Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Jaarplan 2022

Nederland digitaal veilig

Jaarplan NCSC 2022

Het NCSC is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland en heeft een operationeel coördinerende rol. Voor 2022 heeft het NCSC de volgende focusdoelen geformuleerd:

Inleiding

Algemeen

Voor u ligt het jaarplan 2022 van het Nationaal Cyber Security Centrum (NCSC). De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) is opdrachtgever van het NCSC, de Plaatsvervangend Secretaris Generaal (PSG) is eigenaar. Allen zijn onderdeel van het ministerie van Justitie en Veiligheid (JenV).

De Secretaris-Generaal (SG) van het ministerie van JenV en de NCTV bepalen de kaders waarbinnen het NCSC haar taken en activiteiten uitvoert. De NCTV stelt de beleidsdoelen en door de SG zijn de bedrijfsdoelen gesteld. Het NCSC is gevraagd op eigen wijze invulling te geven aan de doelstellingen dan wel aan te geven onder welke voorwaarden deze doelstellingen gerealiseerd kunnen worden.

Afbakening

In dit jaarplan wordt aangegeven welke resultaten binnen de gestelde kaders in 2022 van het NCSC mogen worden verwacht.

Opbouw van het jaarplan

Het jaarplan bestaat uit twee hoofdstukken. In hoofdstuk 1 worden het wettelijk kader en de belangrijkste thema's beschreven die het NCSC voor komend jaar van de NCTV heeft meegekregen. In hoofdstuk 2 zijn deze vertaald naar doelstellingen voor het NCSC voor 2022. Dit hoofdstuk biedt eveneens inzicht in de taakuitvoering door het NCSC binnen de gestelde kaders.

Over het NCSC

Het NCSC is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland en heeft een operationeel coördinerende rol. Zij begrijpt digitale kwetsbaarheden. Verbindt partijen. Deelt kennis en informatie. Beperkt dreigingen en voorkomt maatschappelijke schade.

De Rijksoverheid en organisaties in vitale sectoren zijn onze belangrijkste afnemers. Wij ondersteunen hen bij het treffen van maatregelen om cyberdreiging tegen te gaan of bij incidenten te herstellen. Zodat zij de continuïteit van hun dienst kunnen waarborgen. De aandacht voor economische veiligheid groeit en NCSC zet hier extra op in.

Wereldwijd zien we dat het cyberdomein continu in ontwikkeling is. Zo heeft het op afstand werken door corona en de wens te verduurzamen een verdere vlucht genomen. De energietransitie zorgt voor de ontwikkeling van nieuwe ketens in de vitale infrastructuur. En heeft ook het gebrek aan grondstoffen en de gevolgen daarvan voor de toelevering van computerchips effecten voor zowel het NCSC als vitale sectoren. NCSC spant zich maximaal in om aan de vraag vanuit de samenleving te voldoen door informatie te delen en coördinerend op te treden, uiteraard binnen de wettelijke mogelijkheden.

Daarnaast is ook het Nederlandse stelsel rondom cybersecurity volop in beweging. Nieuwe partijen krijgen een rol in dit stelsel en andere partijen zijn nog zoekende naar hun rol hierbinnen. Ook trajecten om het stelsel beter te laten functioneren zijn in ontwikkeling. Denk hierbij bijvoorbeeld aan het Landelijk Dekkend Stelsel (LDS), een netwerk van cybersecurity samenwerkingsverbanden, publiek en privaat. Het LDS heeft als doel informatie sneller en efficiënter met elkaar te delen.

Tegelijkertijd zien wij dat het aantal doelgroepen de afgelopen jaren, maar ook de komende jaren verder stijgt. Enerzijds omdat steeds meer vakdepartementen zien hoe belangrijk cybersecurity is en vooral welke impact het uitvallen van digitale voorzieningen heeft op de maatschappij en nationale veiligheid. Anderzijds omdat ontwikkelingen in Europa, waaronder de nieuwe Netwerk- en Informatieveiligheid (Nib) richtlijn, zorgen voor zeer grote aantallen nieuwe doelgroepen. Dit vraagt om een NCSC dat wendbaar, flexibel en schaalbaar is. Een NCSC dat ondanks de verschillende ontwikkelingen en bewegingen in het veld in staat is haar wettelijke taken goed en zorgvuldig uit te voeren.

Hoofdstuk 1

Wettelijke taken

Het NCSC is expert op het gebied van cyberdreigingen en -kwetsbaarheden. Kennis en analyse van de weerbaarheid van de doelgroepen (Rijk en vitale sectoren) van het NCSC is van cruciaal belang om Nederland digitaal veiliger te maken en te houden.

Het NCSC heeft conform de Wet beveiliging netwerk- en informatiesystemen (Wbni) diverse taken ter voorkoming of beperking van de uitval of het verlies van integriteit van de systemen van Rijks- en vitale organisaties. Is er sprake van een dreiging of een incident in netwerk- en informatiesystemen van vitale aanbieders of onderdelen die vallen onder de Rijksoverheid, dan is het NCSC het aangewezen Computer Security Incident Response Team (CSIRT)

Ook levert het NCSC een bijdrage aan de verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving.

Wettelijke kerntaken

- De wettelijke kerntaken van het NCSC zijn het voorkomen of beperken van uitval van beschikbaarheid of verlies van integriteit van de netwerk- en informatiesystemen van de Rijksoverheid en vitale aanbieders;
- Het bijstaan van Rijksoverheid en vitale aanbieders bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van hun producten of diensten te waarborgen of te herstellen;
- Het informeren en adviseren van deze aanbieders en anderen in en buiten Nederland over dreigingen en incidenten met betrekking tot informatiesystemen van de Rijksoverheid en vitale aanbieders
- Het verrichten van analyses en technisch onderzoek naar aanleiding van (aanwijzingen voor) bovenvermelde dreigingen en incidenten;
- De taken als centraal contactpunt als bedoeld in de Nib-richtlijn;
- De taken als CSIRT voor aanbieders van essentiële diensten.

Wanneer het NCSC tijdens het uitvoeren van haar wettelijke taak op informatie stuit dat ook gevolgen kan hebben voor andere, niet vitale partijen, meldt zij dit bij daarvoor aangewezen partijen. Het NCSC mag daarnaast ook het algemene publiek adviseren op het gebied van digitale dreigingen en incidenten.

Overige taken

- Het NCSC heeft een operationeel coördinerende rol binnen de nationale crisisstructuur in geval van een ernstig ICT-incident of een ICT-crisis. Hierbij heeft het NCSC tevens tot taak andere internationale CERT-partners adequaat te informeren, zeker op Europees niveau.
- Het NCSC heeft, samen met het Digital Trust Centre van het Ministerie van Economische Zaken en Klimaat de opdracht gekregen om te komen tot een Nationaal Detectie Netwerk: het Landelijk Dekkend Stelsel (LDS).

De wettelijke taken geven de kaders aan waarbinnen het NCSC haar doelen voor 2022 bepaalt.

Hoofdstuk 2

Doelstellingen

In het jaarplan 2022 heeft het NCSC twee belangrijke focuspunten: verhogen van de weerbaarheid en incident response. Deze twee focuspunten komen voort uit de wettelijke taken en de ontwikkelingen die wij zien op cybersecurity gebied. Vanuit deze twee focuspunten zijn de doelstellingen voor 2022 geformuleerd.

Verhogen weerbaarheid

Het verhogen van cyberweerbaarheid is een van de hoofddoelstellingen van het NCSC. Als wij gezamenlijk de Nederlandse (en Europese) cyberweerbaarheid verhogen, zijn wij beter opgewassen tegen aanvallen van buiten.

Het aandachtgebied van het NCSC ten aanzien van cyberweerbaarheid speelt zich af binnen vier gebieden: EU, Rijksoverheid, Vitaal en doelgroep organisaties. Hieronder nemen we u mee door de aandachtsgebieden voor 2022 en de rol (en het doel) die het NCSC nastreeft.

EU

De Europese ontwikkelingen binnen het *Network and Information Systems Directive* (NIS) / *Critical Entities Resilience* (CER) *Directive* kunnen leiden tot een toename van het aantal doelgroep-organisaties van het NCSC. Het NCSC heeft ter voorbereiding een interne werkgroep opgericht om snel met organisatiebrede en afgestemde input te komen. De uitkomsten van de werkgroep dienen eveneens ter voorbereiding en positiebepaling van het NCSC om toegerust te zijn op de toename. Vanuit de operationeel coördinerende rol adviseert het NCSC de NCTV, als stelselverantwoordelijke, over het omgaan met de groei en wordt gezamenlijk, vanuit beider rol, opgetrokken in het met externe partners verder brengen van de gewenste inrichting van het stelsel.

Rijkspartijen en CIO Rijk

In 2021 is door diverse partijen gewerkt aan een plan voor een versterkt Rijksbreed *Security Operations Center* (SOC) stelsel. Dit stelt Rijkspartijen beter in staat zelf hun digitale weerbaarheid te vergroten. Het NCSC ondersteunt en adviseert deze partijen hierbij. Omdat dit stelsel nog in de kinderschoenen staat, zal het NCSC in 2022 inzetten op de doorontwikkeling van de gezamenlijke visie en de samenwerkingsafspraken.

Vitale partners

Zichtbaarheid van het NCSC bij (nieuwe) doelgroepen is altijd van groot belang en maakt onderdeel uit van ons producten en diensten portfoliomanagement. Middels het ontwikkelen van producten en diensten die aansluiten bij de doelstelling tot het verhogen van de cyberweerbaarheid van vitale partners.

(Doelgroep)organisaties

Het verhogen van de cyberweerbaarheid van de organisatie en dat van (doelgroep)organisaties doet het NCSC middels zes paden:

1. Bijdragen aan het nationaal oefen- en testprogramma. Dit doen wij o.a. door dit jaar voorbereidingen te treffen voor ISIDOOR 2023 en deelname aan cyberoefeningen en publiek-private initiatieven zoals bijvoorbeeld de Cybersecurity Alliantie;
2. De rol van het NCSC ten aanzien van testen wordt afgestemd met NCTV en vastgelegd;
3. Doorontwikkeling van het huidige Nationaal Detectie Netwerk (NDN);
4. Door in te zetten op structurele samenwerking en het vergroten van de Economische Veiligheid van vitale infrastructuur middels Expertiseteams, draagt het NCSC bij aan het verkrijgen van inzicht in dreigingen, weerbaarheid en passende maatregelen. Hiermee zorgen wij er samen met onze partners voor dat besluitvormers in staat zijn een weloverwogen besluit te nemen bij complexe vraagstukken;
5. Het NCSC levert een bijdrage aan de doorontwikkeling van het LDS om de dekking van het stelsel te verduurzamen en snelheid van informatiedeling te verhogen;
6. Internationale samenwerking verder verstevigen o.a. door het verder ontwikkelen van EU CSIRTs Netwerk (CNW) en het leveren van een actieve bijdrage in kennis, netwerk en expertise aan beleidsvorming op EU-niveau.

Incident response

Het verder ontwikkelen van incident response is een belangrijk speerpunt voor 2022. Want des te sneller we allemaal kunnen acteren en reageren op mogelijke incidenten en gesignaleerde kwetsbaarheden, hoe digitaal veiliger wij Nederland kunnen houden. De incident response doelstellingen richten zich met name op Rijksoverheid, Vitaal en (doelgroep)organisaties, zoals in de Wbni is beschreven.

Beveiligingsadviezen

In 2021 is het NCSC begonnen met het project *Beveiligingsadviezen*. In dit project onderzoeken wij hoe we beveiligingsadviezen nog meer kunnen laten aansluiten op de behoeften en het volwassenheidsniveau van de ontvanger. Hoewel dit project nog niet is afgerond is al wel duidelijk dat een belangrijke uitkomst zal zijn dat automatisering nodig is om de steeds grotere doelgroep met een steeds grotere variëteit aan behoeften en volwassenheidsniveau goed te kunnen bedienen. Dit project zal een deel van 2022 doorlopen. Lessen die we daaruit trekken zullen worden getoetst, ontwikkeld en geïmplementeerd.

Gerichte pilot Pas-toe-leg-uit methodiek

In 2022 zal het NCSC een gerichte pilot/oefening uitvoeren om te toetsen hoe de opzet van de werkwijze en methodiek in/met de partijen in het netwerk werkt. Eind 2022 zijn de werkprocessen gereed voor de implementatiefase.

Werkwijze rondom incidenten binnen Rijksoverheid (CIO Rijk)

Met de introductie van het Besluit CIO Stelsel Rijk in 2021 heeft CIO Rijk, en afgeleid daarvan CISO Rijk, een prominente taak gekregen rondom de beheersing van security incidenten binnen het Rijk en op Rijksniveau. Deze verantwoordelijkheden en bevoegdheden dienen op een adequate manier ingepast te worden in de processen en werkwijzen rondom opschaling, incident management en crisisbeheersing. Het NCSC zal samen met CISO Rijk afspraken maken over de onderlinge taakverdeling en deze oefenen.

Afsluitend

De wereld van cybersecurity is een dynamisch en snel veranderende wereld. De opgedragen beleids- en bedrijfsvoeringdoelstellingen voor 2022 zijn dan ook ambitieus. Het NCSC ziet het als haar taak om deze te realiseren en ziet de uitvoering ervan met enthousiasme en vertrouwen tegemoet.


Verbinden
Het NCSC is het nationale CSIRT.
Voorkomen
Het NCSC bevordert digitale weerbaarheid voor Rijksoverheid en vitale processen.
Begrijpen
Het NCSC is een kennisautoriteit.

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

februari 2022