Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Stand van de uitvoering 2022

26 april 2023

Inhoud

Voorwoord

Geachte lezer,

Graag neem ik u mee in de eerste Stand van de uitvoering van het Nationaal Cyber Security Centrum (NCSC). Wij zijn de cybersecurityautoriteit van Nederland. Sinds 2012 werken we samen met onze partners aan een digitaal veilig en weerbaar Nederland. Dat is belangrijk voor bijvoorbeeld onze infrastructuur, veilig betalingsverkeer, schoon drinkwater uit de kraan en om de voeten droog te houden.

Het NCSC is een zelfstandige taakorganisatie van het ministerie van Justitie en Veiligheid. De governance van het ministerie van Justitie en Veiligheid is ingericht door middel van het sturingsmodel JenV. Het sturingsmodel JenV biedt heldere kaders voor sturen, beheersen, toezicht houden en verantwoorden. Het sturingsmodel kent drie rollen. Die van opdrachtnemer, opdrachtgever en eigenaar. Gezamenlijk vormen deze drie partijen de driehoek. Het NCSC is binnen onze driehoek opdrachtnemer. De beleidsverantwoordelijkheid voor cybersecurity ligt bij onze opdrachtgever. Dat is de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV). De Plaatsvervangend SG Justitie en Veiligheid is eigenaar van het NCSC.

Begrijpen, verbinden en voorkomen zijn de leidende principes in het werk van het NCSC. We **begrijpen** de kwetsbaarheden en dreigingen in het digitale domein. We identificeren en duiden risico's en trends. De kennis die we verzamelen is breed toegankelijk. We **verbinden** partijen, kennis en informatie. Als overheidsorganisatie zijn we de verbindende schakel in een netwerk van nationale en internationale partners. We **voorkomen** maatschappelijke schade en beperken dreigingen, bieden vakkundige ondersteuning en advies en bieden concreet handelingsperspectief.

Het NCSC heeft een breed pallet aan producten, waaronder onderzoeken, analyses en beveiligingsadviezen. In geval van een crisis staan we 24/7 paraat. Onze cybersecuritywerkzaamheden voeren we niet alleen uit. Dit doen we met een uitgebreid netwerk van partners. Door effectief samen te werken brengen we cyberdreigingen in kaart, analyseren deze en adviseren en informeren we organisaties in Nederland, zodat zij de juiste maatregelen kunnen treffen. Zo stellen we Nederland in staat om digitaal weerbaar te zijn. Samen maken we Nederland digitaal veilig.

Op dit moment komt er veel op het NCSC af. Zo zorgt nieuwe wet- en regelgeving onder andere voor een forse uitbreiding van het aantal organisaties en bedrijven dat we ondersteunen. Ook krijgen we te maken met nieuwe opdrachtgevers en afnemers van onze producten en diensten. Verder gaat het NCSC de komende tijd integreren met het DTC en CSIRT-DSP van het ministerie van Economische Zaken. De transitie naar deze nieuwe nationale cybersecurityorganisatie en de genoemde ontwikkelingen vragen veel van onze medewerkers en organisatie.

Uitdagingen en dilemma's
Bij de uitvoering van onze werkzaamheden lopen we, net als andere uitvoeringsorganisaties, tegen uitdagingen en dilemma's aan. In deze stand van de uitvoering vertellen we hoe we hiermee omgaan, wat we zelf doen, maar ook wat er volgens het NCSC nodig is om ons werk nog beter te kunnen uitvoeren om zo samen Nederland digitaal veilig te maken en te houden. In deze Stand van de uitvoering schetsen we onze uitdagingen en dilemma's aan de hand van de volgende onderwerpen:

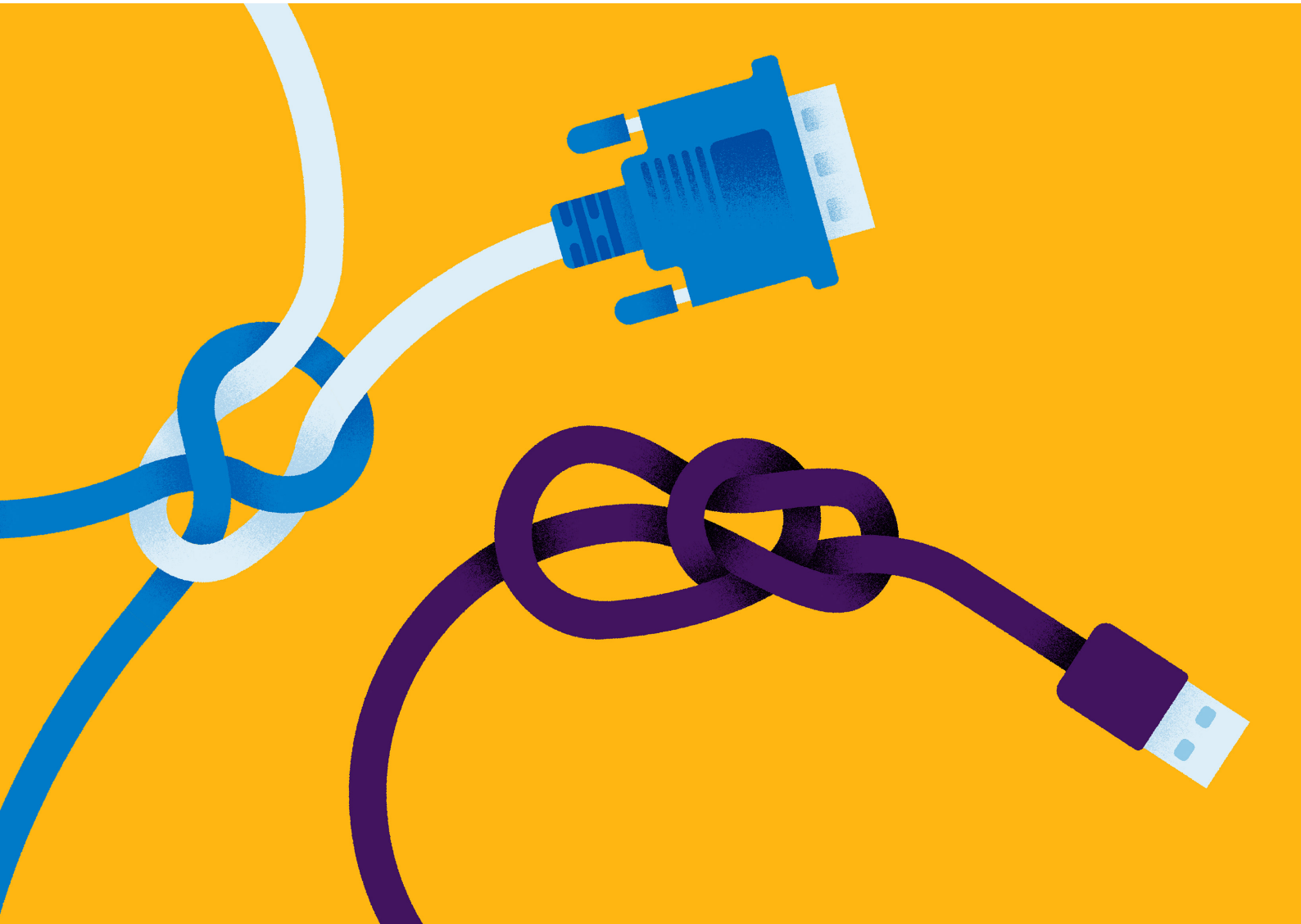
- Toename complexiteit
- Gegevensdeling
- Arbeidsmarkt
- Samenwerking

We hopen zo een goed beeld te geven van onze werkzaamheden en de uitdagingen waar we voor staan. Mocht u vragen hebben, dan nodigen we u van harte uit om hierover met ons in gesprek te gaan.

Met hartelijke groet,

Hans de Vries
Directeur NCSC

1. Toename complexiteit



Internationaal speelveld, meer wetgeving

In de Staat van de uitvoering 2022 is opgenomen dat de complexiteit van wetgeving en de stapeling van nieuw beleid met afstand het grootste knelpunt is voor burgers, ondernemers en uitvoeringsorganisaties. Het NCSC herkent dit knelpunt ook binnen het speelveld waarin wij opereren. We doen ons werk in een complex en dynamisch landschap met een sterke Europese en mondiale component. Met name de Europese component leidt in toenemende mate tot een fundamentele verandering van het speelveld. Europa is leidend in de nieuwe wetgeving op het cyber(security)domein en dit heeft duidelijk een steeds grotere impact op burgers en bedrijven. De wereld verandert snel en ingrijpend door toenemende (afhankelijkheid van) digitalisering en automatisering. Hierdoor wordt cybersecurity nog belangrijker.

Meer beleid, meer regeldruk

In dit complexe speelveld krijgt het NCSC te maken met veel nieuwe wetten en/of beleidsinitiatieven vanuit Brussel. Die nieuwe wetgeving en beleid zorgen in meer of mindere mate voor meer druk op onze uitvoering. Een goed voorbeeld hiervan is de nieuwe Network and Information Security-Directive 2 (NIS2). Minder bekend, maar ook van invloed zijn de mededelingen rondom cyber defense, het Europese Cyber Shield, de Cyber Resilience Act en de recent aangekondigde Cyber Solidarity Act. Alle plannen die onder deze beleidsinitiatieven worden aangekondigd dienen, onder andere door het NCSC, te worden omgezet in concrete acties. Deze opeenstapeling van nieuw beleid heeft impact op de uitvoering.

Het NCSC signaleert daarnaast een groeiende regeldruk bij bedrijven die voortvloeit uit zowel sectorspecifieke wetgeving als ‘algemene’ wetgeving, zoals de CER-richtlijn, NIS2 of de AVG. Een voorbeeld van sectorspecifieke wetgeving is de Digital Operational Resilience Act (DORA). Deze Europese wet uit 2020 legt extra regeldruk op de financiële sector onder meer door een aparte meldplicht voor incidenten, bovenop de meldplicht uit de NIS2. Een ander voorbeeld is de Electricity Network Code(s) die ook een eigen meldplicht kent voor elektriciteitsproducenten.

Het lukt de Europese Commissie tot op heden niet om de verschillende verplichtingen onder elkaar te zetten en daarmee inzichtelijk te maken welke organisaties aan welke regels moeten voldoen.

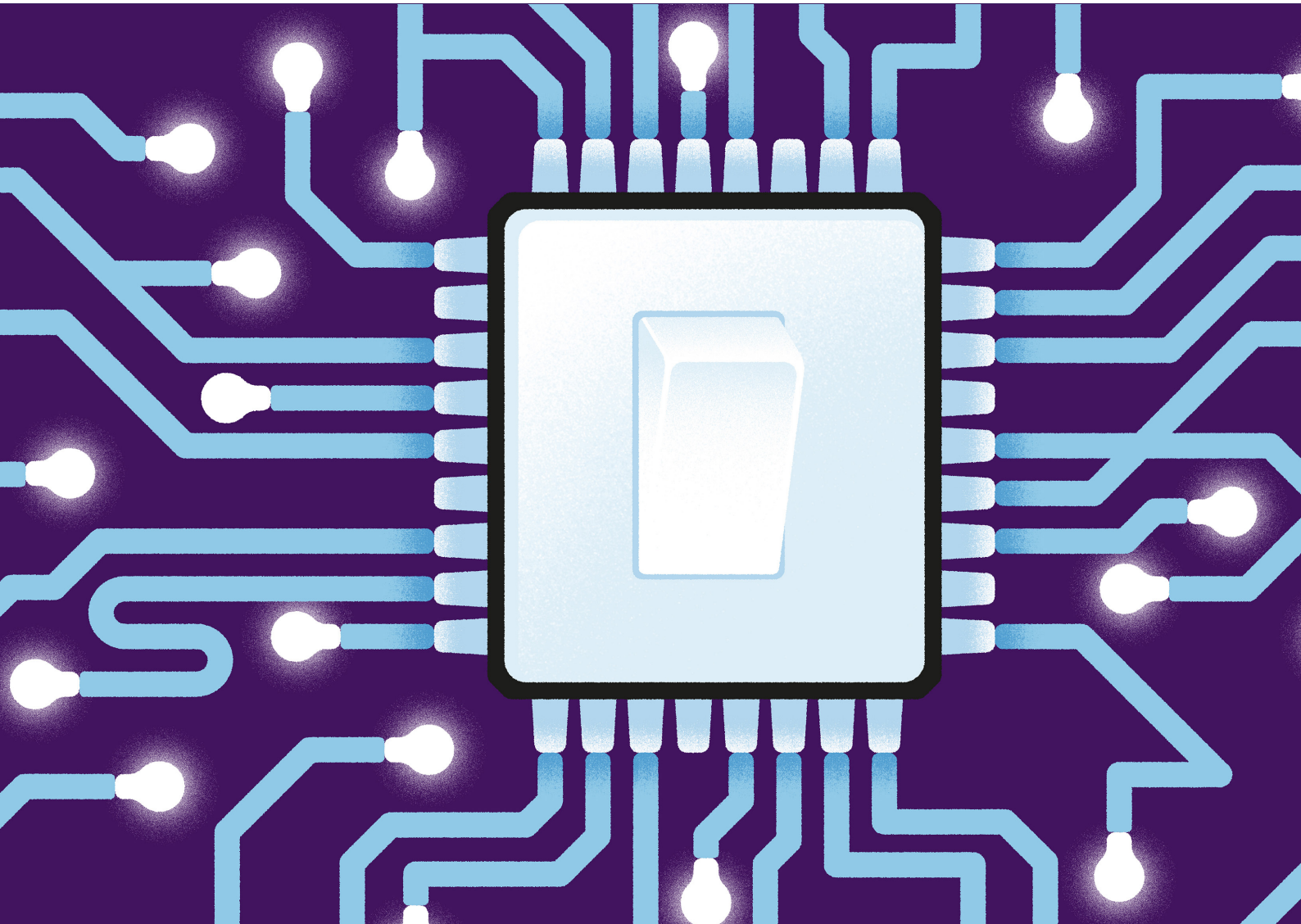
Uitvoering onder druk

De Europese en internationale ontwikkelingen op het gebied van wet- en regelgeving ten aanzien van cybersecurity vormen een risico voor de uitvoering van werkzaamheden door het NCSC. Die ontwikkelingen kunnen in toenemende mate leiden tot verschillende, uiteenlopende en soms zelfs tegenovergestelde uitkomsten die voor het NCSC tot ongewenste situaties en/of onuitvoerbare opdrachten kunnen leiden. De uitvoering van het NCSC komt onder druk te staan door de snelheid waarmee nieuwe beleidsinitiatieven worden genomen zonder dat voldoende tijd wordt genomen om initiatieven integraal door te denken en met elkaar in overeenstemming te brengen. Een voorbeeld hiervan is de EU-inzet om de samenwerking tussen civiele en militaire structuren te bevorderen (cyber defense communication). Dit beleidsvoornemen is in november 2022 uitgebracht en moet al in juni 2023 worden vastgesteld. Dat is extra complex in een werkveld, waarin capaciteit beperkt voorhanden is. Tenslotte merkt het NCSC op dat een uitvoeringstoets tot op heden geen onderdeel uitmaakt van het Europese wetgevingsproces.

Behoefte aan uitvoerbaar beleid

In algemene zin is het belangrijk om bij de totstandkoming van beleid of wetgeving de uitvoerbaarheid ervan voldoende in ogenschouw te nemen. Voor het uitvoeren van beleid en wetgeving is beschikbare of benodigde capaciteit uiteraard een belangrijk aspect. Op nationaal niveau worden, onder andere met de introductie van het Beleidskompas, al waardevolle stappen gezet. Op Europees niveau lijkt aandacht voor de uitvoerbaarheid van beleid of wetgeving vooralsnog onderbelicht. Het NCSC pleit voor harmonisatie van wetgeving, waardoor regeldruk op bedrijven en organisaties vanuit algemene en sectorspecifieke wetgeving wordt verminderd.

2. Gegevensdeling



Juridisch kader NCSC

Om ons werk goed te kunnen doen, moet het NCSC gegevens kunnen delen met anderen. Zowel nationaal als internationaal. Het juridisch kader waarbinnen het NCSC opereert, en dus ook gegevens deelt, is de Wet Beveiliging Netwerk- en informatiesystemen (Wbni). De Wbni is sinds 9 november 2018 van kracht en regelt de wettelijke taken van het NCSC op het gebied van cybersecurity. Doel van de Wbni is de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en zo maatschappelijke ontwrichting te voorkomen.

Primair heeft het NCSC de taak om vitale aanbieders en organisaties binnen de rijksoverheid te informeren en adviseren over digitale dreigingen en incidenten. Het NCSC beschikt regelmatig ook over informatie over digitale dreigingen en/of incidenten die relevant is voor andere organisaties. Bijvoorbeeld voor distributeurs van voedselwaren, politieke partijen, energieleveranciers, softwarebedrijven of containeroverslagbedrijven. Vanwege beperkingen in de Wbni kon het NCSC die informatie niet altijd verstrekken aan die andere organisaties.

Wijziging Wbni was noodzakelijk

Om die reden is, mede op verzoek van het NCSC, de Wbni per 1 december 2022 gewijzigd. Door deze wetswijziging heeft het NCSC de mogelijkheid om in ruimere zin dreigings- en incidentinformatie te delen met zogeheten OKTT's. Dit zijn organisaties die objectief kenbaar tot taak hebben om organisaties of het publiek te informeren over dreigingen en incidenten. OKTT's fungeren als zogenoemde schakelorganisaties voor andere organisaties en bedrijven. Hun rol is om organisaties en hun achterban te voorzien van informatie en advies over kwetsbaarheden en cyberdreigingen. Daarnaast biedt de wijziging van de Wbni een wettelijke basis voor het NCSC om in bijzondere gevallen dreigings- of incidentinformatie rechtstreeks met andere organisaties te delen. Van een bijzonder geval is sprake als een branche geen schakelorganisatie heeft én als het informatie betreft over een serieuze dreiging of incident met mogelijk aanzienlijke gevolgen voor de continuïteit van de dienstverlening van de organisatie.

Meer wettelijke ruimte nodig

Het NCSC is blij met de recente wijziging van de Wbni. Het geeft ons meer ruimte om invulling te kunnen geven aan onze taak om Nederland digitaal veilig te houden. Toch lopen we in de praktijk nog steeds tegen situaties aan, waarbij we wel beschikken over informatie die we graag zouden willen delen met anderen, maar de huidige Wbni geen of onvoldoende ruimte biedt om dit te doen.

Zo mag het NCSC op basis van de huidige Wbni uitsluitend vertrouwelijke gegevens verstrekken als de geheimhouding van die gegevens voldoende is gewaarborgd en als die gegevens alleen worden gebruikt voor het doel waarvoor zij worden verstrekt (art. 20 Wbni). Daarnaast geldt dat we gegevens die herleid kunnen worden tot een organisatie, zonder diens instemming, alleen mogen verstrekken als dat bijdraagt aan maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer. Als laatste voorwaarde geldt dat het NCSC deze gegevens uitsluitend mag delen met OKTT's, CSIRT's, andere computercrisisteams (aangewezen bij ministeriële regeling of behorend tot een bij die regeling aangewezen categorie) en de Nederlandse inlichtingen- en veiligheidsdiensten. Hierdoor kunnen we nu geen informatie delen met internationale partners, zoals CERT's/CSIRT's buiten de EU. Meer wettelijke ruimte op dat vlak zou het uitwisselen van gegevens makkelijker en de samenwerking met internationale partners effectiever maken. Het kunnen delen van gegevens met internationale partners buiten de EU is van direct belang voor de Nederlandse digitale weerbaarheid.

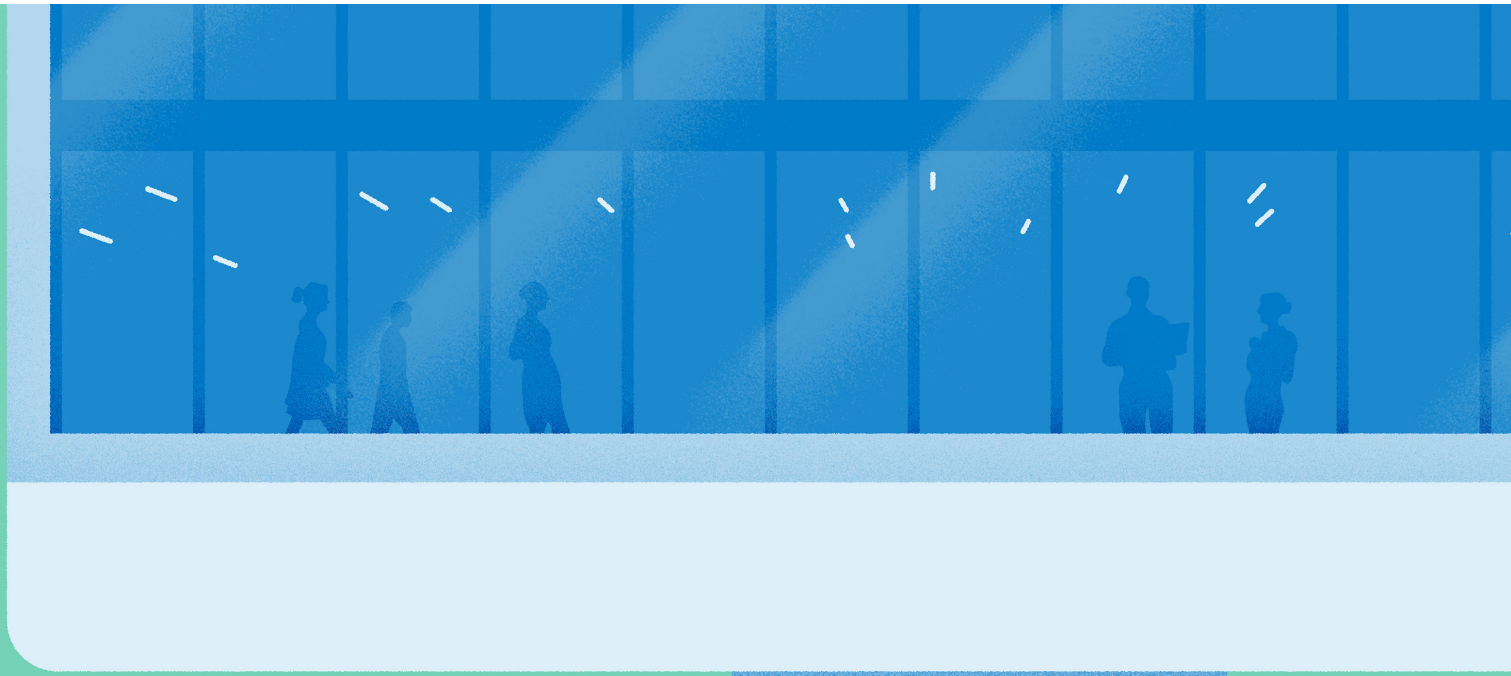
Meer beoordelings- en handelingsruimte

Dillema's rondom gegevensdeling bespreken we met de beleidsverantwoordelijke en onze opdrachtgever, de NCTV. Bij incidenten bekijken we samen welke mogelijkheden er wel zijn, passend bij de specifieke casus. Door een verruiming van de Wbni op bovenstaande punten kunnen we gelukkig al steviger invulling geven aan onze rol in een mondiaal speelveld. Hierdoor ontstaat meer professionele beoordelings- en handelingsruimte voor het NCSC om ook internationaal gegevens te delen die naar een organisatie herleidbaar zijn.

Deze verbetering neemt helaas niet alle drempels weg. Het wettelijke begrip "*tot een aanbieder (organisatie) (vertrouwelijk) te herleiden gegeven*" zorgt in de praktijk nog voor een belemmering. Het spreekt voor zich dat wij omzichtig om moeten gaan met vertrouwelijke gegevens. In de wet is naar onze opvatting onvoldoende duidelijk aangegeven wanneer daar sprake van is. In de memorie van toelichting is opgenomen dat een naam van een organisatie vertrouwelijk en herleidbaar kan zijn, terwijl juist dat soort gegevens openbaar zijn en vaak proactief worden uitgedragen door de organisaties. Hieruit is ook afgeleid dat dit geldt voor IP-adressen van organisaties, terwijl ook deze openbaar van aard zijn. De memorie van toelichting van de Wbni heeft dus enkel de herleidbaarheid beschreven, maar niet wat die gegevens dan vertrouwelijk maakt. Het zou ons in de praktijk helpen wanneer duidelijker wordt dat dergelijke (duidelijk) herleidbare gegevens alleen dan als vertrouwelijk moeten worden aangeduid, wanneer zij worden gecombineerd met andere gegevens. Gegevens zoals nog niet geopenbaarde kwetsbaarheden (openbaar CVE-nummer), zeer specifiek door een aanbieder (organisatie) gebruikte systemen, of gemaakte afspraken met de betrokken aanbieder.

Daarnaast geldt, dat de beleving in de buitenwereld voor wat betreft de aard van het IP-adres de praktijk hindert. Veelal leeft het beeld dat een IP-adres een persoonsgegeven is, omdat dit te herleiden valt naar een eindgebruiker en daarmee tot een natuurlijke persoon. Dat is niet het geval voor een organisatie als het NCSC. Voor een dergelijke herleidbaarheid is – naast het IP-adres – nog een veelheid aan andere gegevens nodig, zoals een timestamp en abonneegegevens van een internettoegangsverlener (ISP). Het NCSC heeft niet de bevoegdheid om die gegevens bij ISP's op te vragen en dat willen wij ook niet. Ons oogmerk is het veilig houden van systemen. Omdat die overal ter wereld kunnen staan en vanuit die positie onze doelgroepen (vitale en rijksorganisaties) kunnen bedreigen, is het soms noodzakelijk om ook gegevens te delen met nationale CERT's buiten de EU. De redenering dat een IP-adres altijd een persoonsgegeven betreft, maakt dat dan niet eenvoudig.

3. Arbeidsmarkt



Cybersecurityprofessionals moeilijk te vinden

Bij het NCSC werken momenteel ongeveer 270 medewerkers in dienst of op inhuurbasis. Het afgelopen jaar had het NCSC, mede door een uitbreiding van onze taken en werkzaamheden, relatief veel vacatures openstaan. Het is voor het NCSC als kleinere en specialistische uitvoeringsorganisatie niet eenvoudig om in de huidige krappe arbeidsmarkt voldoende gekwalificeerde medewerkers te vinden. Een aantal vacatures staat hierdoor langer open. Kandidaten die reageren op vacatures beschikken helaas steeds vaker niet over een passend profiel. Dat geldt zowel voor onze technische- en cybersecurityfuncties als voor meer algemene vacatures voor staf- en bedrijfsvoeringsfuncties. Daarbij komt ook dat het verloop onder ons personeel, in deze arbeidsmarkt, groter is dan enkele jaren terug.

Werven nieuw personeel en afstemming driehoek

Het NCSC zet vol in op het werven van nieuw personeel. Hierbij wordt ook gekeken naar het verbeteren van de arbeidsmarktcommunicatie en de candidate journey. Een tekort aan personeel kan gevolgen hebben voor het behalen van de doelstellingen die we ons als NCSC hebben gesteld. De voortgang op onze doelstellingen bespreken we periodiek in ‘driehoeksgesprekken’ met onze opdrachtgever, de NCTV, en de eigenaar, Plaatsvervangend SG Justitie en Veiligheid. Hierbij gaat het over de voortgang, continuïteit en eventueel te nemen maatregelen in relatie tot de opdracht aan het NCSC. Voor dat laatste is het afgelopen jaar een ‘leidraad prioritering’ opgesteld. Deze leidraad dient als instrument om in voorkomende gevallen keuzes te kunnen maken en waar nodig te herprioriteren als het gaat om de benodigde inzet van mensen en middelen voor de verschillende doelstellingen.

Mogelijkheden werving beperkt

De mogelijkheden voor het NCSC om nieuw personeel te werven en huidige medewerkers te behouden, zijn voor het NCSC helaas beperkt. Als uitvoeringsorganisatie van de Rijksoverheid zijn we gebonden aan de arbeidsvoorwaarden die voortvloeien uit de CAO Rijk. In ons organisatie- en formatiebesluit is vastgelegd welke functies en functieschalen van toepassing zijn. Hierdoor is individueel maatwerk vanuit werkgeversperspectief slechts beperkt mogelijk.

Specifiek voor onze operationele cybersecurityfuncties geldt dat onze partners, zowel publiek als privaat, allemaal in dezelfde krappe cybersecurityvijver vissen. We zien als NCSC graag dat meer studenten kiezen voor een opleiding op het gebied van cybersecurity, zodat het NCSC, maar ook onze publiek en private partners vacatures eenvoudiger kunnen invullen. Als NCSC stimuleren we de mogelijkheid om te leren en ontwikkelen. Dit doen we onder andere door stage- en leer-/arbeidsplaatsen aan te bieden aan studenten en onze proactieve inbreng in het Rijks I-traineeship programma. Door intensievere begeleiding van stagiaires, medewerkers met een leer-, arbeidsplaats en Rijkstrainees willen we de goede kandidaten aan het NCSC binden. Daarnaast heeft het NCSC contact gelegd met andere partijen om te kijken of we zo meer arbeidsparticipanten kunnen verleiden bij het NCSC aan de slag te gaan. Naast het werven van nieuwe medewerkers, is het boeien en behouden van medewerkers een belangrijk onderwerp. Zo wordt de onboarding voor nieuwe medewerkers de komende tijd flink geüpdatet en hard gewerkt aan het opstellen van leer- en ontwikkellijnen.

Digitale veiligheid en weerbaarheid staan voorop

Gezien de huidige krappe arbeidsmarkt is extra belangrijk om realistisch te zijn over de uitvoerbaarheid van de ambities van het NCSC. Hiermee doelen we op de voorziene uitbreiding van onze (wettelijke) taken en doelgroep die voortvloeit uit de implementatie van de Europese richtlijn NIS2, alsmede de extra opdrachten die voor 2023 en daarna worden voorzien. Mede daarom wordt in onze uitvoeringstoetsen voor beleidsintensiveringen en nieuwe opdrachten extra aandacht besteed aan het absorptievermogen van het NCSC. (Structureel) Beschikbare financiering voor beleidsintensivering of –ambitie is niet vanzelfsprekend om te zetten in benodigde beschikbare capaciteit. Dit gegeven zal ons naar verwachting ook de komende periode nog parten spelen, waardoor we in de gesprekken met onze opdrachtgever en eigenaar voor lastige keuzes komen te staan. De digitale veiligheid en weerbaarheid van Nederland staan daarbij voorop.

4. Samenwerking

Complexiteit, gegevensdeling en arbeidsmarkt zijn prominente thema's die in alle gesprekken over deze Stand van de uitvoering 2022 naar voren zijn gekomen. Op het gebied van samenwerking, een relatief kleiner thema, ervaren we niet direct knelpunten of dilemma's. Toch willen we hierover graag twee aandachtspunten benoemen.

Samenwerking private partijen

Het eerste aandachtspunt is marktwerking en dienstverlening door private partijen op het gebied van cybersecurity. Het NCSC verricht werkzaamheden die veelal ook worden aangeboden door commerciële dienstverleners. Onze publiek-private samenwerking met cybersecuritybedrijven is uitstekend. Vaak trekken we samen op en vullen onze diensten elkaar goed aan. Vragen over deze samenwerking die ons bezighouden zijn: Hoe houden we die goede relatie ook de komende jaren in stand? Hoe verhouden we ons als overheidsorganisatie tot de cybersecuritymarkt en hoe voorkomen we onderlinge concurrentie? Bijvoorbeeld als het gaat om het werven van personeel op een krappe arbeidsmarkt.

Samenwerking Caribisch deel van het Koninkrijk

Een ander aandachtspunt is onze inzet op, en samenwerking met, het Caribisch deel van het Koninkrijk. Inzet- en samenwerkingsmogelijkheden worden vaak beperkt, doordat wet- en regelgeving nu nog onvoldoende op elkaar aansluiten. Het NCSC geeft invulling aan samenwerking binnen de huidige juridische mogelijkheden en zet zich in om de mogelijkheden om samen te werken verder uit te breiden.

Slotwoord

Aan de hand van bovenstaande vier onderwerpen hebben we u getracht mee te nemen in de wereld van cybersecurity en de uitdagingen waar we op dit moment mee te maken hebben. Zoals u heeft kunnen lezen, liggen deze vooral op het vlak van nieuwe (Europese) wetgeving en beleid in relatie tot uitvoerbaarheid van die nieuwe regels. Het NCSC ziet de noodzaak voor scherpere cybersecuritywetgeving, maar pleit voor afstemming en harmonisering van nieuw beleid, om overbelasting van de uitvoering van cybersecurity in het publiek-private domein te voorkomen. Het behouden en werven van cybersecurityprofessionals is hierbij een belangrijke uitdaging. Als het gaat om de huidige wetgeving zien we graag dat er meer mogelijkheden komen om gegevens te delen, bijvoorbeeld met onze buitenlandse partners. Hierdoor kan het NCSC zijn belangrijke rol in een sterk internationaal speelveld duurzaam en effectief blijven invullen.

Het NCSC kijkt uit naar de komende periode waarin ze zich zo goed mogelijk zal voorbereiden op de voorziene uitbreiding van onze wettelijke taken en werkzaamheden. Ondertussen blijven onze medewerkers zich 24/7 inzetten voor een digitaal veilig en weerbaar Nederland.

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

26 april 2023