Veelgestelde vragen over de NIS 2-richtlijn

Over de richtlijn Netwerk en informatiebeveiliging (NIS 2)

De Europese Unie wil overheden, bedrijven en organisaties weerbaarder maken door de cyberveiligheid te vergroten. Daarvoor wordt nieuwe wet- en regelgeving ontwikkeld. Eén daarvan is de richtlijn Netwerk en informatiebeveiliging (afgekort als NIS 2-richtlijn, in Nederland ook wel NIB-richtlijn genoemd), die zich richt op het weerbaarder maken van organisaties tegen cyberaanvallen.

Gevolgen NIS 2-richtlijn voor leden SURF nog niet helemaal duidelijk

SURF krijgt veel vragen over deze nieuwe richtlijn en de gevolgen daarvan voor de leden. Op dit moment werkt de overheid aan een wetsvoorstel om de NIS 2-richtlijn in Nederland te implementeren in de Wet beveiliging netwerk- en informatiesystemen (Wbni). De gevolgen voor onze leden zijn nog niet helemaal duidelijk. Op deze pagina delen we de informatie die wij hebben. Zodra er nieuwe informatie bekend is, werken we deze pagina bij.

Vragen?

Neem contact op met Nicole van Deursen van SURF.

Op de hoogte blijven?

Deze pagina is verplaatst naar Security Expertise Centrum en wordt voortaan daar bijgehouden. De wiki wordt niet meer onderhouden.

Veelgestelde vragen en antwoorden over de richtlijn Netwerk en Informatiebeveiliging (NIS 2)

De NIS 2-richtlijn komt van het Europees Parlement en beschrijft maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie. De richtlijn is op 16 januari 2023 in werking getreden. Het is een herziening van de oorspronkelijke NIS-richtlijn (NIS 1) uit 2016. EU-lidstaten hebben tot 17 oktober 2024 de tijd om deze om te zetten in nationale wet- en regelgeving. In Nederland krijgt dat zijn beslag in de herziening van de bestaande Wet Beveiliging Netwerk en Informatiesystemen (Wbni).

- Lees de volledige tekst van de NIS 2-richtlijn: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32022L2555&qid=1678274777536
- Lees de factsheet van de Europese Commissie: https://digital-strategy.ec.europa.eu/en/library/directive-measures-high-common-level-cybersecurity-across-union-0.

De Wet beveiliging netwerk- en informatiesystemen (Wbni) is er op gericht om de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en zo maatschappelijke ontwrichting te voorkomen. De Wbni verplicht aanbieders van essentiële diensten en digitale dienstverleners om maatregelen te nemen om hun ICT te beveiligen tegen incidenten. Voor ernstige incidenten geldt een meldplicht. De NIS 1-richtlijn is in Nederland geïmplementeerd via de Wbni, die per 9 november 2018 geldt. De komst van de NIS 2-richtlijn leidt daarom tot een herziening van de Wbni.

Naast de Wbni trad op 9 november 2018 ook het Besluit beveiliging netwerk- en informatiesystemen (Bbni) in werking. In het Bbni staan onder meer welke organisaties vallen onder de Wbni. De huidige vitale aanbieders zijn onder andere drinkwatervoorziening, energie en de financiële sector.
Organisaties die via de Wbni onder de NIS 2-richtlijn (komen te) vallen, krijgen te maken met rechten, plichten en toezicht. De eisen hangen af van of de organisatie is gekwalificeerd als essentiële of belangrijke entiteit. Rechten zijn bijvoorbeeld het recht op bijstand bij incidenten in de vorm van advies en informatie door een Computer Security Incident Response Team (CSIRT), en bij het treffen van maatregelen om continuïteit van diensten te waarborgen of herstellen. Onder plichten vallen:

- Zorgplicht: het treffen van **passende** maatregelen om incidenten te voorkomen en risico's te beheersen en gevolgen van incident zoveel mogelijk te beperken.
- Meldplicht: incidenten en risico's met significante gevolgen binnen 24 uur melden aan de toezichthouder en het aangewezen CSIRT voor de sector. Wat significant betekent is nog niet vastgesteld. Parameters die bepalen wat de drempelwaarde is om een incident te moeten melden zijn bijvoorbeeld het aantal getroffen gebruikers, de duur van de verstoring en de grootte van het getroffen geografisch gebied.
- Register: Er komt een register waarin entiteiten die onder de NIS 2-richtlijn vallen zich moeten registreren.
- Toezicht: Er komt toezicht op de naleving van de zorgplicht en meldplicht.

Welke maatregelen treffen?

Wat passende maatregelen zijn zal naar verwachting niet in een landelijk normenkader worden opgelegd, maar aan de sectoren worden overgelaten. Daarbij zegt de overheid zoveel mogelijk te willen aansluiten bij al bestaande methodieken. Veel leden van SURF werken al met het SURFaudit informatiebeveiliging toetsingskader of met de ISO 27000-serie. In artikel 21 van de NIS 2-richtlijn staan echter ook enkele concrete maatregelen die organisaties minimaal moeten treffen. Een deel daarvan komt al voor in het SURFaudit informatiebeveiliging toetsingskader en de ISO normen.

Toezichthouder voor SURF-leden nog niet bekend

Op dit moment is nog niet duidelijk wie de toezichthouder wordt voor de SURF-leden die onder de NIS 2-richtlijn (komen te) vallen. Ook is niet duidelijk of dit voor alle op SURF aangesloten instellingen dezelfde wordt. De rijksoverheid verkent momenteel of een centrale toezichthouder kan worden aangewezen. De mate van toezicht (en de maximale boete in geval van overtreding van de verplichtingen uit de NIS 2-richtlijn) is voor essentiële entiteiten anders dan voor belangrijke entiteiten. SURF ziet als coöperatie/samenwerkingsorganisatie geen rol voor zichzelf als toezichthouder in het stelsel.

Onduidelijk hoe rol en samenwerking Computer Security Incident Response Teams (CSIRT) uitvalt

Tenslotte wordt momenteel door de NCTV onderzocht hoe de rol van CSIRT's en de onderlinge samenwerking onder de nieuwe wet gaat uitvallen. Binnen de huidige Wbni is SURFcert – de sectorale CERT voor onderwijs en onderzoek – aangemerkt als een vitaal computercrisisteam. De impact op de rol en dienstverlening van SURFcert wordt momenteel onderzocht. De verantwoordelijke vakminister bepaalt voor de sector welke CSIRT deze wettelijke taak gaat uitvoeren.

Samenwerkingonderzoeksinstellingen mag binnen de SURF-cooperatie niet in de weg staan

Bij OCW heeft SURF aandacht gevraagd voor het punt dat het vallen onder verschillende sectoren met diverse toezichthouders, kaders en CSIRT's, samenwerking van onderzoeksinstellingen binnen SURF niet in de weg moet staan.
De wetgeving gaat inderdaad ook toeleveranciers raken van SURF-leden die onder de NIS 2-richtlijn (komen te) vallen. In artikel 21 staat als een van de 10 basismaatregelen namelijk dat de toeleveringsketen (rechtstreekse leveranciers en dienstverleners) moet worden beveiligd. Hierbij gaat het om een passend beveiligingsniveau op basis van een risicoanalyse. Het NBA-kader en de ISO 27000-normen, die veel van de instellingen al hanteren, bieden hiervoor aanknopingspunten.

Daarnaast moet de fabrikant of aanbieder van ICT-producten of ICT-diensten ook voorzien in de noodzakelijke procedures om kwetsbaarheidsinformatie van derden te ontvangen. Voor SURF zelf als (niet publieke) aanbieder van digitale diensten is nog onduidelijk of de organisatie zelf onder de NIS 2-richtlijn valt. Ook deze vraag is voorgelegd aan OCW.
SURF-leden werken al aan het versterken van hun weerbaarheid. Het is aan te bevelen dat CISO's en besturen zichzelf geïnformeerd houden over de ontwikkelingen en met de brancheverenigingen in overleg gaan als er grote bezwaren of zorgen zijn.

Het Nationaal Cyber Security Centrum adviseert organisaties zich alvast voor te bereiden op hun zorgplicht door maatregelen te nemen die de veiligheid en weerbaarheid van hun processen en diensten verbeteren. Naast de basismaatregelen kan je denken aan het:

- Inventariseren en analyseren van risico's.
- Opstellen van bedrijfscontinuïteitplannen en protocollen voor crisisbeheersing.
- Identificeren van alternatieve toeleveringsketens.
- Bewustwording van personeel van risico's en te nemen maatregelen.

Ook is het verstandig om budget en capaciteit te reserveren dat nodig is om aan de richtlijnen te voldoen.
De meest in het oog springende verschillen zijn:

- De NIS 2-richtlijn hanteert een groter toepassingsgebied waardoor er meer organisaties (entiteiten) en sectoren onder vallen, waaronder centrale overheidsorganen. Een EU-lidstaat kan bovendien besluiten om het toepassingsgebied verder uit te breiden naar regionale en lokale overheidsorganen en onderwijsinstellingen, met name wanneer zij kritieke onderzoeksactiviteiten verrichten.
- De NIS 2-richtlijn verplicht alle organisaties voor wie de richtlijn op van toepassing is om passende beveiligingsmaatregelen te treffen. Daarbij wordt rekening gehouden met de stand van de techniek en het risico. De richtlijn bevat ook een aantal minimale eisen waaraan organisaties moeten voldoen. Ook worden hierbij verplichtingen ten aanzien van de beveiliging van de gehele keten van toeleveranciers opgelegd.
- De NIS 2-richtlijn bevat in tegenstelling tot NIS 1 verplichtingen voor besturen van organisaties (artikel 20 en uitgangspunten 133 en 137).
- De NIS 2-richtlijn wijzigt de categorisering van sectoren en entiteiten waarop de richtlijn van toepassing is. Waar NIS 1 sprak over aanbieders van essentiële diensten en aanbieders van digitale diensten, heeft de NIS 2-richtlijn het over essentiële en belangrijke entiteiten. De classificatie als essentiële, dan wel belangrijke, entiteit heeft gevolgen voor verplichtingen op het gebied van rapportage, de wijze waarop toezicht wordt uitgeoefend, en het toepasselijke boeteregime bij overtreding van de verplichtingen in de richtlijn. Deze zijn voor essentiële en belangrijke entiteiten verschillend.

De NIS 2-richtlijn heeft een groter toepassingsgebied dan NIS 1. Deels is de richtlijn van toepassing op meer sectoren, deels biedt de richtlijn de nationale wetgevers ook verdere ruimte om additionele organisaties aan te wijzen die onder de richtlijn komen te vallen.

Het grotere toepassingsgebied leidt ertoe dat de NIS 2-richtlijn ook van toepassing is of kan worden voor verschillende categorieën SURF-leden. Hierover is tot nu toe het volgende bekend:

1. Onderwijssector: NIS 2-richtlijn kan van toepassing worden verklaard door de nationale wetgever (artikel 2 lid 5 sub b).
2. Onderzoekssector: NIS 2-richtlijn is van toepassing als je voldoet aan de criteria zoals die in de richtlijn zijn opgenomen (artikel 2 lid 1 jo. Bijlage II en overweging 36).
3. Zorgsector: NIS 2-richtlijn is van toepassing (artikel 2 lid 1 jo. Bijlage I).
4. Centrale overheidsinstanties: NIS 2-richtlijn is van toepassing (artikel 2 lid 2 sub f onder i).

5. Regionale en lokale overheidsinstanties: NIS 2-richtlijn kan van toepassing worden verklaard door de nationale wetgever (artikel 2 lid 2 sub f onder ii dan wel artikel 2 lid 5 sub a).

Van toepassing verklaring NIS 2-richtlijn voor onderwijssector

Een EU-lidstaat kan ervoor kiezen de richtlijn van toepassing te verklaren voor *onderwijsinstellingen, met name wanneer zij kritieke onderzoeksactiviteiten verrichten* (artikel 2 lid 5 sub b). De conceptwet die Nederland momenteel opstelt, bevat de mogelijkheid om hoger onderwijsinstellingen onder de NIS 2-richtlijn onder te brengen. Dit is nog niet definitief. Definitieve aanwijzing vindt plaats in lagere regelgeving, nadat eerst een **impactanalyse** heeft plaatsgevonden. Definitieve duidelijkheid over de van toepassing verklaring komt met de herziening van de Wbni, maar mogelijk ook pas later als de Wbni verder wordt geconcretiseerd in een besluit (zoals de huidige Bbni).

Impactanalyse

Voordat mogelijk wordt overgegaan tot het aanwijzen van (een deel van de) HO-instellingen, voert OCW eerst een impactanalyse uit. Deze analyse zal een aantal maanden in beslag nemen. Hierin zal onder andere aandacht zijn voor:
* Bestuurlijke afspraken.
* De mogelijke link met de basislijst sensitieve technologie.
* De mogelijke raakvlakken met andere sectoren.
* De mogelijke impact op betrokken stakeholders.

2022

NIS 2-richtlijn vastgesteld door de Europese Raad.

2023

Voorbereiding nationale implementatie in Wbni

- Maart: beleidskader CSIRT-stelsel gereed
- April: besluit over CSIRT-stelsel
- November/December: start internetconsulatie: een periode van 6 weken, waarin burgers, bedrijven en overheidsinstellingen mogelijke verbeteringen kunnen aangeven in de wet- en regelgeving die in voorbereiding is. De resultaten van de consultatie worden vervolgens gepubliceerd en waar mogelijk verwerkt in het wetsvoorstel. Het wetsvoorstel wordt gepubliceerd op internetconsultatie.nl. De exacte datum waarop de consultatie start is nog niet bekend.
- Na Wbni volgen algemene maatregelen van bestuur

2024

Implementatie in nationale wetgeving (uiterlijk 17-10-2024)

2027

EC evalueert NIS-2 Directive
Als de NIS 2-richtlijn op een organisatie van toepassing is, wordt deze organisatie vervolgens gekwalificeerd als een essentiële dan wel belangrijke entiteit. Deze kwalificatie vindt deels plaats op basis van duidelijke criteria in de richtlijn zelf. Deels is het echter ook aan de nationale wetgever om de kwalificatie te doen.

De kwalificatie als essentiële of belangrijke entiteit heeft gevolgen voor de mate van toezicht op het nakomen van verplichtingen uit de NIS 2-richtlijn. **Als de organisatie een essentiële entiteit is, is het toezicht proactief.**Toezichthouders kunnen steeds controleren of de juiste processen aanwezig zijn en correct worden nageleefd (toezicht ex ante). **Voor belangrijke entiteiten vindt het toezicht achteraf plaats** en moet de organisatie in het geval van een cyberincident kunnen aantonen de juiste processen te hebben geïmplementeerd (toezicht ex post). Ook verschillen de maximale boetebedragen bij het niet nakomen van de verplichtingen uit de NIS 2-richtlijn al naar gelang de organisatie een essentiële dan wel belangrijke entiteit is.

Op dit moment verwachten we voor de SURF-leden het volgende ten aanzien van deze kwalificatie:

1. Onderwijssector: voor zover NIS 2-richtlijn van toepassing wordt verklaard worden deze organisaties aangemerkt als een belangrijke entiteit.
2. Onderzoekssector: voor zover NIS 2-richtlijn van toepassing wordt verklaard worden deze organisaties in hun geheel aangemerkt als een belangrijke entiteit.
3. Zorgsector: essentiële of belangrijke entiteit, afhankelijk van de omvang.
4. Centrale overheidsinstanties: essentiële entiteit.
5. Regionale of lokale overheidsinstanties: belangrijke entiteit.

Begrip vitale aanbieder in Wbni

In de Wbni is het begrip *vitale aanbieder* geïntroduceerd bovenop de begrippen *essentiële dienstverlener* en *digitale dienstverlener* zoals die in NIS 1 worden gebruikt. Dit begrip zal naar verwachting wijzigen om een onderscheid te kunnen maken tussen de verschillende kwalificaties die in de NIS 2-richtlijn zijn opgenomen. We weten dat op dit moment interdepartementaal wordt gewerkt aan een herziening van het beleidskader 'vitaal'. Dit beleidskader kent een nauwe verwevenheid met de NIS 2-richtlijn en de Richtlijn Weerbaarheid Kritieke Entiteiten (CER-richtlijn). De overheid verkent momenteel wat precies tot de vitale infrastructuur of -processen moet worden gerekend.

- De brancheverenigingen UNL en VH vertegenwoordigen de belangen van de universiteiten en hogescholen in hun gesprekken met OCW.
- MBO Digitaal en de MBO Raad vertegenwoordigen de belangen van de mbo-instellingen en volgen de ontwikkelingen. De NIS2-richtlijn lijkt vooralsnog niet van toepassing op de mbo-sector.
- OCW werkt samen met andere ministeries aan de implementatie van de NIS 2-richtlijn in een nieuwe Wbni. Gesprekken van SURF met OCW hebben vooral als doel om informatie te verzamelen, de leden voor te lichten en om de consequenties voor de SURF-organisatie en SURFcert in kaart te brengen.
- SURF onderhoudt contacten met de brancheverenigingen en met de SURF-leden via de gebruikelijke kanalen. SURF verzamelt en deelt zoveel mogelijk informatie over dit onderwerp. De leden van SURF vallen onder meerdere ministeries en de relevantie van de NIS 2-richtlijn en daaruit volgende herziening van de Wbni kan per sector verschillen. De rol van SURFcert wordt momenteel nog onderzocht.
- Het is aan de leden zelf om de vereisten van nieuwe wetgeving binnen de eigen instellingen te implementeren.

Het is goed om alvast vooruit te kijken. In de NIS 2-richtlijn staat niet veel anders dan de goede cybersecurity principes die we al kennen. In Nederland geldt voor de hoger onderwijssector een compliance eis van volwassenheidsniveau 3 op alle controls uit het SURFaudit informatiebeveiligingstoetsingskader. Daarmee zijn instellingen al op weg naar een redelijke basis van processen voor informatiebeveiliging.

In de NIS 2-richtlijn staan soortgelijke eisen, bijvoorbeeld in artikel 21. De nadruk ligt op risicomanagement. De beveiliging van het systeem waar je aan werkt moet passend zijn bij de risico's en de risicobereidheid van de eigenaar. Als er hoge beveiligingseisen worden gesteld aan het systeem, kan het dus zijn dat je nog meer technische en organisatorische maatregelen wilt treffen dan het minimale uit betreffende artikel 21 of uit bijvoorbeeld de SURF security baseline. Bovendien moet de systeemeigenaar de risicobeoordeling regelmatig herhalen en regelmatig toetsen of de maatregelen effectief zijn. Je wens om het volgend jaar niet weer opnieuw te moeten doen gaat dus nooit in vervulling: er moet voor altijd regelmatig opnieuw een beoordeling worden gedaan en maatregelen aangescherpt, passend bij het risico.

Onderzoek en kennisveiligheid

Indien het systeem waar je aan werkt betrekking heeft op onderzoeksdata kun je ook het Loket Kennisveiligheid bezoeken. Daar staat nog aanvullende informatie over risicoanalyse en cyberveiligheid van gevoelige kennis.