18 okt 2024 -03:00

België zet de standaard: eerste lidstaat die nieuwe Europese regels volledig invoert voor cyberveiligheid (NIS2)

Bedrijven kunnen nu echt aan de slag

België is de eerste Europese lidstaat die de nieuwe NIS2-wetgeving volledig uitvoert. Deze regels versterken aanzienlijk het niveau van cyberveiligheid. Naar schatting minstens 2.500 Belgische organisaties zijn vanaf vandaag verplicht om zich te registreren op de website atwork.safeonweb.be en om veiligheidsmaatregelen te nemen. Ze hebben hiermee de sleutel in handen om hun cyberveiligheid naar een hoger niveau te tillen.

Bij aanvallen met ransomware en datadiefstal worden kwetsbare organisaties dagelijks slachtoffer van cybercriminelen die inspelen op zichtbare veiligheidslekken of het ontbreken van tweestapsverificatie (2FA). De nieuwe Europese richtlijn voor Network en Information Security (NIS2) wil dit een halt toeroepen. Deze richtlijn is ontworpen om de weerbaarheid van EU-landen tegen cyberdreigingen te verhogen en werd in België omgezet in de NIS2-wet.

Positieve impact op cyberveiligheid

“Momenteel zijn er al een 200-tal organisaties bij ons geregistreerd, maar we verwachten dat dit de komende weken sterk zal stijgen”, vertelt Miguel De Bruycker, directeur-generaal van het Centrum voor Cybersecurity België (CCB).

“De NIS2-wetgeving breidt de bestaande cyberveiligheidsregels uit naar meer sectoren. Organisaties moeten NIS2 niet zien als een last, maar als een kans om hun veerkracht te versterken”, vertelt Valéry Vander Geeten, Head of Legal bij het Centrum voor Cybersecurity België (CCB). “De wetgeving maakt een onderscheid tussen belangrijke en essentiële organisaties, afhankelijk van sector en omvang.”

Op enkele uitzonderingen na is de wet NIS2 van toepassing op organisaties van een bepaalde omvang die in België zijn gevestigd en binnen de Europese Unie ten minste één van de in de bijlagen bij de wet genoemde diensten verlenen. Het groottecriterium houdt in dat de entiteit minstens 50 voltijdse werknemers moet hebben of een jaaromzet (of jaarlijks balanstotaal) van meer dan 10 miljoen euro. Het aantal betrokken sectoren is dus aanzienlijk toegenomen, van 7 naar 18.

Notificatie van incidenten en registratie zijn de eerste stappen

Organisaties moeten vanaf 18 oktober significante incidenten binnen 24 uur rapporteren aan het CCB, gevolgd door verdere informatie binnen 72 uur en een finaal rapport binnen 30 dagen.

Daarnaast moeten alle NIS2-bedrijven en organisaties zich voor 18 maart 2025 aanmelden op het portaal op atwork.safeonweb.be via een wettelijke vertegenwoordiger. De registratie vraagt om informatie over de organisatie, inclusief contactpersoon, sector en omvang. Na registratie krijgen bedrijven toegang tot aanvullende diensten om te helpen bij het identificeren en beperken van cyberbedreigingen op maat van het netwerk en domein van elk bedrijf.

CyberFundamentals framework: een stap voor stap aanpak

Alle entiteiten moeten de nodige maatregelen nemen om hun cyberbeveiliging te verhogen. Het CCB heeft hiervoor het CyberFundamentals framework ter beschikking gesteld. Het CCB ondersteunt organisaties met een risicobeoordeling, waarmee elke organisatie het juiste niveau van CyberFundamentals kan bepalen. Dit innovatief kader bevat per veiligheidsniveau stapsgewijs bijkomende maatregelen, gebaseerd op internationale cybersecuritynormen en inzichten volgens de ervaring bij duizenden incidenten.

Het sluitstuk: certificering

“Essentiële entiteiten moeten daarnaast regelmatig een beoordeling ondergaan, gebaseerd op de CyberFundamentals of de norm ISO 27001” vertelt Johan Klykens, Directeur Certificatie bij het Centrum voor Cybersecurity België (CCB). “Deze certificering biedt bedrijven een heldere methode om aan te tonen dat zij hun verantwoordelijkheden betreffende cyberveiligheid genomen hebben.“

In gevallen waarbij IT-diensten worden uitbesteed, blijft de wettelijke verantwoordelijkheid echter bij de organisatie zelf. Het is cruciaal om aan leveranciers garanties en certificaten te vragen, wat via het kader van CyberFundamentals mogelijk is. Bovendien raadt het CCB aan om de cybersecurity-eisen van de belangrijkste ICT-leveranciers op te nemen in de beoordeling op maat van de organisatie.

Het spreekt voor zich dat het CCB alle organisaties, die niet onder de NIS2-wetgeving vallen, aanmoedigt om te werken aan cyberbeveiliging via de CyberFundamentals. Het feit dat een organisatie niet wordt beschouwd als een entiteit die onder de NIS2-wetgeving valt, betekent niet dat zij de vereisten van de wetgeving kan negeren. In de praktijk zal een groot aantal organisaties aan de eisen moeten voldoen omdat ze diensten verlenen aan NIS2-entiteiten.

Alle hulpmiddelen staan hier ter beschikking

Centrum voor Cyber Security België
Wetstraat 18
1000 Brussel
België
http://www.ccb.belgium.be

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

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