La cybersécurité et les dangers liés à l’Internet des objets

31 octobre 2022

Auteurs

Eric Lavallée

Associé, Agent de marques de commerce Associé, et Avocat

Selena Lu

Associée, Avocate

Alors que le gouvernement canadien manifeste son intention de légiférer en matière de cybersécurité (voir le projet de loi C-26 visant à mettre en place une *Loi sur la protection des cybersystèmes essentiels*), plusieurs entreprises ont déjà entrepris des démarches sérieuses pour sécuriser leurs infrastructures informatiques. Toutefois, l’Internet des objets et trop souvent négligé lors de ces démarches.

Pourtant, plusieurs appareils sont directement connectés aux infrastructures informatiques les plus importantes pour les entreprises. Les robots industriels, les dispositifs qui contrôlent l’équipement de production en usine ou ceux qui aident les employés sur la route à effectuer leurs livraisons en sont des exemples. Des systèmes d’exploitation ainsi que diverses applications sont installés sur ces appareils. Le fonctionnement même de nombreuses entreprises et la sécurité de certains renseignements personnels dépendent de la sécurité de ces appareils et de leurs logiciels. Par exemple :

> Une attaque pourrait viser les systèmes de contrôle d’équipement de fabrication en usine et entraîner une

interruption de la production de l'entreprise ainsi que des coûts importants de remise en fonction et des délais de production;
En visant les équipements de production et les robots industriels, un attaquant pourrait subtiliser les plans et les paramètres de fabrication de différents procédés, ce qui pourrait mettre en péril les secrets industriels d'une entreprise;
Des lecteurs de codes à barres utilisés pour la livraison de colis pourraient être infectés et transmettre des renseignements, notamment des renseignements personnels, à des pirates informatiques

L'*Open Web Application Security Project* (OWASP), un organisme sans but lucratif, a publié une liste des dix plus grands risques de sécurité pour l'Internet des objets[1]. Les gestionnaires d'entreprises qui utilisent de tels équipements doivent être conscients de ces enjeux et prendre des mesures pour mitiger ces risques. Nous nous permettons de commenter certains de ces risques dont la mitigation requiert des politiques adaptées et une saine gouvernance au sein de l'entreprise :

Mots de passe faibles ou immuables : certains dispositifs sont vendus avec des mots de passe initiaux connus ou faibles. Il est important de s'assurer que, dès leur installation, ces mots de passe sont changés, puis d'en garder un contrôle serré. Seul le personnel informatique désigné devrait connaître les mots de passe permettant de configurer ces appareils. De plus, il faut éviter d'acquérir des équipements ne permettant pas une gestion de mots de passe (par exemple, dont le mot de passe est immuable).
Absence de mises à jour : l'Internet des objets repose souvent sur des ordinateurs dont les systèmes d'exploitation ne sont pas mis à jour pendant leur durée de vie. Il en résulte que certains appareils sont vulnérables parce qu'ils utilisent des systèmes d'exploitation et des logiciels ayant des vulnérabilités connues. À cet égard, une saine gouvernance permet d'une part de s'assurer que de tels appareils sont mis à jour, et d'autre part, de n'acquérir que des appareils permettant de procéder aisément à de telles mises à jour régulières.
Gestion déficiente du parc d'appareils connectés : Certaines entreprises n'ont pas un portrait clair de l'Internet des objets déployés au sein de leur entreprise. Il est impératif d'avoir un inventaire de ces appareils, de leur rôle au sein de l'entreprise, du type de renseignements qui s'y trouvent et des paramètres essentiels à leur sécurité.
Manque de sécurité physique : Dans la mesure du possible, l'accès à ces appareils devrait être sécurisé. Trop souvent, des appareils sont laissés sans surveillance dans des lieux où ils sont accessibles au public. Des directives claires doivent être données aux employés pour que ceux-ci adoptent des pratiques sécuritaires, notamment en ce qui concerne l'équipement destiné à être déployé sur la route.

Le **conseil d'administration** d'une entreprise joue un rôle clé en matière de cybersécurité. En effet, le défaut des administrateurs de s'assurer qu'un système de contrôle adéquat est mis en place et d'assurer une surveillance des risques peut engager leur responsabilité. Dans ce contexte, voici quelques éléments que les entreprises devraient considérer pour assurer une saine gouvernance :

Revoir la composition du conseil d'administration et réviser la matrice des compétences afin de s'assurer que l'équipe possède les compétences requises;
Offrir de la formation à tous les membres du conseil d'administration afin de développer la cybervigilance et leur donner des outils pour remplir leur devoir d'administrateur; et
Évaluer les risques associés à la cybersécurité, notamment ceux découlant des appareils connectés, et établir les moyens de mitiger ces risques.

La Loi 25, soit la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, prévoit plusieurs obligations destinées au conseil d'administration, notamment celle de nommer un responsable de la protection des renseignements personnels et celle d'avoir un plan de gestion et un registre des incidents de confidentialité. À cet effet, nous vous invitons à consulter le bulletin suivant : Modifications aux lois sur la protection des renseignements personnels : ce que les entreprises doivent savoir (lavery.ca)

Finalement, une entreprise doit en tout temps s'assurer que les identifiants, mots de passe et autorisations auprès des fournisseurs permettant au personnel informatique d'intervenir ne sont pas entre les mains d'une seule personne ou d'un seul fournisseur. Ceci placerait l'entreprise en position de vulnérabilité si la relation avec cette personne ou ce fournisseur venait à se dégrader.

---

1. Voir notamment OWASP top 10