CRA EVIDENCE WHITEPAPER

De EU-verordening cyberweerbaarheid: praktische conformiteitsgids

Whitepaper voor fabrikanten, importeurs en distributeurs van producten met digitale elementen.

Versie	1.0
Status	In ontwikkeling
Grondslag	Verordening (EU) 2024/2847

Wijzigingshistorie

Dit is een levend document. Het wordt bijgewerkt naarmate de Europese richtsnoeren, geharmoniseerde normen en marktpraktijk onder de CRA zich ontwikkelen.

Versie	Datum	Beschrijving
1.0	17 mei 2026	Eerste uitgave. Behandelt toepassingsgebied, classificatie, ingrijpende wijziging, essentiële vereisten, kwetsbaarheidsafhandeling, technische documentatie, conformiteitsbeoordelingsroutes en interactie met AI Act, Data Act, ESPR en productaansprakelijkheid.

Inhoud

Samenvatting

IN 60 SECONDEN

Waar het over gaat: verbonden hardware- en softwareproducten die op de EU-markt worden aangeboden, waarbij beveiliging een productconformiteitsvereiste is en geen aanbevolen praktijk.

Wanneer het gaat gelden: meldingen volgens artikel 14 vanaf 11 september 2026; volledige technische, documentatie- en CE-markeringsverplichtingen vanaf 11 december 2027.

Wat u moet opleveren: beoordeling van cyberbeveiligingsrisico's, SBOM, technische documentatie, gebruikersinstructies, EU-conformiteitsverklaring, CE-markering en meldingen van incidenten en kwetsbaarheden volgens artikel 14.

Wie moet handelen

Fabrikanten dragen de hoofdlast. Importeurs en distributeurs hebben zorgvuldigheidscontroles voordat zij producten beschikbaar stellen.

Wat verandert

Cyberbeveiliging wordt onderdeel van productconformiteit: veilig ontwerp, kwetsbaarheidsafhandeling, documentatie, CE-markering en acties na marktintroductie.

Eerste deadline

Melding volgens artikel 14 start op **11 september 2026** voor actief uitgebuite kwetsbaarheden en ernstige incidenten.

Volledige toepassing

Volledige technische conformiteit geldt vanaf **11 december 2027**. Eerdere producten vallen eronder na een ingrijpende wijziging, maar de meldplicht blijft gelden.

Bewijsruggengraat

De technische documentatie bevat risicobeoordeling, SBOM, onderbouwing van de ondersteuningsperiode, testbewijs, gebruikersinstructies, verklaring en bewijs van conformiteit met de essentiële cyberbeveiligingsvereisten.

Conformiteitsroute

De meeste producten kunnen module A gebruiken. Belangrijke en kritieke producten kunnen een aangemelde instantie of EU-cyberbeveiligingscertificeringnodig hebben.

Wat is de Verordening cyberweerbaarheid?

De Cyber Resilience Act (CRA), in Nederland de Verordening cyberweerbaarheid en formeel Verordening (EU) 2024/2847, is het eerste EU-brede kader dat cyberbeveiliging verplicht stelt voor producten met digitale elementen die op de EU-markt worden aangeboden. De gezaghebbende tekst staat op EUR-Lex.

De CRA geldt voor fabrikanten, importeurs en distributeurs van verbonden hardware en software. De verordening dekt producten van consumenten-IoT tot industriële besturingssystemen. De praktische verandering is duidelijk: cyberbeveiliging moet worden ontworpen, onderbouwd, onderhouden en bewaakt als onderdeel van productconformiteit.

Niet-naleving van de essentiële cyberbeveiligingsvereisten of de verplichtingen van artikel 13 en 14 kan leiden tot boetes tot 15 miljoen euro of 2,5% van de wereldwijde jaaromzet, naargelang welke hoger is. Er gelden lagere niveaus: tot 10 miljoen euro of 2% voor schending van andere genoemde verplichtingen, en tot 5 miljoen euro of 1% voor het verstrekken van onjuiste, onvolledige of misleidende informatie aan aangemelde instanties of markttoezichtautoriteiten. Markttoezichtautoriteiten kunnen ook corrigerende maatregelen eisen, beschikbaarheid beperken, producten uit de handel nemen of terugroepacties verlangen.

Belangrijke datums voor conformiteitsplanning

De CRA is op **10 december 2024** in werking getreden. Het praktische conformiteitswerk draait om drie mijlpalen: aangemelde instanties in **juni 2026**, meldingen in **september 2026** en volledige technische conformiteit in **december 2027**.

OPMERKING

Status van de richtsnoeren van de Commissie: De Europese Commissie publiceerde op 3 maart 2026 ontwerprichtsnoeren voor de CRA. De consultatie sloot op 13 april 2026. De richtsnoeren zijn niet definitief, maar ze zijn bruikbaar als planningsmateriaal voor marktintroductie, vrije en open-source software, ondersteuningsperioden, ingrijpende wijziging, productclassificatie, due diligence op componenten, gegevensverwerking op afstand, kwetsbaarheidsbeheer en samenloop met andere EU-wetgeving. Grensvragen rond de AI Act en DORA kunnen nog verdere richtsnoeren nodig hebben.

10 december 2024

Inwerkingtreding

Overgangsperiode begint

11 juni 2026

Aangemelde instanties

Hoofdstuk IV geldt

11 september 2026

Meldingen

Artikel 14 gaat gelden

11 december 2027

Volledige toepassing

Technische vereisten, CE-markering, documentatie en conformiteitsbeoordeling

BEGIN HIERMEE

Begin met meldingsgereedheid. De deadline van artikel 14 komt eerder dan volledige technische conformiteit en geldt ook voor producten die al op de EU-markt zijn.

Omdat de meldplicht op **11 september 2026** begint, moet meldingsgereedheid de eerste implementatiestroom zijn: **detectie, triage, gebruikerscommunicatie en meldprocessen voor autoriteiten** moeten werken voordat volledige technische conformiteit vereist is.

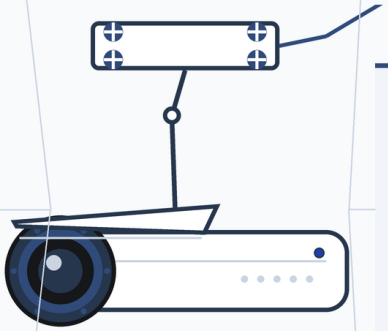
Producten die voor **11 december 2027** op de markt zijn aangeboden, vallen alleen onder de technische vereisten van de CRA als zij vanaf die datum een **ingrijpende wijziging** ondergaan. De meldplicht werkt anders: artikel 14 geldt voor **alle producten binnen het toepassingsgebied**, ook voor producten die al op de EU-markt zijn.

De CRA over de productlevenscyclus

STAP 01
Productscope bepalen
Scope, classificatie, supportperiode en risicoanalyse

STAP 02
Veilig ontwikkelen
Veilige defaults, codeanalyse, SBOM en dependencybeheer

STAP 03
Valideren en documenteren
Securitytests, vulntriage, technisch dossier en gebruikersinfo



STAP 04
Op de markt brengen
EU-DoC, CE-markering en releasebesluit

STAP 05
Monitoren en bijwerken
CVE’s, adviezen, exploitactiviteit, beveiligingsupdates en openbaarmaking

STAP 06
Support en samenwerking
Artikel 14, gebruikersinfo, autoriteitsvragen en supporteinde

Verbonden IP-camera, van productplanning tot ondersteuning na marktintroductie onder de CRA

Welke producten vallen onder het toepassingsgebied

Toepassingsgebied en uitsluitingen

De CRA geldt voor hardware- en softwareproducten waarvan het beoogde of redelijkerwijs voorzienbare gebruik een directe of indirecte gegevensverbinding met een apparaat of netwerk omvat. Dat omvat computers, smartphones, netwerkapparatuur, IoT-apparaten, industriële besturingssystemen en toepassingen voor gegevensverwerking.

Deze categorieën zijn uitdrukkelijk uitgesloten:

- Medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek die onder Verordeningen (EU) 2017/745 en 2017/746 vallen
- Voertuigsystemen die onder Verordening (EU) 2019/2144 vallen
- Luchtvaartuitrusting die onder Verordening (EU) 2018/1139 valt
- Scheepsuitrusting die onder Richtlijn 2014/90/EU valt
- Producten die uitsluitend voor nationale veiligheid of defensie zijn ontwikkeld
- Zuiver mechanische producten zonder digitale elementen of netwerkverbinding

Als geen duidelijke uitsluiting geldt, behandel uw verbonden product dan als product binnen het toepassingsgebied.

OPMERKING

Maatwerkproducten: een smalle uitzondering. Bouwt u een product dat op maat is gemaakt voor één specifieke zakelijke gebruiker, onder een schriftelijke overeenkomst tussen u en die gebruiker, dan kunt u afwijken van twee vereisten: de standaard beveiligde configuratie (u moet wel een pad terug naar de oorspronkelijke veilige toestand aanbieden) en de kosteloze beveiligingsupdates (de overeenkomst kan een andere commerciële basis vastleggen). Al het overige geldt onverkort: kwetsbaarheidsafhandeling, de overige cyberbeveiligingsvereisten, melding volgens artikel 14, technische documentatie, CE-markering, conformiteitsbeoordeling en de ondersteuningsperiode. Dit is geen algemene B2B-uitzondering en dekt geen kant-en-klare producten die aan bedrijven worden verkocht.

Productclassificatie bepaalt de beoordelingsroute

Uw productcategorie bepaalt hoe u conformiteit aantoont.

Categorie	Voorbeelden	Conformiteitsbeoordeling
Standaard "niet-geclassificeerd"	Algemene software en verbonden consumentenproducten die niet in de belangrijke of kritieke categorieën vallen	module A: zelfbeoordeling

Categorie	Voorbeelden	Conformiteitsbeoordeling
Belangrijk "klasse I"	Identiteit, browser, wachtwoordmanager, antivirus, VPN, netwerkbeheer, router, slim deurslot, beveiligingscamera en vergelijkbare producten	module A alleen waar toepasselijke geharmoniseerde normen, gemeenschappelijke specificaties of certificeringsschema's worden toegepast zoals vereist; anders module B+C of module H
Belangrijk "klasse II"	Hypervisors, containerruntimes, firewalls, IDS/IPS en manipulatiebestendige microprocessors	module B+C, module H of een toepasselijk Europees cyberbeveiligingscertificeringsschema met ten minste betrouwbaarheidsniveau "substantieel"
Kritieke producten	Beveiligde elementen, smartcards, slimme-meter-gateways en hardware security boxes	Europese cyberbeveiligingscertificering waar vereist en beschikbaar; anders gelden de routes voor klasse II

De vier productcategorieën

De tabel hierboven toont voorbeelden. De volledige referentie waaraan u de kernfunctionaliteit van uw product toetst, staat hieronder.

Standaardproducten

De meeste producten komen hier uit. Elk product met digitale elementen waarvan de kernfunctionaliteit niet overeenkomt met een vermelding in de lijsten van belangrijke of kritieke producten hieronder, wordt behandeld als standaard. De conformiteitsroute is module A: zelfbeoordeling.

Veelvoorkomende voorbeelden:

- Smart-tv's en streamingapparaten.
- Netwerkprinters en multifunctionele kantoorapparaten.
- Bluetooth-luidsprekers en consumentengeluidsproducten.
- Mediaspeler-softwaretoepassingen.
- Spelcomputers, e-readers en vergelijkbare consumentenelektronica.
- Slimme keukenapparatuur zoals ovens, koelkasten en vaatwassers zonder beveiligingsfuncties.
- Slimme lampen en verbonden verlichting zonder beveiligingsfuncties.
- Activiteitsmeters zonder gezondheidsbewakingsdoel.
- Mobiele toepassingen voor algemeen gebruik die geen browser, wachtwoordmanager of VPN-app zijn.
- Kantoorsoftware zoals tekstverwerkers en spreadsheets.

De lijst hierboven is illustratief. De lijsten voor belangrijke en kritieke producten hieronder zijn uitputtend.

Belangrijke producten (klasse I)

Verplichte beoordeling door een derde partij, tenzij toepasselijke geharmoniseerde normen, gemeenschappelijke specificaties of certificeringsschema's worden toegepast zoals vereist.

1. Software en hardware voor identiteitsbeheer en beheer van bevoorrechte toegang, inclusief lezers voor authenticatie en toegangsbeheer (waaronder biometrische lezers).
2. Op zichzelf staande en ingebedde browsers.
3. Wachtwoordmanagers.
4. Software die zoekt naar, verwijdert of in quarantaine plaatst van schadelijke software.
5. VPN-producten.
6. Netwerkbeheersystemen.
7. Systemen voor beveiligingsinformatie- en gebeurtenisbeheer (SIEM).
8. Bootmanagers.
9. Software voor public key infrastructure en uitgifte van digitale certificaten.
10. Fysieke en virtuele netwerkinterfaces.
11. Besturingssystemen.
12. Routers, modems voor internetverbinding en switches.
13. Microprocessors met beveiligingsfuncties.

14. Microcontrollers met beveiligingsfuncties.
15. ASIC's en FPGA's met beveiligingsfuncties.
16. Virtuele assistenten voor algemeen gebruik in het slimme huis.
17. Slimme-huisproducten met beveiligingsfuncties (slimme deursloten, beveiligingscamera's, babyfoons, alarmsystemen).
18. Met internet verbonden speelgoed met interactieve functies (spreken, filmen, locatiebepaling).
19. Persoonlijke draagbare apparaten met gezondheidsbewakingsdoeleinden (waar Verordeningen (EU) 2017/745 of 2017/746 niet van toepassing zijn), of draagbare apparaten bedoeld voor gebruik door kinderen.

Belangrijke producten (klasse II)

Verplichte beoordeling door een derde partij, strengere route. Zelfbeoordeling is niet beschikbaar, ook niet wanneer geharmoniseerde normen bestaan.

1. Hypervisors en containerruntimesystemen die gevirtualiseerde uitvoering van besturingssystemen en vergelijkbare omgevingen ondersteunen.
2. Firewalls, inbraakdetectie- en inbraakpreventiesystemen.
3. Manipulatiebestendige microprocessors.
4. Manipulatiebestendige microcontrollers.

Kritieke producten

Europese cyberbeveiligingscertificering vereist waar het schema beschikbaar is. Anders geldt de route voor klasse II.

1. Hardwareapparaten met security boxes.
2. Gateways voor slimme meters binnen slimme-metersystemen zoals gedefinieerd in artikel 2, punt 23, van Richtlijn (EU) 2019/944, en andere apparaten voor geavanceerde beveiligingsdoeleinden, onder meer voor beveiligde cryptoverwerking.
3. Smartcards en vergelijkbare apparaten, waaronder beveiligde elementen.

Komt de kernfunctionaliteit van uw product overeen met een vermelding op de lijst voor belangrijke of kritieke producten, dan valt het in die klasse. Integreert uw product een van die vermeldingen als component maar is zijn eigen kernfunctionaliteit iets anders, dan verandert die integratie uw klasse niet (artikel 7, lid 1).

Hoe te classificeren: kernfunctionaliteit, niet integratie

De lijsten hierboven vertellen u wat de categorieën zijn. Zij vertellen u niet hoe u ze toepast op uw product. Het antwoord van de CRA is één term: **kernfunctionaliteit**.

Uw klasse wordt bepaald door wat de kernfunctionaliteit van uw product is, niet door welke componenten het integreert. Komt de kernfunctionaliteit overeen met de lijsten voor belangrijke producten, dan is het product belangrijk (klasse I of klasse II). Komt zij overeen met de lijst voor kritieke producten, dan is het product kritiek. Geen van beide, dan is het standaard. Dat is de hele toets.

De praktische waarborg zit in de tweede zin van artikel 7, lid 1. Het integreren van een belangrijke component duwt het integrerende product niet in de belangrijke klasse. Een firewallbibliotheek inbedden in een slimme-huishub maakt de hub geen firewall. Overweging 45 zegt het in heldere bewoordingen: firewalls en inbraakdetectiesystemen zijn belangrijk klasse II, maar andere producten die ze toevallig integreren zijn dat niet.

Gebruik deze volgorde om uzelf te classificeren.

1. **Benoem de kernfunctionaliteit van uw product in één zin.** Lukt dat niet, dan faalt de rest van de analyse. Richt u op datgene zonder welke het product niet zou functioneren.
2. **Controleer de lijsten voor belangrijke producten hierboven.** Een match in klasse I of II maakt het product belangrijk.
3. **Controleer de lijst voor kritieke producten hierboven.** Een match maakt het product kritiek. Een Europese cyberbeveiligingscertificeringsroute geldt waar het schema beschikbaar is; anders geldt de route voor klasse II.
4. **Geen match op een van beide lijsten.** Het product is standaard. Module A: zelfbeoordeling is de route.
5. **Documenteer de redenering.** Een memo van één pagina met de verklaring over de kernfunctionaliteit, de lijstcontrole en de gekozen route hoort in de technische documentatie.

Twee uitgewerkte voorbeelden.

Slimme-huishub met ingebouwde wachtwoordmanager. Kernfunctionaliteit: orkestratie van routines tussen consumenten-IoT-apparaten in een woning. De wachtwoordmanagercomponent, los verkocht door zijn eigen fabrikant, is op zichzelf een belangrijk klasse I-product. De kernfunctionaliteit van de hub is woningautomatisering, geen referentiebeheer. De hub blijft standaard.

Besturingssysteem op basis van functieset. Een product wordt op de markt gebracht als slimme-huisapparaat, maar de hoofdfuncties zijn initialisatie van hardware en randapparaten, procesplanning, geheugenbeheer en een systeemaanroep-interface. Dat is de kernfunctionaliteit van een besturingssysteem. Besturingssystemen zijn een belangrijk klasse I-product. Het product is belangrijk klasse I, ongeacht de marketing.

Verrast uw classificatie de rest van het team, dan heeft de verklaring over de kernfunctionaliteit nog een ronde nodig voordat u verzendt.

Wanneer de cloud deel uitmaakt van uw product

De meeste producten met digitale elementen leunen op iets buiten het apparaat: een cloudbackend, een mobiele begeleidende app, een server voor updates over de lucht, een authenticatieportaal, een apparaatbeheersysteem. De CRA behandelt die niet allemaal als uw product. Zij behandelt ze als onderdeel van het product alleen wanneer **beide** onderstaande voorwaarden waar zijn (artikel 3, lid 2):

- De software is **ontworpen en ontwikkeld door uw team, of onder uw verantwoordelijkheid**.
- Het product **zou een van zijn functies niet kunnen uitvoeren** zonder die software.

Faalt een van beide voorwaarden, dan ligt de afstandsservice buiten de productgrens voor de CRA. Een SaaS van een derde die u niet bezit, ook al communiceert uw product ermee, is geen onderdeel van uw product. Een website die het product promoot maar geen functie ervan ondersteunt, is dat evenmin.

Wanneer een externe component binnen het toepassingsgebied valt, valt zij dat **als onderdeel van het product**. De technische documentatie, conformiteitsbeoordeling, EU-conformiteitsverklaring, kwetsbaarheidsafhandeling en meldtermijnen van artikel 14 dekken de cloudcomponent samen met het apparaat.

Gebruik deze matrix om de zaak snel te beslechten.

Component	Onderdeel van het product?
Mobiele begeleidende app die met het apparaat koppelt	**Ja.** U heeft hem ontworpen en het apparaat kan niet worden ingericht of gebruikt zonder hem.
Cloudbackend die de gegevens van het apparaat opslaat en verwerkt	**Ja.** U heeft hem ontworpen en het dashboard of de hoofdfunctie werkt niet zonder hem.
Server voor updates over de lucht	**Ja.** U heeft hem ontworpen en het apparaat kan geen beveiligingsupdates ontvangen zonder hem.
Authenticatieportaal dat toegang tot het apparaat regelt	**Ja.** U heeft het ontworpen en gebruikers kunnen er niet zonder inloggen.
Marketingwebsite voor het product	**Nee.** Ondersteunt geen productfunctie.
SaaS van een derde waarmee het product integreert (niet uw eigendom)	**Nee.** Niet door u ontworpen. De derde partij draagt eigen verplichtingen onder NIS 2.
Generieke cloudinfrastructuur waarop uw dienst draait (IaaS of PaaS)	**Nee.** Niet door u ontworpen. De infrastructuuraanbieder valt onder NIS 2.

Een veelvoorkomend patroon: een slimme-huisapparaat met een mobiele app, een updateserver en een cloudbackend. Alle drie zijn ontworpen door de fabrikant en het apparaat kan zijn aangeprezen functies niet uitvoeren zonder ze. Alle drie zijn onderdeel van het product. De CRA-verplichtingen gelden voor het hele geheel. Praat de cloudbackend vervolgens met een analytische SaaS van een derde, dan is die SaaS geen onderdeel van het product. De derde partij draagt eigen verplichtingen onder NIS 2.

De CRA eist geen beveiligingsmaatregelen voor het netwerk en de informatiesystemen van de fabrikant als geheel. Zij eist beveiliging voor de afstandsservices die onderdeel zijn van het product. De grens ligt bij het product, niet bij het bedrijf.

Uw toeleveringsketen: wie doet wat onder de CRA

De CRA legt de hoofdverplichtingen bij u als fabrikant, maar importeurs en distributeurs hebben ook taken die bepalen hoe uw product de markt bereikt. Drie dingen zijn van belang voor u om te weten.

Wie	Wat zij vóór levering controleren	Wat zij doen bij een kwetsbaarheid	Wanneer zij uw plichten overnemen
Importeur	CE-markering, de EU-conformiteitsverklaring, gebruikersinstructies in de juiste taal, uw contactgegevens op of bij het product	Informeert u zonder onnodige vertraging; informeert markttoezichtautoriteiten rechtstreeks als het product een significant cyberbeveiligingsrisico oplevert	Wanneer zij uw product onder hun eigen naam of handelsmerk in de handel brengen, of het ingrijpend wijzigen
Distributeur	CE-markering, dat u en de importeur uw deel hebben gedaan, dat de vereiste documenten het product vergezellen	Informeert u zonder onnodige vertraging; informeert markttoezichtautoriteiten rechtstreeks als het product een significant cyberbeveiligingsrisico oplevert; kan stoppen met het beschikbaar stellen van het product	Zelfde aanleiding als voor importeurs

Voor een fabrikant betekent dit drie praktische dingen:

- Uw CE-markering, uw EU-conformiteitsverklaring en uw gebruikersinstructies moeten correct zijn en in de juiste taal op het moment dat een distributeur ze controleert. Kanaalpartners zijn verplicht deze te verifiëren en kunnen weigeren het product beschikbaar te stellen als ze ontbreken of niet kloppen.
- U heeft een heldere, laagdrempelige contactroute nodig die importeurs en distributeurs kunnen gebruiken om kwetsbaarheden te melden in uw kwetsbaarheidsafhandelingsproces. Zij zullen die gebruiken.
- Een partner die uw product opnieuw labelt, onder eigen naam of handelsmerk in de handel brengt of ingrijpend wijzigt, wordt de fabrikant voor die variant. De volledige plichten rond technische documentatie, conformiteitsbeoordeling, melding en ondersteuningsperiode gaan voor die versie over op die partij. Zie *Wanneer iemand anders de fabrikant wordt* in het volgende hoofdstuk voor de regel rond ingrijpende wijziging.

Ingrijpende wijziging: wanneer hernieuwde conformiteit geldt

Nadat uw product op de markt is, splitst de CRA latere wijzigingen in twee kampen. De meeste zijn routine en vragen niets extra. Sommige zijn ingrijpend. Een ingrijpende wijziging wordt voor CRA-doeleinden behandeld als een nieuw product dat op de markt wordt aangeboden. Dat betekent een nieuwe conformiteitsbeoordeling, een vernieuwde technische documentatie, een nieuwe conformiteitsverklaring en CE-markering op de nieuwe versie.

De toets is kort en zit in de definitie van ingrijpende wijziging (artikel 3, lid 30). Een wijziging is ingrijpend als één van deze uitspraken klopt:

- Zij heeft **gevolgen voor de conformiteit** met de essentiële cyberbeveiligingsvereisten.
- Zij **wijzigt het beoogde doel** waarvoor het product is beoordeeld.

Geldt geen van beide, dan is de wijziging niet ingrijpend. Documenteer de redenering toch en bewaar haar in het dossier. De analyse hoort bij het bewijsspoor.

Wat niet als ingrijpend telt

Twee uitzonderingen doen het meeste werk in de praktijk.

Beveiligingsupdates en bugfixes die het cyberbeveiligingsrisico verlagen zonder het beoogde doel te wijzigen, zijn niet ingrijpend. Een bekende kwetsbaarheid patchen, invoervalidatie aanpassen om een fout te dichten of een component herbouwen om een CVE aan te pakken, vallen alle aan deze kant van de streep.

Refurbishment, onderhoud en reparaties zijn ook niet automatisch ingrijpend. Zij worden alleen ingrijpend als zij het beoogde doel veranderen of de conformiteit met de essentiële cyberbeveiligingsvereisten raken.

Klein werk aan de gebruikersinterface blijft eveneens aan de veilige kant. Een taal toevoegen, een pictogrammenset wisselen of een schermindeling polijsten is op zichzelf geen ingrijpende wijziging. Een nieuw invoerelement toevoegen dat passende invoervalidatie vereist, kan dat wel zijn.

Reserveonderdelen

De CRA stelt reserveonderdelen op een smalle, specifieke manier vrij. **Identieke reserveonderdelen**, gemaakt volgens dezelfde specificaties als de componenten die zij vervangen, vallen volledig buiten het toepassingsgebied van de verordening. Functionele vervangingen niet.

Gebruik deze matrix om de zaak snel te beslechten.

Vervanging	Hostproduct op de markt vóór 11 december 2027	Hostproduct op de markt op of na 11 december 2027
Identiek aan de oorspronkelijke component, dezelfde specificaties	Reserveonderdeel buiten CRA-toepassingsgebied. Geen verplichtingen door de vervanging.	Reserveonderdeel buiten CRA-toepassingsgebied. Geen verplichtingen door de vervanging.
Functioneel gelijkwaardig, ander ontwerp of andere specificatie	De vervanging is zelf een CRA-product. Het hostproduct heeft geen CRA-verplichtingen, omdat het de toepassingsdatum voorgaat.	De vervanging is een CRA-product. Beoordeel of de vervanging in het hostproduct een ingrijpende wijziging is met de tweetraps-toets hierboven.

Twee praktische gevolgen. Ten eerste hangt de vrijstelling af van identieke specificatie. Een draadloze module die op een andere chipset is herbouwd, is geen identiek reserveonderdeel, ook al merkt de klant het verschil niet. Ten tweede draagt de fabrikant die een functionele vervanging levert de CRA-verplichtingen voor dat onderdeel, ongeacht wie het hostproduct heeft gemaakt.

Software-updates en feature flags

Softwarereleases zijn de meest voorkomende bron van vragen over ingrijpende wijziging. De tweetraps-toets beslecht ze nog steeds.

Een patch die een kwetsbaarheid verhelpt, is niet ingrijpend. Een feature toggle die een capaciteit aanzet waarvoor het product nooit is beoordeeld, is dat wel. Een modelupgrade die het product laat beslissen over nieuwe categorieën input ook. Bevat een release zowel een fix als een nieuwe functie, beoordeel dan de functie.

Bundeling telt minder dan inhoud. Of een functie-update apart aankomt of in dezelfde release als een beveiligingspatch, doet er voor de beoordeling niet toe.

Werkt u met feature flags of gefaseerde uitrol, dan telt het moment van activering voor eindgebruikers in productie, niet de oplevering van de binary die de vlag bevat.

De beslissing in de praktijk

Gebruik deze volgorde bij elke wijziging voordat zij wordt opgeleverd.

1. **Wijzigt de verandering het beoogde doel van het product?** Zo ja: ingrijpend. Voer de conformiteitsbeoordeling opnieuw uit voor de nieuwe versie.
2. **Heeft de verandering gevolgen voor de conformiteit met de essentiële cyberbeveiligingsvereisten?** Zo ja: ingrijpend. Voer de conformiteitsbeoordeling opnieuw uit voor de nieuwe versie.
3. **Anders:** niet ingrijpend. Documenteer de analyse en ga door onder de bestaande technische documentatie.

Zit het product in de belangrijke of kritieke klasse en vroeg de route de eerste keer om een beoordeling door een derde partij, dan brengt een ingrijpende wijziging u terug op dezelfde route. Informeer de derde partij vooraf over elke wijziging die waarschijnlijk ingrijpend is. Zelfbeoordeling is geen achterdeur om een belangrijk product achteraf opnieuw te classificeren.

Gevolgen wanneer een wijziging ingrijpend is

Een ingrijpende wijziging wordt behandeld als een nieuw product dat op de markt wordt aangeboden. Voor de fabrikant betekent dat:

- Werk de technische documentatie voor de gewijzigde versie bij.
- Voer de conformiteitsbeoordeling opnieuw uit langs de route die de productklasse voorschrijft.
- Geef een nieuwe EU-conformiteitsverklaring uit voor de gewijzigde versie.
- Breng de CE-markering opnieuw aan, met de nieuwe verklaring in het dossier.
- Bewaar de documentatie van de vorige versie voor de volledige bewaartermijn. De nieuwe versie wist haar niet.

Voor softwareproducten in het bijzonder kunt u beveiligingsupdates tijdens de ondersteuningsperiode beperken tot de laatste versie die u op de markt heeft gebracht, mits gebruikers van eerdere versies kosteloos en zonder nieuwe hardware naar de laatste versie kunnen overstappen.

Veldeenheden die al onder de eerdere conformiteit zijn verkocht, blijven ongewijzigd. De verplichting hangt aan de gewijzigde versie die beschikbaar wordt gesteld, niet aan identieke eenheden die haar voorgaan.

Wanneer iemand anders de fabrikant wordt

Bent u niet de oorspronkelijke fabrikant en voert u een ingrijpende wijziging door, dan behandelt de CRA u als de fabrikant voor die versie. De volledige verplichtingen van de artikelen 13 en 14 komen op u te rusten. Dezelfde regel geldt wanneer u het product onder uw eigen naam of handelsmerk op de markt aanbiedt (artikel 21).

Dit vangt meer situaties op dan teams gewoonlijk verwachten:

- Een systeemintegrator die een firmwarebouw op maat voor een klant levert, met nieuwe functies.
- Een wederverkoper die een product whitelabelt en het beoogde doel in zijn marketing wijzigt.
- Een dienstverlener die een apparaat van een derde bundelt met eigen firmware.

In elk geval erft de actor die de wijziging heeft gemaakt de fabrikantverplichtingen voor die versie: technische documentatie, conformiteitsbeoordeling, melding, kwetsbaarheidsafhandeling en de rest. Het etiket "importeur" of "distributeur" beschermt hen niet meer op het moment dat zij een van beide grenzen overschrijden.

Wat u op orde moet hebben

Gebruik dit onderdeel als werkchecklist. De nadere uitleg per vereiste volgt daarna.

Beoordeling van cyberbeveiligingsrisico's

Voordat u een product op de markt aanbiedt, heeft u een beoordeling van cyberbeveiligingsrisico's in het dossier nodig. Het is het document dat in uw eigen woorden uitlegt waarom het product veilig is om uit te leveren en op de markt te houden.

De beoordeling moet dekken:

- Het beoogde doel van het product en de gebruikssituaties die u redelijkerwijs kunt voorzien
- De omstandigheden en omgeving waarin het product zal werken
- De gegevens en functies die bescherming nodig hebben
- De dreigingen die van toepassing zijn en de controles waarop u vertrouwt om ze te beheersen
- De verwachte gebruiksduur van het product

Hoe de meeste teams haar opbouwen. Geloofwaardige methodologieën komen samen op dezelfde stappen: identificeer de te beschermen onderdelen (gegevens die het product verwerkt, beveiligingsmateriaal zoals sleutels en referenties, functies waarvan het verlies gebruikers zou schaden), breng in kaart waar elk onderdeel staat of beweegt, modelleer dreigingen per onderdeel en omgeving met vertrouwelijkheid, integriteit en beschikbaarheid als dimensies, scoor impact en waarschijnlijkheid, besluit welke restrisico's worden geaccepteerd en welke worden beperkt, en herbeoordeel na elke ronde controles (elke nieuwe sleutel, elk certificaat en elke authenticatiefunctie is zelf een nieuw te analyseren onderdeel).

Threat modelling. Stap drie hierboven is de meest technische en kent eigen gevestigde technieken. STRIDE categoriseert dreigingen als spoofing, tampering, repudiation, information disclosure, denial of service en elevation of privilege; breed gebruikt, past op de meeste verbonden producten. LINDDUN breidt het beeld uit voor producten die persoonsgegevens verwerken, en voegt linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness en non-compliance toe; nuttig waar het gegevensbeschermingsregime overlapt met CRA-plichten. PASTA doorloopt een proces van zeven fasen, van bedrijfsdoelstellingen tot acceptatie van restrisico; nuttig voor complexe systemen waarin het aanvalsbeeld het ontwerp stuurt. Geen van deze is CRA-specifiek en de CRA verplicht er geen. Kies de techniek die past bij het blootstellingsprofiel van uw product.

Waar u een uitgewerkte methodologie vindt. De CRA schrijft geen methode voor. De Duitse federale dienst voor informatiebeveiliging (BSI) publiceert Technische Richtlijn TR-03183, de meest gedetailleerde CRA-conforme risicobeoordelingsmethodologie die publiek beschikbaar is. ENISA publiceert bredere richtsnoeren voor CRA-implementatie.

Houd de beoordeling actueel gedurende de ondersteuningsperiode. Wijzigt het dreigingsbeeld, wijzigen de componenten of wijzigt het gebruik, dan wijzigt de beoordeling mee.

Bepaling van de ondersteuningsperiode

Elk product heeft een gedefinieerde ondersteuningsperiode nodig en u moet de einddatum publiceren op het moment van aankoop. De ondersteuningsperiode is het venster waarin u kwetsbaarheden afhandelt, beveiligingsupdates uitlevert en de technische documentatie actueel houdt.

Hoe lang die moet zijn

Ten minste vijf jaar. Wordt het product naar verwachting korter dan vijf jaar gebruikt, dan moet de ondersteuningsperiode aansluiten op die kortere gebruiksduur. Wordt het langer gebruikt, dan moet de ondersteuningsperiode dat langere gebruik weerspiegelen; producten zoals routers, besturingssystemen en industriële controllers rechtvaardigen routinematig meer dan vijf jaar.

Factoren om mee te wegen

Houd bij het bepalen van de periode op evenredige wijze rekening met:

- Redelijke gebruikersverwachtingen voor het product
- De aard van het product, waaronder het beoogde doel
- EU-wetgeving die al een levensduur voor deze productcategorie vastlegt
- Ondersteuningsperioden van vergelijkbare producten op de markt
- De beschikbaarheid van de operationele omgeving waarvan het product afhankelijk is
- De ondersteuningsperioden van geïntegreerde componenten die kernfuncties leveren
- Richtsnoeren van de ADCO-samenwerkingsgroep of de Commissie voor de productcategorie

De redenering achter de gekozen periode hoort in de technische documentatie. Markttoezichtautoriteiten kunnen erom vragen.

Wat u moet publiceren

Vermeld het einde van de ondersteuningsperiode op het moment van aankoop, met ten minste de maand en het jaar, op een goed toegankelijke plek. Heeft het product een gebruikersinterface, toon dan een melding wanneer het product het einde van zijn ondersteuningsperiode bereikt.

Bewaring van updates

Elke beveiligingsupdate die tijdens de ondersteuningsperiode aan gebruikers beschikbaar is gesteld, moet ten minste 10 jaar na uitgifte beschikbaar blijven, of voor de rest van de ondersteuningsperiode, naargelang welke periode langer is.

Due diligence op componenten

Een product bestaat uit componenten. Sommige heeft u zelf geschreven, sommige gekocht, sommige uit een opensource-repository gehaald. De CRA behandelt het product als geheel voor conformiteit, dus de componenten tellen mee. Zit een kwetsbaarheid in een component, dan zit zij in uw product. Krijgt een component geen beveiligingsupdates, dan krijgt uw product die ook niet.

Fabrikanten moeten due diligence uitoefenen op componenten van derden, ook op vrije en opensourcecomponenten. De componenten mogen de cyberbeveiliging van het product niet in gevaar brengen.

Hoeveel due diligence genoeg is, hangt af van het cyberbeveiligingsrisico dat de component draagt. Een bibliotheek die authenticatie afhandelt, is niet hetzelfde als een lettertypebibliotheek. Gebruik een of meer van deze controles, evenredig aan het risico:

1. **Controleer op CE-markering op de component.** Is de component zelf een CRA-product en heeft de leverancier conformiteit aangetoond, dan staat de CE-markering op de component. Dat toont het CRA-werk van de leverancier aan.
2. **Controleer de geschiedenis van beveiligingsupdates.** Een component die regelmatig beveiligingsupdates uitbrengt, is een beter risico dan een component die jaren stil is geweest. Kijk naar de releasecadans en het recente patroon van beveiligingsadviezen.
3. **Controleer de component tegen kwetsbaarheidsdatabases.** De Europese kwetsbaarheidsdatabase en publieke CVE-databases vertellen u wat bekend is over de component. Een bekende CVE zonder patch is een rode vlag.
4. **Voer aanvullende beveiligingstests uit.** Waar het bovenstaande niet voldoende is, test de component in uw integratiecontext: statische analyse, dynamische analyse, fuzzing of een gerichte beveiligingsbeoordeling.

Voor componenten die zijn geïntegreerd voordat hun eigen leverancier volledig onder de CRA valt (dus zolang geen CE-markering beschikbaar is), gebruikt u de overige drie controles. De due-diligenceplicht pauzeert niet omdat de toeleveringsketen nog inloopt.

Bewijs om in het dossier te bewaren

De technische documentatie moet uw due diligence laten zien, niet alleen claimen. Bewaar:

- Een lijst van componenten van derden in het product, herleidbaar tot versies, inclusief opensourcecomponenten. De SBOM is de natuurlijke plaats.
- De beveiligingsdocumentatie van de leverancier die u heeft beoordeeld: beveiligingsbeleid, programma's voor kwetsbaarheidsopenbaarmaking, toezeggingen over de ondersteuningsperiode.
- Integratietestrapporten die aantonen dat de component zich veilig gedraagt in uw product.
- Beveiligingsclausules in contracten of SLA's met commerciële leveranciers: meldtermijnen voor kwetsbaarheden, toezeggingen over de ondersteuningsperiode, escalatieregels.
- Een registratie van de mitigaties op productniveau die u heeft toegevoegd waar due diligence op componenten grenzen onthulde: sandboxing, beperkte rechten, invoervalidatie, netwerksegmentatie.

Wanneer u een kwetsbaarheid in een component vindt

Identificeren uw due diligence of monitoring na marktintroductie een kwetsbaarheid in een component, dan moet u twee dingen doen. Informeer eerst de persoon of entiteit die de component onderhoudt. Is de component opensource, dan is dat het upstream-project. Verhelp en mitigeer vervolgens de kwetsbaarheid in uw product binnen dezelfde termijnen als elke andere kwetsbaarheid die u ontdekt. Heeft u een fix gebouwd, deel dan de code of documentatie met de onderhouder, in een machineleesbaar formaat waar dat van toepassing is.

De CRA staat niet toe dat u wacht op de onderhouder van de component voordat u uw eigen gebruikers beschermt. De termijn voor kwetsbaarheidsafhandeling van uw product loopt onafhankelijk van die van de upstream.

De 13 cyberbeveiligingsvereisten voor het product

Elk product met digitale elementen moet voldoen aan dertien basisvereisten voor beveiliging wanneer het op de markt wordt aangeboden, en gedurende de ondersteuningsperiode blijven voldoen. Zij zijn de bodem voor wat cyberbeveiliging onder de CRA in productterm betekent.

De dertien vereisten zijn:

- Geen bekende uitbuitbare kwetsbaarheden op het moment van marktintroductie
- Standaard beveiligde configuratie
- Beveiligingsupdates, inclusief automatische updates met opt-out
- Bescherming tegen ongeoorloofde toegang
- Vertrouwelijkheid van opgeslagen, verzonden en verwerkte gegevens
- Integriteit van gegevens, firmware en configuratie
- Minimale gegevensverwerking
- Beschikbaarheid en weerbaarheid, ook tegen denial-of-serviceaanvallen
- Geen negatieve impact op andere verbonden apparaten of netwerken
- Beperkt aanvalsoppervlak, inclusief externe interfaces
- Beperkte incidentimpact door mitigatie van uitbuiting
- Registratie van beveiligingsrelevante activiteiten met opt-out voor de gebruiker
- Veilige en permanente verwijdering van gegevens en portabiliteit

Elke vereiste wordt later in de gids in detail uitgewerkt, met de praktische betekenis en het bewijs dat u in het dossier hoort te bewaren.

De 8 vereisten voor kwetsbaarheidsafhandeling

Fabrikanten hebben ook processen voor kwetsbaarheidsafhandeling nodig die gedurende de ondersteuningsperiode blijven draaien:

1. Kwetsbaarheden identificeren en documenteren (inclusief softwarestuklijst, SBOM)
2. Risicobeheer en tijdige beveiligingsupdates
3. Regelmatige beveiligingstests
4. Informatie over beveiligingsupdates en openbaarmaking van kwetsbaarheden
5. Beleid voor gecoördineerde kwetsbaarheidsopenbaarmaking (CVD)
6. Contact voor delen en melden van kwetsbaarheden
7. Veilige mechanismen voor verspreiding van updates
8. Kosteloze beveiligingsupdates met adviesberichten

Meldtermijnen van artikel 14

Deze verplichtingen gelden vanaf **11 september 2026**. Zij gelden voor fabrikanten van producten met digitale elementen binnen het toepassingsgebied, ook wanneer die producten voor **11 december 2027** op de markt zijn aangeboden. Micro-ondernemingen en kleine ondernemingen zijn niet algemeen vrijgesteld van meldingen. De boeteverlichting voor kleine ondernemingen is beperkt: zij ziet alleen op de eerste **24-uursdeadline voor de vroegtijdige waarschuwing**.

De CRA onderscheidt drie niveaus van kwetsbaarheidsstatus:

- **Kwetsbaarheid:** elke zwakke plek die kan worden uitgebuit
- **Uitbuitbare kwetsbaarheid:** een zwakke plek die onder realistische omstandigheden kan worden gebruikt
- **Actief uitgebuite kwetsbaarheid:** een kwetsbaarheid waarvan bevestigd is dat die in een aanval is gebruikt

Wanneer de klok start

U zit niet op de klok zodra een signaal binnenkomt. De klok start nadat u een eerste beoordeling heeft gedaan en met een redelijke mate van zekerheid weet dat een kwetsbaarheid in uw product actief wordt uitgebuit, of dat een ernstig incident de beveiliging van uw product heeft gecompromitteerd. De nadruk ligt op een prompte eerste beoordeling, niet op wachten tot het volledige onderzoek is afgerond. Brengt een klant, onderzoeker, autoriteit of andere derde een mogelijk probleem onder uw aandacht, beoordeel het dan zonder vertraging en start de klok zodra die beoordeling u de redelijke zekerheid geeft.

Wanneer u een **actief uitgebuite kwetsbaarheid** vaststelt, geldt deze meldingstijdlijn:

Termijn	Wat is vereist	Waar melden
Binnen 24 uur	Vroegtijdige waarschuwing over actieve uitbuiting	ENISA via nationale CSIRT
Binnen 72 uur	Kwetsbaarheidsmelding: getroffen product, algemene aard van exploit en kwetsbaarheid, mitigerende maatregelen, corrigerende maatregelen die gebruikers kunnen nemen en gevoeligheidsmarkering waar van toepassing	ENISA via nationale CSIRT
Uiterlijk 14 dagen nadat een corrigerende of mitigerende maatregel beschikbaar is	Eindrapport: beschrijving van de kwetsbaarheid, ernst, impact, beschikbare informatie over kwaadwillende actoren en details van de beveiligingsupdate of andere corrigerende maatregel	ENISA via nationale CSIRT

Wanneer u een **ernstig incident** vaststelt dat gevolgen heeft voor de beveiliging van het product, geldt deze meldingstijdlijn:

Termijn	Wat is vereist	Waar melden
Binnen 24 uur	Vroegtijdige waarschuwing, inclusief of vermoed wordt dat het incident door onrechtmatige of kwaadwillige handelingen is veroorzaakt	ENISA via nationale CSIRT
Binnen 72 uur	Incidentmelding: aard van het incident, eerste beoordeling, mitigerende maatregelen, corrigerende maatregelen die gebruikers kunnen nemen en gevoeligheidsmarkering waar van toepassing	ENISA via nationale CSIRT
Binnen een maand na de incidentmelding van 72 uur	Eindrapport: gedetailleerde incidentbeschrijving, ernst, impact, waarschijnlijke dreiging of oorzaak, en toegepaste of lopende mitigerende maatregelen	ENISA via nationale CSIRT

Meldingen worden bijgewerkt naarmate u meer weet

De inzendingen van 24 uur, 72 uur en 14 dagen (of een maand) zijn fasen van dezelfde melding, geen aparte indieningen. Elke fase voegt de informatie toe die in de vorige nog niet beschikbaar was. De CSIRT die als coördinator is aangewezen, kan ook op elk moment om een tussentijdse update vragen. U hoeft informatie die u al heeft verstrekt niet te herhalen.

Meldingen worden ingediend via het **CRA-éénloketmeldplatform**, gerouteerd via het nationale Computer Security Incident Response Team (CSIRT) in de hoofdlidstaat van de fabrikant, met gelijktijdige toegang voor ENISA.

Uw gebruikers informeren

Nadat u op de hoogte bent, moet u de getroffen gebruikers van de kwetsbaarheid of het incident informeren en, waar passend, alle gebruikers, over risicobeperkende en corrigerende maatregelen die zij kunnen toepassen. Dat is niet hetzelfde als publieke openbaarmaking. De plicht is om de informatie bij de gebruikers te krijgen die haar nodig hebben om zichzelf te beschermen, evenredig aan het risico. Voor producten die in gevoelige of essentiële omgevingen worden gebruikt, beperkt u gedetailleerde technische informatie tot de betrokken klanten zolang de kwetsbaarheid niet is gemitigeerd; vroege publieke detail kan uitbuiting makkelijker maken.

Zodra de kwetsbaarheid is verholpen of gemitigeerd, kan bredere openbaarmaking gepast worden om gebruikers te helpen verifiëren dat hun producten niet langer geraakt zijn en om algemeen bewustzijn te vergroten. Houd het detailniveau en de timing evenredig aan het restrisico. Informeert u gebruikers niet tijdig, dan kan de CSIRT die informatie zelf verstrekken waar zij dat evenredig en nodig acht.

Actief uitgebuite kwetsbaarheid	
24 uur	vroegtijdige waarschuwing
72 uur	kwetsbaarheidsmelding
14 dagen na corrigerende maatregel	eindrapport

Ernstig incident	
24 uur	vroegtijdige waarschuwing
72 uur	incidentmelding
een maand na de 72-uursmelding	eindrapport

Corrigerende maatregelen wanneer een product niet conform is

Weet u, of heeft u reden om te vermoeden, dat een product dat u op de markt heeft aangeboden, of een van uw processen, niet voldoet aan de essentiële cyberbeveiligingsvereisten van de CRA, dan moet u direct handelen. De plicht loopt vanaf marktintroductie en de hele ondersteuningsperiode door.

De drie opties

1. **In overeenstemming brengen.** Verhelp het product of het proces. Voor softwareproducten is dat doorgaans een beveiligingsupdate of een proceswijziging. Pas de fix toe op de ondersteunde versies.
2. **Uit de handel nemen.** Stop met het beschikbaar stellen van het product op de markt. Trek het terug uit uw toeleveringsketen en bij detailhandelaren, integrators en wederverkopers die voorraad houden.
3. **Terugroepen.** Haal het product terug van gebruikers die het al hebben. Pas dit toe waar het cyberbeveiligingsrisico voor gebruikers significant is en een fix of intrekking alleen niet volstaat.

De keuze is evenredig aan het risico, geen vaste volgorde. Een te patchen kwetsbaarheid met een werkende fix betekent meestal *in overeenstemming brengen*. Een product dat niet veilig in het veld kan worden hersteld, betekent meestal *uit de handel nemen* en, wanneer het actief in gebruik is met een significant risico, *terugroepen*.

Wat u ook moet doen

- **Meld via de keten van artikel 14** wanneer de non-conformiteit een actief uitgebuite kwetsbaarheid of een ernstig incident is. De meldingstijdlijn staat hierboven.
- **Informeer gebruikers** over de non-conformiteit en over corrigerende maatregelen die zij zelf kunnen toepassen. Zie *Uw gebruikers informeren* hierboven voor de evenredigheidsregels.
- **Werk mee** met elk gemotiveerd verzoek van een markttoezichtautoriteit, inclusief het verstrekken van technische documentatie in een taal die zij kan lezen.
- **Bewaar bewijs.** Houd de registraties bij die laten zien wat u heeft gevonden, wanneer u het heeft gevonden, wat u eraan heeft gedaan en hoe u heeft gecommuniceerd met gebruikers en autoriteiten. De technische documentatie en EU-conformiteitsverklaring moeten ten minste 10 jaar na marktintroductie beschikbaar blijven, of voor de volledige ondersteuningsperiode, naargelang welke periode langer is.

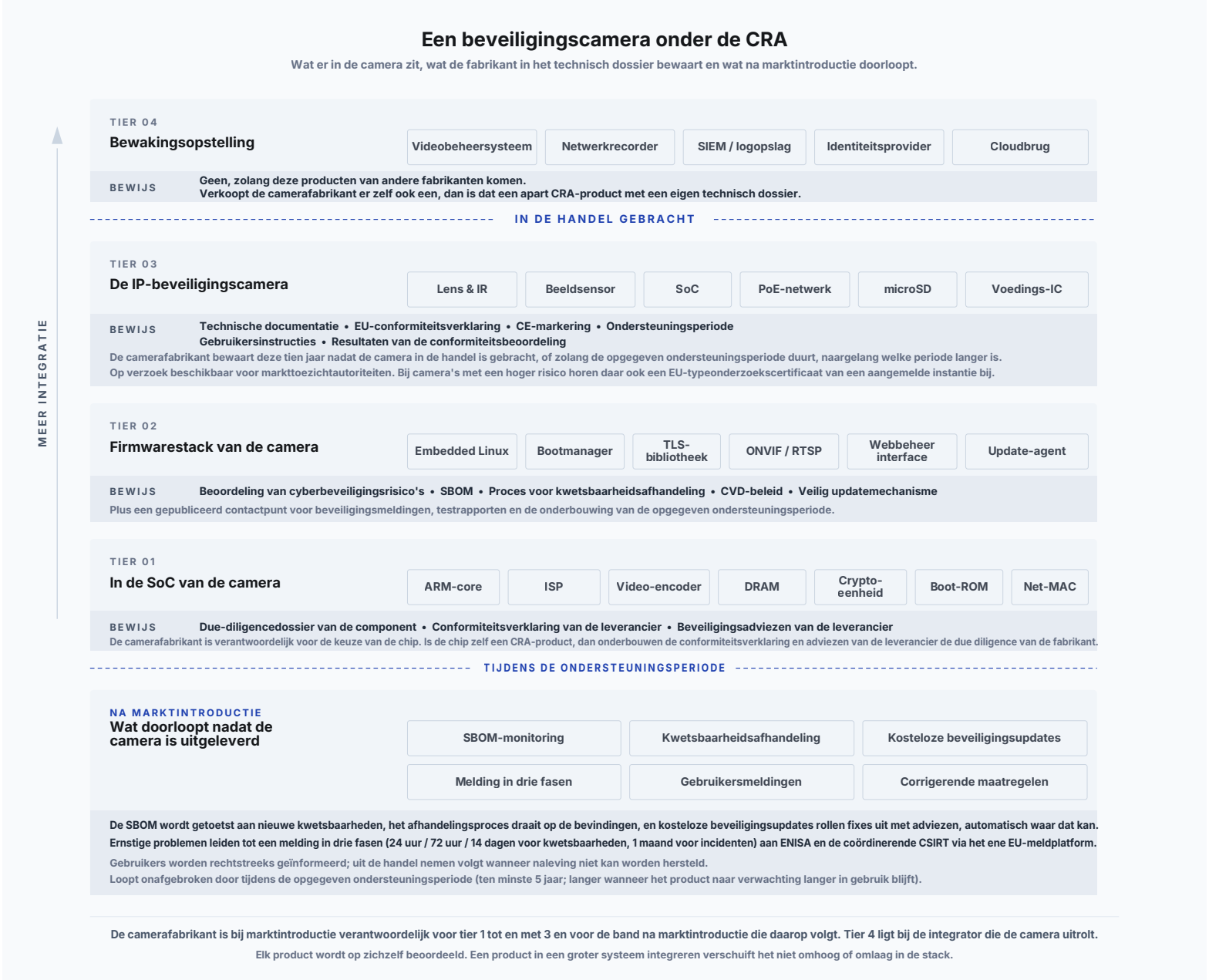
Productdocumentatievereisten

Documentatie moet ten minste **10 jaar** worden bewaard nadat het product op de markt is aangeboden, of voor de **volledige ondersteuningsperiode**, naargelang welke periode langer is. Op hoofdlijnen heeft de technische documentatie acht bewijsfamilies nodig:

1. Algemene productbeschrijving
2. Details van ontwerp, ontwikkeling en productie (inclusief SBOM)
3. Beoordeling van cyberbeveiligingsrisico's
4. Bepaling van de ondersteuningsperiode
5. Toegepaste geharmoniseerde normen en specificaties
6. Testrapporten
7. EU-conformiteitsverklaring
8. Volledige SBOM (op verzoek van markttoezichtautoriteiten)

Checklist voor de conformiteitsbeoordelingsroute

Gebruik de classificatietabel hierboven om de route vast te stellen. Bewaar daarna de routebeslissing in de technische documentatie, samen met de normen, specificaties, het certificeringsschema of het bewijs van de aangemelde instantie waarmee de keuze is onderbouwd.



Een uitgewerkt voorbeeld. Dezelfde gelaagde structuur geldt voor elk product met digitale elementen, niet alleen voor beveiligingscamera's.

Cyberbeveiligingsvereisten voor het product

a. Geen bekende uitbuitbare kwetsbaarheden op het moment van marktintroductie

Lever niet uit met publiek bekende uitbuitbare kwetsbaarheden die nog niet zijn behandeld. Een bekende kwetsbaarheid kan komen uit een publieke database, een leveranciersbericht, een klantmelding of uw eigen interne tracker.

Om aan deze vereiste te voldoen:

- Controleer kwetsbaarheidsdatabases (waaronder Common Vulnerabilities and Exposures, CVE) vóór elke release
- Gebruik statische en dynamische applicatiebeveiligingstests (SAST/DAST) in uw build-pipeline
- Voer afhankelijkheidsscans uit voor alle componenten van derden en opensourcecomponenten
- Documenteer uw besluit over risicoacceptatie of mitigatie voor elke vastgestelde kwestie

b. Standaard beveiligde configuratie

Het product moet veilig zijn in de standaardtoestand. Schakel onnodige diensten uit, vermijd zwakke standaardreferenties en houd elke onveilige inwerkingstellingsmodus kort en gecontroleerd. De vereiste voor standaardconfiguratie kan worden aangepast voor maatwerkproducten die volgens schriftelijke overeenkomst aan zakelijke gebruikers worden geleverd, maar een pad terug naar de oorspronkelijke veilige toestand moet beschikbaar blijven.

Om aan deze vereiste te voldoen:

- Schakel poorten voor toegang op afstand en debuginterfaces uit in standaardbouwen
- Dwing sterke standaardauthenticatiemechanismen af
- Beperk beheerderfuncties tot bevoegde gebruikers
- Implementeer een veilige fabrieksreset die alle instellingen en firmware terugzet naar een bekende veilige toestand en gebruikersgegevens verwijdert

c. Beveiligingsupdates, inclusief automatische updates met opt-out

Het product heeft een patchmechanisme nodig dat na uitrol met beveiligingsproblemen kan omgaan. Waar automatische updates passend zijn, schakelt u die standaard in en geeft u gebruikers een heldere manier om uit te stellen of zich af te melden.

Om aan deze vereiste te voldoen:

- Implementeer cryptografische ondertekening en integriteitsverificatie voor updatepakketten
- Bied rollbackpreventie en logging van update-gebeurtenissen
- Bouw meldingssystemen die gebruikers op de hoogte stellen van openstaande updates
- Sta gebruikers toe automatische updates uit te stellen of uit te schakelen via een heldere configuratie-interface

d. Bescherming tegen ongeoorloofde toegang

Toegangscontroles moeten zowel lokale als externe interfaces beschermen. Het doel is voorkomen dat ongeoorloofde gebruikers bij functies, gegevens, configuratie of beheersurfaces komen.

Om aan deze vereiste te voldoen:

- Dwing wachtwoordcomplexiteitsbeleid en sterke standaardreferenties af
- Implementeer multifactorauthenticatie (MFA) waar passend
- Pas rolgebaseerde toegangscontrole (RBAC) en sessietime-outafhandeling toe
- Log mislukte toegangspogingen, gebruik anomaliedetectie om ongeoorloofde activiteit te markeren en breng die gebeurtenissen naar boven voor beoordeling en melding

e. Vertrouwelijkheid van opgeslagen, verzonden en verwerkte gegevens

Gevoelige gegevens hebben bescherming nodig in rust, tijdens verzending en tijdens verwerking.

Om aan deze vereiste te voldoen:

- Gebruik gestandaardiseerde versleutelingsalgoritmen (bijvoorbeeld AES-256 voor data in rust, TLS voor data in transit)
- Pas veilige sleutelbeheerpraktijken toe
- Scheid vertrouwelijke gegevens van niet-kritieke systeemcomponenten
- Houd auditlogs bij voor alle gebeurtenissen rond gegevenstoegang

f. Integriteit van gegevens, firmware en configuratie

Deze vereiste dekt het systeem zelf (firmware, software, configuratiebestanden) en de gegevens die het verwerkt (metingen, besturingscommando's, gebruikersinvoer).

Om aan deze vereiste te voldoen:

- Implementeer secure boot en ondertekende firmware zodat alleen vertrouwde code wordt uitgevoerd
- Gebruik runtime-verificatie om manipulatiepogingen te detecteren en te melden
- Pas cryptografische hashing en digitale handtekeningen toe om de integriteit van gegevens te beschermen
- Bouw infrastructuur die cryptografische sleutels kan genereren, distribueren en verifiëren over systeem- of organisatiegrenzen heen

g. Minimale gegevensverwerking

Verzamel en verwerk alleen de gegevens die nodig zijn voor het beoogde doel van het product. Dit geldt voor persoonsgegevens en technische gegevens.

Om aan deze vereiste te voldoen:

- Voer privacy-impactbeoordelingen of oefeningen voor gegevensbescherming door ontwerp uit om onnodige gegevensstromen in kaart te brengen
- Verwijder ongebruikte telemetrie, diagnostiek of achtergrondverzameling of maak die optioneel
- Implementeer instelbare opties voor gegevensverzameling zodat uitgebreide verzameling op basis van context aan of uit kan

h. Beschikbaarheid en weerbaarheid, ook tegen denial-of-serviceaanvallen

Tijdens incidenten of aanvallen moeten kernfuncties van het product beschikbaar blijven of op een gecontroleerde manier falen.

Om aan deze vereiste te voldoen:

- Implementeer circuit breakers, retry-logica, fallback-mechanismen en watchdog-timers
- Pas resourcebeperkingen toe om uitputting van middelen te voorkomen
- Gebruik rate limiting en invoervalidatie om bescherming tegen denial-of-servicescenario's te bieden
- Pas filtering op netwerkniveau toe om overbelastingspogingen te blokkeren

i. Geen negatieve impact op andere verbonden apparaten of netwerken

Het product mag geen andere systemen in dezelfde omgeving verstoren. Het hoort zich voorspelbaar te gedragen en buitensporig gebruik van gedeelde resources te vermijden.

Om aan deze vereiste te voldoen:

- Implementeer traffic shaping en beperk broadcast- of multicastgebruik
- Zorg voor naleving van specificaties voor communicatieprotocollen
- Gebruik zelfmonitoring om verstorend gedrag zoals netwerk-flooding of resource-uitputting te detecteren en te voorkomen

j. Beperkt aanvalsoppervlak, inclusief externe interfaces

Beperk toegangspunten en blootgestelde functionaliteit. Dit omvat fysieke poorten, draadloze interfaces, API's, debugservices en onnodige softwarecomponenten.

Om aan deze vereiste te voldoen:

- Schakel ongebruikte diensten, poorten en interfaces uit in productiebouwen
- Verstevig systeem-standaarden en beperk gebruikersrechten
- Modulariseer softwarearchitecturen om componenten van elkaar te isoleren
- Pas principes van veilig softwareontwerp toe en voer threat modelling uit om onnodige blootstelling te identificeren en te verwijderen

k. Beperkte incidentimpact door mitigatie van uitbuiting

Ga ervan uit dat sommige aanvallen zullen slagen. Het productontwerp hoort te beperken hoe ver schade zich kan verspreiden.

Om aan deze vereiste te voldoen:

- Scheid systeemcomponenten en draai ze in geïsoleerde omgevingen met sandboxing of containerisatie
- Dwing rechtenscheiding af zodat kritieke functies met de minimaal vereiste rechten draaien
- Ontwerp zo dat compromittering van één component een aanvaller geen controle over het volledige systeem geeft

l. Registratie van beveiligingsrelevante activiteiten met opt-out voor de gebruiker

Registreer beveiligingsrelevante activiteit, zoals toegangspogingen en gegevenswijzigingen, zodat zij gemonitord en geaudit kan worden. Gebruikers hebben een opt-outmechanisme waar de CRA dat vereist.

Om aan deze vereiste te voldoen:

- Implementeer gestructureerde logging (bijvoorbeeld JSON-logs met tijdstempels)
- Bied lokale logopslag met logrotatie en opties voor remote log streaming
- Monitor gebeurtenissen zoals inlogpogingen, configuratiewijzigingen en software-updates op anomalieën
- Bied een heldere voor gebruiker zichtbare mogelijkheid om logging uit te schakelen waar dat is toegestaan

m. Veilige en permanente verwijdering van gegevens en portabiliteit

Gebruikers hebben een praktische manier nodig om gegevens en instellingen permanent te verwijderen. Waar gegevens naar een ander product of systeem kunnen worden overgedragen, moet die overdracht veilig gebeuren.

Om aan deze vereiste te voldoen:

- Implementeer een veilige wisfunctie die opslagregio's overschrijft of sleutels cryptografisch vernietigt
- Gebruik geauthenticeerde en versleutelde kanalen voor overdrachten ten behoeve van portabiliteit om blootstelling tijdens de overdracht te voorkomen

Vereisten voor kwetsbaarheidsafhandeling

1. Kwetsbaarheden identificeren en documenteren

U moet weten welke softwarecomponenten in het product zitten en welke bekende kwetsbaarheden daarop van toepassing zijn. Een softwarestuklijst (SBOM) geeft u die machineleesbare inventaris.

Om aan deze vereiste te voldoen:

- Integreer SBOM-generatie rechtstreeks in uw CI/CD-pipeline zodat elke build een actuele componentinventaris oplevert
- Gebruik gevestigde formaten zoals CycloneDX, SPDX of SWID voor interoperabiliteit
- Voer geautomatiseerde kwetsbaarheidsscans uit tegen CVE-lijsten en databases zoals CISA KEV en ENISA EUVD
- Onderhoud de SBOM als onderdeel van uw technische documentatie gedurende de ondersteuningsperiode en stel haar op verzoek aan markttoezichtautoriteiten beschikbaar

2. Risicobeheer en tijdige beveiligingsupdates

Worden kwetsbaarheden gevonden, los ze dan snel op en lever beveiligingsupdates uit. Scheid waar mogelijk beveiligingspatches van functionele updates, zodat kritieke fixes snel kunnen worden geïnstalleerd.

Om aan deze vereiste te voldoen:

- Ontwerp uw updatemechanisme zo dat beveiligingsfixes kunnen worden uitgerold zonder een volledige systeemupdate te vereisen
- Structureer software en firmware zodat kritieke componenten onafhankelijk kunnen worden gepatcht
- Lever updates via veilige kanalen met integriteitscontroles
- Houd registraties van update-activiteiten bij om traceerbaarheid te ondersteunen en naleving aan te tonen

3. Regelmatige beveiligingstests

Beveiligingstests zijn geen eenmalige exercitie. Test producten gedurende de hele levenscyclus naarmate dreigingen, afhankelijkheden en productgedrag veranderen. Laat de risicobeoordeling het type en de frequentie van tests sturen.

Om aan deze vereiste te voldoen:

- Voer penetratietests uit om aanvallen uit de echte wereld te simuleren
- Pas statische en dynamische code-analyse toe om beveiligingszwakheden te vinden
- Gebruik fuzztests om fouten in invoerafhandeling bloot te leggen
- Plan en documenteer beveiligingscodebeoordelingen en architectuurbeoordelingen formeel, vooral na significante ontwerp- of functiewijzigingen

4. Intake, CVD-beleid en adviezen rond kwetsbaarheden

Dekt de plichten rond intake, gecoördineerde openbaarmaking en adviezen (de punten 4, 5 en 6 van de samenvatting hierboven), die in de praktijk als één workflow draaien.

De CRA noemt drie aparte vereisten voor hoe u rond kwetsbaarheden communiceert: een manier voor mensen om problemen te melden, een beleid voor gecoördineerde openbaarmaking en een advies wanneer u een fix uitlevert. Hier staat wat elke plicht vraagt.

Intake

Geef melders een heldere, laagdrempelige route. Publiceer een zichtbare contactmethode voor kwetsbaarheidsmeldingen (een specifiek e-mailadres of webformulier). Ondersteun veilige communicatie, bijvoorbeeld door een PGP-sleutel te publiceren. De plicht dekt meldingen over uw eigen product en over de componenten van derden die het bevat.

Triage

Bevestig elke melding, log haar in een trackingsysteem, wijs haar toe voor beoordeling en los haar op binnen vastgelegde termijnen. Stuur bevestiging en statusupdates terug aan de melder. Zit het probleem in een component van een derde, route het dan parallel met uw eigen herstel naar de upstream-onderhouder.

Beleid voor gecoördineerde kwetsbaarheidsopenbaarmaking

Publiceer een CVD-beleid dat verwachtingen vastlegt voor melders en partners: contactmethode, verwachte reactietijden, waartoe u zich verbindt en wat u van hen vraagt. Coördineer openbaarmaking om gebruikers te beschermen en de bijdrage van de melder te erkennen.

Adviezen bij fix

Zodra een fix beschikbaar is, publiceer een advies voor de opgeloste kwestie. Vermeld de CVE-identificator, de getroffen productversies, een gestandaardiseerde ernstscore (bijvoorbeeld CVSS) en heldere, toegankelijke informatie over wat gebruikers moeten doen. Schrijf in taal die toegankelijk is voor zowel technische beheerders als niet-technische gebruikers.

Uitgestelde publieke openbaarmaking

U mag publieke openbaarmaking alleen uitstellen waar u een terecht gemotiveerde reden heeft dat de cyberbeveiligingsrisico's van directe openbaarmaking zwaarder wegen dan de voordelen, en alleen tot gebruikers de kans hebben gehad de fix toe te passen. Documenteer de redenering.

5. Veilige mechanismen voor verspreiding van updates

Het updatemechanisme moet betrouwbaar en bestand tegen manipulatie zijn. Waar automatische updates technisch haalbaar zijn, verkorten zij de tijd dat gebruikers blootgesteld blijven.

Om aan deze vereiste te voldoen:

- Verzend updates over veilige kanalen en verifieer ze via digitale handtekeningen
- Pas updates zo toe dat onvolledige of beschadigde installaties worden voorkomen
- Gebruik differentiële of modulaire updates om hinder te beperken en fixes sneller bij systemen te krijgen
- Houd updatelogs bij zodat gebruikers of beheerders de updatestatus kunnen verifiëren

6. Kosteloze beveiligingsupdates met adviesberichten

Lever beveiligingsupdates snel en zonder extra kosten uit, behalve waar een aparte overeenkomst geldt voor maatwerkproducten voor zakelijke gebruikers. Elke update heeft een helder adviesbericht nodig dat gebruikers vertelt wat er is veranderd en wat zij moeten doen.

Om aan deze vereiste te voldoen:

- Onderhoud een distributiesysteem dat gebruikers direct kan informeren of updates automatisch kan toepassen, afhankelijk van de productcontext
- Schrijf adviesberichten in taal die begrijpelijk is voor zowel technische als niet-technische gebruikers
- Vermeld ernstinformatie in adviesberichten waar relevant
- Vertel gebruikers welke actie te ondernemen, zoals de update toepassen, een configuratie aanpassen of letten op tekenen van compromittering
- Verspreid beveiligingsupdates zonder vertraging zodra ze beschikbaar zijn, zodat gebruikers niet blootgesteld blijven terwijl de fix al bestaat
- Publiceer adviezen via een door de fabrikant beheerd kanaal en koppel ernaar vanaf de ondersteuningspagina van het product

De plichten van kosteloos en zonder vertraging lopen door voor de duur van de gepubliceerde ondersteuningsperiode. De uitzondering voor maatwerk verandert alleen de commerciële basis; adviesberichten blijven gelden.

Inhoud van de technische documentatie

Technische documentatie

De technische documentatie is het centrale bewijs van CRA-conformiteit. Zij moet de ontwerp-, technische en procedurele maatregelen dekken die worden gebruikt om aan de essentiële cyberbeveiligingsvereisten te voldoen. Zij moet **vóór marktintroductie** bestaan en gedurende de **ondersteuningsperiode** actueel blijven.

Technisch bewijs door de engineeringworkflow heen

Stap 1	**Afbakenen en classificeren**	Productdoel, beoogd gebruik, marktintroductiebesluit, productklasse, route via normen.
Stap 2	**Architectuur en risico**	Architectuur, gegevensverbindingen, gebruiksvoorwaarden, risicobeoordeling, mitigaties.
Stap 3	**Componenten en SBOM**	Machineleesbare SBOM, componenten van derden, leveranciersinput, kwetsbaarheidstracking.
Stap 4	**Bouwen, testen, bijwerken**	Veilige standaardinstellingen, hardening, testrapporten, veilig updatemechanisme, adviesberichten.
Stap 5	**Release en ondersteuning**	Gebruikersinstructies, EU-verklaring, CE-bewijs, onderbouwing van de ondersteuningsperiode, updaterecords.

De technische documentatie heeft acht verplichte componenten. Samen leggen zij uit **wat het product is**, **hoe het is gebouwd en getest**, **welke risico's zijn overwogen**, **welke normen zijn toegepast** en **hoe het zal worden ondersteund** zodra het op de markt is. U hoeft de juridische rubrieken niet te kopiëren, maar elk onderwerp moet zijn gedekt.

Nr.	Component	Wat het moet bevatten
1	Algemene productbeschrijving	Beoogd doel en functies, relevante softwareversies, foto's of illustraties (voor hardware), gebruikersinformatie en instructies
2	Details van ontwerp, ontwikkeling en productie	Architectuurbeschrijving (componenten en interacties), softwarestuklijst (SBOM), processen voor kwetsbaarheidsafhandeling (CVD-beleid, contactpunt, veilige updatemechanismen), productie- en monitoringprocessen inclusief validatie
3	Beoordeling van cyberbeveiligingsrisico's	Gedocumenteerde analyse van productrisico's, uitleg hoe elke essentiële cyberbeveiligingsvereiste op het product van toepassing is, mitigatie van vastgestelde risico's
4	Bepaling van de ondersteuningsperiode	Documentatie van de factoren die zijn gebruikt om de ondersteuningsperiode vast te stellen, zoals gebruikersverwachtingen, vergelijkbare producten en wettelijke richtsnoeren
5	Toegepaste geharmoniseerde normen en specificaties	Lijst van geharmoniseerde normen, gemeenschappelijke specificaties of EU-certificeringsschema's; indicatie of zij volledig of deels zijn toegepast; alternatieve oplossingen waar normen niet zijn toegepast
6	Testrapporten	Bewijs van conformiteit voor zowel het product als de processen voor kwetsbaarheidsafhandeling
7	EU-conformiteitsverklaring	Kopie van de verklaring die de technische documentatie verbindt met CE-markeringsverplichtingen
8	Volledige SBOM (op verzoek)	Markttoezichtautoriteiten kunnen de volledige SBOM opvragen om naleving te verifiëren

Eén geconsolideerd technisch dossier kan zowel de CRA als andere toepasselijke EU-wetgeving dekken (bijvoorbeeld de Richtlijn radioapparatuur of de ESPR), mits alle toepasselijke verplichtingen erin staan.

EU-conformiteitsverklaring

De EU-conformiteitsverklaring is de formele verklaring van de fabrikant dat het product voldoet aan de toepasselijke CRA-cyberbeveiligingsvereisten. Elke verklaring moet bevatten:

- Productnaam, type en unieke identificatoren
- Naam en adres van de fabrikant (of gemachtigde vertegenwoordiger)
- Verklaring van uitsluitende verantwoordelijkheid van de aanbieder
- Productbeschrijving die traceerbaarheid waarborgt (optioneel met afbeelding)
- Expliciete verklaring van conformiteit met de relevante Uniewetgeving
- Verwijzingen naar gebruikte geharmoniseerde normen, specificaties of certificeringen
- Gegevens van een eventueel betrokken aangemelde instantie (naam, nummer, procedure, certificaatnummer)
- Ondertekeningsblok: plaats, datum, naam, functie en handtekening van de ondertekenaar

Eenmaal ondertekend is de verklaring juridisch bindend en bevestigt zij de volledige verantwoordelijkheid van de fabrikant voor cyberbeveiligingsconformiteit.

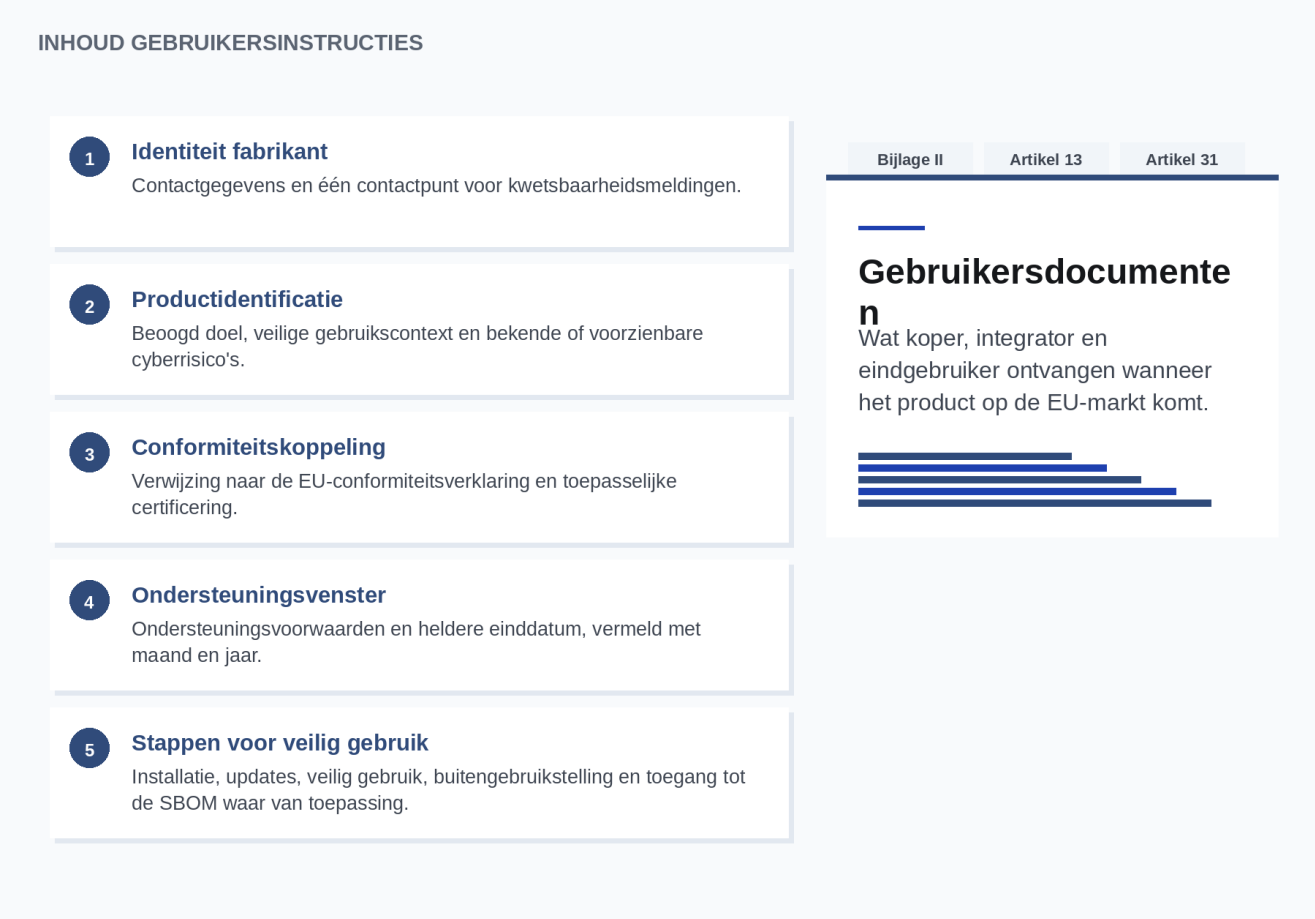
Een vereenvoudigde verklaring is toegestaan voor gebruik op verpakkingen of in handleidingen, in de vorm: "Hierbij verklaart [fabrikant] dat het product [type/aanduiding] voldoet aan Verordening (EU) 2024/2847. De volledige tekst van de EU-conformiteitsverklaring is beschikbaar op: [webadres]." Deze vereenvoudigde vorm behoudt transparantie en vermindert papierwerk, en is met name nuttig voor kleine fabrikanten of multi-product-portfolio's.

Gebruikersinformatie en -instructies

Gebruikersinformatie en -instructies zijn een voorwaarde voor rechtmatige marktintroductie. Fabrikanten moeten instructies ten minste **10 jaar** beschikbaar houden, of voor de **volledige ondersteuningsperiode**. Importeurs en distributeurs moeten controleren of de instructies bestaan, actueel zijn en in de juiste EU-taal worden geleverd voordat zij het product op de markt aanbieden of leveren.

De gebruikersinstructies moeten bevatten:

- Identiteit en contactgegevens van de fabrikant
- Eén contactpunt voor kwetsbaarheidsmeldingen
- Productidentificatie, beoogd doel en veilige gebruikscontext
- Bekende of voorzienbare cyberrisico's
- Koppeling naar de EU-conformiteitsverklaring
- Ondersteuningsvoorwaarden en heldere einddatum van ondersteuning
- Stapsgewijze beveiligingsinstructies voor installatie, updates, veilig gebruik, buitengebruikstelling en (indien van toepassing) integratie en toegang tot de SBOM



De juiste conformiteitsbeoordelingsroute kiezen

module A: zelfbeoordeling

Module A (interne controle) staat u toe zelf te certificeren dat uw product voldoet aan de essentiële cyberbeveiligingsvereisten, met volledige verantwoordelijkheid voor zowel ontwerp als productie. Deze route is beschikbaar voor fabrikanten van standaardproducten (niet-geclassificeerd). Zij is ook beschikbaar voor belangrijke producten van klasse I alleen wanneer de relevante geharmoniseerde normen, gemeenschappelijke specificaties of Europese cyberbeveiligingscertificeringsschema's beschikbaar zijn en worden toegepast zoals de CRA-routeregels vereisen.

Onder module A moet u:

- Uitgebreide technische documentatie opstellen
- Het ontwerp van het product, de productieprocessen, de cyberbeveiligingsmechanismen en de procedures voor kwetsbaarheidsafhandeling beschrijven
- Doorlopende verantwoordelijkheid voor blijvende conformiteit dragen gedurende de hele levenscyclus van het product
- Een plan voor beveiligingsupdates en kwetsbaarheidsbeheer uitvoeren tijdens de operationele levensduur van het product
- Registraties ten minste 10 jaar beschikbaar houden

module B en C: productgerichte beoordeling

Modules B en C gelden waar verificatie door een derde van een specifiek producttype vereist is. Zij gelden voor belangrijke klasse I-producten waar de fabrikant relevante geharmoniseerde normen, gemeenschappelijke specificaties of certificeringsschema's niet, slechts gedeeltelijk of niet kan toepassen. Voor belangrijke klasse II-producten moet de fabrikant module B+C, module H of een toepasselijk Europees cyberbeveiligingscertificeringsschema met ten minste betrouwbaarheidsniveau "substantieel" gebruiken.

Module B (EU-typeonderzoek): Een aangemelde instantie onderzoekt een representatief productmonster en de bijbehorende technische documentatie. Zij verifieert naleving van alle essentiële cyberbeveiligingsvereisten en geeft een EU-typeonderzoekscertificaat af wanneer het ontwerp van het product aan de CRA-criteria voldoet.

Module C (conformiteit met het type, productiecontrole): De fabrikant zorgt ervoor dat alle productie-eenheden overeenkomen met het onder module B gecertificeerde type. De fabrikant brengt de CE-markering aan, geeft de EU-conformiteitsverklaring uit en houdt registraties ten minste 10 jaar beschikbaar. Samen waarborgen modules B en C dat een specifiek productmodel technisch conform is en dat elke productiebatch consistent blijft met het goedgekeurde ontwerp.

module H: procesgerichte beoordeling (volledige kwaliteitsborging)

Module H (volledige kwaliteitsborging) richt zich op het volledige interne kwaliteitssysteem van de fabrikant in plaats van op individuele producttests. Zij is beschikbaar voor belangrijke klasse I- en klasse II-producten. Kritieke producten gebruiken de certificeringsroute waar de relevante voorwaarden zijn vervuld; waar die voorwaarden niet zijn vervuld, gebruiken zij dezelfde routes die beschikbaar zijn voor belangrijke klasse II-producten.

Onder module H moet u:

- Een kwaliteitssysteem opzetten en onderhouden dat ontwerp, ontwikkeling, productie, testen en kwetsbaarheidsafhandeling dekt voor de hele productcategorie
- Het kwaliteitssysteem ter beoordeling en goedkeuring voorleggen aan een aangemelde instantie
- Doorlopend toezicht aanvaarden (audits, inspecties en procesbeoordelingen) door de aangemelde instantie om blijvende conformiteit te verifiëren

Eenmaal goedgekeurd mag u conformiteitsverklaringen uitgeven voor alle producten die onder dat kwaliteitssysteem worden gemaakt, zonder het onderzoek door de aangemelde instantie voor elk afzonderlijk producttype te herhalen.

Het sleutelverschil tussen routes:

- Modules B+C: focus op het product. Een representatief producttype wordt getest en gecertificeerd.
- Module H: focus op het proces. Het volledige ontwerp- en productiesysteem van de fabrikant wordt gecertificeerd en gemonitord.

CONFORMITEITSBEOORDELINGSROUTES

A

module

Zelfbeoordeling

Standaardproducten en belangrijke klasse I waar geharmoniseerde normen, gemeenschappelijke specificaties of certificeringsschema's volledig zijn toegepast. Fabrikant draagt volledige verantwoordelijkheid voor ontwerp en productie.

B+C

module

Type en productie

Vereist voor belangrijke klasse I zonder toepasselijke normen en als onderdeel van de route voor belangrijke klasse II. Aangemelde instantie onderzoekt een representatief type; fabrikant zorgt dat elke productie-eenheid overeenkomt.

H

module

Volledige kwaliteitsborging

Beschikbaar voor belangrijke klasse I en II. De aangemelde instantie keurt het ontwerp-, ontwikkel-, productie-, test- en kwetsbaarheidsafhandelingssysteem van de fabrikant integraal goed en auditeert het.

Flow voor marktintroductie

De CRA in het bredere EU-regelgevingskader

De CRA staat niet op zichzelf. De vraag voor een fabrikant is praktisch: waar bespaart mijn CRA-werk inspanning onder een ander EU-regime, en waar heb ik nog steeds aparte verplichtingen die parallel lopen?

Waar uw CRA-werk hergebruikt kan worden

- **Hoog-risico AI-systemen (AI Act, Verordening 2024/1689).** Is uw product een hoog-risico AI-systeem binnen het toepassingsgebied van de CRA, dan wordt het voldoen aan de essentiële cyberbeveiligingsvereisten van de CRA geacht te voldoen aan de cyberbeveiligingsvereisten van de AI Act voor zover die door uw EU-conformiteitsverklaring worden gedekt. De conformiteitsbeoordelingsprocedure loopt in de regel via het AI Act-regime, met een uitzondering voor belangrijke en kritieke CRA-producten. De cyberbeveiligingsrisicobeoordeling van de CRA moet AI-specifieke risico's zoals datavergiftiging en adversariële aanvallen meenemen.
- **Geconsolideerde risicobeoordeling met andere Uniewetgeving.** De CRA staat uitdrukkelijk toe dat de cyberbeveiligingsrisicobeoordeling onderdeel vormt van een bredere risicobeoordeling die door een andere Uniewetshandeling wordt vereist, wanneer het product onder beide regimes valt. Eén beoordelingsartefact, twee regelgevende toepassingen.
- **Eén technisch dossier over regimes heen.** Zoals al genoemd in het hoofdstuk over de technische documentatie kan één geconsolideerd technisch dossier de CRA samen met andere toepasselijke Uniewetgeving dekken, mits de verplichtingen van elk regime worden geadresseerd. Nuttig waar hetzelfde product al documentatie nodig heeft onder de Richtlijn radioapparatuur, de Verordening ecologisch ontwerp voor duurzame producten of andere productwetgeving.
- **Gedeelde definities van refurbishment, onderhoud en reparatie.** De CRA importeert deze definities uit de Verordening ecologisch ontwerp voor duurzame producten. Wanneer u analyseert of een serviceactie als ingrijpende wijziging telt, zijn de Ecodesign-definities de referentie, niet een CRA-specifieke term.

Waar aparte verplichtingen blijven gelden

- **AI Act voor al het overige.** Cyberbeveiliging is slechts één snede van de AI Act. Risicoclassificatie, transparantie, datasetgovernance, menselijke controle, monitoring van AI-gedrag na marktintroductie en de rest zijn AI Act-plichten die de CRA niet adresseert. CRA-conforme cyberbeveiliging is geen vermoeden van AI Act-conformiteit als geheel.
- **Ecodesign en inhoud van het digitale productpaspoort.** Eisen aan energie-efficiëntie, duurzaamheid, repareerbaarheidsscores en de duurzaamheidsinhoud van het digitale productpaspoort vallen niet onder de CRA. Het CRA-bewijsspoor kan naast het Ecodesign-werk liggen maar vervangt het niet.
- **IoT-gegevenstoegangsrechten van de Data Act.** De Data Act geeft gebruikers contractuele rechten om de gegevens die hun verbonden producten genereren in te zien, te delen en over te dragen. De CRA dekt de beveiliging van die gegevens; zij regelt het toegangsrechtenregime niet. Andere verplichting, ander bewijs.
- **Productaansprakelijkheid voor gebrekkige producten.** De Richtlijn productaansprakelijkheid (2024/2853) houdt strikte aansprakelijkheid bij de fabrikant. Ontbrekende beveiligingsupdates na marktintroductie kunnen het aansprakelijkheidstriggerende gebrek zijn. Contracten, verzekering en incidentdraaiboeken moeten dit risico afdekken naast CRA-conformiteit.

Hoe CRA Evidence helpt

CRA Evidence zet EU CRA-verplichtingen om in verifieerbaar productbewijs en combineert een conformiteitsplatform met technisch advies.

Platform

Eén plaats om het bewijs achter CRA-gereedheid te beheren:

- **SBOM- en componentinventaris:** CycloneDX-, SPDX- en HBOM-records voor productversies en releases
- **CI/CD-bewijsautomatisering:** CLI- en API-workflows voor scans, SBOM-uploads, release gates en auditrecords
- **Ondertekende SBOM en herkomst:** versiegebonden bewijs, leveranciersverklaringen en due-diligencerecords
- **Kwetsbaarheidsoperaties:** CISA KEV, EPSS, VEX, monitoring, triage en meldworkflows
- **Technische documentatie en CE-bewijs:** EU-verklaringsrecords, bewaargeschiedenis en QR-gekoppelde productconformiteitspaspoorten

Technisch advies

Gerichte ondersteuning om CRA-verplichtingen te vertalen naar engineeringbesluiten voor product, architectuur, releaseproces en leveranciersmodel.

- **Technische gereedheidssprint:** gapreview van de essentiële vereisten, architectuuraanbevelingen en geprioriteerd actieplan
- **CRA-programmaleiding:** verantwoordelijkheidsmodel, verplichtingstracking, bewijsmijlpalen en onderhoud van technische documentatie
- **Plan voor autoriteiten en incidentrespons:** meldworkflows, inquiry playbooks, gebruikerscommunicatie en gereedheid van bewijspakketten
- **Regulatoire afstemming:** CRA-bewijs verbinden met Data Act, ESPR, AI Act, RED en sectorspecifieke vereisten
- **Technische workshops:** sessies op afstand of locatie met product, engineering, security, compliance en leveranciers

Tool-agnostisch: CRA Evidence integreert met CycloneDX, SPDX, Grype, Trivy, CI/CD-pipelines en issue trackers.

Een praktische eerste stap

Kies één productfamilie. Breng de eigenaar, scopebeslissing, SBOM, kwetsbaarheidsworkflow, hiaten in technische documentatie en releasebewijs in kaart. Dat geeft het team een concrete CRA-basis zonder conformiteit tot een apart project te maken.

Bekijk wat CRA Evidence voor uw product dekt op craevidence.com/nl. Tarieven en planopties staan op craevidence.com/nl/prijzen.