Avec les sources d'entrées dues aux machines connectées et à des systèmes intégrant des objets connectés (IIoT), les entreprises sont plus vulnérables. Les organisations les plus performantes peuvent se doter d'un service dédié ou de consultants externes – les règles d'intrusion physiques ne doivent pas être négligées.

Pour préserver / développer la souveraineté (du pays) et un bon niveau d'activité et d'emploi sur le territoire grâce à une performance accrue, 3 points sont aussi à développer pour l'axe cybersécurité :

- Partage de données clients :
  - Enjeux :
    - Notamment quand on développe des produits complexes (mêlant par exemple électronique et mécaniques) il convient de gagner en temps précision et d'accroitre l'interopérabilité entre les systèmes et entreprises.
    - Les interfaces et outils sont loin d'être standardisés
    - Les notions d'éthique et d'anonymisation des données doivent être posées.
  - *Pistes possibles :*
    - *Mise en place de standards : les éditeurs proposent plusieurs solutions comme le format IDF (intermediate data format).*
    - *Tracer les modifications : garantir que les modifications soient prises en compte avec d'autres solutions avec des protocoles de dialogue comme ECAD-MCAD Collaborator, ou Mentor Graphics et PTC…*
    - *Liens directs avec la CAO (là encore des outils distincts)*
    - *Simulation / visualisation : qui rajoute également la difficulté des puissances de calculs avec des machines plus puissantes*

- Cybersécurité interne :
  - Enjeu : Le blocage partiel ou total de la production ou d'une autre activité de l'entreprise pour des raisons d'insuffisance de structure de protection est un point discriminant pour des donneurs d'ordre ou sous-traitants qui seront de plus en en plus amenés à
    - Partager des données ou des outils collaboratifs en temps réel (jumeaux ; partages de données…)
    - Sécuriser leur supply chain (et donc mesurer la vulnérabilité globale de leur écosystème)
  - *Pistes possibles :*
    - *Mettre en place les diagnostics (plusieurs dispositifs existants) - Souscrire une assurance cybersécurité pour couvrir les coûts potentiels associés à une violation de la sécurité.*
    - *Prévenir : Cartographier les installations / Segmenter le réseau / Renforcer les authentifications / Renforcer les équipements (cf. nombre d'équipements connectés). Utiliser des services sécurisés (SFTP, HTTPS, OPC UA…)/Réaliser les mises à jour*
    - *Détecter et agir : avec des outils dédiés comme des sondes de détection OT (équipement, virtuel ou physique, connecté au système d'information afin de le cartographier et de le surveiller) des processus et une organisation SOC (Security Operation Center) pour la protection des données et la prévention du piratage.*
    - *Pour les TPE et PME à minima appliquer les consignes suivantes :*
      https://www.entreprises.gouv.fr/files/files/secteurs-d-activite/numerique/anssi-guide-tpe_pme-cybersecurite.pdf

      https://www.bpifrance.fr/sites/default/files/2021-12/Guide%20de%20cyber.pdf

- Compétences :
  - Enjeux :
    - Le sujet doit être suivi par la direction générale en tant qu'enjeu de résilience. Elle peut avoir la capacité à intégrer des profils plus portés sur ces sujets (data) et orientés résolution de problèmes, pensée analytique, communication, établissement de relations et curiosité en plus des connaissances « de base » en systèmes informatiques.
    - L'externalisation reste une voie courante.
  - *Piste possible : Dédier / former des collaborateurs à interagir avec les prestataires.*

Référence(s) :

- Étude prospective de l'impact de l'évolution des industries mécaniques sur l'emploi et les besoins de compétences
  Date de publication : 05/2024