Aanvraag duidingsonderzoek Security 2.0 technieken

Inleiding

The Hague Security Delta (HSD) is ervan overtuigd dat de wereld alleen veiliger wordt als krachten worden gebundeld. Wij geloven dat kennisuitwisseling en samenwerking cruciaal zijn om te komen tot noodzakelijke, rendabele veiligheidsinnovaties. Nu en in de toekomst.
Als onafhankelijke organisatie stimuleert en faciliteert HSD Office kennisdeling en verbinden we partijen.

In het nieuwe beleidskader van EZK worden topsectoren omgebogen naar maatschappelijke uitdagingen waaronder veiligheid. In cross over met technologieën zoals machine learning en AI liggen ICT kansen in de combinatie veiligheid en economie. HSD denkt bij te kunnen dragen aan het denken via samenwerking naar doen) via deze studie.

Binnen deze taak valt een studie naar technische duiding en strategische inbedding van actuele fenomenen binnen de cyber security. Deze aanvraag voor een onderzoek beschrijft dergelijke actuele fenomenen, schetst de urgentie binnen het Nederlands cyberlandschap en stelt mogelijke onderzoeksvragen vast.

Het doel is een rapportage waarin een strategische en technische schets wordt gegeven van de toekomst van cybersecurity. Het secundaire doel is dat HSD haar kennisrol vervult en samen met het netwerk beziet waar vervolgprogrammering mogelijk is.

De keuze van de onderwerpen is gebaseerd op ons huidige beeld. Mochten de onderzoekers van mening zijn dat bepaalde fenomenen die hier niet genoemd zijn wel aandacht verdienen, dan staat HSD open voor suggesties.

Security blijft achter

Het laatste CSBN (Cyber Security Beeld Nederland) is somber over de toekomst van onze huidige cyber security aanpak. We verhogen de dijken, maar het water stijgt sneller.

Het functioneren van de maatschappij wordt steeds afhankelijker van cyber security, terwijl cyberaanvallen nog steeds profijtelijk, laagdrempelig en weinig riskant voor aanvallers zijn.
Naast een gebrek aan basismaatregelen constateert het NCSC een toenemende inmenging van statelijke actoren. Gebrek aan cybersecurity verhoogt het risico op maatschappelijke ontwrichting.

Er is daarom een trendbreuk nodig in cybersecurity. Uit gesprekken met bij HSD aangesloten partners blijkt dat veelbelovende technologieën die hierbij toegepast kunnen worden reeds bestaan of in

ontwikkeling zijn. HSD wil een duidingsvraag uitzetten naar een drietal van deze technologieën om te onderzoeken of en hoe ze kunnen bijdragen aan een intrinsiek veiliger cybersecuritylandschap:

- intrinsiek veilig, korte termijn: data diodes
- intrinsiek veilig, lange termijn: quantum encryptie
- schaalbaar met de toename van de complexiteit: AI supported cyber security.

1. Data Diodes

Een data diode of unidirectioneel netwerk is een toepassing die ervoor zorgdraagt dat data slechts één kant op kan bewegen. Het is een middel om information security te garanderen.
Data diodes worden gebruikt in high security omgevingen om netwerken met een verschillende security classificatie met elkaar te verbinden. Denk hierbij aan defensie, kernreactoren of drinkwatervoorziening.

Voorbeeld: Tussen het flight control system en het onboard entertainment system aan boord van moderne vliegtuigen zit een data diode, zodat gegevens (oproepen) wel van het control system naar het entertainment system kunnen vloeien, maar niet de andere kant op.

Nu de OT (operational technology) en de IT wereld elkaar steeds dichter naderen en zelfs resulteren in een nieuwe trend in de Internet of Things is de bescherming die data diodes kunnen bieden meer van belang dan ooit. OT systemen zijn ontworpen om 30 jaar te draaien zonder updates of aanpassingen, terwijl IT systemen maandelijks gepatcht dienen te worden.

De in Nederland als vitaal A aangemerkte partijen hebben reeds ervaring met het gebruik van data diodes. Daarnaast zijn er veel partijen die niet als Vitaal A zijn gekenmerkt, maar waarvan de security ook onontbeerlijk is voor een veilig en economisch krachtig land. Over hoe deze partijen de overstap zouden moeten maken naar het gebruik van data-diodes is nog onbekend.

Hierbij wordt opgemerkt dat in nieuwe Cyber wetgeving een wettelijke verplichting is opgenomen om data diodes als vitaal A te gebruiken.

Bekeken zou moeten worden wat de wensen, behoeften en investeringsmogelijkheden van deze partijen zijn, en hoe binnen deze bandbreedtes een aanbod van data diodes gestalte kan krijgen. Nederland is niet het enige land dat met deze vraagstukken speelt - een consortium met ervaren buitenlandse partners ligt dan ook voor de hand.

Relevantie

De NCSRA-III stelt in het Defence hoofdstuk dat aandacht besteed dient te worden aan hoe de bescherming van legacy systemen vormgegeven dient te worden. Hier dient bescherming geboden te worden aan bestaande systemen. Data diodes zijn hier een geëigend middel. Als voorbeelden voor onderzoek wordt genoemd [NCSRA-III, PAG 15]:

- Technologies for attack containment and deception (e.g. to thwart attacks)

- Hardware defences, and safe and secure deployment of physical devices

In het hoofdstuk Design van de NCSRA-III wordt gekeken naar hoe nieuwe systemen by design veilig gemaakt zouden kunnen worden, met onder meer als voorbeelden:

- Security solutions for device management for industrial and consumer products, including IoT devices, spanning the entire lifecycle (design, p11)
- Resilient design for security in insecure environments (design, p11)
- Compartmentalisation solutions for hardware, software, and networks (design, p11)

Onderzoek en doorontwikkeling van data diodes zou hier uitstekend inpassen. Een duiding, zoals gevraagd in dit studievoorstel, zou daarmee aanleiding kunnen zijn van verder wetenschappelijk onderzoek.

Onderzoeksvragen

Wij zouden in deze studie de volgende vragen beantwoord willen zien:

Hoofdvraag:
Wat zijn de technische en maatschappelijke eisen bij het implementeren van data diodes bij subvitale Nederlandse partijen?

Subvragen:

Hoe worden data diodes momenteel ingezet? Waar? Waar nog niet? Wat zijn de ervaringen?

Wat is binnen de industrie het kennisniveau met betrekking tot data diodes in het algemeen? Zijn ze voldoende bekend of is zendingswerk nodig? Worden ze voldoende gebruikt? Wat is de reden voor partijen om ze niet in te zetten?

Wat zijn de ervaringen met de verschillende aanbieders? Zijn er partijen die al open source data diodes gebruiken? Wat zijn de behoeften? Wat is nodig om aan deze behoeften tegemoet te komen, en welke partijen zouden dat kunnen realiseren?

Wat is de gewenste functionaliteit door subvitale partijen gesteld aan data diodes? Wijkt deze af van de wensen en mogelijkheden van vitale partijen?

Welke strategische buitenlandse partners hebben voldoende kennis in huis en ervaring met data diodes voor de genoemde partijen, hoe zouden wij kunnen aansluiten in een gezamenlijke aanpak?

Heeft NL een kennispositie om hier ook export product van van te maken? Zo ja, hoe of welke aanpak om die positie uit te nutten?

2. Quantum security

Om de veiligheid van een cryptografisch systeem te beoordelen moet rekening worden gehouden met hoe lang het systeem in gebruik zal zijn en hoe lang de data beschermd moeten blijven. Daarna moet worden ingeschat of de rekenkracht die binnen de levensduur van het systeem beschikbaar kan komen het vastgestelde veiligheidsniveau ondermijnt.
Voor veel systemen, en vooral overheidssystemen die langlevende data beschermen, betekent dat verschillende decennia vooruitkijken.

Door verschillende wetenschappers wordt aangenomen dat met de verdere ontwikkeling van quantumcomputers asymmetrische cryptografie op den duur gebroken kan worden. Dat betekent dat nu het moment is om te investeren in quantumveilige oplossingen.

Technisch gezien worden er in het algemeen twee richtingen voorgesteld:

- quantum key distributie (QKD) - gebruik maken van quantum computing om sleutels aan te maken en uit te wisselen
- post quantum cryptografie (PQC) - het ontwerpen van quantumveilige cryptografie die hard/softwarematig op klassieke computers geïmplementeerd kan worden.

Het onderzoek naar quantumcomputing bevindt zich nog voornamelijk in de fundamentele fase,. Nederland kan trots zijn op het feit dat we in de top van het quantumonderzoek meedraaien. Het is dan ook een speerpunt van het Nederlandse beleid en brengt verschillende onderzoeks-, overheids- en commerciële instellingen samen.
Deze voorsprong zou wellicht gebruikt kunnen worden om in samenwerking proeftuinen op te zetten om quantumveilige oplossingen te testen. Overheid en wetenschap zijn hierbij gebaat, maar er is ook economisch belang. Early investment kan het bedrijfsleven een voorsprong geven.

Een overgang naar quantumveilige oplossingen omhelst ook maatschappelijke component. Wanneer zou de huidige security vervangen moeten worden en wat zijn de gevolgen, hoe zou het traject moeten verlopen, met welke landen zou Nederland moeten optrekken?

Relevantie

NCSRA-III, hoofdstuk Design
Post-quantum crypto, and associated migration paths (p11)

NCSRA-III, hoofdstuk Privacy
Privacy enhancing technologies (p29)

Horizon 2020, Emerging Themes and Communities, Area 3: Disruptive information technologies
Quantum Engineering

Onderzoeksvragen

Wij zouden in deze studie de volgende vragen beantwoord willen zien:

Hoofdvraag:

Welke invloed zou de doorontwikkeling van quantumcomputers kunnen hebben op de huidige security? Is er sprake van een serieus risico of eerder van een hype?

Subvragen:

Welke strategische stappen zijn nodig om cyber security quantum resistent te maken?

Op welke termijn kunnen quantumaanvallen verwacht worden, en hoe lang duurt het om de securitymechanismes daartegen bestand te maken?

Wat is de mogelijke invloed van quantumtechnologieën op nieuwe securitytoepassingen zoals blockchain?

Wat is de waarde van quantum encryptie (QKD) ten opzichte van post quantum cryptografie (PQC)?

3. Zelflerende systemen

AI, kunstmatige intelligentie, doet met rasse schrede intrede in onze samenleving. Het betreft dan ANI (artificial narrow intelligence). De toepassingen hiervan hebben een steeds sterkere invloed op de maatschappij. Deze trend zal naar verwachting de komende jaren stevig doorzetten. De ontwikkelingen gaan vooral hard in het deelgebied van de zelflerende systemen. Duiding van dit verschijnsel vond reeds plaats in het boekje: The Hague Security Delta - Notitie Risico-Analyse in Onzekerheid Artificial Intelligence (kansen en bedreigingen).

In dat boekje worden de ontwikkelingen van de AI in de breedte geduid. In het kader van deze aanvraag is behoefte aan een meer specifieke en praktische duiding van de mogelijkheden van zelflerende systemen in de cybersecurity.

De sterke groei van het aantal security incidenten zorgt dat deze zonder ondersteuning niet meer bij te houden zijn. Dit kan leiden tot onnodig verlies van confidentiality, integrity en availability. AI kan hier wellicht in helpen. Ook is het denkbaar dat zelflerende systemen ingezet kunnen worden om geautomatiseerd security tests uit te voeren en zo zwakheden in software aan te treffen.

Relevantie

NCSRA-III, hoofdstuk Defence:
Automated defence (e.g. automating software-defined networking and attack reaction) (p15)

NCSRA-III, hoofdstuk Attacks:
Predictive analysis to identify malicious activity trends and attackers' next steps (p20)

Onderzoeksvragen

Wij zouden in deze studie de volgende vragen beantwoord willen zien:

Hoofdvraag:

Wat zijn de technische en strategische mogelijkheden voor de inzet van zelflerende systemen als tool voor cybersecurity?

Subvragen:

Kunnen zelflerende systemen opgezet worden gericht op cyber security?

Wat is hiervoor nodig?

Welke partijen hebben hier baat bij?

Wat is de rol van Big Data in het trainen van op cyber security gerichte zelflerende systemen?

Welke partijen werken reeds aan oplossingen?

Wat is er voor nodig om deze zelflerende systemen in een zo realistisch mogelijke omgeving te testen?

Zouden zelflerende systemen een oplossing kunnen vormen voor het probleem dat nog teveel bedrijven hun basisveiligheid niet op orde hebben?

Opdracht

VORM

Wij vragen voor elk van de genoemde onderwerpen een notitie in de vorm van een **kort boekwerkje van 20 a 30 pagina's**.

In deze notities wordt in heldere taal, en voorzien van relevante voorbeelden (waar nodig uit andere domeinen) uitleg gegeven over en duiding gegeven aan de genoemde onderwerpen.

DOEL

In deze notities zouden we graag een **technische en strategische duiding** zien van mogelijkheden en beperkingen, economische en strategische meerwaarde van de gekozen securitytechnieken. De nadruk van de notitie moet liggen op **praktische toepasbaarheid**: beslissers binnen overheid en bedrijfsleven zouden aan de hand van de aanbevelingen in de notities in staat moeten zijn de komende jaren strategische keuzes te maken.

DOELGROEP

De primaire doelgroep van de boekwerkjes zijn **beslissers**: wel de intelligentie, maar beperkte de kennis op het terrein van cyber security. Gevoed door de juiste technische en strategische input zijn zij in staat om op hoofdlijnen de juiste beslissingen te nemen.

TAAL

De notities dienen in het **Engels** geschreven te worden.

ROUTE

HSD gelooft in de meerwaarde van samenwerking. Wij willen dat dit project in **samenwerkingsverband** tussen twee of meer onderzoekende instanties wordt uitgevoerd.

We vragen om een *agile* aanpak met **tussentijdse deliverables en ijkpunten** om te kunnen bijsturen wanneer hiertoe behoefte is.

De studie zal bestaan uit een **component literatuurstudie en een component expertkennis.** Ten behoeve van dat laatste zullen interviews met voor dat onderwerp relevante partijen worden afgenomen. Per onderwerp denken wij aan **10 - 15 interviews.** HSD is gezien haar netwerk in staat om mee te denken welke partijen geïnterviewd zouden kunnen worden.

We staan open voor een alternatieve aanpak.

PLANNING

Wij stellen ons de volgende tijdslijn voor:

Juli/augustus: uitzetten opdracht
September+ begin oktober: terugkoppeling deelresultaten
Half oktober: afronding
November: bekendstelling

CONTEXT

De duiding dient te resulteren in boekjes die voldoende handvatten verschaffen om de kernwerkzaamheden van HSD op dit gebied een **praktische impuls, richting en draagvlak** te geven.

Het is niet de bedoeling om studies van andere partijen te dupliceren of voor de voeten te lopen. De nadruk ligt dan ook op daar waar de HSD meerwaarde kan geven: praktische technische en strategische duiding voor partijen binnen de triple helix.

Vervolg
De notities zullen middels HSD Cafés bekend worden gemaakt, met bijbehorende lezingen en werksessies, waardoor het HSD Netwerk en ander publiek (het is immers openbaar toegankelijk) in staat wordt gesteld kennis te nemen van de rapporten, en mogelijke toepasbaarheid, en waarbij mogelijke programmering door HSD, en dus samenwerking gericht op innovaties, tot stand kan worden gebracht.

RICHTLIJNEN

Deze aanvraag en de resulterende notities zijn geschreven op basis van de volgende voor HSD belangrijke richtlijnen:

- Wat is de ontwikkeling
- Wat is de vraag
- wat is het aanbod
- Wat is nodig
- Wie is nodig
- Hoe bereiken we het samen
- Publiek en economisch belang
- Praktisch