Communautés connectées

Janvier 2023

ITSAP.00.222

Nos vies dépendent de plus en plus des technologies de l'information et des communications (TIC) qui nous permettent d'interagir avec le monde numérique. Au sein d'une communauté connectée, des technologies recueillent et analysent des données sur l'environnement, établissant un lien entre le monde réel qui nous entoure et les systèmes numériques, de sorte à améliorer l'efficacité des infrastructures publiques et des services municipaux. Ces espaces sont communément appelés villes intelligentes, mais on les nomme aussi villes ou lieux connectés qui utilisent des systèmes intelligents.

De grandes quantités de données sont recueillies grâce à différents dispositifs, comme des caméras et des capteurs, qui sont connectés aux réseaux Internet des objets (IdO) et Internet industriel des objets (IIdO). Malgré leur potentiel d'optimisation du monde qui nous entoure, il faut savoir que les communautés connectées présentent de sérieux défis sur le plan de la sécurité en raison des surfaces d'attaque accrues dont peuvent se prévaloir les auteurs de menace pour exploiter les dispositifs et causer des préjudices dans le monde réel. Les données qui sont recueillies par les systèmes connectés et qui y sont stockées sont hautement sensibles et doivent donc être protégées.

À quoi ressemble une communauté connectée?

Les infrastructures traditionnelles regroupent des composantes matérielles et logicielles qui sont indépendantes l'une de l'autre. Les communautés connectées se composent d'infrastructures physiques intégrées et d'infrastructures numériques, par exemple de réseaux, d'algorithmes, de dispositifs IdO et sans fil, d'applications et de capteurs connectés. L'intégration de ces infrastructures permet de créer des systèmes cyberphysiques, qui sont une forme avancée de technologies opérationnelles (TO), pouvant transformer la qualité de vie des citoyennes et citoyens. Les TO désignent le matériel et les logiciels servant à surveiller et à transformer les processus qui ont une incidence sur le monde physique. Exemples d'infrastructures et de services publics dans une communauté connectée :

Transports : Les caméras et autres capteurs pour feux de circulation ou lampadaires, ainsi que les capteurs dans les véhicules, les appareils cellulaires et les GPS peuvent recueillir de l'information en temps réel concernant les conditions de circulation. Grâce à ces données, les appareils peuvent alors suggérer des itinéraires différents, la congestion routière peut être atténuée et les véhicules d'urgence peuvent être avantagés.

Énergie : Grâce à des compteurs intelligents, des communautés peuvent évaluer leur utilisation énergétique et diminuer leurs émissions de carbone. C'est grâce aux infrastructures de mesure avancées que des données concernant les services publics sont recueillies, par exemple les compteurs d'électricité, de gaz, de chauffage et d'eau qui permettent d'assurer l'efficacité des services offerts. L'éclairage intelligent qui s'active uniquement au besoin afin de réduire la surconsommation en est aussi un exemple.

Déchets et pollution : Des capteurs installés sur des poubelles permettent de détecter celles qui sont pleines et d'en aviser les services de gestion des déchets pour qu'ils les vident sans que tout leur parcours soit perturbé. Les technologies IdO font aussi partie intégrante du recyclage des déchets : production d'énergie, surveillance de la qualité de l'air pour mesurer les niveaux de pollution et amélioration des systèmes de gestion des eaux usées.

Gouvernance : Bon nombre de pays sont en consultation avec l'industrie et des organes gouvernementaux pour établir des lois et des cadres réglementaires mettant de l'avant des normes à respecter. Ces normes visent à accroître la sécurité cybernétique, à normaliser l'étiquetage des produits et à promouvoir le renforcement des audits et de la conformité. L'établissement de ces normes s'avère important lorsqu'il est question de la sécurité des citoyennes et citoyens ainsi que des effets sur les cybersystèmes essentiels.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-222-2023F-PDF
ISBN 978-0-660-46912-6

Défis et risques pour les communautés connectées

La nature des infrastructures essentielles interconnectées et des réseaux centralisés de même que les quantités importantes de données recueillies par l'intermédiaire des communautés connectées présentent des risques de sécurité et des défis importants pour votre organisation. Une attaque ciblant les infrastructures d'une communauté connectée pourrait en effet causer l'interruption de fonctions essentielles et permettre à des auteurs de menace d'exploiter des données organisationnelles et personnelles. Notons entre autres les exemples suivants :

- Au fil du temps, des **fuites de données** ont mené à l'accumulation d'une énorme quantité d'informations que peuvent exploiter des auteurs de menace. En ayant en main des données organisationnelles ou des données sur un gouvernement, la localisation ou la consommation énergétique, les auteurs de menace détiennent des détails de nature sensible sur la vie quotidienne d'une personne, des renseignements personnels ou des documents de planification des activités.
- Les **cyberattaques** sont monnaie courante au sein des communautés connectées, car ces communautés ne se limitent pas à un seul système. Une surface d'attaque accrue permet d'ailleurs aux auteurs de menace de cibler un aspect d'une infrastructure essentielle, ce qui **peut avoir des effets** sur d'autres systèmes.
- L'intégration d'infrastructures désuètes ou non prises en charge peut présenter des défis pour des organisations et doit donc être gérée avec précaution si ces infrastructures ne doivent pas être connectées aux autres. Les ententes des fournisseurs de service peuventaussi indiquer qu'ils n'assurent pas la maintenance régulière des systèmes **patrimoniaux** .
- L'élaboration des **lois** et des **cadres juridiques** régissant la façon de recueillir des données afin d'assurer la protection des citoyennes et citoyens peut aussi représenter un défi. Il peut également être difficile pour les gens d'empêcher la collecte de leurs données personnelles.

Les systèmes cyberphysiques présentent de nouveaux types de risques qui diffèrent de ceux des systèmes de TIC ou de TO. Les stratégies d'atténuation à adopter pour les communautés connectées dépendront en fait des types de technologies concernées, de leur utilisation et des risques particuliers qui en découlent.

Bien qu'il puisse s'avérer impossible d'appliquer toutes les mesures d'atténuation raisonnables pour tous les types d'infrastructures, voici certaines mesures auxquelles pourrait s'intéresser votre organisation .

- Des stratégies de sécurité usuelles pourraient protéger vos systèmes et vos réseaux, mais nécessitent l'examen attentif de vos fournisseurs et de spécialistes en la matière. Notons entre autres l'établissement de zones dans un réseau, la surveillance, les contrôles d'accès, les pare-feu, l'authentification multifacteur et le chiffrement de bout en bout.
- Les évaluations de la protection de la vie privée et des risques liés à la sécurité sont essentielles et doivent être menées avant le déploiement de toute application ou plateforme connectée. Ces évaluations permettent notamment de déterminer les risques, de préparer et de mettre à l'essai les interventions, et d'exiger la correction régulière des composantes logicielles.
- Grâce à l'élaboration de politiques et de procédures pour protéger les données et à une éducation axée sur la sensibilisation et la transparence offerte dans le cadre de consultations publiques, les citoyennes et citoyens ont de plus en plus confiance en la communauté connectée dans laquelle ils ou elles vivent. Par exemple, la transparence concernant la collecte, le stockage et l'utilisation des données permet aux citoyennes et citoyens de donner leur consentement éclairé. De plus, l'application de mesures de protection de la vie privée garantit que seule l'information nécessaire est recueillie.

Les publications suivantes contiennent des détails et des conseils sur les différents systèmes brièvement mentionnés dans la présente publication :

- Protéger vos technologies opérationnelles (ITSAP.00.051)
- Élaborer un plan en cas d'incident (ITSAP.40.003)
- Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)
- La sécurité du Wi-Fi (ITSAP.80.002)
- Exigences de base en matière de sécurité pour les zones de sécurité de réseau (Version 2.0) (ITSP.80.022)
- Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004)
- Les outils de sécurité préventive (ITSAP.00.058)

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**.