PRÉPAREZ-VOUS À LA DIRECTIVE NIS2

APPROACH CYBER VOUS AIDE À NAVIGUER DANS LA NOUVELLE LÉGISLATION VISANT À RENFORCER LA CYBERSÉCURITÉ EN EUROPE, ET À PRENDRE LES MESURES ADÉQUATES POUR VOUS Y CONFORMER RAPIDEMENT.

Commencez à temps

Avec l'adoption de la directive NIS2 (Network and Information Systems Directive), l'Union européenne (UE) renforce ses exigences en matière de cybersécurité pour une large gamme d'entreprises et d'organisations. La directive a été transposée en droit belge par la loi adoptée par le parlement fédéral ce 19 avril 2024. De nombreux secteurs sont concernés, et la NIS2 leur impose de prendre des mesures de cybersécurité renforcées, une obligation de notification d'incidents, et une supervision par l'autorité de cybersécurité nationale.

Les entités concernées ont jusqu'au 18 octobre 2024 pour se conformer à la loi NIS2 belge.
Ce qui signifie que celles-ci devraient déjà avoir pris toutes les mesures exigées.

Êtes-vous concernés par la NIS2 ?

La portée de la directive NIS2 est considérablement élargie par rapport à sa version antécédente, la NIS1, pour inclure un plus grand nombre d'entreprises et organisations de nombreux secteurs. La directive NIS2 s'adresse aux organisations d'une certaine taille qui fournissent des services dans des secteurs critiques. Les entités dans ces secteurs sont considérées comme vitales pour le maintien des fonctions sociétales ou économiques critiques en Belgique. La taille (« size cap ») et le service fourni sont ainsi les deux principaux critères pour déterminer si la directive NIS2 s'applique à une organisation. Les secteurs concernés sont les suivants :

- **Les secteurs hautement critiques :** tels que l'énergie, les transports, le secteur bancaire et infrastructures de marchés financiers (également soumis à DORA), la santé, l'eau potable, les eaux usées, les infrastructures numériques, la gestion des services TIC, l'administration publique (centrale et régionale) et l'espace.

- **Les autres secteurs critiques :** tels que les services postaux et d'expédition, la gestion des déchets, la chimie, et le secteur des denrées alimentaires, la fabrication (« manufacturing »), les fournisseurs numériques, et la recherche.

Sauf exception, une organisation doit être considérée au moins comme une moyenne entreprise pour se voir appliquer la directive NIS2. Une moyenne entreprise dispose d'un effectif équivalent au moins à 50 travailleurs à temps plein et/ou réalise un chiffre d'affaires annuel total (ou le total du bilan annuel) qui excède 10 millions d'euros.

La directive NIS2 établit également une distinction entre entités « essentielles » et « importantes ». Cette distinction se fait sur la base de la taille de l'entité et du service fourni.
La différence entre entités essentielles et importantes réside principalement dans les mécanismes de contrôle et de sanctions. Les entités essentielles seront contrôlées de manière plus régulière et stricte que les entités importantes.

Et pour les entreprises non visées, qu'en est-il ?

La NIS2 ne spécifie pas explicitement les obligations pour les entreprises qui ne rentrent pas dans ce périmètre. Toutefois, Même si une entreprise n'entre pas dans le champ d'application de la NIS2, elle peut néanmoins être affectée indirectement en tant que fournisseur, ou choisir de suivre certaines pratiques recommandées pour améliorer sa cybersécurité.

La directive NIS2 s'adresse aux organisations d'une certaine taille qui fournissent des services dans des secteurs critiques, les entités dites « essentielles » et « importantes ».

Un organe de supervision et de contrôle, le CCB

Chaque État membre de l'UE doit désigner une ou plusieurs autorités compétentes pour superviser l'application de la directive, assurer la mise en œuvre des mesures de sécurité appropriées, et gérer les incidents et crises de cybersécurité. En Belgique, l'autorité compétente est le Centre pour la Cybersécurité Belgique (CCB). Les entités concernées ont le devoir de s'enregistrer auprès du CCB, via le portail Safeonweb@work. Sauf exception, cette obligation peut être réalisée jusqu'au 18 mars 2025.

Les organisations belges concernées ont l'obligation de s'enregistrer elles-mêmes auprès du Centre pour la Cybersécurité Belgique (CCB), avant le 18 mars 2025.

Quelles sont vos obligations ?

Les entités concernées doivent prendre les mesures appropriées et proportionnées pour gérer les risques qui menacent la sécurité de leurs réseaux et des systèmes d'information, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

Les entités concernées devront également notifier, sans retard injustifié, au CSIRT national les cyber-incidents significatifs (en Belgique, au cert.be). Enfin les entités essentielles ont le devoir d'effectuer des évaluations régulières de la conformité, vérifiées par un organisme de contrôle de la conformité.

Contactez-nous pour plus d'information concernant les mesures appropriées et proportionnées.

Le CCB dispose du pouvoir d'adopter des mesures pour inciter les entités à prendre les mesures qui s'imposent. À cette fin, il peut, par exemple, exiger la réalisation d'audits externes réguliers, effectuer des inspections ou solliciter la production de certains documents.

Le CCB pourra notamment émettre des avertissements ou des instructions contraignantes afin de remédier aux insuffisances constatées ou encore d'informer leurs clients.

La NIS2 impose un renforcement de vos mesures de gestion des risques en matière de cybersécurité, ainsi qu'une obligation de notification des incidents dans délais, sous l'égide du CCB.

Quelles sont les sanctions en cas de non-conformité ?

La directive NIS2 renforce non seulement les exigences de cybersécurité, et vos obligations, mais elle prévoit aussi des sanctions plus strictes pour garantir la conformité.

Ainsi, les violations en matière de mesures de gestion des risques ou de notification d'incident pourront être punies par des amendes administratives dissuasives.

Dans ce cas, l'amende est de type RGPD. Pour les entités essentielles, ces amendes peuvent atteindre 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial. Pour les entités importantes, elles s'élèvent à 7 millions ou 1,4 % du chiffre d'affaires annuel mondial. Et en cas de récidive pour les mêmes faits dans un délai de trois ans, le montant de l'amende administrative est doublé. A noter que ces amendes ne s'appliquent pas aux autorités publiques, contrairement aux autres sanctions administratives qui s'appliqueront bel et bien.

Les sanctions sont sévères et dissuasives pour garantir la conformité. Elles sont dans certains cas d'un niveau comparable à celles du RGPD.

Un top management désormais directement concerné

La NIS2 intensifie la responsabilisation de la direction de chaque entité, afin que la cybersécurité devienne un véritable sujet de discussion jusqu'au niveau du conseil d'administration. Afin de les sensibiliser davantage, les personnes physiques qui représentent ces entités, pourront être tenues responsables du non-respect des obligations de la directive.

Les sanctions sont sévères, allant jusqu'à une amende personnelle pour le CEO, et les administrateurs, ou une interdiction temporaire d'occuper un poste de direction.

Il est donc impératif que le conseil d'administration puisse saisir facilement les enjeux de la sécurité de l'information et évaluer la pertinence des mesures prises pour renforcer cette sécurité.

Le top management est tenu directement responsable de la conformité à la NIS2. En cas de non-respect des obligations, des sanctions et amendes personnelles sont prévues.

Quels sont les mesures à mettre en place ?

Tout d'abord en matière de gouvernance, le top management devra approuver les mesures de gestion des risques en matière de cybersécurité, superviser leur mise en œuvre et pourront être tenus responsables des éventuels manquements.

Afin qu'ils comprennent les mesures qu'ils approuvent, les membres de la direction devront suivre une formation de cybersécurité et offrir régulièrement une formation similaire aux membres de leur personnel.

Les mesure de sécurité devront être appropriées et proportionnées, selon une analyse de risques. Bien entendu, il conviendra de mettre en place toutes les pratiques de base en matière de cyberhygiène. Mais ces mesures ne suffisent pas.

La NIS2 exige une démarche globale et complète, un système de gestion et d'amélioration continue, incluant un ensemble de mesures de sécurités techniques (tels que par ex. le chiffrement, la cryptographie, l'authentification à plusieurs facteurs, etc) et non-techniques (tels que des politiques et des procédures, une organisation, un plan de continuité des activités, une gestion des backups, une gestion de crise, une gestion de la sécurité des fournisseurs et prestataires de services, une sécurité physique et périmétrique, la sécurité des ressources humaines, etc). Des mesures additionnelles ont également été ajoutées dans la loi NIS2 belge.

Les mesures à mettre en place sont techniques et non-techniques. Au-delà de ces mesures, c'est un véritable système de gestion de risque et d'amélioration continue qui est exigé.

Vous n’êtes pas seul ! Approach Cyber est à vos côtés

La conformité à la NIS2 est l’un des sujets majeurs de conformité en 2024, et une réponse efficace nécessite une préparation et une expertise approfondies. Voici comment nous vous accompagnons à vous préparer et à assurer la conformité avec la NIS2 :

1. Evaluation des risques et analyse des gaps

- Nous effectuons une évaluation complète des risques pour identifier les vulnérabilités et les menaces potentielles dans vos réseaux et systèmes d'information.
- Nous réalisons une analyse des gaps pour comparer vos pratiques actuelles avec les exigences de la NIS2, selon les cadres de références cités par le CCB (tels que le CyberFundamentals ou « CyFun », et l’ISO27001).

2. Mise en place de mesures de sécurité

- Nous implémentons les mesures techniques et organisationnelles appropriées pour gérer les risques identifiés, selon les recommandations du CCB.
- Nous assurons que toutes les mesures de sécurité sont régulièrement mises à jour et testées pour répondre aux nouvelles menaces et aux exigences de la NIS2.

3. Établissement de protocoles de réponse aux incidents

- Nous développons des protocoles détaillés pour la détection, la notification, le rapportage, et la réponse aux incidents de cybersécurité, selon les exigences du CCB et du RGPD quand des données personnelles sont impliquées.
- Nous formons votre personnel à reconnaître et à réagir efficacement aux incidents de sécurité, y compris les fuites de données personnelles.

4. Sensibilisation et formation

- Nous formons la direction et vos employés sur les bonnes pratiques de cybersécurité et sur les procédures à suivre en cas d'incident.
- Nous sensibilisons l'ensemble de votre organisation à l'importance de la conformité à la NIS2.

5. Documentation et conformité réglementaire

- Nous documentons toutes les politiques, dont la politique de sécurité de l’information, la politique de vulnérabilités coordonnées, indispensables prérequis NIS2, ainsi que les procédures et mesures de sécurité mises en place.
- Nous maintenons une documentation à jour pour pouvoir démontrer votre conformité aux autorités en cas de besoin.

6. Surveillance, entretien et certification

- Nous assurons un suivi régulier et une mise à jour continue de vos mesures de sécurité pour garantir une conformité durable, notamment par l'établissement de tableaux de bord à destination de la direction et du conseil d'administration.
- Pour les entités essentielles, nous vous accompagnons à préparer et passer les audits, inspections et certifications CyFun ou ISO27001 dans les délais légaux (18 avril 2027).

Une vraie expertise de terrain est cruciale pour assurer la conformité, répondre efficacement aux incidents et protéger vos infrastructures critiques.

Contactez-nous pour de plus amples informations sur les étapes clés pour la conformité NIS2 et découvrez comment nous les mettons en pratique. En nous basant sur les cadres de références cités par le CCB et notre expérience réussie auprès de nombreuses organisations, nous sommes prêts à vous accompagner dans chaque étape de votre parcours de conformité.

Approach Cyber vous accompagne à chaque étape de votre parcours de conformité. En nous basant sur les cadres de références cités par le CCB et notre expérience réussie auprès de nombreuses organisations.

Quels sont les avantages de la directive NIS2 pour votre organisation ?

Au-delà de la conformité, la NIS2 offre l'opportunité de vous différencier sur le marché, ou de montrer le bon exemple si vous êtes un pouvoir public. Les entreprises qui démontrent un engagement proactif en matière de cybersécurité peuvent non seulement minimiser les risques de perturbations opérationnelles, mais également renforcer la confiance de leurs clients et partenaires.

La NIS2 permet aux entreprises de se différencier sur le marché et de renforcer la confiance des clients et partenaires en montrant un engagement proactif en matière de cybersécurité.

Témoignage de notre CEO

« *C'est l'un des sujets brûlants de l'année en matière de conformité, aux côtés de l'AI Act. Plutôt que de percevoir la NIS2 comme un deuxième RGPD, avec ses pressions réglementaires et ses sanctions, voyons-la comme une opportunité de renforcer la cyber sérénité de votre entreprise dans un paysage numérique menaçant* », **David Vanderoost, CEO d'Approach Cyber.**

Pourquoi choisir Approach Cyber en tant que partenaire pour votre conformité ?

Nous nous mobilisons pour vous fournir les ressources, les outils et l'expertise nécessaires pour naviguer efficacement dans ce paysage réglementaire complexe. En collaborant avec nous, vous pouvez être assuré que votre organisation est bien préparée pour répondre aux défis de la NIS2 et pour protéger vos actifs numériques contre les menaces potentielles.

Approach Cyber se positionne comme votre partenaire de choix pour vous accompagner dans cette démarche :

- **Un partenaire solide et reconnu :** Établie depuis plus de 20 ans, avec de nombreuses références et ses certifications ISO 27001/27701, Approach Cyber est un prestataire de services de référence en Belgique.
- **Pouvant vous faire bénéficier de subsides régionaux :** si votre entreprise est une PME, vous pouvez bénéficier d'une aide financière substantielle de la part de votre région. Approach Cyber est un prestataire de services reconnu/labelisé par les autorités des trois régions du pays.
- **En pleine coopération sectorielle :** Nous participons activement à des initiatives de partage d'informations et d'expériences sur la NIS2, et à des groupes sectoriels pour aider les entreprises (par ex. Agoria, UWE/AKT, CyberWal, Cyber Security Coalition, SecAppDev, ISACA, FSMA, etc).
- **Une équipe pluridisciplinaire de plus de 100 personnes :** Nous offrons une expertise à la fois technique, stratégique et juridique pour vous guider à travers les exigences complexes de la NIS2.
- **Des solutions personnalisées et orientées business :** Nous développons des solutions sur mesure adaptées à vos besoins spécifiques, et à la taille de votre organisation. Nous adressons les défis et besoins en matière de cybersécurité à tous les échelons, jusqu'au conseil d'administration.
- **Une « approach » globale et intégrée :** nous offrons une gamme complète de services en cybersécurité (360°) avec une approche tout-en-un. Nos partenariats technologiques forts nous permettent de fournir des solutions avancées et intégrées, simplifiant la gestion de votre sécurité. Cela vous libère pour vous concentrer sur vos opérations principales sans la complexité de coordonner plusieurs prestataires.

Contactez-nous

N'hésitez pas à nous contacter pour en savoir plus sur la directive NIS2 et comment nous pouvons vous aider à vous y conformer.

info@approach-cyber.com
+32 10 83 22 11
+32 3 366 21 76