



Solution Brief

Insight NIS2 Assessment Service

Bent u klaar voor de nieuwe richtlijn voor netwerkinformatiebeveiliging (NIS2)?

Achtergrond

De nieuwe richtlijn NIS2 treedt op 18 oktober 2024 in werking en is bedoeld om de veerkracht en beveiliging van de netwerk- en informatiesystemen binnen de EU te verbeteren. Het heeft de breedte en diepte van de oorspronkelijke richtlijn uitgebreid met uitgebreidere beveiligingscontroles, strengere vereisten voor het melden van incidenten en meer handhavingsmaatregelen met sancties.

De lijst van sectoren in scope is toegenomen en er wordt een onderscheid gemaakt tussen essentiële en belangrijke bedrijven.

De sectoren NIS2 zijn van toepassing op

Essentiële sectoren		Belangrijke sectoren	
	Energie-		Koeriersdiensten
	Transport		Afvalverwerking
	Bankwezen		Chemische stoffen
	Financiële marktinfrastructuur		Voedsel
	Gezondheidssector		Productie van medische devices
	Drinkwater		Digitale Providers
	Afvalwaterverwerking		Onderzoeksorganisaties
	Digitale infrastructuur	<p>Essentiële sectoren Grote bedrijven met 250 of meer werknemers, 50 miljoen euro aan jaaropbrengsten en/of totaal saldo van 43 miljoen euro of meer.</p> <p>Essentiële/belangrijke sectoren Middelgrote bedrijven met 50 of meer werknemers, een jaaromzet van 10 miljoen euro en/of een totaal saldo van 43 miljoen euro of meer aan assets.</p>	
	Service management		
	Openbaar bestuur		
	Ruimte		

Hoe Insight kan helpen

Insight kan u helpen om u voor te bereiden op en klaar te zijn om te voldoen aan de nieuwe NIS2-richtlijn door uw huidige situatie te beoordelen en eventuele hiaten en verbeteringen te identificeren die aan te pakken zijn om compliance te bereiken.

Aandachtspunten

- Risicoanalyse
- Zakelijke continuïteit
- Beveiliging van de supply chain
- Beveiliging van netwerkinformatiesystemen
- Incidentmanagement
- Doelmatigheid
- Human Factors
- Cryptografie en encryptie
- Fysieke beveiliging
- Multi-Factor-authenticatie

Onze oplossing

De security- en compliance-specialisten van Insight geven een assessment op basis van de Europese NIS2-richtlijnen.

Het National Cyber Security Centre (NCSC) heeft 14 high-level beveiligingsprincipes gepubliceerd die moeten worden geïmplementeerd in de vorm van het Cyber Assessment Framework (CAF).

Beveiligingsrisico's beheren	<ul style="list-style-type: none">▪ Governance▪ Risico-management▪ Access Management▪ Supply chain
Bescherming tegen cyberaanvallen	<ul style="list-style-type: none">▪ Beleid en procedures voor de bescherming van diensten▪ Identiteits- en toegangscontrole▪ Gegevensbeveiliging▪ Systeembeveiliging▪ Robuuste netwerken en systemen▪ Bewustwording en opleiding van personeel
Cyberbeveiligingsgebeurtenissen detecteren	<ul style="list-style-type: none">▪ Reactie- en herstelplanning▪ Verbetering
De impact van cyberbeveiligingsincidenten minimaliseren	<ul style="list-style-type: none">▪ Response and recovery planning▪ Improvements

Onze assessment omvat de volgende elementen

- **Kick-offgesprek: doelen en activiteitenplan** bepalen
- **Assessment:** documentatieanalyse en reeks interviews
- **Workshop:** om bevindingen en mogelijke verbeterpunten te bespreken
- **Documentatie NIS2-assessment:** Gedetailleerd rapport en volgende stappen.

Insight kan dan aanvullende diensten leveren ter ondersteuning bij het corrigeren en nakomen van uw verplichtingen en het verbeteren van uw beveiliging om NIS2-compliance te bereiken.

Ga naar nl.insight.com en kom in contact met uw Insight-accountmanager voor extra resources en ondersteuning.

Over Insight

Bij Insight hebben we de expertise, vaardigheden, tools, processen en ervaring om u te begeleiden bij het realiseren van uw volledige potentieel en het optimaliseren van uw concurrentievoordeel.

					
Wereldwijde schaal en dekking	Operational Excellence en systemen	Next-generation technische vaardigheden	Een gecertificeerde en bekroonde partner van grote aanbieders van beveiligingsoplossingen	Begrip van ISO 270001	Brede beveiligingsmogelijkheden

Neem contact op met uw Insight-accountmanager voor meer informatie.

055 53823 20 | nl.solutions@insight.com | nl.insight.com

Insight 