# Richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie (NIS2-richtlijn) — Veelgestelde vragen

## NIS2-richtlijn

### Waarom heeft de Commissie een nieuwe NIS-richtlijn voorgesteld?

De NIS-richtlijn — de eerste EU-wetgeving inzake cyberbeveiliging — is het eerste horizontale instrument voor de interne markt dat gericht is op het verbeteren van de veerkracht van netwerk- en informatiesystemen in de Unie tegen cyberbeveiligingsrisico's. Ondanks de opmerkelijke verwezenlijkingen van de NIS-richtlijn heeft de NIS-richtlijn een aantal beperkingen laten zien. De digitale transformatie van de samenleving, die door de COVID-19-crisis is geïntensiveerd, heeft het dreigingslandschap uitgebreid. Er zijn nieuwe uitdagingen aan het licht gekomen die aangepaste en innovatieve antwoorden vereisen.

Om het effect te kunnen analyseren en de tekortkomingen van de NIS-richtlijn te kunnen vaststellen, heeft de Commissie een uitgebreide raadpleging van belanghebbenden gehouden. De Commissie heeft de volgende hoofdpunten vastgesteld:

- onvoldoende cyberweerbaarheid van bedrijven die in de EUactief zijn
- inconsistente veerkracht tussen de lidstaten en sectoren
- onvoldoende gemeenschappelijk begrip van de belangrijkste bedreigingen en uitdagingen tussen de lidstaten
- gebrek aan gezamenlijke crisisrespons.

Daarom heeft de Commissie, om te reageren op de toenemende bedreigingen als gevolg van digitalisering en onderlinge verbondenheid, in december 2020 een herziene reeks toekomstbestendige regels voorgesteld om het niveau van cyberweerbaarheid in de Unie te versterken, waarover de medewetgevers op 13 mei 2022 een politiek akkoord hebben bereikt en de nieuwe richtlijn eind november 2022 formeel hebben aangenomen.

### Hoe heeft de COVID-19-crisis de nieuwe richtlijn beïnvloed?

Sinds de COVID-19-crisis is de Europese economie afhankelijker geworden van digitale oplossingen dan ooit tevoren. Sectoren en diensten worden steeds meer onderling verbonden en onderling afhankelijk. Dit heeft geresulteerd in een groeiend en snel evoluerend cyberdreigingslandschap: elke verstoring, zelfs in eerste instantie beperkt tot één entiteit of één sector, kan in ruimere zin cascade-effecten hebben, wat kan leiden tot verreikende en langdurige negatieve gevolgen voor de dienstverlening op de gehele interne markt.

De COVID-19-pandemie heeft aangetoond dat onze steeds meer onderling afhankelijke samenlevingen kwetsbaarder zijn in het licht van onverwachte risico's. Het heeft de reeds opkomende kwesties in de huidige NIS-richtlijn geïntensiveerd en diende als katalysator voor de herziening ervan. Een concrete wijziging van de NIS-richtlijn in het licht van deze crisis was het uitbreiden van het toepassingsgebied van de nieuwe richtlijn, met meer specifieke elementen in de gezondheidssector, zoals entiteiten die onderzoek en ontwikkeling van geneesmiddelen verrichten.

### Op welke elementen van de vorige NIS-richtlijn bouwt de NIS2-richtlijn voort?

De NIS2-richtlijn bevat wettelijke maatregelen om het algemene niveau van cyberbeveiliging in de EU te verhogen, teneinde bij te dragen tot de algemene werking van de interne markt. Het bouwt voort op de drie belangrijkste pijlers die de basis vormden van de NIS1-richtlijn:

1. Voortbouwend op de NIS1-strategie voor de beveiliging van netwerk- en informatiesystemen, om een hoog niveau van paraatheid van de lidstaten te bereiken, verplicht de NIS2-richtlijn de lidstaten om een nationale cyberbeveiligingsstrategie vast te stellen. De lidstaten moeten ook nationale computerbeveiligingsincidentresponsteams (CSIRT's) aanwijzen die verantwoordelijk zijn voor de behandeling van risico's en incidenten, een bevoegde nationale cyberbeveiligingsautoriteit en één centraal contactpunt (SPOC). Het

SPOC moet een verbindingsfunctie uitoefenen om te zorgen voor grensoverschrijdende samenwerking tussen de autoriteiten van de lidstaten met de betrokken autoriteiten in andere lidstaten en, in voorkomend geval, met de Commissie en het Enisa, en om te zorgen voor sectoroverschrijdende samenwerking met andere bevoegde autoriteiten in zijn lidstaat.

2. De NIS2-richtlijn handhaaft ook het NIS1-kader tot oprichting van de NIS-samenwerkingsgroep ter ondersteuning en vergemakkelijking van de strategische samenwerking en de uitwisseling van informatie tussen de lidstaten, en het CSIRT-netwerk, dat snelle en doeltreffende operationele samenwerking tussen de nationale CSIRT's bevordert.
3. De NIS1-richtlijn zorgt ervoor dat cyberbeveiligingsmaatregelen worden genomen in zeven sectoren, die van vitaal belang zijn voor onze economie en samenleving en die sterk afhankelijk zijn van ICT, zoals energie, vervoer, bankieren, financiële marktinfrastructuren, drinkwater, gezondheidszorg en digitale infrastructuur.

Openbare en particuliere entiteiten die door de lidstaten zijn aangemerkt als aanbieders van essentiële diensten (OES) in deze sectoren, moeten een cyberbeveiligingsrisicobeoordeling uitvoeren en passende en evenredige beveiligingsmaatregelen nemen. Zij zijn verplicht ernstige incidenten aan de bevoegde autoriteiten te melden. Bovendien moeten aanbieders van belangrijke digitale diensten (digitaledienstverleners of DSP's), zoals zoekmachines, cloudcomputingdiensten en onlinemarktplaatsen, ook voldoen aan de beveiligings- en kennisgevingsvereisten van de richtlijn. Tegelijkertijd zijn deze laatste onderworpen aan een zogenaamde „light-touch"-regelgeving, die inhoudt dat deze entiteiten niet onderworpen zijn aan ex-antetoezichtmaatregelen.

De NIS2-richtlijn breidt het toepassingsgebied van sectoren aanzienlijk uit en voert een omvangsdrempel in om te bepalen welke entiteiten binnen het toepassingsgebied ervan vallen en zou verplicht zijn significante cyberbeveiligingsincidenten aan de nationale bevoegde autoriteiten te melden.

## Wat zijn de kernelementen van de NIS2-richtlijn?

De NIS2-richtlijn heeft tot doel de tekortkomingen van de vorige regels aan te pakken, deze aan te passen aan de huidige behoeften en deze toekomstbestendig te maken.

Daartoe breidt de richtlijn het toepassingsgebied van de vorige regels uit door nieuwe sectoren toe te voegen op basis van hun mate van digitalisering en onderlinge verwevenheid en hoe cruciaal zij zijn voor de economie en de samenleving, door een duidelijke regel inzake groottedrempels in te voeren, wat betekent dat alle middelgrote en grote ondernemingen in geselecteerde sectoren in het toepassingsgebied zullen worden opgenomen. Tegelijkertijd laat het de lidstaten een zekere discretionaire bevoegdheid om kleinere entiteiten met een hoog veiligheidsrisicoprofiel aan te wijzen dat ook onder de verplichtingen van de nieuwe richtlijn moet vallen.

De nieuwe richtlijn maakt ook een einde aan het onderscheid tussen aanbieders van essentiële diensten en aanbieders van digitale diensten. Entiteiten worden ingedeeld op basis van hun belang en onderverdeeld in twee categorieën: essentiële en belangrijke entiteiten, die aan een ander toezichtstelsel zullen worden onderworpen.

Het versterkt en stroomlijnt de beveiligings- en rapportagevereisten voor bedrijven door een risicobeheerbenadering op te leggen, die een minimumlijst van basisbeveiligingselementen bevat die moeten worden toegepast. De nieuwe richtlijn bevat preciezere bepalingen over het proces voor de melding van incidenten, de inhoud van de verslagen en de tijdschema's.

Bovendien richt NIS2 zich op de beveiliging van toeleveringsketens en leveranciersrelaties door individuele bedrijven te verplichten cyberbeveiligingsrisico's in de toeleveringsketens en leveranciersrelaties aan te pakken. Op Europees niveau versterkt de richtlijn de cyberbeveiliging van de toeleveringsketen voor belangrijke informatie- en communicatietechnologieën. De lidstaten kunnen in samenwerking met de Commissie en Enisa gecoördineerde veiligheidsrisicobeoordelingen van kritieke toeleveringsketens op Unieniveau uitvoeren, voortbouwend op de succesvolle aanpak die is gevolgd in de context van de aanbeveling van de Commissie over cyberbeveiliging van 5G-netwerken.

De richtlijn voorziet in strengere toezichtsmaatregelen voor nationale autoriteiten, strengere handhavingsvereisten en harmonisering van sanctieregelingen in de lidstaten.

Het versterkt ook de rol van de samenwerkingsgroep bij het vormgeven van strategische beleidsbeslissingen en vergroot de informatie-uitwisseling en samenwerking tussen de autoriteiten van de lidstaten. Het versterkt ook de operationele samenwerking binnen het CSIRT-netwerk en richt het Europees netwerk voor cybercrisisverbindingsorganisaties (EU-CyCLONe) op ter ondersteuning van het gecoördineerde beheer van grootschalige cyberincidenten en -crises.

NIS2 creëert ook een basiskader met verantwoordelijke sleutelactoren voor gecoördineerde openbaarmaking van kwetsbaarheden voor nieuw ontdekte kwetsbaarheden in de hele EU en creëert een EU-kwetsbaarheidsdatabank voor algemeen bekende kwetsbaarheden in ICT-producten en -diensten, die door het EU-agentschap voor cyberbeveiliging (Enisa) moet worden beheerd en onderhouden.

## Welke sectoren en soorten entiteiten zullen de NIS2 bestrijken?

De NIS2 heeft betrekking op entiteiten uit de volgende sectoren:

Sectoren met een hoge kriticiteit: energie (elektriciteit, stadsverwarming en -koeling, olie, gas en waterstof); vervoer (lucht, spoor, water en weg); bankieren; financiële-marktinfrastructuren; gezondheid, met inbegrip van de vervaardiging van farmaceutische producten, met inbegrip van vaccins; drinkwater; afvalwater; digitale infrastructuur (internetuitwisselingspunten; DNS-dienstverleners; Registers voor TLD-namen; aanbieders van cloud computingdiensten; aanbieders van datacenterdiensten; netwerken voor de levering van inhoud; verleners van vertrouwensdiensten; aanbieders van openbare elektronische-communicatienetwerken en openbaar beschikbare elektronische-communicatiediensten); ICT-dienstbeheer (beheerde dienstverleners en aanbieders van beheerde beveiligingsdiensten), openbaar bestuur en ruimte.

Andere kritieke sectoren: post- en koeriersdiensten; afvalbeheer; chemische stoffen; levensmiddelen; vervaardiging van medische hulpmiddelen, computers en elektronica, machines en uitrusting, motorvoertuigen, aanhangwagens en opleggers en andere vervoermiddelen; digitale aanbieders (online marktplaatsen, online zoekmachines en platforms voor sociale netwerkdiensten) en onderzoeksorganisaties.

## Hoe zal het NIS2 de beveiligingsvereisten en de rapportageverplichtingen voor incidenten van de entiteiten versterken en stroomlijnen?

Uit de evaluatie van de huidige voorschriften inzake beveiligings- en meldingsvereisten voor incidenten is gebleken dat de lidstaten deze voorschriften in sommige gevallen op aanzienlijk verschillende manieren hebben toegepast. Dit heeft geleid tot een extra last voor ondernemingen die in meer dan één lidstaat actief zijn.

Als het gaat om cybersecurity-eisen, willen we er bovendien zeker van zijn dat alle bedrijven de nodige kernelementen in hun beleid inzake cyberbeveiligingsrisicobeheer aanpakken.

Om deze reden bevat NIS2 een lijst van 10 belangrijke elementen die alle bedrijven moeten aanpakken of uitvoeren als onderdeel van de maatregelen die zij nemen, met inbegrip van incidentafhandeling, beveiliging van de toeleveringsketen, verwerking en openbaarmaking van kwetsbaarheden, het gebruik van cryptografie en, indien van toepassing, encryptie.

Wat de melding van incidenten betreft, moeten we het juiste evenwicht vinden tussen de behoefte aan snelle rapportage om de mogelijke verspreiding van incidenten te voorkomen, en de noodzaak van diepgaande rapportage om waardevolle lessen te trekken uit individuele incidenten. De nieuwe richtlijn voorziet in een aanpak in meerdere fasen van de melding van incidenten. De getroffen ondernemingen hebben 24 uur de tijd om het CSIRT of de bevoegde nationale autoriteit voor het eerst op de hoogte te stellen van een incident, zodat zij ook hulp kunnen inroepen (geleiding of operationeel advies over de tenuitvoerlegging van mogelijke mitigatiemaatregelen) indien zij daarom verzoeken. De vroegtijdige waarschuwing moet worden gevolgd door een melding van incidenten binnen de 72 uur na kennisneming van het incident en een eindverslag uiterlijk een maand later.

## Hoe zullen de nieuwe regels worden gecontroleerd en gehandhaafd?

De nieuwe NIS-richtlijn stelt toezicht en handhaving centraal in de taken van de bevoegde autoriteiten en vormt een samenhangend kader voor alle toezicht- en handhavingsactiviteiten in de lidstaten.

Om het toezicht op doeltreffende naleving te versterken, voorziet het NIS2 in een minimumlijst van toezichtmiddelen waarmee bevoegde autoriteiten toezicht kunnen houden op essentiële en belangrijke entiteiten. Deze omvatten regelmatige en gerichte audits, controles ter plaatse en daarbuiten, verzoeken om informatie en toegang tot documenten of bewijsmateriaal.

Bovendien voorziet de nieuwe richtlijn in een differentiatie van toezichtregelingen tussen essentiële en belangrijke entiteiten, teneinde een billijk evenwicht van verplichtingen voor zowel entiteiten als bevoegde autoriteiten te waarborgen.

Wat de handhavingbetreft, bestaat er tot nu toe een algemene terughoudendheid tussen de lidstaten om sancties op te leggen aan entiteiten die geen beveiligingsmaatregelen hebben ingevoerd of incidenten niet hebben gemeld. Dit kan negatieve gevolgen hebben voor de cyberweerbaarheid van entiteiten. Om de handhaving doeltreffend te maken, voorziet de nieuwe richtlijn in een consistent kader voor sancties in de hele Unie. Daarom stelt zij een minimumlijst van administratieve sancties vast voor inbreuken op de in de NIS2-richtlijn vastgestelde verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging. Deze sancties omvatten bindende instructies, het uitvoeren van de aanbevelingen van een beveiligingsaudit, het bevel om beveiligingsmaatregelen in overeenstemming te brengen met NIS-

vereisten en administratieve boetes. Met betrekking tot administratieve geldboeten maakt de nieuwe NIS-richtlijn onderscheid tussen essentiële en belangrijke entiteiten. Wat essentiële entiteiten betreft, moeten de lidstaten voorzien in een bepaald niveau van administratieve geldboeten, met name een maximum van ten minste 10 000 000 EUR of 2 % van de totale wereldwijde jaaromzet van het voorgaande boekjaar, indien dit hoger is. Wat belangrijke entiteiten betreft, verplicht NIS2 de lidstaten om te voorzien in een maximumboete van ten minste 7 000 000 EUR of ten minste 1,4 % van de totale wereldwijde jaaromzet van het voorgaande boekjaar, indien dit hoger is.

Bij de uitoefening van hun handhavingsbevoegdheden moeten de bevoegde autoriteiten terdege rekening houden met de specifieke omstandigheden van elk geval, zoals de aard, de ernst en de duur van de inbreuk, de veroorzaakte schade of de geleden verliezen, het opzettelijke of nalatig karakter van de inbreuk.

Om te zorgen voor een reële verantwoordingsplicht voor de cyberbeveiligingsmaatregelen op organisatorisch niveau, bevat NIS2 bepalingen inzake de aansprakelijkheid van natuurlijke personen met leidinggevende functies in de entiteiten die onder het toepassingsgebied van de nieuwe NIS-richtlijn vallen.

## Hoe stelt de Commissie voor om de cybercrisisbeheersing te verbeteren?

De nieuwe regels verbeteren de manier waarop de EU grootschalige cyberincidenten en -crises voorkomt, behandelt en reageert. Zij doen dit door duidelijke verantwoordelijkheden, passende planning en meer EU-samenwerking in te voeren. NIS2 verplicht de lidstaten om nationale autoriteiten aan te wijzen die verantwoordelijk zijn voor cybercrisisbeheersing, voert nationale grootschalige plannen voor cyberincidenten en crisisrespons in, en richt het Europees netwerk voor cybercrisisverbindingsorganisatie (EU-CYCLONe) op ter ondersteuning van het gecoördineerde beheer van grootschalige cyberincidenten en crisissituaties op operationeel niveau. Dit netwerk is een belangrijke component die bijdraagt tot de totstandbrenging van het EU-kader voor cybercrisisbeheersing dat de Commissie in 2017 heeft geschetst met de aanbeveling over gecoördineerde respons op grootschalige incidenten en crises.

## Welke lidstaat heeft rechtsmacht over de entiteiten die onder het toepassingsgebied van NIS 2 vallen?

In de regel worden essentiële en belangrijke entiteiten geacht onder de jurisdictie te vallen van de lidstaat waar zij zijn gevestigd. Indien de entiteit in meer dan één lidstaat is gevestigd, moet zij onder de jurisdictie van elk van deze lidstaten vallen. De bevoegde autoriteiten van elk van deze lidstaten dienen samen te werken, elkaar wederzijdse bijstand te verlenen en, in voorkomend geval, gezamenlijke toezichtmaatregelen uit te voeren. Er zijn verschillende uitzonderingen op deze regel:

- aanbieders van openbare elektronische-communicatienetwerken of -aanbieders of openbare elektronische-communicatiediensten vallen onder de jurisdictie van de lidstaat waar zij hun diensten aanbieden.
- overheidsinstanties vallen onder de bevoegdheid van de lidstaat waar zij zijn gevestigd.
- bepaalde soorten entiteiten vallen onder de jurisdictie van de lidstaat waar zij hun hoofdvestiging in de Unie hebben. Deze entiteiten omvatten aanbieders van domeinnaamsysteemdiensten, registers van topdomeinnamen, entiteiten die domeinnaamregistratiediensten aanbieden, aanbieders van cloud computingdiensten, aanbieders van datacenterdiensten, aanbieders van netwerken voor contentlevering, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, onlinezoekmachines en socialenetwerkplatforms. Dit moet ervoor zorgen dat dergelijke entiteiten niet te maken krijgen met een groot aantal verschillende wettelijke vereisten, aangezien zij in bijzonder hoge mate grensoverschrijdende diensten verlenen. Met het oog op doeltreffend toezicht moeten de lidstaten dit soort entiteiten onder meer meedelen wanneer de hoofdvestiging van de entiteit en haar andere juridische vestigingen in de Unie of, indien zij niet in de Unie zijn gevestigd, de plaats waar de vertegenwoordiger van de entiteit is aangewezen, in kennis stellen. Enisa zou verplicht zijn een register op te zetten en bij te houden met de op basis daarvan door de lidstaten verstrekte informatie.

## Hoe zullen de regels de samenwerking verbeteren?

De samenwerking tussen de EU wordt bevorderd door de lidstaten in staat te stellen gezamenlijk op te treden en opkomende veiligheidsrisico’s als gevolg van de lopende digitale transformatie aan te pakken.

Meer in het bijzonder zullen de lidstaten gezamenlijk toezicht kunnen houden op de tenuitvoerlegging van de EU-regels en elkaar wederzijds kunnen bijstaan in het geval van grensoverschrijdende wanpraktijken, een meer gestructureerde dialoog met de particuliere sector kunnen voeren en de openbaarmaking van kwetsbaarheden in software en hardware die op de interne markt worden verkocht, kunnen coördineren. Zij zullen ook op gecoördineerde wijze kunnen werken om de

veiligheidsrisico’s en -bedreigingen in verband met nieuwe technologieën te beoordelen, zoals voor het eerst met 5G.

Delidstaten zullen gebruikmaken van EU-samenwerking om de nationale capaciteiten te verbeteren door middel van uitwisseling van personeel tussen autoriteiten en collegiale toetsingen. De bestaande groepen, met name de samenwerkingsgroep die nationale cyberbeveiligingsautoriteiten en het netwerk van responsteams voor computerbeveiligingsincidenten (CSIRT’s) bijeenbrengt, zullen bijdragen tot de bevordering van de samenwerking op zowel strategisch als technisch niveau.

## Hoe verhoudt dit initiatief zich tot ander EU-beleid?

De NIS2-richtlijn is nauw verbonden met twee andere initiatieven, de richtlijn inzake de veerkracht van kritieke entiteiten (CER) en de verordening inzake digitale operationele veerkracht voor de financiële sector (wet inzake digitale operationele veerkracht, DORA).

Het toepassingsgebied van de NIS 2 en de richtlijn inzake de veerkracht van kritieke entiteiten (CER-richtlijn) is grotendeels afgestemd om ervoor te zorgen dat de fysieke en cyberweerbaarheid van kritieke entiteiten op alomvattende wijze wordt aangepakt. Entiteiten die in het kader van de CER-richtlijn als kritieke entiteiten zijn aangemerkt, worden ook onderworpen aan de cyberbeveiligingsverplichtingen van de NIS2-richtlijn. Voorts moeten de nationale bevoegde autoriteiten in het kader van de CER- en de NIS2-richtlijn regelmatig relevante informatie uitwisselen, zoals over risico’s, cyberdreigingen en -incidenten en over niet-cyberrisico’s, dreigingen en incidenten. De samenwerkingsgroep in het kader van NIS2 zal regelmatig en ten minste eenmaal per jaar bijeen moeten komen met de krachtens de CER-richtlijn opgerichte Groep voor de veerkracht van kritieke entiteiten.

Wat de financiële sectorbetreft, zal DORA, hoewel de nieuwe NIS-richtlijn kredietinstellingen, exploitanten van handelsplatformen en centrale tegenpartijen omvat die onder het toepassingsgebied ervan vallen, op deze entiteiten van toepassing zijn wat betreft verplichtingen inzake risicobeheer en rapportage op het gebied van cyberbeveiliging. Tegelijkertijd is het belangrijk om een sterke relatie te onderhouden voor de uitwisseling van informatie tussen de financiële sector en de andere sectoren die onder NIS 2 vallen. Daartoe zouden de Europese toezichthoudende autoriteiten (ESA’s) voor de financiële sector en de nationale bevoegde autoriteiten in de financiële sector in het kader van de DORA kunnen deelnemen aan de besprekingen van de NIS-samenwerkingsgroep. Bovendien zouden de bevoegde autoriteiten van DORA relevante informatie kunnen raadplegen en delen met het centrale contactpunt (SPOC’s) en CSIRT’s die zijn opgericht in het kader van NIS2. De bevoegde autoriteiten, SPOC’s of de CSIRT’s die in het kader van NIS2 zijn opgericht, ontvangen ook gegevens over belangrijke ICT-gerelateerde incidenten van de bevoegde autoriteiten in het kader van DORA. Bovendien moeten de lidstaten de financiële sector blijven opnemen in hun cyberbeveiligingsstrategieën en kunnen de nationale CSIRT’s de financiële sector in hun activiteiten bestrijken.

## Wat zijn de volgende stappen?

Delidstaten moeten de richtlijn uiterlijk op 17 oktober 2024 (21 maanden na de inwerkingtreding van de NIS2) omzetten. Vervolgens moet de Commissie de werking van de richtlijn periodiek evalueren en hierover vóór 17 oktober 2027 voor het eerst verslag uitbrengen aan het Parlement en de Raad.