17 Mar 2025 -06:02

Mobilisation pour la cybersécurité : 2 410 organisations dans les secteurs critiques belges améliorent leur protection

Depuis l'entrée en vigueur de la loi NIS2 en octobre de l'année passée, 2 410 organisations dans des secteurs critiques se sont enregistrées auprès du Centre pour la Cybersecurité Belgique (CCB). Une initiative de cybersécurité d'une ampleur sans précédent est en cours à travers le pays. Au cours de cette période, le nombre de cyberincidents signalés a augmenté de 80%.

La cybercriminalité devrait exploser dans les années à venir. La nouvelle directive européenne sur la sécurité des réseaux et de l'information (NIS2) vise à améliorer la cybersécurité et la résilience des services essentiels et clés dans des secteurs bien définis de l'UE.

La Belgique a été le premier État membre européen à mettre en œuvre intégralement la nouvelle directive NIS2. Les organisations belges soumises à NIS2 disposent jusqu'au 18 mars 2025 pour effectuer leur enregistrement réglementaire sur la plateforme dédiée atwork.safeonweb.be et mettre en œuvre des mesures de sécurité telles que la protection contre les cyberattaques et les violations de données.

Qui s'est déjà enregistré aujourd'hui?

Au total, plus de 4 500 organisations – tous secteurs confondus – se sont déjà enregistrées. Dans les secteurs critiques tels que l'énergie, le transport, les soins de santé, l'infrastructure numérique, le gouvernement, l'industrie manufacturière, etc., 2 410 organisations NIS2 se sont déjà enregistrées à ce jour.

Une estimation basée sur les chiffres du SPF Économie nous amène à un total d'environ 2 500 organisations dans le champ d'application du NIS2. Ce chiffre est susceptible d'évoluer dans le futur.

« *Nous nous attendons à ce que le nombre d'enregistrements d'entités NIS2 et de notifications d'incidents ou de cybermenaces augmente encore dans les mois à venir, avant de se stabiliser. Les organisations belges déploient des efforts considérables pour renforcer leur niveau de cybersécurité*. »

Augmentation du nombre de rapports d'incidents

Au cours des 18 derniers mois, le CCB a reçu un total de 556 notifications de cyberincidents. Entre les mois d'août 2023 et septembre 2024, nous avons reçu en moyenne 25 notifications par mois. Depuis l'entrée en vigueur de la loi NIS2 l'an dernier, il y a eu 226 incidents, soit une moyenne de 45 par mois. Cela représente une augmentation de 80% par rapport à la période précédente. Le nombre de notification d'incidents a augmenté en raison de la mise en œuvre de la loi NIS2. Rien n'indique en effet qu'il y ait davantage de cyberattaques visant les organisations belges.

« *Nous avons constaté que, par le passé, les organisations ne savaient pas comment s'y prendre ou n'estimaient pas nécessaire de notifier les incidents* », souligne Miguel De Bruycker. « *Il y a eu une sous-déclaration dans le passé. Le nombre de notifications d'incidents significatifs n'a pas augmenté en soi* ».

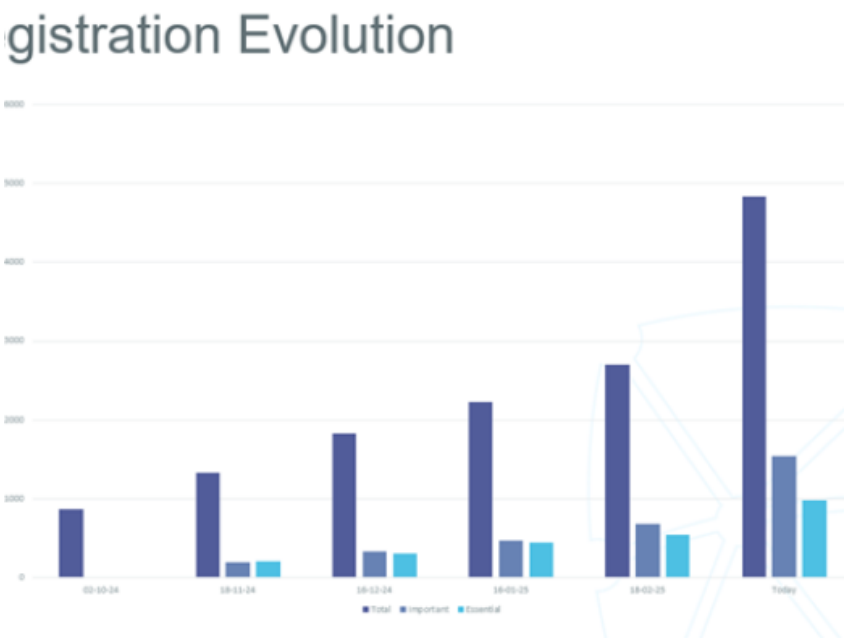
Une organisation enregistrée en vaut 2

Les entités NIS2 ne sont pas les seules à pouvoir s'enregistrer. L'enregistrement offre également de nombreux avantages à toutes les autres organisations.

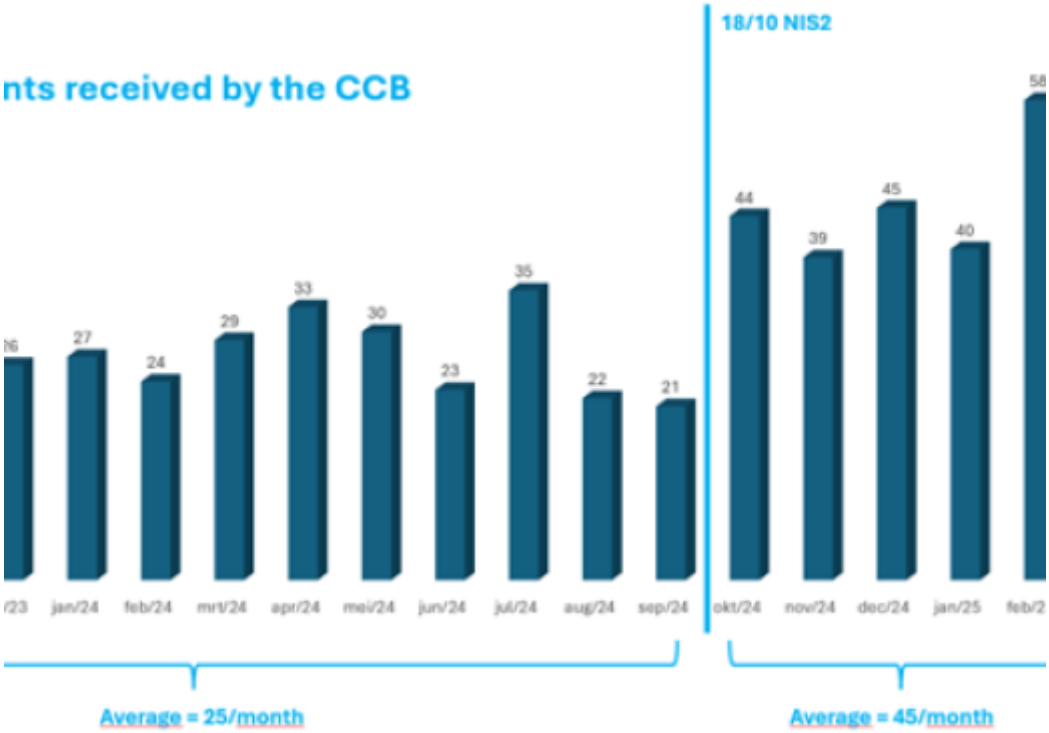
"*En février 2025, nous avons subi une cyberattaque et, grâce à notre enregistrement, nous avons pu compter sur une intervention rapide et efficace de la part de la BCC. Son utilité a été prouvée depuis. Les services supplémentaires sont également très utiles*", déclare Dirk Declerck, CEO du Port d'Ostende.

Les organisations enregistrées bénéficient d'un accès gratuit aux services suivants:

- Priorité : Après l'enregistrement, si une vulnérabilité est détectée sur un système associé à un nom de domaine ou une adresse IP enregistrés (grâce aux quelques données demandées au départ), le CCB peut alerter les organisations très rapidement. Toutefois, les organisations NIS2 ont la priorité sur les autres organisations.
- Alertes sur les cybermenaces: ce système aide les organisations à enquêter sur les cybermenaces potentielles sur leur réseau et à les atténuer en recevant des notifications sur les vulnérabilités et les infections.
- Rapport d'analyse rapide: les organisations peuvent recevoir un rapport qui donne un aperçu des faiblesses en matière de sécurité et des possibilités d'amélioration.
- Auto-évaluation: grâce à un bref questionnaire, les organisations peuvent identifier des faiblesses et recevoir des recommandations ciblées.
- Modèles de politique : des *policy templates* de cybersécurité prêtes à l'emploi.



Registration



Incidents

Centre pour la Cybersécurité Belgique
Rue de la Loi 18
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Michele Rignanese
Porte-parole(NL/FR/E)
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be

Katrien Eggers
Porte-parole(NL/FR/E)
+32 485 76 53 36
katrien.eggers@ccb.belgium.be