

NIS2 en de Cbw

Een pragmatisch eBook
voor compliance



Inhoud

Even vooraf	3
Van NIS2 naar Cbw	4
Het wettelijk kader	6
Kernprincipes	9
Implementatie	12
Is NIS2 voor jou van toepassing?	14
Samenvatting	15
Slotwoord	16

Even vooraf

Digitale systemen vormen in toenemende mate de ruggengraat van onze samenleving. Cruciale sectoren als gezondheidszorg, het bankwezen en nutsvoorzieningen kunnen niet meer zonder een veilige en goed werkende digitale infrastructuur. Dat maakt hen ook kwetsbaar voor kwaadwillenden die uit zijn op financieel gewin of ontwrichting van de maatschappij.

In dat speelveld zijn de cyberrisico's de afgelopen jaren sterk vergroot. Technologische, maatschappelijke en geopolitieke ontwikkelingen liggen daaraan ten grondslag. Cybercriminaliteit is sterk geprofessionaliseerd en uitgegroeid tot een geoliede miljardenbusiness. Veel landen hebben digitale wapens stevig verankerd in hun militaire arsenaal. Ook ontwikkelingen als het toenemende hybride werken zorgen voor nieuwe risico's. Het is niet de vraag of, maar wanneer organisaties te maken krijgen met een cyberaanval.

Dat vraagt om meer dan enkel maatregelen. Het vraagt ook om wetgeving rondom securityvoorzieningen voor alle organisaties die een onmisbare rol spelen in de maatschappij. Met NIS2 helpt de EU de lidstaten om nationale wetgeving in te voeren die hun cyberweerbaarheid versterkt.

NIS2 heeft potentieel grote gevolgen. Ook voor jouw organisatie. De wetgeving die hieruit voortvloeit is niet vrijblijvend. Non-compliance kan naast een vergroot risico op ernstige cyberincidenten resulteren in hoge boetes. Nog nooit was het zo belangrijk om security op voorhand goed geregeld te hebben.

“Het is niet de vraag of, maar wanneer organisaties en instellingen te maken krijgen met een cyberaanval.”

Wat je kan verwachten van dit eBook

In dit eBook gaan we uitgebreid in op NIS2 en de Nederlandse wetgeving die hierop is gebaseerd: de Cyberbeveiligingswet (Cbw). We geven antwoord op veelgestelde vragen, leggen de verschillen bloot met NIS, zoomen in op de juridische aspecten van de richtlijn en bieden handvatten voor organisaties en instellingen die zich op de Cbw moeten voorbereiden.



Van NIS naar Cbw

NIS2 is een afkorting van Network Information Security 2. Het is een door de EU opgestelde richtlijn die de basis is voor nationale wetgeving rondom cybersecurity in alle lidstaten van de EU. Op deze manier wil het Europees Parlement het beveiligingsniveau en de cyberweerbaarheid in heel Europa versterken. NIS2 beschrijft welke maatregelen organisaties en instellingen minimaal zouden moeten nemen om hun digitale systemen te beveiligen, op welke organisaties die richtlijn van toepassing is en welke consequenties non-compliance met zich meebrengt.

Richtlijn vs. verordening

NIS2 zelf is zoals gezegd een richtlijn. Het is geen keiharde verordening maar bevat wel wat ze in juridische kringen een 'resultaatverplichting' noemen. Het is aan de afzonderlijke EU-lidstaten om NIS2 te vertalen naar nationale wetgeving die zo effectief mogelijk is. In Nederland wordt NIS2 met name geïmplementeerd in de Cyberbeveiligingswet (Cbw). Naar verwachting wordt de wet in het tweede kwartaal van 2026 van kracht. Veel organisaties zijn dan ook druk bezig met de voorbereiding op de Cbw.

Opvolger van NIS

NIS2 is niet helemaal nieuw. Al sinds 2016 bestaat de NIS-richtlijn. In Nederland is deze richtlijn opgenomen in de Wbni (Wet beveiliging netwerk- en informatiesystemen). NIS2 is de directe opvolger van NIS.

De richtlijn is op een aantal punten bijgewerkt. Niet voor niets: NIS2 sluit beter aan bij de huidige ontwikkelingen en toegenomen cyberdreigingen. Zo is NIS2 op veel meer organisaties van toepassing. Naast vitale sectoren is NIS2 gericht op bijvoorbeeld ICT-dienstverleners en de maakindustrie (zie 'Voor wie is NIS2 bedoeld?'). Verder kan de richtlijn impact hebben op organisaties die zelf niet onder NIS2 vallen, maar wel een rol spelen in vitale toeleveringsketens. Daarnaast omvat NIS2 een meldplicht voor cyberincidenten. Ook zijn lidstaten verplicht om de naleving te controleren, voor de meest vitale organisaties zelfs proactief.

In ontwikkeling

De NIS2-richtlijn is sinds 17 oktober 2024 van toepassing in de Europese Unie. Daarmee is de kous niet af. Naast het creëren van nationale wetgeving moeten lidstaten ook een manier vinden om te controleren op naleving.

Ook laten de beschreven maatregelen de nodige ruimte voor praktische invulling. Net als bij de AVG zullen diverse sectoren op zoek moeten naar een effectieve vertaling van de wetgeving naar de praktijk.

NIS en NIS2 door de jaren heen

2013

De Europese Commissie publiceert de **Europese Unie Cybersecurity Strategie**, waarin de behoefte aan een gecoördineerde aanpak van cybersecurity binnen de EU-lidstaten wordt benadrukt.

2016

6 augustus: het Europees Parlement en de Raad van de Europese Unie keuren de **Network and Information Security-richtlijn** (NIS-richtlijn) goed.

2019

EU-lidstaten moeten **Computer Security Incident Response Teams** (CSIRT's) oprichten om samenwerking en informatie-uitwisseling tussen lidstaten en het Europees Agentschap voor Cybersecurity (ENISA) te faciliteren.

2018

9 mei: deadline voor EU-lidstaten om de NIS-richtlijn om te zetten in hun **nationale wetgeving**.

2021

EU-lidstaten werken verder aan de **implementatie van de NIS-richtlijn** en het versterken van hun cybersecurity-capaciteiten in overeenstemming met de vereisten.

2023

Januari 2023 start van de **implementatie-termijn** van 21 maanden. Binnen deze termijn moeten EU-lidstaten de richtlijn omzetten naar wetgeving.

2022

28 november 2022 de Europese Raad stelt de **NIS2-richtlijn** vast

27 december 2022 publicatie van de NIS2-richtlijn in de **Official Journal** van de Europese Unie

Zomer 2023

start van een **internetconsultatie-periode** van 6 weken. Hierin kunnen burgers, bedrijven en overheidsinstellingen mogelijke verbeteringen aangeven in de wet- en regelgeving die in voorbereiding is. De resultaten daarvan worden gepubliceerd op de overheidswebsite **www.internetconsultatie.nl**

2026

Naar verwachting treedt de Cyberbeveiligingswet in het tweede kwartaal van 2026 in werking. Vanaf dat moment moeten organisaties aan de wet voldoen.

Het wettelijk kader

Voor wie geldt NIS2?

NIS2 richt zich op organisaties en instellingen met een belangrijke maatschappelijke functie. NIS2 maakt onderscheid tussen 'essentiële' en 'belangrijke' organisaties. Uiteindelijk is NIS2 ten opzichte van de oude NIS-richtlijn op meer organisaties van toepassing.

NIS2 is van toepassing op de volgende doelgroepen:

1. Essentiële organisaties
2. Belangrijke organisaties

Hieronder zetten we de 'doelgroep' van NIS2 uiteen:

1. Essentiële entiteiten

Missiekritische organisaties bevinden zich in de volgende sectoren:



Energie



Vervoer



Bankwezen



Infrastructuur voor de financiële markt



Drinkwater



Afvalwater



Digitale infrastructuur



Beheer van ICT-diensten



Post- en koeriersdiensten



Afvalstoffenbeheer



Levensmiddelen



Gezondheidszorg



Overheid



Ruimtevaart

2. Belangrijke entiteiten

(Middel-)grote organisaties bevinden zich in de volgende sectoren:



Post- en koeriersdiensten



Afvalstoffenbeheer



Levensmiddelen



Maakindustrie



Chemische stoffen



Onderzoek

+ Alle essentiële sectoren

Dit zijn grote organisaties die een kritieke rol vervullen in de maatschappij. Met 'groot' doelt NIS2 op organisaties met **meer dan 250 medewerkers of een netto-omzet van meer dan 50 miljoen euro en een balanstotaal van meer dan 43 miljoen euro.**

Naast essentiële entiteiten spreekt NIS2 ook van belangrijke entiteiten. Dit zijn de middelgrote organisaties binnen de essentiële entiteiten, of actief in een van de zes aanvullende sectoren. Met middelgroot bedoelt de richtlijn organisaties met **minimaal 50 werknemers of een jaaromzet of balanstotaal van meer dan 10 miljoen euro.**

Maar let op!

Er is een aantal kleine bedrijven dat niet past in een van de bovenstaande categorieën, maar toch moet voldoen aan de Cbw. Het gaat dan bijvoorbeeld om bedrijven die een belangrijke rol spelen in de infrastructuur van het internet en dus strategische doelwitten zijn voor cyberaanvallen. Denk aan bedrijven die toplevel-domeinnamen beheren, verleners van domeinnaamregistratiediensten, of aanbieders van openbare communicatienetwerken of -diensten.

Benieuwd of jouw organisatie onder de Cbw valt? Bekijk dan de flowchart op pagina 14.

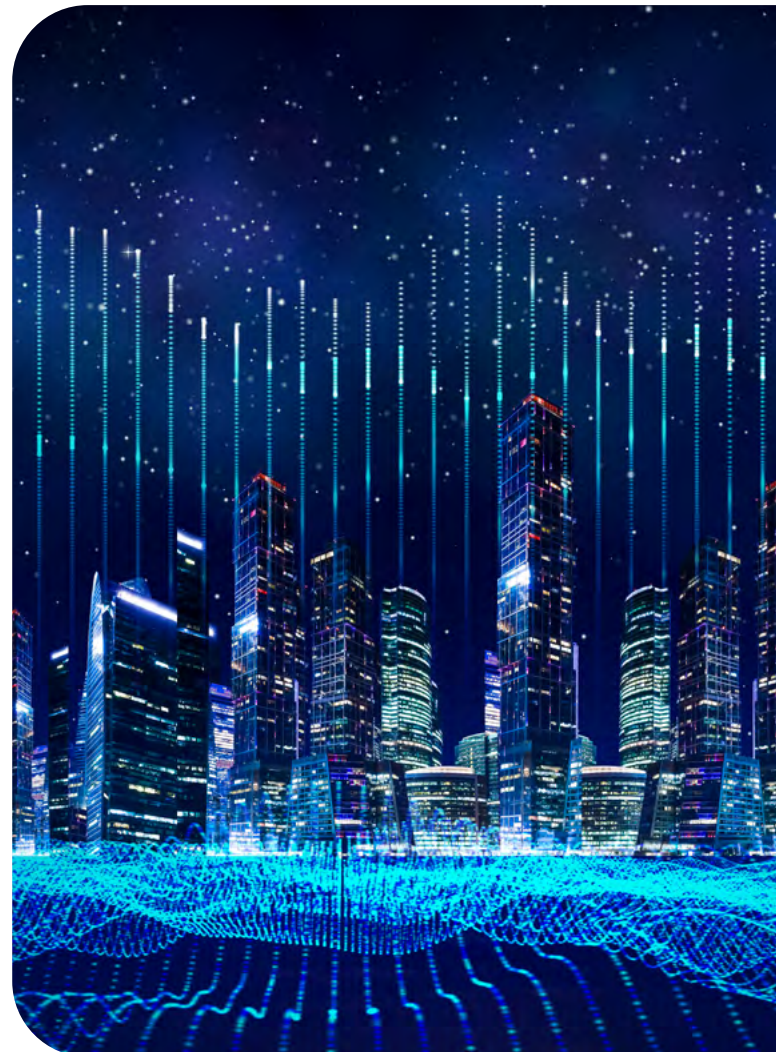
Cbw in de keten

Organisaties die belangrijk of essentieel zijn en dus onder de Cbw vallen, moeten erop toezien dat hun leveranciers (de keten) voldoende securitymaatregelen hebben genomen. Deze leveranciers vallen zelf niet per definitie onder de Cbw, maar zij kunnen wel degelijk te maken krijgen met strengere securityeisen. En dat is niet voor niets, want cyberaanvallen lopen steeds vaker via de toeleveringsketen. Het is dus van groot belang dat je ketenpartners hun security ook op orde hebben.

Controle en handhaving

Een belangrijk verschil met de eerste NIS-richtlijn is de manier waarop controle op die naleving plaatsvindt. Alle organisaties die binnen de categorie 'essentieel' vallen, kunnen proactieve, steekproefsgewijze controles verwachten. Dat betekent dat ze ieder moment, zonder enige aanleiding moeten kunnen aantonen dat ze aan de wet voldoen.

Ook organisaties uit de categorie 'belangrijk' moeten aan de Cbw voldoen. Voor hen gelden de proactieve controles echter niet. Zij moeten pas aantonen dat ze aan de wet voldoen wanneer daar een duidelijke aanleiding voor is. Dat is in de praktijk doorgaans een (ernstig) cyberincident.



Boetes

Voldoet een organisatie na controle niet aan de richtlijn? Dan kan de sectorale toezichthouder een boete uitdelen. Het is aan de lidstaten zelf om de hoogte van die boete te bepalen, passend bij de aard en ernst van de nalatigheid. De boetes voor de meest ernstige gevallen van nalatigheid zijn als volgt (de maximale boete is steeds het hoogste bedrag van de gegeven keuzes):

- **Voor essentiële organisaties:**

Maximaal 10 miljoen of 2% van de wereldwijde jaaromzet.

- **Voor belangrijke organisaties:**

Maximaal 7 miljoen of 1,4% van de wereldwijde jaaromzet.

Bestuur aansprakelijk

Een opvallende toevoeging is dat het bestuur aansprakelijk is voor het niet naleven van de Cbw. Daarmee wordt compliance een nog belangrijker thema in de boardroom.



Kernprincipes

De Cbw werkt een aantal verplichtingen uit voor organisaties die onder de wet vallen. Belangrijke onderdelen zijn de zorgplicht en de meldplicht.

1. Zorgplicht

De zorgplicht houdt in dat de organisatie de nodige securitymaatregelen moet treffen gericht op het waarborgen van de digitale veiligheid en de continuïteit van de dienstverlening.

NIS2 schrijft niet exact voor welke technologieën of oplossingen organisaties moeten gebruiken.

De richtlijn spreekt van 'passende en evenredige technische, operationele en organisatorische maatregelen', en ook 'rekening houdend met de stand van de techniek'.

Wel geeft NIS2 een opsomming van de aandachtsgebieden die organisaties ten minste in orde moeten hebben:

- **Beleid rondom risicoanalyse**
Organisaties moeten beleid hebben geformuleerd rondom de periodieke analyse van securityrisico's. Denk daarbij aan een regelmatige analyse van de externe risico's, maar ook pentests voor het doorlichten van de kwetsbaarheden in de IT-infrastructuur.
- **Analyse van de effectiviteit van de securitymaatregelen**
Organisaties moeten regelmatig controleren of de genomen maatregelen afdoende zijn.
- **Beveiliging van de toeleveringsketen**
Nieuw in NIS2 is de aandacht voor ketenveiligheid. De maatregelen moeten niet alleen gericht zijn op het voorkomen van incidenten in de eigen organisatie, maar op de bescherming van de gehele keten. Dat betekent dat organisaties afspraken moeten maken met hun toeleveranciers en dienstenpartners over bijvoorbeeld de omgang met en beveiliging van elkaars data en de beveiliging van onderlinge communicatie.
- **Aandacht voor cyberhygiëne en security-awareness**
NIS2 stelt in tegenstelling tot NIS ook een goede cyberhygiëne verplicht. Organisaties moeten er dus op toezien dat hun medewerkers zich digitaal veilig gedragen. Een voorwaarde daarvoor is dat zij zich bewust zijn van de risico's en weten hoe ze die zoveel mogelijk kunnen beperken. Regelmatige trainingen op het gebied van security-awareness zijn daarmee verplicht. Ook voor bestuursleden: zij moeten binnen 2 jaar na inwerkingtreding van de wet een training volgen.



- **Beleid rondom cryptografie en encryptie**
NIS2 is wat deze securitymaatregel betreft vrij concreet. Organisaties moeten waar mogelijk encryptie toepassen. Bijvoorbeeld voor de versleuteling van gevoelige data- en communicatiestromen.

- **Beleid voor fysieke beveiliging rondom personeelstoegang en activa**
Cybercriminelen kunnen ook via fysieke toegang tot ziekenhuizen, zorginstellingen en systemen een aanval opzetten. Daarom verlangt NIS2 ook aandacht voor de fysieke beveiliging. Organisaties moeten weten wie er aanwezig is en welke toegangsrechten medewerkers, patiënten/cliënten en bezoekers hebben.

- **Gebruik van multifactorauthenticatie (MFA) en beveiliging van communicatiestromen**
NIS2 noemt concreet het gebruik van multifactorauthenticatie waar dat passend zou zijn.

- **Beveiliging van informatiesystemen**
Informatiesystemen moeten voldoende beveiligd zijn tegen cyberaanvallen, malware en andere digitale bedreigingen. Welke securitycontrols precies 'passend en evenredig' zijn verschilt per organisatie, maar te denken valt aan oplossingen voor identiteits- en toegangsbeheer, endpointsecurity en XDR (Extended Detection and Response). Voor organisaties die intensief van de (multi) cloud gebruikmaken, zijn SASE (Secure Access Service Edge)-oplossingen een logische keuze en best practice.

- **Beveiliging bij het ontwerpen, ontwikkelen en onderhouden van netwerk- en informatiesystemen**

Een goed netwerkbeheer en adequate beveiliging van het netwerk zijn een must. NIS2 noemt ook expliciet dat organisaties adequaat moeten reageren op nieuw ontdekte kwetsbaarheden.

Vulnerability Management helpt bij het tijdig op de hoogte zijn van nieuwe kwetsbaarheden en compliancy. Vervolgens is een goed update- en patchbeleid onmisbaar om de gevonden kwetsbaarheden te dichten. Aansluiting bij een SOC en/of Incident Respons-dienstverlening zijn goede toevoegingen voor detectie en respons van security-incidenten.

- **Incidentenafhandeling**
Organisaties moeten een incident-responseplan paraat hebben. In zo'n plan staat beschreven welke stappen de organisatie doorloopt bij een cyberincident en wie waarvoor verantwoordelijk is.

- **Continuïteit van de dienstverlening**
Na een incident moeten organisaties hun dienstverlening zo snel mogelijk weer kunnen hervatten. Dat vereist bijvoorbeeld een gedegen back-up- en recoverybeleid, crisisbeheer, continuïteitsplannen die regelmatig worden getest en de nodige noodvoorzieningen. Denk bij dat laatste aan reservelaptops en werkplekken.

2. Meldplicht

In tegenstelling tot de oude NIS-richtlijn kent NIS2 ook een meldplicht voor significante incidenten. Wanneer organisaties te maken krijgen met een verstoring in de digitale dienstverlening, dan zijn ze verplicht deze te rapporteren bij de betreffende autoriteit. Deze meldplicht is op sommige punten vergelijkbaar met die in de AVG. Onder deze privacywet zijn organisaties verplicht ernstige datalekken te melden bij de Autoriteit Persoonsgegevens (AP). Overigens is een melding bij de AP nog steeds verplicht als er persoonsgegevens betrokken zijn..

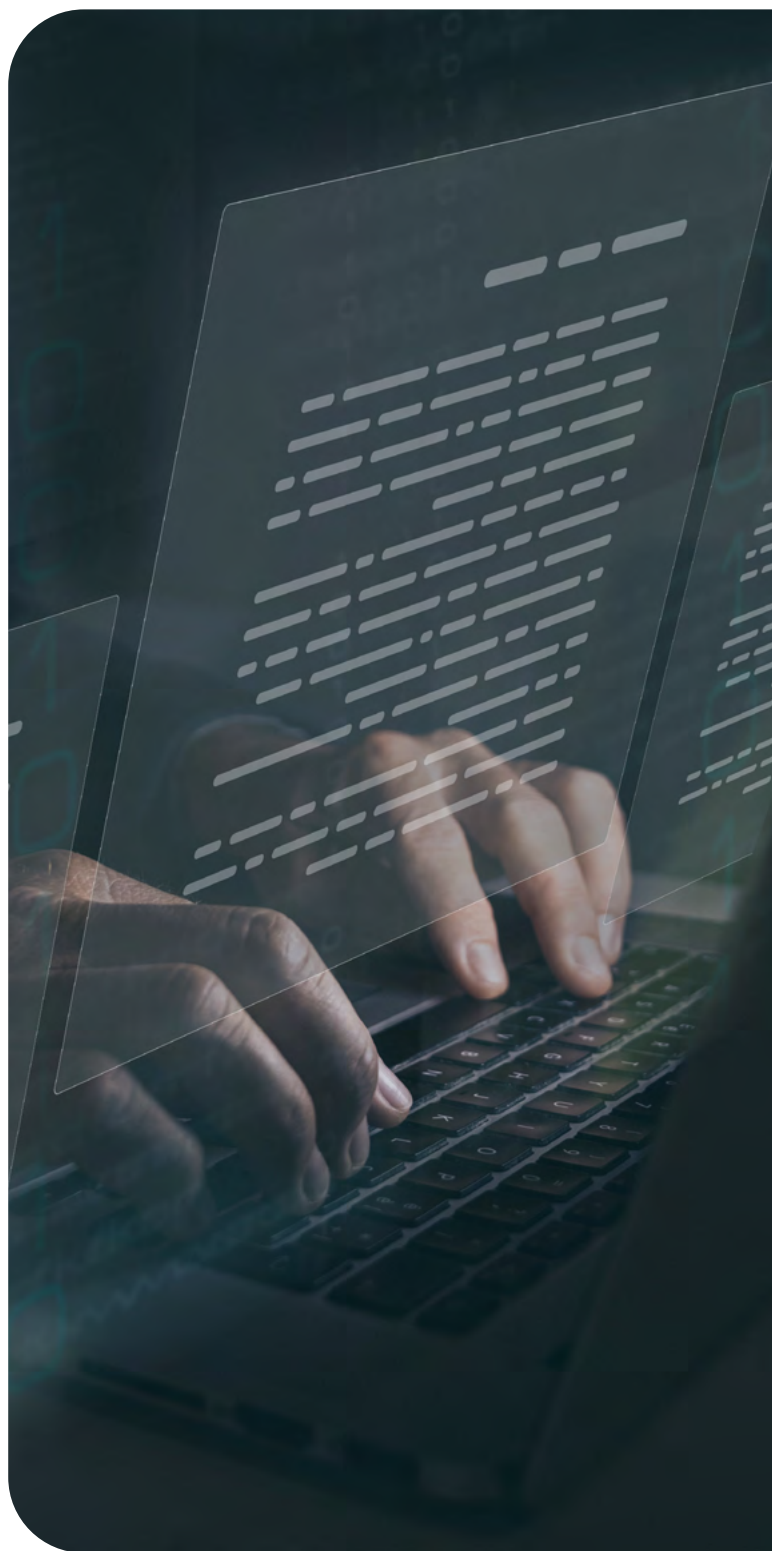
Rapportagevereisten

NIS2 stelt de volgende eisen aan een melding:

- De rapportage moet in alle gevallen zo snel mogelijk plaatsvinden.
- Heeft het incident de dienstverlening verstoord? Dan moet de organisatie het incident binnen 24 uur rapporteren.
- In alle andere gevallen moet de melding binnen 72 uur plaatsvinden.

Van alle incidenten moet de getroffen organisatie na een maand een eindverslag inleveren. Daarin staan onderzoeksresultaten, de gevolgen van de aanval en de genomen maatregelen om herhaling te voorkomen. Organisaties moeten de rapportage indienen bij de betreffende toezichthouder.

Bij ernstige incidenten die de dienstverlening raken, moeten afnemers van diensten geïnformeerd worden om de impact te beperken en hen in staat te stellen maatregelen te nemen.



Implementatie

Voldoen aan de Cbw is niet vanzelfsprekend. Voor een solide en weerbare securityomgeving is het noodzakelijk deze onder de loep te nemen en waar nodig verbeteringen aan te brengen.

Tegelijkertijd is compliance zelf niet het allerbelangrijkste. Cyberincidenten kunnen verstrekende gevolgen hebben voor de organisatie, de klanten en de maatschappij als geheel. Daarmee is een goede security een haast vanzelfsprekende voorwaarde voor een stabiele bedrijfsvoering, en tegelijkertijd een morele en

maatschappelijke verplichting.

Een intrinsieke motivatie om de security op orde te krijgen is noodzakelijk, wil het niet bij een eenmalige exercitie blijven. Het is, ongeacht de motivatie, belangrijk zo snel mogelijk aan de slag te gaan met het in orde brengen van de securityomgeving. Nu is er nog tijd om zaken goed aan te pakken. Vanaf het moment dat NIS2 is omgezet in wetgeving heeft ieder ernstig incident mogelijk niet alleen economische en maatschappelijke, maar ook juridische gevolgen. Met onderstaande stappenplan en tips helpen we je op weg richting Cbw-compliance.

Stap 1

Risicoanalyse uitvoeren

- Identificeer en analyseer de mogelijke risico's en bedreigingen voor de informatiebeveiliging binnen de organisatie. Evalueer de mogelijke impact van deze risico's en bedreigingen op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.
- Prioriteer de risico's op basis van de kans dat een incident zich voordoet en wat dan de impact is.

Stap 2

Beveiligingsmaatregelen implementeren

- Selecteer de beveiligingsmaatregelen die geschikt zijn voor jouw organisatie op basis van de geïdentificeerde risico's en bedreigingen, en toets deze aan de NIS2-richtlijn.
- Implementeer technische en organisatorische maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van data en systemen te waarborgen.
- Zorg ervoor dat de beveiligingsmaatregelen voldoen aan de vereisten en aanbevelingen van de NIS2-richtlijn.

Stap 3

Incident-responseplannen ontwikkelen

- Ontwikkel plannen en procedures om effectief te reageren op beveiligingsincidenten.
- Definieer rollen en verantwoordelijkheden van betrokken medewerkers bij het detecteren, rapporteren en reageren op incidenten.
- Stel een proces op voor het evalueren en herstellen van de systemen en gegevens na een beveiligingsincident.
- Train medewerkers regelmatig in het volgen van het incident-responseplan.

Stap 4

Bewaking en evaluatie

- Stel een monitoringprogramma op om afwijkingen en incidenten te detecteren en te rapporteren.
- Evalueer regelmatig de effectiviteit van de beveiligingsmaatregelen en incident-responseplannen.
- Pas de maatregelen aan op basis van lessen uit eerdere incidenten of wijzigingen in de omgeving.
- Zorg ervoor dat je voldoet aan de rapportageverplichtingen van de NIS2-richtlijn.

Maak waar mogelijk gebruik van bestaande raamwerken

Er zijn diverse raamwerken in omloop die waardevol zijn voor NIS2-compliance. Deze raamwerken bieden houvast, zijn een inspiratiebron voor te nemen securitymaatregelen en leiden je stap voor stap richting een weerbare en veerkrachtige cybersecurityomgeving. Het is belangrijk dat zo'n raamwerk goed past bij je organisatie, zowel qua grootte als organisatielcultuur.

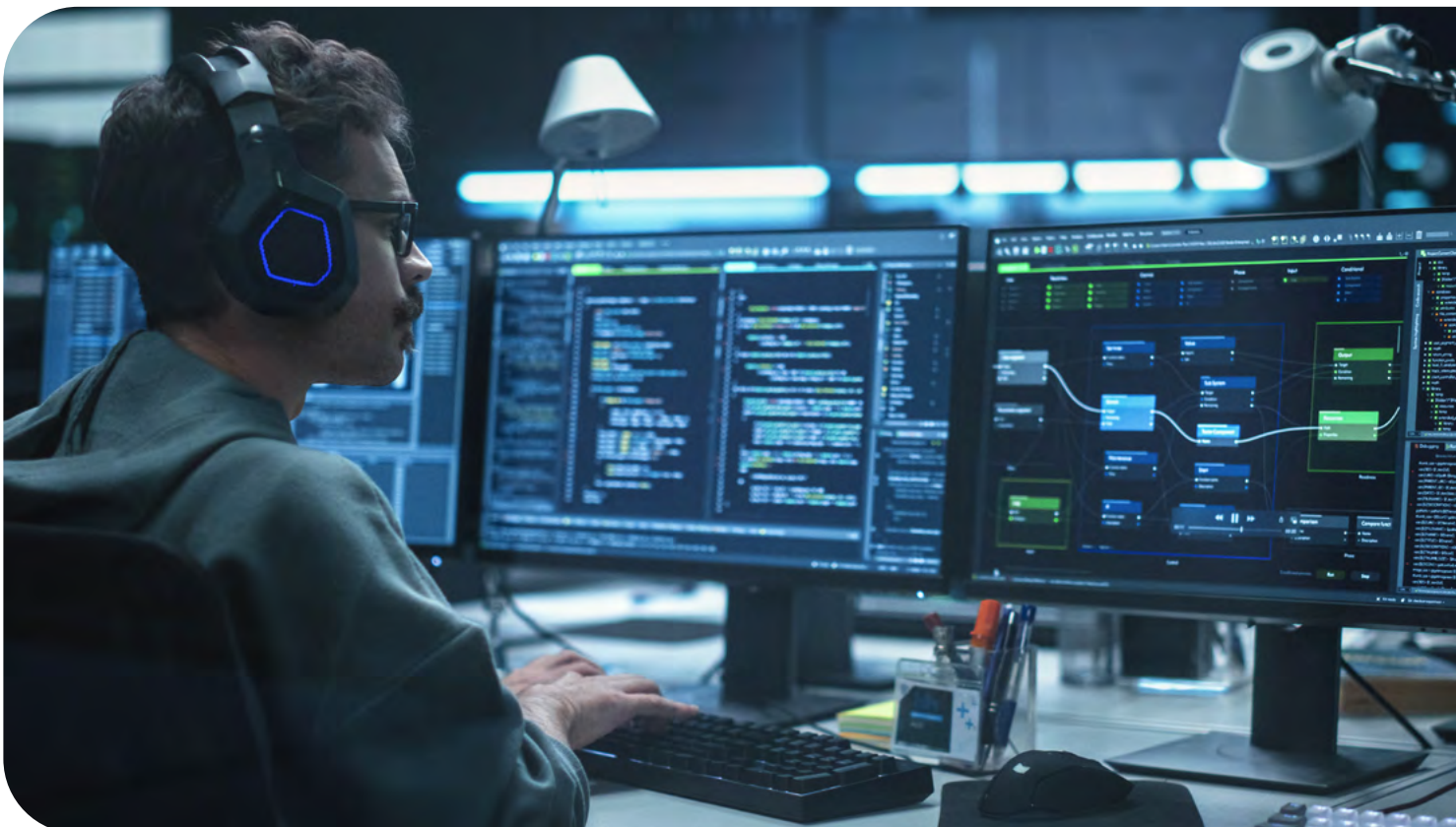
Een goed en veelgebruikte verzameling maatregelen is bijvoorbeeld de CIS Controls. Dit is een lijst met meer dan 150 best practices, opgesteld door organisaties die ooit zelf zijn getroffen door een ernstige cyberaanval. De CIS Controls maatregelen zijn voor de organisaties die het raamwerk hebben samengesteld een soort 'lessons learned'.

De maatregelen zijn onderverdeeld in 3 niveaus, zodat ze voor ieder type en grootte organisatie een gezonde mix bieden.

Bestaande certificeringen

Wellicht is jouw organisatie net klaar met een ISO 27001- of NEN 7510 traject. Dan kunnen we je geruststellen: NIS2 maakt bestaande securitycertificeringen allesbehalve overbodig. Dergelijke gerenommeerde certificeringstrajecten zijn een goede manier om security te structureel te integreren in de organisatie. Let wel: een dergelijke certificering maakt je niet meteen automatisch ook NIS2-compliant. Voldoen aan de normen is verplicht, het certificaat halen niet.

Lever je ICT-diensten aan 'essentiële' of 'belangrijke' organisaties of instellingen? Dan kunnen lidstaten zelfs vereisen dat je over een door de EU erkende certificering beschikt.



Is NIS2 voor jou van toepassing?

Valt jouw organisatie binnen 1 van deze sectoren?



Heeft jouw organisatie meer dan 250 medewerkers?

Levert jouw organisatie aan 1 van deze sectoren?



Ja.
Je bent verplicht om te voldoen aan de NIS2

Heeft jouw organisatie meer dan 10 miljoen omzet?

Nee.
Wel zullen er indirecte eisen aan je gesteld worden.

Speelt jouw organisatie een belangrijke rol in de infrastructuur van internet of de overheid?



Ja.
Je bent verplicht om te voldoen aan de NIS2

Nee.
Je bent **niet** verplicht om te voldoen aan de NIS2

Ja.
Je bent verplicht om te voldoen aan de NIS2

Nee.
Je bent **niet** verplicht om te voldoen aan de NIS2

Valt jouw organisatie binnen 1 van deze sectoren?

Post- en koeriersdiensten, Afvalstoffenbeheer, Levensmiddelen, Chemische stoffen, Onderzoek, Maakindustrie



Essentiële entiteiten

Belangrijke entiteiten

Samenvatting

- NIS2 is een EU-richtlijn die tot doel heeft de cybersecurity en cyberweerbaarheid in heel Europa te versterken.

 - Het is de opvolger van de NIS-richtlijn en dient als basis voor nationale wetgeving in verschillende lidstaten.

 - In Nederland wordt NIS2 vertaald naar de Cyberbeveiligingswet. Deze treedt naar verwachting in het tweede kwartaal van 2026 in werking.

 - NIS2 is van toepassing op essentiële en belangrijke organisaties. Indirect krijgen ook hun ketenpartners met strengere securityeisen te maken.

 - Kleine organisaties of instellingen die een belangrijke rol spelen in de internetinfrastructuur en overheidsinstanties vallen ook onder NIS2.

 - NIS2 vereist het nemen van beveiligingsmaatregelen en melding van cyberincidenten.

 - De naleving van NIS2 kan worden gecontroleerd, met proactieve controles voor essentiële organisaties en controles op aanleiding voor belangrijke organisaties.
- Niet-naleving kan leiden tot boetes, waarvan de maximale bedragen afhankelijk zijn van de categorie van de organisatie.

 - Het bestuur is aansprakelijk voor de NIS2-compliance.

 - Belangrijke onderdelen van NIS2 zijn de zorgplicht en de meldplicht.

 - De zorgplicht vereist dat organisaties passende en evenredige technische, operationele en organisatorische maatregelen nemen om digitale veiligheid en continuïteit te waarborgen.

 - Organisaties moeten ook voldoen aan de meldplicht en incidenten binnen 24 uur (bij verstoring van dienstverlening) of binnen 72 uur (in andere gevallen) melden aan de betreffende autoriteit.

 - Bestaande raamwerken zoals CIS Controls en certificeringen zoals ISO 27001/2, NEN 7510 of BIO 2 zijn nuttig voor NIS2-compliance.

Slotwoord

Een sterke security was al nooit een vrijblijvende zaak, maar NIS2 heeft daarover iedere mogelijke twijfel weggenomen. Tegelijkertijd mag het voorkomen van boetes nooit de belangrijkste drijfveer van het op orde hebben van je security.

Het achterliggende doel van de EU is weliswaar ‘hoog-over’: het vergroten van de weerbaarheid van de lidstaten. Toch is precies dat doel niet alleen relevant voor de EU als geheel, maar ook voor iedere afzonderlijke organisatie.

Een ernstig cyberincident heeft namelijk potentieel desastreuze gevolgen. In de eerste plaats voor de organisatie zelf, zoals een verstoorde dienstverlening, diefstal van organisatiegeheimen, ontevreden patiënten of cliënten en (onherstelbare) imagoschade. Zaken die uiteindelijk een organisatie definitief de das kunnen omdoen, en veel meer schade berokkenen dan welke boete dan ook. Maar ook voor de samenleving als geheel, zoals bij grootschalige datalekken, economische nevenschade en uitval van cruciale voorzieningen.

Een sterke security is dan ook geen kwestie van een ‘vinkje’ om boetes en juridische rompslomp te voorkomen. Het is een ethische, morele en economische missie. NIS2 is daarbij niet het einddoel, maar slechts een hulpmiddel. Bovendien verwachten we dat NIS2 en de Cbw die hieruit voortvloeit niet het juridische eindstation zijn op het gebied van security.

Het realiseren van een weerbare en veerkrachtige organisatie is altijd waardevol. Voor je organisatie, voor mens en maatschappij en als een goede basis voor toekomstige securitywetgeving.



Meer weten?

Heb je nog vragen over dit eBook, NIS2 of de Cbw?
Wil je eens vrijblijvend sparren met onze experts
over de gevolgen voor jouw organisatie?
Neem dan contact op met je accountmanager
of vul het [contactformulier](#) in.