Ministerie van Economische Zaken

Gids Cyber Resilience Act

Versie 2.0

Inhoudsopgave

Leeswijzer en disclaimer
U bent fabrikant, importeur of distributeur van een product met digitale elementen. Dan zult u met de Cyber Resilience Act te maken gaan krijgen. Voor u is deze gids samengesteld, een hulpmiddel om op een toegankelijke manier inzicht in de belangrijkste aspecten van de Cyber Resilience Act te krijgen. Aan de inhoud van deze gids kunnen geen rechten worden ontleend. De wettekst van de Cyber Resilience Act blijft altijd leidend.

Heeft u feedback op deze gids?
E-mail dan naar teamcra@minezk.nl. Uw feedback wordt gebruikt om deze gids te verbeteren.

Leest u een geprinte versie van deze gids?
Op www.ondernemersplein.overheid.nl vindt u altijd de laatste versie.

De Cyber Resilience Act

De Cyber Resilience Act (CRA), in het Nederlands de Verordening cyberweerbaarheid, is een Europese verordening die zich richt op het verbeteren van de beveiliging van producten met digitale elementen. Gebruikers in de EU moeten erop kunnen vertrouwen dat producten digitaal veilig zijn. Door de CRA moeten digitale producten aan essentiële veiligheidseisen voldoen en moeten deze producten voor de hele verwachte gebruiksduur van het product veilig gehouden worden door veiligheidsupdates. Dit zorgt ervoor dat consumenten en bedrijven veilig gebruik kunnen maken van digitale producten.

Op 10 december 2024 is de CRA in werking getreden en daarmee is de gefaseerde inwerkingtredingstermijn van in totaal drie jaar van start gegaan. Tijdens deze periode worden technische normen uitgewerkt en wordt tijd geboden aan fabrikanten om al tijdens de ontwikkeling van een product met digitale elementen rekening te houden met de eisen uit de CRA. Vanaf 11 september 2026 gaat de meldplicht voor actief misbruikte kwetsbaarheden en incidenten in. Vanaf 11 december 2027 gaan alle eisen in en moeten alle producten met digitale elementen die op de Europese markt gebracht worden voldoen aan de CRA.[1]

De volledige wettekst vindt u hier.[2]

Wat betekent de Cyber Resilience Act voor uw organisatie?

De CRA is van toepassing op producten met digitale elementen die op de Europese markt aangeboden worden en maakt een verdeling in vier verschillende soorten producten. Sommige producten met digitale elementen zijn uitgezonderd, bijvoorbeeld omdat zij al onder andere wetgeving vallen. Het is van belang of u het product met digitale elementen als fabrikant, importeur of distributeur op de Europese markt brengt. Afhankelijk van het soort product en welk type marktdeelnemer u bent zijn er andere verplichtingen van toepassing.

[1] Voor draadloos verbonden apparatuur (zoals laptops, slimme deurbellen, etc.) geldt overigens al vanaf augustus 2025 dat deze aan cybersecurityeisen moeten voldoen op grond van de Radio Equipment Directive.

[2] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202402847.

Begrippenlijst[3]

Product met digitale elementen: een software- of hardwareproduct en zijn oplossingen voor gegevensverwerking op afstand, met inbegrip van software- of hardwarecomponenten die afzonderlijk in de handel worden gebracht.

Gegevensverwerking op afstand: gegevensverwerking vanop een afstand waarvoor de software is ontworpen en ontwikkeld door de fabrikant of onder de verantwoordelijkheid van de fabrikant, en bij gebreke waarvan het product met digitale elementen een van zijn functies niet zou kunnen vervullen.

Fabrikant: een natuurlijke of rechtspersoon die producten met digitale elementen ontwikkelt of vervaardigt of die producten met digitale elementen laat ontwerpen, ontwikkelen of vervaardigen, en die onder zijn naam of merk tegen betaling, met een verdienmodel of gratis in de handel brengt.

Importeur: een in de Unie gevestigde natuurlijke of rechtspersoon die een product met digitale elementen in de handel brengt dat de naam of het merk van een buiten de Unie gevestigde natuurlijke of rechtspersoon draagt.

Distributeur: een andere natuurlijke of rechtspersoon in de toeleveringsketen dan de fabrikant of de importeur, die een product met digitale elementen in de Unie op de markt aanbiedt zonder de eigenschappen daarvan te beïnvloeden.

Ingrijpende wijziging: een wijziging van het product met digitale elementen nadat het in de handel is gebracht, die gevolgen heeft voor de conformiteit van het product met digitale elementen met de essentiële cyberbeveiligingsvereisten van deel I van bijlage I of leidt tot een wijziging van het beoogde doel waarvoor het product met digitale elementen is beoordeeld.

Beoogde doel: het gebruik waarvoor een product met digitale elementen door de fabrikant is bedoeld, met inbegrip van de specifieke context en voorwaarden van het gebruik, zoals gespecificeerd in de informatie die door de fabrikant in de gebruiksinstructies, reclame- of verkoopmaterialen en verklaringen, alsook in de technische documentatie is verstrekt.

Redelijkerwijs voorzienbaar gebruik: gebruik dat niet noodzakelijk het beoogde doel is dat door de fabrikant in de gebruiksinstructies, reclame- of verkoopmaterialen en verklaringen, alsook in de technische documentatie is verstrekt, maar dat waarschijnlijk voortvloeit uit redelijkerwijs voorzienbaar menselijk gedrag of redelijkerwijs voorzienbare technische handelingen of interacties.

[3] Artikel 3 Cyber Resilience Act (Definities).

CE-markering: een markering waarmee een fabrikant aangeeft dat een product met digitale elementen en de door de fabrikant ingestelde processen in overeenstemming zijn met de essentiële cyberbeveiligingsvereisten van bijlage I en andere toepasselijke harmonisatiewetgeving van de Unie die in het aanbrengen ervan voorziet.

Conformiteitsbeoordeling: het proces waarbij wordt nagegaan of aan de essentiële cyberbeveiligingsvereisten van bijlage I is voldaan.

Actief uitgebuite kwetsbaarheid: een kwetsbaarheid waarvoor betrouwbare bewijzen bestaan dat een kwaadwillige actor die heeft uitgebuit in een systeem zonder toestemming van de systeemeigenaar.

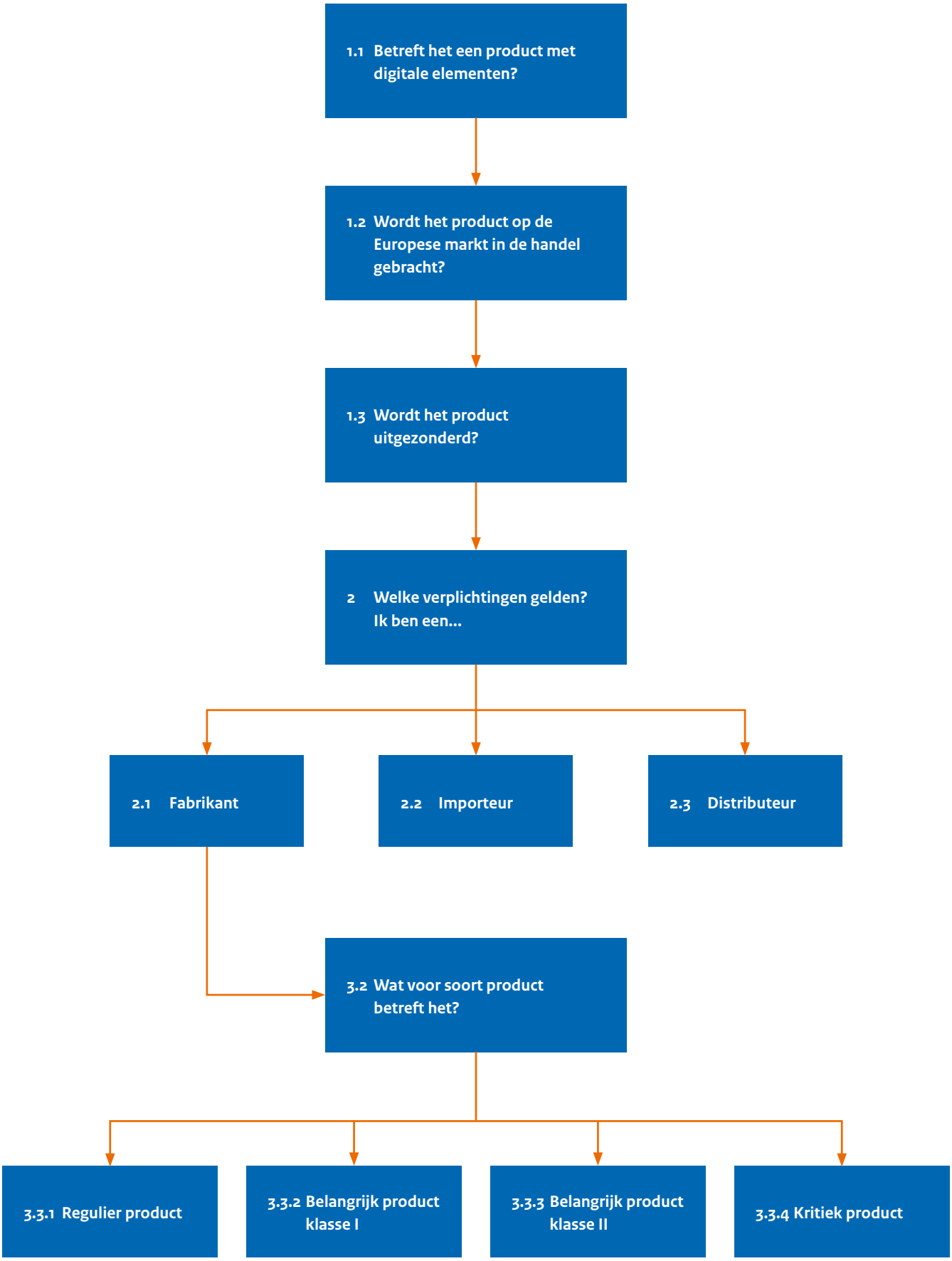
Incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen: een incident dat negatieve gevolgen heeft of kan hebben voor het vermogen van een product met digitale elementen om de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of functies te beschermen.

Ondersteuningsperiode: de periode gedurende welke een fabrikant ervoor moet zorgen dat kwetsbaarheden van een product met digitale elementen doeltreffend en in overeenstemming met de essentiële cyberbeveiligingsvereisten van deel II van bijlage I worden aangepakt.

Kwetsbaarheid: een zwakheid, vatbaarheid of gebrek van een product met digitale elementen die/dat door een cyberdreiging kan worden uitgebuit.

Geharmoniseerde norm: een geharmoniseerde norm zoals gedefinieerd in artikel 2, punt 1, c), van Verordening (EU) nr. 1025/2012.

Conformiteitsbeoordelingsinstantie: een conformiteitsbeoordelingsinstantie zoals gedefinieerd in artikel 2, punt 13, van Verordening (EG) nr. 765/2008.


1.1 Betreft het een product met digitale elementen?
1.2 Wordt het product op de Europese markt in de handel gebracht?
1.3 Wordt het product uitgezonderd?
2 Welke verplichtingen gelden? Ik ben een...
2.1 Fabrikant
2.2 Importeur
2.3 Distributeur
3.2 Wat voor soort product betreft het?
3.3.1 Regulier product
3.3.2 Belangrijk product klasse I
3.3.3 Belangrijk product klasse II
3.3.4 Kritiek product

1 Toepassingsbereik van de Cyber Resilience Act

1.1 Betreft het een product met digitale elementen?

In beginsel vallen alle **producten met digitale elementen** die in de Europese Unie (EU) in de handel worden gebracht onder de Cyber Resilience Act (CRA). Onder producten met digitale elementen vallen alle software en hardware producten en bijbehorende **oplossingen voor gegevensverwerking op afstand**. Diensten vallen niet onder de CRA. Een oplossing voor gegevensverwerking op afstand valt alleen onder de CRA wanneer het essentieel is voor de functionaliteit van een product met digitale elementen dat onder de CRA valt. Ook afzonderlijke software- en hardwarecomponenten vallen onder de CRA.

1.2 Wordt het product op de Europese markt in de handel gebracht?

De CRA vereist dat een product met digitale elementen in de handel wordt gebracht. Dit betekent dat een product met digitale elementen voor het eerst in de Unie op de markt aanboden moet worden. Om onder de CRA te vallen, moet een product met digitale elementen in het kader van een handelsactiviteit, ofwel commercieel aangeboden moeten worden. Niet-commercieel aangeboden (open-source) software of producten die voor intern gebruik worden ontwikkeld vallen niet onder de CRA.

De verplichtingen van de CRA zijn gekoppeld aan het op de markt aanbieden van een product met digitale elementen, en gelden dus alleen in situaties waarbij het product commercieel wordt aangeboden.

1.3 Uitzonderingen

Verschillende producten met digitale elementen zijn al gereguleerd door andere sectorspecifieke cybersecurityeisen en vallen daarom niet onder de CRA. Dit is het geval bij medische hulpmiddelen, producten voor motorvoertuigen, producten voor de burgerlijke luchtvaart en de uitrusting van zeeschepen.[4] Ook is de CRA niet van toepassing op reserveonderdelen die precies hetzelfde werken als het origineel, of producten die uitsluitend voor doeleinden van nationale veiligheid, defensie of de verwerking van gerubriceerde informatie zijn ontwikkeld.

[4] Artikel 2 lid 2 CRA benoemt de specifieke verordeningen en richtlijnen waarop de uitzonderingen zien.

2 Welke verplichtingen gelden?

In de Cyber Resilience Act (CRA) worden drie marktdeelnemers genoemd: de fabrikant, de importeur en de distributeur. Een **fabrikant** ontwikkelt of vervaardigt producten, of laat producten ontwerpen, ontwikkelen of vervaardigen, en brengt deze onder zijn (merk)naam in de handel. Een **importeur** is in de Europese Unie (EU) gevestigd en brengt een product in de handel dat de (merk)naam van een buiten de EU gevestigde partij draagt. Een **distributeur** is een andere partij in de toeleveringsketen dan de fabrikant of importeur, die een product in de EU op de markt aanbiedt zonder de eigenschappen te beïnvloeden. Importeurs of distributeurs die een product onder eigen naam in de handel brengen, of een **ingrijpende wijziging** uitvoeren op een product, worden ook gezien als fabrikant onder de CRA.

De CRA legt verplichtingen op aan de fabrikanten, en afgeleid voor importeurs en distribiteurs. De marktdeelnemers moeten ervoor zorgen dat de producten met digitale elementen aan bepaalde eisen (blijven) voldoen, ook zijn marktdeelnemers verplicht verantwoording af te leggen over de conformiteit aan deze eisen. Dit wordt gedaan door verschillende documentatie- en meldplichten.

2.1 Ik ben fabrikant

Een fabrikant is een natuurlijke of rechtspersoon die een product maakt (of laat ontwerpen en maken) en dat vervolgens onder zijn eigen naam of een handelsmerk op de markt brengt. Als fabrikant heeft u dezelfde plichten, of u nu in de EU of daarbuiten gevestigd bent. Vanaf de ontwerpfase moet u rekening houden met de CRA.

De CRA legt de volgende verplichtingen op aan fabrikanten:

- Bij het ontwerpen, ontwikkelen en produceren van het product zorgen dat het voldoet aan de essentiële cybersecurity-eisen. In paragraaf 3.1 van deze gids wordt ingegaan op de essentiële cybersecurity-eisen zoals die zijn opgenomen in bijlage I bij de CRA. Hiervoor moet een **cybersecurity-risicobeoordeling** uitgevoerd worden:
  - daartoe beoordeelt de fabrikant ten eerste de cyberbeveiligingsrisico's die verbonden zijn aan het product;
  - met deze cybersecurityrisicobeoordeling houdt de fabrikant rekening tijdens de plannings-, ontwerp-, ontwikkelings-, productie-, leverings- en onderhoudsfase van het product, om zo de cybersecurityrisico's tot een minimum te beperken, incidenten te voorkomen en de gevolgen daarvan zo veel mogelijk te beperken;
  - de beoordeling van de cyberbeveiligingsrisico's omvat ten minste een analyse van cyberbeveiligingsrisico's op basis van het **beoogde doel** en het **redelijkerwijs voorzienbaar gebruik**, alsook de voorwaarden van het gebruik, van het product met digitale elementen, zoals de operationele omgeving of de te beschermen activa, waarbij rekening wordt gehouden met de verwachte gebruiksduur van het product;
  - in de beoordeling van de cyberbeveiligingsrisico's wordt vermeld of, en zo ja op welke wijze, de beveiligingsvereisten van deel I, punt 2, van bijlage I bij de CRA, van toepassing zijn op het desbetreffende product met digitale elementen en op welke wijze die vereisten worden uitgevoerd op basis van de beoordeling van de cyberbeveiligingsrisico's;
  - ook wordt aangegeven hoe de fabrikant deel I, punt 1, van bijlage I, en de in deel II van bijlage I bij de CRA, vastgestelde vereisten inzake de respons op kwetsbaarheden toepast;
  - de cybersecurityrisicobeoordeling wordt gedocumenteerd en zo nodig bijgewerkt tijdens de ondersteuningsperiode.
  - indien van toepassing: ten aanzien van geïntegreerde componenten van derden heeft een fabrikant een passende zorgvuldigheidsverplichting, namelijk dat de fabrikant nagaat dat ook de van derden afkomstige geïntegreerde componenten of die de beveiliging van het product dat zij op de markt brengen niet in gevaar brengen. Componenten zijn ook producten die aan de CRA moeten voldoen, dus daarbij kan worden gekeken naar de **CE-markering**. Bij componenten die niet

los op de markt zijn aangeboden, dat kan met name het geval zijn bij open source componenten, moet de fabrikant dit op een andere manier nagaan.
- Vastleggen van de cyberbeveiligingsrisico's van het product in de **technische documentatie**.
- Uitvoeren van een **conformiteitsbeoordeling** om te controleren of het product aan de essentiële cybersecurity-eisen voldoet.
- Toevoegen van de volgende informatie op het product met digitale elementen:
  - Het type-, partij- of serienummer.
  - De zichtbare, leesbare en onuitwisbare CE-markering (tenzij niet mogelijk of gerechtvaardigd, op de verpakking).
- Toevoegen van de volgende informatie op de verpakking van het product of een bij het product toegevoegde document:
  - De naam, de geregistreerde handelsnaam of het geregistreerde merk.
  - Het postadres, het e-mailadres of andere digitale gegevens.
  - De website waarop contact met de fabrikant kan worden opgenomen.
- Bepalen van de verwachte gebruiksduur en het vermelden van de het einde van de ondersteuningstermijn bij het moment van aankoop door middel van de maand en het jaar.

2.1.1 *Kwetsbaarhedenrespons*

Nadat de producten door gebruikers in gebruik zijn genomen moet het product gedurende de verwachte gebruiksduur veilig worden gehouden, rekening houdende met redelijke verwachtingen, aard van het product, diens beoogde doel en EU-regelgeving die de levensduur van producten met digitale elementen bepaalt. De **ondersteuningsperiode** moet minstens vijf jaar zijn, tenzij de verwachte gebruiksperiode korter is.

Als er een **kwetsbaarheid** wordt ontdekt, moet daarvoor zo snel mogelijk een gratis veiligheidsupdate worden aangeboden. Alleen bij maatwerkoplossingen voor zakelijke afnemers mag contractueel worden afgesproken dat er wel kosten in rekening worden gebracht voor kwetsbaarhedenrespons.

Producten moeten worden aangeboden met de instelling dat updates in beginsel automatisch worden geïnstalleerd, waarbij wel een opt-out mogelijkheid moet worden gegeven als automatisch updaten niet gewenst wordt door de gebruiker. Bij producten voor industriële omgevingen wordt niet vereist dat er automatisch updates worden geïnstalleerd, want dat zou onwenselijk zijn.

2.1.2 *Meldplicht*

Fabrikanten moeten het melden als ze kennis krijgen van een actief misbruikte kwetsbaarheid of als er sprake is van een ernstig incident dat gevolgen heeft voor de beveiliging van het product. Dit geldt voor gepatchte en niet-gepatchte kwetsbaarheden. Vanaf 11 september 2026 moeten fabrikanten van producten met digitale elementen dit melden via het digitale meldloket van het Nationaal Cyber Security Centrum.[5] Deze melding is tegelijkertijd toegankelijk voor ENISA (Europees Agentschap voor netwerk- en informatiebeveiliging).

Bij een **actief uitgebuite kwetsbaarheid** moet de volgende informatie worden gemeld binnen de daarvoor geldende deadlines:

- Zonder onnodige vertraging en in ieder geval binnen 24 uur nadat de fabrikant er kennis van heeft gekregen: een vroegtijdige waarschuwing, met vermelding van:
  - de actief uitgebuite kwetsbaarheid

[5] Dit geldt voor fabrikanten die hun EU-hoofdvestiging in Nederland hebben. De verordening gaat ervan uit dat dit het geval is wanneer de besluiten met betrekking tot de cyberbeveiliging van zijn product met digitale elementen hoofdzakelijk in Nederland worden genomen. Indien de hoofdvestiging niet op die manier kan worden bepaald, is de lidstaat waar de fabrikant de vestiging met het grootste aantal werknemers in de Unie heeft bepalend: als dit Nederland is, meldt de fabrikant bij het NCSC. Indien de fabrikant de hoofdvestiging in een andere lidstaat heeft, moet de fabrikant in die lidstaat melden.

  - in voorkomend geval de lidstaten waarvan de fabrikant weet dat het product er beschikbaar is gesteld.
- Binnen 72 uur nadat de fabrikant kennis heeft gekregen: een kwetsbaarheidsmelding, met daarin algemene informatie, voor zover beschikbaar, over:
  - het desbetreffende product met digitale elementen;
  - de algemene aard van de uitbuiting en van de betroffen kwetsbaarheid;
  - alle genomen corrigerende of risicobeperkende maatregelen (patch);
  - corrigerende of risicobeperkende maatregelen die gebruikers kunnen nemen;
  - in voorkomend geval: hoe gevoelig de fabrikant de gemelde informatie acht.
- Binnen 14 dagen nadat een corrigerende of risicobeperkende maatregel (patch) beschikbaar is gesteld: een eindverslag, met tenminste de volgende informatie:
  - beschrijving van de kwetsbaarheid, inclusief de ernst en gevolgen ervan;
  - indien beschikbaar: informatie over de kwaadwillige actor die de kwetsbaarheid heeft uitgebuit;
  - details over de beveiligingsupdate of andere corrigerende maatregel die beschikbaar zijn gesteld om de kwetsbaarheid te verhelpen.

Bij elk ernstig **incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen** moet de volgende informatie worden gemeld binnen de daarvoor geldende deadlines:

- Zonder onnodige vertraging en in ieder geval binnen 24 uur nadat de fabrikant er kennis van heeft gekregen: een vroegtijdige waarschuwing, met vermelding van:
  - de actief uitgebuite kwetsbaarheid;
  - in voorkomend geval de lidstaten waarvan de fabrikant weet dat het product er beschikbaar is gesteld.
- Binnen 72 uur nadat de fabrikant kennis heeft gekregen: een incidentmelding, met daarin algemene informatie, voor zover beschikbaar, over:
  - de aard van het incident;
  - een eerste beoordeling van het incident;
  - alle genomen corrigerende of risicobeperkende maatregelen (patch);
  - corrigerende of risicobeperkende maatregelen die gebruikers kunnen nemen;
  - in voorkomend geval: hoe gevoelig de fabrikant de gemelde informatie acht.
- Binnen één maand na indiending van de incidentmelding: een eindverslag, met tenminste de volgende informatie:
  - gedetailleerde beschrijving van de kwetsbaarheid, inclusief de ernst en gevolgen ervan;
  - het soort bedreiging of de grondoorzaak die waarschijnlijk tot het incident heeft geleid;
  - toegepaste en lopende beperkende maatregelen.

De meldplicht geldt voor alle producten met digitale elementen in de EU, ook voor producten die vóór 11 december 2027 in de handel zijn gebracht.

2.2 Ik ben importeur

Een importeur is een in de Unie gevestigde natuurlijke of rechtspersoon die een product uit een land buiten de EU in de EU in de handel brengt. Als importeur moet u ervoor zorgen dat de fabrikant heeft voldaan aan alle verplichtingen in verband met het product dat u in de handel brengt.
Om een product met digitale elementen in de handel te mogen brengen moet de importeur ervoor zorgen dat:

- de fabrikant de juiste procedure voor de conformiteitsbeoordeling heeft gevolgd
- de fabrikant de technische documentatie heeft opgesteld, de CE-markering heeft aangebracht en aan alle traceerbaarheidsverplichtingen heeft voldaan (de vermelding van de contactgegevens van de fabrikant, het type, partij- of serienummer van het product).
- bij het product de nodige handleiding en veiligheidsinformatie zit in een voor consumenten en andere eindgebruikers gemakkelijk te begrijpen taal

- op het product, de verpakking of de documentatie uw naam, handelsnaam of handelsmerk en contactadres duidelijk vermeld staan.

Alleen producten met digitale elementen die voldoen aan de essentiële cyberbeveiligingsvereisten, waarbij de door de fabrikant ingestelde processen voor kwetsbaarhedenrespons voldoen aan de essentiële cyberbeveiligingsvereisten, mogen in de EU in de handel worden gebracht. Wanneer de importeur weet of redenen heeft om aan te nemen dat een product of de door de fabrikant ingestelde processen voor kwetsbaarhedenrespons niet aan de CRA voldoen, mag het product niet in de handel worden gebracht zolang dit niet door de fabrikant is hersteld. Als het product een significant cybersecurityrisico inhoudt moet de importeur dit melden aan de fabrikant en de toezichthouder/RDI.

De importeur moet er ook voor zorgen dat de nodige corrigerende maatregelen worden genomen als het product al in de handel is gebracht, zoals het in overeenstemming brengen met de regelgeving, terugroepen of van de markt halen. Ook moeten importeurs die kennis krijgen van een kwetsbaarheid in een product dit zonder onnodige vertraging laten weten aan de fabrikant.

2.3 Ik ben distributeur

Een distributeur is een natuurlijke of rechtspersoon in de toeleveringsketen die een product op de EU-markt brengt dat hij het product met digitale elementen heeft verkregen van een fabrikant, een importeur of een andere distributeur. Als distributeur moet u ervoor zorgen dat het product met digitale elementen aan de regels van de CRA voldoet wanneer u het in de handel brengt.

Voordat een distributeur een product met digitale elementen op de markt aanbiedt, gaat de distributeur zorgvuldig na of:

- het product met digitale elementen in voorzien van de CE-markering.
- het product met digitale elementen is voorzien van technische documentatie en de EU-conformiteitsverklaring.

3 Cybersecurityeisen voor producten die in de EU op de markt komen

3.1 Essentiële cyberbeveiligingsvereisten

Producten met digitale elementen moeten aan de in bijlage 1 bij de Cyber Resilience Act (CRA) genoemde cybersecurityeisen voldoen voordat ze in de Europese Unie (EU) op de markt aangeboden mogen worden. Deze eisen worden opgedeeld in:

Deel I Cyberbeveiligingsvereisten met betrekking tot de eigenschappen van producten met digitale elementen

1. Producten met digitale elementen worden zodanig ontworpen, ontwikkeld en geproduceerd dat zij een passend cyberbeveiligingsniveau op basis van de risico's waarborgen.
2. Op basis van de in artikel 13, lid 2, bedoelde beoordeling van cyberbeveiligingsrisico's en indien van toepassing, moeten producten met digitale elementen:

a. op de markt worden aangeboden zonder bekende uitbuitbare kwetsbaarheden;
b. op de markt worden aangeboden met een standaard beveiligde configuratie, tenzij anders overeengekomen tussen de fabrikant en de zakelijke gebruiker met betrekking tot een product met digitale elementen op maat, met inbegrip van de mogelijkheid om het product in zijn oorspronkelijke toestand te herstellen;
c. garanderen dat kwetsbaarheden kunnen worden aangepakt door middel van beveiligingsupdates, waaronder, indien van toepassing, door automatische beveiligingsupdates die worden geïnstalleerd binnen een passende termijn en die als standaardinstelling zijn ingeschakeld, met een duidelijk en gebruiksvriendelijk opt-outmechanisme, door de melding van beschikbare updates aan gebruikers, en door de mogelijkheid om die tijdelijk uit te stellen;
d. zorgen voor bescherming tegen ongeoorloofde toegang door middel van passende controlemechanismen, met inbegrip van maar niet beperkt tot authenticatie-, identiteits- of toegangsbeheersystemen, en melding maken van eventuele ongeoorloofde toegang;
e. de vertrouwelijkheid van opgeslagen, verzonden of anderszins verwerkte persoonsgegevens of andere gegevens beschermen, bijvoorbeeld door relevante inactieve gegevens of gegevens in overdracht met behulp van geavanceerde mechanismen te versleutelen, en door andere technische middelen te gebruiken;
f. de integriteit van opgeslagen, verzonden of anderszins verwerkte gegevens, persoonsgegevens of andere gegevens, commando's, programma's en configuraties beschermen tegen manipulatie of wijziging die niet door de gebruiker is toegestaan, en melding maken van beschadiging;
g. uitsluitend persoons- of andere gegevens verwerken die toereikend en ter zake dienend zijn en beperkt zijn tot wat noodzakelijk is met betrekking tot het **beoogde doel** van het product met digitale elementen (minimale gegevensverwerking);
h. de beschikbaarheid van essentiële en basisfuncties beschermen, ook na een incident, onder meer door middel van weerbaarheids- en beperkingsmaatregelen tegen denial of serviceaanvallen;
i. de negatieve impact van de producten zelf of van verbonden apparaten op de beschikbaarheid van diensten die door andere apparaten of netwerken worden geleverd, tot een minimum beperken;
j. worden ontworpen, ontwikkeld en geproduceerd om kwetsbaarheden voor aanvallen, met inbegrip van externe interfaces, te beperken;
k. worden ontworpen, ontwikkeld en geproduceerd om de gevolgen van een incident te beperken met behulp van passende mechanismen en technieken om uitbuiting te beperken;
l. beveiligingsgerelateerde informatie verstrekken door relevante interne activiteiten te registreren en te monitoren, met inbegrip van de toegang tot of wijziging van gegevens, diensten of functies, met een opt-outmechanisme voor de gebruiker;
m. gebruikers de mogelijkheid bieden om alle gegevens en instellingen veilig en gemakkelijk permanent te verwijderen en, indien die gegevens naar andere producten of systemen kunnen worden overgedragen, ervoor zorgen dat dat op een veilige manier gebeurt.

Deel II Vereisten inzake de respons op kwetsbaarheden

Fabrikanten van producten met digitale elementen moeten:

1. kwetsbaarheden en componenten in producten met digitale elementen vaststellen en documenteren, onder meer door een softwarestuklijst op te stellen in een algemeen gebruikt en machineleesbaar formaat waarin ten minste de afhankelijkheden van de producten op het hoogste niveau worden aangegeven;
2. in verband met de risico's die verbonden zijn aan producten met digitale elementen, kwetsbaarheden onverwijld aanpakken en verhelpen, onder meer door beveiligingsupdates te verstrekken; indien technisch haalbaar moeten nieuwe beveiligingsupdates afzonderlijk van de functionaliteitsupdates worden verstrekt;
3. de beveiliging van het product met digitale elementen op doeltreffende en regelmatige wijze testen en evalueren;
4. zodra een beveiligingsupdate beschikbaar is gesteld, informatie delen en openbaar maken over verholpen kwetsbaarheden, met inbegrip van een beschrijving van de kwetsbaarheden, informatie aan de hand waarvan gebruikers het betreffende product met digitale elementen kunnen identificeren, de gevolgen van de kwetsbaarheden, de ernst ervan en duidelijke en toegankelijke informatie die gebruikers helpt de kwetsbaarheden te verhelpen; in naar behoren gemotiveerde gevallen kunnen fabrikanten, wanneer zij van mening zijn dat de beveiligingsrisico's van openbaarmaking zwaarder wegen dan de beveiligingsvoordelen, het openbaar maken van informatie over een verholpen kwetsbaarheid uitstellen totdat de gebruikers de mogelijkheid hebben gekregen de desbetreffende patch uit te voeren;
5. een beleid inzake gecoördineerde openbaarmaking van kwetsbaarheden invoeren en handhaven;
6. maatregelen nemen om het delen van informatie over potentiële kwetsbaarheden in hun product met digitale elementen en in componenten van derden in dat product te vergemakkelijken, onder meer door een contactadres te verstrekken voor de melding van de kwetsbaarheden die in het product met digitale elementen zijn ontdekt;
7. voorzien in mechanismen om updates voor producten met digitale elementen veilig te verspreiden om ervoor te zorgen dat kwetsbaarheden tijdig en, waar van toepassing voor beveiligingsupdates, automatisch worden verholpen of beperkt;
8. ervoor zorgen dat, wanneer er beveiligingsupdates beschikbaar zijn om vastgestelde beveiligingsproblemen aan te pakken, die onverwijld en — tenzij anders overeengekomen tussen een fabrikant en een zakelijke gebruiker met betrekking tot een product met digitale elementen op maat — kosteloos worden verspreid, vergezeld van adviezen met relevante informatie voor gebruikers, onder meer over eventueel te nemen maatregelen.

Zoals te lezen is in paragraaf 2.1 van deze gids gelden de verplichtingen voor fabrikanten, welke afgeleide verplichtingen gelden voor importeurs en distributeurs zijn opgenomen in respectievelijk paragraaf 2.2 en 2.3 van deze gids. De importeur en distributeur moeten controleren of een fabrikant ervoor gezorgd heeft dat het product aan deze eisen voldoet, zodat ook producten van buiten de EU aan deze eisen voldoen.

Nadat de producten in gebruik zijn genomen door gebruikers moet het product met digitale elementen gedurende de verwachte gebruiksduur veilig worden gehouden.

3.1.1 *Risicobeoordeling*

Fabrikanten controleren door middel van een **risicobeoordeling** of het product met digitale elementen aan de in bijlage 1 bij de CRA genoemde cybersecurityeisen (zie ook paragraaf 3.1 van deze gids) voldoet voordat het in de EU op de markt wordt gebracht. De risicobeoordeling moet uitgevoerd worden in de

ontwerpfase, maar loopt door tot in de productiefase. Ook als u uw producten door anderen laat ontwerpen of produceren, bent u voor de risicobeoordeling verantwoordelijk. Het doel hiervan is dat fabrikanten de cybersecurityrisico's tot een minimum beperken, incidenten voorkomen en de gevolgen van incidenten met een minimum beperken.

De informatie over de risicobeoordeling moet in de **technische documentatie** worden opgenomen.

De technische documentatie moet ten minste de volgende informatie, voor zover van toepassing op het desbetreffende product met digitale elementen bevatten:

1. een algemene beschrijving van het product met digitale elementen, met inbegrip van:
   a. het beoogde doel ervan;
   b. versies van software die van invloed zijn op de naleving van de essentiële cyberbeveiligingsvereisten;
   c. wanneer het product met digitale elementen een hardwareproduct is, foto's of illustraties waarop de externe kenmerken, markering en interne lay-out te zien zijn;
   d. gebruikersinformatie en -instructies zoals beschreven in bijlage II bij de CRA;
2. een beschrijving van het ontwerp, de ontwikkeling en de productie van het product met digitale elementen en de procedures inzake de respons op kwetsbaarheden, met inbegrip van:
   a. noodzakelijke informatie over het ontwerp en de ontwikkeling van het product met digitale elementen, met inbegrip van, indien van toepassing, tekeningen en schema's en een beschrijving van de systeemarchitectuur waarin wordt uitgelegd hoe softwarecomponenten voortbouwen op elkaar of elkaar aanvullen en zijn geïntegreerd in de algemene verwerking;
   b. noodzakelijke informatie en specificaties van de door de fabrikant ingestelde processen inzake de respons op kwetsbaarheden, met inbegrip van de softwarestuklijst, het gecoördineerde beleid inzake openbaarmaking van kwetsbaarheden, bewijs van het verstrekken van een contactadres voor de melding van de kwetsbaarheden en een beschrijving van de gekozen technische oplossingen voor de veilige verspreiding van updates;
   c. noodzakelijke informatie en specificaties van de productie- en monitoringprocessen van het product met digitale elementen en de validering van die processen;
3. een beoordeling van de cyberbeveiligingsrisico's waartegen het product met digitale elementen wordt ontworpen, ontwikkeld, geproduceerd, geleverd en onderhouden, met inbegrip van de wijze waarop de essentiële cyberbeveiligingsvereisten van deel I van bijlage I van de CRA van toepassing zijn (zie ook paragraaf 3.1 van deze gids);
4. relevante informatie die in aanmerking is genomen om de ondersteuningsperiode van het product met digitale elementen te bepalen;
5. een lijst van de geheel of gedeeltelijk toegepaste geharmoniseerde normen waarvan de referenties in het Publicatieblad van de Europese Unie zijn bekendgemaakt, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelingen die zijn vastgesteld op grond van Verordening (EU) 2019/881 en, indien die geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelingen niet zijn toegepast, een beschrijving van de gekozen oplossingen om aan de essentiële cyberbeveiligingsvereisten van de delen I en II van bijlage I bij de CRA (zie ook paragraaf 3.1 van deze gids) te voldoen, met inbegrip van een lijst van andere relevante technische specificaties die zijn toegepast. In het geval van gedeeltelijk toegepaste geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsregelingen, wordt in de technische documentatie gespecificeerd welke delen zijn toegepast;
6. verslagen van de tests die zijn uitgevoerd om de conformiteit van het product met digitale elementen en van de procedures inzake de respons op kwetsbaarheden met de toepasselijke essentiële cyberbeveiligingsvereisten van de delen I en II van bijlage I bij de CRA (zie ook paragraaf 3.1 van deze gids) te verifiëren;
7. een exemplaar van de EU-conformiteitsverklaring;

8. indien van toepassing, de softwarestuklijst, ingevolge een met redenen omkleed verzoek van een markttoezichtautoriteit, op voorwaarde dat dat noodzakelijk is om die autoriteit in staat te stellen de naleving van de essentiële cyberbeveiligingsvereisten van bijlage I bij de CRA (zie ook paragraaf 3.1) te controleren.

3.1.2 *Technische normen*

De onder paragraaf 2.1 van deze gids genoemde cybersecurityeisen uit bijlage 1 bij de CRA worden door CEN/CENELEC en ETSI vertaald in concrete technische maatregelen waarmee een product aan de eis kan voldoen. Wanneer de Europese Commissie een norm goedkeurt is er sprake van een **geharmoniseerde norm**. Deze normen kunnen door fabrikanten gebruikt worden bij de conformiteitsbeoordeling van reguliere producten en belangrijke producten klasse 1. De verschillende soorten producten onder de CRA worden in de volgende paragraaf toegelicht.

3.2 Wat voor soort product betreft het?

De Cyber Resilience Act (CRA) maakt onderscheid tussen vier verschillende soorten producten:

1. Reguliere producten,
2. Belangrijke producten klasse 1,
3. Belangrijke producten klasse 2, en
4. Kritieke producten.

De hoofdregel is dat een fabrikant de conformiteitsbeoordeling zelf mag doen. Dit kan anders zijn wanneer het een belangrijk product met digitale elementen betreft. Producten met digitale elementen die zijn aangemerkt als kritiek product moeten altijd langs een conformiteitsbeoordelingsinstantie.

3.2.1 *Reguliere producten*

Onder reguliere producten worden alle producten met digitale elementen verstaan die niet als belangrijk of kritiek zijn aangemerkt in bijlage 3 en 4 van de CRA. Dit zijn bijvoorbeeld mobiele apps, videogames of netwerkapparatuur. Voor deze producten mag een zelfbeoordeling worden toegepast.

3.2.2 *Belangrijke producten klasse 1*

In bijlage 3 bij de CRA worden de belangrijke producten met digitale elementen genoemd. De belangrijke producten zijn in twee klassen verdeeld.

In de eerste klasse vallen de volgende producten:

1. software en hardware voor identiteitsbeheersystemen en voor het beheer van geprivilegieerde toegang, met inbegrip van lezers voor authenticatie en toegangscontrole, waaronder biometrische lezers
2. op zichzelf staande en ingebedde browsers
3. wachtwoordbeheer
4. software die kwaadaardige software opzoekt, verwijdert of in quarantaine plaatst
5. producten met digitale elementen met de functie van virtueel particulier netwerk (VPN)
6. netwerkbeheersystemen
7. Security information and event management-systemen (SIEM) (beveiligingsinformatie en evenementenbeheer)
8. Bootmanagement

9. publiekesleutelinfrastructuur en software voor de afgifte van digitale certificaten
10. fysieke en virtuele netwerkinterfaces
11. besturingssystemen
12. routers, modems bestemd voor verbinding met het internet, en netwerkswitches
13. microprocessoren met beveiligingsgerelateerde functies
14. microcontrollers met beveiligingsgerelateerde functies
15. toepassingsspecifieke geïntegreerde schakelingen (ASIC) en veld-programmeerbare gatearrays (FPGA) met beveiligingsgerelateerde functies
16. virtuele assistenten voor slimme huizen voor algemene doeleinden
17. producten voor slimme huizen met beveiligingsfuncties, met inbegrip van slimme deursloten, beveiligingscamera's, babymonitoringsystemen en alarmsystemen
18. met het internet verbonden speelgoed dat onder de Speelgoedrichtlijn valt en sociale interactieve functies (bv. spreken of filmen) of locatietraceringsfuncties heeft
19. persoonlijke wearables die op een menselijk lichaam moeten worden gedragen of geplaatst en bedoeld zijn voor gezondheidsmonitoring (zoals tracking) (en geen medische hulpmiddelen voor in-vitrodiagnostiek zijn), of persoonlijke wearables die bestemd zijn voor gebruik door en voor kinderen

Zelfbeoordeling van deze producten mag alleen op basis van geharmoniseerde normen. Wanneer er geen geharmoniseerde Europese norm is, moet het product met digitale elementen beoordeeld worden door een **conformiteitsbeoordelingsinstantie**.

3.2.3 *Belangrijke producten klasse 2*

In de tweede klasse van bijlage 3 bij de CRA worden als belangrijke producten aangemerkt:

1. hypervisors en container runtime systems die de gevirtualiseerde uitvoering van besturingssystemen en soortgelijke omgevingen ondersteunen
2. firewalls, inbraakdetectiesystemen en inbraakpreventiesystemen (intrusion detection and prevention systems)
3. manipulatiebestendige microprocessoren
4. manipulatiebestendige microcontrollers

Deze producten met digitale elementen moeten altijd door een conformiteitsbeoordelingsinstantie beoordeeld worden voordat zij op de markt mogen worden aangeboden.

3.2.4 *Kritieke producten*

Bijlage 4 bij de CRA benoemt de kritieke producten met digitale elementen. Dit zijn:

1. hardwareapparaten met beveiligingskastje
2. gateways voor slimme meters binnen slimme-metersystemen en andere apparaten voor geavanceerde beveiligingsdoeleinden, onder meer voor beveiligde cryptoverwerking
3. smartcards of soortgelijke apparaten, met inbegrip van secure elements (beveiligde elementen)

Voor deze apparaten kan in de toekomst worden voorgeschreven dat zij worden gecertificeerd volgens een geschikt certificatieschema onder de Cyber Security Act. Zo lang dit niet is voorgeschreven moet een kritiek product met digitale elementen verplicht langs een conformiteitsbeoordelingsinstantie.

Deze brochure is een uitgave van:

Ministerie van Economische Zaken
Bezuidenhoutseweg 73 | 2594 AC Den Haag
Postbus 20401 | 2500 EK Den Haag

September 2025 | Publicatie-nr. 0925-108