Bezoek eyesecurity.be

Een complete guide voor de implementatie van NIS2 in België

Voorwoord Anne Masson

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 cyberweerbaarheid van Europese organisaties en daarmee de EU in zijn geheel verder bevorderen. Dat geldt zowel voor organisaties die onder de oude NIS vielen als voor organisaties die daar nog niet onder vielen, maar wel een belangrijke rol spelen in onze samenleving.

Voor veel organisaties is daarmee een belangrijke reden ontstaan 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 willen nemen. Cybersecurity beschermt niet alleen je bedrijf, je werknemers en jouw systemen, maar ook je klanten en andere stakeholders en uiteindelijk de gehele samenleving. Iedereen wil kunnen vertrouwen op goed doorlopende diensten en een omgeving waarin gevoelige en persoonlijke gegevens veilig blijven.

Dat kun je alleen bieden door cybersecuritymaatregelen te nemen. Niet alleen om de kans op een cyberaanval of een ander incident zo klein mogelijk te maken, maar ook om goed te reageren als er onverhoopt toch iets 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

14 december 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

17 mei 2024: De Belgische overheid publiceert de invoer van de NIS2 richtlijn in een koninklijk besluit.

17 oktober 2024: Inwerkingstreding Belgische NIS2-wet.

17 maart 2025: Organisaties die onder de NIS2 vallen, moeten zich nu geregistreerd hebben bij het CCB.

Q1- 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 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.

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.
- **Ook op uw bedrijf toepasbaar?** De NIS2-richtlijn is gericht op organisaties van een bepaalde omvang die diensten verlenen in kritieke sectoren die zijn opgenomen in de **bijlagen I en II van de richtlijn**. De omvang ("size cap") en de geleverde dienst zijn de twee belangrijkste criteria om te bepalen of de NIS2-richtlijn van toepassing is op een organisatie.

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?

België is volledig klaar met de uitwerking van de regels rondom de NIS2-richtlijn. Om de praktische implementatie van deze maatregelen te vergemakkelijken, adviseert het Centrum voor Cybersecurity België dat alle NIS2-entiteiten gebruikmaken van het CyberFundamentals (CyFun®) Framework.

Dit framework bevat alle vereiste elementen en zorgt ervoor dat een organisatie een vermoeden van conformiteit kan verkrijgen. Het invoeren van CyFun Governance helpt om het risico op een cyberaanval zo klein mogelijk te houden.

Het is alvast duidelijk dat organisaties die onder de NIS2 vallen, moeten voldoen aan een zorgplicht en een meldplicht. De zorgplicht omvat een reeks essentiële cyberbeveiligingsmaatregelen die door elk bedrijf moeten worden genomen. Denk hierbij aan incidentafhandeling, beveiliging van de toeleveringsketen, basis cyberhygiëne en de implementatie van multi-factor authenticatie. Deze maatregelen moeten ervoor zorgen dat de organisatie haar cyberweerbaarheid kan waarborgen en voorbereid is op eventuele incidenten.

Daarnaast geldt ook de meldplicht, die bepaalt wat er moet gebeuren als er een incident plaatsvindt. Zodra een significant incident zich voordoet, moet dit onverwijld en uiterlijk binnen 24 uur gemeld worden aan de bevoegde toezichthouder en het CSIRT dat aan de betreffende sector is toegewezen. Binnen 72 uur moet een verdere rapportage volgen, en uiterlijk één maand na de incidentmelding dient er een eindrapport ingediend te worden. Indien het eindrapport niet kan worden ingediend omdat het incident nog aan de gang is, moet er een voortgangsverslag worden opgemaakt en, zodra het incident is afgehandeld, een eindverslag.

In België werd anderhalf jaar geleden het CyberFundamentals Framework geïntroduceerd, waaraan organisaties die onder de NIS2 vallen moeten voldoen. Dit framework kan als voorbeeld gebruikt worden voor de implementatie van maatregelen om de organisatie voor te bereiden op de verplichtingen van de NIS2. De kans is groot dat veel van deze maatregelen overeenkomen met de implementatie in Nederland. De naleving van de NIS2 wordt gecontroleerd door het Centrum voor Cybersecurity België (CCB).

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 openbaar te maken en om binnen een bepaalde termijn maatregelen te nemen om alsnog aan de regels te voldoen.

Voor organisaties die als essentieel worden beschouwd, kunnen nog strengere maatregelen van toepassing zijn. De toezichthouder kan de rechter verzoeken om de certificering of vergunning van de organisatie op te schorten, of zelfs om bestuursleden te schorsen. Bestuurders kunnen bovendien persoonlijk aansprakelijk worden gesteld wanneer een organisatie in gebreke blijft. Deze persoonlijke aansprakelijkheid betekent dat bestuursleden het risico lopen om zelf verantwoordelijk te worden gehouden voor de schade of gevolgen van het niet voldoen aan de NIS2.

Daarnaast kunnen er aanzienlijke boetes worden opgelegd. Voor essentiële bedrijven kan de boete oplopen tot maximaal 10 miljoen euro of 2% van de totale wereldwijde jaaromzet van het voorgaande boekjaar. Voor belangrijke bedrijven kan de boete oplopen tot 7 miljoen euro of 1,4% van de totale omzet. Deze hoge boetes dienen ook een extra doel. Ze geven bedrijven een business case om te overwegen: wil je je geld uitgeven aan cybercriminelen die je gegevens versleutelen én een boete van de autoriteiten omdat je je cybersecurity niet op orde hebt, of investeer je liever een fractie van deze bedragen in degelijke cybersecurity? Goede cybersecurity heeft bovendien als bijkomend voordeel dat het zichzelf terugbetaalt. 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?

NIS2 is op 17 oktober 2024 ingegaan in België. Dit betekent dat organisaties zich nu moeten registeren. Begin daarna zo snel mogelijk met het nemen van maatregelen. Allereerst omdat het enige tijd kan duren voordat je volledig voldoet aan de eisen. Daarnaast omdat dit de kans op cyberaanvallen – en dus financiële en reputatieschade – kleiner maakt. Deze stappen moet je nu al zetten.

Deze stappen kun je nu al zetten.

1

Controleer of je onder de NIS2 valt.

Doe de **compliance check** van Eye Security en ontdek of jouw organisatie moet voldoen aan de NIS2.

2

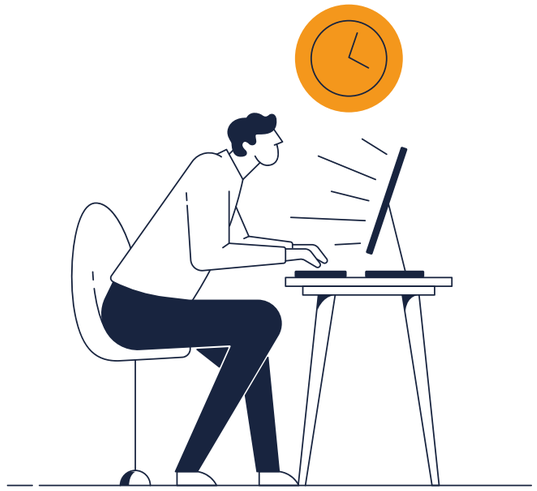
Registreer je organisatie.

Organisaties die onder de NIS2 vallen moeten zich op **deze website** registreren.

3

Gebruik het CyFun Framework voor voorbereiding.

Volg de **richtlijnen van het Centrum voor Cybersecurity België** om je cyberweerbaarheid te versterken.



Zo kan Eye Security je ondersteunen

Wil je je cyberweerbaarheid versterken en voorbereid zijn op mogelijke cyberdreigingen? Eye Security kan je hierbij helpen. Onze diensten bieden een solide basis om risico's te beperken en je organisatie beter te beschermen tegen cyberaanvallen.

Een van de diensten die we aanbieden is **Managed Extended Detection and Response (MXDR)**. Deze dienst omvat niet alleen de afhandeling van incidenten, maar ook de continue monitoring van je endpoints en cloudomgeving om aanvallen vroegtijdig te detecteren en te voorkomen. Dit is een belangrijke stap richting betere bescherming en draagt ook bij aan een deel van de vereisten die worden gesteld binnen de NIS2-richtlijn.

Daarnaast bieden we een **Awareness-service**, waarin we je medewerkers trainen om bewuster om te gaan met cyberveiligheid. Regelmatige phishing-simulaties en extra trainingen helpen medewerkers beter te reageren op bedreigingen en vergroten de algehele veiligheid van je organisatie.

Onze MDR-dienst is een grote stap in de goede richting van NIS2 compliance. Het versterkt niet alleen de cyberweerbaarheid van je organisatie, maar helpt ook bij het voldoen aan enkele belangrijke aspecten van de richtlijn. Wil je de cyberveiligheid van jouw organisatie naar een hoger niveau tillen?

↘ Neem dan **contact met ons op** voor meer informatie over wat wij voor jouw bedrijf kunnen betekenen.

eye.