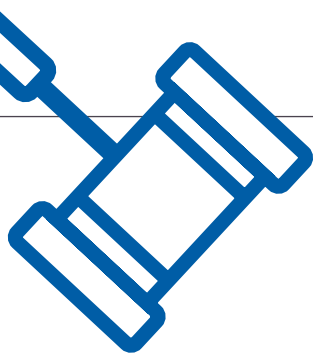


NIS2 en CRA: uitstel is geen optie meer

Nieuwe EU-regels dwingen organisaties tot actie

Zowel de NIS2 als de Cyber Resilience Act treden op korte termijn in werking. Voldoen aan deze Europese regelgeving op het gebied van cybersecurity en cyberweerbaarheid kan flinke inspanningen vereisen van de organisaties die er aan moeten voldoen, ziet Louise de Gier.

IN 2026 WORDT EINDELIJK DE NIS2, DE NETWERK EN INFORMATIE-BEVEILIGINGSRICHTLIJN GEÏMPLEmenteerd in de Nederlandse Cyberbeveiligingswet (Cbw). Dit had al in oktober 2024 moeten gebeuren. De verwachting is dat de Cbw in het tweede kwartaal van 2026 in werking zal treden. Het moment voor bedrijven om actie te nemen kan niet langer worden uitgesteld. In december 2024 is de Cyber Resilience Act (CRA) van kracht geworden en is de gefaseerde inwerkingtreding van drie jaar van start gegaan om bedrijven de tijd te geven aan de CRA te voldoen. De CRA wordt eind 2027 van kracht. De CRA heeft betrekking op de cyberweerbaarheid van producten met digitale elementen. Vanaf 11 september 2026 worden bedrijven echter al verplicht om te voldoen aan de rapportageverplichtingen. Dus ook hier moeten bedrijven aan de slag. Er staan bovendien hoge boetes op het niet nakomen van deze meldplicht.

> Voor de risicoanalyse op grond van de CRA is geen voorgeschreven methode

Van toepassing

De NIS2 geldt voor organisaties die diensten verlenen of activiteiten ontplooien in de EU, ook als ze buiten de EU gevestigd zijn. De NIS2 is van toepassing op achttien sectoren, zoals energie, vervoer, digitale infrastructuur, beheer van ICT-diensten, vervaardiging van chemische producten, fabrikanten van onder ander machines, apparaten, werktuigen, transportmiddelen en de overheid. De NIS2 is van toepassing als organisaties voldoen aan bepaalde drempelwaarden. Het minimum is een omzet of balanstotaal van €10 miljoen of een personeelsbestand van 49 personen of meer. Daarnaast geldt de NIS2 voor bepaalde organisaties die niet aan een drempelwaarde moeten voldoen, zoals overheidsinstanties en openbare elektronische communicatienetwerken of -diensten. Vervolgens wordt er nog een onderscheid gemaakt tussen een

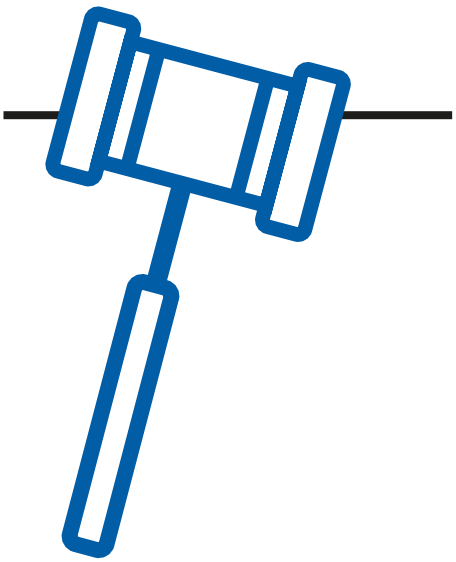
Beelden: Shutterstock

belangrijke en essentiële entiteit. Bij essentiële entiteiten (minimum jaaromzet van €50 miljoen of een balanstotaal van €43 miljoen of meer dan 249 medewerkers) is er sprake van pro actief toezicht. De toezichthoudende autoriteiten kunnen uit eigen beweging bij een bedrijf binnenkomen of informatie opvragen. De boetes zijn hoger dan bij belangrijke entiteiten.

Of de NIS2 van toepassing is, is lang niet altijd makkelijk te bepalen. In de bijlagen I en II bij de NIS2 met de sectoren wordt verwezen naar andere Europese regelgeving waarin definities van begrippen zoals vervoer, energie, fabrikanten van machines of beheerder van ICT-diensten zijn opgenomen. De definities zijn soms niet één op één toe te passen op de dienstverlening van een organisatie.

Bij bedrijven die onderdeel zijn van een concern kan het daarnaast soms lastig zijn om de drempelwaarden te berekenen omdat niet alleen moet worden uitgegaan van de eigen entiteit maar ook van de partner of verbonden onderneming [(1)]. Daarnaast kan de regelgeving per Europees land verschillen omdat de nationale lidstaten bij de implementatie van de NIS2 eigen keuzes mogen maken. Ook kan dezelfde onderneming zowel als belangrijke als essentiële entiteit kwalificeren omdat de onderneming in meerdere sectoren actief is. En als de NIS2 niet rechtstreeks op de onderneming van toepassing is kan de NIS2 toch indirect van groot belang zijn omdat bedrijven en overheden verantwoordelijk zijn voor de cyberveiligheid van de kritieke directe toeleveranciers en dienstverleners. De toezichthouders eisen dat de onderneming of overheid waarop de NIS2 van toepassing is, kan aantonen

Cyberbeveiligingsrisico's moeten tot een minimum worden beperkt



dat er passende afspraken gemaakt zijn met de kritieke toeleveranciers en dienstverleners.

Wie werkt met CRA?

De CRA is van toepassing op producten met digitale elementen die op de markt zijn gebracht in de EU na 11 december 2027, of substantieel zijn aangepast na die datum. Dit geldt ook voor leveranciers van buiten de EU. Dat kan software of hardware zijn met internetconnectiviteit of netwerkcapaciteit of met het internet verbonden consumentenproducten. Diensten vallen niet onder de CRA. Afzonderlijke software- en hardwarecomponenten vallen er wel onder.

De CRA is van toepassing op producten met digitale elementen die commercieel worden aangeboden in de Europese Unie. Er zijn geen drempelwaarden zoals bij de NIS2. Wel zijn bepaalde productcategorieën uitgezonderd, zoals medische hulpmiddelen, producten voor motorvoertuigen, burgerlijke luchtvaart en uitrusting van zeeschepen.

Ook hier kan het lastig zijn om te bepalen of de CRA van toepassing is. Een app die kan worden gedownload via een app store, software die samen met hardware wordt geleverd zoals het besturingssysteem van een laptop en smart home systemen vallen onder de CRA. Pure SaaS die volledig als dienst draait op de servers van de leverancier valt niet onder de CRA. Andere SaaS kan weer wel onder de CRA vallen. Een vaatwasmachine met embedded software voor het vaatwasprogramma maar zonder mogelijkheden om te verbinden met andere producten of netwerken valt niet onder de CRA.

Reguliere producten met digitale elementen vormen de laagste categorie. Daarnaast wordt onderscheid gemaakt tussen klasse 1: belangrijke producten met digitale elementen, zoals software en hardware voor identiteit beheer, netwerkbeheersystemen, besturingssystemen, virtuele assistenten voor slimme huizen, beveiligingscamera's, alarmsystemen, en klasse 2: belangrijke producten, zoals firewalls, manipulatiebestendige microprocessoren en microcontrollers. De zwaarste categorie zijn kritieke producten met digitale elementen, zoals hardware-apparaten met een beveiligingskastje en smartcards. Het onderscheid is van belang voor de risicoanalyse en de vereisten waaraan de conformiteitsbeoordeling moet voldoen.

Er gelden verplichtingen voor fabrikanten, importeurs en distributeurs. De meeste verplichtingen gelden voor de fabrikanten, deze worden in dit artikel benoemd. Een importeur of distributeur die ingrijpende wijzigingen doorvoert op een product wordt gezien als fabrikant.

Risicoanalyse op hoofdlijnen

Zowel de NIS2 als de CRA verplichten tot het uitvoeren van een risicoanalyse.

NIS2/Cbw

De risicoanalyse moet per entiteit worden uitgevoerd, gebaseerd op een all hazard benadering. Denk dus ook aan personen die betrokken zijn bij de beveiliging van netwerk- en informatiesystemen, benodigd materieel, toegang, imago et cetera. Het beleid moet schriftelijk worden vastgelegd en aantoonbaar worden toegepast. Breng in kaart wat er mis kan gaan, wat is de kans dat dit gebeurt, wat zijn de gevolgen en welke acties moeten worden genomen in geval van een incident. Wat is essentieel voor de organisatie?

Bij deze risicoanalyse moeten ook de kritieke toeleveranciers en dienstverleners die impact kunnen hebben op de netwerk- en informatiesystemen betrokken worden.

Op basis van de risicoanalyse moet een overzicht worden opgesteld van de risico's met betrekking tot de beveiliging van de netwerk- en informatiesystemen en moeten maatregelen genomen worden als de risicoanalyse daartoe aanleiding geeft [2].

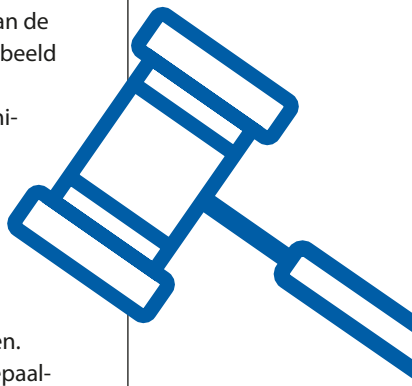
De risicoanalyse die op basis van de Cbw moet worden uitgevoerd kan onderdeel zijn van een grotere of gecombineerde risicoanalyse, zoals de analyse op basis van de CRA.

CRA

Net zoals bij de NIS2 is er voor de risicoanalyse op grond van de CRA geen voorgeschreven methode om de risico's te analyseren. De risicoanalyse heeft betrekking op de cyberbeveiligingsrisico's die verbonden zijn aan een product met digitale elementen tijdens de plannings-, ontwerp-, ontwikkelings-, productie-, leverings- en onderhoudsfase. De cyberbeveiligingsrisico's moeten tot een minimum beperkt worden onder meer met betrekking tot de gezondheid en veiligheid van gebruikers [3].

De beoordeling van de aanpak van de geïdentificeerde risico's moet schriftelijk worden vastgelegd om ervoor te zorgen dat het product voldoet aan de relevante essentiële eisen, bijvoorbeeld geharmoniseerde normen. Als slechts een deel van de geharmoniseerde norm wordt toegepast of de norm niet alle relevante eisen dekt, moet dat worden vastgelegd. De beoordeling van de geïdentificeerde risico's moet in de technische documentatie worden opgenomen. Dat moet ook gebeuren indien bepaalde cyberbeveiligingsvereisten niet van toepassing zijn [4].

De risicoanalyse heeft betrekking op het gehele product met digitale elementen gedurende de levensduur inclusief gegevensverwerking en ondersteunende functies. Uitgegaan moet



Reacties en bijdragen

Voor reacties en nieuwe bijdragen van IT-experts:

Tanja de Vrede
020-2467230
t.d.vrede@agconnect.nl

worden van het beoogde doel van het gebruik en het redelijkerwijs voorzienbare gebruik en misbruik van het product. Dit kan een lastige inschatting zijn, bijvoorbeeld voor de fabrikant van een component.

Verplichtingen op hoofdlijnen

NIS2

Risicoanalyse per entiteit

Registratieplicht: Voor alle organisaties die onder de Cbw vallen geldt een registratieplicht.

Beleid met betrekking tot: bedrijfscontinuïteit, zoals back-up en crisisbeheer, beveiliging toeleverancierssketen, beveiliging netwerk- en informatiesystemen, zoals reageren en communiceren over kwetsbaarheden, effectiviteit maatregelen cyberbeveiligingsrisico's, kennis, beoordeling en goedkeuring cybermaatregelen door het bestuur (het bestuur is verantwoordelijk en aansprakelijk voor cybermanagement), cyberhygiëne, zoals opleiding bestuur en personeel, cryptografie en encryptie, beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en assets, multifactorauthenticatie, beveiligde spraak-, video- en tekst – en noodcommunicatie systemen, gerichte attenderingen, beveiligingsadviezen en dreigingsinformatie.

Incident Response beleid: plan om incidenten te voorkomen, opsporen, analyseren en beperken.

Meldplicht: incidenten die hebben plaatsgevonden moeten worden gemeld en bestaat uit vier fases: vroegtijdige waarschuwing (24 uur), verdere incidentmelding (binnen 72 uur), tussentijds verslag op verzoek van CSIRT[5] of bevoegde autoriteit, eindverslag (binnen een maand).

CRA

Risico analyse door fabrikanten

Cybersecurity-eisen aan producten en processen: producten mogen alleen op de markt gebracht worden als ze voldoen aan bepaalde cybersecurityvereisten en de technische documentatie gereed is [6]. Producten moeten ontworpen, ontwikkeld en geproduceerd worden in overeenstemming met deze vereisten.

Beoordeling van de cyberbeveiligingsrisico's: wordt schriftelijk vastgelegd en opgenomen in de technische documentatie en zo nodig bijgewerkt tijdens de ondersteuningsperiode. De beveiliging van een product wordt regelmatig getest en geëvalueerd.

Kwetsbaarheden: het product hoeft niet vrij te zijn van alle kwetsbaarheden maar bevat geen actief uitgebuite kwetsbaarheden [7]. Kwetsbaarheden moeten onverwijld worden aangepakt en verholpen onder meer door beveiligingsupdates. De fabrikant beschikt over passend beleid met betrekking tot openbaarmaking, invoeren en handhaven van kwetsbaarheden [8].

Component: bij integratie van componenten zorgen fabrikanten ervoor dat de cyberbeveiliging niet in gevaar komt. Dit geldt ook voor open source componenten.

Ondersteuningsperiode: de fabrikant bepaalt een ondersteuningsperiode gelijk aan de verwachte levensduur van een product met een minimum van 5 jaar tenzij de levensduur korter is.

Conformiteitsbeoordeling: Dat een product conform is, kan worden aangetoond door een Europees cyberbeveiligingscertificaat of op basis van procedures. De eisen die hieraan gesteld worden verschillen voor reguliere, belangrijke of kritieke producten met digitale elementen [9]. De belangrijkste functionaliteit van een product bepaalt in welke categorie het product valt [10].

Rapportageverplichting: de fabrikant moet elke actief uitgebuite kwetsbaarheid en elk ernstig incident [11] melden aan het CSIRT en aan Enisa [12] binnen 24 uur en nadere informatie binnen 72 uur na kennisname verstrekken. Bij een actief uitgebuite kwetsbaarheid moet uiterlijk 14 dagen nadat een corrigerende of risicobeperkende maatregel beschikbaar is een eindverslag worden verstrekt. In geval van een ernstig incident moet binnen een maand na indiening van de melding een eindverslag worden verstrekt.

Referenties

1 Artikel AG Connect – 2025, Louise de Gier, Verborgen impact op verbonden ondernemingen.
2 Cyberbeveiligingsbesluit art. 7 lid 4 en 5
3 Artikel 13.2 en 13.4 Verordening cyberweerbaarheid.
4 Art. 13.4 Verordening cyberweerbaarheid en art. 4.1.1 Blauwe Gids 2022.
5 Het door de overheid aangewezen Computer Security Incident Response Team. In Nederland is dit het NCSC naast andere sectorale instellingen.
6 Verordening cyberweerbaarheid, deel I en II van bijlage I.
7 Actief uitgebuite kwetsbaarheid: een kwetsbaarheid waarvoor betrouwbare bewijzen bestaan dat een kwaadwillige actor die heeft uitgebuit in een systeem zonder toestemming van de systeemeigenaar.
8 Kwetsbaarheid: een zwakheid, vatbaarheid of een gebrek van een product met digitale elementen di/dat door een cyberdreiging kan worden uitgebuit.
9 Verordening cyberweerbaarheid, art. 31 en 32
10 Uitvoeringsverordening (EU) 2025/2392 van de Commissie, overweging 2
11 Het begrip 'ernstig' wordt gedefinieerd in de Verordening Cyberweerbaarheid, art. 14.5
12 European Union Agency for Cybersecurity

Louise de Gier
is IT- en IE-advocaat
bij BOLT Advocaten
in Utrecht.