LABS

GUIDE DE SÉCURITÉ ET CONFIDENTIALITÉ INDUSTRIELLE DE L'IDO

Comment évaluer la technologie et solutions avant l'achat ou le déploiement

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

Le présent guide est un aperçu des questions et des résolutions dans le domaine de l'IdO Industriel(IdOI). Ce domaine est très vaste et englobe de nombreux aspects tels que la sécurité, qui ne sont pas un facteur critique comme dans d'autres secteurs de l'IdO.

En raison de cet aspect crucial de la sécurité dans les systèmes d'IdOI, les acheteurs des systèmes doivent être conscients à la fois de la surface d'attaque et des risques liés à chaque composant et système déployé dans le cadre du système de contrôle industriel.

Du point de vue d'un acheteur, vous devez vous assurer que vous avez mis en œuvre un cadre de gestion des risques pour évaluer et quantifier le risque pour votre organisation. C'est une division typique entre les technologies de l'information (TI) et la Technologie Opérationnelle (TO). TO représente le plus grand risque pour la plupart des entreprises en raison de la possibilité que les composants tels que les actionneurs ou capteurs échouent durant l'utilisation ou deviennent une situation dangereuse. Les attaques peuvent entrainer une perte de revenus, des dommages aux installations ou équipements, des dommages à la réputation, la responsabilité potentielle, et des effets sécuritaires en raison des processus de dommages.

Bien que les risques cybernétiques prendre plusieurs formes, il est important de souligner que la sécurité et la vie privée dans IdOI est un équilibrage pour assurer l'efficacité opérationnelle et le coût des contrôles de sécurité à être déployés. Avoir un programme de sécurité dans le cadre d'un Système de Gestion de la Sécurité de l'Information (SGSI) ou Système de Gestion de la Cyber Sécurité (SGCS) devrait servir de base à la façon dont la sécurité est gérée à partir de la perspective de l'entreprise. Les aspects spécifiques de la sécurité TO devront être gérés à l'aide la combinaison de processus des entreprises via une méthodologie d'Évaluation de la Menace et des Risques (EMR) pour quantifier les risques pour les nouveaux systèmes puis mettre en place des contrôles pour les risques identifiés. Les concepteurs du système doivent être parfaitement au courant de cette approche combinée de ces systèmes IdOI, et il doit s'assurer d'équilibrer les besoins de chacun.

Dans le cadre d'un SGSI et d'un Cycle de Développement Sécurisé(CDS), les praticiens de la sécurité doivent travailler avec les employées de la TO pour s'assurer que la modélisation des menaces a été réalisée. Cela permettra d'assurer une bonne compréhension des vecteurs spécifiques qui peuvent être ciblés pour le système IdOI.

Les intégrateurs de système doivent veiller à ce que les systèmes d'IdOI qu'ils conçoivent satisfont aux exigences de la sécurité et de la confidentialité. Les violations récentes ont montré l'impossibilité d'identifier les risques et mettre en

Œuvre des contrôles d'atténuation ainsi qu'avoir un plan d'infraction constitue une négligence dans de nombreuses juridictions.

Pour des secteurs comme l'énergie, les bâtiments intelligents et les villes intelligentes, les intégrateurs de système ont besoin de travailler avec les équipes de sécurité des clients pour quantifier les risques de mise en œuvre. Ces engagements doivent être formalisés afin de s'assurer que les EMR et les API sont menées pour montrer les documents de vérification de risque entrain dêtre atténué. Les Intégrateurs de systèmes TO seraient bien avisés de se conformer à ces normes telles que IEC 62443 afin de s'assurer qu'ils ont identifié les commandes nécessaires des contrôles du système

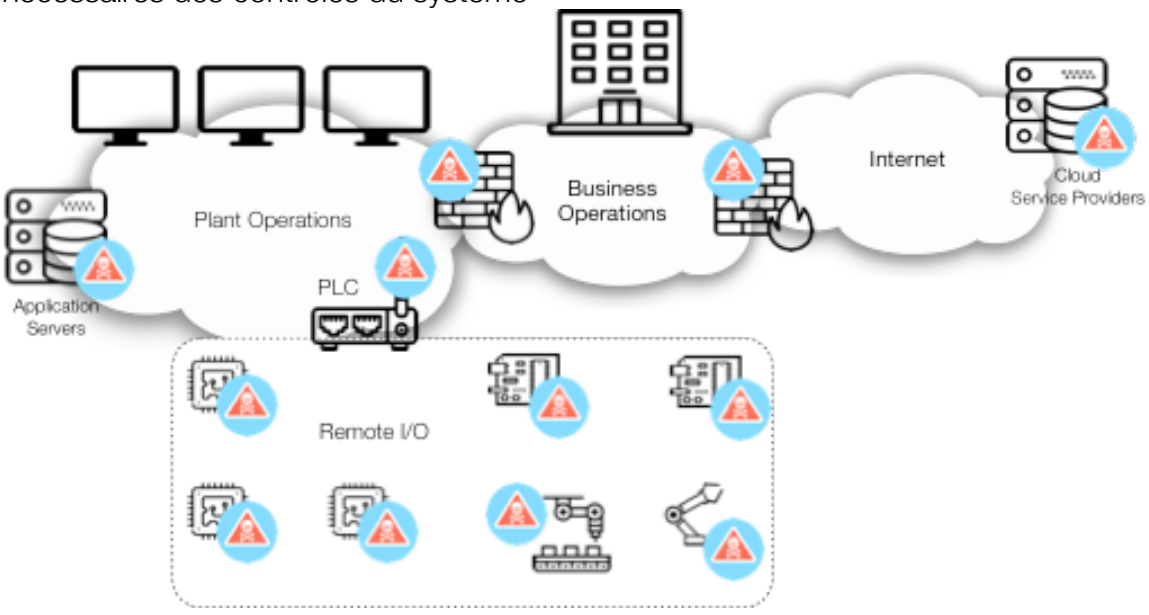

Figure 1 : Vecteurs d'attaques de l'IdOI

Risques :

Lors de la prise en compte des risques spécifiques à l'IdOI, vous devez tenir compte de ce que les résultats possibles pourraient être pour un périphérique donné, un réseau ou une usine sous attaque.

1. Lors de la réalisation d'une EMR, l'actif en vertu de l'évaluation doit être considérée comme un vecteur d'attaque. En tant que tel, il a besoin de plus examiner au minimum les attaques contre les éléments suivants :
    a. Physique
    b. Réseau
    c. Logiciel et/ou microprogrammes
    d. Operations et systèmes de surveillance
    e. Chaîne d'approvisionnement pour tous les composantes de ces systèmes

2. La sécurité physique pour les composants, les réseaux, et les déploiements. Dans de nombreux cas, ces appareils peuvent être facilement compromis une fois que l'accès physique a été obtenue.
3. Violation des rapports de confiance entre les organes et/ou les systèmes. En fonction du scénario de déploiement ou de l'architecture de nombreux déploiements utilisent un modèle de confiance qui permet la communication et la commande et le contrôle de prendre place entre les systèmes de contrôle opérationnel et les capteurs, les actionneurs, les CLP (Contrôleurs de Logique Programmable), les UCD (Unité de Contrôle à Distance), etc. dans un programme en construction.
4. Les déploiements Brown Field ont besoin de menace modèle la solution actuelle et les produits et déterminer les risques et les menaces qui existent avec la nouvelle technologie proposée pour être mis en œuvre. Il s'agirait notamment de produits où l'accès réseau distant est autorisé et devient le point d'attaque initiale de l'appareil.
5. Les déploiements Brown Field permettent à tous les risques et menaces pour la sécurité d'être identifiés et atténués avant la construction. Il est le meilleur scénario pour atténuer les risques cybernétiques. Il est conseillé que les EMR et la modélisation des menaces soient réalisées lorsque la plante ou installations sont en cours de conception. Cela permettra de réduire considérablement les couts liés à la mise en conformité ou à des changements de conception après le fait.
6. L'identité des éléments du système réseau, y compris l'authentification de ces éléments lors de l'exécution. Les opérateurs de systèmes ont besoin de s'assurer que les appareils et les éléments du réseau communiquent correctement et que les anomalies sont identifiées. Les périphériques indésirables et les tentatives d'accès au réseau devrait être rapidement identifiés et atténués.
7. Les contrôles d'accès physiques et logiques doivent être considérés ainsi que les mécanismes qui pourraient être utilisés pour les contourner. Les utilisateurs doivent uniquement être donné accès pour remplir leurs fonctions et toutes les tentatives d'accès ont besoin d'être registrées et cataloguées.
8. L'intégrité d'exécution devrait exister pour des actifs à risque plus élevé afin de s'assurer que des modifications non autorisées ont été apportées au système pendant l'exécution. Si un vendeur a un CDL sécuritaire ils doivent apporter la preuve de ceci ainsi que la certification officielle du produit.
9. L'intégrité de l'amorçage s'assurera qu'en cas de panne ou d'accès physique la compagnie ne peut pas être remplacé par une qui est vulnérable ou menacée. Si un vendeur a un CDL sécurisé, ils doivent apporter la preuve de ceci ainsi que la certification officielle du produit.
10. Les données peuvent être attaqués au cours de plusieurs phases de transformation et de manutention. Toutes ces étapes doivent être considérées. Les phases de données peuvent être considérées comme suit :

a. Quel est le risque pour les données au repos (DAR), ce sont les données stockées sur un support physique ou logique moyen tels que SSD ou la suppression des médias.
b. Quel est le risque pour les données en mouvement (DIM), ce sont les données transmises entre deux ou plusieurs éléments du système
c. Quel est le risque à des données d'utilisation (DEU), ce sont les données qui sont en cours de traitement par une mémoire volatile et un CPU ou microcontrôleur.

11. S'assurer que votre intégrateur de systèmes construit les systèmes basés sur la To à IEC 62443 avec les exigences de contrôle au minimum. Ils devraient également recommander des produits et des solutions qui ont été certifiés selon cette norme.
12. S'assurer que la capacité de résilience de vos appareils est évaluée à travers les tests de robustesse de la communication (TRC). Le TRC assure que l'appareil maintient de manière adéquate les services essentiels tout en étant soumis au trafic de protocole réseau normal et erronées à des taux de trafic normaux et extrêmement élevés (conditions d'inondation). Ces tests comprennent des tests spécifiques pour la susceptibilité aux attaques réseau connus.

Questions à votre fournisseur ou intégrateur de solutions

Dans de nombreux secteurs tels que l'énergie et le pétrole et du gaz de nombreuses autres exigences réglementaires existent. Cela comprend la réalité que plus de vendeurs condidèrent la cybersécurité important et avoir leurs produits essayés à IEC 62443 pour un niveau plus élevé d'assurance. Pendant que c'est un grand pas pour les acheteurs de ces solutions vous devez également tenir en compte les aspects suivants pour réduire le risque et augmenter votre niveau d'assurance.

1. Est-ce que le produit et/ou la solution a été évalué officiellement à IEC 62443 ? Si non, pourquoi ?
2. Le vendeur a t-il un processus formel CDL sécurisé ? Peuvent-ils le prouver ?
3. Quels évaluations tierce ont été menées contre le produit ou la solution comme l'analyse sécurisée du code, les tests de pénétration, et la certification d'autres produits qui pourrait indiquer que e produit a subi un certain niveau de tests de sécurité ?
4. Quelle caractéristique de la technologie le vendeur a dans leur produit/solution IdO qui traite des sujets suivants :
    a. La confiance dans leur infrastructure opérationnelle cela comprend les aspects supplémentaires de :
        i. Assurer l'exécution de code sur le microcontrôleur et les composantes
        ii. Contrôle sécurisé de la mise à jour à partir de serveurs autorisés

iii. Démarrage sécurisé du chargement de code système pour les capteurs, les actionneurs et les autres éléments qui composent la solution
iv. La surveillance sécuritaire à partir des systèmes d'opérations autorisées

b. Si les IPI (Informations Personnellement Identifiables) sont recueillies, la protection de la vie privée a-t-elle été considérée pour les données IPI recueillies. Il peut s'agir de techniques d'identification pour des données stockées dans un entrepôt de données. Les utilisateurs sont-ils tenus de signer une déclaration pour collecter ou stocker leurs données ? Dans quels pays les données sont stockées et traitées et quelles lois s'appliquent ?
c. La gestion des identités et des accès (GIA), ceci couvre de nombreux aspects, mais ils devraient comprendre :
    i. L'identification de l'utilisateur accède au système et aux composants
    ii. L'identification des composantes dans le terrain et durant le déploiement
    iii. L'identification du réseau et de services de communications d'authentification des couches.
d. L'évolutivité doit être considéré non seulement pour le déploiement envisagé aujourd'hui, mais à l'avenir si les composants et services de l'IdOI ne peut pas être

5. Les spécifiques des entreprises et des organisations d'IdOI doivent tenir compte des aspects minimum suivants :
    a. Sécurité fonctionnelle
    b. L'interopérabilité
    c. La résilience
    d. La disponibilité

Que pouvez-vous faire pour réduire considérablement votre exposition

Le moyen le plus rapide pour réduire vos risques de cyber-attaques d'IdOI est de comprendre vos vecteurs de menaces et avoir conscience de la situation des menaces au System de Contrôle Industrielle (SCI). Cela comprend la mise en œuvre du cadre de gestion des incidents nécessaires pour contenir rapidement les violations des données et/ou du système et de retour à l'état de fonctionnement normal.

1. S'assurer que vous disposez de soit un SGCS ou un SGSI qui décrit clairement les biens à protéger et les besoins en matière de risques. En général, ces systèmes auront des politiques et procédures connexes, ainsi que la formation de sensibilisation pour tous les niveaux du personnel.
2. S'assurer que votre processus de gestion du changement comporte les éléments suivants :

    a. Inventaire de l'actif
    b. Processus d'approbation
    c. La documentation de l'évolution et du retour des procédures dans chaque ticket de modification créé, approuvé et traité.
    d. S'assurer que seul le personnel autorisé peut faire des changements de tickets
3. Comprendre vos données en danger au moment de la collecte, le traitement et le stockage de tous les systèmes critiques. Les aspects suivants doivent être pris en compte au minimum :
    a. Quels risques existent si les données étaient compromises ?
    b. Quel est le potentiel des risques de sécurité si le système était compromis ?
4. Se préparer pour le jour ou une violation se produit avec un plan de violation et un plan de gestion des incidents. Cela permettra d'assurer que le personnel dans ces évènements sont bien formés pour réagir, de quarantaine et de restaurer leur système de fonctionnement normal.
5. Évaluer officiellement tous les fournisseurs et intégrateurs de systèmes afin de comprendre leur niveau de compétence en cybersécurité, il s'agira notamment des aspects tels que :
    a. L'utilisation des produits/services conformes à la norme IEC 62443
    b. La réalisation d'une EMR et la modélisation des menaces contre la solution proposée
    c. Avoir des mécanismes permettant de déterminer quand un composant a été compromis ?
    d. Avoir un processus CDL sécurisé pour les produits et solutions en cours de développement
    e. Comment s'assurent-ils que les composants électroniques n'ont pas été compromises ?
6. Quel est le modèle de confiance des composantes déployées ? Comment sont-ils authentifiés à l'installation initiale lorsqu'ils sont sur surveillance et mises à jour ? Comment quelqu'un pourrait-il compromettre ce niveau de confiance ?
7. Ont-ils effectué des vérifications des antécédents de sécurité sur le personnel ?
8. Lire et mettre en œuvre les mesures de contrôle énumérés dans le Guide du NIST 800-82 pour la sécurité du système de contrôle industriel et du NIST Cadre pour les systèmes cyber-physiques

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

1. ISA99 – Détails pour IEC 62443 y compris l'évaluation et le processus de certification
2. NIST - Guide NIST 800-

3. Santé Publique Canada - Principes de sécurité informatique pour la communauté de l'EC

Acronymes

TRC	Test de la Robustesse de la Communication
SGCS	Système de Gestion de Cyber de Sécurité
DAR	Données Au Repos
DIM	Données En Mouvement
DEU	Données En Utilisation
GIA	Gestion des Identités et des Accès
IdO	Internet des objets
SGSI	Système de Gestion de la Sécurité de l'Information
EMR	Évaluation de la Menace et des Risques

Acronymes en anglais

CRT	Communication Robustness Testing
CSMS	Cyber Security Management System
DAR	Data at Rest
DIM	Data in Motion
DIU	Data in Use
IAM	Identity and Access Management
IoT	Internet of Things
ISMS	Information Security Management System
TRA	Threat and Risk Assessment