

## **FFMI : Montée du risque cyber et sécurité numérique**

*(Note d'information FIM)*

La cybersécurité est devenue un enjeu stratégique majeur pour les entreprises industrielles françaises, confrontées à une montée exponentielle des risques cyber. Entre espionnage industriel, attaques par ransomware et menaces sur les chaînes d'approvisionnement, les cyberattaques évoluent en complexité et en impact. Dans un contexte de digitalisation accélérée, de tensions géopolitiques et de dépendance aux infrastructures numériques, protéger les systèmes d'information, les données sensibles et la continuité des activités est désormais vital pour préserver compétitivité et souveraineté.

La cybersécurité englobe l'ensemble des pratiques, technologies et processus visant à protéger les systèmes d'information, les réseaux, les données et les équipements contre les menaces numériques. Ces menaces incluent des attaques malveillantes (ransomware, phishing, DDoS...), des intrusions, des vols de données ou encore des sabotages industriels. Pour les entreprises industrielles, la cybersécurité ne se limite pas aux seuls systèmes informatiques : elle s'étend également aux systèmes industriels (OT), qui pilotent les processus de production, et aux objets connectés (IoT), omniprésents dans les environnements industriels modernes.

Les dirigeants sont également de plus en plus ciblé

Dans un contexte de digitalisation accrue et de dépendance croissante aux outils numériques, la cybersécurité est cruciale pour garantir la continuité des activités, protéger les données stratégiques et assurer la conformité avec des réglementations de plus en plus strictes (RGPD, NIS2). Une attaque réussie peut entraîner des conséquences catastrophiques : paralysie des opérations, pertes financières importantes, atteinte à la réputation, mais aussi compromission des secrets industriels, voire mise en danger des utilisateurs finaux. Pour les entreprises industrielles françaises, exposées à des cybermenaces ciblées du fait de leur rôle stratégique dans des secteurs critiques (énergie, transport, défense), la cybersécurité est devenue une composante clé de leur résilience et de leur compétitivité.

Le développement de la cybersécurité est porté par plusieurs tendances structurelles qui renforcent la menace et en font une priorité stratégique. La première tendance est liée à l'intensification des tensions géopolitiques, où les cyberattaques deviennent des outils de déstabilisation entre États. Les groupes soutenus par des nations (APT – Advanced Persistent Threats) ciblent des infrastructures critiques, comme l'énergie ou les transports, afin d'affaiblir des adversaires économiques ou militaires.

Par ailleurs, la digitalisation massive des entreprises, accélérée par l'industrie 4.0, augmente considérablement la surface d'attaque. L'interconnexion croissante des systèmes IT (technologies de l'information), OT (technologies opérationnelles) et IoT (objets connectés industriels) complexifie la sécurisation des infrastructures et multiplie les points d'entrée pour les cybercriminels. Cette numérisation va de pair avec l'émergence de nouvelles technologies comme l'intelligence artificielle, qui bien qu'offrant des opportunités pour renforcer la sécurité, peut également être utilisée à des fins malveillantes. A ce sujet, on observe une montée des attaques ciblant directement les dirigeants d'entreprises avec une augmentation des « fraudes aux présidents », de campagne de phishing et d'usurpation d'identité sophistiquées par IA.

La montée en puissance de l'économie numérique exacerbe également les risques cyber. Les données deviennent une ressource stratégique, mais aussi une cible privilégiée, qu'il s'agisse de données clients, de propriété intellectuelle ou de secrets industriels. Enfin, le renforcement des régulations en Europe et dans le monde, comme la directive NIS2 ou le RGPD, impose aux entreprises d'adopter des stratégies de cybersécurité robustes, sous peine de sanctions financières et de dommages réputationnels en cas de défaillance.

### **Impacts potentiels**

- Transformation des chaînes d'approvisionnement : vérification de la résilience cyber des partenaires et fournisseurs pour éviter les intrusions par des tiers.
- Conformité réglementaire accrue : adaptation aux exigences de la directive NIS2, RGPD et autres normes spécifiques à l'industrie.
- Renforcement des politiques de sécurité et investissements en cybersécurité : déploiement de solutions de détection, prévention et réponse aux cyberattaques (plan de continuité d'activité, plan de reprise d'activité...)
- Formation et recrutement de talents spécialisés : développement des compétences en cybersécurité industrielle, à la croisée des IT et des OT.
- Prolongation des cycles d'innovation : intégration de mesures de cybersécurité dès la phase de conception des produits (security by design).
- Risque financier et réputationnel accru : une cyberattaque réussie peut entraîner des pertes financières directes, des interruptions d'activité et une atteinte à l'image de l'entreprise.

### **Hypothèses et scénarios**

- Et si demain, les cyberattaques ciblaient en priorité les PME sous-traitantes, devenant le maillon faible des grandes chaînes d'approvisionnement ?
- Et si la cyber résilience des entreprises devenait un critère de sélection des partenaires et des sous-traitants par les donneurs d'ordres ?
- Et si l'IA devenait un outil central pour les cybercriminels, rendant les attaques plus rapides, sophistiquées et difficiles à détecter ?
- Et si la régulation européenne imposait à chaque entreprise une certification de cybersécurité pour opérer sur certains marchés ?

### **Signaux sur le sujet**

- Les attaques ciblant le secteur industriel atteignent un nouveau record au deuxième trimestre 2023

[\(lien\)](#)

- les TPE et PME sont la première cible des cyberattaques

[\(lien\)](#)

- De nouvelles menaces cybers émergent avec la montée de l'IA générative

[\(lien\)](#)

- « Pire que les catastrophes naturelles, les attaques numériques pourraient devenir « non assurables » en raison de leur caractère systémique et de leur coût élevé » Mario Greco, PDG de Zurich Insurance, l'une des plus grandes compagnies d'assurance en Europe



[\(lien\)](#)

- Directive NIS2 entrée en vigueur en 2024 : Renforce les obligations des entreprises en matière de cybersécurité, notamment pour les secteurs critiques.

[\(lien\)](#)

#### **Sources et liens pour aller plus loin**

- [Rapport annuel sur la cybercriminalité 2024 - ANSSI](#)
- [Guide cybersécurité à des destination des dirigeants de TPE, PME et ETI - BPI France](#)