Cyberbeveiligingswet/

NIS2

Wat betekenen de ***10 zorgplicht-maatregelen*** voor uw organisatie?

kiwa

Cyberbeveiligingswet/ ***NIS2***

Wat betekenen de 10 zorgplichtmaatregelen van de Cyberbeveiligingswet/ NIS2 voor uw organisatie?

De Europese NIS2-richtlijn (Network and Information Security Directive) en de aankomende Nederlandse Cyberbeveiligingswet hebben als doel om cyberrisico's tegen te gaan. De richtlijn kent 4 hoofdverplichtingen en 10 zorgplichtvereisten waar veel bedrijven en organisaties in kritieke sectoren verplicht aan moeten gaan voldoen.

Wat zijn deze 10 zorgplichtmaatregelen, hoe hangen ze samen en hoe helpen deze maatregelen om de cyberweerbaarheid van uw organisatie te vergroten?

Ontdek:

1. Wat zijn de 4 hoofdverplichtingen en 10 zorgplichtmaatregelen van de NIS2?
2. De maatregelen rondom het CSMS (Cyber Security Management Systeem)/ ISMS (Information Security Management System)
3. Hoe borgt u de cybersecurity van uw supply chain?
4. Welke maatregelen zorgen voor cyber resilience?
5. De maatregelen voor secure development & systems

'Informatiebeveiliging is een must voor iedere organisatie, ongeacht de sector of de grootte van de organisatie. Of het nu gaat om je IT-systemen, OT-machines of IoT-apparaten, één zwakke schakel kan grote gevolgen hebben.'

Marjolein Veenstra,
Schemamanager / Team lead bij Kiwa

1. Wat zijn ***de 10 zorgplichtmaatregelen*** van de NIS2?

De Cyberbeveiligingswet is de Nederlandse toepassing van de Europese NIS2-richtlijn (Network and Information Security Directive). De precieze details van de Nederlandse wet zijn nog in ontwikkeling, de overheid geeft aan dat de verwachting is dat de Cyberbeveiligingswet in het najaar van 2025 in werking zal treden. Maar de NIS2 is al in werking. Het is dan ook verstandig om nu al aan de slag te gaan met de vereisten en u zo voor te bereiden op de Cyberbeveiligingswet. Wat zijn de 4 hoofdverplichtingen en de 10 zorgplichtmaatregelen precies en hoe hangen ze samen?

De 4 verplichtingen

Laten we eerst kijken hoe de maatregelen met elkaar samenhangen. De Cyberbeveiligingswet bestaat uit 4 belangrijke verplichtingen. Je ziet ze hiernaast.

1

Registratieplicht

Bedrijven die essentiële diensten leveren, moeten zich verplicht registreren bij de overheid: dit doet u bij het Nationaal Cyber Security Centrum (NCSC). Zo weet de overheid wie er onder de wet valt en wie niet.

2

Meldplicht

Als er een cyberincident plaatsvindt, moet dit meteen gemeld worden. Zo kunnen problemen sneller worden opgelost en worden andere bedrijven gewaarschuwd.

3

Zorgplicht

Bedrijven moeten hun beveiliging op orde hebben. Denk aan het nemen van de juiste technische en organisatorische maatregelen om hacks en datalekken te voorkomen. Hieronder vallen de 10 zorgplichtmaatregelen, aangevuld met governance.

4

Toezicht

De overheid houdt een oogje in het zeil. De toezichthouder kan controleren of bedrijven zich aan de regels houden en boetes uitdelen als dat niet zo is.

De 10 zorgplicht-maatregelen

Rondom de zorgplicht heeft de overheid 10 maatregelen gedefinieerd die bedrijven minimaal moeten nemen om zich tegen incidenten te beschermen. Dit worden vaak de NIS2-maatregelen genoemd. Deze 10 zorgplichtmaatregelen zijn:

1. Een risicoanalyse en beveiliging van informatiesystemen

2. Incidentenbehandeling

3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen

4. Beveiliging van de toeleverancierskеten

5. Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden

6. Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen

7. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging

8. Beleid en procedures over het gebruik van cryptografie en encryptie

9. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets

10. Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen

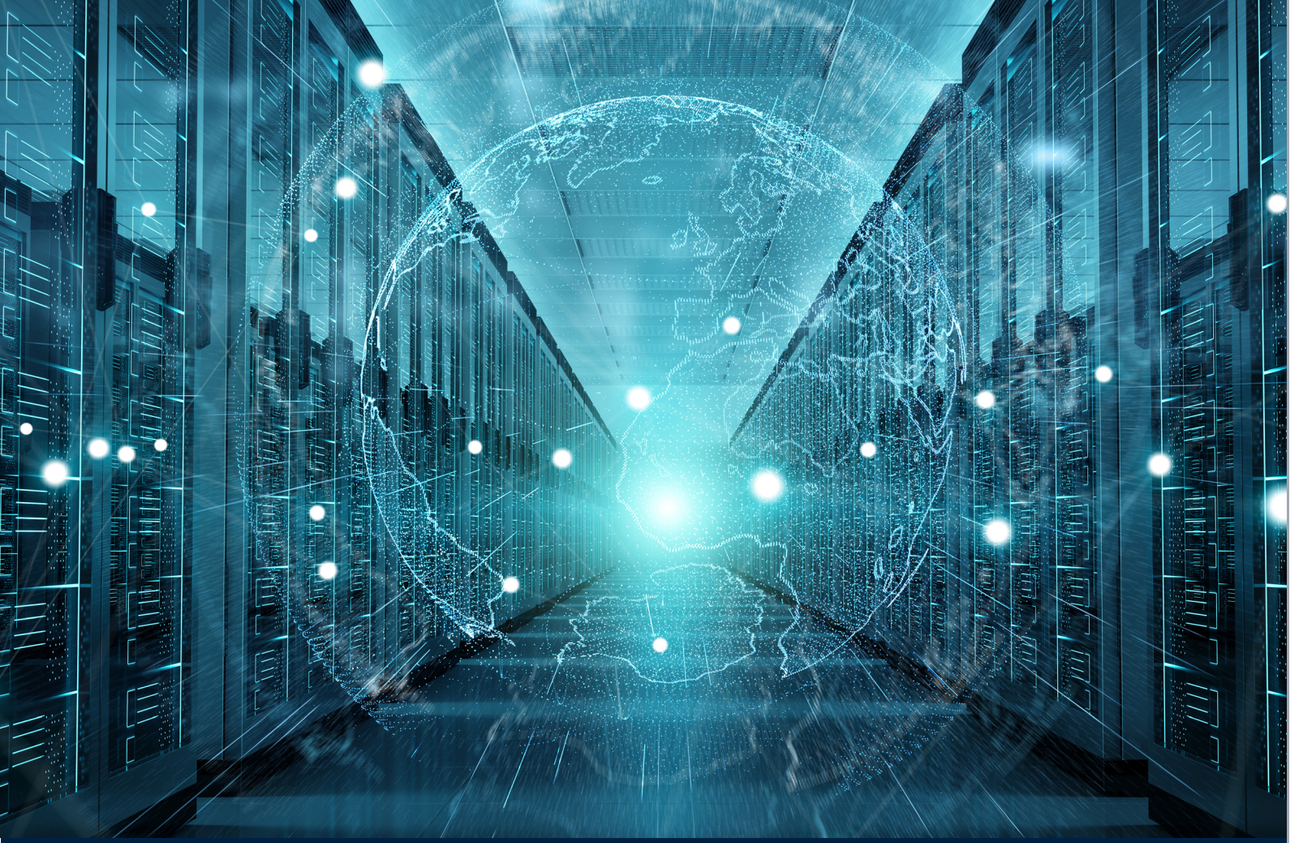
De samenhang binnen de NIS2-maatregelen

Deze maatregelen hangen met elkaar samen en vallen onder te verdelen in overkoepelende thema's. Dit maakt het eenvoudiger om aan de slag te gaan met de verplichte cyberbeveiligingseisen. Onze experts hebben de 10 maatregelen daarom gekoppeld aan 4 thema's:

Cyber Security Management Systeem	Supply Chain Cyber Security	Cyber Resilience	Secure development & systems
1 2 6	4	2 3	5 6 7 8 9 10

De maatregelen per overkoepelend thema

Ontdek in de volgende pagina's de maatregelen per thema, zodat u gericht stappen kunt zetten om uw cyberweerbaarheid te verbeteren én straks te voldoen aan de Cyberbeveiligingswet/ NIS2.



2.
De maatregelen rondom *het CSMS / ISMS*

CSMS (Cybersecurity Management Systeem) en ISMS (Information Security Management System) zijn frameworks waarmee u uw cybersecurityrisico's kunt beheren en controleren. Het helpt uw organisatie om gestructureerd beleid, processen en technologieën in te zetten om zich te beschermen tegen cyberdreigingen. Welke maatregelen zorgen ervoor dat u dit goed inricht?

Kern van cyberbeveiliging

CSMS/ ISMS vormen de kern van de cyberbeveiliging van uw organisatie. Het zorgt voor commitment, risicoanalyse, preventie, incidentmanagement en helpt om deze elementen aan te tonen aan de toezichthouder en de organisatie.

Het CSMS/ ISMS geeft de koers aan en zorgt dat u kunt sturen. Vergelijk het met een schip: zonder koers is het schip stuurloos. Het is de basis van uw 'Plan Do Check Act'-cyclus. Hierin staan de processen benoemd, zodat de organisatie een kader krijgt hoe zij moeten werken.

Oplossingen

Er is geen overkoepelend Cyberbeveiligingswet- of NIS2-certificaat. Wel zijn er bestaande oplossingen die u kunt laten certificeren. Daarnaast geven maturiteitsonderzoeken en audits inzicht in hoever uw organisatie is rondom cyberbeveiliging.

Rondom het CSMS zijn dat bijvoorbeeld:

- Maturiteitsonderzoeken en audits op basis van ISO 27001
- Maturiteitsonderzoeken en audits op basis van IEC 62443
- Maturiteitsonderzoeken en audits op basis van NEN 7510
- Pentesten

Ook zijn er gerichte trainingen, zoals:

- Basiscursus ISO 27001: leg de basis voor structurele Informatiebeveiliging
- IEC 62443-training Training Riskmanagement ISO 31000.

Maatregelen die passen bij een goed CSMS:

Maatregel 1:
Een risicoanalyse en beveiliging van informatiesystemen

Elke organisatie die aan cybersecurity doet, moet een systematiek volgen om ervoor te zorgen dat de processen op de juiste manier uitgevoerd worden. Deze maatregel zorgt ervoor dat organisaties een CSMS inrichten en vervolgens risicoanalyses gaan doen.

Het onderliggende principe van de Cyberbeveiligingswet/NIS2-richtlijn is namelijk risicogebaseerd: voor elke organisatie zijn de cyberrisico's anders en dus ook de maatregelen die deze risico's mitigeren.

Maatregel 2:
Incidentenbehandeling

Organisaties moeten protocollen hebben voor het detecteren, melden en verhelpen van cyberincidenten. Hoe eerder incidenten worden geconstateerd, hoe minder schade deze kunnen doen. Daarbij is het hebben van een protocol essentieel om tijdig de melding te kunnen doen bij de toezichthouder.

Maatregel 6:
Beleid en procedures om de effectiviteit van beheersmaatregelen van cyberbeveiligingsrisico's te beoordelen

Op basis van de risicoanalyse uit maatregel 1, moet u als organisatie de juiste maatregelen opstellen en implementeren. Ook is het van belang dat u deze mitigerende maatregelen periodiek evalueert en verbetert volgens de PDCA-cyclus. Dit staat voor Plan-Do-Check-Act.

3. Hoe borgt u de cybersecurity ***van uw supply chain?***

Een van de belangrijke verbeteringen in de nieuwe Cyberbeveiligingswet/NIS2-richtlijn is dat organisaties inzicht moeten krijgen in de toeleveringsketen. Binnen deze supply chain gaat het niet alleen om uw leverancier, maar ook om de leveranciers van uw leverancier. Belangrijk, maar geen eenvoudige opgave.

Maatregelen voor de cybersecurity van uw supply chain:

Bij dit thema hoort slechts één zorgmaatregel, maar dit is wel een maatregel die tijd vergt. Bovendien kunt u hiermee parallel aan de andere maatregelen beginnen.

Maatregel 4: Beveiliging van de toeleverancierskeketen

Deze maatregel focust zich helemaal op uw leveranciers: organisaties moeten de cybersecurity van hun leveranciers en partners monitoren en managen. Ook vraagt deze maatregel om regelmatige reviews en audits bij uw leveranciers.

Als organisatie kunt u vaak wel uw eigen leveranciers uitvragen, maar niet de leveranciers van uw leveranciers. Dit is dan ook een project op zich: u moet de contracten zo gaan opstellen en aanpassen, dat u grip houdt op uw keten.

Om dit goed te kunnen uitvoeren, heeft u eerst inzicht in de complete supply chain nodig. De keten in kaart brengen is een tijdrovend proces, en ook het aanpassen van de contracten kost tijd. Zaak dus om hier op tijd mee te beginnen, en niet te wachten totdat de Cyberbeveiligingswet van kracht wordt.

Oplossingen

Er zijn verschillende oplossingen die helpen om grip te krijgen op de cyberveiligheid van uw supply chain. Denk bijvoorbeeld aan:

- Supplier Management as a Service, met industriespecifieke normenkaders
- Maturiteitsonderzoeken op basis van IEC 62443

4.
Welke ***maatregelen*** zorgen voor ***cyber resilience***?

Cyber resilience gaat over hoe goed een organisatie in staat is om te blijven functioneren tijdens en na een cyberaanval. Het is de combinatie van preventie, detectie, respons en herstel. Waar cybersecurity vooral focust op het voorkomen van aanvallen, gaat cyber resilience een stap verder door ervoor te zorgen dat een organisatie zelfs na een aanval of storing operationeel blijft.

Maatregelen die cyber resilience ondersteunen:

Voordat u aan de slag gaat met de NIS2-maatregelen rondom cyber resilience, is het van belang dat u eerst het Cyber Security Management Systeem (CSMS) goed hebt ingericht, inclusief de risicoanalyse en mitigerende maatregelen. Dit om cyberincidenten vooraf te voorkomen

De maatregelen bij cyber resilience richten zich vooral op het beperken van de impact van een incident.

Maatregel 2: Incidentenbehandeling

Als er een incident is, is het belangrijk dat uw organisaties heldere protocollen heeft voor het detecteren, melden en verhelpen hiervan. Hoe moet iedereen reageren zodat u zo min mogelijk hinder ondervindt.

Maatregel 3: Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen

Deze maatregel richt zich op plannen om tijdens en na een cyberaanval essentiële diensten te blijven leveren en snel te herstellen. Denk bijvoorbeeld aan het op voorhand processen al zo inrichten, dat er andere processen het over kunnen pakken.

Belangrijk onderwerpen hierbij zijn response (hoe reageert uw organisatie) en recovery (heeft u bijvoorbeeld reservesystemen zodat u meteen weer aan de slag kunt).

Welke normen of frameworks kunt u hiervoor inzetten?

De basis voor cyber resilience is het CSMS, en de frameworks zoals ISO 27001, NEN 7510 en IEC 62443. Een aanvullende standaard is een maturiteitsonderzoek volgens ISO 2230.

5.
De maatregelen voor ***secure development*** and ***systems***

In het vierde overkoepelende thema ligt de focus op de technische laag. Secure development and systems draait om het veilig bouwen en onderhouden van software en IT-systemen. Het gaat erom dat uw organisatie tijdens het ontwerpen, ontwikkelen en beheren van software rekening houdt met mogelijke beveiligingsrisico's.

Maatregelen die secure development en systems borgen:

Het ontwikkelen en beheren van software liggen in elkaars verlengde en komen met ontwikkelingen als SaaS (Software as a Service) en DevOps (Development and Operations) steeds vaker samen. Relevant NIS2-maatregelen bij dit thema zijn:

Maatregel 5:
Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden

Deze maatregel richt zich op het onderhouden van de systemen: software moet actueel en veilig gehouden worden door regelmatige updates en het tijdig patchen van kwetsbaarheden.

Maatregel 6:
Effectiviteit maatregelen en risicomanagement

Als organisatie moet u een helder beleid hebben voor de cyberbeveiliging en procedures voor het omgaan met cyberrisico's. De ontwikkeling van het systeem vraagt ook om een risicoanalyse: wat is het dreigingslandschap voor dit systeem, en welke specifieke maatrelen treffen we daarvoor.

De Cyberbeveiligingswet en NIS2-richtlijn vragen om het treffen van risicogestuurde maatregelen. Als er dreigingen zijn die niet relevant zijn, hoeft u daar geen maatregelen voor te nemen. Maar u moet het wel steeds blijven evalueren, zodat u continue afdoende beschermd bent.

Maatregel 7:
Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging

Van Board of Directors, architect, softwareontwikkelaar en applicatiebeheerder tot gebruikers: iedereen die zich bezighoudt met het ontwikkelen en onderhouden van het systeem óf toegang heeft, moet de basisprincipes van cyberhygiëne kennen.

Overigens gaat het bij de Board of Directors niet alleen om awareness: op boardniveau moet men een risicoanalyse kunnen begrijpen, en kunnen begrijpen wat business continuity is en wat hiervoor nodig is.

Trainingen zijn hierbij cruciaal en relatief eenvoudig te organiseren.

Maatregel 8:
Beleid en procedures over het gebruik van cryptografie en encryptie

Bij deze maatregel gaat het erom dat berichten niet af te luisteren zijn. Versleuteling van gevoelige data moet worden toegepast om gegevens te beschermen, zowel tijdens opslag als tijdens overdracht.

Maatregel 9:
Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van assets

Toegang tot systemen en gegevens moet goed worden gecontroleerd, bijvoorbeeld via multi-factor authenticatie.

Maatregel 10:
Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen

Deze maatregel gaat om de beveiliging van netwerkaspecten. Organisaties moeten geavanceerde technologieën inzetten, zoals firewalls, antivirussoftware en intrusion detection systemen. Kortom, het netwerk moet op basis van risico's gesegmenteerd en gemonitord worden.

Welke oplossingen en trainingen kunt u hiervoor inzetten?

Verschillende oplossingen die voor de eerdere thema's van toepassing zijn, helpen ook bij het borgen van secure development & systems.

Denk bijvoorbeeld aan:

- Maturiteitsonderzoeken en audits op basis van ISO 27001
- Maturiteitsonderzoeken en audits op basis van IEC 62443
- Pentesten

Daarnaast is er een scala aan trainingen voor verschillende kennisniveaus, zoals:

- E-learning Awareness Informatiebeveiliging & Privacy
- Basiscursus ISO 27001: leg de basis voor structurele Informatiebeveiliging
- Praktische training AVG: Slim onderweg met de AVG
- Basiscursus NEN 7510: informatiebeveiliging in de zorg
- IEC 62443-training (Hudson Cybertec)
- Cybersecurity: OT for IT professionals (Hudson Cybertec)
- CSIR-Workshop (Hudson Cybertec)

Aan de slag met de NIS2 zorgplichtmaatregelen?

Wilt u aan de slag met de 10 NIS2 zorgplichtmaatregelen om de cyberweerbaarheid van uw organisatie te vergroten? Of met de andere verplichtingen uit de NIS2?

Vraag een vrijblijvend gesprek aan →

Kiwa en cybersecurity

Kiwa maakt cybersecurity inzichtelijk. Wij testen, inspecteren, certificeren en trainen uw organisatie. Dat doen we onafhankelijk en met kritische blik. Zo krijgt u grip op cyberrisico's, geeft u vertrouwen aan uw klanten en bent u continu up-to-date.

- One-stop-shop: diensten rondom OT, IT en IoT onder 1 dak
- Onafhankelijke, objectieve toetsing
- Kennis van wet- & regelgeving
- Bewezen kwaliteit voor testen, inspecteren, certificeren en trainen
- Toekomstvisie op cybersecurity

www.kiwa.com/cyber-security/

kiwa

Kiwa N.V.
Sir Winston Churchill-laan 273
2288 EA Rijswijk
Nederland

Telefoon (0)88 - 998 49 00
E-mail NL.CyberSecurity.Certification@kiwa.com

kiwa.com