eye.

Bezoek eyesecurity.nl

Een complete guide voor de implementatie van NIS2 in Nederland.

Voorwoord Job Kuijpers

Cyberaanvallen hebben meer impact dan alleen economische schade. Ze vormen een bedreiging voor onze vrije en open samenleving. In het ergste geval verstoort een cyberaanval zelfs het functioneren van ons land.

Alle bedrijven en organisaties spelen een rol in de samenleving. In het licht van de snelle ontwikkelingen rondom cybercriminaliteit besloot de Europese Unie de NIS-richtlijn te hernieuwen. De NIS2 moet de cyberweerbaarheid van Europese organisaties – en daarmee de EU als geheel – verder versterken. Dat geldt zowel voor organisaties die al onder de oude NIS vielen als voor nieuwe sectoren die een cruciale rol spelen in onze samenleving. Tegelijkertijd werkt de EU met wetgeving zoals de Digital Services Act, de Cyber Resilience Act en de Digital Operational Resilience Act om ook platformen, producten en de financiële sector beter te beschermen.

Voor veel organisaties is dit een belangrijke reden om met cybersecurity aan de slag te gaan. Wie niet aan de NIS2 voldoet, loopt straks kans op boetes en andere sancties. Maar dat moet niet de enige reden zijn om maatregelen te nemen. Cybersecurity beschermt niet alleen je bedrijf, je werknemers en je systemen, maar ook je klanten en andere stakeholders – en uiteindelijk de gehele samenleving. Iedereen wil kunnen vertrouwen op goed functionerende diensten en een veilige omgeving voor gevoelige en persoonlijke gegevens.

Dat kan alleen door cybersecuritymaatregelen te nemen. Niet alleen om de kans op een cyberaanval of ander incident te verkleinen, maar ook om effectief te kunnen reageren als het toch misgaat. Het verantwoord melden van een incident helpt bijvoorbeeld om het bewustzijn bij anderen te vergroten en te voorkomen dat we steeds dezelfde fouten maken.

Hoe klein jouw organisatie ook is, je vormt een schakel in een grotere keten. Alleen als iedereen zich inzet, houden we de volledige keten en de samenleving zo veilig mogelijk. Eye Security staat klaar om je daarbij te helpen.

TIJDLIJN NIS2

28 november 2022:
NIS2-richtlijn is vastgesteld door de Europese Raad

januari 2023:
Implementatietermijn van 21 maanden gaat van start. Binnen deze periode moet de richtlijn worden opgenomen in nationale wetgeving

januari 2024:
Minister van Justitie en Veiligheid laat in een kamerbrief weten dat de implementatiedeadline niet gehaald gaat worden

21 mei 2024:
Internetconsultatie van Nederlandse Cyberbeveiligingswet gaat van start

1 juli 2024:
Einde internetconsultatie van de Cyberbeveiligingswet

17 januari 2025:
Organisaties die onder de NIS2 vallen, moeten zich nu geregistreerd hebben

1 juli 2025:
Cyberbeveiligingswet treedt in werking. Organisaties moeten vanaf nu aan de NIS2 voldoen

NIS2: Wat, waarom en wanneer?

De zogenaamde Network and Information Security directive, ofwel de NIS2, is een Europese richtlijn om cybersecurity en weerbaarheid in essentiële en belangrijke diensten in EU-lidstaten te verbeteren. Wat houdt die richtlijn precies in?

De NIS2 volgt de NIS-richtlijn uit 2016 op. Beide richtlijnen zijn bedoeld om cybersecurity bij voor de maatschappij belangrijke bedrijven te verbeteren. Dat doen ze door een aantal beveiligingseisen verplicht te stellen voor bedrijven die door de NIS als essentieel of belangrijk beschouwd worden. Denk daarbij ook aan overheidsdiensten of het bankwezen.

Het aantal cyberdreigingen is de laatste jaren toegenomen en de kans op verstoringen wordt steeds groter. Daarom heeft de Europese Unie gewerkt aan een opvolger van de NIS: de NIS2, die eind 2022 werd aangenomen. Groot verschil met de eerste NIS is dat meer sectoren onder de richtlijn vallen – en dus meer organisaties aan de regels moeten voldoen – en dat er meer verplichtingen komen rondom cybersecurity voor de organisaties die onder de richtlijn vallen.

Dat de NIS2 al op Europees niveau is aangenomen, betekent echter niet dat bedrijven al aan de nieuwe regels moeten voldoen. De richtlijn wordt eerst omgezet naar nationale wetgeving. In Nederland wordt dat de Cyberbeveiligingswet, die 1 juli 2025 van kracht wordt.

Toch is er voor die tijd al actie nodig, onder meer om te zorgen dat je op tijd aan de nieuwe regels rondom cybersecurity voldoet. Zo komt er een nationaal register met daarin alle organisaties die onder de NIS2 vallen. Organisaties moeten zichzelf registreren bij het Nationaal Cyber Security Centrum (NCSC). Registreren is nu al mogelijk via **deze link**, maar dit is voorlopig nog vrijwillig. Pas na de inwerkingtreding van de Cyberbeveiligingswet wordt registratie verplicht.

Wie valt onder de NIS2?

De NIS2 kent twee soorten organisaties die onder de NIS2 vallen: essentiële organisaties en belangrijke organisaties. Het hangt van de sector waarin jouw organisatie opereert, de grootte van jouw bedrijf, je omzet en totale activa af of je aan de NIS2 moet voldoen en in welke van de twee categorieën je dan valt.

De volgende organisaties vallen onder de NIS2:

- **Grote organisaties:** organisaties met minimaal 250 werknemers EN/OF waar sprake is van een jaaromzet van meer dan 50 miljoen euro en een balanstotaal van meer dan 43 miljoen euro. Deze organisaties vallen altijd onder de NIS2 en worden als essentieel gezien, mits zij actief zijn in een bedrijfstak genoemd in Sector 1. Zijn de bedrijfsactiviteiten genoemd in Sector 2 dan wordt de organisatie geclassificeerd als Belangrijk.
- **Middelgrote organisaties:** organisaties met meer dan 50 werknemers EN/OF waar sprake is van meer dan 10 miljoen euro jaaromzet en meer dan 10 miljoen euro aan totale activa. Deze organisaties kunnen onder de NIS2 vallen als zij operationeel zijn in één van de tot belangrijk of essentieel aangemerkte sectoren. In de onderstaande afbeelding is te zien welke sectoren daartoe behoren.
- **Kleine organisaties:** organisaties met minder dan 50 werknemers vallen alleen onder de NIS2 als zij een ministeriële aanwijzing hebben.

Ketenpartners van essentiële of belangrijke organisaties vallen niet onder NIS2, tenzij ze invloed hebben op de digitale beveiliging. Wel kunnen NIS2-gereguleerde organisaties eisen stellen aan hun toeleveranciers.

Of een organisatie wel of niet aan de NIS2 voldoet, is niet altijd gemakkelijk te bepalen. Een goed voorbeeld is de transportsector: een gemiddeld vrachtwagenbedrijf valt niet per se onder de NIS2. Bedrijven in de transportsector worden alleen als essentieel of belangrijk gezien als het om luchtvaartorganisaties gaat of om bedrijven die intelligente vervoerssystemen maken of beheren. Maar transportbedrijven die levensmiddelen of chemische stoffen vervoeren, worden tot de levensmiddelensector of chemische stoffen gerekend en vallen weer wél onder de NIS2.

In de officiële documentatie van de richtlijn staat per genoemde sector een uitgebreide beschrijving van wat voor soort organisaties en bedrijfsactiviteiten onder een sector vallen.

Het is belangrijk om te weten dat organisaties automatisch aan de NIS2 moeten voldoen als zij in de eerdergenoemde categorieën vallen. Een ministerie hoeft organisaties die aan de regels moeten voldoen dus niet expliciet aan te wijzen. Het is aan organisaties zelf om uit te zoeken of zij wel of niet aan de NIS2 moeten voldoen en zich tijdig te registreren.

↘ **Wil je weten of jouw bedrijf onder de NIS2 valt? Doe onze test, gebaseerd op de meest recente informatie die beschikbaar is.**

Waar moet ik aan voldoen?

Nederland is nog druk bezig met het uitwerken van de regels rondom de NIS2. Waar organisaties precies aan moeten voldoen, is dus nog niet helemaal bekend. Veel van regels staan namelijk ook nog niet in de conceptwetgeving. Toch zijn een aantal zaken al wel duidelijk. En die zijn niet alleen van belang om aan de NIS2 te voldoen, maar om überhaupt te zorgen dat het risico op een cyberaanval zo klein mogelijk wordt.

In ieder geval is duidelijk dat organisaties onder de NIS2 moeten voldoen aan een zorgplicht en een meldplicht.

De zorgplicht schetst de belangrijke cyberbeveiligingspraktijken waar ieder bedrijf aan moet voldoen. Denk aan incidentafhandeling, beveiliging van de toeleveringsketen, basis cyberhygiëne en de implementatie van multifactor authentication.

De meldplicht, of incidentrapportage, draait om wat er moet gebeuren als een incident plaatsvindt. Mocht zo'n incident plaatsvinden, dan moet dat binnen 24 uur gerapporteerd worden aan de toezichthouder en het CSIRT dat aan jouw sector is toegewezen. Binnen 72 moet een vervolgreportage komen en na een maand moet een eindrapport worden ingediend.

In Nederland zijn echter nog niet veel gedetailleerde regels bekendgemaakt. Toch is het al wel mogelijk om je meer voor te bereiden en het risico op een cyberaanval zo klein mogelijk te maken. In België werd anderhalf jaar geleden namelijk het Cyber Fundamentals Framework gepubliceerd, waar organisaties die in België onder de NIS2 vallen aan moeten voldoen. Organisaties kunnen deze lijst met eisen gebruiken als voorbeeld om zich voor te bereiden. De kans is groot dat veel van deze maatregelen gaan overeenkomen met de Nederlandse implementatie.

Op de naleving van de NIS2 wordt toezicht gehouden door diverse toezichthouders. Op essentiële organisaties wordt proactief toezicht gehouden. Zij kunnen steekproefsgewijze controles verwachten, waarbij ze moeten kunnen aantonen dat ze aan de wet voldoen. Belangrijke organisaties hebben geen proactieve controles en hoeven alleen aan te tonen dat ze aan de NIS2 voldoen als daar een duidelijke aanleiding voor is.

Wat als ik niet voldoe?

De NIS2 bevat een aantal sancties voor organisaties die niet aan de regels voldoen. Zo kan een toezichthouder een organisatie verplichten om de overtreding in kwestie openbaar te maken en om binnen een bepaalde termijn maatregelen te nemen om alsnog aan de regels te gaan voldoen.

Voor organisaties die als essentieel worden beschouwd, zijn extra maatregelen mogelijk. Zo kan de toezichthouder de rechter verzoeken om de certificering of vergunning op te schorten of om bestuursleden te schorsen. Daarnaast kunnen bestuurders van deze organisaties persoonlijk aansprakelijk worden gesteld.

Tot slot is er een optie om een boete op te leggen. Die boete komt voor essentiële bedrijven neer op maximaal 10 miljoen euro of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar. Belangrijke bedrijven kunnen een boete van maximaal 7 miljoen euro of 1,4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar krijgen.

Deze hoge boetes dienen ook een extra doel. Het geeft bedrijven een business case om uit te werken: wil je je geld uitgeven aan cybercriminelen die je gegevens versleutelen én aan een boete aan een autoriteit omdat je je cybersecurity niet op orde hebt, of investeer je liever een fractie van deze bedragen aan goede cybersecurity? Goede cybersecurity heeft bovendien als voordeel dat het zichzelf terug kan betalen. Het totaalpakket van Eye Security heeft bijvoorbeeld een ROI van 300%.

↘ Meer informatie over de meldplicht en de zorgplicht vind je op de **website van Eye Security**.

Waar begin ik?

Veel is dus nog onduidelijk over de NIS2, waaronder wanneer de regelgeving precies van kracht wordt. Toch wil je als bedrijf nu al stappen zetten. Allereerst omdat het enige tijd kan duren voor je volledig voldoet aan de eisen. Daarnaast omdat dit de kans op cyberaanvallen – en dus financiële en reputatieschade - kleiner maakt. Deze stappen kun je nu al zetten.

1

Controleer of je onder de NIS2 valt

Je kunt nu al controleren of jij onder de NIS2 valt en zo ja, of jouw organisatie essentieel of belangrijk is. Eye Security heeft een **compliancy check** gemaakt waarmee jij kunt zien of je aan de NIS2 moet voldoen.

2

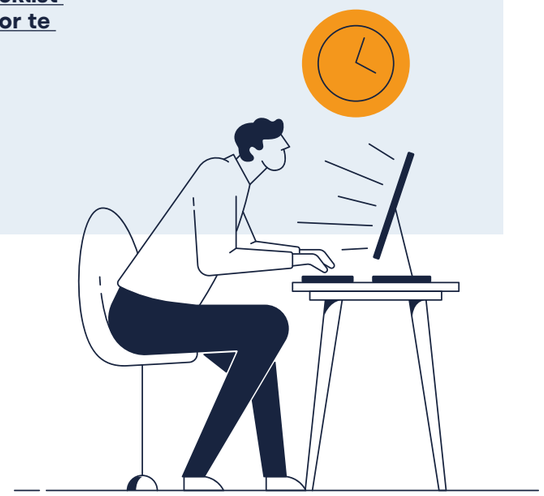
Registreer je organisatie

Organisaties die onder de NIS2 vallen, moeten zich registreren. Weet je niet zeker of dit voor jou geldt? Meld je dan toch aan. Registreren is nu al mogelijk via **deze link**, maar voorlopig nog vrijwillig. Dit wordt pas verplicht na de inwerkingtreding van de Cyberbeveiligingswet. **Download deze checklist om je registratie voor te bereiden.**

3

Controleer hoe compliant jij nu al bent

In aanloop naar de NIS2 kun je al stappen nemen om de cyberweerbaarheid van jouw organisatie te verbeteren. Nieuwsgierig naar hoe compliant en weerbaar je nu al bent? Dat kun je ontdekken via de gratis **NIST-scan** van Eye Security.



Zo kan Eye Security je ondersteunen

Wil je actief aan de slag met de NIS2? Eye Security kan helpen. Niet alleen voldoe je dan aan meer regels van de NIS2, maar je vergroot ook je cyberweerbaarheid en maakt de kans op een incident kleiner.

Eén van de verplichte beveiligingsmaatregelen onder de NIS2 is incidentafhandeling. Eye Security biedt dit als onderdeel van de Managed Extended Detection and Response-dienst. Niet alleen helpen we je bij incident response, maar we monitoren ook jouw endpoints én de cloud om cyberaanvallen te voorkomen.

Daarnaast vereist de NIS2 basis cyberhygiënemaatregelen en -training. Eye Security biedt een optionele Awareness-service, met daarin regelmatige phishing-simulaties en extra training voor medewerkers die in dergelijke e-mails trappen.

Cybersecurity gaat echter verder dan alleen de vereisten uit de NIS2. Wil jij je cyberrisico verlagen? Bekijk dan ons uitgebreide cyberbeschermingspakket of neem **contact met ons op**. We helpen je graag.

↘ Meer weten over de NIS2 en wat Eye Security voor jou kan betekenen? Bekijk onze **NIS2 Resource Hub**.

eye.