Guide sur l'IdO et la sécurité
#IdOAuTravail

Internet des objets

Trousse d'information pour les petites et moyennes entreprises

PENSEZCYBERSECURITE.CA

Canada

Table des matières

#IdOAuTravail

Introduction

La connectivité et l'automation que permet l'Internet des objets (IdO) favorisent le développement de tous les secteurs d'activité, mais elles comportent d'importants risques. Les appareils de l'IdO se connectent à un réseau pour communiquer entre eux et échanger de l'information, créant ainsi de nouveaux points d'accès à l'information sauvegardée sur le réseau et aux appareils utilisant celui-ci. Pour protéger votre petite ou moyenne entreprise (PME) des effets potentiellement dévastateurs de cyberincidents éventuels, vous devez la rendre cybersécuritaire.

En tant que propriétaire ou dirigeant d'une PME, vous croyez peut-être que celle-ci est à l'abri des cyberincidents, mais l'IdO augmente le risque de cyberincident ainsi que la complexité de la cybersécurité.

Dans ce guide, vous apprendrez comment l'IdO fonctionne et quelles incidences il aura sur votre entreprise, en plus des risques qu'il présente pour la sécurité de l'information, la confidentialité et la sécurité en général. Notre stratégie de cybersécurité en cinq étapes vous aidera à mettre en œuvre l'IdO dans votre entreprise de façon sécuritaire et à élaborer une politique sur la sécurité de l'IdO qui s'harmonise à celle sur la cybersécurité déjà en vigueur.

La sécurité de l'IdO est une responsabilité partagée par la direction, le service des TI et le personnel.

En plus du présent guide, vous trouverez, dans **la trousse d'information #IdOAuTravail**, d'autres ressources à partager au sein de votre entreprise **PensezCybersecurite.ca**.

Ce guide fait référence à des sections du Guide Pensez cybersécurité pour les petites et moyennes entreprises, dont il est le compagnon. Le symbole vous indiquera la section à consulter dans le Guide Pensez cybersécurité pour les petites et moyennes entreprises pour obtenir un complément d'information.

L'Internet des objets

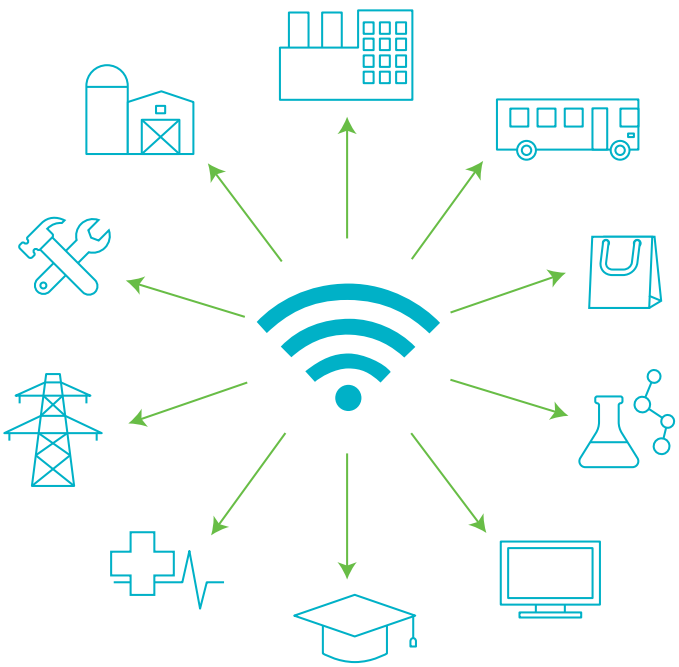
L'IdO est un réseau créé à partir d'appareils intelligents qui sont connectés et qui communiquent entre eux via un réseau comme Internet. Les appareils connectés recueillent et échangent de l'information entre eux grâce à des logiciels, caméras et capteurs capables de détecter la lumière, les sons, la distance, les mouvements, etc. Ils peuvent être contrôlés et surveillés à distance, mais la plupart fonctionnent automatiquement. Parmi les appareils intelligents, on trouve des électroménagers, des serrures, des caméras de sécurité, des équipements de production et des véhicules connectés.

L'Internet multidimensionnel est un prolongement de l'IdO qui englobe le système plus complexe constitué de la communication de machine à machine, de personnes et de processus. Autrement dit, l'Internet multidimensionnel est un réseau composé de personnes, de données, de processus et d'appareils.

L'Internet des objets industriel (IdOI), quant à lui, désigne l'intégration des technologies de l'IdO, de capteurs en réseau et de logiciels dans du matériel de fabrication, etc. On l'appelle aussi l'Internet industriel.

Les secteurs d'activités qui emploient l'IdO

L'Internet des objets est utilisé dans des secteurs d'activité variés, de l'agriculture aux soins de santé en passant par celui de la fabrication.



Voici quelques progrès réalisés grâce à l'IdO :

- **Commerce de détail**
  - Caisses automatisées
  - Gestion des stocks et de l'entrepôt
- **Fabrication**
  - Opérations plus performantes
  - Gestion et entretien des biens
- **Consommateurs**
  - Divertissement
  - Santé et activité physique
- **Bureaux et gouvernement**
  - Amélioration de la productivité et économie d'énergie
  - Sécurité et surveillance
- **Transports**
  - Automatisation et contrôle de la circulation
  - Gestion des parcs de véhicules
- **Soins de santé**
  - Suivi médical
  - Administration automatisée des traitements

L'IdO et les risques pour la sécurité de l'information

La mise en œuvre de l'IdO au sein d'une entreprise comporte un obstacle de taille qu'il importe de surmonter : la sécurité. Une atteinte à la sécurité pourrait avoir d'importantes répercussions sur la réputation et la crédibilité de l'entreprise, et se traduire par une perte de temps et d'argent, en plus d'avoir des conséquences juridiques.

Les appareils de l'IdO se connectent entre eux, mais aussi au réseau de votre entreprise et aux autres appareils qui utilisent celui-ci, sans oublier le fournisseur de l'IdO et les appareils de votre personnel et de vos clients. En raison de cette interconnectivité et de cette automatisation, un cyberincident pourrait avoir des répercussions sur les affaires de votre entreprise, depuis son siège social jusqu'à vos clients en passant par sa chaîne d'approvisionnement.

Qu'il s'agisse d'incidents ciblant des appareils en particulier ou d'incidents indirects causés par des menaces virales comme des logiciels malveillants, les cyberincidents peuvent avoir des effets en aval sur la sécurité des TI de votre entreprise et affaiblir toute l'infrastructure des TI. Par exemple, si votre entreprise possède un parc de camions de livraison pour son système de transport intelligent et que le programmeur ou constructeur des camions est touché par un logiciel malveillant, celui-ci pourrait aussi perturber indirectement tous vos camions connectés. Pour de plus amples renseignements sur les logiciels malveillants, consultez la section Sécurité sur le Web — Programmes malveillants.

Chaque connexion augmente le degré de vulnérabilité de votre entreprise. Il est impossible de protéger l'information qui circule sur votre réseau si vous ne contrôlez pas l'accès des personnes et des appareils qui s'y connectent. Pour de plus amples renseignements sur la sécurité de l'information, consultez la section Sécurité des données.

L'IdO et la confidentialité

Qu'il soit lié à l'IdO ou non, tout cyberincident augmente considérablement les risques de vol, de divulgation ou d'altération de l'information. Ainsi, l'information concernant votre entreprise, vos employés et vos clients pourrait être détruite, altérée, volée ou publiée, ou même « retenue en otage » jusqu'au versement d'une rançon.

Les appareils connectés collectent de grandes quantités de données, ce qui représente un motif de préoccupation pour la confidentialité et l'intégrité des données de l'entreprise. Assurez-vous d'utiliser des appareils connectés qui font preuve de transparence en ce qui a trait à leurs politiques sur la collecte des données. Ces politiques devraient préciser quelle information sera collectée, combien de temps elle sera conservée et à quoi elle servira (à des recherches marketing, etc.).

Si vous déployez l'IdO dans votre entreprise, vous devriez mettre à jour vos politiques concernant la confidentialité. Vous devriez envisager de recourir à une organisation professionnelle spécialisée en cybersécurité pour mener une étude d'impact en matière de confidentialité, établir des normes pour l'IdO et définir des degrés de sécurité pour les rapports entre les utilisateurs et les machines ou appareils. Par exemple, l'utilisation par un employé sûr d'un appareil non sécurisé devrait être considérée comme non sécuritaire et être soumise à des restrictions. Vous pourriez également vous adresser à un conseiller juridique pour comprendre et réévaluer les exigences et responsabilités légales, les déclarations de confidentialité des appareils connectés et les dispositions contractuelles.

Par ailleurs, la sécurité et la confidentialité de l'information concernant vos employés pourraient aussi être compromises par le biais des appareils personnels connectés au réseau de l'entreprise. En informant vos employés sur l'IdO et en leur offrant une formation

sur le sujet, vous contribuerez à protéger leur vie privée. Dans cette optique, vous pourriez élaborer une politique sur l'IdO, semblable à une politique « Apportez votre équipement personnel de communication » (AVEC), qui traite de l'accès au réseau, des appareils autorisés, des mots de passe, des sites Web sécurisés, etc. Pour de plus amples renseignements sur les politiques, consultez la section Questions de gestion — Élaboration de politiques et de normes.

L'IdO et la sécurité

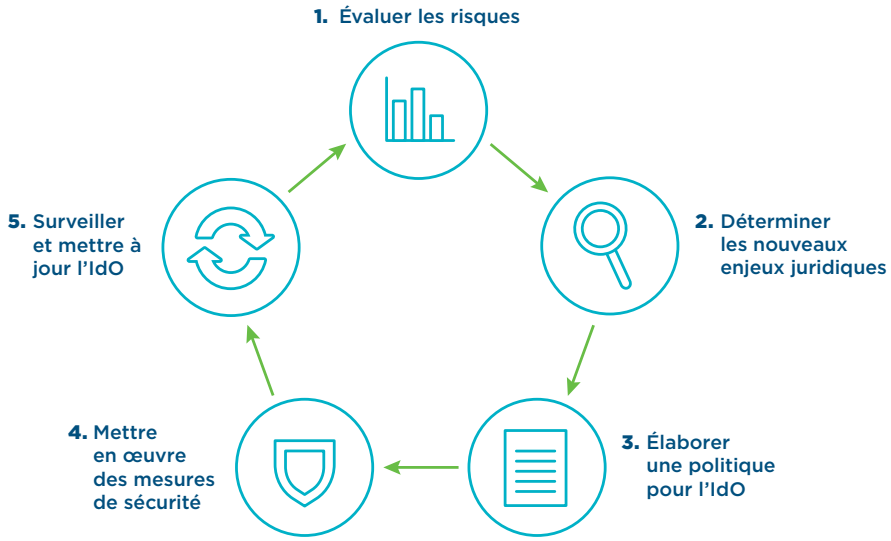
Quand un appareil connecté contrôle des biens matériels et des opérations, comme un véhicule intelligent ou une pompe à insuline, la menace que fait planer un cyberincident éventuel ne se limite pas à une brèche dans la sécurité de l'information. L'utilisation non autorisée ou la prise de contrôle à distance d'un objet connecté pourraient endommager les données et l'équipement de votre entreprise ou causer des dommages physiques à des personnes. Ces dommages pourraient s'avérer coûteux, si vous devez réparer les systèmes et équipements de votre entreprise et rétablir sa réputation. Le rôle que jouent de nombreux objets est bien plus important que l'information qu'ils emmagasinent. Pensez aux conséquences juridiques et financières que pourraient entraîner la défaillance ou le piratage d'un appareil connecté, par exemple. Pour de plus amples renseignements sur la sécurité, consultez la section Sécurité matérielle.

Pour protéger votre équipement, votre personnel et vos clients, le cadre de sécurité de base pour l'IdO devrait tenir compte de l'appareil, de l'aspect contrôle à distance et l'infrastructure des TI, et comprendre :

- Démarrage sécurisé et fonctionnalité de réinitialisation
- Authentification et intégrité
- Chiffrement
- Pare-feu
- Mises à jour
- Détection d'intrusion et production de rapports
- Contrôle et vérification à distance

L'IdO et votre entreprise : stratégie de cybersécurité

L'implantation de la nouvelle technologie de l'IdO nécessite une démarche descendante par étapes. Les cinq étapes de notre stratégie de sécurité couvrent les mesures de base pour mettre en œuvre l'IdO dans une entreprise. Elle peut également servir pour les processus et contrôles relatifs aux TI dans l'entreprise, qu'ils soient établis en réseau ou non. Pour de plus amples renseignements sur les cyberstratégies, consultez la section Questions de gestion — Planification de la cybersécurité.



Étape 1 : Évaluer les risques

La première étape consiste à procéder à une évaluation rigoureuse des risques pour mettre à jour les politiques de sécurité. En raison de l'IdO, des cybercrimes peuvent être commis à des endroits inattendus. Le profil de risque de votre entreprise devrait tenir compte de l'IdO.

- Analysez les menaces et évaluez les risques relativement à la confidentialité en considérant la façon dont les objets connectés interagiront entre eux.
- Vérifiez les applications, appareils, réseaux, banques de données et protocoles de communication. Établissez l'interopérabilité des appareils que vous possédez déjà.
- Quels appareils et quelles personnes utilisent votre réseau? Quelle est l'importance de cette information ? Déterminez toutes les faiblesses de votre réseau et envisagez les pires éventualités.

Étape 2 : Déterminer les nouveaux enjeux juridiques

L'implantation de l'IdO dans votre entreprise pourrait être une source de préoccupation de nature juridique. Vous devriez connaître les responsabilités légales de votre entreprise dans le monde réel comme dans l'univers virtuel.

- Adressez-vous à un conseiller juridique pour connaître vos obligations externes, notamment à l'égard d'une loi provinciale ou fédérale.
- Tenez compte des conséquences juridiques qui pourraient éventuellement découler de la défaillance ou du piratage d'un objet connecté.

Étape 3 : Élaborer une politique pour l'IdO

Pour protéger toutes les activités de votre entreprise, harmonisez votre politique relative à l'IdO à celles concernant la cybersécurité.

- La direction et le service des TI devraient faire en sorte que la responsabilité du déploiement de l'IdO soit partagée à la grandeur et à tous les niveaux de l'entreprise.
- Assurez-vous que les maillons de votre chaîne d'approvisionnement (partenaires, fournisseurs, etc.) prennent les mesures qui s'imposent pour sécuriser leurs propres systèmes.
- Examinez la façon dont l'IdO s'intégrera dans votre stratégie commerciale actuelle. Assurez-vous que l'IdO vous permettra d'atteindre vos objectifs à court et long termes.
- Investissez dans le développement d'une main-d'œuvre qualifiée en offrant de l'information et une formation sur l'IdO à vos employés. Téléchargez notre présentation #IdOAuTravail à l'intention des employés **PensezCybersecurite.ca**. Pour de plus amples renseignements sur les politiques, consultez la section Créez des politiques en matière de cybersécurité plus rigoureuses.

Étape 4 : Mettre en œuvre des mesures de sécurité

Voici une liste de conseils pour assurer la sécurité des objets connectés avant, pendant et après l'implantation de l'IdO.

Selon une étude réalisée en 2017 par Sécurité publique Canada, 57 % des propriétaires ou dirigeants de petites entreprises sont aussi responsables des TI[1]. Envisagez de faire appel à des professionnels ou à des organisations spécialisés en cybersécurité.

Avant l'implantation :

- ☐ Informez-vous sur les objets connectés avant d'en faire l'achat; lisez les avis et obtenez des recommandations; renseignez-vous sur leur capacité de sécurité.
- ☐ Établissez un point de contact avec les fabricants en cas de problème dans le futur.
- ☐ Lisez la documentation des objets : guides de l'utilisateur, instructions, forums de soutien.
- ☐ Élaborez des politiques « Apportez votre équipement personnel de communication » (AVEC) et IdO à l'intention des employés.
- ☐ Évaluez les risques en fonction des politiques et normes actuelles de l'entreprise en matière de TI.

[1] Sécurité publique, Recherche sur l'opinion publique EKOS

Durant l'implantation :

- ☐ Sécurisez votre réseau sans fil. Pour de plus amples renseignements sur le sujet, consultez Exploitez une entreprise plus cybersécuritaire.
- ☐ Changez les noms d'utilisateur et mots de passe par défaut des objets connectés et utilisez des mots de passe forts. Consultez les Pratiques exemplaires en matière d'authentification.
- ☐ Isolez les réseaux sur lesquels circule de l'information sensible; envisagez l'utilisation d'un réseau distinct pour les objets connectés.
- ☐ Vérifiez que le système de l'objet connecté peut être réinitialisé pour supprimer définitivement l'information sensible servant à la configuration.
- ☐ Contrôlez l'accès au réseau pour déterminer qui peut l'utiliser et à partir de quel endroit.
- ☐ Chiffrez les données, commandes et communications, aussi bien celles qui sont inactives que celles qui circulent.
- ☐ Si possible, activez la mise à jour automatique des systèmes d'exploitation, logiciels et micrologiciels; effectuez périodiquement des mises à jour manuelles, au besoin.

Après l'implantation :

- ☐ Mettez en œuvre des processus reproductibles pour vérifier toutes les mesures de protection et contre-mesures de sécurité durant l'implantation.
- ☐ Effectuez régulièrement des tests simulant des « cyberincidents » et des vérifications pour confirmer l'intégrité du réseau.
- ☐ Sauvegardez régulièrement les données au moyen de solutions d'entreposage sûres et redondantes, comme des serveurs multiples ou le nuage; testez périodiquement le processus de récupération des données. Pour de plus amples renseignements sur le sujet, consultez Sécurité des données — Options de sauvegarde et de restauration.

Étape 5 : Surveiller et mettre à jour l'IdO

Surveillez vos réseaux d'IdO et objets connectés.

- Nommez les responsables de l'IdO dans votre entreprise, puis déterminez la fréquence à laquelle l'activité des appareils devrait être surveillée.
- Si possible, mettez en place des outils de vérification automatisée pour surveiller, évaluer, détecter et corriger les problèmes liés à l'IdO. Si l'automatisation n'est pas possible, établissez des procédures pour une surveillance manuelle périodique.

- Déterminez la fréquence et l'ampleur du suivi assuré par la direction. Envisagez des mises à jour trimestrielles.

La mise à jour des logiciels et systèmes d'exploitation ainsi que l'installation de correctifs doivent être effectuées en permanence. Par conséquent, ces étapes devraient être répétées fréquemment et pour chaque nouvel objet connecté. Gardez les voies de communication ouvertes entre la direction et le service des TI. Enfin, assurez-vous que vos employés respectent votre politique sur l'IdO. L'augmentation des objets connectés sur le lieu de travail accroît d'autant le degré de vulnérabilité et de risque dans l'entreprise.

L'IdO et les programmeurs, fabricants et fournisseurs de services

La sécurité de l'IdO devrait être une priorité des programmeurs et fabricants d'objets connectés ainsi que pour les fournisseurs de services et les exploitants de réseaux. Durant la conception, la programmation et la mise en œuvre d'objets connectés, on devrait accorder un degré de priorité élevé aux mesures visant à assurer la sécurité et la confidentialité.

Parmi les pratiques exemplaires relatives à l'IdO, on recommande aux programmeurs et fournisseurs de services de fournir aux consommateurs toute l'information possible sur la sécurité dans un langage simple. On devrait pouvoir consulter l'information sur la sécurité et les déclarations de confidentialité à ces endroits :

- Manuel de l'utilisateur et instructions pour l'utilisation de l'appareil
- Site de l'entreprise
- Application contrôlant l'objet
- Forum de soutien
- Centre d'aide (accessible en ligne ou par téléphone)

Pour de plus amples renseignements et des conseils en matière de cybersécurité dans l'entreprise, consultez l'équipe de l'organisme américain Computer Emergency Readiness à l'adresse https://www.us-cert.gov/ncas/tips (site accessible en anglais seulement).

PENSEZCYBERSECURITE.CA