Cybersécurité et Edge Computing : les 3 questions à se poser

L'Edge Computing est en train de gagner les entreprises industrielles. Sa capacité à traiter et à analyser les données au plus proche des machines et des processus de production, à la périphérie du réseau, est l'un de ses principaux atouts. En réduisant le temps de latence entre la collecte et la restitution des données, il aide les entreprises à optimiser leurs lignes de production et à gagner en efficacité et agilité.

L'impact d'une faille de sécurité dans l'équipement Edge peut se répercuter sur les installations de production et les chaînes d'approvisionnement, faisant baisser la productivité et les revenus. Elaborer une stratégie de sécurité appliquée à l'Edge Computing commence par se poser les bonnes questions :

Les applications logicielles hébergées dans un équipement Edge sont-elles sécurisées ?

A la base de tous les services Edge, le logiciel présente un fort enjeu de sécurité. Les systèmes de sécurité peuvent être considérés comme presque complètement obsolètes s'ils fonctionnent avec des logiciels dépassés. Pour éviter cette erreur, les entreprises devraient concevoir des bonnes pratiques prenant en compte dans leur calendrier de maintenance, la criticité des mises à jours et l'impact sur la production. Ce qui implique nécessairement la collaboration entre les opérateurs du site et les experts en sécurité informatique.

En cas de brèche, comment se protéger contre les attaques physiques et numériques ?

Dans le paysage actuel des menaces en constante évolution, les cyberattaques traditionnelles semblent inoffensives par rapport aux attaques massives de logiciels malveillants. Les entreprises qui déploient des systèmes Edge doivent tenir compte à la fois des menaces numériques et physiques lorsqu'elles élaborent une stratégie de sécurité. Dans la plupart des cas, la protection numérique est couverte par le déploiement d'un logiciel de sécurité – mais la protection physique peut être plus complexe.

Si un pirate accède au système physique, des mesures telles que le contrôle d'identité et la gestion des accès doivent être mises en place pour ajouter un niveau de sécurité supplémentaire et protéger les points de connectivité réels des dispositifs physiques. Cette protection peut également

protéger les entreprises contre les menaces internes, comme l'erreur humaine, qui menacent la chaîne logistique.

Comment mettre en œuvre de nouvelles solutions pour accroître la protection ?

Deux phases s'imposent : évaluer la situation puis établir une base existante comprenant les mesures de sécurité que l'entreprise applique déjà ainsi que les technologies susceptibles de renforcer la protection. Contrairement aux idées reçues, les systèmes Edge peuvent fonctionner avec les logiciels de sécurité OT pour les rendre plus efficaces et efficients. En plaçant les solutions de protection à proximité des points de données critiques, les systèmes Edge réduisent le temps nécessaire aux programmes de sécurité pour enregistrer et traiter les risques.

Cette capacité est particulièrement bénéfique pour les entreprises qui utilisent des dispositifs d'IdO (IoT) à grande échelle, car l'équipe informatique peut ne pas disposer des ressources nécessaires pour identifier immédiatement le point faible de sécurité au moment d'une brèche de sécurité.

Les aspects physiques et numériques de l'Edge exigent des stratégies de sécurité supplémentaires et complètes pour protéger les données et les assets d'une entreprise contre l'intrusion des pirates informatique