IoT : miser sur la sécurisation des systèmes industriels en 2020

En 2019, l'IoT s'accroit au-delà du grand-public

A l'instar du grand public, les industriels exploitent de plus en plus l'Internet des Objets pour optimiser l'automatisation et accroître leur productivité. Les constructeurs automobiles, les compagnies ferroviaires, voire l'industrie agroalimentaire, exploitent des réseaux de capteurs et de senseurs ainsi qu'une multitude d'autres appareils connectés permettant de collecter des données de production et d'alimenter le cloud, afin d'affiner l'analyse de l'efficacité de leurs systèmes.

Ce que les industriels nomment Internet des objets Industriels ou IIoT ne cesse de s'intégrer dans les écosystèmes grâce aux progrès en matière d'automatisation, de l'analyse des données (big data) et de la baisse du coût du matériel.

Selon une récente étude de marché réalisée par IoT Analytics, le total des investissements consacrés aux plateformes IIoT dans le secteur industriel devrait progresser de 1,67 milliard de dollars en 2018 à 12,44 milliards de dollars en 2024, 43 % des industriels destinant ces investissements à l'optimisation générale des processus et 41 % à la visualisation.

Des sociétés telles qu'Emerson, spécialiste des solutions d'automatisation, aident déjà d'autres entreprises à déployer des solutions IIoT pour améliorer leur efficacité.
Récemment, elle a mis en place une passerelle IIoT d'edge computing chez un industriel. Cette passerelle analyse les données des capteurs pour évaluer la vitesse d'usure des amortisseurs des vérins pneumatiques. Plutôt que de les remplacer à la périodicité fixée, les capteurs émettent une alerte lorsqu'une certaine valeur est atteinte. Puis, les amortisseurs sont remplacés.
Des sociétés comme Rolls Royce sont aussi connues pour recourir à cette technologie afin d'analyser des milliers de milliards de points de données fournies par des capteurs en vue d'optimiser la mise au point de leurs moteurs.

L'IIoT apporte de la visibilité aux managers en leur permettant de savoir si les machines fonctionnent, si leurs performances sont bonnes et s'il y a des problèmes. En cas de survenue d'un incident, les données fournies par cette technologie permettent aussi de retracer le lieu de fabrication des pièces et de déterminer si l'incident est lié à la machine, à la pièce ou si son origine est tout autre.

Les systèmes IIoT étant tributaires de ces capteurs pour la collecte et l'analyse d'importantes volumétries de données, il est crucial de mettre en place des contrôles pour sauvegarder ces données et garantir leur intégrité.

Il est facile de négliger qu'il est important d'accorder la priorité adéquate à la protection de ces données. Après tout, il y a peu de chance que ces systèmes gèrent des données sensibles sujettes aux règles de conformité réglementaires comme des informations de santé confidentielles ou des données à caractère personnel.

Il faut néanmoins stocker, gérer et partager en toute sécurité les données générées par les

systèmes IIoT (étalonnages, mesures et autres paramètres) pour en exploiter pleinement les capacités. L'impossibilité d'agir en ce sens risque de s'avérer dramatique et de se solder par des interruptions de service, la perte de propriété intellectuelle et des fuites de données.

En l'absence de mesures de protection des données adaptées, ces systèmes pourraient se retrouver à la merci d'un risque d'attaque industrielle plus grand, comme Triton/Trisis, et entraîner aussi des dommages corporels.

Les avantages de l'Industrial Internet Consortium (IIC)

Ces types de systèmes continuant de proliférer et d'interagir avec les systèmes d'entreprise et les processus métier, il est important de disposer d'une sorte de référence pour les sécuriser. C'est ici qu'intervient l'Industrial Internet Consortium (IIC). Cet organisme à but non lucratif, comptant GE, Microsoft et Dell EMC parmi ses membres fondateurs, a publié cet été un guide sur les bonnes pratiques en matière de protection des données issues des systèmes IIoT.

Comme le souligne l'IIC, la cryptographie, le chiffrement, l'audit, la surveillance et la protection des données (au repos, en mouvement et en cours d'utilisation) sont quelques-unes des seules méthodes de garantie de leur intégrité. Toujours selon ce consortium, se familiariser avec les meilleures pratiques telles que la sécurité, la confidentialité et la résidence des données tout en veillant à leur mapping avec les données IIoT peut aussi améliorer la fiabilité du système.

Bien qu'il ne soit pas l'apanage des environnements industriels, le modèle de maturité de la sécurité des systèmes IoT, également publié par l'IIC et corédigé avec Microsoft, peut aussi être utile pour évaluer la maturité de la sécurité des systèmes IoT.
Ce guide distille des conseils sur la mise en place de pratiques de gouvernance, de contrôles de sécurité et de pratiques de durcissement, telles que l'application de correctifs logiciels, la réalisation d'audits de sécurité et l'intervention adaptée en cas d'incidents, pour les configurations IIoT.

Parmi les autres cadres de développement de systèmes IIoT interopérables figurent l'Industrial Internet Reference Architecture (IIRA) et l'Industrial Internet Security Framework (IISF). Le Centre d'excellence national en cybersécurité américain (National Cybersecurity Center of Excellence - NCCoE), partie intégrante du National Institute of Standards and Technology (NIST), a également publié des conseils dans son rapport Securing the Industrial Internet of Things sorti en août.

Si tous ces cadres fournissent de précieux conseils en matière de sécurisation des systèmes industriels, les entreprises doivent considérer l'IIoT comme ce qu'il est : une chaîne d'approvisionnement complexe. Elles se feraient du tort en ne mettant pas en place un moyen de surveiller les données et de garantir leur intégrité, des usines aux moteurs, aux cylindres et aux capteurs, au sein d'un environnement.