



Directive NIS2 : comment défendre l'industrie belge face aux cybermenaces ?

04 avril 2025, 11:09

Thierry Coutelier

A l'heure où l'industrie accélère sa transformation digitale, les cyberattaques se multiplient, mettant à rude épreuve la résilience des entreprises manufacturières. Avec l'entrée en vigueur récente de la directive européenne NIS2 en Belgique, les entreprises doivent désormais renforcer leur cybersécurité sous peine de sanctions. Entre obligations réglementaires, vulnérabilités fréquentes et bonnes pratiques à adopter, voici comment anticiper et protéger efficacement votre entreprise.

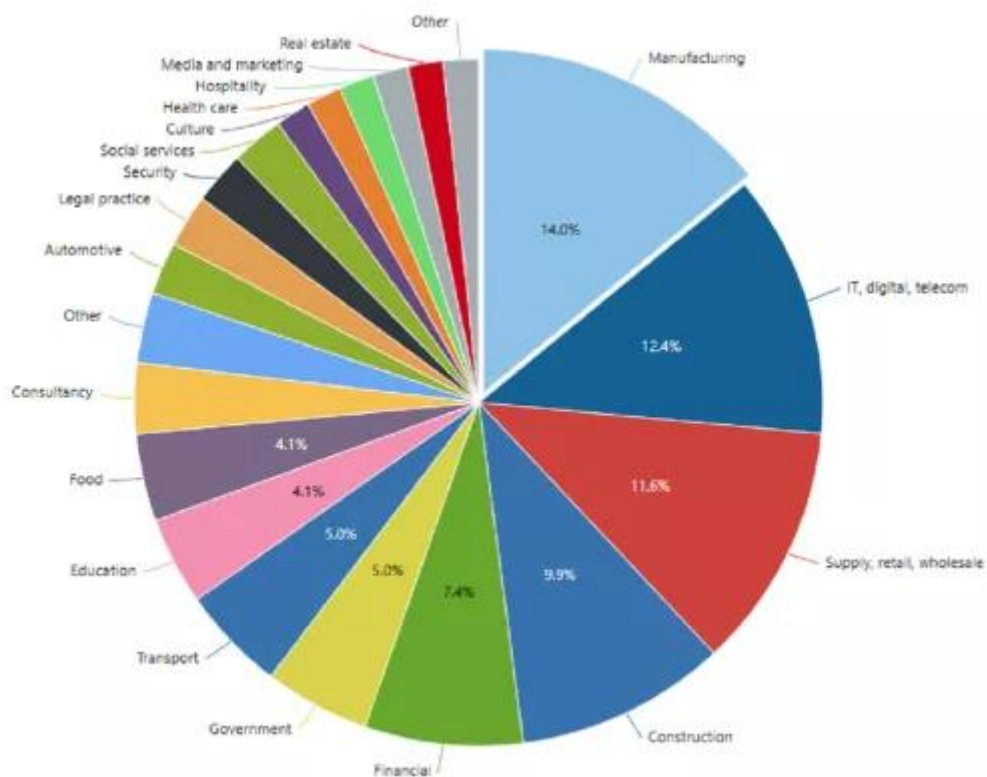
La transformation digitale offre aux industriels de nouvelles opportunités : innovation, optimisation des processus, réduction des coûts et nouvelles sources de revenus. Mais ce virage numérique s'accompagne également d'une augmentation inquiétante des cyberattaques. Aujourd'hui, aucune organisation industrielle n'est épargnée, qu'il s'agisse de grandes multinationales ou de PME locales. Rançongiciels paralysant les chaînes de production, vols massifs de données sensibles, attaques ciblées sur les fournisseurs stratégiques : les incidents se multiplient et gagnent en sophistication.

Depuis le 18 octobre 2024, l'entrée en vigueur en Belgique de la directive européenne NIS2 (Network and Information Security) impose aux entreprises manufacturières des règles strictes afin de prévenir ces risques et renforcer leur cyber-résilience.

Alerte sur les entreprises manufacturières belges

Plusieurs études récentes alertent sur la recrudescence des incidents de cybersécurité touchant au secteur industriel. En 2023 et 2024, le Centre pour la Cybersécurité Belgique (CCB) a recensé respectivement 120 et 109 attaques par rançongiciel contre des organisations belges. Le secteur

e). Chez Sirris, le
cette tendance
ues des cibles



Les conséquences d'une cyberattaque sur les systèmes industriels peuvent être dramatiques : arrêt prolongé des chaînes de production, pertes financières considérables, dégradation rapide de la réputation auprès des clients et des partenaires. Dans certains cas extrêmes, la sécurité même des employés est compromise lorsque les cybercriminels s'en prennent à des systèmes critiques. Sans oublier les fuites de données sensibles, telles que les secrets industriels ou les informations stratégiques.

NIS2 : de nouvelles obligations renforcées

Face à ces menaces croissantes, l'Union européenne durcit le ton avec NIS2, la nouvelle directive sur la sécurité des réseaux et de l'information. Son objectif est de renforcer la résilience des secteurs considérés comme importants ou essentiels, dont l'industrie manufacturière. Concrètement, NIS2 impose désormais aux entreprises belges plusieurs mesures obligatoires, dont :

- l'évaluation régulière des risques cyber pour identifier les vulnérabilités ;
- l'élaboration de plans de réponses aux incidents afin de réagir rapidement en cas d'attaque ;
- le contrôle renforcé des fournisseurs et sous-traitants ;

- les sanctions financières en cas de non-conformité.

Chez Sirris, nous constatons que de nombreuses entreprises sous-estiment encore les impacts d'une non-conformité à NIS2. Pourtant, les sanctions peuvent être sévères, tant financièrement qu'en termes de réputation. Plus qu'une obligation, la cybersécurité est désormais un enjeu crucial de compétitivité et de résilience industrielle.

5 failles courantes en cybersécurité industrielle

Les entreprises industrielles, dont les systèmes IT (informatique) et OT (technologies opérationnelles) sont désormais étroitement interconnectés, restent particulièrement vulnérables. Parmi les failles les plus courantes observées dans l'industrie :

1. **Absence de segmentation du réseau**

Lorsque les systèmes IT/OT sont interconnectés sans séparation claire, une seule faille suffit à compromettre l'ensemble des infrastructures.

2. **Logiciels obsolètes**

Nombre d'usines utilisent encore des systèmes d'exploitation et des logiciels datant de plusieurs décennies, sans aucune mise à jour. Elles deviennent ainsi des cibles faciles pour les hackers.

3. **Hameçonnage (phishing) et ingénierie sociale**

Les cybercriminels exploitent la faiblesse humaine : un simple e-mail frauduleux peut suffire pour infiltrer un système.

4. **Mauvaise gestion des accès**

Un accès trop large aux systèmes sensibles par les employés permet aux cybercriminels d'exploiter des comptes sécurisés pour s'infiltrer.

5. **Failles dans la chaîne d'approvisionnement**

Les fournisseurs et prestataires tiers peuvent être des points d'entrée pour les cyberattaques affectant toute l'infrastructure industrielle.

Ces failles, bien connues des cybercriminels, nécessitent une vigilance constante et des mesures de protection renforcées.

Cinq mesures clés pour renforcer votre sécurité

Aucune entreprise est totalement invulnérable, mais il existe des mesures simples et efficaces pour limiter considérablement les risques :

1. **Segmenter les réseaux IT et OT**

Séparer les environnements IT et OT permet de limiter la propagation d'une attaque et d'éviter qu'un problème sur un système bureautique ne paralyse la production.

2. **Maintenir les logiciels à jour**

Les mises à jour de sécurité sont essentielles pour corriger les failles exploitées par les hackers. Un système obsolète est une cible facile.

3. **Former et sensibiliser les employés aux risques cyber**

Les collaborateurs constituent la première ligne de défense. Sensibilisez-les aux attaques de phishing, aux mots de passe sécurisés et aux bonnes pratiques en matière de cybersécurité.

4. **Renforcer la gestion des accès**

L'accès aux systèmes critiques doit être limité aux seules personnes autorisées.

L'authentification multi-facteurs (MFA) et la gestion des droits d'accès par rôle sont des solutions efficaces.

5. Sécuriser la chaîne d'approvisionnement

Les fournisseurs doivent respecter des normes de cybersécurité strictes. Vérifiez qu'ils appliquent des contrôles adéquats pour éviter d'être exposé à des vulnérabilités indirectes.

Ces bonnes pratiques sont accessibles à toutes les entreprises et permettent d'éviter des pertes financières considérables. Chez Sirris, nous sommes d'avis que de petites actions aujourd'hui peuvent éviter des catastrophes majeures demain.

Anticiper pour mieux résister

Les cybermenaces évoluent rapidement, et l'industrie ne peut plus ignorer les enjeux liés à la cybersécurité. Si la mise en conformité avec la directive NIS2 constitue un défi, elle représente surtout une opportunité pour renforcer la compétitivité et la résilience des entreprises industrielles. Investir aujourd'hui dans la cybersécurité garantit la continuité des opérations et protège l'avenir de l'industrie.

Que vous soyez dans la fabrication ou les services numériques, CyberActive, une initiative dont Sirris est partenaire, vous aide à naviguer dans le monde des cybermenaces grâce à des formations, des supports pédagogiques et des vidéos explicatives sur tous les aspects de la cybersécurité.

[Découvrez le programme et inscrivez-vous](#)

CyberActive est une initiative de Sirris, Howest, l'Université atholique de Louvain et la Vrije Universiteit Brussel. Financé par le SPF Economie et l'Union Européenne (Next Generation)

Auteurs



Thierry Coutelier