Comment mettre fin aux préoccupations concernant la sécurité de l'IdO

Un rapport de la série de documents d'information sur l'IdO, présenté par Bell | Mai 2017

IDC
Analyze the Future

Gérez le risque plutôt que de chercher à l'éviter

Cinquante-deux pour cent des moyennes et grandes organisations canadiennes ont déjà adopté des solutions de l'Internet des objets (IdO) afin de profiter d'avantages comme des coûts réduits et des expériences clients améliorées. Qu'est-ce qui empêche l'autre 48 % de leur emboîter le pas?

Les recherches d'IDC démontrent que la deuxième préoccupation en ce qui a trait aux déploiements de solutions IdO au Canada est la sécurité. Chaque semaine apporte son lot de nouvelles concernant des crises de cybersécurité. De plus en plus, l'IdO devient à la fois la cible et le mécanisme de distribution des pirates informatiques.

La menace provenant des dispositifs intelligents connectés est-elle une raison d'éviter l'IdO? Non.

IDC croit fermement que la réponse est que **les organisations doivent gérer le risque plutôt que de chercher à l'éviter.** Le potentiel de l'IdO pour améliorer l'efficacité et la productivité et créer de nouvelles sources de revenus et de nouveaux modèles opérationnels est trop important pour être éclipsé par des problèmes de sécurité qui peuvent être efficacement atténués. L'adoption et la mise en œuvre de pratiques exemplaires en matière de sécurité protégeront les initiatives IdO contre les menaces à la sécurité.

Vulnérabilités de l'IdO sur le plan de la sécurité

De quelle manière l'IdO change-t-il l'équation en matière de sécurité? Le tableau ci-dessous fait ressortir quelques-unes des principales vulnérabilités qui diffèrent des problèmes de sécurité des TI traditionnelles. Ce rapport met en évidence les pratiques exemplaires offrant des solutions à ces vulnérabilités de l'IdO.

Points d'extrémité et dispositifs

Les points d'extrémité et les dispositifs sont :

- Physiquement accessibles : Des attaques en personne sont possibles.
- Peu efficaces sur le plan informatique : Il est plus difficile de les rendre conformes aux exigences de chiffrement.
- Fondamentalement bavards : Ils sont conçus pour « communiquer » entre eux. Ce bavardage signifie que les dispositifs peuvent être attaqués par d'autres appareils intégrés à la « guirlande » des dispositifs IdO.

Réseau

Les solutions IdO sont fondées sur la connectivité. Contrairement aux anciennes solutions de communication de type machine-machine ou SCADA, les solutions IdO :

- Utilisent des réseaux publics ou privés qui sont reliés aux applications d'affaires de base.
- Peuvent fonctionner à l'extérieur des coupe-feu traditionnels.
- Peuvent transmettre des renseignements qui devraient être chiffrés lorsqu'ils sont acheminés sur le réseau.
- Peuvent compliquer la tâche des administrateurs de réseau lorsque ceux-ci essaient de repérer ou d'identifier des dispositifs ou comportements indésirables.

Données et applications

Les données sous-jacentes qui sont transmises par les points d'extrémité aux systèmes et bases de données internes sont l'élément primordial. Les vulnérabilités incluent :

- Les attaques par contournement d'authentification en vertu desquelles les pirates tentent de deviner les noms d'utilisateurs ou les mots de passe en utilisant des processus automatisés qui font appel à une approche essais-erreurs.
- Les bases de données et les versions et correctifs d'application périmés.
- L'absence d'une surveillance soutenue.
- L'omission de chiffrer les données.

Pratiques exemplaires en matière de sécurité des points d'extrémité et des dispositifs

La diminution des prix des capteurs et modules connectés est l'une des principales raisons pour lesquelles l'IdO a connu une forte ascension au cours des dernières années. Les entreprises canadiennes doivent s'efforcer de sécuriser les points d'extrémité et les dispositifs tout en saisissant les avantages que leur procure l'IdO.

- **Assurez-vous que les points d'extrémité IdO utilisent des règles qui permettent de contrôler la conformité de la configuration des mots de passe.** Le nombre impressionnant de dispositifs connectés qui sont expédiés partout dans le monde (30 milliards de dispositifs en 2020 à l'échelle mondiale) signifie que les paramètres des mots de passe par défaut des fabricants seront connus des pirates informatiques. Les plans de mise en œuvre doivent prévoir que les configurations seront régulièrement mises à jour et que les dispositifs seront authentifiés en utilisant des clés uniques générées dynamiquement. Il ne devrait jamais y avoir de mots de passe par défaut ou de dispositifs connectés non protégés. Utilisez du matériel infalsifiable comme les cartes SIM pour stocker des données d'identification, d'authentification et d'autorisation.

Lorsque vous retirez des périphériques du service, effacez toutes les données sensibles qu'ils contiennent. Théoriquement, vous devriez utiliser le logiciel de la plateforme IdO pour les désactiver à distance et obtenir ainsi une filière d'audit.

- **Faites appel à une tierce partie respectée, comme un exploitant de réseau mobile, pour procéder à la certification des dispositifs de bout en bout avant de les déployer, afin d'améliorer la sécurité.** Certains fournisseurs regroupent l'authentification et le chiffrement des dispositifs et des services réseau. Les dispositifs non enregistrés sont ignorés et la sécurité repose sur une utilisation limitée aux dispositifs authentifiés.
- **Mettez en place une surveillance et une gestion continues des dispositifs.** Les entreprises doivent surveiller de manière proactive les changements apportés à la configuration des dispositifs, les tentatives d'authentification et les communications d'arrivée afin de bloquer les actions qui constituent une menace et de mettre à jour les dispositifs. Les plateformes de gestion IdO permettent aux clients de surveiller les points d'extrémité. Certaines plateformes IdO envoient automatiquement des alertes si une carte SIM est transférée dans un dispositif indésirable, ce qui permet au client de désactiver la carte SIM.

Ne comptez pas sur la « sécurité par l'obscurité ». L'approche qui consiste à se cacher dans l'immensité de l'Internet ne fonctionne tout simplement pas. Il existe des moteurs de recherche comme Shodan.io qui permettent à n'importe qui de chercher des dispositifs connectés, depuis les interphones de surveillance jusqu'aux systèmes de contrôle industriels (SCI). Les dispositifs seront trouvés et exploités. L'obscurité ne constitue donc pas une approche envisageable.

- **Procédez régulièrement à la vérification des dispositifs connectés.** Les organisations doivent connaître le nombre de dispositifs qu'elles possèdent, la nature de ces dispositifs ainsi que leur emplacement et pouvoir déterminer à quand remonte leur dernière utilisation.
- **Évitez les dispositifs qui offrent des capacités non nécessaires à leurs services et fonctionnement de base.** L'utilisation de périphériques dotés de fonctions additionnelles superflues, qu'il s'agisse de caméras, de microphones ou d'autres options, introduit des vulnérabilités imprévues.
- **Planifiez la mise hors service des dispositifs.** Lorsque vous retirez des périphériques du service, effacez toutes les données sensibles qu'ils contiennent. Théoriquement, vous devriez utiliser le logiciel de la plateforme IdO pour les désactiver à distance et obtenir ainsi une filière d'audit.

Surveillez et contrôlez les communications locales entre les serveurs et les dispositifs de stockage.

Pratiques exemplaires en matière de sécurité du réseau

Le réseau jouera un rôle essentiel dans la détection des menaces, la réponse aux incidents, le contrôle de l'accès et l'application des politiques pour l'IdO utilisé en entreprise.

- **Conservez vos solutions IdO sur des réseaux distincts, indépendants du réseau fédérateur interne.** Il n'y a aucune raison pour que les appareils CVC de l'immeuble résident sur le même réseau que les systèmes de paiement ou les systèmes financiers de votre entreprise. Les dispositifs déployés sur des réseaux internes ou dans des nuages privés sont mieux protégés contre les attaques, mais ils requièrent tout de même une procédure d'authentification rigoureuse ainsi qu'un accès réservé aux ports de communication communs (TCP, FTP, etc.) pour les protéger contre des accès inappropriés par les employés. Segmentez vos réseaux pour tenir les processus clés séparés. Les réseaux sans fil publics (cellulaires) offrent une sécurité robuste et isolent votre solution IdO, limitant ainsi son exposition en cas d'atteinte à la sécurité.

Les dispositifs déployés sur des réseaux internes ou dans des nuages privés sont mieux protégés contre les attaques, mais ils requièrent tout de même une procédure d'authentification rigoureuse ainsi qu'un accès réservé.

- **Envisagez d'utiliser un nom de point d'accès (APN) privé et des cartes de circuits intégrés universels autorisées (UICC ou SIM).** Cela réduira l'empreinte de vulnérabilité, comparativement à une utilisation de l'Internet public.
- **Mettez en œuvre des solutions de surveillance sans fil** qui recherchent les points d'extrémité, déterminent si ce sont des points d'extrémité légitimes, fantômes ou hostiles, et les retracent jusqu'à un emplacement précis afin qu'ils puissent être désactivés ou récupérés. Cela ressemble beaucoup à la mise en œuvre de solutions de gestion de la mobilité dans les entreprises pour les déploiements de téléphones intelligents et de tablettes. Les logiciels de plateforme IdO comme Jasper peuvent lancer des alertes automatisées si le numéro d'identité internationale d'équipement mobile (IMEI) est changé, afin que les administrateurs de réseau puissent faire enquête et désactiver la carte UICC, au besoin. Les solutions de surveillance peuvent être déployées par les services des TI ou confiées à des tierces parties qui peuvent surveiller les dispositifs 24 heures sur 24, 7 jours sur 7.
- **Déployez des solutions de coupe-feu en périphérie** pour gérer les communications entre un système intelligent et ses composantes en amont sur l'Internet.
- **Utilisez un processus de chiffrement fort pour les données en transit.** En plus des protocoles SSL (Secure Socket Layer) et TLS (Transport Layer Security) utilisés avec une connexion pour serveur IP, les réseaux et appareils cellulaires ajoutent une couche de sécurité supplémentaire.
- **Tenez compte de la durée de la connexion.** Les points d'extrémité doivent-ils être connectés à l'Internet tous les jours de l'année, 24 heures sur 24? Cela expose le système à de plus grands risques permanents que les communications effectuées en lots ou basées sur les exceptions. Songez à utiliser des contrôles réseau pour limiter la durée de la connexion ou restreindre les possibilités de connexion à une période particulière de la journée.
- Limitez l'accès aux ports de communication communs. En fermant les ports auxquels les dispositifs peuvent se connecter (par ex., TCP, FTP, etc.), vous réduirez l'empreinte de vulnérabilité que les pirates informatiques peuvent cibler.

Pratiques exemplaires concernant les serveurs et les dispositifs de stockage

Les composants serveur et les composants de stockage peuvent être très différents, en fonction du cas d'utilisation de l'IdO. Ces composants peuvent également être hébergés localement, dans des centres de données, dans les installations d'un fournisseur de services ou dans le nuage d'un fournisseur de services.

- **Activez les fonctions d'identification et d'authentification pour les serveurs et les dispositifs de stockage.** De plus en plus, les appareils sont livrés avec des outils d'identification et d'authentification qu'il suffit d'activer et d'utiliser. La réhabilitation d'anciens équipements peut entraîner des problèmes à cet égard.
- **Déployez des solutions de contrôle des applications pour « renforcer » les serveurs et les solutions de stockage.** Ces solutions s'appliquent aux systèmes qui reçoivent les données provenant de l'Internet ou qui sont transmises par des capteurs et dispositifs utilisés localement.
- **Envisagez d'utiliser des solutions infonuagiques de plateforme comme service (PaaS) et d'infrastructure comme service (IaaS).** IDC prévoit que d'ici 2020, plus de 30 milliards de points d'extrémité connectés auront été installés. L'infonuagique permet aux organisations de gérer les charges de travail variables générées par ces dispositifs, mais surtout, elle fournit une architecture offrant l'évolutivité et la souplesse qui sont essentielles pour composer avec le déluge de données.
- **Adoptez des approches fondées sur une « sécurité de la prochaine génération »**. Les services des TI doivent délaisser l'utilisation d'une base de données des menaces statique, mais constamment mise à jour, au profit d'approches fondées sur le recours à des algorithmes ou à l'apprentissage machine.

Pratiques exemplaires en matière de sécurité des bases de données

Les solutions IdO génèrent d'importantes quantités de données. À titre d'exemple, le nouvel avion de ligne à réaction C Series de Bombardier utilise des moteurs Pratt & Whitney équipés de 5 000 capteurs générant jusqu'à 10 gigaoctets de données par seconde. Les organisations doivent se concentrer sur la sécurité de leurs bases, entrepôts et lacs de données.

- **Estimez la valeur qu'attribueraient à vos données** des pirates informatiques et utilisez ces renseignements pour déterminer vos priorités en matière d'investissement dans la sécurité. Les données essentielles ou les renseignements de nature hautement délicate comme les données financières, la recherche et le développement ou les données sur les clients doivent faire l'objet d'une protection supérieure.
- **Chiffrez les données inactives pour en protéger la confidentialité** et pour vous assurer que les renseignements ne peuvent être lus que par les parties appropriées. Cela signifie habituellement que vous devez tirer parti de solutions que votre organisation utilise déjà.

Les pirates informatiques ciblent souvent les serveurs et les dispositifs de stockage en raison de l'importante quantité de renseignements qu'ils contiennent.

- **Faites le nécessaire pour qu'il soit impossible de compromettre les justificatifs d'identité des administrateurs et autres identifiants utilisés par défaut.** Les attaques traditionnelles comme l'hameçonnage cibleront ces justificatifs d'identité dans le but de prendre le contrôle des bases de données et des applications.
- **Procédez à des essais dynamiques** avant la mise en œuvre des solutions afin d'exposer (et de corriger) les vulnérabilités exploitables, y compris les attaques par injection SQL, par injection de code indirecte (« cross-site scripting ») et par injection de requêtes illégitimes par rebond (« cross-site request forgery »).
- **Entreprenez une surveillance intensive de l'intégrité du système de fichiers, des processus système discrets et des comportements des employés.** Les technologies d'antilogiciel malveillant et de détection ciblée permettent d'ajouter des capacités d'analyse comportementale afin de découvrir les logiciels malveillants évolués qui sont conçus pour contourner les défenses basées sur la signature. Envisagez d'utiliser des solutions IdO infonuagiques offrant des fonctions de sécurité et de surveillance améliorées afin de permettre à vos ressources en TI internes de se concentrer sur leurs compétences de base.

Pratiques exemplaires en matière de sécurité des applications

Les applications d'entreprise sont à la fois des systèmes d'action et des systèmes d'enregistrement. En d'autres termes, elles peuvent être utilisées pour faire des choses et pour ensuite documenter ces actions. Par conséquent, il est essentiel d'en assurer la confidentialité, l'intégrité et la disponibilité.

- **Installez les mises à jour et les correctifs logiciels dès que possible.** Les menaces informatiques se répandent plus rapidement que les solutions à ces menaces, ce qui fait que les entreprises qui tardent à mettre en œuvre les mises à jour sont plus vulnérables. Envisagez d'adopter des solutions infonuagiques dont le fournisseur assure continuellement la surveillance et la mise à jour de ses applications afin de libérer vos ressources en TI de cette tâche.
- **Limitez l'accès des employés aux systèmes en fonction de leur rôle et des exigences de leur travail.** L'un des vecteurs d'attaque les plus simples consiste à utiliser les identifiants d'employés travaillant dans d'autres services afin d'accéder à des rôles plus essentiels et ainsi gravir les échelons des vulnérabilités de l'entreprise. Les entreprises doivent sécuriser leurs applications en fonction des différents rôles afin de prévenir ces attaques séquentielles.

- **Établissez un isolement logique basé sur les processus.** Les machines connectées modernes, qu'il s'agisse d'automobiles ou d'équipement de production, sont des systèmes complexes et interdépendants équipés de milliers de capteurs et dispositifs de commande. La conception logicielle doit isoler les différents processus de manière à ce qu'une faille dans les systèmes d'infodivertissement n'ouvre pas la porte à une attaque ciblant des éléments du système de transmission ou de direction.
- **Déterminez la maturité de vos principaux fournisseurs IdO sur le plan de la sécurité.** Si une évaluation globale et objective dépasse les capacités de vos équipes des TI et des services d'approvisionnement, faites appel à des experts-conseils qui possèdent l'expérience, les outils et la capacité nécessaires pour évaluer les vulnérabilités de vos solutions IdO sur le plan de la sécurité.

Autres pratiques exemplaires en matière de sécurité

1 Faites de la sécurité une responsabilité qui incombe à chacun

Les secteurs d'activité financent 60 % des projets IdO au Canada.

Toutefois, ces dirigeants d'entreprise veulent laisser la sécurité entièrement entre les mains de leur service des TI. Comme les stratégies d'affaires intègrent de plus en plus des solutions connectées, les dirigeants des secteurs d'activité doivent accélérer le pas et accepter leur responsabilité d'intégrer la sécurité dans la conception de leurs produits et processus, ce qui signifie qu'ils doivent prévoir les budgets nécessaires pour le personnel et les technologies qui leur permettront d'atteindre cet objectif. Les dirigeants d'entreprise sont les mieux placés pour comprendre leur contexte réglementaire, la valeur relative de leurs données et les risques opérationnels pour leur secteur d'activité qu'entraîne une atteinte à la sécurité. Qu'ils le veuillent ou non, la sécurité constitue désormais une part importante du travail des chefs d'entreprise canadiens.

2 Changez votre approche en matière de sécurité

La sécurité évolue constamment. Au cours des 10 ou 15 dernières années, l'industrie a évolué, passant de la « sécurité du périmètre » pour prévenir des attaques à une approche axée sur la détection rapide « des ennemis parmi nos rangs » et sur la reprise des activités lorsque survient une atteinte à la sécurité. Cette transition est primordiale pour les organisations qui mettent en œuvre des initiatives IdO, mais la bonne nouvelle est que cela va dans le sens de la recherche globale d'une plus grande résilience dans le secteur des technologies et en particulier dans l'univers de la cybersécurité.

3 Déployez de multiples solutions

Il n'y a pas de solution miracle pour sécuriser les systèmes IdO, ce qui signifie que les risques associés à l'IdO ne peuvent être atténués au moyen d'un seul produit de sécurité. IDC recommande de déployer de multiples couches de solutions de sécurité pour gérer de manière proactive le risque associé à l'IdO. Évaluez la nécessité, pour votre organisation, de déployer les solutions suivantes :

- Chiffrement des communications pour protéger les communications entre les systèmes intelligents et les systèmes de gestion. Ces communications sont souvent plus sensibles, car elles peuvent inclure des données agrégées, des rapports de gestion de nature délicate ou des données de canal de commande.
- Coupe-feu en périphérie pour gérer les communications entre un système intelligent et ses éléments en amont sur l'Internet.
- Passerelle de sécurité IdO pour fournir aux systèmes locaux des capacités de sécurité combinées comme les filtres, la détection et le chiffrement.

Détection d'intrusion IdO pour surveiller les communications locales entre les différents éléments des systèmes et pour découvrir les dispositifs ou capteurs inappropriés. Ces solutions tiennent à jour des tables d'état pour surveiller les dispositifs et reconnaître les communications anormales. Elles peuvent exiger l'utilisation de dispositifs personnalisés qui décodent les protocoles et analysent le trafic réseau en conséquence.

4 Envisagez de recourir à des services de sécurité gérés

Les entreprises canadiennes se tournent de plus en plus souvent vers des tierces parties compétentes pour gérer leurs besoins en matière de sécurité. De nombreuses organisations ne possèdent pas l'expérience, le temps ou l'argent nécessaires pour faire face au contexte des menaces qui est en constante évolution. On dénote un nombre croissant de vulnérabilités du jour zéro (failles qui sont inconnues des fournisseurs de logiciels) dans les systèmes de contrôle industriels (SCI) qui sont publiées sur le Web. Le maintien en poste d'un personnel de cybersécurité qualifié est un problème de plus en plus courant au sein des entreprises canadiennes.

Les fournisseurs de services de sécurité gérés peuvent vous apporter leur aide ou prendre complètement en charge la sécurité des systèmes et des réseaux. Ces fournisseurs comptent sur un plus grand nombre d'outils et de ressources très bien formées qui leur permettent de détecter les attaques et de mettre en place une défense plus rapidement que la plupart des organisations. Le recours à des services de sécurité gérés pour vous aider avec vos déploiements de solutions IdO peut améliorer la sécurité tout en libérant vos ressources en TI qui pourront se consacrer à des initiatives à caractère plus stratégique.

Il existe des lignes directrices largement reconnues pour la configuration des contrôles et processus de sécurité de vos solutions IdO comme la norme ISO/ IEC 27001:2013, la norme ISO 27018, le programme américain FedRAMP (Federal Risk and Authorization Management Program) et l'infrastructure de cybersécurité de la NIST. **Les organisations devraient procéder à une analyse comparative de leurs propres efforts ou choisir des fournisseurs certifiés afin d'intégrer la sécurité dès le départ.**

Gérez vos préoccupations concernant la sécurité de l'IdO au moyen d'une réponse proactive

L'IdO introduit de nouvelles vulnérabilités, mais les organisations peuvent gérer cette situation en :

1. Découvrant les vulnérabilités (physiques et virtuelles) des points d'extrémité, réseaux, bases de données et applications.
2. Mettant en œuvre et tenant à jour des technologies, politiques et procédures qui réduisent les vulnérabilités découvertes.
3. Surveillant de manière proactive toutes les couches de leur infrastructure afin de détecter les menaces et les atteintes à la sécurité.

Les entreprises canadiennes n'abandonnent pas le courriel, les serveurs Web ou les technologies de médias sociaux simplement en raison de la menace qu'ils représentent pour la sécurité. L'Internet des objets doit être examiné sous le même jour. Les avantages et la valeur qui s'y rattachent sont trop importants pour être éclipsés par des préoccupations concernant la cybersécurité qui peuvent être atténuées en faisant appel aux technologies, processus et partenaires appropriés.

Pour plus d'information sur les pratiques exemplaires en matière de sécurité de l'IdO, communiquez dès maintenant avec un conseiller au service à la clientèle d'affaires de Bell ou visitez le site www.bell.ca/IdO.