La directive NIS2 : un levier et un accélérateur pour la cybersécurité

inetum

Cybersécurité vs Conformité

La cybersécurité est un enjeu essentiel pour les CIO belges. Mais qu'en est-il de la conformité ? Les CIO ont-ils conscience de l'importance de respecter au mieux les réglementations imposées en matière de cybersécurité ?

La réponse à cette question se trouve dans l'étude de marché locale menée par **Beltug**, la plus grande association de CIO et de décideurs IT en Belgique avec 2 200 adhérents.

La cybersécurité reste « top of mind »

Selon **l'enquête annuelle sur les priorités** des décideurs IT de Beltug, la cybersécurité se classe en tête de liste depuis un certain temps. En 2023, l'intelligence artificielle (IA) a eu beau monopoliser l'attention, la cybersécurité figurait à nouveau parmi les premières préoccupations des CIO belges.

Cette année-là, pas moins de 4 priorités du top 10 relevaient de ce thème : élaboration d'une stratégie et d'une architecture de sécurité informatique, sensibilisation des utilisateurs à la sécurité et à la confidentialité, planification de la réponse aux cyberincidents et mise sur pied d'un Centre de Réponse aux Incidents de Sécurité Informatique (CSIRT). Au final, près de la moitié du top 40 des priorités des CIO en 2023 concernaient directement la sécurité.

> Actuellement, aucun décideur IT ne remet vraiment en cause la pertinence des investissements en cybersécurité.
>
> **Levi Nietvelt,**
> *Beltug*

L'enquête utilisateur bisanuelle de Beltug montre aussi que les CIO belges prennent ce thème au sérieux. Les investissements en cybersécurité se maintiennent : début 2023, à peine 3,5 % des entreprises estimaient qu'ils seraient revus à la baisse. Un quart d'entre elles s'attendaient à ce qu'ils restent stables, tandis que près de 7 entreprises sur 10 (68 %) considéraient que ces investissements seraient plutôt revus à la hausse.

La conformité passée sous silence

Lorsque l'on examine l'attention que les CIO belges portent à la conformité, une tout autre image se dessine. À moins de l'assimiler à la gouvernance (des données, IT, de l'IA…) ou aux questions ESG (rapports de durabilité), le terme n'apparaît guère dans la liste des priorités.

Pourtant, la conformité représente d'ores et déjà un défi important, en particulier sur le plan de la cybersécurité et de la confidentialité des données. Et cela ne fera que s'accentuer dans les années à venir : les nouvelles mesures législatives et réglementaires se succèdent à un rythme effréné, notamment au niveau de l'Union européenne. Il n'est pas toujours facile de se tenir au fait des obligations, d'autant que les règles peuvent varier d'un pays à l'autre.

> Vu que la conformité est à peine mentionnée dans la liste des priorités des CIO, est-ce à dire qu'elle n'a pas d'importance à leurs yeux ?
>
> **Levi Nietvelt,**
> *Beltug*

Conformité à la directive NIS2 : la fin de la récréation

Les États et l'UE imposent de plus en plus d'exigences de cybersécurité aux entreprises. Un bon exemple : la directive NIS2, qui succède à la **directive sur la sécurité des réseaux et des systèmes d'information (NIS)** de 2016. La première version est parfois considérée comme la toute première « loi sur la cybersécurité ». Les deux directives, l'ancienne et la nouvelle, ont en tout cas le même objectif final : mieux protéger les entreprises, améliorer la gestion des risques et prévenir les incidents ou au moins, en limiter au maximum les conséquences.

La directive NIS2 s'inscrit dans une vague d'exigences européennes en matière de cybersécurité, allant du règlement eIDAS de 2014 au règlement RSGP de 2023. Même dans le cadre de cette législation toujours plus étendue, la directive NIS2 **se distingue par sa portée** et **son impact profond sur les organisations dans leur ensemble :** elle ne se limite pas à des départements donnés ou à des services, des produits ou des technologies spécifiques.

NIS2 couvre pas moins de **18 secteurs**, soit 11 de plus que la première version, et s'applique à **plus de 180 000 entreprises dans l'Union européenne**. Selon une première estimation du Centre pour la Cybersécurité Belgique (CCB), 2 400 entreprises belges relèveraient du champ d'application de la nouvelle directive européenne. Inetum estime qu'il s'agirait de quelque 3 000 sociétés. Mais en définitive, quel que soit le nombre d'entreprises concernées, la directive NIS2 est **la législation européenne la plus étendue à ce jour en matière de cybersécurité.**

> Quelle que soit votre situation, que vous en releviez directement ou non, la directive NIS2 est une loi importante.
>
> **Levi Nietvelt,**
> *Beltug*

La chaîne d'approvisionnement : une source de pression (en plus)

Non seulement la directive NIS2 étend le champ d'application de la directive initiale, mais en plus, l'impact sur les entreprises qui en relèvent est beaucoup plus important. Les **exigences** que l'UE leur impose, notamment en matière de **reporting**, ont été rendues nettement plus lourdes et plus strictes.

Il en va de même pour les **sanctions** encourues par les entreprises qui ne satisfont pas aux exigences : outre des **amendes administratives**, la désignation d'un superviseur et la suspension de certifications ou d'autorisations – pour ne citer que quelques-unes des sanctions possibles –, le non-respect de la directive pourra entraîner **des conséquences juridiques pour les cadres supérieurs**. Même le CEO de l'entreprise en défaut pourra se voir temporairement interdire l'exercice de fonctions dirigeantes.

Par ailleurs, la nouvelle directive NIS2 met l'accent sur la garantie de la **sécurité opérationnelle (business continuity)**. Et cette exigence s'étend à l'ensemble de la chaîne logistique : **la sécurité de la chaîne d'approvisionnement** fait l'objet d'une attention accrue. De ce fait, la conformité avec la directive est recommandée dans de nombreux cas, y compris pour les organisations auxquelles elle ne s'applique pas directement. En imposant les mêmes normes de conformité tout au long de leur chaîne d'approvisionnement, les entreprises peuvent éviter les fuites de données ou empêcher les pirates informatiques de les atteindre via leurs fournisseurs.

> En un mot : c'est la fin de la récréation. L'Europe veut que toutes les entreprises atteignent un seuil de cybersécurité minimum et la directive NIS2 est un levier qui doit accélérer cette évolution.
>
> **Koen Tamsyn,**
> *Solution Manager*
> *Cybersecurity, Inetum*

Le temps presse !

La Commission européenne a introduit la proposition de nouvelle directive européenne en matière de cybersécurité NIS2 en décembre 2020. Après un processus de négociation rapide, le texte définitif a été adopté deux ans plus tard par le Conseil et le Parlement européen. Il a été publié le 27 décembre 2022 et **entrera officiellement en vigueur en janvier 2023.**

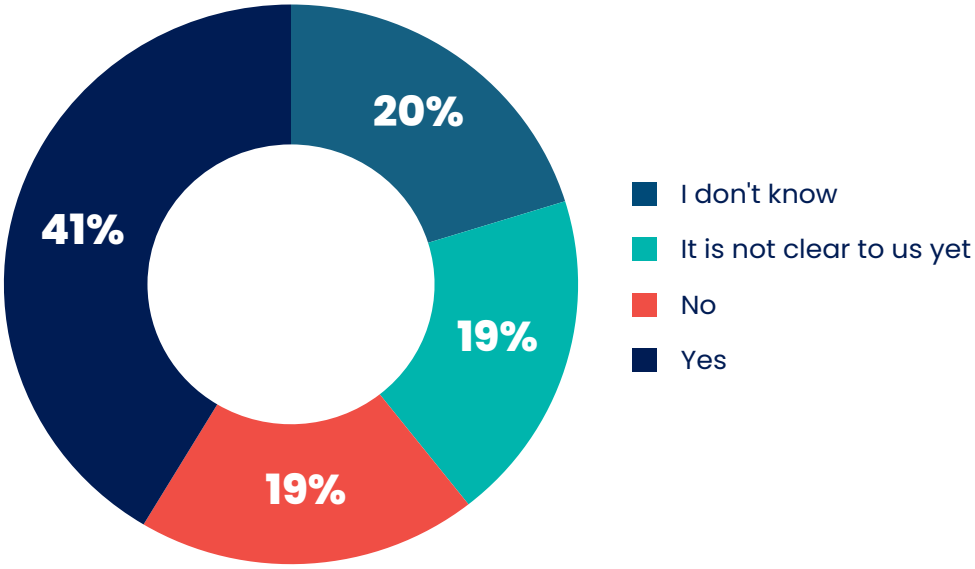
À partir de là, à l'instar de tous les autres États membres de l'UE, la Belgique a 21 mois – le délai court jusqu'en octobre 2024 – pour **transposer la directive en droit national.** Le Conseil des ministres l'a fait le **10 novembre 2023** et le parlement devrait approuver la loi en avril.

Selon les prévisions, à partir **d'octobre 2024**, NIS2 devrait également remplacer la directive NIS existante en Belgique. À partir de ce moment-là, toutes les entreprises et organisations concernées doivent être en conformité avec cette nouvelle réglementation. En cas d'incident cybernétique, votre entreprise pourrait en être tenue responsable et des sanctions pourraient être imposées.

> Octobre 2024 approche rapidement. J'encourage donc vivement chacun à ne pas attendre l'entrée en vigueur de la nouvelle loi et à commencer à remplir toutes ses obligations dès que possible.
>
> **Koen Tamsyn,**
> *Solution Manager*
> *Cybersecurity, Inetum*

Votre organisation est-elle concernée ?

Does your organisation need to comply with the NIS2 directive?
All marks (n=303)



La directive NIS2 s'applique-t-elle à votre organisation ? En 2023, 4 entreprises belges sur 10 (39 %) n'ont pas su répondre à cette question de l'enquête annuelle sur les priorités de Beltug. La moitié d'entre elles n'en avaient aucune idée, tandis que les autres trouvaient que le champ d'application de la directive n'était pas encore assez clair.

Vous pouvez déterminer si votre organisation est concernée à l'aune des critères suivants :

Critère 1 : secteur

La directive NIS2 s'applique à tous les secteurs qui étaient déjà couverts par la première directive NIS, mais aussi à plusieurs nouveaux secteurs, ce qui porte le total à **18 secteurs**. De ce fait, le nombre d'organisations couvertes par la directive augmente.

À cet égard, la directive NIS2 établit une distinction entre les secteurs **critiques** et les secteurs **hautement critiques** :

Secteurs Critiques

- Gestion des déchets
- Produits chimiques
- Fournisseurs numériques
- Denrées alimentaires
- Recherche
- Services postaux et d'expédition
- Fabrication

Secteurs Hautement Critiques

- Eaux usées
- Secteur bancaire
- Gestion des services TIC
- Infrastructure numérique
- Eau potable
- Énergie
- Santé
- Infrastructures des marchés financiers
- Administration publique
- Espace
- Transports

Critère 2 : taille et criticité

Une différence importante par rapport à la première directive NIS est que les organisations sont automatiquement couvertes par la directive NIS2 si elles sont actives dans l'un des secteurs ci-dessus et peuvent être qualifiées d'entité **« essentielle »** ou **« importante »**. Cette qualification dépend de facteurs comme le **secteur**, mais aussi la taille de l'entité – exprimée en chiffre d'affaires et en nombre de travailleurs – et la **criticité** de l'organisation.

Dans les **secteurs critiques**, aucune entreprise n'est essentielle, mais toutes sont **importantes**. Sont exceptées les entreprises qui emploient moins de 50 personnes à temps plein et réalisent un chiffre d'affaires inférieur à 10 millions d'euros : NIS2 ne s'applique pas à elles.

Il en va de même pour les entreprises des **secteurs hautement critiques**, qui comprennent des entités essentielles en plus des entités importantes. Par entités « essentielles », on entend pratiquement toutes les entités qui emploient plus de 250 personnes à temps plein, indépendamment de leur chiffre d'affaires, ainsi que certaines entités qui réalisent plus de 50 millions d'euros de chiffre d'affaires, quel que soit le nombre de personnes qu'elles emploient. La **directive est plus stricte** pour les entités « essentielles », car on considère qu'une perturbation de leurs services aurait un **impact beaucoup plus important** sur l'économie et la société qu'une perturbation des services d'une entité « importante ».

> Si votre organisation a moins de 50 collaborateurs, NIS2 ne s'applique pas à vous. Mais attention, si vous fournissez des services ou des produits critiques à des entreprises qui relèvent de NIS2, vous devrez leur prouver que vous menez vos activités dans le respect des règles de sécurité, le cas échéant avec un audit officiel. En effet, ces entreprises sont aussi responsables des risques liés à leur chaîne d'approvisionnement.
>
> **Arnaud Martin,**
> *Agoria*

Conformité à la directive NIS2 : qu'est-ce que cela signifie pour vous ?

Votre entreprise relève-t-elle de la directive NIS2 sur la base des critères énumérés ci-dessus ? Dans ce cas, vous avez deux exigences majeures à respecter.

Premièrement, vous devez **prendre des mesures pour maîtriser et limiter vos risques en matière de cybersécurité**. Il peut s'agir de mesures techniques, opérationnelles et organisationnelles. L'important est qu'elles soient appropriées et proportionnées. Concrètement, il s'agit d'interventions dans ces dix domaines :

1. Analyse et gestion des risques
2. Politique de sécurité et gestion des actifs
3. Gestion des incidents (prévention, détection et réaction aux incidents)
4. Continuité des activités et gestion des crises
5. Sécurité de la chaîne d'approvisionnement (prise en compte des vulnérabilités des fournisseurs)
6. Gestion et traitement des vulnérabilités
7. Évaluations régulières (assessments)
8. Utilisation du chiffrement le cas échéant
9. Cyberhygiène et la formation à la cybersécurité
10. Utilisation de solutions d'authentification à plusieurs facteurs (MFA) ou d'authentification continue

Deuxièmement, vous devez satisfaire à certaines obligations en matière d'alerte précoce. Les incidents majeurs doivent désormais être signalés sans délai – pour être précis : **dans les 24 heures** – au Centre de Réponse aux Incidents de Sécurité Informatique (CSIRT) ou à l'autorité compétente. Une notification d'incident plus détaillée doit suivre au bout de **trois jours (72 heures)** maximum. Enfin, au plus tard un mois après la notification de l'incident, vous devez présenter un rapport final avec les mesures d'atténuation appliquées et en cours.

> Posez-vous la question : quels sont mes risques actuels ? Et comment puis-je les ramener à un niveau acceptable ?
>
> **Koen Tamsyn,**
> *Solution Manager Cybersecurity, Inetum*

Besoin d'aide ?
Inetum est à vos côtés !

Votre organisation n'a pas l'expertise ou les moyens nécessaires en interne pour se mettre en conformité avec la directive NIS2, ou les adaptations requises entraînent une charge de travail (trop) importante ?

Chez Inetum, nous avons conscience de l'importance de respecter les cadres réglementaires comme la directive NIS2. Nous disposons en outre des **experts** et des **solutions** nécessaires pour vous soutenir et vous conseiller tout au long de votre parcours de conformité.

Conseils/consultance ad hoc

Faites appel à notre équipe de spécialistes en cybersécurité pour analyser et évaluer votre position actuelle en matière de sécurité. Sur la base de cette **évaluation préparatoire**, nous élaborerons ensuite un **plan de sécurité** adapté qui répond à vos besoins spécifiques.

Enfin, pour vous aider à vous conformer aux mesures de base imposées par la directive NIS2, nous vous proposons une vaste gamme d'outils et de services d'accompagnement, comme des **évaluations de risque**, des **procédures de sécurité** et des **plans de réponse aux incidents**.

> Nos services d'évaluation de la maturité des entreprises en matière de cybersécurité ne datent pas d'hier. Nous les avons récemment mis à niveau et adaptés aux exigences de la directive NIS2.
>
> **Koen Tamsyn,**
> *Solution Manager*
> *Cybersecurity, Inetum*

Feuille de route de cybersécurité

Avec notre feuille de route de cybersécurité, nous cartographions votre **maturité** en matière de cybersécurité en trois étapes et analysons vos **vulnérabilités** éventuelles, selon votre implémentation de la directive NIS2. Sur la base de cet instantané, nous formulons des **propositions d'optimisation concrètes**.

Notre feuille de route de cybersécurité se compose d'un volet technologique avec un **scan de données**, ainsi que d'un volet non technique qui s'articule autour d'un **questionnaire** à remplir lors d'un **atelier**.

Au cours de l'évaluation, nous parcourons ensemble ces **trois étapes** :

Étape 1 : préparation de votre évaluation

Au cours d'un entretien préparatoire avec un spécialiste en cybersécurité, nous faisons connaissance, discutons des **objectifs** de votre évaluation et partageons les **exigences système** avec vous. Ainsi, nous pourrons préparer au mieux votre environnement informatique à l'évaluation proprement dite.

Étape 2 : vos ressources IT : collecte et analyse des données

Nous installons un outil dans votre environnement informatique qui se connecte à diverses **plateformes**, tant au niveau **local** (Active Directory, SharePoint, DNS des e-mails, terminaux et serveurs) que dans le **cloud** (Azure, Microsoft 365, ...). Notre spécialiste en cybersécurité effectue alors les scans et les tests nécessaires pour collecter toutes les données pertinentes. Nous menons aussi un entretien avec votre CIO ou votre CISO sur la base d'un **questionnaire** standardisé, afin d'approfondir le positionnement de votre organisation en matière de cybersécurité.

Étape 3 : présentation de votre rapport final

Nous partageons avec vous les résultats, nos conclusions et nos recommandations lors d'une **présentation management**, que nous vous remettons avec le **rapport final** détaillé.

CISO as a service

La cybersécurité n'est pas un aspect statique, mais un **processus cyclique**. Il s'agit d'un chantier permanent qui consiste, d'une part, à aligner vos objectifs de sécurité sur vos objectifs d'entreprise généraux et vos stratégies de gestion des risques et, d'autre part, à vous maintenir en conformité avec les réglementations. La directive NIS2 n'est pas seulement une question de **solutions technologiques**, mais aussi **de politiques et de procédures**.

Pour réussir un audit NIS2, vous devez prévoir des politiques pour couvrir toute une panoplie de domaines : sécurité de l'information, contrôle des accès, réponse aux incidents, chiffrement des données, gestion des fournisseurs, classification et gestion des données, etc.

Vous n'avez pas besoin d'un CISO à temps plein ? Dans ce cas, nous vous présentons notre CISO-as-a-Service : un expert en sécurité qui remplit la fonction de CISO chez vous à temps partiel.

La sécurité ? Un travail d'équipe !

Votre entreprise relève de la directive NIS2 ou vous êtes un fournisseur important d'une entreprise concernée par NIS2 ? Dans ce cas, nous vous recommandons d'effectuer dès à présent une évaluation de cybersécurité et de réaliser une feuille de route de cybersécurité avec nous. Vous aurez ainsi le temps de prendre les mesures nécessaires pour poursuivre vos activités en toute sécurité, conformément à la nouvelle directive. Cette approche réfléchie et progressive vous permettra non seulement d'échelonner vos efforts, mais aussi vos coûts.

CONTACTEZ-NOUS

Inetum
A. Vaucampslaan 42
1654 Huizingen, Belgique
+32 2 801 55 55
www.inetum-realdolmen.world
info@inetum-realdolmen.world

inetum