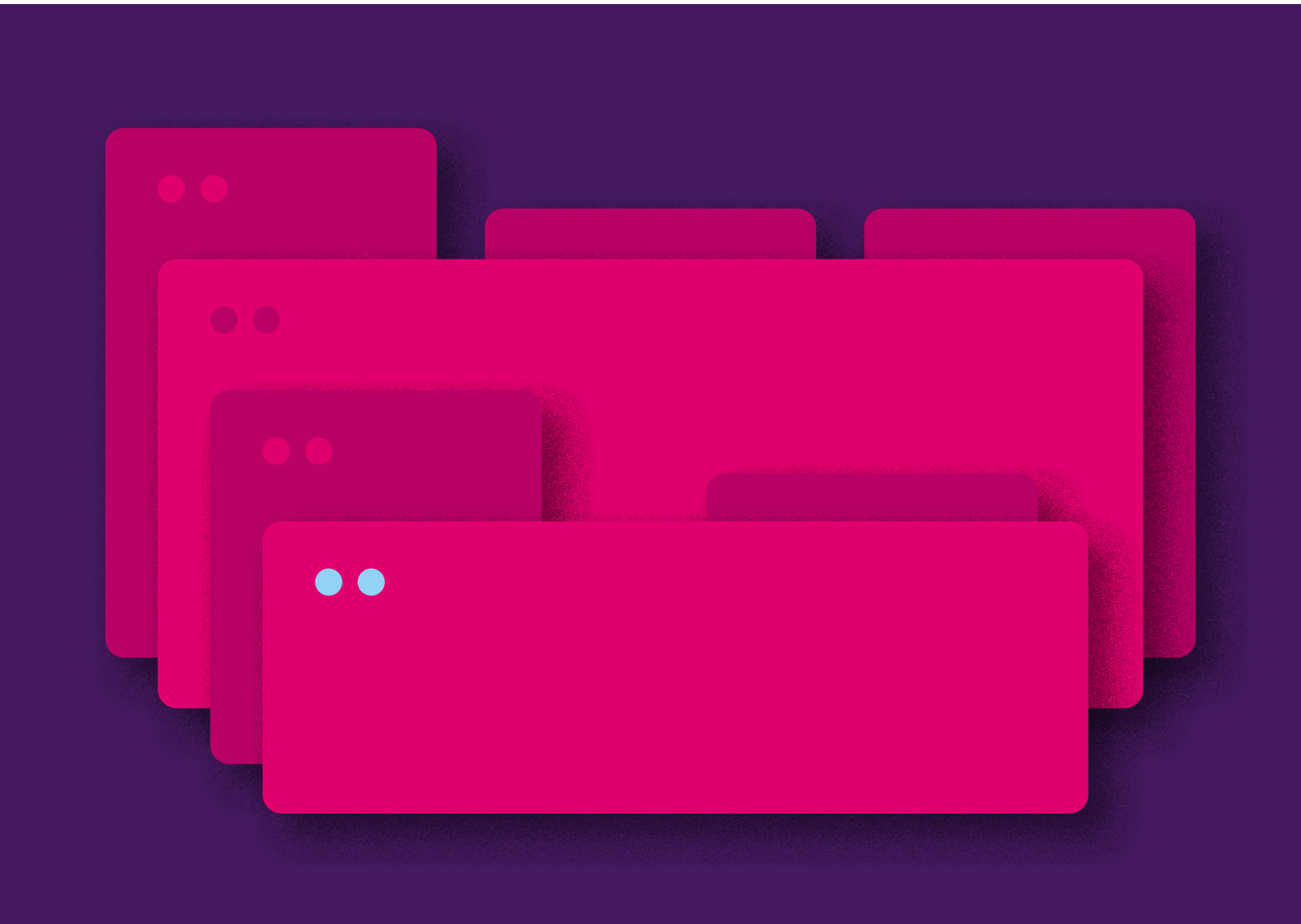
Jaarplan 2024

Nederland digitaal veilig



Het jaarplan in één oogopslag

Wij zijn het Nationaal Cyber Security Centrum.
Als nationale cybersecurity autoriteit werken wij aan een digitaal veiliger Nederland. Voor 2024 hebben wij de volgende drie focusdoelen geformuleerd.

Voorwoord

Onze samenleving is meer dan ooit afhankelijk van de digitale infrastructuur. Met de snelle opkomst van kunstmatige intelligentie, de toenemende cybercriminaliteit en de inzet van digitale middelen bij geopolitieke dreigingen, is cybersecurity in 2024 van fundamenteel belang voor de Nederlandse samenleving en economie. Bij het NCSC werken wij aan een digitaal veiliger Nederland. Wij *begrijpen* digitale kwetsbaarheden en *verbinden* partijen door het delen van kennis en informatie. Hiermee beperken we dreigingen en *voorkomen* we maatschappelijke schade.

Het NCSC versterkt de digitale weerbaarheid van de Nederlandse samenleving. Wij doen dit door vitale organisaties en Rijkoverheid te ondersteunen bij het treffen van maatregelen om cyberdreiging tegen te gaan of bij het herstellen van incidenten. Ook adviseren wij, gezamenlijk met het Digital Trust Center (DTC) en het CSIRT-DSP, het bedrijfsleven bij diverse cybersecurity-vraagstukken. Zodat alle organisaties in Nederland de continuïteit van hun diensten kunnen waarborgen.

Door de komst van de Europese Network and Information Security Directive (NIS2-richtlijn), die eind 2024 in werking treedt, neemt het aantal doelgroepen van het NCSC dit jaar fors toe. Dit vraagt van ons een nieuwe werkwijze. Een van onze centrale opgaves dit jaar is daarom het schaalbaar maken van onze taken, activiteiten en dienstverlening. Naast de uitbreiding van de doelgroepen, groeit ook ons takenpakket. Als gevolg van de Nederlandse Cybersecurity Strategie (NLCS) en de NIS2-richtlijn wordt het NCSC benoemd als *het* Nationaal Computer Security Incident Response Team (CSIRT) van Nederland. In 2024 worden hiertoe nationale en sectorale stelselafspraken gemaakt zodat wij, eind dit jaar, in staat zijn als Nationaal CSIRT, incident respons en SPOC[1]-taken uit te voeren. De implementatie van de NIS2 zal niet in één jaar gereed zijn. De komende jaren zijn stevige investeringen in het NCSC noodzakelijk om de wet robuust uit te kunnen voeren.

Dit jaar staat ook in het teken van de verdere integratie met het DTC en CSIRT-DSP tot één nationale cybersecurity-autoriteit. De samenwerking tussen deze drie organisaties is de afgelopen tijd al geïntensiveerd. De officiële integratie met het CSIRT-DSP vindt dit jaar plaats, waarna in 2025 ook het DTC volgt.

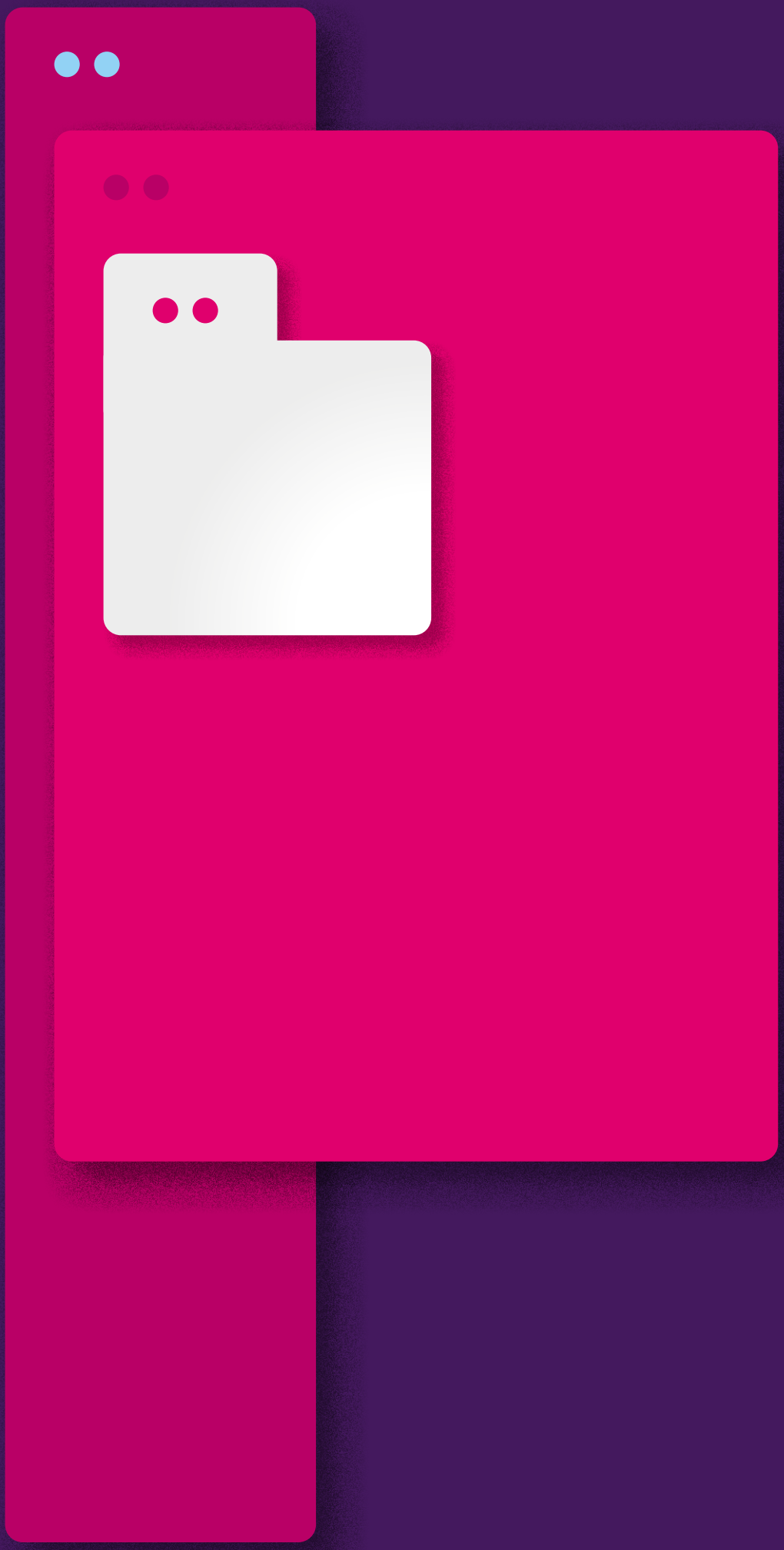
Naast deze grote veranderopgaven blijven wij ons natuurlijk focussen op onze kerndoelen: het begrijpen van nieuwe cyberdreigingen, het verbinden van organisaties binnen het cybersecuritydomein en het voorkomen van cyberaanvallen op de Nederlandse samenleving. Wij werken aan diverse publiek-private samenwerkingen waarin dreigingsinformatie wordt uitgewisseld. Ook zetten wij in 2024 grote stappen in het notificeren van alle Nederlandse slachtoffers en doelwitten van cyberdreigingen en -aanvallen.

Als ik naar dit jaarplan kijk, zie ik een grote taak voor de collega's van het NCSC. De integratie van de drie cybersecurity-organisaties, de implementatie van de NIS2-richtlijn, en de toenemende cyberdreigingen vragen om een buitengewone inzet. Vol vertrouwen in hen én onze organisatie geven wij uitvoering aan dit plan en maken we Nederland stap voor stap digitaal veilig.

Corine Schipper-Derksen
Waarnemend directeur

Over dit jaarplan
Het Nationaal Cyber Security Centrum is een uitvoeringsorganisatie van het ministerie van Justitie en Veiligheid. De plaatsvervangend Secretaris Generaal (pSG) is de eigenaar van het NCSC, de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) is opdrachtgever van het NCSC. De eigenaar en de opdrachtgever bepalen de kaders waarbinnen het NCSC zijn 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. Het jaarplan bestaat uit twee hoofdstukken, waarin het eerste hoofdstuk zal gaan over ons wettelijk kader en in het tweede hoofdstuk leest u de vertaling naar onze doelstellingen voor het aankomend jaar.

1 SPOC betekent Single Point of Contact. Dit houdt in dat het NCSC voor Nederland internationaal het aanspreekpunt is als het gaat over cybersecurity.



Hoofdstuk 1

Wettelijke taken

Het NCSC vindt zijn grondslag in de Wet beveiliging netwerk- en informatie-systemen (Wbni). Deze wettelijke basis verandert flink na de implementatie van de NIS2-richtlijn eind 2024. Deze wijzigingen zijn ook van toepassing op de taken en doelgroepen van het NCSC.

Wettelijke kerntaken

De kerntaken 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' en 'ter verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving'.

- 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 NIS2-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).

Het kan voorkomen dat het NCSC van (inter)nationale partners dreigingsinformatie ontvangt die essentieel is voor organisaties die wij op grond van de wet niet actief ondersteunen. Dit kan informatie zijn waarin een partij op korte termijn te maken krijgt met een cyberaanval, of informatie waarin een partij zich nog niet bewust is dat zij te maken hebben (gekregen) met een cyberaanval. Wij kunnen dan op grond van de Wbni contact opnemen met schakelorganisaties of de organisatie zelf om hen te waarschuwen voor de desbetreffende cyberdreiging.

Overige taken

- De digitale wereld reikt ver buiten onze landsgrenzen en raakt aan vele verschillende disciplines. Het NCSC heeft de taak van operationeel coördinator in Nederland. Dit houdt in dat het NCSC, in geval van incidenten, diverse private en publieke organisaties op basis van relevante digitale invalshoeken bij elkaar brengt. 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). Het NDN is een uniek samenwerkingsverband waarin het NCSC, de AIVD en de MIVD informatie verzamelen over digitale dreigingen en zo vroegtijdig aangesloten Rijksoverheids- en vitale partners en schakelorganisaties binnen het Landelijk Dekkend Stelsel informeert. Ook heeft het NCSC een specifieke opdracht ontvangen om het Landelijk Dekkend Stelsel (LDS) door te ontwikkelen en de samenwerking met het Digital Trust Center (DTC) van het ministerie van Economische Zaken en Klimaat (EZK) te bevorderen.

NIS2-richtlijn

Eind 2024 wordt de Europese NIS2-richtlijn van toepassing. Dit betekent een uitbreiding van de taken van het NCSC en de doelgroepen die wij bedienen. De effecten daarvan zijn naar verwachting dit jaar al zichtbaar, maar zal meer zichtbaar worden in de jaren daarna.

Hoofdstuk 2

Doelstellingen

In het jaarplan 2024 heeft het NCSC drie focuspunten: de veranderopgaven, het verhogen van weerbaarheid en het versterken van incident response.

Veranderopgaven

2024 wordt een belangrijk jaar in de bredere doorontwikkeling van de organisatie én het cybersecuritystelsel. Verschillende opgaven komen dit jaar samen tot uitvoering.

NIS2-richtlijn

Om eind 2024 uitvoering te geven aan de NIS2-richtlijn wordt als nationaal CSIRT een meld- en registratiefunctionaliteit ingericht, zodat organisaties zich kunnen registreren als NIS2-entiteit en incidentmeldingen kunnen doen. Daarnaast is de mogelijkheid gerealiseerd om incident respons en SPOC-taken uit te voeren als nationaal CSIRT en sectoraal CSIRT voor specifieke sectoren. Tot slot wordt een klantcontactpunt opgezet en worden nieuwe doelgroepen middels communicatiecampagnes geïnformeerd over de aanstaande veranderingen.

Schaalbare dienstverlening

Met de inwerkingtreding van de NIS2-richtlijn wordt de doelgroep van het NCSC ongeveer 30 keer groter, terwijl dat voor de organisatie zelf niet geldt. Diat vraagt van het NCSC om op een meer schaalbare manier de dienstverlening te leveren. Deze schaalbaarheid resulteert in snellere, betere en passendere producten. Hiertoe wordt onder andere een digitaal portaal gelanceerd. Doelgroepen kunnen zich geautomatiseerd registreren bij het NCSC en zijn in staat zelf (gepersonaliseerde) producten en diensten af te nemen.

Netcode

De Netcode is Europese regelgeving om de Europese elektriciteitsnetwerken weerbaarder te maken, ook tegen digitale dreigingen. Het ministerie van EZK heeft het NCSC gevraagd om de CSIRT-taken uit de Netcode uit te voeren voor elektriciteitspartijen. Het NCSC werkt aan de uitvoeringstoets en bereidt zich voor om in 2024 invulling te kunnen geven aan deze taken.

De vernieuwde organisatie

In 2024 wordt verder uitvoering gegeven aan het transitieprogramma van de ministeries van JenV en EZK. Aankomend jaar bereidt het NCSC zich voor op de inbedding van CSIRT-DSP, waarna DTC in 2025 volgt. Samen vormen zij één vernieuwde nationale cybersecurityorganisatie die in 2026 vier rollen kan vervullen. De nieuwe organisatie is het **nationaal CSIRT** en het centrale **kennis- en adviescentrum** van Nederland op het gebied van digitale weerbaarheid en cybersecurity. Vanuit die rollen is de organisatie verantwoordelijk voor het bevorderen van een weerbaar digitaal Nederland en het leveren van incident respons. Dit doet zij door als **uitvoeringscoördinator** (rand)voorwaarden te creëren waarbinnen alle organisaties in Nederland hun digitale weerbaarheid op orde kunnen brengen en houden. De nieuwe organisatie adviseert en ondersteunt alle organisaties in Nederland waar mogelijk en stimuleert, organiseert en faciliteert publiek-private en internationale samenwerking. Daarnaast fungeert de nieuwe organisatie als **sectoraal CSIRT** voor aangewezen sectoren.

Verhogen van weerbaarheid

Als wij gezamenlijk de Nederlandse (en Europese) cyberweerbaarheid verhogen, zijn wij beter opgewassen tegen aanvallen van buiten. In 2024 draagt het NCSC hier onder andere op de volgende manieren aan bij.

Landelijk Dekkend Stelsel (LDS)

Het Landelijk Dekkend Stelsel (LDS) is een stelsel waarin het NCSC en DTC samenwerken met publieke- en private organisaties om informatie en kennis uit te wisselen. Het doel van deze kennisuitwisseling is digitale ontwrichting te voorkomen en Nederland cyberweerbaarder te maken. Het NCSC fungeert in het LDS als de spin in het web en deelt via andere schakels de beschikbare informatie. In 2024 draagt het NCSC bij aan dit programma door het verder uitwerken en uitvoeren van het bouwplan.

Versterken SOC Stelsel Rijk (VSSR)

De Centrale SOC-voorziening (CSOC) is een expertisecentrum dat Rijksorganisaties ondersteunt bij monitoring, detectie en SOC-taakuitvoering. In 2024 worden de producten en diensten van het CSOC verder doorontwikkeld en de organisatorische overdracht aan het NCSC voorbereid. Dit gebeurt in opdracht van het ministerie van BZK (CIO Rijk). Het programma moet een aanzienlijke en structurele verbetering van de digitale weerbaarheid van het Rijk realiseren.

Cyclotron

Het programma Cyclotron richt zich op het verstevigen van de publiek-private samenwerking. Het doel is de realisatie van een platform waarbinnen informatie over digitale incidenten en dreigingen gedeeld kunnen worden. Hiermee wordt het mogelijk om gezamenlijk analyses te creëren en een dieper begrip te ontwikkelen voor methoden, technieken en doelstellingen van cyberaanvallers.

Anti-Phishing Shield (APS)

Het Anti-Phishing Shield is een verzamelnaam voor een set maatregelen om phishing tegen te gaan. Hierbij wordt een meld- en analysepunt ingericht waar iedere Nederlander een verdachte e-mail naar toe kan sturen. Vervolgens wordt een analyse gedaan of de URL in de e-mail daadwerkelijk phishing betreft, en volgt een zwarte lijst van phishing-domeinen. De actieve waarschuwing moet het slachtofferschap van phishing en daaropvolgende delicten tegengaan. Onder de beleidsverantwoordelijkheid van DGRR, geeft het NCSC invulling aan de rol van analysepartij.

Adviesportfolio

Het NCSC werkt in 2024 naar een advies- en kennisportfolio van hoge kwaliteit, praktisch en schaalbaar. Met zowel eigen kennis als kennis van andere deskundige organisaties, zoals inspecties en veiligheidsdiensten. Dit advies- en kenniscentrum levert toepasbare preventieadviezen, handreikingen en instrumenten om de digitale weerbaarheid van organisaties te vergroten. Het NCSC voert ook toegepast en fundamenteel onderzoek uit of laat onderzoek uitvoeren om de kennispositie op peil te houden en in praktische kennisproducten te delen.

Incident response

Het bieden van adequate incident response blijft een belangrijk onderwerp voor het NCSC. 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. Dit jaar staat onder meer in het teken van de ontwikkeling tot Nationaal CSIRT, waarbinnen het reageren op incidenten een belangrijk onderdeel is.

Doelwit- en slachtoffernotificatie

In 2024 wordt door een team van het NCSC, DTC en CSIRT-DSP gewerkt aan het vernieuwen en volledig automatiseren van het notificeren van doelwitten en slachtoffers. Dit betekent dat publieke en private organisaties altijd geïnformeerd worden als zij doelwit zijn van een cyberdreiging of slachtoffer zijn geworden van een cyberaanval. Door deze gestandaardiseerde en geautomatiseerde wijze worden organisaties snel en vroegtijdig geïnformeerd en wordt de Nederlandse samenleving beter weerbaar tegen de toenemende cyberdreigingen.

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 2024