JURIDISCH UP TO DATE

Vaktijdschrift voor de juridische praktijk

Juridisch up to Date is een uitgave van Fiscaal up to Date – onderdeel van Rendement Uitgeverij BV
Conradstraat 18
3013 AP Rotterdam
E-mail: redactie@futd.nl

Hoofdredactie
Mr. dr. J. (Harry) van Drongelen
(emer.) universitair hoofddocent Sociaal Recht en Sociale Politiek, Universiteit van Tilburg & (gepens.) senior wetgevingsjurist Ministerie SZW

Mr. A.D.M. (André) van Rijs
Docent bij de vakgroep Private, Business and Labour Law van de Universiteit van Tilburg

Uitgever
Drs. M.P. Hoogerwerf

Abonnementenadministratie
Rendement Uitgeverij BV
Postbus 27020
3003 LA Rotterdam
Telefoon: (010) 243 39 33
E-mail: info@rendement.nl

Abonnementen
Juridisch Up to Date verschijnt 12 keer per jaar. (Proef) abonnementen kunnen ieder moment ingaan, maar slechts worden beëindigd indien uiterlijk twee maanden voor het einde van de abonnementsperiode is opgezegd. Zonder of bij niet-tijdige opzegging wordt het abonnement automatisch verlengd met een jaar. Abonnementen worden geacht zakelijk te zijn. Wilt u een particulier abonnement, dan dient u dit binnen één maand na het aangaan van het abonnement aan ons door te geven. Rendement behoudt zich het recht voor om prijzen en inhoud van de algemene voorwaarden te wijzigen. U kunt de volledige algemene voorwaarden nalezen op www.rendement.nl/av

ISSN 0924-9451
Alle rechten voorbehouden. Geen tekst- en datamining.

Niets uit deze uitgave mag, noch geheel, noch gedeeltelijk, worden overgenomen en/of vermenigvuldigd zonder voorafgaande schriftelijke toestemming van de uitgever.

Hoewel aan de totstandkoming van deze uitgave uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(en) en uitgever geen aansprakelijkheid voor eventuele fouten en onvolkomenheden, noch voor de gevolgen hiervan.

© Rendement Uitgeverij BV 2026

Follow us:
LinkedIn

Lauren Wendrich[1] en Frank Rutgers[2]

(Digitale) Productveiligheid is de nieuwe standaard voor hard- en software

2026-0136

Met de Cyber Resilience Act (Verordening (EU) 2024/2847, hierna: CRA) stelt de Europese Unie verplichte cybersecurity-eisen aan vrijwel alle hardware en software die op de Europese markt wordt gebracht. De verordening geldt gefaseerd: sinds 11 september 2026 moeten fabrikanten actief uitgebuite kwetsbaarheden melden, vanaf 11 december 2027 geldt de CRA volledig. Kern is dat de fabrikant de (digitale) veiligheid van zijn product vanaf het ontwerp meeneemt en gedurende de hele ondersteuningsperiode blijft waarborgen. Zo moet hij gedurende die periode kosteloos beveiligingsupdates beschikbaar stellen. Met een CE-markering toont hij vervolgens aan dat het product aan de eisen voldoet. Dat raakt fabrikanten, importeurs en distributeurs, maar ook afnemers: zij kunnen die CE-markering gebruiken als objectieve maatstaf binnen hun ketenrisicoanalyse onder NIS2 en de Cyberbeveiligingswet.

Bij het beheersen van cyberrisico's in de IT-keten gaat de aandacht al snel uit naar de organisatie waarmee zaken wordt gedaan. Hierbij spreken partijen af wie welke specificaties levert aan wie en onder welke voorwaarden dit gebeurt. Maar, minstens zo bepalend is het product zelf dat wordt geleverd en de keten hierachter. (Digitale) kwetsbaarheden liggen namelijk vaak al besloten in het product zelf of de onderdelen waaruit het product is opgebouwd. Denk hierbij aan oude (niet meer gepatchte) software op digitale apparaten, een IoT-apparaat met een (makkelijk) standaardwachtwoord, of firmware waarop geen updates worden uitgebracht. Grootschalige cyberincidenten van de afgelopen jaren laten zien dat één kwetsbare component in de toeleveringsketen van hard- en software voldoende kan zijn om duizenden organisaties tegelijk te raken. Waar de NIS2-richtlijn en de daaruit voortvloeiende Cyberbeveiligingswet (hierna: Cbw) organisaties verplichten hun keten te beheersen op IT-vlak, grijpt de CRA een ander fundamenteel probleem aan: digitale producten moeten in de basis veilig zijn. In dit artikel bespreken wij de kernverplichtingen, de gefaseerde inwerkingtreding, en hoe fabrikanten, importeurs, distributeurs én afnemers zich hierop nu al kunnen voorbereiden.

Productverantwoordelijkheid

Met de CRA introduceert de Europese Unie verplichte cybersecurity-eisen voor vrijwel alle hardware en software die op de Europese markt wordt gebracht.[3] Waar productwetgeving tot nu toe vooral zag op fysieke veiligheid (zoals de CE-markering voor elektrische apparaten), verplicht de CRA fabrikanten om cybersecurity vanaf de ontwerpfase mee te nemen en te blijven waarborgen. Dit is bijvoorbeeld direct relevant voor bedrijven die onder NIS2/Cbw vallen. De zorgplicht onder de Cbw verplicht hen bij hun ketenmaatregelen rekening te houden met de kwaliteit van de producten van hun leveranciers. Ook de wijze waarop die leveranciers hun producten ontwikkelen en onderhouden speelt daarbij een rol. De CRA normeert precies dat en geeft die beoordeling daarmee een gestandaardiseerd vertrekpunt.

Achtergrond van de Cyber Resilience Act

De CRA is op 10 december 2024 in werking getreden, maar wordt gefaseerd van toepassing.[4] Sinds 11 juni 2026 gelden de bepalingen over de aanmelding van conformiteitsbeoordelingsinstanties al en sinds 11 september 2026 geldt de meldplicht voor *actief uitgebuite kwetsbaarheden* in producten met digitale elementen. Een actief uitbuitbare kwetsbaarheid is een kwetsbaarheid die door een kwaadwillende partij in de praktijk daadwerkelijk kan worden misbruikt.[5] Vanaf 11 december 2027 is de verordening in haar geheel van toepassing, inclusief de essentiële eisen, de conformiteitsbeoordeling en de CE-markeringsplicht.[6] Voor producten die vóór 11 december 2027 al op de markt zijn gebracht, geldt de CRA in beginsel pas bij een ingrijpende wijziging van het product. De meldplichten gelden echter voor alle producten die op dat moment op de markt worden aangeboden.

Reikwijdte: wat is een 'product met digitale elementen'?
De CRA is van toepassing op elk hardware- of softwareproduct met digitale elementen dat een directe of indirecte logische of fysieke gegevensverbinding met een ander apparaat of netwerk heeft, en dat afzonderlijk op de markt wordt gebracht.[7] Dit is een ruim begrip: het omvat niet alleen 'klassieke' IoT-apparatuur zoals slimme thermostaten, routers en industriële sensoren, maar ook standalone software zoals ERP-systemen, mobiele apps, besturingssystemen en zelfs individuele softwarecomponenten of -bibliotheken die als zodanig worden gedistribueerd. Uitgezonderd zijn producten die al onder sectorspecifieke regelgeving vallen (zoals medische hulpmiddelen, motorvoertuigen en burgerluchtvaartapparatuur), producten die uitsluitend voor militaire of nationale veiligheidsdoeleinden zijn ontworpen, en niet-commerciële opensourcesoftware.[8]

De CRA onderscheidt drie risicocategorieën die bepalend zijn voor de zwaarte van de conformiteitsbeoordeling.

i. standaardproducten: hiertoe behoort het overgrote deel van de producten. De fabrikant mag hier in beginsel zelf verklaren dat aan de eisen wordt voldaan;
ii. belangrijke producten (Bijlage III): hieronder vallen onder meer browsers, routers, wachtwoordbeheerders, firewalls, VPN-software en identiteitsbeheersystemen. Deze producten zijn onderverdeeld in klasse I en klasse II;[9]
iii. kritieke producten (Bijlage IV): denk hierbij aan smartcards en beveiligingselementen, zoals de chip in een bankpas, identiteitskaart of UZI-pas of de gateway in de slimme meter thuis.[10]

Kernverplichtingen: essentiële eisen, kwetsbaarhedenbeheer en meldplicht

De CRA legt fabrikanten twee samenhangende sets essentiële vereisten op, uiteengezet in Bijlage I.[11] Het eerste deel van Bijlage I ziet op het product zelf en vereist onder meer dat het product:

i. zonder bekende, uitbuitbare kwetsbaarheden op de markt wordt gebracht;
ii. in een veilige standaardconfiguratie wordt geleverd;
iii. bescherming biedt tegen ongeautoriseerde toegang;
iv. de vertrouwelijkheid en integriteit van verwerkte gegevens waarborgt;
v. gegevensverwerking beperkt tot wat noodzakelijk is;
vi. bestand is tegen aanvallen op de beschikbaarheid (zoals DoS[12]);
vii. het aanvalsoppervlak minimaliseert;
viii. beveiligingsrelevante gebeurtenissen kan registreren; en
ix. gebruikers de mogelijkheid biedt om gegevens en instellingen veilig te verwijderen.

Het tweede deel van Bijlage I ziet op het proces: fabrikanten moeten gedurende de gehele ondersteuningsperiode van het product een effectief kwetsbaarhedenbeheer voeren.[13] Die periode stelt de fabrikant zelf vast: zij weerspiegelt de verwachte gebruiksduur van het product en bedraagt ten minste vijf jaar, tenzij die gebruiksduur van het product korter is. Dit beheer omvat onder meer het opstellen van een inventarisatie van softwarecomponenten (een zogeheten SBOM[14]), een beleid voor gecoördineerde kwetsbaarheidsopenbaarmaking[15], een duidelijk en toegankelijk contactpunt, en het kosteloos beschikbaar stellen van beveiligingsupdates gedurende de ondersteuningsperiode.

Daarnaast introduceert de CRA een strak tijdschema voor het melden van kwetsbaarheden en incidenten.[16] Zodra een fabrikant kennis krijgt van een actief uitgebuite kwetsbaarheid in zijn product, moet hij binnen 24 uur een vroegtijdige waarschuwing indienen bij het nationale CSIRT[17] en het Europese cybersecurityagentschap ENISA. Daarna volgt een uitgebreidere kennisgeving binnen 72 uur en – zodra corrigerende maatregelen beschikbaar zijn – een eindverslag, in beginsel binnen 14 dagen. Dit lijkt sterk op de meldplicht uit de Cbw. Vergelijkbare termijnen gelden voor ernstige incidenten die de veiligheid van het product raken. Deze meldingen verlopen via het door ENISA beheerde centrale meldplatform en gelden specifiek voor het product en niet voor de fabrikant zelf.

Voor importeurs en distributeurs gelden minder zware verplichtingen:

i. zij moeten verifiëren dat een product is voorzien van CE-markering en vergezeld gaat van de vereiste documentatie;
ii. zij mogen geen producten op de markt brengen bij gerede twijfel over de conformiteit; en
iii. zij zijn zelf verplicht kwetsbaarheden en nonconformiteit te melden.

Brengt een importeur een product onder eigen naam of merk op de markt, of wijzigt hij het product ingrijpend, dan wordt hij voor de toepassing van de CRA aangemerkt als fabrikant – met alle verplichtingen van dien.[18] Beheerders van opensourcesoftwareprojecten moeten weliswaar een kwetsbaarhedenbeleid voeren en actief geëxploiteerde kwetsbaarheden melden, maar worden niet met boetes geconfronteerd bij overtreding.[19]

Conformiteitsbeoordeling en CE-markering

Voordat een product met digitale elementen op de markt mag worden gebracht, moet de fabrikant een conformiteitsbeoordelingsprocedure doorlopen. Welke procedure geldt, hangt af van de categorie waarin het product valt.

i. standaardproducten: de fabrikant beoordeelt de conformiteit zelf, via een interne controle. Hij mag ook vrijwillig voor een zwaardere procedure kiezen.
ii. belangrijke producten (Bijlage III): voor klasse I mag de fabrikant volstaan met een interne controle op basis van geharmoniseerde normen. Zijn er geen geharmoniseerde normen of gaat het om een klasse II product, dan moet de beoordeling altijd plaatsvinden door een conformiteitsbeoordelingsinstantie.
iii. kritieke producten (Bijlage IV): deze producten moeten worden gecertificeerd volgens een geschikt certificatieschema onder de Cyber Security Act. Zo lang er nog geen geschikt schema bestaat, moet een kritiek product verplicht langs een conformiteitsbeoordelingsinstantie.

Na een positieve beoordeling stelt de fabrikant een EU-conformiteitsverklaring op en brengt hij de CE-markering aan. De bijbehorende technische documentatie moet gedurende de ondersteuningsperiode én ten minste tien jaar na het op de markt brengen van het product beschikbaar blijven voor de toezichthoudende autoriteit.[20] Hoewel het merendeel van de fabrikanten zelf mag certificeren, betekent dat niet dat de eisen voor hun producten lichter zijn: de bewijslast voor conformiteit ligt volledig bij de fabrikant. Een grondig, goed gedocumenteerde risicoanalyse en een gedegen testtraject zijn dus onmisbaar.

Toezicht en sancties

De Rijksinspectie Digitale Infrastructuur (RDI) houdt toezicht op de naleving van de CRA en geeft handvatten voor fabrikanten, importeurs en distributeurs van producten met digitale elementen in de online gids van het ministerie van Economische Zaken.[21]

De Nederlandse uitvoeringswetgeving – de Uitvoeringswet Verordening cyberweerbaarheid – is op het moment van schrijven nog in behandeling bij de Tweede Kamer, maar de bevoegdheden van de toezichthouder liggen in de verordening zelf al vast:

i. producten van de markt laten halen of terugroepen,
ii. corrigerende maatregelen opleggen; en
iii. als laatste remedie boetes opleggen. [22]

Deze boetes kunnen oplopen tot maximaal € 15 miljoen of 2,5% van de wereldwijde jaaromzet. Voor micro- en kleine ondernemingen geldt een soepeler regime, onder meer voor het missen van de 24-uurstermijn voor de vroegtijdige waarschuwing.[23]

De CRA als toetssteen voor NIS2-ketenrisicoanalyse

De CRA staat niet op zichzelf, maar sluit aan bij de ketenverplichtingen die vitale en belangrijke organisaties al dragen onder NIS2. Die richtlijn is in Nederland geïmplementeerd in de Cbw, die vanaf 15 augustus 2026 geldt.[24] De Cbw verplicht organisaties hun IT-leveranciers te beoordelen en passende beveiligingsmaatregelen contractueel af te dwingen. De CRA geeft daarvoor met de CE-markering en de bijbehorende conformiteitsverklaring een objectieve, wettelijk gestandaardiseerde maatstaf.

Een afnemer moet in zijn eigen ketenrisicoanalyse beoordelen of een softwareleverancier of hardwareproducent 'passende technische en organisatorische maatregelen' treft. Bij een CRA-conform, CE-gemarkeerd product kan hij daarbij in belangrijke mate steunen op die verklaring, in plaats van dit voor iedere leverancier afzonderlijk zelf vast te stellen en te onderbouwen.

Voor afnemers in vitale sectoren is daarbij ook de indeling in verschillende risicocategorieën relevant. Juist de producten waarvan zij voor hun eigen NIS2/Cbw-compliance afhankelijk zijn, vallen doorgaans in de zwaarste categorieën. Denk bijvoorbeeld aan een ziekenhuis dat voor de beveiliging van zijn netwerk gebruikmaakt van firewall- of VPN-software. Dat product valt onder de 'belangrijke producten' van Bijlage III (klasse I of II) en moet aan zwaardere CRA-eisen voldoen. Het ziekenhuis moet deze leverancier bovendien ook beoordelen als onderdeel van zijn eigen ketenrisicoanalyse onder NIS2/Cbw.

Praktische tips voor de praktijk

In de praktijk zien wij dat organisaties die tijdig met de CRA aan de slag gaan, dit vooral doen door hun contracten, inkoopprocessen en interne governance stap voor stap op de nieuwe norm af te stemmen. Voor kleinere organisaties die eerst hun basale cyberhygiëne op orde moeten brengen, biedt de subsidieregeling 'Mijn Cyberweerbare Zaak'[25] daarbij een steuntje in de rug.

Contracten: leg CRA-verplichtingen expliciet vast

IT-leveranciers die kwalificeren als fabrikant, importeur of distributeur doen er goed aan om nu al hun rol en risicoklasse per product te inventariseren, met bijzondere aandacht voor een SBOM en een beleid voor gecoördineerde kwetsbaarheidsopenbaarmaking.

Afnemers kunnen in nieuwe en te verlengen IT-contracten bepalingen opnemen over levering van een actuele SBOM, de ondersteuningsperiode, de meldtermijn bij kwetsbaarheden en incidenten, en een auditrecht op de CRA-conformiteit. Het is daarbij ook raadzaam aandacht te besteden aan aansprakelijkheid: bedingen die aansprakelijkheid voor kwetsbaarheden vrijwel volledig uitsluiten, verhouden zich lastig tot de dwingendrechtelijke zorgplicht van de CRA.

Organisatie: borg productveiligheid in inkoop en governance
Betrek inkoop, IT en juridische zaken vroegtijdig bij de selectie van nieuwe hard- en softwareproducten. Maak CE-markering en CRA-conformiteit daarnaast een vast onderdeel van de leveranciersbeoordeling, naast de bestaande ketenrisicoanalyse onder NIS2/Cbw.

Richt daarnaast een intern proces in om meldingen van leveranciers te ontvangen en te beoordelen. Zo kan een organisatie zo'n melding snel doorvertalen naar haar eigen meldplicht onder NIS2/Cbw. Fabrikanten doen er ten slotte goed aan hun directie of raad van bestuur actief te betrekken bij het kwetsbaarhedenbeleid en de ondersteuningsperiode. De duur van die periode en de inrichting van dat beleid bepalen namelijk mede hoelang en waarvoor de onderneming kan worden aangesproken.

Leveranciers en producten: verifieer conformiteit vóór aankoop
Vraag bij de aanschaf van producten met digitale elementen expliciet naar de risicoclassificatie, de beschikbare technische documentatie en de wijze waarop de fabrikant zijn meldplicht organiseert. Voor producten die (nog) niet onder de volledige CRA-verplichtingen vallen omdat zij vóór 11 december 2027 op de markt zijn gebracht, is het raadzaam om in de overeenkomst vast te leggen dat de leverancier zich inspant om, al dan niet vrijwillig, aan de essentiële eisen te voldoen. Dat geldt zeker wanneer het product wordt ingezet binnen een (zeer) kritieke sector onder NIS2/Cbw.

Passiviteit is ook hier het grootste risico: organisaties die nu investeren in productgerichte due diligence en heldere contractuele waarborgen, staan aanzienlijk sterker wanneer de CRA per 11 december 2027 volledig van toepassing wordt.

Subsidie 'Mijn Cyberweerbare Zaak'
Voor zzp'ers en mkb-bedrijven (tot 50 werknemers, met een jaaromzet van maximaal € 10 miljoen) is de subsidieregeling 'Mijn Cyberweerbare Zaak' relevant: deze vergoedt 50% van de kosten van acht basale cybermaatregelen – waaronder een wachtwoordmanager, MFA, patch-management, back-ups en een risico-inventarisatie – tot maximaal € 1.250 per aanvrager. De aanvraagperiode loopt van 7 september tot en met 30 november 2026, via de Rijksdienst voor Ondernemend Nederland en na het doorlopen van de CyberVeilig Check.[26]

Productveiligheid als nieuwe marktstandaard in de praktijk

Met de CRA verschuift de verantwoordelijkheid voor cyberveiligheid voor het eerst structureel naar het product zelf, als aanvulling op de organisatiegerichte verplichtingen van NIS2 en de Cbw. Voor fabrikanten, importeurs en distributeurs betekent dit een herziening van ontwikkel-, test- en supportprocessen; voor afnemers levert de CE-markering een objectieve maatstaf op waarmee zij hun eigen ketenrisicoanalyse kunnen onderbouwen.

Een deel van de CRA geldt op dit moment al. De volledige toepassing van de CRA volgt op 11 december 2027. Organisaties die hun contracten, inkoopprocessen en governance nu al op deze norm afstemmen, voorkomen dat zij op het laatste moment moeten improviseren.

Noten:

1. Advocaat bij Louwers IP&Tech Advocaten.
2. Advocaat en partner bij Louwers IP&Tech Advocaten.
3. Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen (Cyberweerbaarheidsverorde-ning/Cyber Resilience Act), PbEU 2024, L, 20 november 2024.
4. Artikel 71 CRA; RDI, "Inwerkingtreding Cyber Resilience Act: een nieuw tijdperk van productveiligheid", rdi.nl.
5. Artikel 3, punt 42 CRA.
6. Artikel 71 lid 2 CRA.
7. Artikel 2 lid 1 en artikel 3 sub 1 CRA.
8. Artikel 2 lid 6 en lid 7 CRA.
9. Artikel 7 en Bijlage III CRA. Een aangemelde instantie is en onafhankelijke organisatie die door een nationale autoriteit (in Nederland: de RDI) is aangewezen om namens fabrikanten te toetsen en certificeren dat een product aan de verplichte CRA-eisen voldoet.
10. Artikel 8 en Bijlage IV CRA.
11. Artikel 6 en Bijlage I CRA.
12. Bij een DoS-aanval wordt een product doelbewust overspoeld met verkeer, waardoor het niet meer bereikbaar is voor legitieme gebruikers; bij een DDoS-aanval gebeurt dit vanaf veel computers tegelijk.
13. Artikel 13 CRA en Bijlage I CRA.
14. Een SBOM (software bill of materials) is een gestructureerde, machineleesbare inventarisatie van alle – ook open source – softwarecomponenten in een product, vergelijkbaar met een ingrediëntenlijst, waarmee bekende kwetsbaarheden in die componenten kunnen worden getraceerd.
15. Hierbij meldt een onderzoeker een ontdekte kwetsbaarheid eerst vertrouwelijk aan de fabrikant, die de gelegenheid krijgt een oplossing te ontwikkelen voordat de kwetsbaarheid openbaar wordt gemaakt.
16. Artikel 14 CRA.
17. De nationale instantie – in Nederland het NCSC – die meldingen van kwetsbaarheden en incidenten ontvangt en de afhandeling daarvan coördineert.
18. Artikel 19, artikel 20 en artikel 21 CRA.
19. Artikel 24 en artikel 64 lid 10 CRA.
20. Artikel 28, artikel 29, artikel 30, artikel 31 en Bijlage VII CRA.
21. RDI, Gids Cyber Resilience Act, rdi.nl.
22. Wetsvoorstel Uitvoeringswet Verordening cyberweerbaarheid, aanhangig bij de Tweede Kamer sinds november 2025 (*Kamerstukken II* 2025/26, 36875, nr. 2); Hoofdstuk V, artikel 52-60 CRA.
23. Artikel 64 CRA.
24. Artikel 21 Cbw; Rijksoverheid, "Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten vanaf 15 augustus 2026 van kracht", rijksoverheid.nl.
25. https://www.rvo.nl/subsidies-financiering/mcz
26. NCSC, "Subsidieregeling Mijn Cyberweerbare Zaak", ncsc.nl/subsidie.