ÉVITER LES ÉCUEILS DU MONDE BRANCHÉ : NOUVELLES PRATIQUES EXEMPLAIRES D'ATTÉNUATION DES RISQUES

Publié le 2 septembre, 2022

Catégories: Perspectives, Publications

Le 25 août 2022, le Centre canadien pour la cybersécurité (**CCC**) a mis à jour ses conseils sur l'utilisation des appareils de l'Internet des objets (**IDO**), en vue d'aider les organisations à en atténuer les risques[1].

Qu'est-ce que l'Internet des objets?

L'IDO désigne le réseau formé par les dispositifs Web couramment utilisés qui peuvent se connecter les uns aux autres et se transmettre de l'information : pensons à nos ordinateurs et cellulaires, mais aussi aux moniteurs d'activité personnels, aux téléviseurs, aux thermostats, aux voitures connectées et aux appareils de surveillance de domicile. Ces objets « intelligents » transmettent des données par Internet vers un nuage, où elles sont traitées puis partagées avec d'autres appareils connectés par l'entremise des technologies Bluetooth, Wi-Fi ou d'identification par radiofréquence (RFID).

Pourquoi ces conseils sont-ils importants?

D'ici 2025, le CCC prévoit qu'il y aura plus de 30 milliards de dispositifs connectés à l'IDO, soit quatre appareils par personne en moyenne, d'où l'urgence de prendre les moyens d'assurer la sécurité et la protection de la vie privée des utilisateurs.

On utilise souvent les appareils de l'IDO pour simplifier les tâches courantes, et ainsi améliorer le flux de travail et la productivité. La connexion d'un dispositif de paiement à un téléphone intelligent, pour en faire un outil de paiement simple et convivial, en est un exemple. Les appareils de l'IDO que l'on retrouve en milieu de travail comprennent l'équipement de téléconférence, les dispositifs à commande vocale, les caméras de sécurité en réseau, les téléphones cellulaires de l'organisation et bien plus encore.

Quels sont les enjeux de cette technologie en matière de vie privée et de sécurité?

Pour les organisations, l'IDO représente une occasion sans précédent de favoriser la réussite des employés dans un environnement de travail plus créatif, efficient et innovant, mais il pose aussi d'énormes risques pour la sécurité. En outre, le fait d'autoriser l'utilisation d'appareils intelligents personnels au travail peut accroître ces risques.

Sans examen et contrôles adéquats, les appareils de l'IDO exposent le réseau et les données de l'organisation à d'éventuelles menaces. Les auteurs de menace peuvent exploiter ces vulnérabilités et ainsi compromettre les systèmes internes, en accédant sans autorisation au microphone d'un objet connecté et écouter une conversation, par exemple, ou perturber sciemment l'accès à Internet.

Dans un contexte plus large, la sécurité des appareils de l'IDO concerne aussi des infrastructures essentielles (ex. : activités minières, énergie, transport, domaine médical), et donc le public et l'économie en général.

Comment les organisations peuvent-elles se protéger?

Les organisations doivent examiner soigneusement les implications du déploiement de ces technologies à l'échelle de leurs activités. Pour assurer la sécurité des appareils de l'IDO, le CCC invite les organisations à adopter ou à mettre à jour des plans et des politiques de sécurité qui tiennent compte des capacités et des éventuelles vulnérabilités de leur réseau. Plus particulièrement, le CCC conseille ce qui suit :

- utiliser l'authentification à deux facteurs pour ajouter une couche de sécurité supplémentaire aux dispositifs et applications;
- désactiver les fonctionnalités de connexion automatique;
- choisir une phrase de passe plutôt qu'un mot de passe pour tous les appareils de l'IDO en milieu de travail;
- veiller à ce que les données générées par les appareils de l'IDO soient chiffrées.

Enfin, le CCC souligne le potentiel des appareils de l'IDO pour améliorer les flux de travail et les processus, mais rappelle aux organisations qu'elles héritent des problèmes de sécurité de chaque appareil connecté à leur réseau. L'organisation qui intègre ces technologies à ses activités devrait instaurer des politiques veillant à ce qu'elles soient adoptées, utilisées et gérées de façon sécuritaire. Elle devrait aussi avoir des politiques encadrant le stockage de données sur tous les appareils.

Si vous avez des questions sur ces conseils, le maintien de politiques de vie privée et de cybersécurité conformes, ou la vie privée et la cybersécurité en général, un membre du groupe Protection de la vie privée et des données se fera un plaisir de vous aider.

[1][ps2id id='1' target='/] Centre canadien pour la cybersécurité, *Internet des objets : pratiques exemplaires d'atténuation des risques du CCC* (25 août 2022), disponible ici.

Par Robert Piasentin, Kristen Shaw et Hailey Lonsdale (stagiaire en droit)

Mise en garde

Le contenu du présent document ne fournit qu'un aperçu du sujet et ne saurait en aucun cas être interprété

comme des conseils juridiques. Le lecteur ne doit pas se fonder uniquement sur ce document pour prendre une décision, mais devrait plutôt obtenir des conseils juridiques précis.