c't tech-platform voor de professional

In samenwerking met vodafone business

NIS2

De nieuwe standaard voor cybersecurity

- NIS2 cybersecurity in Europa
- Voor wie geldt de nieuwe wet?
- De verplichtingen van NIS2
- 10 maatregelen om aan de Cbw te voldoen
- Waarom cybersecurity en NIS2 essentieel zijn

NIS2, de nieuwe standaard voor cybersecurity

Op 4 juni 2025 is het wetsvoorstel voor de Cyberbeveiligingswet (Cbw) bij de Tweede Kamer ingediend. Met deze wet wordt de Europese NIS2-richtlijn vertaald naar Nederlandse regelgeving.

De Cbw vormt de nationale implementatie van de Europese Network and Information Security-richtlijn (NIS2), die als doel heeft de cyberweerbaarheid van essentiële en belangrijke diensten binnen de EU te versterken. De noodzaak hiervoor neemt toe door de groeiende afhankelijkheid van digitale systemen en de toename van cyberincidenten.

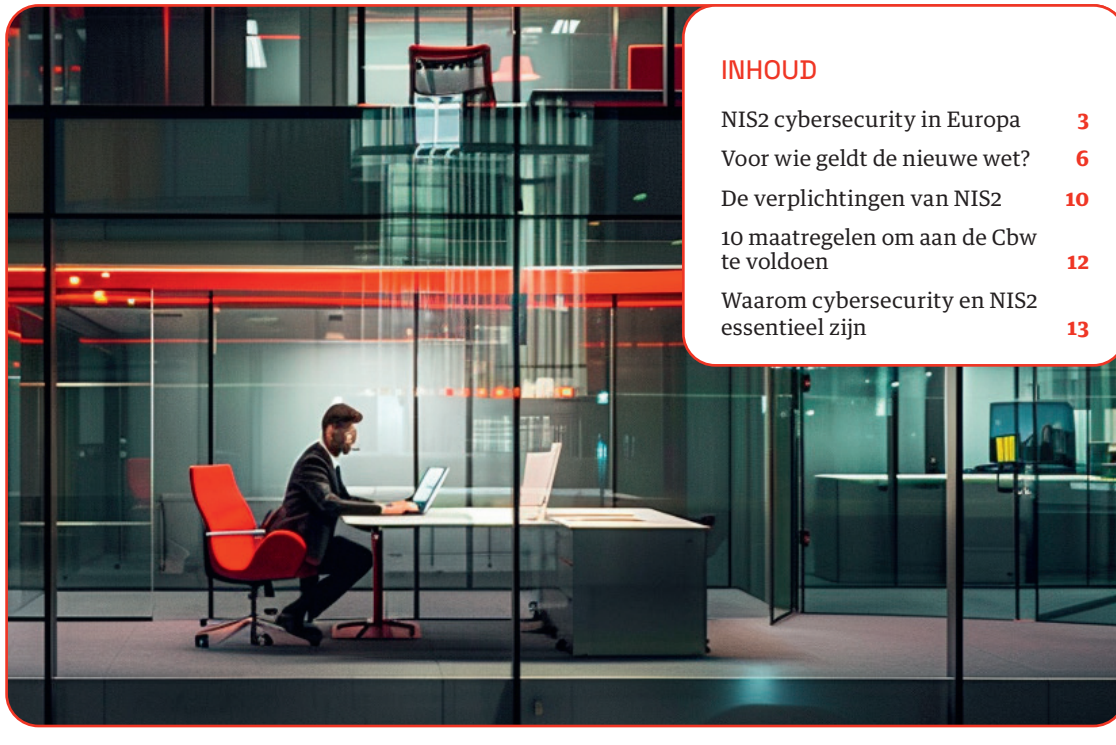
Organisaties die onder de Cyberbeveiligingswet vallen, hebben een zorgplicht en moeten maatregelen nemen om de continuïteit van hun diensten te waarborgen en de informatie te beschermen.

We bespreken hier de achtergrond van NIS2, hoe deze richtlijn tot stand is gekomen en wat de Europese richtlijn betekent op nationaal niveau.
Veel organisaties zullen te maken krijgen met de Cyberbeveiligingswet. Je komt hier te weten of jouw organisatie onder de wet valt, en zo ja, op welk niveau dit zal zijn. Want dit gaat gepaard met een aantal plichten waar organisaties aan moeten voldoen, en deze zijn niet vrijblijvend.

Het is dus van groot belang om je als organisatie goed voor te bereiden op de Cbw. Hopelijk kan dit e-book je daarbij helpen.

Redactie c't

c't x vodafone business



INHOUD

NIS2, de nieuwe standaard voor cybersecurity in Europa

Tien jaar geleden heeft de EU de Network and Information Security-richtlijn geïntroduceerd. Het doel van deze richtlijn is om in Europees verband de cyberbeveiliging en de weerbaarheid van essentiële diensten in de lidstaten te verbeteren. Binnenkort wordt de opvolger, de NIS2, in Nederland van kracht.

De NIS2-richtlijn is al op 16 januari 2023 ingegaan, maar de individuele Europese lidstaten hebben tijd gekregen om deze om te zetten naar nationale wetgeving. Zo wordt de NIS2-richtlijn momenteel in Nederland omgezet naar de Cyberbeveiligingswet (Cbw).

Achtergrond

In 2015 heeft de Europese Unie de Digital Single Market Strategy geformuleerd. Daarin stelde de Europese Commissie als doel om belemmeringen voor de digitale markt weg te nemen, in lijn met het concept van de gemeenschappelijke Europese markt.

De Digital Single Market (DSM) moet er voor zorgen dat de economie, het bedrijfsleven en de samenleving in Europa optimaal profiteren van het nieuwe digitale tijdperk. Het doel is om virtuele grenzen weg te nemen, de digitale connectiviteit te stimuleren en het voor consumenten makkelijker te maken om toegang te krijgen tot online-inhoud vanuit de hele Europese Unie.

Enkele significante zaken zijn binnen de DSM al gerealiseerd, zoals het einde van roamingtarieven, het verbod van ongerechtvaardigde geoblocking en de modernisering van gegevensbescherming (zoals de Algemene Verordening Gegevensbescherming).

Binnen deze strategie werd in 2016 de netwerk- en informatiebeveiliging richtlijn (NIS) geïntroduceerd, die een beveiligingsverplichting verordent voor organisaties die essentiële diensten leveren en een nauwere samenwerking tussen lidstaten moet bevorderen. In Nederland is deze richtlijn in 2016 opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni).

NIS en NIS2

Door de toenemende digitalisering van onze samenleving en door internationale ontwikkelingen groeit ook het aantal cyberbedreigingen die, als ze doelgericht worden ingezet, onze maatschappij ernstig zouden kunnen ontwrichten.

De originele NIS-richtlijn werd onder andere opgezet om aan de noodzaak van betere beveiliging te voldoen. De komst van de nieuwe NIS2-richtlijn moet gaan bijdragen aan een hoger niveau van cybersecurity bij organisaties en een hogere mate van harmonisatie binnen Europa.

Het doel van de NIS is om een cyberbeveiligingsnorm voor de Europese lidstaten te stellen en de onderlinge samenwerking van de lidstaten op het gebied van cyberbeveiliging te vergroten. Hierbij wordt met name gedoeld op bedrijven die werkzaam zijn in sectoren die als ‘essentieel’ worden gekenmerkt. Je moet hierbij denken aan gezondheidszorg, nutsbedrijven en de financiële sector.

Op 4 juni 2025 is het wetsvoorstel voor de Cyberbeveiligingswet ingediend bij de Tweede Kamer. De Cyberbeveiligingswet - Cbw in het kort - is de implementatie van de NIS2-richtlijn in Nederland. Daarmee is het traject gestart om de NIS2-richtlijn om te zetten in nationale wetgeving.

Nadat de Tweede en Eerste Kamer akkoord hebben gegeven, zal de Cyberbeveiligingswet in werking treden. Dit zal naar verwachting in nog in 2026 gebeuren, maar het hangt nog af van wanneer de wet in de Kamers wordt behandeld.

NIS versus NIS2

De NIS2-richtlijn is de opvolger van de NIS-richtlijn die tien jaar geleden werd geïntroduceerd. De nieuwe richtlijn (EU 2022/2555) vervangt de originele NIS.

Het grootste verschil is dat naast de organisaties die als 'essentieel' worden beschouwd, nu ook organisaties worden opgenomen die als 'belangrijk' worden gekenmerkt en eveneens aan bepaalde verplichtingen moeten voldoen. Dit betekent dat meer middelgrote en grote bedrijven binnen de definitie van de richtlijn vallen.

Bovendien kunnen overheden ook kleinere bedrijven met een hoog beveiligingsrisico verplichten om hieraan te voldoen.

De NIS2 heeft bovendien de minimale beveiligingsmaatregelen duidelijker gedefinieerd waar organisaties aan moeten volden (risicomanagement). Zo moeten bedrijven nu ook potentiële risico's van hun toeleveringsketen in kaart brengen.

Criteria

Zoals gezegd vallen organisaties automatisch onder de NIS2-richtlijn als zij volgens bepaalde criteria 'essentiële' of 'belangrijke' diensten leveren. Hierbij is het belangrijk dat 'automatisch' betekent dat de NIS2-richtlijn lidstaten niet de keuzevrijheid geeft om te bepalen wie onder de richtlijn valt.

Verplichtingen van de Cyberbeveiligingswet en nadere regelgeving gelden voor deze organisaties direct zodra de wet in werking treedt.

Bedrijven moeten nu ook potentiële risico's van hun toeleveringsketen in kaart brengen

NIS2: voor wie geldt de nieuwe wet?

De NIS2-richtlijn van de Europese Unie wordt momenteel door de Europese lidstaten omgezet naar nationale wetgeving. In Nederland wordt de richtlijn, die is gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten, geïmplementeerd in de Cyberbeveiligingswet (Cbw). Organisaties moeten op tijd beoordelen of zij onder de Cyberbeveiligingswet vallen, want zij zijn zelf hiervoor verantwoordelijk.

De impact van NIS2 voor organisaties en bedrijven is groot, met name omdat er meer bedrijfstakken onder de nieuwe NIS2-richtlijn vallen dan voorheen het geval was. Indien een organisatie onder de richtlijn valt, heeft deze de verplichting zich te registreren. Het is voor organisaties van groot belang om te beoordelen of en hoe zij getroffen worden door de nieuwe NIS2-richtlijn.

Vallen wij onder de Cyberbeveiligingswet?

Omdat de NIS2 en de omzetting daarvan in de Nederlandse Cyberbeveiligingswet een flinke uitbreiding betekent voor bedrijven die onder de wet gaan vallen, is het belangrijk dat organisaties gaan beoordelen of zij binnen de wet vallen en in welke hoedanigheid.

De Cbw deelt organisaties in twee categorieën in: in essentiële entiteiten en belangrijke entiteiten.

Essentiële entiteit

Essentiële entiteiten staan onder proactief toezicht: de naleving van verplichtingen wordt actief gecontroleerd, ook als er geen incidenten zijn.

Belangrijke entiteit

Belangrijke entiteiten vallen onder reactief toezicht: de controles vinden vooral achteraf plaats, bijvoorbeeld naar aanleiding van signalen van niet-naleving of na een incident. Zoals in het stroomschema op de volgende pagina te zien is, zijn ook hier enkele uitzonderingen van toepassing.

Beoordelen of je organisatie onder de Cbw valt

Veel organisaties vallen onder de aankomende Cyberbeveiligingswet. De organisaties dragen zelf de verantwoordelijkheid om te beoordelen of zij onder deze wet vallen of niet.

Je kunt in enkele stappen controleren of je organisatie tot een essentiële of een belangrijke sector wordt gerekend.

Sectoren

Als eerste stap moet je controleren of je organisatie onder een van de sectoren valt waar de Cyberbeveiligingswet van op toepassing is. In bijlage 1 en 2 van de wet worden gedetailleerde overzichten gegeven van de sectoren en de daaronder vallende soorten entiteiten.

Een kort overzicht van entiteiten biedt het schema op de volgende pagina.

Voorbeelden van sectoren die vallen onder essentiële (Bijlage 1) of belangrijke (Bijlage 2) entiteiten.

Omvangscriteria

Naast dat je moet controleren of jouw organisatie onder een van de sectoren valt zoals deze genoemd staan in bijlage 1 of bijlage 2 van de Cyberbeveiligingswet, speelt ook de omvang van het bedrijf een rol (de zogenaamde size cap). Je moet hiervoor onder andere kijken naar het aantal werknemers, de jaaromzet en het balanstotaal.

Altijd onder de Cbw

Aanbieders van openbare elektronische communicatienetwerken en -diensten, verleners van vertrouwensdiensten, aanbieders van registers voor topleveldomeinnamen, DNS-dienstverleners, verleners van domeinnaamregistratiediensten en overheidsorganisaties vallen altijd onder de Cyberbeveiligingswet – ongeacht hun omvang.

Essentieel of belangrijk

Wanneer jouw organisatie onder bijlage 1 of bijlage 2 van de Cbw valt en als je hebt beoordeeld wat de omvang van jouw organisatie is (groot, middelgroot, klein), moet je nog vaststellen of jouw organisatie kwalificeert als een essentiële entiteit of als een belangrijke entiteit.

Bij de eerdere wetgeving waren vooral bedrijven betrokken die als essentieel werden beschouwd. De NIS2 betrekt nu ook organisaties die belangrijk zijn.

Het onderscheid is van belang op de manier waarop er toezicht wordt gehouden.

Stroomschema

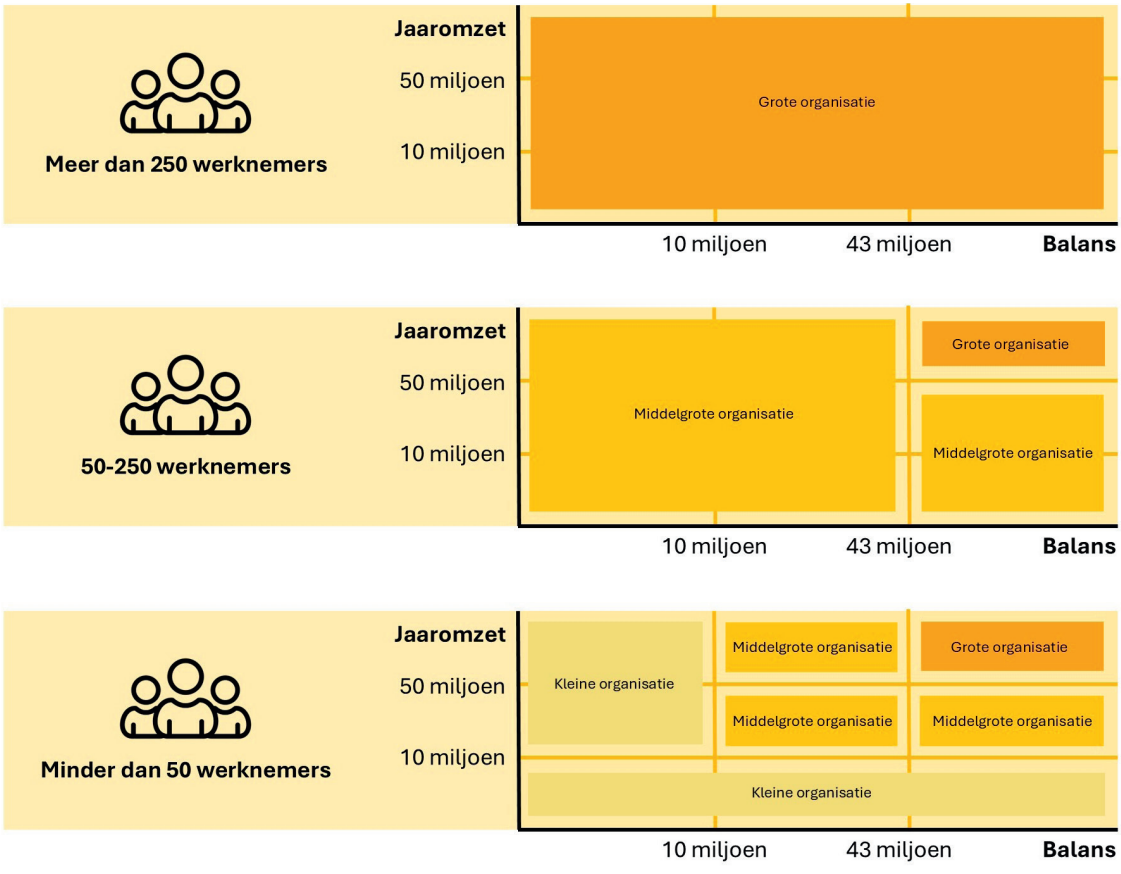
Als je beoordeeld hebt wat de grootte van je organisatie is, kun je met behulp van de stroomschema's (zie verderop) beoordelen of je organisatie onder bijlage 1 (essentiële entiteit) of bijlage 2 (belangrijke entiteit) valt.

Essentiële entiteiten

Grote organisaties in een van de sectoren genoemd in bijlage 1 van de Cyberbeveiligingswet worden aangemerkt als essentiële entiteit.

Daarnaast vallen de volgende organisaties, ongeacht hun omvang, onder deze categorie: centrale en decentrale overheden (zie verdere toelichting hieronder)

- Gekwalificeerde vertrouwensdienstverleners
- Aanbieders van topleveldomeinregisters
- DNS-dienstverleners



Ook middelgrote organisaties die openbare elektronische communicatienetwerken of -diensten aanbieden, worden als essentiële entiteit beschouwd.

Belangrijke entiteiten

Middelgrote organisaties in sectoren uit bijlage 1 die niet als essentiële entiteit kwalificeren worden aangemerkt als belangrijke entiteit.

Daarnaast gelden als belangrijke entiteit:

- Middelgrote en grote organisaties in sectoren genoemd in bijlage 2
- Aanbieders van openbare elektronische communicatienetwerken of -diensten en vertrouwensdiensten, ook als die klein of micro zijn

Overheidsinstanties

Binnen de centrale overheid worden ministeries (inclusief bijbehorende diensten) en zelfstandige bestuursorganen aangemerkt als essentiële entiteiten.

Binnen de decentrale overheid geldt dit voor provincies, gemeenten, waterschappen en samenwerkingsvormen zoals openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties.

Voor deze instanties is de omvang niet relevant voor de kwalificatie als essentiële entiteit.

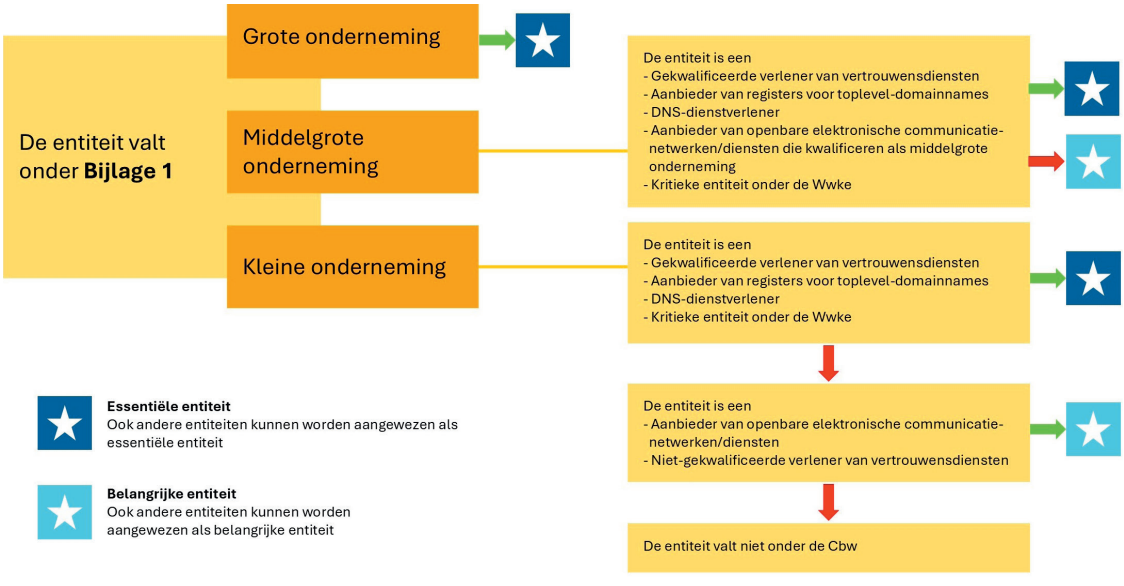
De Nederlandse overheid heeft een zelf-evaluatie-tool uitgebracht waarmee je kunt beoordelen of je organisatie onder de Cyberbeveiliginswet valt en hoe je wordt gekwalificeerd. Scan daarvoor de onderstaande QR-code.

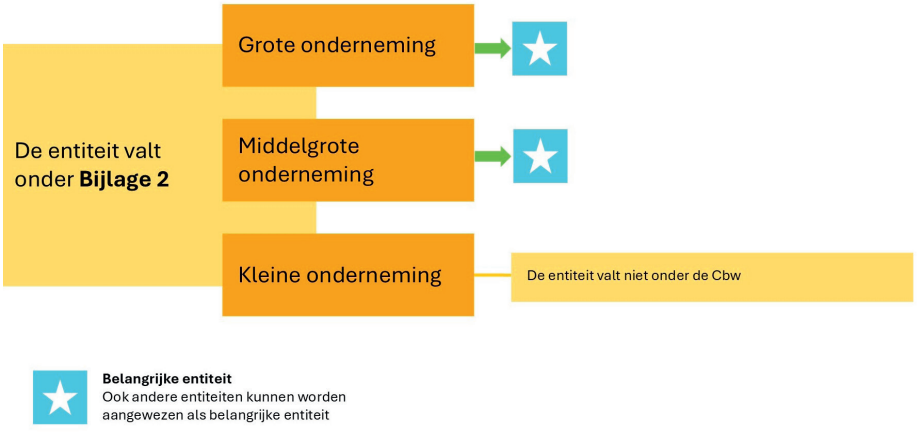
Uitgesloten van de wet zijn overheidsinstanties die zich hoofdzakelijk bezighouden met nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving. Hieronder vallen in ieder geval:

- Het ministerie van Defensie
- De inlichtingen- en veiligheidsdiensten
- Het Openbaar Ministerie
- De politie
- De veiligheidsregio's

Onderwijs

De minister van Onderwijs, Cultuur en Wetenschap kan instellingen voor het hoger onderwijs aanwijzen waardoor zij onder de Cyberbeveiligingswet vallen.





Aan de hand van deze stroomschema's kun je vaststellen of een organisatie kwalificeert als een essentiële entiteit (boven) of als een belangrijke entiteit (onder). Dit is van belang voor de manier waarop er toezicht wordt gehouden.

De verplichtingen van NIS2

De NIS2-richtlijn, die is gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten, wordt in Nederland geïmplementeerd in de Cyberbeveiligingswet (Cbw). Organisaties die onder de Cbw vallen moeten aan enkele verplichtingen voldoen.

Verplichtingen van organisaties

Er zijn drie onderdelen gedefinieerd waar organisaties die onder de Cbw vallen aan moeten voldoen: de zorgplicht, registratieplicht en meldplicht.

Zorgplicht

Organisaties hebben een zorgplicht. Ze moeten dan passende maatregelen nemen om de continuïteit van hun diensten zoveel mogelijk te waarborgen en hun gegevens en informatie te beschermen. Organisaties doen dit op basis van een risicobeoordeling. Momenteel wordt dit nog uitgewerkt, nadere invulling van de zorgplicht voor de overheid zal gebeuren via de Baseline Informatiebeveiliging Overheid (BIO)2.

Bij maatregelen die je organisatie kan nemen, moet je denken aan het formaliseren van het beleid met betrekking tot risicoanalyse, de beveiliging van informatiesystemen en beleid om de effectiviteit van de getroffen maatregelen te analyseren.

Daarnaast moeten organisaties beoordelen hoe de incidentenbehandeling verloopt en de continuïteit (back-upbeheer en herstelplannen, en crisisbeheer) kan worden gewaarborgd.

Nieuw in NIS2 is dat er ook moet worden gekeken naar een effectieve beveiliging van de toeleveringsketen. In de praktijk zal een organisatie afspraken moeten maken met haar rechtstreekse leveranciers of dienstverleners omtrent de beveiliging van systemen en data.

Basispraktijken op het gebied van cyberhygiëne van het personeel en regelmatige training op het gebied van cyberbeveiliging zijn ook van groot belang.

Een overzicht van basisstappen die een organisatie zal moeten nemen vind je verderop.

Registratieplicht

Organisaties die onder de Cbw vallen zijn verplicht zich te registreren en zij moeten gegevens aanleveren voor het entiteitenregister. Organisaties die geregistreerd zijn, ontvangen informatie over cyberdreigingen.

De registratie verloopt via een portaal van het Nationaal Cyber Security Centrum (NCSC). Door zich te registreren geeft een organisatie aan dat deze onder de Cbw valt. De registratie zal pas verplicht zijn na inwerkingtreding van de Cyberbeveiligingswet, maar belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen, kunnen zich nu al op vrijwillige basis registreren bij het NCSC.

Het Nationaal Cyber Security Centrum (NCSC) heeft diverse adviezen ontwikkeld die organisaties kunnen helpen om deze maatregelen te nemen.

Voor meer informatie, scan de QR-code of ga naar www.ncsc.nl

Meldplicht

Indien er in een organisatie een significant cyberincident heeft plaatsgevonden, schrijft de Cyberbeveiligingswet voor dat het incident met worden gemeld bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder van de organisatie. Incidenten worden als significant beschouwd indien ze de continuiteit van de dienstverlening ernstig kunnen verstoren.

Daarbij is het van belang hoeveel mensen worden getroffen, hoe lang het duurt en hoe groot de potentiële schade is die het incident kan opleveren.

Om te voorkomen dat er meerdere malen hetzelfde incident wordt gemeld, dient de melding te gebeuren via het portaal van het Nationaal Cyber Security Centrum. De melding wordt dan automatisch doorgestuurd naar een CSIRT en de toezichthouder.

De meldplicht bestaat uit verschillende stappen:

- Vroegtijdige waarschuwing: de eerste stap is een melding die binnen 24 uur wordt gedaan.
- Vervolgmelding: als tweede stap dient er binnen 72 uur een vervolgmelding te worden gedaan. Deze update bevat aanvullende informatie over het incident, gebaseerd op de eerste melding.
- Eindverslag: de laatste stap is het indienen van een eindverslag. Dit dient uiterlijk een maand na de eerste melding te worden ingediend. Daarin moet een gedetailleerde omschrijving van het incident staan, de ernst ervan en de gevolgen van het incident.

Overigens kunnen organisaties die niet onder de Cbw vallen ook vrijwillige meldingen doen. Die worden niet gedeeld met de toezichthouder.

Aan de slag

De Cyberbeveiligingswet heeft tien zorgplichtmaatregelen geformuleerd waar organisaties ten minste aan moeten voldoen. Organisaties zijn zelf verantwoordelijk voor het vaststellen welke maatregelen passend zijn. Risicomanagement vormt hierbij de basis.

Op de volgende pagina lees je de tien maatregelen om aan de Cbw te voldoen.

10 maatregelen om aan de Cbw te voldoen

1 Maak een risicoanalyse

Een risicoanalyse is een waardevolle eerste stap om de cyberweerbaarheid van je organisatie te versterken. Het geeft inzicht in welke risico's de meeste impact hebben en waar maatregelen het meest nodig zijn. Begin daarom met het in kaart brengen van deze risico's, zodat je gericht kunt verbeteren.

2 Richt incidentrespons in

Incidentrespons beschrijft hoe je handelt tijdens een incident. Door hier vooraf goed over na te denken, voorkom je dat je onder tijdsdruk beslissingen moet nemen. Met een Incident Response Plan (IRP) zorg je ervoor dat je organisatie snel en gecoördineerd kunt reageren. Leg hierin vast hoe je omgaat met cybersecurity-incidenten en hoe je de impact zo klein mogelijk houdt.

3 Uitvalvoorbereiding

Hoe goed je preventieve maatregelen ook zijn, uitval kan niet altijd voorkomen worden. Een goede voorbereiding vergroot de kans dat je organisatie snel weer operationeel is. Denk vooraf na over eventuele herstelmogelijkheden.

4 Een veilige toeleveringsketen

Neem ook risico's in de toeleveringsketen mee in het risicomanagement. Organisaties zijn vaak afhankelijk van leveranciers voor producten en diensten en daardoor deels ook van hun digitale weerbaarheid. Door hier aandacht aan te besteden, verklein je risico's die buiten je directe invloed liggen.

5 Zorg dat cyberhygiëne op orde is

Een sterke basis begint bij goede cyberhygiëne. Door heldere uitgangspunten op te nemen in je cybersecuritybeleid, weet iedereen binnen de organisatie wat er van hen wordt verwacht. Stimuleer veilig gedrag door trainingen en oefeningen aan te bieden. Zo vergroot je het bewustzijn en werk je samen aan een veilige werkomgeving. Een positieve veiligheidscultuur maakt hierbij het verschil.

6 Beveilig netwerk- en informatiesystemen

Zorg dat de netwerk- en informatiesystemen beschermd zijn tegen kwetsbaarheden. Let bij de aanschaf op de ondersteuning door de leverancier en stel duidelijke procedures op voor patchmanagement. Met een laagdrempelig meldpunt kunnen kwetsbaarheden tijdig worden gedeeld.

7 Versterk de beveiliging

Duidelijke afspraken over toegang tot systemen en informatie zijn essentieel. Leg vast wie waar toegang toe heeft en zorg voor goed inzicht in alle assets binnen je organisatie. Bepaal daarnaast voor welke functies screening nodig is, zodat je risico's beheerst en verantwoord met toegang omgaat.

8 Gebruik passkeys voor authenticatie

Overweeg het gebruik van passkeys in plaats van wachtwoorden. Deze moderne techniek, gebaseerd op de FIDO2-standaard, biedt sterke bescherming tegen phishing. Waar wachtwoorden nog nodig zijn, is het verstandig om multifactorauthenticatie toe te passen. Hiermee voeg je een extra beveiligingslaag toe door meerdere verificatiestappen te gebruiken.

9 Stel cryptografiebeleid op

Bescherm gevoelige gegevens door gebruik te maken van encryptie. Leg in een cryptografiebeleid vast waar en hoe je dit toepast. Denk daarbij zowel aan opgeslagen gegevens als aan data die wordt verzonden en ontvangen. Zo zorg je voor een consistente en veilige omgang met informatie.

10 Beoordeel de effectiviteit van maatregelen

Blijf je maatregelen regelmatig evalueren om te zien of ze nog effectief zijn. Door dit bijvoorbeeld jaarlijks te doen, houd je grip op risico's, voldoe je aan wet- en regelgeving en ontdek je waar verbeteringen mogelijk zijn. Zo blijf je continu werken aan een sterke en toekomstbestendige beveiliging.

Waarom cybersecurity en NIS2 essentieel zijn

In de voorgaande artikelen heb je kunnen lezen wat NIS2 is, voor wie de richtlijn geldt en welke verplichtingen daarbij horen. Daarmee ontstaat misschien het beeld dat NIS2 vooral een juridische en organisatorische exercitie is. De praktijk toont anders aan: cybersecurity is geen papieren werkelijkheid, maar essentieel voor de continuïteit van bedrijven.

Als de digitale infrastructuur van je bedrijf niet goed is beveiligd, kan dat verstrekkende gevolgen hebben. Wat gebeurt er als je je cybersecurity niet op orde hebt? En waarom maakt NIS2 dat vraagstuk urgenter?

Aan de hand van het praktijkverhaal van ondernemer Xander wordt duidelijk hoe snel een incident kan escaleren en welke gevolgen dat heeft. Hij had een goed lopend reclamebureau met acht medewerkers en anderhalf miljoen euro omzet. Een cyberaanval veranderde zijn wereld echter van de ene op de andere dag.

Van abstract risico naar concreet incident

Cyberdreigingen worden vaak als abstract gezien. Veel ondernemers weten dat ransomware, phishing en datalekken bestaan, maar beschouwen die risico's als iets dat vooral 'anderen' treft. Die afstand verdwijnt zodra een incident zich daadwerkelijk voordoet.

Ondernemer Xander raakte zijn bedrijf, zijn huis en zijn huwelijk kwijt na een cyberaanval.

Het verhaal van ondernemer Xander laat dat scherp zien. Hij dacht "wat heeft een hacker te zoeken bij een reclamebureau", maar zijn bedrijf werd toch getroffen door een cyberaanval.

Daarmee kregen de aanvallers toegang tot de servers waarop alle bedrijfsgegevens stonden. Wat volgde was geen enkelvoudig geïsoleerd IT-probleem, maar een kettingreactie die het hele bedrijf raakte.

Hij zag op een ochtend de mappen op zijn servers verdwijnen. De stekker eruit trekken bleek geen uitkomst te bieden. De servers waren leeg gehaald, alle data bleek verdwenen en bedrijfsprocessen kwamen stil te liggen.

De impact beperkte zich niet tot IT: ook klanten, leveranciers en financiële stromen werden geraakt.

Xander omschrijft het achteraf als een wake-upcall, juist omdat hij - zoals veel ondernemers - dacht dat zijn maatregelen 'voldoende' waren.

Dit soort incidenten maakt duidelijk waar NIS2 in de kern om draait: het verkleinen van reële risico's die directe gevolgen hebben voor bedrijfsvoering en maatschappij.

Stilstand kost direct geld

Een van de eerste gevolgen van een cyberincident is operationele stilstand. Waar traditionele risico's zoals brand of stroomuitval vaak zichtbaar en tastbaar zijn, manifesteert een cyberaanval zich digitaal - maar met vergelijkbare impact.

Bij Xander betekende de aanval dat systemen lange tijd niet bruikbaar waren. Uitgevoerd werk moest opnieuw gedaan worden, opdrachten konden niet verwerkt worden, communicatie liep vast en medewerkers konden hun werk niet uitvoeren.

In sectoren waar digitale systemen de kern van de operatie vormen, leidt dit vrijwel direct tot omzetverlies.

De directe schade liep bij Xander al snel op tot bijna

driehonderdduizend euro aan gemiste inkomsten en herstelkosten. Daarna groeide het bedrag naar een half miljoen doordat het team maandenlang nauwelijks aan klantwerk toekwam.

Maar ook als de bedrijfsactiviteiten zelf niet digitaal zijn, kunnen ze vaak niet worden uitgevoerd als de digitale infrastructuur wegvalt.

Dat sluit aan bij de zorgplicht die de NIS2: organisaties moeten volgens de richtlijn zelf maatregelen nemen om de continuïteit van hun diensten te waarborgen.

In de praktijk betekent dit dat systemen niet alleen beveiligd moeten zijn, maar ook dat er herstelmogelijkheden aanwezig zijn. Back-ups, failover-structuren en incidentresponsplannen zijn geen formaliteit, maar essentieel om downtime te beperken.

Zonder dergelijke maatregelen verandert een incident al snel in een langdurige verstoring met directe financiële gevolgen.

Data is vaak niet meer terug te halen

Een tweede, vaak onderschat gevolg is dataverlies. In het geval van ransomware worden bestanden versleuteld en pas na betaling (mogelijk) vrijgegeven. Maar zelfs dan is herstel niet gegarandeerd, je moet tenslotte op de eerlijkheid van een criminele organisatie vertrouwen.

In de praktijkcase van Xander bleek zo goed als alle data onherstelbaar verloren. Back-ups waren eveneens aangetast. Dit is een herkenbaar patroon: back-ups bestaan vaak wel, maar blijken bij een incident niet bruikbaar of onvoldoende getest.

Ondanks dure datarecovery bleken bestanden beschadigd en ontbraken essentiële metadata zoals bestandsnamen en mappenstructuur.

NIS2 adresseert dit expliciet door organisaties te verplichten om hun bedrijfscontinuïteit en herstelvermogen te organiseren. Dat betekent onder andere:

- Gescheiden en offline back-ups
- Periodieke tests van herstelprocedures
- Duidelijke prioriteiten in welke systemen eerst moeten worden hersteld

Zonder deze maatregelen wordt een incident niet alleen een tijdelijke verstoring, maar kan het blijvende schade veroorzaken.

Reputatieschade en verlies van vertrouwen

Naast directe financiële schade speelt reputatie een grote rol. Klanten en partners verwachten dat hun gegevens veilig zijn en dat dienstverlening betrouwbaar blijft. Wanneer dat vertrouwen wordt geschaad, heeft dat vaak langdurige gevolgen.

In de praktijk betekent een incident dat:

- Klanten mogelijk overstappen naar concurrenten
- Partners aanvullende eisen stellen
- Nieuwe opdrachten uitblijven

In het geval van het incident bij Xander betekende het dat klanten het vertrouwen verloren. Opdrachten gingen verloren en relaties kwamen onder druk te staan.

Zoals hij zelf aangeeft, zit de grootste schade uiteindelijk niet alleen in geld, maar in vertrouwen: klanten zoeken een andere partij als je dienstverlening stilvalt.

Het verlies van vertrouwen leverde zo mogelijk nog meer schade op dan het incident zelf. Uiteindelijk liep de totale schade op tot meer dan anderhalf miljoen euro, doordat gemiste omzet, niet-declarabele uren, klantverlies en reorganisatiekosten zich bleven opstapelen.

NIS2 legt daarom ook nadruk op transparantie en meldplicht. Incidenten moeten tijdig worden gemeld, zodat betrokken partijen geïnformeerd zijn en risico's kunnen beperken.

Dit voorkomt niet alleen verdere schade, maar dwingt organisaties ook om communicatieprocessen vooraf goed in te richten.

De keten is zo sterk als de zwakste schakel

Een belangrijk verschil tussen de oorspronkelijke NIS-richtlijn en NIS2 is de nadruk op de toeleveringsketen.

Cybersecurity stopt niet bij de eigen organisatie. Aanvallers komen vaak binnen via via leveranciers of gekoppelde systemen.

Denk daarbij bijvoorbeeld aan:

- Externe IT-dienstverleners
- Softwareleveranciers
- Partners met toegang tot systemen

Als één partij in de keten onvoldoende beveiligd is, kan dat gevolgen hebben voor alle aangesloten organisaties. Het is dus belangrijk betrouwbare partners te kiezen voor bijvoorbeeld de internettoegang van je bedrijf.

Daarom verplicht NIS2 organisaties om ook risico's in de keten in kaart te brengen en afspraken te maken met leveranciers. In de praktijk betekent dit bijvoorbeeld:

- Security-eisen opnemen in contracten
- Leveranciers beoordelen op hun beveiligingsniveau
- Toegang tot systemen beperken en monitoren

Het incident van Xander laat zien dat dit geen theoretisch risico is. Ondanks investeringen in beveiliging en beheer bleek één aanval voldoende om alle systemen plat te leggen.

Fatale consequenties

Naast operationele en reputatieschade introduceert NIS2 ook duidelijke juridische consequenties. Organisaties die onder de Cyberbeveiligingswet vallen, krijgen te maken met toezicht en mogelijke sancties.

De boetes kunnen oplopen tot miljoenen euro's of een percentage van de wereldwijde omzet. Daarnaast kunnen bestuurders persoonlijk aansprakelijk worden gesteld bij nalatigheid.

Dit verandert cybersecurity van een IT-aangelegenheid naar een bestuursverantwoordelijkheid. Beslissingen over beveiliging, investeringen en risicomanagement moeten op directieniveau worden genomen.

Voor ondernemers betekent dit dat “we doen al iets aan security” niet langer voldoende is. Er moet aantoonbaar beleid zijn, gebaseerd op risicoanalyse en passende maatregelen.

Die risico’s kunnen groot zijn: ondernemer Xander moest uiteindelijk het faillissement voor zijn bedrijf aanvragen en verloor als gevolgschade zelfs zijn huis en zijn huwelijk.

Waarom juist nu actie nodig is

Hoewel de Cyberbeveiligingswet naar verwachting in 2026 van kracht wordt, is wachten geen realistische optie. Het praktijkvoorbeeld van Xander laat zien dat de risico’s nu al groot zijn.

Bovendien kost het implementeren van de benodigde maatregelen tijd. Denk aan:

- Het uitvoeren van een risicoanalyse
- Het inrichten van incidentrespons
- Het trainen van personeel
- Het aanpassen van processen en contracten

Bedrijven die hier pas mee beginnen wanneer de Cyberbeveiligingswet in werking treedt, lopen het risico achter de feiten aan te lopen. Het praktijkvoorbeeld in dit artikel laat zien waarom dat zo belangrijk is.

Van verplichting naar bedrijfsstrategie

Het is verleidelijk om NIS2 te benaderen als een compliancevraagstuk: voldoen aan regels om boetes te voorkomen. In de praktijk is dat een te beperkte benadering. Het voorbeeld van Xander, maar ook hacks bij andere bedrijven laten zien dat cybersecurity direct samenhangt met:

- Continuïteit van de bedrijfsvoering
- Betrouwbaarheid richting klanten
- Positie in de keten
- Financiële stabiliteit

Een cyberincident kan niet alleen tot stilstand leiden, maar zelfs tot faillissement zoals bij het bedrijf van Xander.

Tot slot

Cybersecurity is veel meer dan een theoretisch risico, je moet NIS2 dan vooral ook niet reduceren tot een administratieve verplichting. De praktijk laat zien dat een incident snel kan leiden tot stilstand, dataverlies en reputatieschade.

Het verhaal van ondernemer Xander maakt duidelijk hoe groot de impact kan zijn: van tonnen directe schade tot een faillissement en persoonlijk verlies.

Voor ondernemers betekent dit dat cybersecurity een integraal onderdeel moet worden van de bedrijfsvoering. Niet alleen om te voldoen aan wetgeving, maar om te voorkomen dat één incident de continuïteit van de organisatie in gevaar brengt.

Voor bedrijven zonder eigen cybersecurity-afdeling kan het verstandig zijn hiervoor een betrouwbare partner te zoeken.

COLOFON

C'T IN SAMENWERKING MET vodafone business

DIT IS EEN UITGAVE VAN F&L MEDIA BV

MET MEDEWERKING VAN

Puck Boone, Daniel Dupré, Susan Gerbrands, Tom Gerrits, Nick Groenewold, Elwin Hodžić, Noud van Kruysbergen, Skip Lelieveldt, Carlijn Masselink, Mylène Nales, Alieke van Sommeren, Marco den Teuling

CONTACT
redactie@ct.nl