

Travailler à la conformité NIS2 avec Secutec Services

Le nouveau cadre réglementaire NIS2 (Network & Information Systems) couvre un champ beaucoup plus large que son prédécesseur. La catégorie des industries essentielles a été élargie et une catégorie supplémentaire a été ajoutée pour les organisations dans les industries « clés ».

Les services de Secutec peuvent jouer un rôle important pour votre organisation sur la voie de la conformité.

Qu'est-ce que le NIS2 et qui est concerné ?

Le cadre NIS2 offre des conditions de base égales pour la **cybersécurité au sein de l'union européenne**. Les organisations sont soumises aux mêmes normes, notamment en matière d'exigences, de contrôle et de sanctions. Les moyennes et grandes entreprises opérant dans l'un des 15 secteurs clés devront se conformer à leurs mesures, mises en œuvre et protocoles de cybersécurité.

La NIS2 est en vigueur depuis le **18 octobre 2024**. Toutes les organisations, y compris les entreprises de votre chaîne d'approvisionnement, doivent être **enregistrées auprès de la DGCC avant mars 2025** et **être pleinement conformes avant avril 2026**. Les plus grandes organisations feront l'objet d'un audit d'ici avril 2027.

Micro



< 10



< €2 M

Petite



10 - 50



< €10 M

Moyenne



50 - 250



< €50 M

Grande



> 250



> €50 M

Domaines clés de la conformité

La direction

Chaque membre de la direction doit avoir une bonne compréhension des efforts de son organisation en ce qui concerne les exigences du NIS2. Ils sont responsables du calcul et du traitement des risques de cybersécurité.

Rapports au gouvernement

Les organisations doivent mettre en œuvre des processus permettant de signaler correctement les incidents aux autorités locales. L'une des exigences stipule que tout incident cybernétique doit être signalé dans les 24 premières heures.

Gestion des risques

Des mesures doivent être mises en œuvre pour minimiser les risques et les conséquences des cyberincidents. Cela comprend la réponse aux incidents, la sécurité de la chaîne d'approvisionnement, la sécurité du réseau, le contrôle d'accès et le cryptage.

Continuité des activités

Les organisations doivent être en mesure d'assurer la continuité de leurs opérations en cas de cyberincident. Cela inclut, sans s'y limiter, la récupération des systèmes, les procédures d'urgence et la conduite d'une équipe d'intervention en cas d'incident.

Secutec et le cadre NIS2

L'infographie ci-dessous montre comment et où Secutec peut apporter une contribution significative à la conformité NIS2 de votre organisation.

Cyber Fundamentals Framework



[HTTPS://CCB.BELGIUM.BE](https://ccb.belgium.be)

Pour plus d'informations sur les réglementations NIS2, visitez le site Web du CCB ou contactez votre autorité nationale de cybersécurité.

À propos de Secutec

La société de cybersécurité Secutec a été fondée en 2005 dans le but de fournir un service inégalé en matière de cybersécurité, de renseignement sur les menaces et de réponse aux incidents. S'appuyant sur notre portefeuille de produits, nos innovations exclusives et nos services internes, nos experts en sécurité informatique vous conseillent et vous guident dans la protection, la gestion et la mise en œuvre de votre posture de cybersécurité, afin que vos investissements informatiques atteignent leur plein potentiel.

Basée à Aartselaar, l'organisation dispose d'une équipe de 85 experts internes et sert plus de 800

clients dans 60 pays. En outre, Secutec a des bureaux aux Pays-Bas, en Autriche, au Canada et une représentation dans la région ANZ (Australie et Nouvelle-Zélande).

Secutec offre des solutions partielles pour la conformité NIS2. Nous déclinons toute responsabilité quant à l'atteinte d'une conformité totale et ne pouvons être tenus responsables en cas d'incidents cybernétiques. Il est conseillé aux clients de mettre en œuvre des stratégies globales et de prendre des mesures supplémentaires pour assurer une conformité totale avec les exigences du NIS2.