Liberte Politique
/

Conjuguer souveraineté et expertise : un impératif en matière de sécurité pour les acteurs industriels

Article rédigé par *Economie Matin*, le *09 janvier 2023*

Source [Economie Matin] : Véritable sujet d'importance stratégique, la cybersécurité se positionne comme une priorité pour l'ensemble des organisations. En effet, de nos jours, aucune entreprise ou structure publique ne peut prétendre être à l'abri d'une attaque.

En ce sens, les entreprises doivent faire évoluer leur gouvernance et s'appuyer sur de nouveaux dispositifs pour élever leur niveau de protection. Dès lors, choisir les bons partenaires pour mener à bien de tels projets est un sujet central. Il faut donc être particulièrement vigilant sur le type de technologie à utiliser. En effet, tous les SI ne se ressemblent pas et la menace peut provenir de différentes directions en fonction de l'organisation des entreprises. C'est notamment le cas des acteurs industriels.

La montée en puissance de l'informatique dans les organisations industrielles

Longtemps relativement préservés des cyberattaques au regard de leurs spécificités (réseaux OT), les industriels sont aujourd'hui plus fortement exposés aux cybermenaces en raison de leur connexion croissante aux systèmes IT. C'est dans ce contexte que l'IT a entrainé de nouvelles vulnérabilités qui peuvent impacter le fonctionnement des industriels. Attention donc à déployer des systèmes spécifiques qui permettent d'échanger des informations entre des systèmes de confiance disjoints en conservant leur étanchéité physique vis-à-vis de cyberattaques ciblées et complexes.

Tirer parti de la fiabilité des systèmes électroniques

À l'inverse des dispositifs purement informatiques, les systèmes électroniques sont plus robustes et offrent un niveau de fiabilité inégalé. Globalement, utiliser l'électronique permet de mettre en œuvre une défense en profondeur synonyme de fiabilité et de confiance. Ce faisant, systèmes IT et OT sont en mesure d'échanger en toute sécurité et ce, que la communication se fasse depuis les réseaux ou des supports amovibles tels que les périphériques USB. Il peut aussi être utile de compléter ces dispositifs en ajoutant une couche supplémentaire type firewall métier qui prendra en considération les spécificités sectorielles des industriels. Cet ensemble d'actions complémentaires permettra d'éviter toute contamination au niveau des couches de transport de données et de garantir l'intégrité des paquets de données en contrôlant leur contenu pour éviter les attaques sur les flux métier.

Retrouver l'intégralité de l'article en cliquant ici

09/01/2023 01:00