SECURE
Cyber Resilience for SMEs

# De essentiële cybersecuritysvereisten van de CRA: Bijlage I, Deel I

20/10/2025

Funded by the European Union

EU-financieringsverklaring: Gefinancierd door de Europese Unie onder Grant Agreement nr. 101190325. De geuite standpunten en meningen zijn echter uitsluitend die van de auteur(s) en geven niet noodzakelijkerwijs de standpunten en meningen van de Europese Unie of het European Cybersecurity Industrial, Technology and Research Competence Centre weer. Noch de Europese Unie, noch de subsidieverstrekkende instantie kan hiervoor verantwoordelijk worden gehouden.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ECCC-disclaimer: Het project wordt ondersteund door het European Cybersecurity Competence Centre en zijn leden.

## DISCLAIMER



Dit document maakt deel uit van Deliverable D4.1 'Guidelines and Materials for SMEs CRA Compliance' van het SECURE-project.

Dit document is een vertaalde versie van de oorspronkelijk Engelstalige richtlijn. Afkortingen worden in het Engels behouden, zoals terug te vinden in de lijst met Afkortingen.

Eerste auteur: *Centrum voor Cybersecurity België (CCB)*

Tweede auteur: *Autoritatea Pentru Digitalizarea Romaniei-NCC-RO (ADR-NCC-RO)*

# Inhoudstafel

# Lijst met Tabellen en Figuren

# Afkortingen

**API** – Application Programming Interface

**APT** – Geavanceerde persistente bedreigingen (Advanced Persistent Threats)

**BSIMM** – Building Security in Maturity Model

**CI/CD** – Continue integratie en continue levering/implementatie (Continuous Integrations and Delivery/Deployment)

**CRA** – Cyber Resilience Act

**CVD** – Gecoördineerde openbaarmaking van kwetsbaarheden (Coordinated Vulnerability Disclosure)

**CVE** – Gemeenschappelijke kwetsbaarheden en blootstellingen (Common Vulnerabilities and Exposures)

**CVSS** – Gemeenschappelijk kwetsbaarheidsscoresysteem (Common Vulnerability Scoring System)

**DAST** – Dynamic Application Security Testing

**DoS** – Denial of Service

**DREAD** – Damage, Reproducibility, Exploitability, Affected Users, and Discoverability

**ENISA** – Agentschap van de Europese Unie voor Cyberbeveiliging

**EOL** – End of Life

**EPSS** – Exploit Prediction Scoring System

**ETSI** – European Technical Standards Institute

**EU** – Europese Unie

**FIRST VCMM** – FIRST Vulnerability Coordination Maturity Model

**GDPR/AVG** – Algemene verordening gegevensbescherming

**HTTPS/TLS** – Hyper Text Protocol Secure/Transport Layer Security

**ICS** – Industrieel controlesysteem (Industrail Control System)

**IEC** – International Electrotechnical Commission

**IoT** – Internet of Things

**IPSec** – Internet Protocol Security

**ISO** – International Standards Organisation

**JTAG** – Joint Test Action Group

**KMO** – Kleine en Middelgrote Onderneming

**LINDDUN** – Linking, Identifying, Non-repudiation, Detecting, Data Disclosure, Unawareness and Non-compliance

**MFA** – Multi-factor authenticatie

**MITRE ATT&CK** – Adversarial Tactics, Techniques and Common Knowledge

**MQTT** – Message Queuing Telemetry Transport

**NIST** – National Institute of Standards and Technology (Verenigde Staten)

**NIST SSDF** – NIST Secure Software Development Framework

**NTIA** – National Telecommunications and Information Administration (Verenigde Staten)

**OPENSSF VEX** – Open-Source Security Foundation Vulnerability Exploitability eXchange

**OS** – Besturingssysteem (Operating System)

**OTA** – Over The Air

**OWASP** – Open Worldwide Application Security Project

**OWASP ASVS** – OWASP Application Security Verification Standard

**OWASP SAMM** – OWASP Software Assurance Maturity Model

**PDE** – Product met digitale elementen

**PSIRT** – Product Security Incident Response Team

**SAST** – Static Application Security Testing

**SBOM** – Software Bill of Materials

**SCA** – Software Composition Analysis

**SIEM** – Security Information and Event Management

**SOC** – Security Operations Centre

**SQL** – Structured Query Language

**SSDLC** – Secure Software Development Lifecycle

**SSL** – Secure Sockets Layer

**STRIDE** – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

**TPM** – Trusted Platform Module

**UART** – Universal Asynchronous Receiver-Transmitter

**USB** – Universal Serial Bus

**VPN** – Virtual Private Network

# *Inleiding*

Om te voldoen aan de **Cyber Resilience Act** (CRA), Verordening (EU) 2024/2847, legt de CRA aan fabrikanten een groot aantal eisen en verplichtingen op. Een van de belangrijkste vereisten is dat je ervoor moet zorgen dat het product met digitale elementen (PDE) dat je op de markt brengt, "is ontworpen, ontwikkeld en geproduceerd overeenkomstig de essentiële cyberbeveiligingsvereisten van deel I van bijlage I"[1] . Bijlage I bestaat uit twee delen: deel I richt zich op cyberbeveiligingseisen met betrekking tot de eigenschappen van het product en deel II behandelt eisen met betrekking tot de respons op kwetsbaarheden. Deel I bestaat verder uit twee punten, waarvan het eerste bepaalt dat

> *"Producten met digitale elementen worden zodanig ontworpen, ontwikkeld en geproduceerd dat zij een passend cyberbeveiligingsniveau op basis van de risico's garanderen"*[2] .

Punt 2 specificeert de vereisten waaraan uw producten moeten voldoen.

Deze richtlijn, die is ontwikkeld in het kader van **het SECURE-project**[3] met als doel **micro-, kleine en middelgrote ondernemingen (kmo's)** te **ondersteunen**, gaat dieper in op beide punten van bijlage I, deel I, en biedt **niet-uitputtende praktische en technische suggesties, voorbeelden en benaderingen om je te helpen bij het naleven van elke vereiste**. Het is belangrijk op te merken dat elke verwijzing naar bestaande normen, instrumenten en kaders louter **suggestief** is en bedoeld is om de CRA-vereisten zo concreet mogelijk te maken. De aanbevelingen zijn gebaseerd op erkende beste praktijken en gangbare benaderingen. De richtlijn zal worden bijgewerkt naarmate de ontwikkeling van specifieke CRA-normen en uitvoeringsmaatregelen van de Europese Commissie vordert tijdens de aanpassingsperiode van 2024 tot 2027.

[1] Art. 13, lid 1, CRA.

[2] Bijlage I, deel I, lid 1, CRA.

[3] Het project "Strengthening EU SMEs Cyber Resilience" (SECURE) biedt financiële steun en begeleiding aan kmo's om te voldoen aan de CRA.



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

# De essentiële cyberbeveiligingsvereisten van de CRA: Bijlage I, Deel I

## 1. Risicogebaseerde cyberbeveiligingsaanpak

Punt 1 van bijlage I, deel I bepaalt dat

> *"Producten met digitale elementen worden zodanig ontworpen, ontwikkeld en geproduceerd dat zij een **passend cyberbeveiligingsniveau op basis van de risico's** garanderen"*[4] .

Dit punt staat centraal in de CRA en is gebaseerd op het principe van "security by design and by default". In wezen betekent dit dat je een **risicogebaseerde cyberbeveiligingsaanpak** voor je product moet ontwikkelen. Deze risicogebaseerde aanpak moet verdedigbaar, gedocumenteerd en evenredig zijn. Beschouw CRA-naleving als een "traceerbaar traject":

productcontext → risico → controles → bewijs

De aanpak voor dit traject moet zorgvuldig worden gedocumenteerd in de verplichte technische documentatie[5] , die cruciaal is voor naleving en controleerbaarheid.

Concreet moeten fabrikanten:

1. De cyberbeveiligingsrisico's van de PDE gedurende de hele levenscyclus beoordelen;
2. Beveiligingsmaatregelen afstemmen op het risiconiveau (bijvoorbeeld een slimme thermostaat versus een industrieel controlesysteem);
3. Rekening houden met dreigingsmodellen, aanvalsoppervlakken en mogelijke gevolgen voor gebruikers en systemen.

Een cruciale eerste stap in de naleving van de CRA is dus het uitvoeren van een **risicobeoordeling** voor jouw PDE. In dit hoofdstuk wordt dieper ingegaan op hoe je een dergelijke risicobeoordeling kunt uitvoeren door mogelijke benaderingen uiteen te zetten en technische suggesties te doen.

Voordat we in detail treden, volgt hieronder een overzicht **met de basisprincipes van risicobeoordelingen** om je geheugen op te frissen. Onderdelen ervan komen in meer detail terug in het eerste hoofdstuk van deze richtlijn, dat je wordt aangeraden te raadplegen. Eerst wordt in de vereenvoudigde samenvatting echter uiteengezet hoe risicobeoordelingen over het algemeen worden aangepakt[6] .

[4] Bijlage I, deel I, punt 1, CRA.

[5] Art. 31, CRA.

[6] Het is van cruciaal belang op te merken dat de Europese Commissie nog officiële richtlijnen moet opstellen voor de uitvoering van de risicobeoordeling voor de CRA. De hier gegeven aanbevelingen vatten de belangrijkste stappen van elke risicobeoordelingsaanpak samen. Een andere aanpak, norm of methodologie kan worden gebruikt, mits deze in overeenstemming is met de gerapporteerde aanpak.



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

## Risicobeoordeling 101

Bij het uitvoeren van een risicobeoordeling kunnen **zes stappen** worden toegepast:

1) Identificatie van **assets** en **bedreigingen** = *identificeer elke asset (wat moet worden beschermd) op basis van de blootstelling aan een bedreiging (wat kan er misgaan);*
2) Beoordeling van **kwetsbaarheden** = *evalueer de kwetsbaarheden*;
3) Overweging en evaluatie van **impact** en **waarschijnlijkheid** = *breng de impact en waarschijnlijkheid van kwetsbaarheden in kaart → dit resulteert in specifieke 'risico's'*;
4) **Risicoanalyse** en **aanvaardbaarheid** = *breng elk risico in kaart en overweeg je aanvaardbaarheidsniveau/risicotolerantie om prioriteiten te stellen voor je acties;*

Naast deze risicobeoordeling zijn er nog twee laatste stappen:

5) Implementatie van **risicobeperkende maatregelen** = *selecteer en pas beveiligingsmaatregelen toe voor elk risico;*
6) Monitoring en herbeoordeling = *monitor de bedreigingen en risico's tijdens elke fase van de levenscyclus van de PDE en houd de risicobeoordeling up-to-date.*

Voor **stap één tot en met drie** kan je een **matrix** ontwikkelen waarmee elke dreiging, kwetsbaarheid en impact geclassificeerd kan worden op basis van een bepaald risiconiveau en een bepaalde score. Om dit te doen, moet je eerst definiëren wat elk niveau (en elke score) voor jou betekent aan de hand van beschrijvende tabellen[7] .

- Laag
- Laag-gemiddeld
- Gemiddled
- Matig-gemiddeld
- Hoog

Tabel 1 :
Voorbeeldmatrix

| Risico/bedreiging | Bedreiging 1 | Bedreiging 2 | Score |
|---|---|---|---|
| Hoog | | | 10 |
| Gemiddeld-hoog | | | |
| Gemiddeld | | | |
| Laag-gemiddeld | | | |
| Laag | | | 0 |

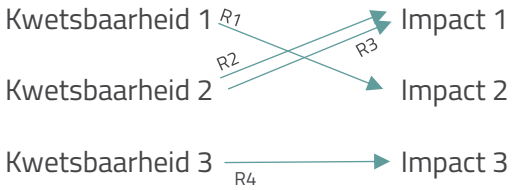
[7] Een "Laag" dreigingsniveau kan bijvoorbeeld een bedreiging zijn die eens in de tien jaar kan voorkomen, terwijl "Hoog" een bedreiging kan zijn die één keer per week kan voorkomen. Je hebt afzonderlijke tabellen nodig voor het beschrijven van bedreigingen, kwetsbaarheden en gevolgen, en risico's – deze laatste ondersteunen de definitie van jouw aanvaardbaarheidsniveau.



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

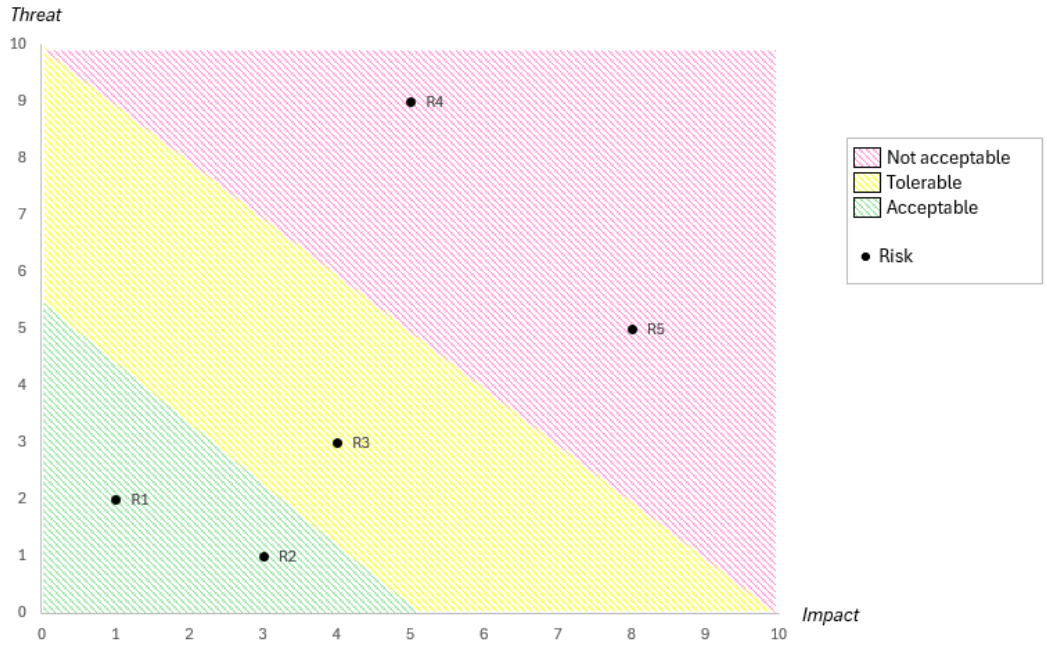
Door de kwetsbaarheden te koppelen aan hun impact kan je vervolgens de verschillende risico's (R) visualiseren:

Figuur 1 :
Visualisatie van risico's




Voor **stap vier** is het belangrijk om de ondervonden risico's in kaart te brengen en je aanvaardbaarheidsniveau of tolerantie voor deze risico's te definiëren. Dit gebeurt vaak aan de hand van kleuren, bijvoorbeeld:

Afbeelding 2 :
Risicotolerantiegrafiek




Op deze manier kan je prioriteiten stellen en voor elk risico risicobeperkende maatregelen en beveiligingscontroles ontwikkelen om de ze tot een aanvaardbaar niveau te beperken.

Zoals eerder vermeld, worden deze elementen van de risicobeoordeling hieronder (hoofdstuk 1 van deze richtlijn) meer in detail behandeld aan de hand van voorbeelden en aanbevolen hulpmiddelen en kaders om je te ondersteunen.

## 1.1. Cybersecurity Risicobeoordeling gedurende een Levenscyclus

Aangezien de cyberbeveiligingsrisico's van je PDE gedurende de hele levenscyclus van het product moeten worden beoordeeld, houdt het uitvoeren van een **risicobeoordeling** in dat



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

**cyberbeveiligingsrisico's** in elke fase van de levenscyclus van een product **worden geïdentificeerd, geanalyseerd en beperkt**:

1. Ontwerp
2. Ontwikkeling
3. Productie
4. Implementatie
5. Gebruik en onderhoud
6. End-of-Life (EOL)

De risicobeoordeling moet voortdurend worden bijgewerkt gedurende de 'ondersteuningsperiode'[8], een periode van ten minste vijf jaar (of, indien de levensduur van het product korter is dan vijf jaar, ten minste tot het einde van de levensduur van het product).

### 1.1.1. Belangrijkste Stappen in de Risicobeoordeling

Bij het uitvoeren van de risicobeoordeling kunnen zes stappen worden overwogen, die elk worden toegelicht in tabel 2 hieronder.

Tabel 2 :
Belangrijkste stappen in de risicobeoordeling

| Belangrijke stap | Toelichting en suggesties |
|---|---|
| **1. Identificeer Assets en Bedreigingen** | Maak een onderscheid tussen:<br>• Assets: wat moet worden beschermd?<br>Bijvoorbeeld firmware, gebruikersgegevens, communicatiekanalen.<br>• Bedreigingen: wat kan er misgaan?<br>Bijvoorbeeld: malware injection, ongeoorloofde toegang. |
| **2. Analyseer Kwetsbaarheden** | Gebruik tools zoals:<br>• Statische codeanalyse; |

[8] Art. 13, lid 8, CRA: De ondersteuningsperiode wordt bepaald door de fabrikant, rekening houdend met de verwachte gebruiksduur van het product, de verwachtingen van de gebruiker, de aard (het beoogde doel) van het product en het recht van de Unie.


Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

| | |
|---|---|
| | • Software composition analysis (SCA);<br>• Penetratietesten;<br>• Bedreigingsmodellering[9] (bijv. STRIDE, DREAD).<br>Opmerking: CVSS en STRIDE kunnen samen worden gebruikt in een dreigingsmodelleringsproces. STRIDE kan helpen bij het identificeren van potentiële dreigingen, waarna CVSS kan worden gebruikt om de ernst van kwetsbaarheden in verband met die dreigingen te beoordelen, waardoor beter prioriteiten kunnen worden gesteld bij het nemen van maatregelen om de risico's te beperken[10] . |
| **3. Evalueer de impact en waarschijnlijkheid van risico's** | Gebruik een risicomatrix om prioriteiten te stellen op basis van:<br>• Impact (bijv. datalek, systeemstoring);<br>• Waarschijnlijkheid (bijv. bekende kwetsbaarheid, aanvalsoppervlak). |
| **4. Analyseer de risico's en hun aanvaardbaarheid** | Bepaal jouw aanvaarbaarheidsniveau en breng de risico's in kaart op basis van de dreiging en impact om je acties te classificeren en prioriteiten te stellen. |
| **5. Implementeer risicobeperkende maatregelen** | Pas beveiligingsmaatregelen toe:<br>bijv. versleuteling, authenticatie, beveiligd opstarten. |
| **6. Monitor en herbeoordeel** | Controleer voortdurend op nieuwe bedreigingen en werk risicobeoordelingen overeenkomstig bij. |

[9] Bedreigingsmodellering wordt verder besproken in punt 1.3.1.

[10] CVSS beoordeelt de ernst van kwetsbaarheden, terwijl risico's ook rekening houden met de impact op het bedrijf en de waarschijnlijkheid.



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

### 1.1.2. Use Cases per Levenscyclusfase

Om de risicobeoordeling concreter te maken, biedt tabel 3 hieronder een overzicht van 'use cases' (scenario's), inclusief een voorbeeld van een risico en een risicobeperkende strategie, per levenscyclusfase.

Tabel 3 :
Use Cases per levenscyclusfase

| Levenscyclusfase | Use Case | Risico | Beperking |
|---|---|---|---|
| **Ontwerp** | Slimme camera | Ongeautoriseerde toegang tot videobeelden | Implementeer end-to-end-encryptie en veilige standaardinstellingen |
| **Ontwikkeling** | Apparaatfirmware | Kwetsbaarheid voor bufferoverloop | Gebruik veilige coderingspraktijken en geautomatiseerde kwetsbaarheidsscans |
| **Productie** | Industriële IoT-gateway | Compromittering tijdens productie | Beveiligde toeleveringsketen en hardware root of trust, verzegeling tegen manipulatie en veilige provisioning |
| **Implementatie** | Consumentenrouter | Standaard inloggegevens blijven ongewijzigd | Wachtwoordwijziging afdwingen bij eerste gebruik |
| **Gebruik en onderhoud** | Verbonden voertuig | Niet-gepatchte softwarekwetsbaarheden | OTA-updates (Over-The-Air) met integriteitscontroles |
| **End of life** | Slimme thermostaat | Achtergelaten apparaat met kwetsbare firmware | Zorg voor veilige instructies voor buitengebruikstelling en gegevenswissing, een beleid voor beveiligingsupdates bij |

| | | | |
|---|---|---|---|
| | | | end-of-life en gegevensexport voor gebruikers |

### 1.1.3. Hulpmiddelen en Kaders om je te Ondersteunen

De onderstaande lijst bevat een aantal tools en kaders die ondersteuning kunnen bieden, hoewel een meer uitgebreide lijst en geharmoniseerde normen nog in ontwikkeling zijn.

- ISO/IEC 27005 – Risicobeheer
- NIST SP 800-30 – Methodologie voor risicobeoordeling
- ENISA Threat Landscape – Geüpdatet dreigingsinformatie
- OWASP ASVS – Verificatie van applicatiebeveiliging
- STRIDE model
- DREAD model
- LINDDUN
- CVSS

## 1.2. Beveiligingsmaatregelen op Maat

De tweede onderdeel van een risicogebaseerde cyberbeveiligingsaanpak is het afstemmen van beveiligingsmaatregelen op het risiconiveau. Deze afstemming moet in verhouding staan tot de risico's die zijn geïdentificeerd in bijlage I, deel I, punt 1. Laten we uitleggen wat dit betekent aan de hand van zes duidelijke stappen, principes en twee voorbeeldproducten: een slimme thermostaat (laag tot matig risico) en een industrieel controlesysteem (ICS) (hoog risico).

### 1.2.1. Voer een Risicoclassificatie van het Product uit

Bij het uitvoeren van een product-specifieke risicobeoordeling is het belangrijk om rekening te houden met de volgende dimensies.

- **Blootstelling aan bedreigingen**: Is het product
  - Verbonden met het internet?
  - Op grote schaal inzetbaar?


Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Openbaar toegankelijk?
- Beoogd gebruik versus redelijkerwijs te verwachten misbruik?

- **Gevolgen van compromittering**: Wat zouden de gevolgen zijn voor de veiligheid, financiële verliezen, privacy en kritieke infrastructuur?
- **Aantrekkelijkheid van een aanval:** zou het een opstapje zijn voor laterale bewegingen?
- **Gebruikersprofiel:** consument, kmo, exploitant van kritieke infrastructuur?

Op basis van deze overwegingen kan het product worden geclassificeerd als laag risico - aanvaardbaar, matig risico – te tolereren, of hoog risico - onaanvaardbaar[11] .

### 1.2.2. Beveiligingsdoelstellingen per Risiconiveau Definiëren

Tabel 4 illustreert hoe de beveiligingsdoelstellingen vervolgens kunnen worden afgestemd op het eerder vastgestelde risiconiveau van het product.

Tabel 4 :
Beveiligingsdoelstellingen per risiconiveau

| Risiconiveau | Beveiligingsdoelstellingen |
|---|---|
| **Laag (bijv. slimme thermostaat)** | • Triviaal misbruik voorkomen;<br>• Privacy waarborgen;<br>• Updatevermogen behouden. |
| **Gemiddeld** | • Detecteer en beperk bekende aanvalsvectoren;<br>• Authenticatie afdwingen;<br>• Beveilig de communicatie. |
| **Hoog (bijv. ICS)** | • Versterkte beveiliging;<br>• Defence-in-depth;<br>• Vertrouwen in de toeleveringsketen;<br>• Beveiligd opstarten; |

[11] Dit vereist dat je vooraf definieert hoe je deze elementen met behulp van een matrix scoort en hoe de scores overeenkomen met risiconiveaus. Voor een nauwkeurigere classificatie kunnen vijf in plaats van drie risiconiveaus worden overwogen: laag, gemiddeld-laag, gemiddeld, gemiddeld-hoog en hoog risico.

| | |
|---|---|
| | • Incidentmonitoring. |

### 1.2.3. CRA Essentiële Vereisten Toewijzen aan het Risiconiveau

Afhankelijk van het risiconiveau kunnen de essentiële CRA-vereisten verschillende praktische toepassingen hebben. Tabel 5 illustreert dit voor lage en hoge risiconiveaus en de respectievelijke voorbeeldproducten, slimme thermostaat en ICS.

Tabel 5 :
Essentiële CRA-vereisten per risiconiveau

| CRA-vereiste | Laag risico | Hoog risico |
|---|---|---|
| **Secure-by-Design en Default** | Debug-poorten uitschakelen; sterke standaardinstellingen | Volledige Software Bill of Materials (SBOM[12] ); beveiligd opstarten; versterkt besturingssysteem |
| **Respons op kwetsbaarheden** | Openbaar CVD-beleid; security.txt; inbox monitoren; patchmechanisme | Bekendmaking van kwetsbaarheden (CVD); PSIRT; rapid response |
| **Logging en monitoring** | Logs van local events | Logregistratie op afstand; SIEM-integratie |
| **Toegangscontrole** | Pin- of app-authenticatie | Role-based access; MFA; toegang met minimale privileges |
| **Update-mechanisme** | OTA-updates met toestemming van de gebruiker | Ondertekende updates; fail-safe rollback |
| **Bescherming tegen ongeoorloofde toegang** | Basisregels voor firewall | Host intrusion detectiesystemen; firmware-integriteitscontroles |

[12] SBOM wordt verder toegelicht in paragraaf 4.1.

### 1.2.4. Bedreigingsmodellering om Maatregelen te Verfijnen

Voor dreigingsmodellering kunnen STRIDE, LINDDUN of aanvalsbomen worden toegepast om de adequaatheid van controles te valideren.

Voor de voorbeeldproducten betekent dit:

- **Slimme thermostaat**: focus op Spoofing, Tampering en Denial of Service;
- **ICS**: alle STRIDE-bedreigingen en geavanceerde aanhoudende bedreigingen (APT's) dekken.

### 1.2.5. Selecteer Controles per Risiconiveau

Tabel 6 suggereert verschillende controles per beveiligingsdomein voor de voorbeeldcases, slimme thermostaat (laag risico) en ICS (hoog risico).

Tabel 6 :
Controles per risiconiveau

| Beveiligingsdomein | Laag risico | Hoog risico |
|---|---|---|
| **Authenticatie** | App-gebaseerde authenticatie; standaard wachtwoordwijziging | MFA; toegangscontrole met certificaten |
| **Firmwarebeveiliging** | Ondertekende firmware; OTA-updates; fail-safe rollback | Beveiligd opstarten; TPM-integratie; supply chain garantie |
| **Communicatie** | HTTPS/TLS | VPN's; IPSec; netwerksegmentatie; zero trust |
| **Monitoring** | Basis logrotatie | Realtime logregistratie; detectie van afwijkingen; SOC-integratie; tijdsgevoelige logs |
| **Gebruikersinterface** | Eenvoudig instellingenpaneel | Gedetailleerde beheerconsole; auditspoor |

### 1.2.6. Bewijs van Naleving

Zoals eerder vermeld, is een belangrijk element voor naleving van de CRA het documenteren van minimaal het volgende bewijs:

- Redenering achter risicoclassificatie;

- Controlebeslissingen gekoppeld aan risico's;
- Test- en validatieresultaten;
- Beleid voor updates en de respons op kwetsbaarheden;
- Afstemming op secure development lifecycle (bijv. ISO/IEC 27034, IEC 62443-4-1);
- Traceerbaarheidsmatrix waarin risico's → controles → verificatietests → bewijs worden weergegeven (te bewaren in Technische Documentatie)

### 1.2.7. Voorbeelden

Tabel 7 bevat aanvullende voorbeelden van implementatiemaatregelen voor de voorbeelden met een laag en hoog risico.

Tabel 7 :
Implementatiemaatregelen per risiconiveau

| Product | Slimme thermostaat | ICS |
|---|---|---|
| **Risico-overwegingen** | • Verbonden met internet, regelt de verwarming in particuliere woningen;<br>• Privacygevoelig, maar geringe veiligheids- of economische impact. | • Wordt gebruikt in kritieke infrastructuur (bijv. waterzuivering);<br>• Grote impact op veiligheid en bedrijfsvoering. |
| **Risicoclassificatie** | Laag risico | Hoog risico |

| | | |
|---|---|---|
| **Implementatiemaatregelen** | • Wijzig het standaardwachtwoord bij het eerste gebruik;<br>• HTTPS-communicatie met back-end;<br>• Ondertekende firmware-updates;<br>• Alleen lokale logregistratie[13] ;<br>• Contactformulier voor basis kwetsbaarheden. | • Secure-by-design hardware met TPM;<br>• Beveiligd opstarten en ondertekende updates met rollback;<br>• Role-based access en MFA;<br>• Netwerksegmentatie en firewallregels;<br>• Logging naar centrale SIEM;<br>• Volledige SBOM bij elke update;<br>• Gecoördineerd proces voor het bekendmaken van kwetsbaarheden (CVD). |

## 1.3. Rekening houden met Dreigingsmodellen, Aanvalsoppervlakken en mogelijke Impact op Gebruikers en Systemen

De CRA benadrukt een risicogebaseerde benadering van cyberbeveiliging. Zoals hierboven aangegeven, betekent dit dat fabrikanten hun beveiligingsmaatregelen moeten afstemmen op realistische bedreigingen, blootstellingspunten en mogelijke gevolgen voor gebruikers en systemen. Dit is geen loze richtlijn, maar een oproep tot een onderbouwde, contextbewuste aanpak. Om deze verplichting effectief te implementeren, moeten drie belangrijke concepten samen worden bekeken: dreigingsmodellen, aanvalsoppervlakken en impactanalyse, die samen de derde en laatste dimensie van de risicogebaseerde cyberbeveiligingsaanpak vormen. Laten we deze elementen een voor een bekijken en zien hoe ze in elkaar passen.

[13] Let op: alleen lokale logs verminderen de forensische waarde; optionele export met toestemming van de gebruiker wordt aanbevolen.

### 1.3.1. Bedreigingsmodellen: wie valt aan, waarom en hoe?

Bedreigingsmodellering is een gestructureerd proces waarbij je vaststelt wie je product zou kunnen aanvallen, hoe ze dat zouden doen en wat hun motivatie is. Denk aan script kiddies, georganiseerde cybercriminelen of zelfs staatsactoren. Hun motieven variëren van financieel gewin tot sabotage of spionage, en hun vaardigheden variëren van basisniveau tot geavanceerd.

Om dit te structureren, kan je methoden gebruiken zoals:

- STRIDE;
- MITRE ATT&CK voor gekende aanvalstechnieken;
- LINDDUN voor privacygerichte bedreigingen;
- Aanvalsbomen of Cyber Kill Chains om aanvalsroutes in kaart te brengen.

Terugkomend op de praktische voorbeelden betekent dit:

- **Slimme thermostaat**: bedreigingen zijn vaak beperkt tot nieuwsgierige buren of willekeurige aanvallen, waarbij iemand de temperatuurinstellingen of het energieverbruik zou kunnen manipuleren;
- **ICS** (bijvoorbeeld in een waterzuiveringsinstallatie): bedreigingen zijn fundamenteel anders - bijvoorbeeld APT-groepen of ransomwarebendes die fysieke processen proberen te saboteren of een bedrijf stil te leggen.

Het resultaat van dreigingsmodellering is een duidelijke lijst met beveiligingsdoelstellingen die specifiek zijn voor het product en de omgeving ervan.

### 1.3.2 Aanvalsoppervlakken: waar kan een aanvaller binnenkomen?

Een aanvalsoppervlak is het totaal van alle punten waarop een aanvaller kan communiceren met, of invloed kan uitoefenen op, het systeem. Hoe meer interfaces en toegangspunten, hoe groter het risico.

Typische aanvalsoppervlakken zijn:

- Netwerkinterfaces zoals Wi-Fi, Bluetooth, MQTT of HTTP;
- Lokale interfaces zoals USB, UART, JTAG (voor foutopsporing);
- Update-mechanismen zoals OTA- of USB-updates;
- API's, mobiele apps, cloud dashboards;
- Externe componenten uit de toeleveringsketen.

Bij het analyseren van deze oppervlakken moet worden gecontroleerd welke componenten onnodig blootgesteld zijn, welke diensten onnodig ingeschakeld zijn en of de toegang voldoende beveiligd is. Idealiter beperk je het aanvalsoppervlak door:

- Beveiligingsprincipes zoals minimale blootstelling, veilige standaardinstellingen en hardening;
- Het uitschakelen van ongebruikte poorten of diensten;
- Authenticatie en versleuteling bij elke interface.

Toegepast op de voorbeelden betekent dit:

- **Slimme thermostaat**: maakt doorgaans gebruik van Wi-Fi en mogelijk Bluetooth, met een eenvoudige cloudverbinding – Debug interfaces kunnen tijdens het testen openstaan en moeten in productie worden gedeactiveerd;
- **ICS-gateway**: wordt fysiek beschermd, met afgeschermde USB-updates, gesegmenteerde netwerken en geen externe interfaces.

Het zorgvuldig in kaart brengen van het aanvalsoppervlak is essentieel om te weten waar beveiliging echt nodig is.

### 1.3.3 Impactanalyse: wat gebeurt er als er iets misgaat?

De laatste stap is het bepalen van de potentiële impact van een succesvolle aanval. De CRA vereist dat beveiligingsmaatregelen in verhouding staan tot deze impact. Dit omvat niet alleen technische schade, maar ook:

- Gevaren voor de gebruiker (bijv. letsel als gevolg van temperatuurregeling);
- Schending van de privacy (bijv. het afleiden van leefpatronen uit thermostaatgegevens);
- Verlies van beschikbaarheid of bedrijfscontinuïteit (bijv. fabriekssluiting);
- Wettelijke aansprakelijkheid (bijv. schending van de CRA of AVG);
- Reputatieschade en marktrisico.

De impact moet vanuit meerdere dimensies worden bekeken:

- Gebruiker: van klein ongemak tot levensbedreigende situaties;
- Organisatie: van verhoogde werkdruk voor de helpdesk tot bedrijfsonderbreking;
- Maatschappij: van onschuldige bugs tot bedreigingen voor kritieke infrastructuur.


Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Ook hier is evenredigheid van cruciaal belang: een speelgoedrobot vereist niet hetzelfde beveiligingsniveau als een medische pomp.

### 1.3.4 Integratie: van analyse tot maatregelen

Wanneer deze drie bouwstenen – dreigingsmodel, aanvalsoppervlak en impact – samenkomen, ontstaat een solide basis voor het op maat maken van beveiligingsmaatregelen.

Een typische aanpak ziet er als volgt uit:

1. Definieer het gebruik en de context van het product;
2. Voer een dreigingsmodellering uit om inzicht te krijgen in actoren, motieven en aanvalsroutes;
3. Breng het aanvalsoppervlak in kaart en identificeer kwetsbaarheden;
4. Analyseer de impact op gebruikers, organisaties en de samenleving;
5. Selecteer maatregelen op basis van risico (risico = waarschijnlijkheid × impact);
6. Documenteer alles voor naleving van de CRA en audits.

Voor de praktische voorbeelden betekent dit:

- **Slimme thermostaat**: krijgt encryptie, een sterk wachtwoordbeleid, ondertekende OTA-updates en een eenvoudige privacyverklaring.
- **ICS-gateway**: krijgt beveiligd opstarten, hardware root of trust, gesegmenteerde netwerken, SIEM-logging, rolbeheer en een complete SBOM met kwetsbaarheidsmonitoring.

## 2. Secure Design en Development

Terugkomend op punt 1 van bijlage I, deel I van de CRA, is de risicogebaseerde cyberbeveiligingsaanpak gebaseerd op het principe van "security by design and by default", namelijk dat PDE's vanaf het begin zo moeten worden ontworpen en ontwikkeld dat ze veilig zijn. Het is niet langer voldoende om beveiliging achteraf als optionele laag toe te voegen; het moet een essentieel onderdeel zijn van het hele productontwikkelingsproces.

'Secure by Design', 'Secure by Default' en het gebruik van veilige ontwikkelingspraktijken vormen de kern van een veerkrachtige digitale productstrategie. Ze zorgen ervoor dat beveiliging geen bijzaak is, maar een structureel en aantoonbaar geïntegreerd onderdeel van het product – precies wat de CRA vereist.


Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Met behulp van internationale standaarden zoals IEC 62443, ISO 27034, OWASP en ENISA-richtlijnen kunnen fabrikanten deze principes efficiënt toepassen en tegelijkertijd aan hun nalevingsverplichtingen voldoen.

Producten moeten voldoen aan de volgende principes:

1. **Secure by design**: beveiliging is vanaf de vroegste ontwikkelingsstadia geïntegreerd;
2. **Secure by default**: standaardinstellingen moeten prioriteit geven aan veiligheid (bijv. sterke wachtwoorden, minimaal aantal open poorten, enz.)
3. **Secure development**: met behulp van veilige coderingspraktijken en dreigingsmodellering.

## 2.1. Security by Design – Veilig vanaf het eerste ontwerp

'Secure by design' betekent dat vanaf de conceptfase rekening wordt gehouden met cyberbeveiliging bij het nemen van beslissingen over architectuur, componentkeuze en interactie tussen subsystemen. Beveiliging moet even fundamenteel zijn als functionaliteit of gebruiksvriendelijkheid.

Praktisch voorbeeld:

Bij het ontwerpen van een slim deurslot worden onmiddellijk de volgende beslissingen genomen:

- End-to-end-encryptie toepassen tussen de app en het slot;
- Sleutels veilig opslaan in een TPM of Secure Element;
- Debug-poorten fysiek uitschakelen na productie.

Relevante standaarden en richtlijnen hiervoor zijn onder meer:

- IEC 62443-4-1: vereist beveiligingsintegratie in de levenscyclus van software;
- ISO/IEC 27034: Applicatiebeveiliging in de levenscyclus van softwareontwikkeling;
- NIST SP 800-218 SSDF;
- ENISA Secure Software Development Good Practices.


Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

## 2.2. Security by Default – Veilig zonder configuratie door de gebruiker

'Security by default' betekent dat producten standaard met de meest veilige configuratie worden geleverd. De gebruiker hoeft dus niet te raden of de beveiliging is ingeschakeld. Beveiliging is de basis, geen optionele 'geavanceerde instelling'.

Voorbeelden van veilige standaardinstellingen:

- Geen gedeelde standaardinstellingen, verplicht instellen van inloggegevens bij de eerste opstart of koppelen zonder wachtwoord met veilige factoren;
- Alleen noodzakelijke netwerkpoorten open (principe van minimale blootstelling);
- Firmware-updates standaard ondertekend en geverifieerd;
- Logging en auditspoor standaard ingeschakeld voor kritieke functies.

Relevante richtlijnen in dit verband zijn:

- OWASP Secure Configuration: Best practices for secure default settings;
- NIST SP 800-128: Gids voor beveiligingsgericht configuratiebeheer.

## 2.3. Secure Coding Practices

De CRA vereist dat softwareontwikkeling wordt uitgevoerd in overeenstemming met aangetoond veilige ontwikkelingspraktijken en met voortdurende aandacht voor bedreigingen. Dit betekent onder andere:

Veilig coderen:

- Invoervalidatie (tegen SQL-injectie, bufferoverflows, enz.);
- Gebruik van veilige bibliotheken en versleuteling;
- Fuzz testing en statische codeanalyse.

Bedreigingsmodellering:
Voor elk onderdeel van de software moet het volgende worden beoordeeld:

- Wie zou dit kunnen aanvallen?
- Hoe zouden ze dat kunnen doen?


Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Wat zou de impact zijn?

Frameworks zoals STRIDE (Microsoft), OWASP Threat Dragon en MITRE ATT&CK kunnen helpen om kwetsbaarheden en aanvalsroutes systematisch in kaart te brengen.

Relevante standaarden en richtlijnen in dit verband zijn onder meer:

- OWASP Secure Coding Practices Checklist;
- ISO/IEC 27001 Annex A.14: Security requirements in development;
- ENISA Threat Modelling Guidelines (2022);
- BSI TR-03161 (Duitsland): Development of Secure Software.

## 2.4. Concrete Maatregelen voor Fabrikanten

Samengevat moet een organisatie die CRA-conforme PDE's wil ontwikkelen:

- Een secure software development lifecycle (SSDLC) hanteren, zoals beschreven in IEC 62443-4-1 of NIST SP 800-218 SSDF;
- Een codebeoordeling en test beleid hebben dat zich richt op kwetsbaarheden (SAST, DAST, fuzzing);
- Systematisch bedreigingsmodellering toepassen op elke belangrijke component;
- Producten leveren met standaard gesloten poorten, ingeschakelde logregistratie en beveiligde toegangspoorten;
- Een PSIRT-functie met duidelijke rollen en on-call processen hanteren;
- Beveiligingskwaliteitspoorten in CI/CD (SAST, DAST, SCA, geheimenscan) met fail-the-build-beleidsregels definiëren.

# 3. Security Management gedurende de Levenscyclus

Naast het veilige ontwerp, de ontwikkeling en de productie van PDE's moet je product ook gedurende de hele levenscyclus veilig blijven. Digitale producten evolueren, en dat geldt ook voor hun beveiliging. Dit betekent dat de beveiliging continu moet worden beheerd en ook na het op de markt brengen van de PDE in acht moet worden genomen.

Concreet moeten fabrikanten[14]:

1. Voortdurend kwetsbaarheden monitoren;
2. Tijdig beveiligingsupdates en patches verstrekken;
3. Een beleid voor het melden van kwetsbaarheden hanteren en risico's op transparante wijze communiceren aan gebruikers en regelgevende instanties.

## 3.1. Voortdurende Monitoring van Kwetsbaarheden

Zodra een product op de markt komt, moeten fabrikanten actief en systematisch kwetsbaarheden opsporen. Dit omvat:

- Het monitoren van kwetsbaarheidsdatabases, zoals de European vulnerability database[15] ;
- Het monitoren van adviezen van leveranciers;
- Het bijhouden van Common Vulnerabilities and Exposures (CVE's) met betrekking tot gebruikte componenten of bibliotheken;
- Het gebruik van een SBOM om afhankelijkheden te identificeren en bij te houden;
- Intern nieuwe kwetsbaarheden monitoren door middel van bug bounty-programma's, penetratietests of beveiligingsaudits.

Voorbeeld:

Een fabrikant van netwerkcamera's maakt gebruik van open-source firmwaremodules. Uit de CVE-database blijkt dat één van deze modules een kritieke kwetsbaarheid bevat (bijvoorbeeld CVE-2023-XXXXX). De fabrikant is verplicht deze informatie te monitoren en te evalueren en, indien relevant, passende maatregelen te nemen.

Relevante informatiebronnen in dit verband zijn onder meer:

- CVE;
- EPSS (Exploit Prediction Scoring System);
- ENISA Vulnerability Management Guidelines;
- ISO/IEC 30111: Vulnerability handling processes.

[14] Hoewel de vereisten voor de respons op kwetsbaarheden uitgebreid worden behandeld in bijlage I, deel II, vloeien ze voort uit punt 1 en 2 van bijlage I, deel I, en worden ze daarom ook behandeld in deze richtlijn.
[15] Art. 17, lid 5, CRA.


Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

## 3.2. Tijdige Beveiligingsupdates en Patches

De CRA verplicht fabrikanten om snel te reageren op bekende kwetsbaarheden en gedurende de ondersteuningsperiode gratis en efficiënte beveiligingsupdates te verspreiden.

Deze updates moeten:

- Digitaal ondertekend en gevalideerd zijn;
- Een fail-safe rollbackmechanisme hebben;
- Automatisch installeerbaar zijn met opt-out-opties en/of met minimale gebruikersinteractie;
- Ten minste 10 jaar na release beschikbaar blijven, of gedurende de rest van de ondersteuningsperiode (afhankelijk van welke periode langer is).

Voorbeeld:

Een fabrikant van slimme thermostaten ontdekt een kwetsbaarheid in de Wi-Fi stack. Binnen twee weken wordt een beveiligingspatch ontwikkeld, getest en verspreid via een ondertekende OTA-update. Gebruikers ontvangen een duidelijke melding en de update wordt automatisch geïnstalleerd wanneer het apparaat opnieuw wordt opgestart.

Relevante informatiebronnen in dit verband zijn onder meer:

- ISO/IEC 29147: Gecoördineerde bekendmaking van kwetsbaarheden (CVD);
- NIST SP 800-40: Guide to Enterprise Patch Management;
- ETSI EN 303 645: Beveiligingsnorm voor IoT consumentenproducten (inclusief mechanismen voor software updates).

## 3.3. Beleid inzake het Melden van Kwetsbaarheden en Transparante Communicatie

Transparantie is essentieel. De CRA vereist dat fabrikanten:

- Een CVD-beleid publiceren;
- Een contactpunt (bijv. security@company.eu) voor meldingen opgeven;
- Gebruikers en autoriteiten zoals ENISA of de nationale toezichthoudende autoriteit snel informeren in geval van ernstige risico's;



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

- Transparant communiceren over beschikbare patches, risicobeperkende maatregelen en resterende risico's.

Voorbeeld:

Een ethische hacker meldt een kritieke kwetsbaarheid in een aangesloten alarmsysteem via het openbare CVD-platform van de fabrikant. Binnen 72 uur wordt de ontvangst bevestigd en na interne analyse wordt ENISA geïnformeerd via het ENISA-platform voor meldingen (nationale eindpunten). Binnen drie weken wordt een patch uitgerold en worden alle gebruikers via e-mail en app-meldingen op de hoogte gebracht van het risico en de oplossing.

Relevante informatiebronnen in dit verband zijn onder meer:

- FIRST Vulnerability Coordination Maturity Model (VCMM);
- ISO/IEC 29147: Richtlijnen voor het bekendmaken van kwetsbaarheden;
- ENISA Coordinated Vulnerability Disclosure Guidelines (2022);
- OpenSSF VEX (Vulnerability Exploitability eXchange).

## 4. Beveiliging van de Toeleveringsketen

De CRA erkent dat een product nooit volledig 'onafhankelijk' is: het bestaat uit tientallen, soms honderden componenten van externe leveranciers, open-sourceprojecten en hardware partners. Daarom stelt de CRA expliciete eisen voor het beheer van cyberbeveiligingsrisico's binnen de toeleveringsketen.

In de praktijk moeten fabrikanten:

1. Een up-to-date en transparant overzicht bijhouden van de gebruikte softwarecomponenten via een SBOM;
2. Van leveranciers eisen dat zij voldoen aan CRA-conforme beveiliging;
3. Risico's in verband met open source en externe afhankelijkheden actief monitoren en beheren.


Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

## 4.1. Software Bill of Materials (SBOM)

Een SBOM is vergelijkbaar met een ingrediëntenlijst voor software: het bevat een overzicht van alle componenten, versies en de herkomst van gebruikte software-elementen, inclusief open-sourcebibliotheken.

De CRA verplicht fabrikanten om een SBOM bij te houden en deze op verzoek aan regelgevende instanties en autoriteiten te kunnen voorleggen. Publicatie van de SBOM voor gebruikers is optioneel[16] . Deze SBOM vormt de basis voor:

- Kwetsbaarheidsanalyse (bijvoorbeeld via CVE-tracking);
- Impact beoordeling in geval van zero-days;
- Audits van de toeleveringsketen.

Voorbeeld:

Een fabrikant van slimme routers stelt een SBOM op waarin duidelijk wordt vermeld dat het product gebruikmaakt van:

- OpenSSL 1.1.1n;
- BusyBox 1.35.0;
- Een aangepaste versie van een open-source firewallmodule.

Wanneer een kwetsbaarheid in OpenSSL (CVE-2022-XXXX) bekend wordt gemaakt, kan de fabrikant onmiddellijk controleren of het product hierdoor wordt getroffen en passend reageren.

Relevante informatiebronnen in dit verband zijn onder meer:

- CycloneDX, SPDX: SBOM-formaten (ook aanbevolen door ENISA en NTIA);
- ISO/IEC 5230 (OpenChain): Supply chain software compliance;
- OpenSSF-tools voor het genereren van SBOM's en het opsporen van kwetsbaarheden.

[16] Indien beschikbaar voor gebruikers, verduidelijk dan waar/hoe gebruikers er toegang toe kunnen krijgen.



Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

## 4.2. Beveiligingsvereisten voor Leveranciers

De CRA eist ook dat fabrikanten ervoor zorgen dat hun leveranciers en externe ontwikkelaars zich houden aan beveiligingsvereisten die vergelijkbaar zijn met die van hun eigen team. Verantwoordelijkheid kan niet worden doorgeschoven; kwetsbaarheden in componenten van derden kunnen ook leiden tot CRA-nalevingsverplichtingen.

Concreet betekent dit:

- Opname van cyberbeveiligingsclausules in leverancierscontracten;
- Het uitvoeren van security due diligence bij het selecteren van softwareleveranciers;
- Periodiek controleren of partners voldoen aan bijvoorbeeld:
    - ISO/IEC 27001 (informatiebeveiliging);
    - IEC 62443-4-1 (veilige productontwikkeling);
    - OWASP SAMM- of BSIMM maturity models.
- Contractuele auditrechten en minimale garantieniveaus (bijv. certificering van conformiteitsclaims) voor kritieke componenten;
- Melding binnen de 24 uur van door leveranciers ontdekte kritieke kwetsbaarheden die invloed hebben op jouw PDE's.

Voorbeeld:

Een fabrikant van medische IoT-apparaten werkt samen met een softwareleverancier in Azië. In het contract is bepaald dat deze leverancier:

- Veilig ontwikkelt in overeenstemming met IEC 62443-4-1;
- Alle gebruikte open-sourcecomponenten documenteert;
- Een kwetsbaarheidsbeleid hanteert met verplichte melding binnen 24 uur.

## 4.3. Risicobeheer van Open-Source en Externe Bibliotheken

Open-source software biedt veel voordelen, maar brengt ook risico's met zich mee: kwetsbaarheden, ontbrekende updates, onduidelijke licenties of onbetrouwbare beheerders. De CRA eist van fabrikanten dat zij deze risico's actief beheren en monitoren.

Best practices zijn onder meer:

- Gebruik afhankelijkheidscanners (bijv. OWASP Dependency-Check, Snyk, Trivy);
- Automatische waarschuwingen voor kwetsbaarheden (bijv. via GitHub Advisories);
- Gebruik alleen onderhouden en matuur open-sourceprojecten;
- Pas beveiligingspoorten toe in CI/CD-pijplijnen (blokkeer builds met bekende CVE's);
- Gebruik VEX om ruis van niet-exploiteerbare CVE's te verminderen;
- Eis een minimale responsiviteit van beheerders bij het selecteren van OSS.

Voorbeeld:

Een fabrikant gebruikt een populaire JavaScript-bibliotheek (bijv. Log4j) in een web interface. Bij het ontdekken van Log4Shell (CVE-2021-44228) weet de fabrikant door middel van SBOM-analyse precies welke versies zijn getroffen en kan hij de getroffen producten segmenteren en patchen.

Relevante informatiebronnen in dit verband zijn onder meer:

- NIST SSDF (Secure Software Development Framework);
- ENISA OSS Security Guidelines;
- OpenSSF Scorecard: Objectieve kwaliteitsbeoordeling van open-sourceprojecten.


Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

## *Conclusie*

Deze richtlijn omvat een eerste **technische uiteenzetting van de vereisten van bijlage I, deel I van de CRA met praktische suggesties en aanbevelingen**. Er worden **vier componenten** belicht die cruciaal zijn voor de naleving van de CRA: (1) een risicogebaseerde cyberbeveiligingsaanpak, die een risicobeoordeling, op maat gemaakte beveiligingsmaatregelen en een afweging van dreigingsmodellen, aanvalsoppervlakken en impact omvat; (2) het secure-by-design/default-principe; (3) beveiligingsbeheer gedurende de hele levenscyclus van je PDE; (4) overwegingen en controles met betrekking tot de toeleveringsketen. Voor elk onderdeel worden **praktische suggesties** gedaan over hoe je deze verplichtingen kunt implementeren en naleven op basis van erkende best practices en standaarden. Deze kunnen echter veranderen op basis van de huidige besprekingen rond CRA-standaarden en verdere ontwikkelingen op het gebied van de regelgeving. Als volgende stappen voor kmo's wordt aanbevolen om aanvullende richtlijnen te raadplegen in de **SECURE-repository**, zoals het **CRA Methodological Compliance Assessment Framework** voor een stapsgewijze toolkit en checklists voor naleving van de CRA, en **CRA 101: Understanding CRA Obligations** voor een beginner-level, beknopt overzicht van de wettelijke CRA-verplichtingen.