Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC Onderzoeksagenda 2023 – 2026

Doing Cybersecurity Research Together!

Voorwoord

Beste lezer,

In de hedendaagse samenleving is een gedegen kennispositie onontbeerlijk. Dit is dan ook de reden waarom kennisontwikkeling en -uitwisseling een van de pijlers van het NCSC vormt. Door onze partners in het veld en onze eigen organisatie te voorzien van de meest actuele inzichten op basis van toegepast en wetenschappelijk cybersecurityonderzoek stellen we hen in staat om zo effectief mogelijk bij te dragen aan het digitaal veiliger maken van onze maatschappij. Kennis van het hier en nu is daarbij van groot belang, maar evenzeer is het zaak om inzicht te verkrijgen in de uitdagingen van de nabije en verre toekomst. Dat biedt namelijk de mogelijkheid om ons tijdig voor te bereiden op de zaken die op ons afkomen, maar schept ook inzicht in de kansen die er liggen om de gezamenlijke toekomst mede vorm te geven. Dat dit geen eenvoudige taak is, is evident. Er zijn weinig onderwerpen die zich zo snel ontwikkelen als cybersecurity.

Deze snelle ontwikkeling van het vakgebied zie je ook terug in de evolutie die de NCSC onderzoeksagenda heeft doorgemaakt. Waar de vorige versie een aantal afzonderlijke thema's agendeerde, wordt deze nieuwe agenda vormgegeven rond het inzicht dat cybersecurity vanuit meerdere vakgebieden onderzocht kan worden. Het NCSC promoot en werkt eraan om de samenwerking tussen diverse vakgebieden te versterken, door onder andere ontwikkelingen en incidenten vanuit meerdere perspectieven te onderzoeken. Dit maakt cybersecurityonderzoek er niet eenvoudiger op, maar zal uiteindelijk leiden tot het maken van de juiste keuzes voor de inzet van mensen en middelen. Zeker in deze roerige tijden kunnen wij ons niet permitteren om slordig met deze schaarse bronnen om te gaan.

De NCSC onderzoeksagenda 2023-2026 vormt een essentieel element in de bestendiging van het NCSC als gezaghebbend kennis- en expertisecentrum op het gebied van cybersecurity binnen Nederland. Vanwege de genoemde multidisciplinariteit is de wederzijdse kruisbestuiving van verschillende onderzoeksdisciplines van groot belang. Ik beveel deze nieuwe agenda dan ook van harte aan en nodig alle partijen uit om de samenwerking met onze onderzoekers op te zoeken.

Deze onderzoeksagenda geeft een voorproefje van hetgeen er voor de komende jaren op de planning staat. De agenda zelf zal 18 en 19 oktober 2022 officieel worden gepresenteerd op de ONE Conference in Den Haag. Dat is bij uitstek de gelegenheid om met de onderzoekers van het NCSC in gesprek te gaan. Juist door de handen ineen te slaan zullen we in staat blijken om de aanwezige onderzoekskracht in ons land te bundelen en aansprekende resultaten te boeken. Uiteindelijk zorgt dit ervoor dat wij gezamenlijk bijdragen aan een veiligere digitale samenleving. Ik wens iedereen veel leesplezier toe en kijk uit naar een vruchtbare samenwerking.

Birgit Dewez
Hoofd a.i. Kennisuitwisseling
Nationaal Cyber Security Centrum

Introductie

NCSC en het onderzoeksteam

Het NCSC richt zich op het **begrijpen** van kwetsbaarheden en dreigingen in het digitale domein, het **verbinden** van partijen, kennis en informatie en het **voorkomen** van maatschappelijke schade en beperken van dreigingen. Hiervoor werken wij ook intensief samen met diverse partners. Het onderzoeksteam van het NCSC draagt bij aan deze taken door wetenschappelijke ontwikkelingen op deze gebieden te duiden en relevante onderzoeken uit te voeren, uit te besteden en te begeleiden. De contactgegevens van het team vindt u op de achterzijde.

Terugblik onderzoeksagenda 2019 - 2022

In 2019 heeft het NCSC de eerste onderzoeksagenda uitgebracht die richting gaf aan ons werk van de afgelopen jaren. Binnen de thema's crisismanagement, risicomanagement, techniek en strategische en sociale aspecten hebben we tientallen onderzoeken uitgevoerd, begeleid en gesteund met financiering en expertise. Een deel hiervan vindt u terug op onze website. De onderzoeksagenda heeft ons in staat gesteld om op vele terreinen onze kennis van cybersecurity uit te bouwen en te delen met partners.

Een aantal van de mooie resultaten vormen input voor verder onderzoek, organisatieveranderingen en publieke aandacht op conferenties en in wetenschappelijke publicaties en vakbladen. Zo hebben wij bijgedragen aan de toegenomen aandacht voor Software Bill of Materials (SBOM), lieten we een studie uitvoeren naar de impact van de nieuwe EU NIB2 Richtlijn op het NCSC en zijn er interessante resultaten gekomen uit de meerjarige samenwerking met TNO. Deze mooie onderzoeken vindt u ook terug op het programma van de ONE Conference 2022 op 18 en 19 oktober te Den Haag.

Bij meerdere onderzoeken hebben wij samengewerkt met diverse partners. We hebben enkelen van hen gevraagd om te reflecteren op afgelopen, huidige en toekomstige projecten. U kunt ze lezen in deze onderzoeksagenda.

Doel NCSC onderzoeksagenda 2023-2026

De NCSC onderzoeksagenda 2023-2026 geeft uitvoering aan de ambitie en wensen van het NCSC en in het bijzonder het onderzoeksteam. Hiermee geven we invulling aan de Nederlandse Cybersecurity Strategie (publicatie in oktober 2022), onze wettelijke basis in de Wbni en de jaarplannen van het NCSC. De onderzoeksagenda is het document dat richting geeft aan de werkzaamheden van het NCSC onderzoeksteam. De agenda wordt gebruikt om onderzoeksvragen uit te zetten, deel te nemen aan onderzoeken of zelf onderzoeken te starten en uit te voeren. We zoeken daarin een balans tussen fundamenteel en toegepast onderzoek en onderzoek dat bijdraagt aan de missie van het NCSC. Hierbij bekijken we per onderwerp en onderzoek door wie of waar onderzoek uitgevoerd wordt. Het NCSC fungeert hierbij als opdrachtgever, uitvoerder, coördinator en verspreider van onderzoek en kennis.

Theoretisch kader en thema's

In de volgende hoofdstukken vindt u uitleg over het theoretisch kader van deze onderzoeksagenda en de drie hoofdthema's. Met deze drie thema's benaderen we cybersecurityonderzoek vanuit drie invalshoeken; het macro-, meso- en microniveau. We kijken zowel op strategisch, tactisch en operationeel niveau naar cybersecurity. Hiermee wordt het NCSC in staat gesteld om middels wetenschappelijk en toegepast onderzoek de digitale veiligheid van landen, organisaties, individuen en alles wat daar tussen zit te verhogen.

De drie thema's zijn opgedeeld in diverse subthema's waarmee we de omvang van dit thema aangeven op basis waarvan het NCSC onderzoek uitvoert, uitbesteedt of op samenwerkt. Daarvoor hebben we diverse mogelijke onderzoekvragen gedefinieerd die ter inspiratie dienen voor de komende jaren. Deze vragen geven onze voornaamste richting aan, hoewel deze niet uitputtend zijn.

De hoofdthema's van de NCSC onderzoeksagenda 2023-2026 zijn:

- Cybersecurity ecosysteem
- Socio-technical cybersecurity: mensen, processen en technologie
- Techniek in cybersecurity

Meer uitleg hierover vindt u in het volgende hoofdstuk.

Vervolgstappen

Ieder jaar bepalen we welke (sub)thema's prioriteit krijgen en verder worden uitgewerkt in onderzoeksvoorstellen. Dit doen we op basis van eerdere (onderzoeks)resultaten en aan de hand van actuele ontwikkelingen zoals die bijvoorbeeld voortvloeien uit het dreigingsbeeld in het CSBN. Na selectie van een subthema worden de voorbeeld onderzoeksvragen als uitgangspunt en inspiratiebron gebruikt. Deze worden dan in overleg met collega's en doelgroepen verder uitgewerkt tot definitieve onderzoeksvragen. Vervolgens voeren we deze onderzoeken zelf uit of we besteden ze uit. De agenda zal ieder jaar worden getoetst aan de inzichten uit het voorgaande jaar. We kunnen besluiten een onderzoekslijn te stoppen of een onderwerp juist verder uit te diepen of te verlengen. Resultaten worden gedeeld met de doelgroepen waarvoor het onderzoek relevant is, in (wetenschappelijke) publicaties en tijdens conferenties.

Theoretisch kader

Cybersecurity is integraal onderdeel van de nationale veiligheid.

Nederlandse overheid biedt veiligheid in vele vormen om de maatschappij zo goed mogelijk te laten functioneren. Door de verregaande digitalisering van het dagelijkse leven is digitale veiligheid en daarmee cybersecurity hierin een essentiële factor geworden. Dit vereist een proactieve houding van de overheid die zorgt voor een maatschappij waarin zijzelf, bedrijven en burgers zich veilig kunnen bewegen in zowel het fysieke als digitale domein. Enerzijds betekent dit dat er een basisniveau van cyberweerbaarheid moet zijn en anderzijds moeten overheid, bedrijven en burgers adequaat kunnen reageren op bestaande en toekomstige dreigingen. Omdat digitalisering en daarmee cybersecurity in alle lagen van onze samenleving is verweven, is het nodig dat we er vanuit meerdere perspectieven en invalshoeken onderzoek naar doen.

Het uitgangspunt van deze onderzoeksagenda is dat cybersecurity vanuit vele vakgebieden onderzocht wordt.

Het is daarmee waardevol om gebeurtenissen, incidenten, digitale fenomenen en digitale technologieën vanuit meerdere invalshoeken te bestuderen. De NCSC onderzoeksagenda 2023-2026 gaat daarom uit van een drielaags model, zijnde het macro-, meso- en microniveau waarbij we sociaal- en gedragswetenschappelijk en technisch georiënteerd onderzoek doen. Een onderzoek of thema hoeft niet enkel vanuit één niveau bestudeerd te worden. Juist onderzoek dat zich beweegt tussen twee niveaus of door alle lagen heen, kan veel toegevoegde waarde hebben. Het NCSC onderzoekscluster is hier bij uitstek geschikt voor dankzij de diverse achtergronden en onderzoeksinteresses van de medewerkers.

Cybersecurity is een vakgebied dat volop in ontwikkeling is. Dat maakt het een geliefd onderwerp om te onderzoeken. De NCSC onderzoeksagenda 2023-2026 zet uiteen op welke thema's en onderwerpen het onderzoekscluster zich de komende jaren zal focussen. Daarnaast geeft de brede aanpak van de drie niveaus ons voldoende ruimte om in te gaan op interessante samenwerkingen met externe partners.

"Innovaties op het gebied van cybersecurity zijn van vitaal belang om weerbaar te zijn en te blijven in de toekomst. Daarvoor is het van groot belang dat we als Nederland een sterke internationale kennis- en innovatiepositie hebben. De kennisontwikkeling van het NCSC is daarbij van grote waarde door hun unieke positie tussen de dagelijkse praktijk van cybersecurity operaties en de onderzoekswereld. dcypher stimuleert kennisontwikkeling door samenwerking tussen bedrijfsleven, overheid en kennisinstellingen. Om hierin succesvol te zijn is het van groot belang dat we van elkaar weten wat we doen en waar we naartoe willen. Vanuit dat opzicht is het voor de innovatieketen van cybersecurity van grote waarde dat deze agenda er nu is."

Eddy Boot
Directeur dcypher

1. Cybersecurityecosysteem

Bij het eerste hoofdthema benaderen we vanuit het macroniveau cybersecurity als ecosysteem Met name theorieën uit de sociale en gedragswetenschappen zijn bij dit perspectief relevant. Onderzoek vanuit het macroniveau levert onder andere inzicht in het krachtenveld waarin de Nederlandse overheid en het NCSC in het bijzonder moeten opereren. De subthema's zijn gericht op geopolitieke invloeden, ecosysteemrisico's en samenwerking in diverse vormen en op diverse niveaus.

1.1 Cybersecurity in een tijdperk van 'great power competition'

De afgelopen twee decennia hebben we een (voorzichtige) terugkeer gezien naar een wereld van competitie tussen grootmachten in het internationale politieke systeem. Met het einde van de Koude Oorlog werd een periode ingeluid van hegemonie door de Verenigde Staten. Die periode lijkt ten einde te komen nu China en Rusland duidelijk hun plek in de internationale politiek opeisen. Dit heeft grote effecten op de internationale veiligheid, en daarmee ook cyberveiligheid. Recente veranderingen in de focus van Westerse landen laten zien dat bescherming van het eigen grondgebied en bescherming van de eigen normen en waarden in eigen land dominanter zijn geworden. De gevolgen van deze terugkeer naar great power competition zijn hierbij goed zichtbaar in het cybersecurity domein. Het heeft directe gevolgen voor de hoeveelheid en soort cyberaanvallen die landen en organisaties op zich af zien komen. Bij internationale organisaties zijn discussies op gang gekomen over hoe het internet het beste ingericht kan worden door Chinese en Russische voorstellen die de huidige status quo uitdagen, door bijvoorbeeld wijzigingen voor te stellen in IP-protocollen. Daarnaast is er ook steeds meer aandacht voor digitale soevereiniteit en strategische autonomie. Met onderzoeken binnen dit thema leveren we inzicht in welke invloed geopolitiek heeft op het werk van het NCSC en welke rol het NCSC kan innemen in het internationale speelveld.

Mogelijke onderzoeksvragen

- Welke effecten heeft de wens voor meer digitale soevereiniteit binnen de EU op de positie van Nederland, en NCSC in het bijzonder, in internationale gremia, zoals IWWN, ICANN, IETF etc.?
- Welke rol zou het NCSC kunnen innemen bij vraagstukken rondom strategische autonomie? Hoe verhoudt deze rol zich tot andere Nederlandse organisaties in het cybersecuritystelsel?
- Hoe beïnvloedt het gebruik van sleuteltechnologieën, zoals 5G en AI, het werk van het NCSC in internationale samenwerkingen?
- Hoe gebruiken staten een strategisch voordeel op een of meerdere sleuteltechnologieën om andere strategische doelen te bereiken?

1.2 Ecosysteemrisico's

Het is meer en meer duidelijk geworden dat netwerkafhankelijkheden tussen organisaties en sectoren van cruciaal belang zijn voor het functioneren van diverse vitale processen. Zonder energie functioneert er bijvoorbeeld zeer weinig meer in ons land. Met de vaststelling en uiteindelijke inwerkingtreding van de NIB2 Richtlijn zal het aantal vitale sectoren en organisaties significant toenemen. Dit betekent dat het nog relevanter wordt om goed in beeld te hebben welke processen afhankelijk van elkaar zijn en waar mogelijke risico's zich bevinden. Onderzoeken helpen het NCSC om haar doelgroepen te adviseren over netwerkafhankelijkheden en welke risico's verbonden zijn aan onderdeel zijn van ketens en netwerken. Op die manier kan het NCSC invulling geven aan een belangrijke kennispositie over de effecten van de NIB2 Richtlijn voor de eigen organisatie en doelgroepen.

Mogelijke onderzoeksvragen

- Welke bekende standaarden en best practices voor risicomanagement passen het beste bij actuele supply chain vraagstukken in organisaties?
- Welke impact heeft de convergentie van IT en OT voor de safety en security van de Nederlands vitale infrastructuren?
- Hoe is de samenwerking tussen ketenpartners ingericht buiten formele initiatieven? Bijvoorbeeld in niet-vitale processen. Hoe ziet de samenwerking eruit tussen grote bedrijven en het niet-vitale MKB die wel leveren aan een vitale keten?
- Hoe kunnen cyberrisico's rond de afhankelijkheden van dienstenleveranciers inzichtelijk gemaakt worden?
- Hoe hangen risico's in één sector samen met risico's in andere sectoren en hoe modelleer je dat?

- Wat is de risicoperceptie van consumenten van essentiële diensten en hoe wijkt die af van de risico-inschatting door de leveranciers van die diensten? Wat hebben consumenten en inkopers nodig om cybersecurityaspecten een belangrijk onderdeel te maken van hun aankoopbeslissing? Welke acteerbare (gedragsbeïnvloedende) informatie hebben zij nodig?
- Wat zijn de lessons learned (vanuit toezichthouder en de onder toezicht gestelde) vanuit de oude/huidige NIB1 richtlijn en wat kunnen nieuwe vitaal aangemerkte partijen hiervan meenemen?

1.3 Samenwerking

De afgelopen twee decennia hebben we een (voorzichtige) terugkeer gezien naar een wereld van competitie tussen grootmachten in het internationale politieke systeem. Met het einde van de Koude Oorlog werd een periode ingeluid van hegemonie door de Verenigde Staten. Die periode lijkt ten einde te komen nu China en Rusland duidelijk hun plek in de internationale politiek opeisen. Dit heeft grote effecten op de internationale veiligheid, en daarmee ook cyberveiligheid. Recente veranderingen in de focus van Westerse landen laten zien dat bescherming van het eigen grondgebied en bescherming van de eigen normen en waarden in eigen land dominanter zijn geworden. De gevolgen van deze terugkeer naar great power competition zijn hierbij goed zichtbaar in het cybersecurity domein. Het heeft directe gevolgen voor de hoeveelheid en soort cyberaanvallen die landen en organisaties op zich af zien komen. Bij internationale organisaties zijn discussies op gang gekomen over hoe het internet het beste ingericht kan worden door Chinese en Russische voorstellen die de huidige status quo uitdagen, door bijvoorbeeld wijzigingen voor te stellen in IP-protocollen. Daarnaast is er ook steeds meer aandacht voor digitale soevereiniteit en strategische autonomie. Met onderzoeken binnen dit thema leveren we inzicht in welke invloed geopolitiek heeft op het werk van het NCSC en welke rol het NCSC kan innemen in het internationale speelveld.

"Bij Agentschap Telecom werken we aan een veilig verbonden Nederland. Een Nederland dat kan rekenen op goede telecommunicatie- en IT-netwerken, die bovendien veilig en betrouwbaar gebruikt kunnen worden. We houden er toezicht op dat iedereen zich aan de regels, eisen en voorwaarden houdt. Agentschap Telecom onderzoekt, signaleert en agendeert diverse ontwikkelingen die met digitale weerbaarheid en digitale veiligheid te maken hebben. Kennis delen en elkaar versterken is daarbij essentieel. De samenwerking tussen NCSC en Agentschap Telecom in onderzoek is daarbij van groot belang en continueren we graag. Zo werkten wij samen op onderzoek naar de risico's van onderlinge afhankelijkheden in de keten van digitale infrastructuur en leveranciers van netbeheerders en op onderzoek naar het vermogen van organisaties om te herstellen van een ICT-incident. Ook hebben we samengewerkt in het onderzoek naar de relatie tussen geopolitieke ontwikkelingen en technologische veranderingen in de (toekomstige) internetinfrastructuur, met focus op de transportlaag."

Dr. Jessica de Groot-Overweg
Onderzoeker telekwetsbaarheid
Agentschap Telecom

Mogelijke onderzoeksvragen

- Welke toekomstige rol neemt het NCSC in het Nederlandse cybersecuritystelsel en hoe bevorderen we daarmee samenwerking tussen organisaties?
- **Wet- en regelgeving op (inter)nationaal vlak.**
  - Wat zijn de overeenkomsten en verschillen tussen diverse relevante wet- en regelgevingen en compliance kaders?
  - Hoe verhoudt de NIB2 Richtlijn zich tot de veelvoud aan standaarden en compliance kaders? Hoe komen we van een cultuur die vanuit compliance vinkjes zet naar een cultuur met risicogedreven kiezen van maatregelen? Hoe gaan de verschillende toezichthouders daar dan mee om? In Nederland is het vaak 'pas toe of leg uit', maar in andere landen gaat de inspectie op de letter en niet op de geest van de standaard.
- **Internationaal**
  - Hoe hebben andere NCSC's hun kennismanagement ingericht en hoe verrichten zij wetenschappelijk onderzoek en maken ze er gebruik van? Welke (internationale) samenwerkingen zijn op dit vlak mogelijk?
  - Hoe kunnen internationale CSIRTs effectief samenwerken met het uitwisselen van informatie over kwetsbaarheden?
- **Nationaal**
  - Welke factoren dragen bij aan nationale situation awareness in het kader van cybersecurity risicomonitoring en crisismanagement?
  - Wat is de invloed van wet- en regelgeving (NIB2 Richtlijn, Cybersecurity Act, diverse sectorale compliance kaders) op de samenwerking tussen toezichthouders, CSIRTs, ISACs en andere stakeholders in Nederland?
  - Welke kaders, processen en tools moeten worden ontwikkeld voor het centraal verzamelen van verplichte en vrijwillige incidentmeldingen en forensisch onderzoek naar root-cause?
- **Organisatorisch**
  - Wat is de invloed van besturingsmechanismen van een organisatie op het niveau van cybersecurity in die organisatie?

2. Socio-technical cybersecurity: *mensen, processen en technologie*

Om daadwerkelijk te begrijpen hoe mensen zich gedragen, is het noodzakelijk dat we een idee hebben van hun omgang met technologie en data. De enorme hoeveelheden verschillende technologieën die tegenwoordig beschikbaar zijn, zorgen ervoor dat er veel te kiezen valt. Er lijkt altijd wel een goedkopere, snellere, makkelijkere manier te zijn om je werk of privéactiviteiten vorm te geven. Security wordt door velen nog als belemmerend gezien en iets waar omheen gewerkt moet worden om snel en wendbaar te zijn. Als we als uitgangspunt nemen dat technologie en security faciliterend moeten zijn, kunnen ontwikkelaars, beleidsmakers en uitvoerders met de gebruiker meedenken in de ontwikkeling van producten en diensten.

2.1 Security by design

Het NCSC heeft in de afgelopen twee jaar samen met de Universteit Leiden onderzoek verricht naar security by behavioural design. In dit onderzoek lag de focus op hoe producten en diensten veiliger kunnen worden gemaakt door rekening te houden met menselijk gedrag. De centrale vraag hierbij was: hoe houden organisaties momenteel rekening met menselijk gedrag bij het ontwerpen en inrichten van hun producten en diensten? Het NCSC is voornemens deze onderzoekslijn voort te zetten en eveneens breder te kijken naar hoe het gebruik van security by design in zowel systemen als processen gestimuleerd kan worden. Door specifiek te focussen op het gedragscomponent leveren we meer inzicht in hoe dit vaak onderbelichte component ingezet kan worden om veiligere producten en diensten te ontwikkelen en te gebruiken.

Mogelijke onderzoeksvragen

- Wat zijn organisatorische en economische incentives voor organisaties om veiligheid te verhogen?
- Hoe kunnen cybersecurityrisico's effectief gecommuniceerd worden door de systemen zelf? Hoe kan een user-interface-design ervoor zorgen dat eindgebruikers kiezen voor de meest veilige optie(s)?
- Hoe kunnen we onderwerpen als joint situation awareness, AI, mens-computer interactie, computer-computer interactie, Humanistic Intelligence bestuderen en toepassen op cybersecurity?
- Hoe zou een proces of security technologie eruit zien als het wordt herontworpen volgens design thinking principes?
- Kan cyber informed engineering helpen om soft- en hardware ontwikkelaars te stimuleren veilige systemen te ontwikkelen?

"De samenwerking met het NCSC maakt het voor ons mogelijk om aan interessante onderzoeksprojecten te werken met een directe impact op de maatschappij. De kennis die het NCSC heeft en produceert in samenwerking met kennisinstellingen, aangevuld met hun hub- en netwerkfunctie, maakt het mogelijk om theoretische wetenschappelijke kennis en inzichten in te zetten bij het opstellen van aanbevelingen voor cybersecurityoplossingen in de praktijk. Ons project over security by behavioural design combineert wetenschap met de praktijk door richtlijnen en methoden te ontwikkelen gebaseerd op wetenschappelijke inzichten en empirisch onderzoek met verschillende organisaties in Nederland."

Dr. Tommy van Steen
Assistant professor Universitet Leiden in `security by behavioural design'

2.2 Communicatie en datagedreven werken

Het onderwerp communicatie gaat uit van effectiviteit van kennis- en informatie-uitwisseling waarbij de gebruiker van de informatie en diens kennis en vaardigheden centraal staan. Datagedreven werken is een speerpunt zowel binnen het ministerie van Justitie en Veiligheid als in de ontwikkeling van het cybersecurity vak. Het draagt bij aan betere besluitvorming, informatiedeling en risicoanalyse en het verbetert de impact van communicatie over de urgentie van cybersecurity.

Mogelijke onderzoeksvragen

- Hoe kan communicatie over cybersecurityrisico's aangepast worden aan het kennisniveau en referentiekader van de gebruiker?
- Cognitieve dimensie van situation awareness: hoe ga je als medewerker om met alle informatie die je krijgt?
- Welke communicatiestrategieën kunnen worden toegepast om de urgentie van cybersecuritymaatregelen en investeringen te laten doordringen bij bestuurders en ondernemers?
- Hoe kan evidence based besluitvorming helpen bij meer effectieve besluitvorming en uitvoering?
- Wat is de impact van data visualisatie op situation awareness?
- Hoe kan (sectorale) incidentdata worden geanalyseerd en worden toegepast in statistische analyses en voorspellende algoritmes?
- Incident reporting obligation: er zijn veel autoriteiten om een incident aan te rapporteren. De NIB2 Richtlijn eist een single point of contact.
    - Wat moet worden gemeld, hoe, wanneer, in welke volgorde? Is hier een best practice of standaard voor die we moeten promoten?
    - Hoe is de meldcultuur in de vitale sectoren?
    - Welke technologie wordt daarvoor gebruikt?
    - Hoe gaat de verwerking van de melding en hoe werken de competent authorities vervolgens samen?
    - Welke metrics zijn eruit te halen?
- Hoe kunnen we effectief communiceren over risico's van kwetsbaarheden?

2.3 Future Internet

De technische fundamenten van het internet zijn over de jaren heen langzaam veranderd, bijgestuurd en bijgeschaafd. Door het grootschalig gebruik en de grote belangen is het onmogelijk om fundamentele wijzigingen te maken. Dit maakt dat security by design toepassen op het internet erg lastig en beperkt is. Er zijn verschillende initiatieven om een alternatief *Future Internet* te ontwikkelen.

Mogelijke onderzoeksvragen

- Wat zijn uitgangspunten voor een beter beveiligd internet? Welke rol heeft het NCSC hierin?
- Hoe worden de belangen van security en surveillance tegen elkaar afgewogen? En hoe gaat dat met andere belangen?
- Kan de verdere ontwikkeling van Future Internet leiden tot een versplintering van het internet?
- Hoe kan het toekomstige internet bijdragen aan een digitaal veiliger Nederland?

3. Techniek in cybersecurity

Techniek in cybersecurity heeft een duale rol: aan de ene kant is dit het niveau waarop dreigingen zich concreet manifesteren, aan de andere kant is het een hulpmiddel om veiligheid te bereiken. Het creëert een relatie met een wisselwerking met het meso- en macro- niveau; aan de ene kant wordt techniek gestuurd door deze niveaus, aan de andere kant is het voedend om de omgeving te kunnen begrijpen.

3.1 Informatie rond kwetsbaarheden

Omgaan met kwetsbare software en diensten blijft een kernactiviteit van cybersecurity. Ervaring leert dat het belangrijk is om zo snel mogelijk informatie rondom kwetsbaarheden te verkrijgen, te duiden en uit te wisselen. Verschillende delen van dit proces worden geautomatiseerd, terwijl menselijke input nodig blijft om informatie te interpreteren, te verrijken en naar de juiste partijen door te sturen. De ontvangen partijen zouden dan in staat moeten zijn om zo efficiënt mogelijk hun eigen context toe te kunnen passen op de ontvangen informatie.

Mogelijke onderzoeksvragen

- Wat is de impact van het automatiseren van informatiestromen rondom kwetsbaarheden?
- Wat voor kansen bieden deze automatische informatiestromen?
- Wat is de beste manier om data van en over kwetsbaarheden te ontsluiten als open data?
- CVSS is per definitie geen risicoscore. Is het desondanks toch mogelijk om (semi-)automatisch een risicoscore te maken?
- Hoe kan een NCSC-kwetsbaarheidsinschaling aansluiten bij de brede doelgroep die ieder een eigen context heeft?
- Hoe kunnen begrippen rondom digitale risico's verder gestandaardiseerd en geduid worden?

"De groeiende complexiteit en impact van cyberaanvallen vragen om een gedegen aanpak om de cyberweerbaarheid te vergroten. Tno draagt hieraan bij door samen met organisaties zoals het ncsc onderzoek vanuit een breed perspectief uit te voeren, waarbij technologie, organisatorische en menselijke factoren van cybersecurity worden meegenomen. In ons onderzoek staat de toepassing centraal: hoe kunnen de resultaten uit het onderzoek worden ingezet om de nederlandse samenleving weerbaarder te maken tegen cyberaanvallen? Het ncsc speelt daarbij een belangrijke rol om vraag en kennis aan elkaar te koppelen. Door gezamenlijk en meerjarig onderzoek te programmeren wordt ingespeeld op de uitdagingen van nu en de toekomst."

Gwen Jansen-Ferdinandus
Programmamanager Gezamenlijk research programma NCSC-TNO namens TNO

3.2 Impact van encryptie

Encryptie is een hulpmiddel om integriteit en vertrouwelijkheid te kunnen bereiken. Dit biedt mogelijkheden om data af te schermen en dit kan zowel in positieve als negatieve zin ingezet worden. Dat wil zeggen, het kan vertrouwelijke gegevens beschermen tegen meekijkers, maar het kan ook gebruikt worden om (communicatie met) malware af te schermen. Binnen dit thema kijken we naar praktische gevolgen van steeds verdergaande encryptie van data. Zo'n beetje het gehele netwerkverkeer is tegenwoordig op een of andere manier afgeschermd. De steeds verdergaande ontwikkeling van de kwantumcomputer maakt het noodzakelijk om op korte termijn nieuwe vormen van encryptie in te gaan zetten. Het wordt steeds duidelijker welke vormen de nieuwe standaarden aan gaan nemen.

Mogelijke onderzoeksvragen

- Wat is de rol van netwerkdetectie in de toekomst?
- Zijn er creatieve oplossingen mogelijk zodat netwerkdetectie mogelijk blijft?
- Zijn er andere middelen om vergelijkbare detectiedoelen te behalen?
- Hoe verloopt de transitie naar kwantumveilige encryptie?
- Wat heeft post-kwantum-encryptie voor gevolgen in de praktijk?
- Wat voor nieuwe mogelijkheden bieden post-kwantum encryptie?

3.3 Fundament van het internet

Het fundament van het internet wordt stukje bij beetje verbeterd. Om de robuustheid te verhogen en om de beveiliging op te schroeven. Voorbeelden hiervan zijn toevoegingen aan DNS om dit veiliger te maken en verbeteringen aan de routering van het internet (BGP). Tegelijkertijd wordt er steeds meer gemeten aan het internet om adaptatie van deze standaarden, ontwikkelingen of juist verstoringen in kaart te brengen.

Mogelijke onderzoeksvragen

- Worden de best practices uit de huidige standaarden in Nederland toegepast?
- Wat voor dreigingen vloeien voort uit de huidige standaarden binnen het internet?
- Hoe kunnen partijen gestimuleerd worden om het fundament van het internet te verbeteren op het gebied van ICT-veiligheid (open-source-gemeenschap, internetproviders, internetexchanges, overheden, multilaterale organisaties)?

Bijlagen

Referenties

1. Council of Europe (CoE), Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security Capacity Centre (GCSCC), Geneva Centre for Security Policy (GCSP), Global Partners Digital (GPD), International Criminal Police Organization (INTERPOL), International Telecommunication Union (ITU), Microsoft, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Potomac Institute for Policy Studies (PIPS), RAND Europe, World Bank, United Nations Institute for Disarmament Research (UNIDIR), United Nations Office of Counter-Terrorism (UNOCT), United Nations University (UNU). (2021). "Guide to Developing a National Cybersecurity Strategy 2nd Edition – Strategic engagement in cybersecurity".
2. Dcypher (2018) "National Cyber Security Research Agenda." Herbert Bos, Michel van Eeten, Sandro Etalle, Frank Fransen, Jaap Henk Hoepman, Erik Poll, Jan Piet Barthel (eds). Dcypher.
3. Herve Debar, Fabio Di Franco, Athanasios Vasileios Grammatopoulos, Irene Mantzouranis, Evangelos Markatos (2021) "Cybersecurity Research Directions for the EU's Digital Strategic Autonomy" ENISA.
4. National Coordinator for Security and Counterterrorism (2022), "Cybersecurity Assessment Netherlands 2022".
5. National Coordinator for Security and Counterterrorism, (2022) "Netherlands Cybersecurity Strategy".
6. National Cyber Security Centre Netherlands (2019) "NCSC Research Agenda 2019-2022".
7. National Cyber Security Centre United Kingdom (2021) "NCSC Annual Review".

Onderzoeksmethode

De NCSC Onderzoeksagenda 2023-2026 is op de volgende wijze tot stand gekomen:

1. **Scope definiëren en deskresearch:** de eerste stap was het definiëren van de scope van de onderzoeksagenda. Het vertrekpunt voor de afbakening vormde de NCSC Onderzoeksagenda 2019-2022, het Cyber Security Beeld Nederland 2021 en 2022 en ontwikkelingen zoals beschreven in diverse rapporten van de OVV (Citrix-rapport), de CSR en wetenschappelijke instellingen. Daarnaast vormt de wettelijke taak van het NCSC het uitgangspunt voor deze onderzoeksagenda. Parallel hieraan is deskresearch uitgevoerd om de scope te vergelijken met andere (voormalige) EU-lidstaten (Verenigd Koninkrijk, Duitsland, Denenmarken, België), de Verenigde Staten, alsmede internationale organisaties (EU, ENISA, NAVO, OSVE, Interpol, OESO, VN). De documenten die zijn gebruikt in de desk research vindt u terug bij de referenties.
2. **Analyse en ontwikkeling eerste versie:** de resultaten van de desk research zijn getoetst aan de missie van het NCSC. In een kwalitatieve analyse is gekeken naar overeenkomsten en verschillen in dossiers, doelen en prioritering. Rekening houdend met de nationale prioriteiten en focus van het NCSC is de scope van de onderzoeksagenda vastgesteld en op basis van bovenstaande analyse is de eerste versie geschreven.
3. **Verzamelen input interne en externe experts:** na interne inventarisatie zijn interviews uitgevoerd met interne en externe cybersecurity experts. Het doel was om eerdere bevindingen te trianguleren en te valideren binnen het netwerk van het NCSC. De interviews hebben bijgedragen aan de evaluatie van de onderzoeksthema's.
4. **Verfijning en ontwikkeling definitieve versie:** op basis van alle bevindingen voortvloeiend uit de desk research en de interviews is de definitieve versie van de onderzoeksagenda geschreven.

Publicatie
Nationaal Cyber
Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
+31 (0)70 751 5555

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

oktober 2022