Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

EZ / NCTV

Nationaal Cyber Security Centrum
Staf
Bestuurlijke Ondersteuning

Turfmarkt 147
2511 DP Den Haag
Postbus 117
2501 CC Den Haag
www.ncsc.nl

Contactpersoon
[redacted]

Datum
8 april 2025

Onze referentie
CRA

memo

quick scan uitvoeringstoets CRA

Aanleiding

Op 13 december 2024 heeft het NCSC een schriftelijk verzoek ontvangen van NCTV en EZ om een uitvoeringstoets te doen op de meldplicht uit de Cyber Resilience Act (CRA).

Opzet

In deze quick scan wordt, na een algemene introductie op de meldplicht van de CRA en de voorziene rol en taak van het NCSC, op pragmatische wijze kort en bondig aandacht geschonken aan onderstaande thema's. Deze thema's vloeien voort uit de binnen de BBR J&V en het NCSC afgesproken werkwijze voor uitvoeringstoetsen.

1. uitvoerbaarheid;
2. handhaafbaarheid;
3. inschatting haalbaarheid beoogde invoeringsdatum;
4. effecten op de doelgroep (doenvermogen en menselijke maat);
5. inschatting van de benodigde capaciteit van de taakorganisatie of keten;
6. effecten op de uitvoeringskosten;
7. duiding van mogelijke risico's en knelpunten, bijvoorbeeld bij samenloop van verschillende beleidsinitiatieven;
8. impact en haalbaarheid op IV/ICT;
9. communicatie over de nieuwe regeling;
10. gegevensuitwisseling, verantwoordings- en beleidsinformatie[1].

Algemene introductie op de CRA en de meldplicht

De CRA is een EU-verordening die regelt dat producten met digitale elementen (alle hard- en software en componenten) aan cybersecurityvereisten moeten voldoen voordat ze mogen worden aangeboden op de interne markt. Ook moeten fabrikanten van producten met digitale elementen onder de CRA actief uitgebuite kwetsbaarheden en ernstige incidenten melden bij het Agentschap van de Europese Unie voor cyberbeveiliging (hierna: ENISA) én het als coördinator aangewezen CSIRT. Dat wordt in Nederland het NCSC, op grond van artikel 16 van de Cbw jo. art. 2a AMvB Cbw.

[1] Incl. gegevensvastlegging t.b.v. de invoeringstoets

Nationaal Cyber Security Centrum
Staf
Bestuurlijke Ondersteuning

Datum
8 april 2025

Onze referentie
CRA

De CRA is op 20 november 2024 officieel gepubliceerd. Vanaf 20 dagen na de datum van publicatie, geldt een implementatietermijn van 21 maanden voor de meldplicht bij kwetsbaarheden en incidenten. Dit betekent dat de meldplicht vanaf 11 september 2026 zal gelden, en dat het meldloket per die datum gereed moet zijn voor ontvangst van deze meldingen.

Op grond van de CRA doen fabrikanten de melding in de lidstaat waar zij hun hoofdvestiging in de Unie hebben. De meldingen worden ingediend via een (nog door ENISA op te richten) centraal Europees meldingsplatform, met gebruikmaking van de eigen elektronische endpoints per lidstaat. De CRA-meldingen dienen tegelijkertijd toegankelijk te zijn voor ENISA. De als coördinator aangewezen CSIRT dient in beginsel de meldingen vervolgens via dit centrale meldingsplatform te delen met de andere lidstaten waarin het digitale product beschikbaar is gesteld, tenzij een 'cyberbeveiligingsgerelateerde reden voor uitstel' van deze verdere verspreiding van toepassing is.

De voorziene rol en taken van het NCSC
Het NCSC is (of wordt) het als coördinator aangewezen CSIRT voor Nederland en wordt gevraagd om het elektronisch meldloket in te richten alwaar fabrikanten hun CRA meldingen kunnen doen.

Verder is gevraagd in de uitvoeringstoets rekening te houden met art. 14 t/m 17 van de CRA, incl. relevante overwegingen 65 t/m 76, hetgeen betekent dat het meldloket in ieder geval geschikt dient te zijn voor de in die artikelen beschreven taken:

- Het via een elektronisch meldloket ontvangen van meldingen van fabrikanten (inclusief vrijwillige meldingen door fabrikanten of andere natuurlijke of rechtspersonen) over actief uitgebuite kwetsbaarheden en ernstige incidenten die gevolgen hebben voor de beveiliging van producten met digitale elementen in de drie in artikel 14 genoemde stadia: vroegtijdige waarschuwing, kwetsbaarheidsmelding respectievelijk incidentmelding en eindverslag.
- Het indien nodig verzoeken en ontvangen van een tussentijds verslag over relevante updates van de status.
- Aansluiting van het elektronische meldloket waarop NCSC de melding ontvangt op het centrale meldingsplatform, en gelijktijdige toegankelijkheid van de melding voor ENISA.
- Informeren van gebruikers wanneer dat evenredig en noodzakelijk wordt geacht om de gevolgen van een kwetsbaarheid of incident te voorkomen of beperken wanneer de fabrikant zelf niet tijdig de gebruikers informeert.
- Onverwijlde doorzending van de melding aan andere nationale CSIRTs via het centrale meldingsplatform.
- Beoordeling mogelijk uitstellen van de verspreiding van meldingen aan andere CSIRTs in geval van toepassing van de 'cyberbeveiligingsgerelateerde redenen voor uitstel', in dat geval informeren van ENISA over dit besluit en motiveren ervan.
- Beoordeling zeer uitzonderlijke omstandigheden op verzoek van de fabrikant om de gelijktijdige melding aan ENISA uit te stellen.
- De Rijksinspectie Digitale Infrastructuur (RDI) moet geïnformeerd worden over kwetsbaarheden of incidenten waarvan melding is gedaan en die RDI nodig heeft voor de uitvoering van haar taak als nationale markttoezichtsautoriteit.
- Het verlenen van helpdeskondersteuning aan fabrikanten met betrekking tot de meldplicht op grond van artikel 14, met name aan fabrikanten die als micro-onderneming of mkb kunnen worden aangemerkt.

Nationaal Cyber Security Centrum
Staf
Bestuurlijke Ondersteuning

Datum
8 april 2025

Onze referentie
CRA

Onzekerheden en scenario's

In het verzoek om de uitvoeringstoets te doen zijn een aantal onzekere factoren benoemd. Zo is nog niet bekend welke voorwaarden zullen gelden voor de uitzonderingsgronden voor het uitstellen van verspreiden van meldingen. Ook is het Europese centrale meldingsplatform waar het meldloket op moet worden aangesloten nog niet ingericht.

Een andere onzekerheid die in het verzoek niet wordt benoemd is onbekendheid met de sector. Het aantal fabrikanten dat in Nederland onder de werking van de CRA valt en daarmee potentieel hun meldingen bij het meldloket indient is onbekend. Ook is onbekend hoeveel meldingen deze fabrikanten naar schatting bij het meldloket zullen of moeten doen. Deze laatste onzekerheden maken dat het voor het NCSC momenteel niet mogelijk is om een inschatting te maken van de structurele capaciteit die op termijn benodigd is voor de beoordeling en opvolging van CRA meldingen die worden gedaan in het elektronisch meldloket.

In het verzoek om de uitvoeringstoets is met het oog op onzekere factoren rondom de uitvoering van de meldplicht gevraagd om met verschillende scenario's te werken.

Scenario 1: meest basic mogelijke inrichting van alleen een nationaal meldpunt waarbij meldingen van kwetsbaarheden en incidenten kunnen worden ontvangen

Scenario 2: scenario 1 + selectie aan de voorkant (=toepassing van uitzonderingsgronden)

Scenario 3: scenario 1, 2 + aansluiting op een (nog onbekend) centraal meldingsplatform (= 'poort' naar ENISA)

Conclusie en advies

De voor het NCSC voorziene rol en taken voor de meldplicht uit de CRA zijn op basis van deze quick scan uitvoeringstoets uitvoerbaar als aan een aantal hieronder nader genoemde randvoorwaarden wordt voldaan.

Uitwerking per toetsingscriterium

1. Uitvoerbaarheid

Het NCSC acht de taken die voorzien zijn voor het NCSC in scenario 1 uitvoerbaar. Het NCSC heeft een meld- en registratiefunctionaliteit gemaakt voor de NIS2/Cbw en kan naar inschatting met wat aanpassingen deze functionaliteit bruikbaar maken als meldloket voor de CRA. De incidentele kosten voor het aanpassen van deze functionaliteit worden bij punt 6 uitgewerkt, evenals de structurele kosten voor het beheer en onderhoud van het meldloket.

De taken die zijn voorzien onder scenario 2 zijn eveneens uitvoerbaar voor het NCSC. Daartoe zullen we additionele (structurele) capaciteit moeten aantrekken en deze medewerkers moeten opleiden om een goede beoordeling van meldingen te kunnen doen. Ook de beoordeling en opvolging van meldingen gaat capaciteit kosten. Omdat momenteel onduidelijk is hoeveel fabrikanten onder de CRA in Nederland bij het meldloket hun meldingen zullen doen en hoeveel meldingen dat op jaarbasis zullen zijn, kunnen we geen inschatting maken van de benodigde capaciteit.

Nationaal Cyber Security Centrum
Staf
Bestuurlijke Ondersteuning

Datum
8 april 2025

Onze referentie
CRA

De taken onder scenario 3 zijn naar verwachting ook uitvoerbaar. We kunnen het Nederlandse meldloket laten aansluiten op de architectuur van het Europese centraal meldingsplatform. Dit centraal meldingsplatform dient te worden opgericht door ENISA. Bovendien dient ENISA, in samenwerking met het CSIRT-netwerk, specificaties te verstrekken voor de technische, operationele en organisatorische maatregelen met betrekking tot de oprichting, het onderhoud en de veilige werking van het centrale meldingsplatform. Dit kan aanzienlijke gevolgen hebben voor de aansluiting en functionaliteiten van het nationale meldpunt en de kosten die hiermee gepaard gaan.

Het NCSC voorziet met de inwerkingtreding van de meldplicht van de CRA ook een toename in werklast ten aanzien van Coordinated Vulnerability Disclosure (CVD) taken. Deze toename is in de quick scan uitvoeringstoets buiten beschouwing gelaten en zal bij een herijking van de uitvoeringstoets CRA, indicatief in februari 2026, nader in kaart moeten worden gebracht.

2. Handhaafbaarheid
Handhaving in het kader van de CRA is niet aan het NCSC. Dit toetsingscriterium is dan ook niet uitgewerkt.

3. Inschatting haalbaarheid beoogde invoeringsdatum
Als tijdig aan de benodigde randvoorwaarden wordt voldaan kan het NCSC vanaf 11 september 2026 een elektronisch meldloket voor de CRA in bedrijf hebben.

4. Effecten op de doelgroep
De CRA regelt dat producten met digitale elementen (alle hard- en software en componenten) aan cybersecurityvereisten moeten voldoen voordat ze mogen worden aangeboden op de interne markt. Ook moeten fabrikanten van producten met digitale elementen onder de CRA actief uitgebuite kwetsbaarheden en ernstige incidenten melden bij het Agentschap van de Europese Unie voor cyberbeveiliging (hierna: ENISA) én het als coördinator aangewezen CSIRT, in Nederland het NCSC.

5. Inschatting van de benodigde capaciteit van het NCSC
Het NCSC zal naar verwachting meer werk krijgen door de inwerkingtreding van de CRA en de meldplicht voor fabrikanten. Los van de incidentele capaciteit die moet worden ingezet voor het inrichten van het elektronische meldloket, heeft het NCSC capaciteit nodig voor beheer en onderhoud van het meldloket. Daar is een redelijke schatting van te maken die hieronder bij uitvoeringskosten nader is uitgewerkt.
Waar momenteel geen redelijke schatting van gemaakt kan worden is de structureel benodigde capaciteit voor de beoordeling en opvolging van CRA-meldingen. Dat komt omdat niet bekend is hoeveel fabrikanten onder de CRA hun meldingen in NL zullen doen, en hoeveel meldingen dat op jaarbasis kunnen worden. Ook de capaciteit voor de helpdeskondersteuning is sterk afhankelijk van het aantal fabrikanten en meldingen, en de vragen die aan de helpdesk gesteld gaan worden.

De NCTV en EZ hebben het NCSC gevraagd om vooralsnog uit te gaan van 2 FTE voor de beoordeling en opvolging van CRA meldingen en helpdeskondersteuning. Deze 2 FTE is nadrukkelijk slechts een eerste basis om vanaf de inwerkingtreding van de CRA meldplicht op 11 september 2026 ook daadwerkelijk capaciteit

beschikbaar te hebben voor de beoordeling en opvolging van CRA meldingen en helpdeskondersteuning. In de periode daarna zal moeten blijken of 2 FTE overeenkomt met de toegenomen werklast voor het NCSC.

6. Effecten op de uitvoeringskosten

De inrichting van een nationaal meldpunt voor de CRA brengt, zoals onder 5 reeds geïntroduceerd, incidentele en structurele kosten voor de uitvoering met zich mee. De incidentele kosten hebben betrekking op het ontwerp en de bouw van de meldfunctionaliteit. Afhankelijk van hoe deze functionaliteit moet worden ingericht liggen de incidentele kosten op basis van onze huidige schatting tussen de 220.000 euro voor een variant waarbij het bestaande NIS2 meldformulier kan worden aangepast voor de CRA en er geen koppeling met het ENISA portaal hoeft te worden gebouwd (maar wel een rapport moet worden gegenereerd) en de 510.000 euro voor een variant waarbij een apart kwetsbaarheden meldpunt op het NCSC portaal moet worden ingericht en een API koppeling met het meldportaal van ENISA moet worden bewerkstelligd.
Structurele kosten voor beheer van deze applicatie worden vooralsnog geschat op 75.000 euro per jaar voor personeel en techniek. Hier kan te zijner tijd, en afhankelijk van de keuze die gemaakt worden een herberekening op plaatsvinden.

De structurele kosten voor benodigde capaciteit voor het beoordelen van CRA meldingen en de opvolging ervan zijn op dit moment door het NCSC niet in te schatten. De NCTV en EZ hebben het NCSC gevraagd om vooralsnog uit te gaan van 2 FTE voor de beoordeling en opvolging van CRA meldingen en helpdeskondersteuning. Het NCSC gaat in deze uitvoeringstoets indicatief uit van schaal 12 functionarissen die op basis van gehanteerde HOT-tarieven een structurele kostenpost van 143.000 euro per FTE euro op jaarbasis met zich meebrengen.

Samengevat zijn de uitvoeringskosten voor de verschillende scenario's dan:

Scenario 1: 220.000 euro tot 510.000 euro incidenteel voor de meest basic inrichting van alleen een nationaal meldpunt waarbij meldingen van kwetsbaarheden en incidenten kunnen worden ontvangen en 75.000 euro per jaar structureel om deze applicatie te beheren.

Scenario 2: kosten scenario 1 plus 286.000 euro per jaar structureel voor 2 FTE voor de beoordeling en opvolging van meldingen.

Scenario 3: kosten scenario 1 en 2 plus evt. extra kosten waar gelet op de onzekerheid over het Standard Reporting Platform van ENISA momenteel geen inschatting van te maken is.

7. Duiding van mogelijke risico's en knelpunten

Het NCSC ziet de onzekerheden t.a.v. de CRA als risico. Het grootste risico is dat het op dit moment onduidelijk is hoe het Standard Reporting Platform van ENISA eruit gaat zien en wanneer het gereed is. Dat heeft mogelijk (aanzienlijke) gevolgen voor de hoogte van het bedrag dat nodig is om het Nederlandse meldloket daarop aan te sluiten en het moment waarop we dat als NCSC kunnen realiseren. Uit onze eigen contacten met ENISA begrijpen we dat het nog wel even kan duren voordat er meer duidelijk is over het Standard Reporting Platform van ENISA.

Het NCSC ziet een knelpunt t.a.v. de helpdeskondersteuning en de rol/verantwoordelijkheid van het NCSC als aangewezen CSIRT. Het is niet onze rol om te adviseren over een meldplicht. Wel zien we een rol voor ons om in het kader van art. 14 CRA fabrikanten te informeren over hoe een melding moet worden gedaan en wat er in een melding moet staan. We zien als CSIRT geen rol voor ons bij adviseren over de meldplicht zelf en of die in specifieke gevallen al dan niet van toepassing is.

8. Impact en haalbaarheid op IV/ICT
CRA taakuitvoering is, met de huidige kennis en inzichten, IV/ICT matig uitvoerbaar en realiseerbaar. Het vereist, zoals onder punt 5 en 6 geschetst, aanpassingen van NCSC systemen en het vereist koppelingen met Europese systemen die nog ontwikkeld moeten worden. De aanpassingen en koppelingen kunnen worden gerealiseerd als de benodigde randvoorwaarden tijdig worden ingevuld (o.a. duidelijkheid over het Standard Reporting Platform van ENISA en beschikbaarheid benodigde financiële middelen).

9. Communicatie over de nieuwe regeling
Communicatie over de CRA is primair niet aan het NCSC maar aan de beleidsverantwoordelijke. In overleg kunnen we t.a.v. de uitvoering van de meldplicht onze bestaande communicatiekanalen aanwenden om fabrikanten (mede) te informeren over de CRA meldplicht en het meldloket.

10. Gegevensuitwisseling, verantwoordings- en beleidsinformatie
Het delen van gegevens of informatie over kwetsbaarheden binnen producten die binnen het bereik van de CRA liggen, lijkt door de EU wetgever beperkt te zijn vormgegeven. Er lijkt een harde knip te bestaan tussen de taken van het CSIRT onder NIS2 en de taken van het als coördinator aangewezen CSIRT onder de CRA. De taken van die laatste zijn beperkt tot het bepaalde in de artikelen 14 t/m 17 CRA en zijn hierboven reeds omschreven.

Het bestaan van een dergelijk hard onderscheid tussen de taken van het CSIRT in het algemeen en de taken van het als coördinator aangewezen CSIRT onder de CRA is ook wel logisch. Het bereik van de CRA is immers beperkt tot "*op de markt aangeboden producten met digitale elementen waarvan het beoogde doel of het redelijkerwijs voorzienbaar gebruik een directe of indirecte logische of fysieke gegevensverbinding met een apparaat of netwerk omvat*". Die omschrijving is een andere dan het bereik van de NIS2, dat ziet op "*een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie*" en stelt regels t.a.v. essentiële en belangrijke entiteiten en de door hen gebruikte netwerk- en informatiesystemen. Systemen dus, waar de onder de CRA vallende producten een gegevensverbinding mee aan kunnen gaan, maar die daarmee niet zélf ook een netwerk- of informatiesysteem worden.

De gegevensuitwisseling die onder het regime van de CRA voor de door de lidstaat aangewezen coördinerend CSIRT is toegestaan, is dan ook uitvoerig beschreven binnen de artikelen 14 t/m 17 van de CRA. Dit omvat niet alleen de bevoegdheid om meldingen door te zetten naar de coördinerende CSIRT's van andere EU lidstaten, maar ook om het publiek over een bij zo'n meldingen betrokken kwetsbaarheid te informeren. Deze laatste bevoegdheid is overigens beperkt tot die gevallen waarin "*bewustmaking van het publiek noodzakelijk is om een ernstig*

Nationaal Cyber Security Centrum
Staf
Bestuurlijke Ondersteuning

Datum
8 april 2025

Onze referentie
CRA

incident met gevolgen voor de beveiliging van het product met digitale elementen te voorkomen of te beperken of om een lopend incident af te handelen, of indien de bekendmaking van het incident anderszins in het algemeen belang is" en kan alleen plaatsvinden na raadpleging van de betrokken fabrikant. Zie daartoe artikel 17, lid 2, CRA. In het kader van de uitvoering van deze verordening is het dan noodzakelijk hierop een beleid te formuleren, waarin deze elementen als afwegingskader zijn verwerkt.

Overigens is het informeren van gebruikers van het product onder de CRA, primair belegd bij de betreffende fabrikant. Zie daartoe artikel 14, lid 8. Het als coördinator aangewezen CSIRT kan echter, wanneer dit informeren van gebruikers niet tijdig door de fabrikant plaatsvindt, tot een dergelijk informeren overgaan, indien dit "*evenredig en noodzakelijk wordt geacht om de gevolgen van die kwetsbaarheid of dat incident te voorkomen of te beperken.*". In het kader van de uitvoering van deze verordening is het dan noodzakelijk hierop een beleid te formuleren, waaruit dan volgt wanneer een dergelijke handeling evenredig en noodzakelijk moet worden geacht.

Concluderend: voor wat betreft het onderwerp gegevensdeling lijkt de CRA goed uitvoerbaar voor het NCSC als coördinerend CSIRT, wanneer wij als zodanig worden aangewezen op grond van het bepaalde in artikel 17 Cbw. Zoals hierboven aangeven is er duidelijk onderscheid gemaakt tussen de taken van het CSIRT in het algemeen, onder het regime van de NIS2 en onze vertaling daarvan, de Cbw, en de taken van het op grond van die regelgeving aangewezen coördinerend CSIRT, dat de taken onder het regime van de CRA zal uitvoeren. Dit noopt in het geval van artikel 14, lid 8, CRA tot het ontwikkelen van aanvullend beleid voor specifiek deze taak, nu dit artikellid – anders dan de taken van het CSIRT op grond van de NIS2 – beoordelingsruimte laat aan het als coördinator aangewezen CSIRT.