18 oct 2024 -03:00

La Belgique est le premier État membre de l'Union européenne à mettre complètement en œuvre les nouvelles règles en matière de cybersécurité (NIS2)

Les entreprises peuvent agir dès maintenant

La Belgique s'affirme comme pionnière européenne en matière de cybersécurité, devenant le premier État membre à mettre pleinement en œuvre la nouvelle législation NIS2. Cette avancée majeure va renforcer considérablement le niveau de cyber résilience d'un grand nombre d'entités actives dans notre pays. On estime à au moins 2.500 le nombre d'organisations belges concernées, lesquelles devront s'enregistrer sur le site atwork.safeonweb.be et mettre en œuvre les mesures requises. Ces entités détiennent désormais la clé pour propulser leur cybersécurité vers de nouveaux sommets.

Chaque jour, des organisations vulnérables sont victimes de cybercriminels qui exploitent habilement les failles de sécurité visibles ou l'absence de vérification en deux étapes (2FA), perpétrant ainsi des attaques par ransomware et des vols de données. La nouvelle directive européenne sur la sécurité des réseaux et de l'information (NIS2) vise à améliorer cette situation préoccupante. La directive a été conçue pour accroître la résilience des pays de l'UE face aux cybermenaces toujours plus sophistiquées et a été transposée en Belgique par la loi NIS2.

Impact positif sur la cybersécurité

"Environ 200 organisations se sont déjà enregistrées, mais nous anticipons une augmentation significative de ce nombre dans les semaines à venir", a déclaré Miguel De Bruycker, directeur général du Centre pour la Cybersécurité Belgique (CCB).

"La législation NIS2 étend les règles de cybersécurité existantes à un éventail plus large d'organisations et de secteurs. Les organisations concernées ne doivent toutefois pas considérer NIS2 comme un fardeau mais comme une opportunité de renforcer leur résilience", explique Valéry Vander Geeten, responsable juridique au Centre pour la Cybersécurité Belgique (CCB). "La législation établit une distinction entre des entités qualifiées d'essentielles ou d'importantes, en fonction de leur secteur d'activité et de leur taille".

Sauf exceptions, la loi NIS2 s'applique aux organisations d'une certaine taille qui sont établies en Belgique et qui fournissent dans l'Union européenne au moins un des services listés dans les annexes de la loi. Le critère de taille implique que l'entité doit compter un effectif d'au moins 50 travailleurs à temps plein ou un chiffre d'affaires annuel (ou un total de bilan annuel) supérieur à 10 millions d'euros. Le nombre de secteurs concernés connaît ainsi une expansion significative, passant de 7 à 18.

La notification des incidents et l'enregistrement sont les premières étapes

À partir du 18 octobre, les organisations ont l'obligation de signaler tous les incidents significatifs au CCB sans délai injustifié et au plus tard dans les 24 heures, puis de fournir une notification complémentaire dans les 72 heures et enfin de rédiger un rapport final dans les 30 jours.

Par ailleurs, toutes les entreprises et organisations concernées par NIS2 doivent impérativement s'inscrire sur le portail atwork.safeonweb.be par l'intermédiaire d'un représentant légal avant le 18 mars 2025.

L’enregistrement nécessite la fourniture d’informations sur l’organisation, incluant la personne de contact, le secteur d’activité et la taille de l’entité. Une fois l’enregistrement effectué, les entreprises bénéficieront d’un accès à des services supplémentaires conçus pour les aider à identifier et à atténuer les cybermenaces, adaptés spécifiquement au réseau et au domaine de chaque entreprise.

Le référentiel “CyberFondamentaux”: une approche étape par étape

Toutes les entités sont tenues de prendre les mesures nécessaires pour renforcer leur cybersécurité. Dans cette optique, le CCB a élaboré le référentiel des CyberFondamentaux. La CCB accompagne les organisations en mettant à leur disposition une évaluation des risques permettant à chaque organisation de déterminer le niveau approprié de CyberFondamentaux à mettre en place. Ce cadre innovant propose des mesures progressives, pour chaque niveau de sécurité, appuyant sur les normes internationales de cybersécurité et sur l’expérience acquise à travers l’analyse de milliers d’incidents.

La dernière pièce : la certification

“Les entités essentielles ont également l’obligation de se soumettre à des évaluations régulières basées sur les CyberFondamentaux ou la norme ISO 27001”, explique Johan Klykens, directeur de la certification au Centre pour la Cybersécurité Belgique (CCB). “Cette certification offre aux entreprises une méthode claire et tangible pour démontrer qu’elles ont pleinement assumé leurs responsabilités en matière de cybersécurité.”

Cependant, il est crucial de noter que lorsque les services informatiques sont externalisés, la responsabilité juridique incombe toujours à l’organisation elle-même. Il est donc essentiel d’exiger des garanties et des certificats auprès des fournisseurs, une démarche rendue possible grâce au référentiel des CyberFondamentaux. En outre, le CCB recommande vivement d’inclure les exigences de cybersécurité des principaux fournisseurs de services informatiques dans l’évaluation personnalisée de l’organisation.

Il va sans dire que le CCB encourage fortement les organisations non couvertes par la législation NIS2 à s’investir activement dans le renforcement de leur cybersécurité par le biais des CyberFondamentaux. Le fait qu’une organisation ne soit pas considérée comme une entité soumise à la loi NIS2 ne signifie pas qu’elle pourra ignorer les exigences de la loi. Dans la pratique, un grand nombre d’organisations devront s’y conformer car elles fournissent des services à des entités NIS2.

Toutes les ressources pour entreprendre cette démarche cruciale sont mises à di…

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