DE NIEUWE NIS2 WETGEVING

Wat je moet weten

Op 9 mei 2018 werd de eerste NIS wetgeving aangenomen. Deze wetgeving beoogt een hoog niveau van cybersecurity te waarborgen in alle lidstaten van de Europese Unie [EU]. Deze wetgeving wordt nu uitgebreid met NIS2, waardoor meer bedrijven in aanraking komen met de wetgeving en bijbehorende verplichtingen. In deze whitepaper zullen we bespreken wat de wetgeving inhoudt én wat dit betekent voor bedrijven binnen de EU.

WAT IS NIS2?

Network and Information Systems Directive 2 [NIS2] is de tweede Europese richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Europese Unie. Het is een wetgevingskader dat tot doel heeft de cybersecurity te verbeteren door het verplicht stellen van beveiligingsmaatregelen voor exploitanten van essentiële diensten en digitale dienstverleners.

SCOPE

Eén van de belangrijkste veranderingen in de NIS2 wetgeving is de uitbreiding van het toepassingsgebied. De oorspronkelijke richtlijn gold alleen voor aanbieders van essentiële diensten en digitale dienstverleners. Met de NIS2 wetgeving worden ook andere bedrijven en organisaties opgenomen.

De sectoren in de tabel hiernaast zijn opgenomen in de nieuwe wetgeving omdat zij een belangrijke rol spelen in de [digitale] economie en dus een potentieel doelwit zijn voor cyberaanvallen. Hierdoor moeten zij voldoen aan de verplichtingen die behoren tot de NIS2 wetgeving.

SECTOREN DEEL I	SECTOREN DEEL II
Energie	Digitale aanbieders
Transport	Post- en koeriersdiensten
Bankwezen	Afvalstoffenbeheer
Infrastructuur financiële markt	Levensmiddelen
Gezondheidszorg	Chemische stoffen
Drinkwater	Onderzoek
Digitale infrastructuur	Vervaardiging / manufacturing
Beheerders ICT-diensten	
Afvalwater	
Overheidsdiensten	
Ruimtevaart	

ESSENTIËLE ORGANISATIES

Dit zijn grote organisaties die actief zijn in een sector uit deel I [zie tabel] van de NIS2-richtlijn. Een organisatie is groot op basis van de volgende criteria:

- Minimaal 250 werknemers of;
- een jaaromzet van meer dan €50 miljoen en een balanstotaal van meer dan €43 miljoen.

BELANGRIJKE ORGANISATIES

Dit zijn middelgrote organisaties die actief zijn in een sector uit deel I [zie tabel] en middelgrote en grote organisaties die actief zijn in een sector uit deel II [zie tabel]. Een organisatie is middelgroot op basis van de volgende criteria:

- Minimaal 50 werknemers of;
- een jaaromzet en balanstotaal van meer dan €10 miljoen.

CUBICS

VERPLICHTINGEN

Bedrijven en organisaties die onder het nieuwe toepassingsgebied van de NIS2 wetgeving vallen, hebben verschillende verplichtingen die ze moeten nakomen. Het naleven hiervan moet leiden tot een verbeterde cybersecurity in de EU. Enkele van de belangrijkste verplichtingen zijn:

ZORGPLICHT

Om te voldoen aan de zorgplicht moeten bedrijven beveiligingsmaatregelen implementeren om hun netwerken en informatiesystemen te beschermen tegen cyberaanvallen. Dit gaat om bijvoorbeeld het implementeren van toegangscontroles, het monitoren van netwerken en systemen, het uitvoeren van regelmatige audits en het toepassen van encryptie.

MELDPLICHT

Bedrijven moeten incidenten met betrekking tot hun netwerken en informatiesystemen melden aan de bevoegde nationale autoriteiten. Hierbij gaat het om incidenten als datalekken en cyberaanvallen die een negatief effect kunnen hebben op de beschikbaarheid, integriteit of vertrouwelijkheid van de betrokken systemen en gegevens.

RAPPORTEREN

Bedrijven moeten regelmatig rapporteren over beveiligingsincidenten en de genomen beveiligings-maatregelen aan de bevoegde nationale autoriteiten. Hierbij moeten ze rapporteren over de omvang en aard van de incidenten, de genomen maatregelen en de evaluatie van de effectiviteit van deze maatregelen.

RISICOANALYSE

Het is vereist om regelmatig risicoanalyses uit te voeren. Dit moeten bedrijven doen door onder andere het identificeren van mogelijke risico's, het evalueren van de potentiële impact hiervan en het implementeren van maatregelen om deze te verminderen.

SAMENWERKEN

Het is verplicht om samen te werken met andere lidstaten om de cybersecurity te verbeteren en om incidenten en dreigingen te bestrijden die een grensoverschrijdend effect hebben.

Het is belangrijk dat bedrijven die onder het nieuwe toepassings-gebied van de NIS2 wetgeving vallen, zich bewust zijn van deze verplichtingen en dat ze actief werken aan het verbeteren van de cybersecurity van hun netwerken en informatiesystemen.

CUBICS

WAT NU?

Wat je nu al kunt doen om te voldoen aan de wetgeving.

INCIDENT RESPONSE PLAN

Bedrijven moeten een duidelijk Incident Respons Plan implementeren dat beschrijft hoe te handelen bij een cyberaanval of ander beveiligingsincident. Het plan moet onder andere procedures bevatten voor het melden van incidenten aan de autoriteiten en relaties, het herstellen van systemen en gegevens en het uitvoeren van een grondige evaluatie van het incident om te voorkomen dat dit in de toekomst opnieuw gebeurt.

RISICOANALYSES

Bedrijven en organisaties die onder het nieuwe toepassingsgebied van de NIS2 wetgeving vallen, moeten zorgen voor compliance met de wetgeving en de vereisten van de autoriteiten van de lidstaat waarin zij actief zijn. Dit kan betekenen dat er aanvullende beveiligingsmaatregelen moeten worden genomen en dat er regelmatige risicoanalyses moeten worden uitgevoerd.

KENNIS DELEN

Bedrijven moeten samenwerken met andere partijen binnen hun sector en met de autoriteiten om de cybersecurity te verbeteren en te zorgen voor een gezamenlijke aanpak bij incidenten en dreigingen. Dit kan bijvoorbeeld gebeuren door het delen van kennis en informatie over bedreigingen en kwetsbaarheden, het uitvoeren van gezamenlijke risicoanalyses en het gezamenlijk uitvoeren van incidentrespons.

SECURITY AWARENESS

Het is cruciaal om medewerkers te trainen en bewust [aware] te maken van de NIS2 wetgeving en de vereisten voor cybersecurity. Dit kan helpen om te voorkomen dat medewerkers onbedoeld kwetsbaarheden creëren in het systeem en kan helpen bij het tijdig signaleren van beveiligingsincidenten.

WORD NIS2 COMPLIANT MET NIS2 DESK

De NIS2 wetgeving die vanaf oktober 2024 gaat gelden brengt nieuwe verantwoordelijkheden en eisen met zich mee op het gebied van de cyberweerbaarheid van jouw organisatie. Onze NIS2 Desk service zorgt ervoor dat alle benodigde documentatie op één centrale plek staat.

013 750 76 00

verkoopit@cubics.nl

Klik hier!

CUBICS

SCAN DE QR EN LEES ALLES OVER ONZE DIENST!