La crise a renforcé les enjeux de cybersécurité en augmentant le nombre d'attaques.

Les compétences en cybersécurité industrielle sont rares, malgré les formations existantes qui sont de bon niveau. Il faut pouvoir se prémunir des risques de contrôle à distance par des tiers malveillants, c'est très compliqué.

La cybersécurité des systèmes industriels et des solutions clients est une activité critique.

La cybersécurité en lien avec la transition numérique et la connectivité et en termes de souveraineté française et européenne est critique. Le risque porte sur l'intrusion dans les systèmes de pilotage énergétique. Il faut pouvoir visualiser les différents points de connexion sur le réseau électrique, donc il y a besoin de développer des logiciels. C'est problématique pour les systèmes industriels également. C'est une activité particulièrement critique pour les ETI et les PME. Un client s'est par exemple fait voler tous les plans électriques de son site industriel.

La crise a mis en exergue certains défis, en lien avec les clients : le partage de données, les quantité de stockage des serveurs, la cybersécurité... Certains n'ont pas pris la juste mesure des enjeux de cybersécurité : même les petites entreprises sont concernées par le rançonning. Même si les montants exigés ne sont pas exorbitants, c'est bloquant.

La cybersécurité est un des 21 domaines stratégiques se rapportant à des compétences nouvelles, disruptives et donc à staffer fortement.

Le second axe prioritaire de notre politique est celui de la transition digitale, ce qui inclut la cybersécurité, les échanges de données et les bases de données nécessaires aux véhicules.

Référence(s) :

- Activités critiques
  Date de publication : 05/2021