SIEMENS

L'ingéniosité au service de la vie

Document d'information sur la cybersécurité

Cybersécurité pour la protection des infrastructures critiques

siemens.ca/cybersecurity

La numérisation et la mondialisation transforment les paradigmes et entraînent de nouvelles possibilités. Des milliards d'appareils sont reliés par l'Internet des objets et interagissent à un tout nouveau niveau. Ces technologies changent notre façon de vivre, de communiquer et de travailler. Elles permettent de mettre en place de nouvelles applications et de nouveaux modèles d'entreprise dans l'ensemble des secteurs et marchés verticaux industriels. L'intelligence artificielle, l'analyse des mégadonnées, les chaînes de blocs et les technologies infonuagiques améliorent notre monde d'innombrables façons.

Mais ces nouvelles connexions sont associées à de nouvelles vulnérabilités. Elles augmentent également notre risque d'exposition à des cyberattaques malveillantes. Le monde a constaté à quel point de telles attaques peuvent influer sur des élections démocratiques. De plus en plus, les infrastructures critiques comme les banques, le gouvernement, l'industrie et les services de santé sont également des cibles. Près de 600 milliards $ (US), soit pratiquement 1 % du PIB mondial, sont perdus chaque année en raison de la cybercriminalité[1].

Les pirates informatiques ne s'attaquent pas seulement aux PC classiques. Depuis que le programme malveillant Stuxnet a fait la manchette partout dans le monde en 2010, les entreprises de fabrication ont compris que la présence croissante de la numérisation estompe la frontière entre les bureaux et les infrastructures qui contrôlent les installations industrielles. En conséquence, les exploitants d'usines ont dû se préparer à affronter tous les défis connus du secteur des technologies de l'information (TI) – comme la cyberattaque mondiale WannaCry l'a confirmé en mai 2017. De plus en plus de produits, de solutions et de services reposant sur des logiciels utilisés dans des infrastructures critiques, l'éventail des risques relatifs à la cybersécurité continuera de prendre de l'ampleur. Ainsi, plus de huit milliards d'appareils, y compris des machines, des installations, des capteurs et des produits, communiquent désormais entre eux, ce qui représente une augmentation d'environ 30 % depuis 2016. Ce nombre continuera à augmenter considérablement – plus de 20 milliards d'ici 2020[2].

La cybersécurité relative aux TI comme nous la connaissons a progressé, mais il reste encore beaucoup à faire par rapport à la cybersécurité des infrastructures critiques, appelée cybersécurité des technologies d'exploitation.

Le message est clair. Ne pas protéger les systèmes qui relient et contrôlent nos maisons, nos hôpitaux, nos usines, nos réseaux électriques et nos infrastructures pourrait entraîner des conséquences dévastatrices. Le monde numérique a besoin d'un niveau de sécurité de base correspondant aux mesures de sécurité généralement acceptées que nous tenons pour acquises dans le monde non numérique. Pour favoriser la confiance à l'égard de la cybersécurité, une vaste alliance d'entreprises et de gouvernements agissant de concert est requise. Personne ne peut y arriver seul. Des décisions doivent être prises maintenant.

En tant que membre fondateur de la Charte de confiance, Siemens porte l'enjeu de la cybersécurité à un niveau supérieur. De concert avec plusieurs autres grandes entreprises comme Daimler et IBM, l'entreprise a lancé une puissante initiative mondiale : Les produits futurs de toutes les entreprises partenaires seront conçus et mis en service conformément à des principes de cybersécurité ambitieux.

Siemens emploie des experts en cyberprotection pour examiner les installations industrielles dans le monde entier afin de détecter des menaces potentielles provenant d'Internet, avertit les entreprises des incidents relatifs à la sécurité et coordonne des contre-mesures proactives. L'entreprise emploie actuellement environ 1 300 experts en cybersécurité. Siemens dispose ainsi de solides bases pour se protéger, de même que ses clients, à l'aide de produits et de systèmes sécurisés. De plus, les systèmes de cybersécurité comptent parmi les « technologies d'entreprise fondamentales » de Siemens – c'est-à-dire les domaines technologiques et d'innovation qui sont de la plus haute importance stratégique.

Par conséquent, l'entreprise possède une expertise approfondie dans le domaine de la cybersécurité et des défis croissants qui y sont associés. Cela s'applique en particulier au système d'exploitation pour l'Internet des objets (IdO) MindSphere de Siemens. Plus de 1,4 million d'appareils de divers clients sont maintenant connectés à ce système. Tous ces appareils doivent être protégés, d'autant plus que leur nombre ne cesse d'augmenter. En plus de se concentrer sur les clients industriels, Siemens fournit également des services de cybersécurité aux fournisseurs, aux exploitants de réseaux électriques et au secteur de la santé.

Au Canada, en mai 2018, Siemens a créé un centre mondial de cybersécurité à Fredericton, au Nouveau-Brunswick, en collaboration avec Opportunités Nouveau-Brunswick. Le centre est opérationnel et se concentre sur la recherche et le développement, les services-conseils et les services gérés. Le centre de cybersécurité de Siemens vise à réunir l'expertise de Siemens dans la protection des infrastructures critiques et l'écosystème de cybersécurité émergent du Nouveau-Brunswick, créant ainsi un potentiel pour des exportations mondiales de méthodes, de technologies et de protocoles Internet créés à l'échelle locale. L'entreprise devrait créer jusqu'à 30 emplois hautement qualifiés dans la province d'ici 2020, et 30 autres au cours de la phase 2, tout en soutenant la formation, l'éducation et la recherche et développement. Les nouveaux postes devraient être dans les domaines de l'ingénierie, de la recherche et des services-conseils.

En 2019, Siemens a poursuivi son engagement en matière de cybersécurité en se joignant à l'Institut canadien sur la cybersécurité de l'Université du Nouveau-Brunswick.

[1] 2018 Economic Impact of Cybercrime report by The Center for Strategic and International Studies (CSIS) https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

[2] Communiqué de presse de Gartner, 2017. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

siemens.ca/cybersecurity

Siemens Canada limitée
1577 North Service Road East
Oakville (Ontario) L6H 0H6