Wat is NIS2 en wat betekent het voor jouw organisatie?

CaptureTech

Wat is NIS2 en wat betekent het voor jouw organisatie?

Omdat we steeds meer afhankelijk worden van digitale voorzieningen en netwerken kunnen phishing, ransomware aanvallen en malware een grote impact hebben op een samenleving. Ook bij de wetgevers in Brussel is dit niet onopgemerkt voorbij gegaan en staat cybersecurity inmiddels hoog op de agenda. Daarom heeft het Europees Parlement besloten de bestaande NIS richtlijn nieuw leven in te blazen en komt met de NIS2.

NIS2 in het kort

- De Europese richtlijn voor Cyber Security
- Heeft aangescherpte beveiligingseisen
- Van toepassing op meer organisaties
- De NIS2 legt sancties op bij het niet nakomen

European Parliament

Wat is het verschil tussen de NIS1 & NIS2?

NIS2 breidt zijn toepassingsgebied uit naar middelgrote en kleine organisaties binnen de relevante sectoren, in tegenstelling tot NIS1, dat alleen van toepassing was op grote organisaties. De meldingsdrempels voor incidenten zijn verlaagd onder NIS2, waarbij een groter scala aan incidenten nu verplicht moeten worden gemeld.

De herziening van de richtlijn is niet zonder reden: NIS2 sluit beter aan bij de actuele ontwikkelingen en de groeiende bedreiging van cyberaanvallen. Deze nieuwe versie is van toepassing op een bredere groep organisaties, naast de vitale sectoren, waaronder ook ICT-dienstverleners, de maakindustrie en organisaties die een cruciale rol spelen in vitale toeleveringsketens. Daarnaast introduceert NIS2 een meldplicht voor cyberincidenten, en lidstaten worden verplicht om de naleving te controleren, met zelfs proactieve controles voor de meest vitale organisaties.

Voor wie geldt de NIS2?

1. Essentiële organisaties
2. Belangrijke organisaties
3. Ketenpartners van essentiële of belangrijke organisaties
4. Kleine bedrijven die vallen onder de uitzondering (strategische doelwitten)
5. Apart aangewezen organisaties

NIS2 Zelfevaluatie

De overheid heeft een handige online tool ontwikkeld waarmee je voor jouw organisatie bepaalt:

- Is de NIS2-richtlijn van toepassing op de organisatie?
- Is de organisatie Essentieel of Belangrijk?
- Valt de organisatie onder Nederlands toezicht?
  Link: **https://regelhulpenvoorbedrijven.nl/NIS-2-NL/**

Essentiële organisaties

Deze categorie omvat substantiële organisaties die een cruciale functie vervullen in de samenleving. 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.

- Energie
- Vervoer
- Bankwezen
- Infrastructuur voor de financiële markt
- Drinkwater
- Afvalwater
- Digitale infrastructuur
- Beheer van ICT-diensten
- Gezondheidszorg
- Overheid
- Ruimtevaart

Een opmerkelijk verschil met de oorspronkelijke NIS-richtlijn betreft de benadering van nalevingscontroles. Organisaties binnen de categorie 'essentieel' kunnen proactieve, willekeurige inspecties verwachten.
Dit betekent dat ze te allen tijde, zonder specifieke aanleiding, moeten kunnen aantonen dat ze aan de wettelijke vereisten voldoen. Als een organisatie na controle niet aan de richtlijn voldoet, heeft de sectorale toezichthouder de bevoegdheid om een boete op te leggen. Voor essentiële organisaties bedraagt deze boete minimaal 10 miljoen euro of 2% van de wereldwijde jaaromzet.

Belangrijke organisaties

Naast de essentiële entiteiten benadrukt NIS2 ook de relevantie van belangrijke entiteiten. Deze omvatten middelgrote organisaties binnen de essentiële entiteiten of actief in een van de zes aanvullende sectoren. Met 'middelgroot' verwijst de richtlijn naar organisaties met minimaal 50 werknemers, of een jaarlijkse omzet of balanstotaal van meer dan 10 miljoen euro, maar met minder dan 250 werknemers en een omzet van maximaal 50 miljoen euro.

- Post- en koeriersdiensten
- Afvalstoffenbeheer
- Levensmiddelen (voeding)
- Maakindustrie (vervaardiging/manufacturing)
- Chemische stoffen
- Onderzoek
- Digitale aanbieders

Ook organisaties die worden geclassificeerd als 'belangrijk' moeten zich aan de NIS2-richtlijn houden. Echter, voor hen zijn proactieve inspecties niet verplicht. Ze worden alleen gevraagd om aan te tonen dat ze aan de wettelijke vereisten voldoen wanneer er duidelijke aanleiding is, meestal als gevolg van een (ernstig) cyberincident in de praktijk.

Ketenpartners

Een extra categorie van organisaties die moeten voldoen aan de NIS2-wetgeving omvat diegenen die deel uitmaken van het kernproces van de toeleveringsketen van een essentiële of belangrijke organisatie. Dit impliceert dat jouw leveranciers of dienstverlenende partners, zelfs als ze niet actief zijn in eerdergenoemde sectoren of minder dan 50 medewerkers hebben, en daarom niet worden gelabeld als 'essentieel' of 'belangrijk', toch moeten voldoen aan NIS2.

De EU heeft deze categorie niet zonder reden toegevoegd. In het verleden zijn namelijk verschillende grootschalige cyberaanvallen op organisaties in vitale sectoren gestart bij een partner in de keten. Het is dus van cruciaal belang dat ook zij hun beveiliging op orde hebben. Dit betekent dat wanneer we spreken over essentiële of belangrijke bedrijven, hun toeleveranciers ook allemaal onder de NIS2-regelgeving vallen.

Uitgezonderde kleine bedrijven

Een aantal kleine bedrijven valt niet binnen de eerder genoemde categorieën, maar moet toch voldoen aan de NIS2-wetgeving. Dit geldt met name voor bedrijven die een cruciale rol spelen in de infrastructuur van het internet en daardoor strategische doelwitten zijn voor cyberaanvallen. Voorbeelden hiervan zijn bedrijven die toplevel-domeinnamen beheren, aanbieders van domeinnaamregistratiediensten, of leveranciers van openbare communicatienetwerken of -diensten. Ook overheidsinstanties in deze sectoren vallen automatisch onder de NIS2-richtlijn.

Automatische toepassing

Als jouw organisatie actief is in een van de genoemde categorieën, ben je automatisch verplicht om te voldoen aan NIS2. Dit markeert een significant verschil met de initiële versie van NIS, waarbij expliciete aanwijzing door een ministerie vereist was. Deze vereiste is nu niet langer van toepassing.

"Met de **opkomst van NIS2** groeit de **noodzaak voor organisaties** om hun **cybersecuritymaatregelen** te **versterken**. Bij **CaptureTech** staan we **klaar om onze klanten** te begeleiden en te **ondersteunen** bij het **voldoen** aan deze **wetgeving**, zodat ze **optimaal beschermd** zijn tegen cyberdreigingen."

Mike Warbie
Cyber Security Consultant bij CaptureTech

Boetes bij het niet naleven

Indien een organisatie na controle niet aan de richtlijn voldoet, heeft de sectorale toezichthouder de bevoegdheid om een boete op te leggen. Lidstaten hebben de autonomie om de hoogte van deze boete te bepalen, passend bij de aard en ernst van de nalatigheid. De boetes voor de meest ernstige gevallen van nalatigheid worden als volgt vastgesteld (waarbij de minimale boete altijd het hoogste bedrag van de gegeven keuzes is):

- Voor essentiële organisaties: minimaal 10 miljoen euro of 2% van de wereldwijde jaaromzet.
- Voor belangrijke organisaties: minimaal 7 miljoen euro of 1,4% van de wereldwijde jaaromzet.

Hoofdelijke aansprakelijkheid

Een opvallende verandering in de NIS2-wetgeving is dat alle bestuurders persoonlijk verantwoordelijk en hoofdelijk aansprakelijk zijn voor de naleving ervan. Niemand kan zich achter de beslissingen of nalatigheid van anderen verschuilen. NIS2 is dus relevant voor alle leden van de directie.

Kernprincipes van NIS2

NIS2 legt specifieke verplichtingen op aan bepaalde organisaties, die over het algemeen in twee hoofdaspecten kunnen worden onderverdeeld:

Zorgplicht

Deze plicht vereist dat de organisatie passende veiligheidsmaatregelen neemt om de digitale veiligheid en de continuïteit van haar dienstverlening te waarborgen. NIS2 specificeert niet precies welke technologieën of oplossingen organisaties moeten implementeren. De richtlijn benadrukt echter het belang van 'passende en evenredige technische, operationele en organisatorische maatregelen', waarbij rekening wordt gehouden met de stand van de techniek.

Meldplicht

Organisaties moeten binnen een maand na een incident een eindverslag indienen. Dit verslag bevat onderzoeksresultaten, de gevolgen van de aanval en de genomen maatregelen om herhaling te voorkomen. De organisaties moeten dit rapport indienen bij de relevante autoriteit, op dit moment het Nationaal Cyber Security Centrum (NCSC).

Toegevoegde sectoren in de NIS2

NIS 1 en NIS 2

- Energie
- Transport
- Bankwezen
- Infrastructuur financiële markten
- Gezondheidszorg
- Drinkwater
- Digitale infrastructuur
- Digitale dienstverlening

NIS 2 aanvullende sectoren

- Levensmiddelen
- Maakindustrie
- Post & Koeriersdiensten
- Openbare elektronische communicatienetwerken
- ICT-dienstverlening
- Afvalwater
- Afvalstoffenbeheer
- Overheidsdiensten
- Ruimtevaart
- Onderzoek
- Chemische stoffen

Valt jouw organisatie in één van deze sectoren?

Nee → Levert jouw organisatie aan één van deze sectoren?

Ja → Heeft jouw organisatie minder dan 50 werknemers?

Ja → Nee, je bent niet verplicht om te voldoen aan NIS2

Nee → Heeft jouw organisatie minder dan 10 miljoen euro omzet?

Ja → Ja, je bent verplicht om te voldoen aan NIS2

Nee → Ja, je bent verplicht om te voldoen aan NIS2

Ja → Ja, je bent verplicht om te voldoen aan NIS2

Nee → Levert jouw organisatie een belangrijke rol in de infrastructuur van het internet of de overheid?

Ja → Ja, je bent verplicht om te voldoen aan NIS2

Nee → Nee, je bent niet verplicht om te voldoen aan NIS2

Wat betekent de NIS2 voor Operational Technology (OT)?

Operationele omgevingen (OT) zijn even kwetsbaar als het midden- en kleinbedrijf (MKB) op het gebied van veiligheid. Ondanks de aanzienlijke aandacht die wordt besteed aan IT-cybersecurity, wordt vaak vergeten om het bewustzijn van de cybersecurity in operationele omgevingen te vergroten, terwijl cyberaanvallen op fabrieken en industriële bedrijven desastreuze gevolgen kunnen hebben.

De kwetsbaarheid van OT-netwerken wordt veroorzaakt door verschillende factoren, waaronder het feit dat deze omgevingen 10 tot 15 jaar achterlopen op het gebied van cybersecurity in vergelijking met IT-omgevingen, waardoor ze vaak ontbreken aan ingebouwde beveiliging. Veel industriële bedrijfsnetwerken zijn nog steeds gebaseerd op "platte" architecturen, wat betekent dat één blootgelegde kwetsbaarheid toegang kan verschaffen tot het gehele netwerk. Het vraagstuk van het beheer van OT-beveiliging blijft onopgelost, met onduidelijkheid over verantwoordelijkheden en effectieve samenwerking met IT-beveiligingsmanagers. Ook is de remote toegang tot OT-systemen sterk toegenomen tijdens de COVID-19-pandemie, wat vaak resulteert in slecht beveiligde verbindingen met de buitenwereld.

Het is niet vreemd dat OT-systemen ook onder NIS2 vallen. Ze zijn te vinden in een groot aantal sectoren en voeren een breed scala aan taken uit, variërend van het bewaken van kritieke infrastructuur (CI) tot het besturen van robots op een productievloer. Steeds vaker zien we dat OT-systemen worden gekoppeld aan IT-systemen waardoor er efficiënter gewerkt kan worden. Operationele processen worden dan ook in rap tempo geautomatiseerd en gedigitaliseerd. Allerlei data over deze processen worden verzameld en vormen de belangrijkste input om de productie te optimaliseren. Ze worden nauwkeurig en automatisch geanalyseerd en gebruikt om voorspellingen te doen over de performance, onderhoud, degradatie en efficiency. Bedrijven die data analyses, big data en machine learning modellen gebruiken om trends te herkennen, verbeteringen te signaleren en updates door te voeren, zijn sneller en beter in staat om hun performance te optimaliseren.

Echter brengt dit ook de nodige cyberrisico's met zich mee. Het ongemerkt openzetten van de achterdeur in OT-systemen kan gevaarlijke situaties veroorzaken en een enorme maatschappelijke impact hebben. Veel operationele technologie ondersteunt immers onze vitale infrastructuur. Denk aan drinkwatervoorzieningen, elektriciteitsnetten, olie en gasvoorzieningen, de infrastructuur van onze communicatie en het openbaar vervoer. Een strategische cyberaanval kan tot grote maatschappelijke verstoringen leiden.

Het is van groot belang dat deze kwetsbaarheden serieus worden genomen en dat er passende maatregelen worden genomen om de cybersecurity van OT-systemen te versterken. Dit omvat onder meer het implementeren van strikte toegangscontrole, regelmatige audits van systemen en processen, het updaten van verouderde systemen en het creëren van duidelijke verantwoordelijkheden voor OT-beveiliging binnen organisaties.

Conclusie

In het licht van deze ontwikkelingen is duidelijk dat NIS2 een belangrijke mijlpaal is voor cybersecurity in Europa. Het dekt meer sectoren en veel meer organisaties, inclusief hun ketenpartners, legt strengere verplichtingen op en heeft een scherpere handhaving dan voorheen. Ondanks de uitdagingen is dit ook een kans om cybersecurity op een hoger niveau te krijgen.

De Europese NIS2-richtlijn wordt op dit moment omgezet in Nederlandse wetgeving. Het belangrijkste advies is dus om je voor te bereiden en niet te wachten tot de richtlijn van kracht wordt. Neem daarom contact op met onze cybersecurity specialisten voor een volledig advies, toegesneden op jouw situatie. We beoordelen of je onder de NIS2 richtlijn valt, analyseren welke eventuele tekortkomingen er zijn in je huidige cybersecurity strategie, stellen vast welke maatregelen er nodig zijn, en helpen je met de implementatie van ervan.

CaptureTech

Meer informatie

T: +31 (0) 252 241 544
+32 (0) 34 491 159
E: info@capturetech.com

www.capturetech.com

Volg ons:

Connecting **systems**, **data** and **people**