NIS2-Richtlijn

Cyberbeveiligingswet

De NIS2-richtlijn is gericht op essentiële organisaties en sectoren waarvan de uitval van diensten kan leiden tot verstoringen in de samenleving en de economie.

Valt uw organisatie onder de Cyberbeveiligingswet?

De sector waarin een organisatie actief is en de omvang van de organisatie bepalen of deze onder de NIS2-richtlijn en de Cyberbeveiligingswet valt. De grootte van een organisatie wordt vastgesteld aan de hand van twee categorieën, waarvoor de volgende criteria zijn gedefinieerd:

Grote organisaties

Minimaal **250** medewerkers in dienst

Jaaromzet van minimaal **50** miljoen euro of een balanstotaal van minimaal **43** miljoen euro

Middelgrote organisaties

Minimaal **50** medewerkers in dienst

Jaaromzet van minimaal **10** miljoen euro of een balanstotaal van minimaal **10** miljoen euro

Voor welke sectoren geldt de NIS2?

Zeer kritieke sectoren

- Energie ⚡
- Transport 🚚
- Bankwezen 🏦
- Infrastructuur financiële markt 💳
- Gezondheidszorg ⛑️
- Drinkwater 🚰
- Digitale infrastructuur 💻
- Beheerders van ICT-diensten 👷
- Afvalwater 💧
- Overheids-diensten 🏛️
- Lokale overheden 🏢
- Ruimtevaart 🚀

Zeer kritieke sectoren

- Digitale aanbieders 🖥️
- Post- en koeriersdiensten ✉️
- Afvalstoffenbeheer ♻️
- Levensmiddelen 📦
- Chemische stoffen 🧪
- Onderzoek 🔬
- Vervaardiging 🏭

Hoe wordt er toezicht gehouden?

Voor belangrijke entiteiten geldt dat toezicht achteraf plaatsvindt, bijvoorbeeld als er aanwijzingen zijn voor het niet naleven van de wet, of als er een incident heeft plaatsgevonden. In alle gevallen kan de toezichthouder **beveiligingsaudits en –scans** uitvoeren en informatie verzoeken die nodig is om de risicobeheer maatregelen van de betrokken entiteit te beoordelen.

Wat zijn de consequenties voor mijn bedrijf?

Als je de richtlijn niet juist naleeft

Sancties en Boetes: Financiële straffen voor overtredingen.

Reputatieschade: Verlies van vertrouwen bij klanten en partners.

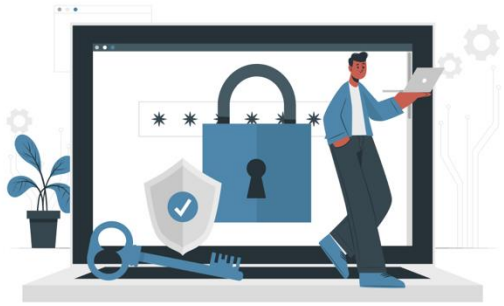
Verlies van Toegang tot Diensten: Mogelijke uitsluiting van bepaalde diensten.

Juridische Gevolgen: Risico op rechtszaken en juridische procedures.

Verhoogde Risico's: Groter risico op cyberincidenten en datalekken.

Toezicht en Controle: Verhoogd toezicht door autoriteiten.

Overzicht NIS2-Richtlijn



Wat betekent de Cyberbeveiligingswet voor uw organisatie?

Wat nu?

AEGIS To the rescue!

AEGIS biedt verschillende oplossingen om u van alle zorgen rondom deze wet te verlossen.
Wij hebben 3 pakketten samengesteld, waardoor elk bedrijf een frisse en passende oplossing kan vinden voor hun problemen.
Twijfelt u na het lezen nog of uw organisatie behoefte heeft aan extra hulp bij het naleven van de NIS2? Doe de quiz op onze website!

Registratieplicht

Organisaties zijn wettelijk verplicht zich te registreren in het entiteitenregister. Het Nationaal Cyber Security Centrum (NCSC) heeft een online registratievoorziening ontwikkeld waarmee organisaties zichzelf kunnen registreren en aanmelden. Sinds 17 oktober 2024 is het mogelijk om zich vrijwillig aan te melden via een webformulier op www.ncsc.nl. Aangezien alle lidstaten over een register moeten beschikken, biedt dit ook een Europees overzicht van het aantal entiteiten dat onder de NIS2-richtlijn valt.

Zorgplicht

De Cyberbeveiligingswet legt een zorgplicht op aanorganisaties, waardoor zij verplicht zijn om zelf een risicoanalyse uit te voeren. Op basis van deze analyse moeten zij passende en evenredige maatregelen nemen om de beveiliging van hun netwerk- en informatiesystemen te waarborgen. De bestuursleden van de entiteiten zijn verantwoordelijk voor het goedkeuren van deze maatregelen en het toezicht houden op de uitvoering ervan. Om deze taken effectief te kunnen vervullen, is het noodzakelijk dat zij een opleiding volgen.

Meldplicht

De richtlijn vereist dat NIS2-organisaties significante incidenten melden bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder. Er is een gefaseerde meldplicht van toepassing.

De eerste melding, een vroegtijdige waarschuwing, moet binnen 24 uur na de ontdekking van het incident plaatsvinden. Dit betreft incidenten die de continuïteit van de diensten van de organisatie aanzienlijk kunnen verstoren.
CSIRTs kunnen vervolgens ondersteuning en bijstand bieden. De criteria voor wat als een significant incident wordt beschouwd, worden nog verder uitgewerkt.

Factoren die bijdragen aan de significantie van een incident zijn onder andere de omvang van de financiële verliezen voor betrokkenen en/of de (operationele) schade die aan
andere entiteiten wordt toegebracht.

Voor het indienen van meldingen heeft het NCSC een centraal meldpunt opgezet. Het Meldportaal, dat is ingericht voor significante meldingen, kan ook worden gebruikt voor het vrijwillig melden van niet-significante incidenten of bijna-incidenten.