprise et vos données, vous devez porter votre attention sur les risques qui peuvent exister lors de la construction de votre solution d'IdO à l'aide d'un vendeur ou une organisation tiers. Les vendeurs et les fournisseurs de solutions doivent fournir un niveau de base d'assurance pour se protéger contre l'exploitation facile de leurs produits et services sur le terrain. Lors de la comparaison des fournisseurs pour la sécurité, n'oubliez pas que le plus de sécurité vaut toujours la peine. Le plus d'informations et d'assurance qu'un fournisseur peut fournir autour de leur position de sécurité et de confidentialité, le mieux pour vous et vos clients qui dépendent de ces solutions pour le revenu.

1. Est-ce que le fournisseur a un CDL sécuritaire ? Peut-il le prouver ?
2. Est-ce que le produit/service a subi un test ou une évaluation formelle de la sécurité ? Quels rapports peuvent-ils fournir pour prouver cela ?
3. Est ce que le fournisseur de services a subi un processus officiel de certification comme ISO, PCI-DSS, FIPS, Critères Communs ou d'autres évaluations formelles équivalentes ? Les autoévaluations peuvent fournir une vue sur les contrôles de sécurité, mais ils ont tendance à mettre le vendeur dans une lumière positive où la sécurité et la confidentialité sont concernés.
4. S'assurer que tous les appareils et composants ont la capacité d'être de mis à jour au niveau logiciel et peuvent être bien contrôlés pour la disponibilité et l'utilisation fonctionnelle.
5. Est-ce que le vendeur a un programme de divulgation des vulnérabilités et des règles de confidentialité affichée sur le site web ?
6. Vérifier la liste EVC pour déterminer le nombre de vulnérabilités connues existent actuellement pour le vendeur ? Cela fournira un bon aperçu des risques actuels de la solution, mais fournira une vue rapide de la qualité du code du vendeur.
7. Le vendeur a t'il une liste de messagerie de sécurité ?

Que faire pour réduire considérablement votre exposition :

1. Mener un EMR avec la portée suivante :
    a. Analyse complète du système
    b. Bibliothèques des fournisseurs tiers
    c. EVC des fournisseurs reliées aux produits et composants
    d. Mis à jour de la solution sur le terrain
    e. Modifier la résistance de la solution
    f. Administration des comptes utilisateur
    g. Surveillance du système et de la solution contre une attaque ou un compromis

    h. Inscrivez-vous à la liste de diffusion de sécurité du vendeur et de ses alertes
2. Déterminer le risque résiduel du système et déterminer ensuite si vous pourriez avoir besoin de l'assurance cybernétique pour vous protéger contre ce risque
3. Avez-vous un processus de traitement des incidents ? Si non, faites que cela soit créé et mis en œuvre. Cela comprend la formation de tous les membres du personnel qui auront besoin d'appuyer cet effort, y compris l'engagement des équipes de relations publiques et juridiques.
    a. Créer un organigramme qui :
        i. Identifie les données à risque des solutions de l'IdO. Quel est le pire des cas si ces données étaient compromises et exposées au public. Quel pourrait être l'impact possible à votre entreprise, vos clients et clients potentiels ?
        ii. Identifie tous les systèmes à considérer
    b. Pour chaque système
        i. Déterminer la meilleure pratique ou norme à utiliser pour contrôler la mise en œuvre
        ii. Quels contrôles sont nécessaires
        iii. Comment allez-vous détecter une défaillance dans ce contrôle ?
        iv. Comment allez-vous détecter une défaillance de ce système ?
        v. Le cas échéant, comment pouvez-vous réduire les risques?
4. Document, document, document ! S'assurer que vous créez une documentation qui décrit clairement le processus de gestion des risques et ce qui a été fait pour évaluer et atténuer ces risques. Cela peut inclure des informations venant des fournisseurs, des prestataires de service et d'autres qui fourniront le service à votre organisation.

Des informations supplémentaires sur la sécurité et les risques pour la vie privée peuvent être trouvés sur les sites suivants :

1. EVC – La liste de vulnérabilités (Lien en Anglais)
2. RepèreBug – Liste des problèmes de sécurité connus du logiciel. Bon point de départ pour repérer les vulnérabilités inconnues ou non classifiées (Lien en Anglais)
3. Sécurité Publique Canada – Le site de cybersécurité pour la sécurité Publique a plusieurs publication qui seraient utiles pour les petites et moyennes entreprises à mieux faire face aux défis de la cybersécurité.
4. LPRPDÉ – Nouvelle législation prévue d'être adoptée en automne 2017 pour toutes les entreprises quelle que soit la taille ou la nature de l'entreprise.

Acronymes

EVC	Expositions et les Vulnérabilités Courantes
SPG	Système de Positionnement Global
SGSI	Systèmes de Gestion de la Sécurité de l'Information
PTSH	Protocol de Transport Sécuritaire Hypertext
EIVP	Évaluation de l'Impact de la Vie Privée
LPRPDÉ	Loi sur la Protection des Renseignements Personnels et les Documents Électroniques
IDES	Identificateur De l'Ensemble des Services
PS	Protocol Sécurisé
EMR	Évaluation de la Menace et des Risques
RPV	Réseau Privé Virtuel

Acronymes en anglais

CVE	Common Vulnerabilities and Exposures
GPS	Global Positioning System
ISMS	Information Security Management System
HTTPS	Hypertext Transport Protocol Secure
PIA	Privacy Impact Assessment
PIPEDA	Personal Information Protection and Electronic Documents Act
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TRA	Threat and Risk Assessment
VPN	Virtual Private Network