Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Jaarplan 2026

Nationaal Cyber Security Centrum

Veilig vooruit in een digitaal weerbaar Nederland

Voorwoord

Het jaar 2025 liet opnieuw zien dat digitale dreigingen niet abstract of ver weg zijn, maar tastbaar en dichtbij. Cyberaanvallen raken onze samenleving in de kern: de rechtstaat, de zorg, energie, logistiek en communicatie. Achter de schermen werkt het NCSC, met inmiddels meer dan 400 collega's, eraan om Nederland digitaal weerbaarder te maken.

Sprekende recente voorbeelden zijn de Citrix- en de Ivanti-casussen, incidenten die een grote impact hebben op het vertrouwen in digitale systemen. En die duidelijk maken dat digitale veiligheid onlosmakelijk verbonden is met de werking van onze instituties en onze democratie.

We zien ook hoe geopolitieke spanningen steeds meer een digitale dimensie krijgen. In de voortdurende oorlog in Oekraïne zien we hoe cyberoperaties kritieke infrastructuur verstoren en desinformatie verspreiden. Ook Nederland is doelwit van statelijke actoren die onze energievoorziening, financiële sector en overheid testen op weerbaarheid.

Onze koers sluit naadloos aan bij de Nederlandse Cybersecuritystrategie (NLCS). De strategische lijnen en ambities voor een digitaal weerbaar Nederland vertalen we in dit jaarplan naar concrete acties en prioriteiten voor 2026. Acties die gericht zijn op een goede samenwerking en coördinatie in het cybersecuritystelsel, onder meer door een optimale publiek-private samenwerking. Alle organisaties in Nederland moeten op onze ondersteuning kunnen rekenen, waar het gaat om vergroting van de digitale weerbaarheid.

Twee grote veranderingen komen in 2026 in het werk van het NCSC samen. Sinds 1 januari zijn het Digital Trust Center (DTC) en het Computer Security Incident Response Team for Digital Service Providers (CSIRT-DSP) samengevoegd in het NCSC. Dit betekent dat het NCSC een versterkte positie in het cyberstelsel heeft gekregen. We zijn nu één nationale cybersecurityorganisatie, die niet alleen de Rijksoverheid en vitale sectoren bedient, maar ook digitale dienstverleners en het bedrijfsleven, met 2,4 miljoen ondernemingen! Door deze bundeling van kennis, diensten en netwerken kunnen we sneller, effectiever en breder optreden.

De andere grote verandering is de Cyberbeveiligingswet (CbW), die naar verwachting in de tweede helft van dit jaar in werking treedt. Deze wet vergroot de wettelijke taken en verantwoordelijkheden van het NCSC, en legt de basis voor een steviger, toekomstbestendig stelsel.

Cyberveiligheid vraagt om politieke prioriteit, bestuurlijke vastberadenheid en structurele investeringen. Het is daarom belangrijk dat ook het nieuwe kabinet cybersecurity hoog op de agenda heeft staan. Nederland heeft de kennis, de mensen en de internationale positie om een voortrekkersrol te blijven spelen in Europa en daarbuiten. Samen kunnen we ervoor zorgen dat onze samenleving veilig, vrij en weerbaar blijft – ook in het digitale domein.

Matthijs van Amelsfort
Directeur NCSC

Transitie naar de nationale cybersecurityorganisatie

2026 is voor het NCSC een jaar van transitie. Twee belangrijke, strategische ontwikkelingen komen samen.

- De Cyberbeveiligingswet (Cbw) treedt later dit jaar in werking.
- Het NCSC groeit verder, met de integratie van het Digital Trust Center (DTC) en de CSIRT-DSP, het Cyber Security Respons team voor digitale dienstverleners. Dit betekent dat het NCSC niet meer alleen voor vitale sectoren en de overheid werkt, maar voor alle bedrijven en organisaties in Nederland.

Dit zijn cruciale stappen in de ontwikkeling van het NCSC, die in lijn zijn met de Nederlandse Cybersecuritystrategie 2022-2028. We volgen daarmee het ingeslagen ‘groeipad’ en werken verder aan een toekomstbestendige cybersecurityorganisatie.

We vergroten het bereik en de efficiëntie van onze activiteiten, zodat steeds meer organisaties inzicht hebben in dreigingen in hun sector. Met dat inzicht stellen we ze in staat geïnformeerde besluiten te nemen over hun cyberveiligheid.

Deze opdracht vergt niet alleen een groei aan medewerkers, maar een digitale transformatie. Het NCSC kiest voor een wendbare, datagedreven en naar buiten gerichte manier van werken. Met producten en diensten voor nieuwe én bestaande doelgroepen.

Later in het jaar zal de onderliggende vernieuwde organisatiestructuur van het versterkte NCSC in werking treden. Tijdens onze ‘verbouwing’ blijft de winkel open: groei en continuïteit lopen dus parallel.

Vier rollen

Met de nieuwe versterkte positie van het NCSC in het cyberstelsel vervullen we vier belangrijke rollen:

Uitvoeringscoördinator

Kennis- en adviescentrum

Nationaal CSIRT

Sectoraal CSIRT

De vier rollen vullen elkaar aan. Voor onze operationele activiteiten als CSIRT is een goede positie als kennis- en adviescentrum en uitvoeringscoördinator noodzakelijk. Tegelijkertijd versterken de inzichten die we als CSIRT opdoen onze informatie- en kennispositie.

Rol 1. **Uitvoeringscoördinator**

Het NCSC draagt eraan bij dat organisaties in Nederland kunnen groeien in cyber- en digitale weerbaarheid. Samenwerking met andere (inter)nationale partners binnen de overheid, het bedrijfsleven, de wetenschap en het maatschappelijk middenveld is onontbeerlijk. Het NCSC heeft hierin een coördinerende rol. We delen kennis, faciliteren netwerken en bevorderen de benodigde samenwerking. Van het Cyberweerbaarheidsnetwerk (CWN) tot het VSSR-programma, dat Security Operations Centers (SOC's) ondersteunt.

Ons doel is een samenhangend cybersecuritystelsel waarin iedereen zijn rol optimaal kan vervullen en organisaties en bedrijven niet alleen staan. Want alleen samen bouwen we verder aan de digitale weerbaarheid van Nederland.

Ambities voor 2026

Het Cyberweerbaarheidsnetwerk (CWN) gaat een belangrijke rol spelen in de cyberweerbaarheid van Nederland. Het NCSC faciliteert in dit netwerk de samenwerking tussen publieke en private partners. Het Bouwplan Cyberweerbaarheidsnetwerk, dat in september 2025 verscheen, vormt het gezamenlijke startpunt.

Het Bouwplan bevat deelplannen van 5 functies: Informatiedeling, Doelwit- en Slachtoffernotificatie, Incidentafhandeling, Kennisuitwisseling en Opleiden, Trainen en Oefenen (OTO). In 2026 zal het NCSC met de verschillende doelgroepen werken aan deze functies, en ook de dekkingsgraad van dit netwerk vergroten. Dus meer organisaties die in netwerken samenwerken. Met als doel: beter inzicht te krijgen in wat er nodig is om alle organisaties digitaal weerbaarder te maken.

Rol 2. **Kennis- en adviescentrum**

Het NCSC functioneert namens de overheid als een centraal expertisepunt voor cybersecurity binnen Nederland. We werken aan kennisopbouw en -uitwisseling op het gebied van digitale weerbaarheid. Die kennis vertalen we naar praktisch toepasbare adviezen, die aansluiten bij de behoefte van onze doelgroepen. We geven inzichten en tools die zijn afgestemd op specifieke situaties, diverse sectoren en verschillende kennisniveaus. Zo raken organisaties voorbereid op incidenten en stimuleren we het lerend vermogen van het hele cybersecuritystelsel.

Door actieve kennisuitwisseling met publieke en private partners in binnen- en buitenland blijven we vooroplopen in innovatie en zorgen we dat organisaties profiteren van de nieuwste inzichten.

Ambities voor 2026

De integratie van het Digital Trust Center (DTC) en het Cyber Security Respons team voor digitale dienstverleners (CSIRT-DSP) in het vernieuwde NCSC betekent dat we vanaf nu voor veel meer doelgroepen zichtbaar en vindbaar moeten worden. We zijn er voor alle bedrijven en organisaties, ook die niet onder de Cbw of de Wet weerbaarheid kritieke entiteiten vallen.

De kennis en ervaring die DTC heeft opgebouwd met hun doelgroepen (zoals de voormalige DTC-community) gebruiken we voor de doorontwikkeling van producten en diensten. We zorgen ervoor dat deze kennis vindbaar is en aansluit op de behoeftes van deze nieuwe doelgroepen.

Rol 3. **Nationaal CSIRT**

Bij cyberdreigingen en incidenten is het NCSC altijd bereikbaar. We detecteren, analyseren en reageren 24/7 op cyberaanvallen en kwetsbaarheden. We leveren tijdige waarschuwingen, actuele dreigingsinformatie en ondersteuning bij incidentrespons – van het eerste signaal tot herstel.

Als nationaal Computer Security Incident Response Team (n-CSIRT) voeren we op nationaal niveau regie bij kwetsbaarheden, cyberdreigingen en incidenten. Ook zijn we Single Point of Contact (SPOC) voor Europese landen voor de uitwisseling van informatie en aanspreekpunt voor het internationale CSIRT-netwerk.

Ambities in 2026

Dit jaar is er bijzondere aandacht voor de door-ontwikkeling van monitoring en detectie van kwetsbaarheden binnen het Nationaal Detectie Netwerk. Een andere prioriteit is een goed functionerend meld- en registratieproces in het kader van de nieuwe Cyberbeveiligingswet (Cbw) en de Cyber Resilience Act (CRA). Voor de Cbw gaat dit proces in zodra de wet in werking treedt, voor de CRA in september van dit jaar.

Als n-CSIRT stimuleren we de samenwerking binnen de nationale en internationale netwerken en coördineren we de afhandeling van (bijna) incidenten op nationaal niveau.

Rol 4. **Sectoraal CSIRT**

Als sectoraal Computer Security Incident Response Team (s-CSIRT) zijn we het centrale aanspreekpunt voor organisaties binnen vitale sectoren zoals de energie- en drinkwaterbedrijven.

We helpen deze sectoren met dreigingsbeelden, wisselen informatie uit en dragen zorg voor incidentmanagement, -coördinatie en waar nodig -respons. We detecteren, analyseren en reageren 24/7 op cyberaanvallen zoals we dat ook als n-CSIRT doen. Verder delen we grootschalig inzichten over trends, dreigingen en kwetsbaarheden, toegespitst op uitdagingen en behoeften van de sectoren, zowel in het domein van Informatietechnologie (IT) als Operationele Technologie (OT).

Ambities in 2026

In 2026 werken we aan de vergroting van de zichtbaarheid en herkenbaarheid van onze organisatie en dienstverlening. We stimuleren wederzijdse kennisdeling binnen de sectoren, over thema's als industriële controlesystemen, veiligheid in de keten van toeleveranciers en risicoanalyse.

Samen met andere sectorale CSIRTs ontwikkelen we manieren om informatie snel te delen, in alle fases van mogelijke incidenten.

Dit zijn – voorzover nu bekend – de andere CSIRT's en de sectoren waarvoor zij werken:

IBD-CERT	gemeenten
NCSC	digitale aanbieders, post- en koeriersdiensten, afvalstoffenbeheer, chemische stoffen, levensmiddelen, aanbieders ict-diensten, digitale infrastructuur, ministeries, provincies, industrieel afvalwater, vervaardiging, drinkwater, ruimtevaart, energie, infrastructuur financiële markten, vervoer
CERT-WM	waterschappen, huishoudelijk afvalwater
Z-CERT	gezondheidszorg en de vervaardiging van medische apparatuur
SURFcert	onderzoek en onderwijs

De wettelijke basis

De wettelijke basis voor het werk van het NCSC is vastgelegd in verschillende wetten: de Wet beveiliging netwerk- en informatiesystemen (Wbni) de Wet weerbaarheid kritieke entiteiten, de Wet bevordering digitale weerbaarheid bedrijven, de Europese NIS2-richtlijn, dit jaar vertaald in de nationale Cyberbeveiligingswet (Cbw), de Network Code on Cybersecurity (NCCS) en vanaf september 2026 de Cyberweerbaarheidsverordening (Cyber Resilience Act - CRA).

Deze wetten hebben als doel de digitale weerbaarheid van de Europese Unie, en van Nederland, te versterken. Zodat we de gevolgen van cyberincidenten beperken en maatschappelijke ontwrichting voorkomen.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Mei 2026