Sécurité de l'Internet des objets (IdO)

Juillet 2022 ITSAP.00.012

Qu'est-ce que l'IdO?

L'Internet des objets (IdO) désigne le réseau formé par les dispositifs Web utilisés couramment qui peuvent se connecter les uns aux autres et se transmettre de l'information. Ces objets « intelligents » comprennent non seulement les ordinateurs, les téléphones intelligents et les tablettes, mais aussi les moniteurs d'activité personnels, les téléviseurs, les thermostats et les voitures. Les dispositifs de l'IdO ne cessent de se multiplier. Selon IoT Analytics[1], il y aura plus de 30 milliards de dispositifs connectés à l'IdO d'ici 2025, ce qui représente une moyenne de quatre appareils par personne. Voilà pourquoi il est de plus en plus important de comprendre comment utiliser en toute sécurité les appareils IdO au sein de votre organisation.

Comment fonctionne l'IdO?

Les appareils IdO nécessitent peu d'intervention de votre part une fois la configuration initiale terminée. Ils sont munis de capteurs intégrés, de composants électriques et de logiciels qui recueillent des données et de l'information dans l'environnement où ils se trouvent. Les données sont transmises par Internet vers le nuage, où elles sont traitées et partagées avec d'autres appareils connectés au réseau par les technologies Bluetooth ou d'identification par radiofréquence (RFID pour *Radio-Frequency Identification*).

Comment les appareils IdO modifient-ils le flux de travail?

Les dispositifs IdO facilitent et simplifient les tâches et processus courants, ce qui permet aux employés de s'occuper d'autres priorités. Par exemple, il existe des dispositifs de paiement mobile qu'on peut connecter à un téléphone intelligent, une façon simple d'accepter des paiements n'importe où.

Les dispositifs IdO permettent aux organisations de faire des économies.
Par exemple, les systèmes automatisés de chauffage et de climatisation réduisent la consommation d'énergie et les coûts des services publics.

Quels types de dispositifs IdO sont utilisés par les organisations?

À première vue, il n'est pas toujours facile de reconnaître les dispositifs IdO en milieu de travail. En voici quelques exemples :

- Équipement de téléconférence
- Tableaux intelligents
- Haut-parleurs et autres dispositifs à commande vocale
- Capteurs d'équipement intelligent
- Compteurs intelligents (compteurs électriques, compteurs d'eau, etc.)
- Détecteurs de mouvement et moniteurs d'air
- Caméras de sécurité en réseau
- Parcs de véhicules organisationnels
- Appareils multifonction (imprimantes, télécopieurs)
- Appareils électroménagers intelligents (bouilloires, réfrigérateurs, etc.)
- Systèmes de terminaux de point de vente
- Systèmes de contrôle d'immeubles (chauffage, ventilation, climatisation, électricité, eau)
- Téléphones cellulaires et équipement TI portable d'une organisation
- Montres intelligentes et moniteurs d'activité

Note : Autoriser les employés à utiliser leurs appareils intelligents personnels au travail peut accroître les risques pour la sécurité.

Consultez le document suivant pour en savoir plus sur les appareils mobiles au travail : *Sécurité des appareils des utilisateurs finaux pour les modèles de déploiement Prenez*

SÉRIE SENSIBILISATION

No de cat. D97-1/00-012-2022F-PDF
ISBN 978-0-660-43939-6

Quels sont les risques?

Les contrôles de sécurité et les capacités de chiffrement des appareils IdO actuels sont faibles et inadéquats, ce qui les rend vulnérables à d'éventuelles menaces. Les auteurs de menace peuvent exploiter ces vulnérabilités notamment pour :

- compromettre les systèmes de régulation des conditions ambiantes et les électroménagers intelligents (comme les cafetières, les systèmes électriques, le chauffage) dans les lieux de travail, ce qui pourrait entraîner des pertes de profits (p. ex. le sabotage des régulateurs de température dans la salle des serveurs pour causer la défaillance d'équipement);
- obtenir un accès non autorisé aux contrôles de sécurité d'un immeuble (p. ex. pour déverrouiller des portes ou capter les images des caméras de surveillance);
- prendre le contrôle d'un appareil multifonction pour interrompre l'accès à Internet (p. ex. lors d'une attaque par le réseau de zombies Mirai);
- accéder à distance aux microphones d'appareils IdO pour écouter des conversations sensibles;
- prendre le contrôle des fonctions d'un véhicule (p. ex. saboter les freins);
- contrôler l'équipement médical d'un hôpital (p. ex. nuire aux appareils d'imagerie par résonance magnétique [IRM]);
- accéder à des données sensibles ou à des renseignements personnels (comme les noms et numéros de cartes de crédit de clients) en passant par des appareils IdO non sécurisés et connectés aux réseaux d'entreprises.

Quel impact a l'IdO sur les infrastructures essentielles?

L'IdO est souvent utilisé dans le cadre d'opérations industrielles (p. ex. fabrication, énergie, transport, domaine médical) qui contribuent aux infrastructures essentielles (IE). L'IdO rend possibles des communications de machine à machine qui améliorent les processus opérationnels en optimisant la productivité, la sécurité, la durabilité et les coûts.

Or, malgré les processus opérationnels améliorés, les opérations industrielles et les IE peuvent être plus à risque lors de l'utilisation de l'IdO. Connecter de nombreux appareils à des systèmes qui gèrent des fonctions hautement sensibles peut entraîner des risques de vulnérabilités externes touchant les processus et l'approvisionnement. De plus nombreuses connexions à des appareils, des réseaux TI et à Internet représentent de plus nombreux angles d'attaque pour les cybercriminels.

Pour en savoir plus, consultez le document : Considérations en matière de sécurité pour les infrastructures essentielles (ITSAP.10.100), sur notre site Web.

Comment assurer la sécurité des appareils IdO?

Avant d'adopter des dispositifs IdO dans votre organisation, il importe de faire de la recherche sur les protocoles de sécurité et de comprendre les types de données transmises et reçues par ces dispositifs. Comme les appareils IdO se retrouveront de plus en plus en milieu de travail, votre organisation devra mettre en œuvre des plans et des politiques visant à réduire le risque que des incidents de cybersécurité touchent votre réseau. Ces plans et politiques devraient tenir compte des points ci-dessous :

- Restreindre la connexion des appareils IdO personnels à un réseau distinct (p. ex. un réseau Wi-Fi invité)
- Modifier les mots de passe par défaut des appareils IdO. Si les règles de mot de passe le permettent, choisir une phrase de passe plutôt qu'un mot de passe pour tous les appareils IdO en milieu de travail.
- Utiliser l'authentification à deux facteurs pour ajouter une couche de sécurité supplémentaire aux dispositifs ou aux applications.
- Veiller à ce que les données générées par les appareils IdO soient chiffrées.
- Désactiver toutes les fonctionnalités de connexion automatique (p. ex. l'autoconfiguration *plug and play*).
- Mettre à jour les logiciels et appliquer les correctifs de sécurité aux appareils IdO (si le produit le permet).
- Surveiller, détecter et corriger tout problème de sécurité lié aux appareils IdO (votre fournisseur peut vous aider avec ce processus).
- Isoler les réseaux IdO pour limiter l'accès aux systèmes dans lesquels sont gérées des données sensibles.
- Faire de la recherche pour trouver les évaluations des clients et les évaluations de sécurité concernant les divers fabricants et produits.

Que faut-il retenir?

Les appareils IdO peuvent aider votre organisation à améliorer l'efficacité des flux de travail et des processus, mais ils comportent des risques sur le plan de la cybersécurité. Leur utilisation en milieu de travail peut soulever des préoccupations liées à la protection de la vie privée des employés si des technologies intelligentes sont utilisées pour surveiller leurs activités professionnelles et leurs déplacements.

Il conviendra de mettre en œuvre des politiques au sein de votre organisation afin de veiller à ce que les appareils IdO soient adoptés, utilisés et gérés en toute sécurité. De plus, votre organisation devrait avoir des politiques pour un stockage de données approprié sur tous les appareils.

Référence:

[1] IOT ANALYTICS. *State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time*, novembre 2020.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.