AXE 4

RÉSILIENCE ET CONFIANCE NUMÉRIQUE

Objectif : *Protéger votre patrimoine numérique pour faire de la sécurité le fondement de votre résilience et de votre crédibilité commerciale.*

L'ENJEU

Ne laissez pas la sécurité être le maillon faible de votre chaîne de valeur — faites-en la base de votre approche commerciale.

Dans un contexte marqué par la convergence des technologies de l'information avec les technologies opérationnelles (TI/TO) et la montée des cyberattaques, la résilience numérique n'est plus optionnelle : elle est devenue un avantage concurrentiel.

3 RÔLES DU DIRIGEANT OU DE LA DIRIGEANTE

Instaurer une culture « confiance zéro »

Mettre fin au modèle du « chèque en blanc » : exiger l'authentification pour chaque accès, chaque humain, chaque équipement.

Négocier la convergence technologique

Veiller à ce que la sécurité informatique ne compromette jamais la disponibilité et la sécurité physique de l'usine.

Garantir la souveraineté et la réversibilité

S'assurer contractuellement que l'entreprise reste propriétaire de ses données et qu'elle pourra changer de fournisseur.

PAR OÙ COMMENCER — LISTE DE VÉRIFICATION

1 ADOPTER LE PARADIGME « CONFIANCE ZÉRO »

- **Recenser tous les accès actifs au réseau** — *Ex. : humains, équipements, fournisseurs distants.*
- **Activer l'authentification à deux facteurs (2FA)** — *En priorité, vous devez commencer par le progiciel de gestion intégré (ERP), la messagerie et l'accès production.*
- **Chiffrer tous les flux de données** — *Des bureaux aux capteurs, vous devez protéger ces flux.*

2 SÉCURISER LA PRODUCTION (TI/TO)

- **Segmenter le réseau de l'usine en zones étanches** — *Une infection sur un robot ne doit pas paralyser l'usine.*
- **Lister les équipements opérationnels exposés sur Internet** — *Ex. : automates, SCADA et robots, qui sont souvent non corrigés.*
- **Adapter les protocoles pour éliminer toute latence critique** — *La sécurité ne doit jamais entraver la production.*

3 CONCEVOIR DANS UNE OPTIQUE DE SÉCURITÉ

- **Inclure la cybersécurité dès le début de chaque projet** — *Il faut éviter de l'ajouter en fin de développement.*
- **Viser la conformité à la norme ISO 27001 ou à une norme équivalente** — *C'est un levier important pour les grands donneurs d'ordre.*
- **Former les équipes aux bonnes pratiques de base** — *80 % des incidents viennent d'une erreur humaine.*

4 PROTÉGER LA PROPRIÉTÉ INTELLECTUELLE FUTURE

- **Inventorier vos données critiques** — *Ex. : brevets, secrets de fabrication, formules, savoir-faire.*
- **Évaluer le risque « récolter maintenant, décrypter plus tard »** — *Des données volées aujourd'hui seront déchiffrables dans 5 à 10 ans.*
- **Planifier la migration vers la cryptographie post-quantique** — *Vous devez prioriser les actifs ayant une longue durée de vie.*

5 PRÉPARER L'ÈRE DES TECHNOLOGIES SANS INTERFACE VISUELLE

- **Tester des interactions par gestes ou présence** — *L'opérateur collabore sans toucher d'écran.*
- **Évaluer les capteurs biométriques au plancher** — *Ces derniers permettent une identification fluide et sécurisée en temps réel.*
- **Définir les règles de gouvernance des données biométriques** — *On rappelle ici l'importance de la Loi 25 en matière de consentement, de rétention et d'accès.*

6 IDENTIFIER LES OBSTACLES ET ANGLES MORTS

- ⚠ **Ne pas confondre conformité et sécurité réelle** — *Une certification ISO n'arrête pas l'hameçonnage.*
- ⚠ **Auditer les accès distants des fournisseurs d'équipements** — *Ces accès sont souvent non sécurisés et imposés contractuellement.*
- ⚠ **Vérifier les clauses de propriété des données dans les contrats avec vos fournisseurs** — *Beaucoup de PME ont cédé leurs données sans le savoir.*
- ⚠ **Évaluer la dépendance aux plateformes propriétaires** — *Ce verrouillage signifie une perte de souveraineté et empêche la réversibilité.*
- ⚠ **Auditer les droits d'accès AVANT de déployer Copilot ou tout autre agent IA** — *Copilot explore tout ce à quoi un ou une employée a accès, y compris les données salariales, les contrats et les secrets industriels consultés sans intention malveillante.*

ACTION PRIORITAIRE : Cette semaine, dressez la liste de tous les accès distants actifs sur votre réseau (fournisseurs, sous-traitants, équipements) — leur nombre risque de vous surprendre. Ces accès forment la première surface d'attaque de votre entreprise.

Avec la participation financière de Québec

ADRIQ
PROMOUVOIR • MOBILISER • ACCOMPAGNER