BarentsKrans

Navigeren door NIS2
Toename van cyberbeveiliging en risicobeheer

De richtlijn inzake netwerk- en informatiebeveiliging (NIS2) heeft tot doel de cyberbeveiliging en veerkracht van essentiële diensten in de EU-lidstaten te verbeteren. NIS2 breidt het toepassingsgebied van de huidige NIS-richtlijn aanzienlijk uit door meer sectoren te bestrijken. De richtlijn bevat ook strengere en uitgebreidere beveiligingsnormen en eisen voor het melden van incidenten.

Marc Elshof
advocaat | partner

T: +31 70 376 06 87
M: +31 6 46 376 108
marc.elshof@barentskrans.nl

Sectoren onder NIS2

De uiterste datum voor EU-lidstaten om de NIS2 om te zetten in nationale wetgeving is 17 oktober 2024. De NIS2 is van toepassing op entiteiten die kunnen worden aangemerkt als een **Essentiële Entiteit** of een **Belangrijke Entiteit**.

Essentiële Entiteiten

- Entiteiten (inclusief gelieerde ondernemingen) met meer dan 250 werknemers of een jaaromzet van meer dan 50 miljoen euro en een jaarbalans van meer dan 43 miljoen euro, die actief zijn in een van de onderstaande sectoren:
  - Energie
  - Transport
  - Bankwezen
  - Infrastructuur financiële markt
  - Gezondheidzorg
  - Drinkwater en afvalwater
  - Digitale infrastructuur
  - ICT-dienstenbeheer (B2B)
  - Overheidsdiensten
  - Ruimtevaart
- Gekwalificeerde aanbieders van vertrouwensdiensten, registers van topleveldomeinnamen en DNS-dienstverleners
- Middelgrote aanbieders van openbare elektronische communicatienetwerken of van openbare elektronische communicatiediensten
- Overheidsinstanties
- Exploitanten van essentiële diensten, zoals aangewezen door een EU-lidstaat
- Bedrijven die zijn geïdentificeerd als kritieke entiteiten volgens de Richtlijn kritieke entiteiten
- Bedrijven die door een EU-lidstaat als essentiële entiteiten zijn aangemerkt

Belangrijke Entiteiten

- Entiteiten, niet zijnde Essentiele Entiteiten, die actief zijn in een van de onderstaande sectoren:
  - Energie
  - Transport
  - Bankwezen
  - Infrastructuur financiële markt
  - Gezondheidzorg
  - Drinkwater en afvalwater
  - Digitale infrastructuur
  - ICT-dienstenbeheer (B2B)
  - Overheidsdiensten
  - Ruimtevaart
  - Post- en koeriersdiensten
  - Afvalbeheer
  - Chemische stoffen
  - Levensmiddelen
  - Productie van medische, machine-, computer-, transport-, en motorvoertuigen
  - Online marktplaatsen, online zoekmachines en sociale netwerkdiensten
  - Onderzoek

Verplichtingen onder de NIS2

Bestuursorganen

De bestuursorganen van Essentiële en Belangrijke Entiteiten moeten de door die entiteiten genomen maatregelen voor het beheer van cyberrisico's goedkeuren en toezicht houden op de uitvoering ervan. Leden van de bestuursorganen kunnen persoonlijk aansprakelijk worden gesteld voor inbreuken.

De leden van de bestuursorganen van Essentiële en Belangrijke Entiteiten zijn verplicht om een opleiding te volgen en moeten deze entiteiten aanmoedigen om hun werknemers regelmatig soortgelijke opleidingen aan te bieden. Het doel is dat werknemers voldoende kennis en vaardigheden verwerven om risico's te identificeren en cyberbeveiliging risicomanagement paktijken te beoordelen, evenals hun impact op de diensten die door de entiteit worden geleverd.

Technische, operationele en organisatorische maatregelen

Essentiële en Belangrijke Entiteiten moeten passende en evenredige technische, operationele en organisatorische maatregelen nemen om risico's te beheren en de impact van incidenten te voorkomen of te minimaliseren. Deze maatregelen omvatten ten minste:

- Beleid inzake risicoanalyse en beveiliging van informatiesystemen;
- Incidentafhandeling;
- Bedrijfscontinuïteit;
- Beveiliging van de toeleveringsketen, rekening houdend met de kwetsbaarheden die specifiek zijn voor elke directe leverancier en dienstverlener en de algemene kwaliteit van producten en cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, inclusief hun veilige ontwikkelingsprocedures;
- Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de behandeling en openbaarmaking van kwetsbaarheden;
- Beleid/procedures om de effectiviteit van cyberbeveiliging te beoordelen;
- Basis cyberhygiënepraktijken en cyberbeveiligingstraining;
- Beleid en procedures voor cryptografie en versleuteling;
- Personeelsbeveiliging, toegangscontrolebeleid en activabeheer; en
- Gebruik van multi-factor authenticatie of oplossingen voor continue authenticatie.

Kennisgevingsverplichtingen

Essentiële en Belangrijke Entiteiten moeten de bevoegde nationale autoriteit op de hoogte stellen van elk incident dat een aanzienlijke impact heeft op de levering van hun diensten. Een incident is belangrijk als:

- Het ernstige operationele verstoring van de dienstverlening of financieel verlies voor de betrokken entiteit heeft veroorzaakt of kan veroorzaken; of
- Het andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

Essentiële en Belangrijke Entiteiten moeten bevoegde nationale instantie op de hoogte brengen van een belangrijk incident:

- Binnen 24 uur nadat ze op de hoogte zijn van het incident, inclusief of het significante incident vermoedelijk is veroorzaakt door onwettige of kwaadwillige handelingen of een grensoverschrijdend effect kan hebben;
- Binnen 72 uur na kennisname van het incident, met inbegrip van een update van de initiële waarschuwing en een initiële beoordeling van de ernst, de impact en de indicatoren van de aantasting; en
- Binnen een maand na de bijgewerkte kennisgeving een eindverslag. Dit verslag moet een beschrijving bevatten van het incident, het type bedreiging en de hoofdoorzaak, de genomen maatregelen en of het ernstige incident een grensoverschrijdend effect heeft.

Vertegenwoordiger

DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten aanbieden, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, die niet in de EU zijn gevestigd maar diensten aanbieden in de EU, moeten een vertegenwoordiger in de EU aanwijzen. De vertegenwoordiger moet gevestigd zijn in een van de EU-lidstaten waar de diensten worden aangeboden

SANCTIES

Niet-monetaire sancties

NIS2 geeft nationale toezichthoudende autoriteiten verschillende handhavingsbevoegdheden, waaronder:

- Nalevingsbevelen;
- Bindende instructies;
- Bevelen tot het uitvoeren van beveiligingsaudits;
- Bevelen tot kennisgeving van bedreigingen aan klanten van entiteiten.

Administratieve boetes

Voor Essentiële Entiteiten

- Anticiperend en reactief toezicht door nationale toezichthoudende autoriteiten;
- Administratieve boetes van maximaal € 10.000.000, of 2% van de totale wereldwijde jaaromzet, afhankelijk van welk bedrag hoger is.

Voor Belangrijke Entiteiten

- Reactief toezicht door nationale toezichthoudende autoriteiten;
- Administratieve boetes van maximaal € 7.000.000, of 1,4% van de totale wereldwijde jaaromzet, afhankelijk van welk bedrag hoger is.