Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Jaarplan 2023

Nederland digitaal veilig

Jaarplan NCSC 2023

Als nationale cybersecurity autoriteit zorgen wij voor een digitaal veiliger Nederland. Voor 2023 heeft het NCSC de volgende drie focusdoelen geformuleerd:

Inleiding

Algemeen

Voor u ligt het jaarplan 2023 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 opdrachtgever en eigenaar bepalen de kaders waarbinnen het NCSC haar taken en activiteiten uitvoert en stellen jaarlijks beleids- en bedrijfsdoelen op. Het NCSC is, als de aangewezen uitvoeringsorganisatie, gevraagd invulling te geven aan de doelstellingen. Het resultaat leest u in dit jaarplan.

Opbouw van het jaarplan

Het jaarplan bestaat uit twee hoofdstukken. In hoofdstuk 1 wordt het wettelijk kader beschreven. In hoofdstuk 2 zijn deze vertaald naar doelstellingen voor 2023. Dit hoofdstuk biedt eveneens inzicht in de taakuitvoering door het NCSC binnen de gestelde kaders.

Het NCSC in 2023

Het NCSC werkt aan een digitaal veiliger Nederland. De digitale infrastructuur is van levensbelang: voor het betalingsverkeer, schoon water uit de kraan en om de voeten droog te houden. Wij **begrijpen** digitale kwetsbaarheden en **verbinden** partijen door het delen van kennis en informatie. Hiermee beperken we dreigingen en **voorkomen** we maatschappelijke schade.

Onze primaire doelgroepen zijn vitale organisaties en de Rijksoverheid. Wij ondersteunen hen bij het treffen van maatregelen om cyberdreiging tegen te gaan of bij het herstellen van incidenten. Zodat zij de continuïteit van hun dienst kunnen waarborgen. De komende jaren neemt het aantal doelgroepen voor het NCSC stevig toe als gevolg van de nieuwe Europese richtlijn Netwerk- en Informatiebeveiliging (NIB2-richtlijn).

Naast de NIB2-richtlijn is in 2022 ook de Nederlandse Cybersecurity Strategie (NLCS) vastgesteld. Hierin krijgt het NCSC onder andere de opgave om als nationaal Computer Security Incident Response Team (CSIRT) op te treden. Aankomend jaar wordt daartoe een flinke investering gedaan in de (verdere) ontwikkeling van initiatieven zoals een incidentenregister, Cyclotron en publiek-private afspraken rondom het beter notificeren van slachtoffers van cyberaanvallen en mogelijke doelwitten.

Tot slot is in 2022 ook gekozen voor het samengaan van het NCSC, CSIRT-DSP en DTC. Deze organisaties worden op termijn samengevoegd tot één nationale cybersecurity autoriteit. Deze ambities vormen de basis voor een nieuwe werkwijze en een flink veranderprogramma.

Al deze ontwikkelingen, van binnen en buiten de organisatie, vragen om een NCSC dat wendbaar, flexibel en schaalbaar is. Een NCSC dat ondanks de verschillende ontwikkelingen in staat is haar wettelijke taken goed en zorgvuldig uit te voeren. Dit jaarplan is ambitieus, maar gebalanceerd, en bouwt door op de vele stappen die zijn gezet in 2022 en de ervaring die daarbij is opgedaan.

Hoofdstuk 1

Wettelijke taken

Het NCSC voert de taken uit zoals opgenomen in de Wet beveiliging netwerk- en informatiesystemen (Wbni) of voortvloeien uit de implementatie van de NIB-richtlijn.

Wettelijke kerntaken

Deze taken zijn bedoeld 'ter voorkoming of beperking 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.
- 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 Respons Team (CSIRT).

Wanneer het NCSC tijdens het uitvoeren van haar wettelijke taak op informatie stuit die ook relevant is voor andere, niet vitale partijen, meldt zij dit bij een schakelorganisatie of – in dringende gevallen – direct bij de betreffende partij. Het NCSC adviseert daarnaast ook het algemene publiek 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 CSIRT's adequaat te informeren, zeker op Europees niveau.
- Het NCSC heeft een specifieke opdracht voor het mede tot stand doen komen van het Nationaal Detectie Netwerk (NDN), Landelijk Dekkend Stelsel (LDS) en de samenwerking met het Digital Trust Centre (DTC) van het ministerie van Economische Zaken en Klimaat (EZK).

De wettelijke taken geven de kaders aan waarbinnen het NCSC haar doelen voor 2023 bepaalt.

Hoofdstuk 2

Doelstellingen

In het jaarplan 2023 heeft het NCSC drie focuspunten: verhogen van de weerbaarheid, incident response en voorbereiden op de toekomst.

Verhogen weerbaarheid

Als wij gezamenlijk de Nederlandse (en Europese) cyberweerbaarheid verhogen, zijn wij beter opgewassen tegen aanvallen van buiten. Hieronder staan een 8-tal manieren waarop het NCSC in 2023 bijdraagt aan de cyberweerbaarheid van organisaties en haar doelgroepen.

Oefenen

Dit jaar organiseert het NCSC samen met de NCTV de nationale cybercrisisoefening ISIDOOR. In deze oefening wordt met een groot aantal publieke en private organisaties het nieuwe LCP-Digitaal geoefend.

Testen

Het NCSC werkt, samen met CIO Rijk, aan een gezamenlijke testkalender binnen de Rijksoverheid. Ook formuleert het NCSC een aanpak voor structurele inzet van testen binnen de vitale sectoren.

Nationaal Detectie Netwerk (NDN)

Dit jaar staat in het teken van het robuust maken van de NDN-infrastructuur en de inzet hiervan bij externe dienstverlening (zoals CTI en dreigingsanalyses). Ook worden, in samenwerking met CIO Rijk, het resterende deel van de NDN-partijen binnen het Rijk aangesloten.

Expertiseteams

Het NCSC neemt deel aan gemiddeld drie geprioriteerde expertiseteams. Dit zijn teams bestaande uit rijksambtenaren, die in opdracht van de taskforce Economische Veiligheid digitale vraagstukken over nationale veiligheid beantwoorden. Het NCSC heeft de rol van procesbegeleider en inhoudelijk adviseur.

Landelijk Dekkend Stelsel (LDS)

Het NCSC zorgt vanuit haar operationeel coördinerende rol voor een efficiënt en effectief LDS. Hiervoor wordt een blauwdruk opgesteld met stelselafspraken en randvoorwaarden.

Internationaal

Het NCSC levert een actieve bijdrage aan EU-beleidsvorming vanuit kennis, netwerk en expertise. Dit doen we door in 2023 te investeren in internationaal relatiemanagement, capaciteitsopbouw en strategisch leverancier- en relatiemanagement.

Cyclotron

In 2023 worden de eerste stappen gezet om te komen tot het samenwerkingsplatform Cyclotron. Via dit platform zijn publieke en private partners in staat informatie via een vertrouwde digitale omgeving onderling te delen. Parallel aan dit traject loopt het opzetten van een overlegstructuur met de CICC-partners en het verder uitwerken van de samenwerking met I&V partners.

Versterkt SOC Stelsel Rijk (VSSR)

CIO Rijk heeft tot doel om te komen tot een versterkt SOC stelsel Rijk. Het NCSC draagt bij aan de uitvoering van het plan omdat het programma VSSR een aanzienlijke en structurele verbetering van de digitale weerbaarheid van het Rijk moet realiseren.

Incident response

Incident response blijft een hoofdpijler voor het NCSC, ook in 2023. Want des te sneller het NCSC kan acteren en reageren op mogelijke incidenten en gesignaleerde kwetsbaarheden, hoe beter we in staat zijn om de gevolgen te beperken en andere organisaties te beschermen. In een notendop gaat Incident response over drie dingen: het voorkomen van schade, het beperken van schade en het leren van lessen (voor anderen) om beter weerbaar te worden.

Beveiligingsadviezen

In 2022 zijn belangrijke stappen gezet in het optimaliseren van het proces rond beveiligingsadviezen en het uitwisselen van informatie over kwetsbaarheden, incidenten en dreigingen. In 2023 wordt dit verder geautomatiseerd en worden beveiligingsadviezen onderdeel van het NCSC-portaal.

Pas toe of leg uit

In 2023 wordt de werkwijze ‘pas toe of leg uit’ geïmplementeerd voor adviezen waarbij een Nationaal Veiligheidsadvies Cyber (NVAC) wordt afgegeven. Binnen deze aanpak hebben doelgroepen een keuze: de (beveiligings)adviezen opvolgen, of kunnen uitleggen waarom ze een ander besluit nemen. Het proces hiervoor is samen met de doelgroepen opgesteld.

Voorbereiden op de toekomst

Tegelijkertijd is 2023 een kanteljaar naar de toekomst. Naast het uitvoeren van onze wettelijke taken bereiden wij ons voor op de implementatie van de NIB2-richtlijn en het vormgeven van de acties uit de NLCS. Vanuit de NIB2-richtlijn komt een forse groei aan doelgroepen die gebruik gaan maken van de producten en diensten van het NCSC. Dit betekent een andere manier van (samen)werken om de wettelijke taken te vervullen en producten en diensten passend te maken. Zo wordt gewerkt aan een dienstverleningsmodel dat uitgaat van schaalbaarheid, wendbaarheid en samenwerking met stelselpartners. Ook worden weerbaarheids- en dreigingsanalyses uitgevoerd voor de nieuwe sectoren. Vanuit de NLCS zet het NCSC verdere stappen om zich te verbreden tot nationaal CSIRT en wordt de integratie van NCSC, DTC en CSIRT-DSP verder vormgegeven.

Afsluitend

De wereld van cybersecurity is een dynamisch en snel veranderende wereld. De opgedragen beleids- en bedrijfsvoeringsdoelstellingen voor 2023 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.
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 2023