

Directive NIS2 : sécurisez votre production connectée

09 avril 2025, 13:59

Thierry Coutelier
Olivier Gramaccia

Êtes-vous prêt à faire face aux nouvelles obligations de cybersécurité imposées par la directive NIS2 ?

Capteurs connectés, machines intelligentes, robots collaboratifs… L'Internet des Objets (IoT) transforme la production industrielle. Les processus deviennent plus efficaces, la productivité s'améliore, la compétitivité augmente. Mais cette révolution technologique expose aussi votre entreprise à de nouveaux risques cyber. La directive NIS2 vous aide à renforcer votre niveau de cybersécurité.

Depuis le 18 octobre 2024, la directive européenne NIS2 est en vigueur en Belgique. Elle impose aux entreprises actives dans des secteurs critiques, dont l'industrie manufacturière, de renforcer leur cyber-résilience.

NIS2 : une obligation légale et un enjeu stratégique

Si votre entreprise utilise des équipements connectés (IoT) dans sa production, son stockage ou sa logistique, vous êtes potentiellement concerné par la directive NIS2. Et pas uniquement d'un point de vue technique : en cas de non-conformité, la responsabilité des dirigeants peut être engagée. Vous devez donc savoir dans quel niveau votre société est catégorisée afin de connaître vos obligations.

Ignorer NIS2 ? Voici trois risques majeurs :

- **Perturbation des opérations :** une cyberattaque peut paralyser vos lignes de production, entraîner des pertes financières et des retards de livraison.
- **Fuite de données sensibles :** les informations confidentielles sur vos produits, clients, procédés ou finances peuvent être compromises.
- **Atteinte à la réputation :** une faille de sécurité peut éroder la confiance de vos clients et partenaires.

Pour déterminer votre niveau NIS2, consultez la page web du CCB :

Déterminez votre niveau NIS2

CyberFundamentals : la méthode de mise en conformité du CCB

Pour aider les entreprises à se préparer, le Centre pour la Cybersécurité Belgique (CCB) a mis en place un cadre appelé CyberFundamentals. Il propose des mesures concrètes et adaptées à la taille et au profil de risques de chaque organisation. Ce cadre se décline en quatre niveaux d'assurance : « Small », « Basic », « Important » et « Essential ». D'autres certifications, telles que l'ISO 27001, peuvent faciliter la conformité à NIS2. Les mesures de cybersécurité mises en œuvre doivent être proportionnées aux risques encourus par l'entreprise.

Si votre entreprises compte plus de 50 ETP ou dépasse les 10 millions d'euros de chiffre d'affaires, vous êtes au minimum soumis au niveau « Important » de NIS2. Et même si vous ne l'êtes pas, suivre les recommandations du niveau « Basic » vous permet déjà de sécuriser efficacement vos systèmes et de répondre aux attentes de vos clients.

Niveau « Basic » : les fondamentaux pour protéger vos objets connectés

Le niveau « Basic » ne parle pas explicitement d'IoT, mais plusieurs mesures s'appliquent directement à ces dispositifs. En voici une sélection, organisée selon cinq catégories :

Identifier :

- **ID.AM-1 :** Cette mesure consiste à faire l'inventaire des appareils physiques, y compris tous les objets connectés (IoT) reliés au réseau de l'organisation.
- **ID.AM-2 :** Similaire à ID.AM-1, cette mesure se concentre sur l'inventaire des plateformes et applications logicielles. Il est donc également nécessaire de répertorier les logiciels et applications spécifiques utilisés par les appareils IoT.

- **ID.AM-3 :** Cette mesure met l'accent sur la schématisation de la communication organisationnelle et des flux de données. Dans le contexte de l'IoT, cartographiez vos flux : d'où viennent les données IoT, où vont-elles et comment circulent-elles ?
- **ID.RA-1 :** Identifier les menaces et les vulnérabilités liées à vos périphériques IoT. Cela vous permettra d'évaluer au mieux le risque et d'agir en conséquence.

Projeter :

- **PR.AC-1 :** Gérer correctement les identifiants des objets connectés (IoT) : éviter les mots de passe par défaut, appliquer des règles fortes, ne pas les partager.
- **PR.AC-3 (mesure clé) :** Sécuriser l'accès à distance aux appareils IoT, avec une identification forte (comme la MFA). De plus, isoler les appareils du réseau principal si possible (voir PR.AC-5).
- **PR.AC-4 (mesure clé) :** Appliquer le principe du moindre privilège aux appareils IoT : ne donner que les accès nécessaires aux utilisateurs ou systèmes.
- **PR.AC-5 :** Segmenter le réseau pour isoler les objets connectés et limiter les risques de propagation en cas d'attaque.
- **PR.DS-1 :** Chiffrer les données stockées sur les appareils IoT, et si possible, aussi celles en transit (PR.DS-2).
- **PR.IP-4 (mesure clé) :** Faire des sauvegardes régulières des données et configurations des appareils IoT, et les tester
- **PR.MA-1 (mesure clé) :** Maintenir les appareils à jour avec les derniers correctifs et mises à jour de sécurité.
- **PR.PT-1 (mesure clé) :** Effectuer et tester des sauvegardes régulières des données des appareils IoT et de leurs configurations. En cas d'incident, cela permet de restaurer les appareils et les données à un état antérieur à l'incident.
- **PR.PT-4 :** Assurer la maintenance des appareils IoT pour garantir leur sécurité. Installer des correctifs et mises à jour de sécurité pour les systèmes d'exploitation et les logiciels utilisés par les appareils IoT.

Détecter :

- **DE.CM-1 :** Surveiller le réseau pour repérer les activités suspectes des appareils IoT, en utilisant des outils pour détecter les anomalies de trafic.
- **DE.CM-4 (mesure clé) :** Détecter les logiciels malveillants pour protéger les IoT. Utiliser des solutions anti-malware pour bloquer les infections ciblant ces appareils.

Répondre :

- **RS.RP-1 :** Avoir un plan de réponse aux incidents IoT, incluant la détection, l'analyse, le confinement, la suppression et le rétablissement des appareils IoT compromis.

Rétablir :

- **RC.RP-1 :** Prévoir un plan de restauration des appareils IoT et des services associés après un incident de sécurité. Ce plan doit inclure les procédures de restauration des données, de reconfiguration des appareils et de reprise des services.

Bon à savoir : cette liste n’est pas exhaustive. D’autres mesures peuvent être pertinentes pour la sécurité de l’IoT en fonction du contexte et des besoins spécifiques de l’organisation.

Les mesures de cybersécurité du niveau « Basic » ont un impact significatif sur la sécurité des objets connectés (IoT). Mettre en œuvre ces mesures en tant qu’organisation permet de renforcer la production de vos données, de réduire les risques de cyberattaques et d’accroître votre cyber-résilience dans un environnement où l’IoT est de plus en plus présent.

Consultez le guide complet du niveau « Basic » :

CyberFundamentals - Niveau « Basic » (PDF)

Niveau « Important » : pour les moyennes et grandes entreprises

Les organisations de taille moyenne à grande doivent aller plus loin. Le niveau « Important » comprend des mesures complémentaires suivantes :

- L’identification des dépendances et des fonctions critiques (ID.BE-4)
- L’établissement des exigences de résilience (ID.BE-5)
- L’évaluation des risques liés à la chaîne d’approvisionnement (ID.SC)
- La configuration sécurisée des équipements (PR.IP-1)
- La restriction des supports amovibles (PR.RT-2)
- Le principe de la moindre fonctionnalité (PR.PT-3)
- La surveillance physique des installations (DE.CM-2)
- L’analyse de vulnérabilités (DE.CM-8)

En appliquant ces mesures, votre PME se conforme à la loi et protège ses opérations, ses données et sa réputation. Sécuriser vos périphériques IoT et leur gestion renforce la résilience de votre entreprise face aux cybermenaces et vous assure un avenir prospère.

En résumé :

- NIS2 est en vigueur en Belgique depuis le 18 octobre 2024.
- Elle s’applique à de nombreuses PME industrielles utilisant l’IoT.
- Le niveau « Basic » du CCB est une base solide pour sécuriser vos équipements.
- Sirris vous accompagne dans la mise en conformité.

Sirris vous accompagne vers la conformité

Mettre en œuvre la directive NIS2 demande une stratégie claire et une bonne compréhension des enjeux industriels.

Sirris vous aide à :

- Evaluer vos risques IoT.
- Identifier votre niveau NIS2.
- Mettre en place les bonnes pratiques.
- Renforcer la formation de vos équipes.

Passez à l'action dès maintenant !

Protégez vos objets connectés. Sécurisez votre production. Préparez votre avenir.

Contactez un expert Sirris :

Thierry COUTELIER

Consultez le guide CyberFundamentals – Niveau « Basic » (PDF)

A consulter également :

- La page officielle NIS2 – CCB
- Les formations gratuites CyberActive (projet co-financé par le SPF Economie et l'Union européenne)

Article rédigé dans le cadre de l'Antenne Normes IoT, avec le soutien du SPF Economie.

Auteurs



Thierry Coutelier



Olivier Gramaccia