WHITEPAPER

Alles wat je moet weten over de **NIS2-richtlijn**

EVERSHEDS SUTHERLAND & ESET Digital Security
Progress. Protected.

Inhoudsopgave

Inleiding

Beste lezer,

Bedankt voor het downloaden van onze whitepaper over de NIS2-richtlijn. In deze whitepaper zullen we in gaan op de belangrijkste aspecten van de NIS2-richtlijn en hoe deze van toepassing is op bedrijven in Nederland.

De NIS2-richtlijn, ook wel bekend als de nieuwe versie van de Network and Information Systems Directive, is een Europese richtlijn die gericht is op het versterken van de cyberbeveiliging in de Europese Unie (EU). De richtlijn is ontworpen om bedrijven te helpen zich te beschermen tegen cyberdreigingen en om ervoor te zorgen dat de cyberinfrastructuur van de EU robuust is.

Nu de richtlijn definitief gepubliceerd is krijgen lidstaten 21 maanden de tijd om de bepalingen uit de richtlijn te verweven in de lokale wetgeving.

In deze whitepaper zullen we een overzicht geven van de belangrijkste bepalingen van de NIS2-richtlijn en hoe deze van toepassing zijn op bedrijven in Nederland. We zullen ook ingaan op de verplichtingen die bedrijven hebben om aan de richtlijn te voldoen en hoe wij, ESET in Nederland en Eversheds Sutherland Nederland, daarbij kunnen ondersteunen.

We hopen dat deze whitepaper nuttig zal zijn voor bedrijven die op zoek zijn naar meer informatie over hoe ze zich kunnen beschermen tegen cyberdreigingen en hoe ze aan de NIS2-richtlijn kunnen voldoen.

ESET in Nederland en Eversheds Sutherland Nederland

Wat is de NIS2-richtlijn?

NIS2

Is jouw organisatie middelgroot of groot en actief binnen één van de kritieke sectoren zoals energie, vervoer, gezondheid en digitale infrastructuur? Dan kan nieuwe wetgeving vanuit de EU veel invloed hebben op de eisen voor cybersecurity binnen jouw organisatie. "Deze Europese richtlijn gaat ongeveer 160.000 entiteiten helpen hun greep op de veiligheid te versterken en van Europa een veilige plaats om te leven en om te werken maken. De wet moet ook het delen van informatie met de particuliere sector en partners over de hele wereld mogelijk maken. ''Als we op industriële schaal worden aangevallen, moeten we op industriële schaal reageren", zei de Nederlandse Europarlementariër Bart Groothuis hierover.

Omdat cybersecurity ontzettend belangrijk is voor de bescherming van onze samenleving, heeft de Europese Unie (EU) in 2016 de Directive on Security of Network and Information Systems (NIS Directive) geïntroduceerd. Hoewel deze Europese richtlijn heeft gezorgd voor meer samenhang binnen de EU op het gebied van netwerk- en informatiebeveiliging, moet de cyberweerbaarheid volgens het Europees Parlement nog verder omhoog om de samenleving te beschermen. Met de toenemende digitalisering en grote hoeveelheid cyberaanvallen is de NIS-richtlijn herzien en verbeterd. De NIS2-richtlijn zal dan ook een groter bereik hebben en zich richten op meer sectoren, om op die manier de cyberweerbaarheid van de EU-lidstaten gelijk te trekken en vergroten.

Risicomanagement en samenwerking

Maar hoe gaat deze herziene richtlijn zorgen voor betere cyberweerbaarheid? De NIS2 probeert op verschillende manieren het cybersecurityniveau binnen EU-lidstaten te verbeteren. De richtlijn scherpt opgelegde beveiligingseisen aan, richt zich op het aanpakken van de beveiliging van supply chains (de productie- of toeleveringsketen), het stroomlijnen van rapportageverplichtingen, strengere toezichtmaatregelen en het invoeren van handhavingsvereisten met geharmoniseerde sancties in alle lidstaten. Daarbij wordt ook het belang van informatie delen en (inter)nationale samenwerking op het gebied van crisismanagement benoemd.

Omvang van de NIS2

De NIS2-richtlijn heeft invloed op een stuk meer sectoren dan de oorspronkelijke NIS-richtlijn. De NIS-richtlijn wees alleen Gezondheidszorg, Vervoer, Bankwezen En Financiële Marktinfrastructuur, Digitale Infrastructuur, Watervoorziening, Energie en Digitale Dienst Aanbieders aan met de ruimte voor lidstaten om zelf te definiëren welke organisaties als essentieel bestempeld werden. De NIS2 introduceert uniforme regels voor middelgrote en grote instanties die actief zijn in kritieke sectoren, zoals energie, vervoer, gezondheid en digitale infrastructuur. Hieronder vallen nu onder andere 'zeer kritieke sectoren', waaronder energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, beheer van ICT-diensten (B2B), overheid en ruimtevaart en 'kritieke sectoren', zoals post- en koeriersdiensten, afvalstoffenbeheer, chemicaliën, levensmiddelen, vervaardiging, digitale aanbieders en onderzoek. Alle middelgrote en grote ondernemingen in deze sectoren gaan onder de wetgeving vallen.

Ontdek de classificatie van jouw organisatie

Essentieel of belangrijk?

De manier waarop gehandhaafd zal gaan worden hangt af van de categorie waarin een organisatie valt. Onder de NIS2 zijn er namelijk twee categorieën waaronder organisaties gaan vallen. Organisaties kunnen bestempeld worden als essentieel of als belangrijk. Of een organisatie bestempeld wordt als essentieel of belangrijk hangt af van of de organisatie onder een kritieke of een zeer kritieke sector valt en hangt samen met de bedrijfsgrootte.

BINNEN WELKE SECTOR VALT JOUW ORGANISATIE?

- ENERGIE
- VERVOER
- BANKWEZEN
- GEZONDHEIDSZORG
- DRINKWATER
- AFVALWATER
- DIGITALE INFRASTRUCTUUR
- BEHEER VAN ICT-DIENSTEN (B2B)
- OVERHEID
- RUIMTEVAART
- INFRASTRUCTUUR VOOR DE FINANCIËLE MARKT
- POST- EN KOERIERSDIENSTEN
- AFVALSTOFFENBEHEER
- VERVAARDIGING
- DIGITALE AANBIEDERS
- ONDERZOEK
- VERVAARDIGING, PRODUCTIE EN DISTRIBUTIE VAN CHEMISCHE STOFFEN
- PRODUCTIE, VERWERKING EN DISTRIBUTIE VAN LEVENSMIDDELEN

*** Groot:**
meer dan 250 medewerkers en een jaaromzet van minimaal 50 miljoen euro (of een balanstotaal van minimaal 43 miljoen euro).

*** Middelgroot:**
meer dan 50 en minder dan 250 medewerkers en een jaaromzet van maximaal 50 miljoen euro (of een balanstotaal van maximaal 43 miljoen euro).

HOE GROOT IS JOUW ORGANISATIE?

*** GROTE ORGANISATIES**

*** MIDDELGROTE ORGANISATIES**

GROTE ORGANISATIES

MIDDELGROTE ORGANISATIES

ESSENTIEEL *

* Er zijn enkele uitzonderingen op de regel, waarbij entiteiten zoals bijvoorbeeld gekwalificeerde aanbieders van vertrouwensdiensten, topleveldomeinnamen registers alsook DNSdienstverleners, aangewezen kunnen worden als essentieel ongeacht de grote van hun organisatie. Voor alle uitzonderingen zie Artikel 3, lid 1.

BELANGRIJK

Middelgrote organisaties met minder dan 250 medewerkers en een jaaromzet van maximaal 50 miljoen euro (of balanstotaal van maximaal 43 miljoen euro) die actief zijn in zeer kritieke sectoren worden beschouwd als belangrijk, samen met andere grote en middelgrote organisaties in kritieke sectoren. Alleen grote organisaties die de plafonds voor middelgrote organisaties overschrijden en onder zeer kritieke sectoren vallen, worden beschouwd als 'essentieel'. Sommige organisaties worden automatisch als "essentieel" beschouwd, ongeacht hun grootte, als een storing in hun dienstverlening ernstige gevolgen zou hebben of ze de enige aanbieder zijn. Dit geldt ook voor organisaties die openbare communicatienetwerken en -diensten leveren, dienstverleners van vertrouwensfuncties, en dienstverleners voor topleveldomeinnamen en domeinnaamregistratie.

In principe richt de NIS2-richtlijn zich niet op kleine en micro-ondernemingen die minder dan 50 werknemers hebben en een jaaromzet van minder dan 7 miljoen euro hebben (of een balanstotaal van minder dan 5 miljoen euro). Maar als ze een sleutelrol hebben voor de samenleving, economie, sectoren of diensten, moeten lidstaten ervoor zorgen dat ze wel onder deze richtlijn vallen. Het grootste verschil tussen essentiële en belangrijke entiteiten zit in de monitoring van het naleven van de regels. Bij de essentiële aanbieders is het toezicht straks proactief. Dit betekent dat bij deze organisaties actief gecheckt zal worden of de wetgeving wordt nageleefd. Bij de belangrijke aanbieders vindt het toezicht achteraf plaats, als er aanwijzingen zijn dat er sprake is van een incident. Mocht na een incident blijken dat de organisatie niet de vereiste stappen heeft genomen, dan zullen ook deze organisaties te maken kunnen krijgen met mogelijke consequenties van het niet naleven van deze wetgeving.

Wat kunnen we verwachten van de NIS2?

Dit zullen we uit leggen aan de hand van twee casussen.

1

Energiebedrijf BrightEnergies met 500 werknemers kreeg met de invoering van de NIS-richtlijn al te maken met verplichtingen op securityvlak. In de NIS-wetgeving (in Nederland opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen) werd de sector waartoe zij behoorde ('energie') als vitale aanbieder geclassificeerd. De huidige directeur Lennard was toen nog niet werkzaam bij BrightEnergies, maar er is documentatie welke maatregelen en processen toen aangepast of vernieuwd zijn. In 2022 kwam hem ter ore dat er nieuwe NIS-wetgeving zou komen. In die nieuwe wetgeving is een energiebedrijf een 'essentiële entiteit'. Met de invoering van de NIS-wetgeving waren er al behoorlijk wat veranderingen doorgevoerd. Omdat hackers het in andere landen (zoals Luxemburg, Italië en Portal) al meerdere malen voorzien hebben op energiebedrijven, wil Lennard er alles aan doen om te zorgen dat Bright niet getroffen wordt. De NIS2-wetgeving krijgt dan ook een hoge prioriteit.

2

Afvalverwerker en recyclingbedrijf Waste2Resource viel voorheen nog niet onder de NIS of andere cybersecurity-wetgeving. De afgelopen jaren werd echter duidelijker dat ook als afvalverwerker je te maken kunt krijgen met een cyberaanval: een concurrent lag in 2021 dagen stil door ransomware waardoor de vuilniswagens niet konden rijden. Het IT-team van Waste2Resource is blij dat zij onder de NIS2-richtlijn vallen, maar er komt wel veel bij kijken. Het team, onder leiding van de pas aangenomen CISO Kayleigh, is momenteel druk bezig met de voorbereiding zoals het maken van een risicoanalyse. Zij en haar team weten in ieder geval al dat zij onder de NIS2-richtlijn worden gezien als belangrijke organisatie en dus te maken krijgen met een zorgplicht en een reactieve meldplicht.

Verplichtingen en implicaties

Dankzij de NIS2 moeten steeds meer sectoren uitgebreidere cybersecurity-vereisten aan gaan houden en moeten belangrijke en essentiële entiteiten maatregelen nemen om beveiligingsrisico's te beheren. Ze moeten dus onder andere back-ups maken, risico-analyses uitvoeren en verplicht incidenten met aanzienlijke impact op de dienstverlening melden. Om de administratieve druk laag te houden zal het management van een organisatie verantwoordelijk worden voor de naleving van de bepalingen uit de NIS2-richtlijn.

Dit nieuwe beleid betekent een grote stap voor veel bedrijven, groot of klein. Zowel de overheid als bedrijven zullen meer verantwoordelijkheid moeten dragen. Dit heeft ook financiële gevolgen: het ICT-budget van bedrijven die nu nog niet onder de richtlijn vallen, verwacht maximaal 22% te stijgen en voor bedrijven die al onder de richtlijn vallen, maximaal 12%. De administratieve lasten zullen ook stijgen. Of deze extra ICT-uitgaven zich zullen terugverdienen en bedrijven concurrentievoordelen zullen opleveren door het hoger niveau van cyberbeveiliging, moet nog blijken.

De verwachtingen zijn dat de NIS2-richtlijn niet alleen tot strengere handhaving en verplichtingen zal leiden, maar ook tot een veiligere digitale economie in de Europese Unie en een bescherming tegen cyberaanvallen.

Wat gaat de NIS2 betekenen voor jouw **organisatie?**

In de NIS2-richtlijn zal zoals eerder besproken onderscheid gemaakt worden tussen twee categorieën; essentiële en belangrijke sectoren, waar eerst alleen onderscheid werd gemaakt tussen vitale organisaties die wel onder de NIS vielen en niet-vitale organisaties. Alle sectoren en organisaties die onder NIS2 zullen gaan vallen zijn van groot belang voor de samenleving. Het zou grote problemen opleveren voor de samenleving als deze organisaties hun werk niet meer kunnen doen.

Cyberaanvallen kunnen grote impact hebben. Niet alleen op organisaties, maar ook op de maatschappij.
Enkele voorbeelden van grote aanvallen zijn:

NotPetya

De verspreiding van NotPetya ransomware in 2017 waarbij onder andere de Rotterdamse haven stil kwam te liggen

2017

Mandemakers gr. & VDL

Bij de ransomware-aanvallen op de Mandemakers Groep en VDL werd de bedrijfsvoering van deze organisaties ernstig verstoord

2021

Bakker Logistiek

Door de aanval op Bakker Logistiek hadden supermarkten dagenlang geen kaas in de schappen

2021

Kaseya

Door de aanval op softwareleverancier Kaseya kregen cybercriminelen toegang tot de systemen van duizenden bedrijven

2021

De twee categorieën zijn gecreëerd omdat niet alle sectoren op de dezelfde schaal impact zouden hebben op de samenleving in het geval van een incident. Hieronder leggen wij je uit wat het verschil is tussen de twee groepen – essentieel en belangrijk – en wat de invloed hiervan is op welke veranderingen NIS2 teweeg zal brengen.

Zorg- en meldplicht

Alle organisaties die onder NIS2 vallen – essentieel of belangrijk – zullen moeten gaan voldoen aan hun zorgplicht. De richtlijn bevat een lijst met soorten maatregelen waar aanbieders minimaal aan moeten voldoen. Voorbeelden hiervan zijn:

- Risicobeoordeling voor beveiliging van informatiesystemen
- Aandacht voor crisismanagement en operationele continuïteit bij groot cyberincident
- Veiligheid van de toeleveringsketen waarborgen
- Zorgplicht voor waarborgen van veiligheid van netwerk- en informatiesystemen
- Gebruik van cryptografie en versleuteling
- Beleid en procedures voor beoordeling van effectiviteit van risicobeheersmaatregelen

De Europese Commissie behoudt het recht voor om met gedelegeerde- en uitvoeringsbesluiten maatregelen nader te specificeren en met extra maatregelen uit te breiden. Lidstaten kunnen dan de ruimte krijgen om specifieke maatregelen op te leggen, waarbij ze rekening kunnen houden met nationale en sectorale omstandigheden. Ook de meldplicht zal voor alle organisaties gelden die onder de NIS2 vallen. Deze meldplicht houdt in dat getroffen organisaties binnen 24 uur nadat zij zich bewust worden van het incident een melding moeten maken bij de aangewezen instantie, gevolgd door een rapport binnen een maand.

De NIS2 in een notendop

BELANRIJK

Zoals in de casus van **Waste2Resource**

Middelgrote organisaties actief in één van de 11 'zeer kritieke sectoren' of middelgrote en grote organisaties actief in een van de 7 'kritieke sectoren'

ESSENTIEEL

Zoals in de casus van **Bright Energies**

Grote organisaties actief in de 'zeer kritieke sectoren'

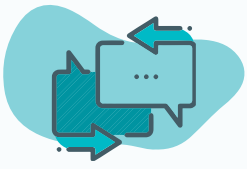
ZORGPLICHT

- Hanteren van een basisniveau van digitale hygiëne en invoeren van cybersecurity educatie
- Risicobeoordeling voor beveiliging van informatiesystemen
- Aandacht voor crisismanagement en operationele continuïteit bij groot cyberincident
- Veiligheid van de toeleveringsketen waarborgen
- Zorgplicht voor waarborgen van veiligheid van netwerk- en informatiesystemen, waaronder het reageren en communiceren van kwetsbaarheden

- Zorgen voor de digitale veiligheid van personeel, toegangsbeleid en het beveiligen van de digitale bedrijfsmiddelen
- Gebruik van cryptografie en versleuteling
- Invoeren dan wel toepassen van multifactor-authenticatie en/of beveiligde interne communicatie
- Beleid en procedures voor beoordeling van effectiviteit van risicobeheersmaatregelen

Reactieve monitoring **(na incident)**

Proactieve monitoring **(ook buiten incidenten om)**



MELDPLICHT (IN 2 FASEN)

- 1e melding binnen 24 uur (ter voorkomen van potentiële verspreiding)
- Eindmelding binnen 1 maand na het incident

Administratie geldboete voor het niet opvolgen van de zorg- of meldplicht:

- Een maximale boete van ten minste **7.000.000** euro
- of **ten minste 1,4%** van de wereldwijde jaaromzet in het voorgaande boekjaar; afhankelijk van welk bedrag hoger is

Administratie geldboete voor het niet opvolgen van de zorg- of meldplicht:

- Een maximale boete van ten minste **10.000.000** euro
- of **ten minste 2%** van de wereldwijde jaaromzet in het voorgaande boekjaar; afhankelijk van welk bedrag hoger is

Daarnaast kunnen vergunningen tijdelijk opgeschort worden of kan een natuurlijk persoon, zoals de algemeen directeur, tijdelijk geschorst worden.

Monitoring

Waar de twee categorieën in zullen verschillen is de manier waarop gecheckt wordt of de organisaties zich aan de opgelegde eisen houden. Bij sectoren en organisaties die als essentieel bestempeld worden, zal er proactief gemonitord worden of zij aan de eisen voldoen. Er zal dus actief gecheckt worden en de gevolgen van wanbeleid zullen dan ook kunnen gelden zonder dat er een incident heeft plaatsgevonden. **Energiebedrijf BrightEnergies** bereidt zich dus actief voor de aankomende handhaving, omdat het een essentieel bedrijf is. Lennard heeft de security- en complianceteams bij elkaar geroepen om het te hebben over dit onderwerp. Nog meer dan ten tijde van de NIS-wetgeving wordt intern benadrukt dat voldoen aan de regeling van groot belang is en werkgroepen worden opgezet om dit in goede banen te leiden.

Bij de tweede categorie, belangrijke entiteiten, zal het checken van de naleving van de wet op een reactieve manier plaatsvinden. Dit betekent dat deze organisaties pas na een incident gecontroleerd zullen worden op het naleven van de wetgeving en eisen. Mocht er achteraf blijken dat er niet genoeg actie is ondernomen en de eisen niet zijn nagekomen dan kunnen er naar aanleiding van een incident dezelfde sancties volgen als voor essentiële entiteiten.

Afvalverwerker en recyclingbedrijf **Waste2Resource** krijgt te maken met reactieve handhaving, pas na een incident zal gecontroleerd worden of zij aan alle eisen van de NIS2 voldoen. Het bedrijf wil alles zo goed mogelijk regelen en Kayleigh besluit alles te documenteren, proactief of reactief maakt voor haar weinig verschil: “Als alles maar goed geregeld is aan de achterkant!”

Melden

Twee- fasen-melding

De NIS2-richtlijn voorziet in een ‘twee-fasen-aanpak’ voor de melding van incidenten. De eerste melding is erop gericht om de potentiële verspreiding van incidenten te beperken en de entiteiten in de gelegenheid te stellen om steun te zoeken. De tweede melding dient grondig te zijn, en moet ervoor zorgen dat geleerd kan worden van eerdere incidenten. Daarnaast heeft het tevens als doel de veerkracht van individuele bedrijven en hele sectoren ten aanzien van cyber dreigingen gaandeweg te verbeteren. Afgezien van de verplichting om de eerste melding in te dienen, ligt de focus bij de eerste melding bij de behandeling van incidenten.

Eerste melding

1

Zonder onnodige vertraging en in ieder geval binnen 24 uur na het bekend raken met het incident moet er een eerste melding worden gedaan bij de Rijksinspectie Digitale Infrastructuur (RDI, voorheen Agentschap Telecom), de Nederlandse overheidsorganisatie die zorgt voor een betrouwbare en beschikbare digitale infrastructuur, of het CISRT waarbij, indien mogelijk, moet worden aangegeven of het incident is veroorzaakt door een onwettige of kwaadwillige handeling. Het gaat hierbij om de strikt noodzakelijke informatie. Binnen 24 uur na indiening van deze melding krijgt de meldende entiteit een antwoord met eerste feedback van de bevoegde nationale autoriteit of het CSIRT. Indien de entiteit daarom verzoekt, kunnen richtsnoeren voor de uitvoering van mogelijk risicobeperkende maatregelen worden ontvangen en eventueel aanvullende technische ondersteuning. In het geval van een incident van criminele aard, ontvangt de entiteit tevens richtsnoeren voor het melden van het incident aan de rechtshandhavingsinstanties.

Eindmelding

2

Uiteindelijk zal binnen één maand na indiening van de eerste melding, oftewel het eerste verslag, een eindverslag worden ingediend met i) een gedetailleerde beschrijving van het incident, de ernst en gevolgen ervan, ii) het soort dreiging of de oorzaak die waarschijnlijk tot een incident heeft geleid en iii) toegepaste en lopende beperkende maatregelen. In gemotiveerde gevallen en in overleg met de bevoegde autoriteit kan van de 24-uur termijn voor de eerste melding en één maand termijn van het verslag worden afgeweken.

1

Het is crisis bij BrightEnergies. Een aanvaller is het netwerk binnengedrongen, niemand weet hoe dat kon en wat er moest gebeuren op dat moment. En dan is ook nog eens de CISO niet te bereiken! Iedereen is in rep en roer en als vervanger neemt IT-specialist Menno de touwtjes in handen. Hij meldt het incident binnen 24 uur bij de RDI. Samen met een externe partij wordt naargeestig gezocht naar de back-ups van het bedrijf. Die worden gevonden en zo weet de organisatie ergere gevolgen te voorkomen, doordat ze toegang hebben tot hun belangrijke data. Niettemin heeft het bedrijf een aantal dagen platgelegen, met alle gevolgen van dien. Een maand na het incident wordt een uitgebreide beschrijving en de oorzaak in een eindmelding gerapporteerd. Dat alles toch niet zo goed geregeld was op securitygebied was een grote eye-opener voor directeur Lennard. Deze crisis heeft flinke gevolgen voor BrightEnergies.

2

Waste2Resource krijgt te maken met een ransomware-aanval, net als de concurrent in 2021. Dankzij de processen die CISO Kayleigh per se gedocumenteerd wilde hebben kan het IT-team vrij snel een recente back-up terugzetten. Na iets minder dan 24 uur is de organisatie weer up en running, dankzij de vereisten van de NIS2 valt de schade mee. Kayleigh is maar één ding vergeten, de eerste melding. Gelukkig attendeert één van haar teamgenoten haar nog net op de valreep dat de eerste melding binnen 24-uur moet worden gedaan. “Vergeet ook de eindmelding niet in te plannen!” zegt Kayleighs collega nog voordat zij naar huis gaat.

Significante cyberdreigingen

Er is een regelgeving vastgesteld voor het melden van incidenten met grote gevolgen in de NIS2-richtlijn. Bedrijven moeten ook elke significante cyberbedreiging die ze tegenkomen en die tot een groot incident kan leiden, melden. Wat betreft het begrip “cyberbeveiliging” sluiten we aan bij de definitie van de Europese Unie voor cyberbeveiliging en certificering van IT. Een incident wordt als significant beschouwd als het tot aanzienlijke operationele verstoring of financiële verliezen leidt voor het bedrijf of als het personen of organisaties aanzienlijke materiële of immateriële schade kan veroorzaken.

Vrijwillige meldingen

Bedrijven buiten het bereik van de NIS2-richtlijn kunnen op vrijwillige basis melding maken van significante incidenten, cyberbedreigingen of bijna-incidenten. De verantwoordelijke autoriteit volgt hierbij het meldingsproces. Bij vrijwillig ingediende meldingen mogen geen extra verplichtingen worden opgelegd.

Omvang verplichtingen

De Europese Commissie kan verdere richtlijnen geven over de informatie, het formaat en het meldingsproces voor zowel incidenten met grote gevolgen als cyberbedreigingen. De omvang van de verplichtingen kan daardoor uitgebreid worden.

Boetes en Sancties

Bij de meld- en zorgplicht komt ook een vorm van handhaving om de effectieve naleving van de regels te verzekeren. Autoriteiten krijgen hiervoor verschillende toezichtacties- en middelen tot hun beschikking.

Cybersecurity en -weerhaarheid wordt door NIS 2 een boardroom issue gemaakt. Naast bekende handhavingsmodaliteiten – waaronder boetes, sancties en het publieke schandpaal effect – staat persoonlijke aansprakelijkheid van bestuurders op het spel. De tijd van onwetenheid en weg delegeren is voorbij. // **Olaf van Haperen - Eversheds Sutherland**

Minimum sancties

De NIS2-richtlijn bevat een verplichte lijst met sancties, waaronder inspecties ter plaatse, beveiligingsaudits, beveiligingsscans, informatieverzoeken en verzoeken om toegang tot gegevens. Sommige sancties zijn gelijk voor alle landen, andere niet, zoals sancties voor ernstige overtredingen. In die gevallen moeten de landen zelf zorgen voor effectieve, evenredige en afschrikwekkende sancties. Het type sanctie (strafrechtelijk of administratief) wordt ook bepaald door het land zelf. Sancties moeten passen bij de ernst en aard van de overtreding en moeten rekening houden met factoren zoals de veroorzaakte schade, samenwerking met de bevoegde autoriteit en andere omstandigheden.

Administratieve boetes

In plaats van of naast de andere maatregelen, kunnen administratieve boetes worden opgelegd, afhankelijk van de omstandigheden van het geval. Bij het opleggen van een administratieve boete moeten dezelfde elementen als bij de andere sancties worden meegenomen. Inbreuken kunnen worden bestraft met administratieve boetes van maximaal 10 miljoen euro of 2% van de jaarlijkse wereldwijde omzet van het bedrijf, afhankelijk van wat hoger is. Lokale toezichthouders moeten hun eigen beleid voor het opleggen van boetes ontwikkelen.

BOETES

Tot minimaal 10 miljoen euro of 2% van de totale wereldwijde omzet

SCHORSING

Personen met een relevante autoriteit of management rol kunnen worden geschorst

1

BrightEnergies krijgt na de ransomware-aanval te maken met sancties. Als essentiële entiteit zijn zij verplicht om hun security goed op orde te hebben. De CISO wordt geschorst en een forse boete volgt. Directeur Lennard besluit dat security vanaf nu topprioriteit nummer 1 is voor de IT-teams en wil geavanceerde securityoplossingen implementeren om aanvallen proactief te voorkomen.

2

Waste2Resource ontloopt gelukkig de santies. Het incident heeft bij Kayleigh wel de ogen geopend, ze stapt naar de CEO en kaart aan dat ze met wat meer budget denkt de organisatie nog beter te kunnen beveiligen. Hoewel de CEO de ernst inziet is hij al vrij tevreden, "we voldoen toch netjes aan de richtlijnen?", Kayleigh krijgt iets meer budget maar geen vetpot.

Samen voor een weerbare toekomst

Verder zal er door de NIS2 voor gezorgd worden dat er een European Cyber Crises Liaison Organisation Network (EU-CyCLONe) opgericht wordt om support en coördinatie te bieden in het geval van een grootschalige cyberaanval in de EU. Ook zal er door experts op gehamerd worden om samen te werken en onderling tussen lidstaten van elkaar te leren om zo tips uit te delen en onderling vertrouwen te vergroten.

Hulp nodig met de **implementatie van NIS2?**

Dit kan ESET in Nederland voor jouw organisatie betekenen

Als Europese leverancier op het gebied van digital securityoplossingen denken wij graag met je mee en helpen wij je graag bij de vraagstukken die je hebt met betrekking tot de NIS2 of de implementatie hiervan.

Mogelijkheden die wij bieden op het gebied van NIS2:

- Kennisdeling via onze kanalen zoals de Digital Security Guide of ons corporate blog
- Interactieve sessies zoals workshops
- Meedenken m.b.t. compliance en doorvoeren NIS2 maatregelen
- Voorzien van securityoplossingen die bijdragen aan compliance
- Onze specialisten zijn altijd bereikbaar om jouw vragen te beantwoorden

Dit kan Eversheds Sutherland voor jouw organisatie betekenen

- Compliance advisering over de gehele scope van NIS2
- Advies over aansprakelijkheid van de entiteit, groep en de bestuurder (persoonlijk)
- Advies over de materiële en territoriale toepasselijkheid en de reikwijdte van de verplichtingen onder NIS2
- Classificatie als essentiële of belangrijke entiteit en daaruit voortvloeiende compliance verplichtingen
- Vragen omtrent de bevoegdheid van een leidende toezichthouder
- Vertegenwoordiging bij toezichthouders en het publiek
- Vertegenwoordiging en advies bij handhaving en boetes
- Advies over de omvang van de zorgplicht gezien de classificatie van de entiteit
- Incident response en melding van incidenten bij bevoegde toezichthouders
- Advies over aansprakelijkheid en contractuele verplichtingen leveranciers
- Opstellen, beoordelen en implementeren van beleid, verklaringen en andere compliance documentatie

Meer informatie?
Neem contact met ons op!

Robbert Santifort

Principal Associate
Eversheds Sutherland

robbertsantifort@
eversheds-sutherland.com

+316 81 880 472

Olaf van Haperen

Technology Partner
Eversheds Sutherland

olafvanhaperen@
eversheds-sutherland.com

Astrid Oosenbrug

Public Affairs Officer
ESET Nederland

astrid.oosenbrug@
eset.nl

+316 25 129 947

Bronnen

https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555&from=EN

•

https://www.europarl.europa.eu/news/nl/press-room/20221107IPR49608/
cyberbeveiliging-parlement-neemt-nieuwe-wet-aan-om-veerkracht-eu-te-versterken


EVERSHEDS
SUTHERLAND
&
eset
Digital Security
Progress. Protected.