SECURITY

INNOVATION STORIES

20 koplopers over innovatie in het cybersecuritydomein

Auteur: Bram de Bruijn
Co-auteur: Frank van Summeren

SECURITY

INNOVATION STORIES

20 koplopers over innovatie in het cybersecuritydomein

Auteur: Bram de Bruijn
Co-auteur: Frank van Summeren

Colofon

Titel: Security Innovation Stories: 20 koplopers over innovatie in het cybersecuritydomein
Auteur: Bram de Bruijn
Co-auteur: Frank van Summeren
Redactie: Anja den Hertog & Charelle Kooy
Vormgeving en **omslagontwerp:** Estelle Valkenburg
Grafische vormgeving: Estelle Valkenburg
Uitgeverij: Beyond Products B.V.
Druk: Eerste druk
Jaar van uitgave: 2024

's Hertogenbosch, 2024

Frank van Summeren Bram de Bruijn

Voorwoord

In een wereld die met ongekende snelheid digitaliseert, vormt cybersecurity de hoeksteen van onze moderne samenleving. Het is de onzichtbare wachter die waakt over de integriteit van onze gegevens, de bescherming van onze privacy en de continuïteit van onze bedrijfsvoering. Innovatie binnen het domein van cybersecurity is daarom geen keuze meer, maar een noodzaak. Een voortdurende race tegen de klok, waarin de uitdagers iedere keer inventiever worden en de verdediging steeds veerkrachtiger moet zijn.

In dit boek betreden we het toneel van digitale veiligheid door de ogen van twintig koplopers en challengers in de sector. Zij zijn de denkers en doeners die de frontlinie van digitale weerbaarheid vormgeven. Hun inzichten zijn een verzameling van visies, ervaringen en benaderingen die het spectrum van innovatie in cybersecurity ontrafelen en opnieuw definiëren.

Elke geïnterviewde biedt een unieke kijk op de toekomst van digitale beveiliging, deelt praktische voorbeelden en belicht de innovaties van nu en de toekomst. Innovaties die niet enkel onze technologie, maar ook onze maatschappelijke normen en waarden zullen vormen.

Dit boek is meer dan een verzameling van gesprekken. Het is een naslagwerk voor iedereen die betrokken is bij of geïnteresseerd is in de vitale wereld van cybersecurity. Elk gesprek staat op zichzelf, maar met één rode draad: het belang van innovatie binnen cybersecurity. Moge hun ervaringen en inzichten je bewapenen met de kennis en het begrip om je eigen bijdrage te leveren aan de veiligheid van onze digitale wereld. Hierbij wil ik Anja den Hertog bedanken voor het initiatief en uiteraard Frank van Summeren, die als co-auteur zijn bijdrage heeft geleverd aan dit resultaat.

Veel leesplezier en inspiratie gewenst,

Bram de Bruijn

Inhoudsopgave

1

Inleiding 9

2

Definities 12

3

Dimitri van Zantvliet 16
Directeur cybersecurity bij de NS

4

Fleur van Leusden 22
CISO bij de Kiesraad

5

Prof. dr. Peter de Kock 28
Founder van Pandora Intelligence

6

Renza Grüter 36
CPO van Zerocopter

7

Stef Liethoff 43
CEO bij SBL Cyber Security

8

Erik de Jong 50
Strategy Director van Securify

9

Dave Maasland 57
CEO van ESET Nederland

10

Jurjen Harskamp 65
Co-founder en CEO van Hunt & Hackett

11

Martijn van de Beek 73
Directeur van onderzoeksbureau Hoffmann

12

Christian Prickaerts 81
Directeur van Fox Crypto

13

Menno Stijl 87
Venture builder in de security industrie

14

Lara Hemstede 93
Founder van Cyber Proof & Rise App

15

Anouk Vos 98
Medeoprichter van Revnext

16

Evelien Bras 105
Directeur van FERM

17

Daan Rijnders 112
Kwartiermaker voor Digitaal Veilig Den Haag

18

Joris den Bruinen 118
Directeur van Security Delta (HSD)

19

Ben Kokkeler 128
Directeur-bestuurder van het Centrum voor Veiligheid en Digitalisering (CVD)

20

Hans de Vries 134
(oud) Directeur van het NCSC

21

Rutger Leukfeldt 139
Bijzonder hoogleraar en senior onderzoeker op het gebied van cybercrime

22

Queeny Rajkowski 145
VVD Tweede Kamerlid

Inzichten 151

Inzichten

Innovatie op sectorniveau

1

Innovatie in Nederland en Europa blijft achter. **152**

2

De markt is nog onvolwassen. Klanten ervaren daardoor ‘solution uncertainty’, wat de adaptatie van nieuwe oplossingen beperkt. **155**

3

Cybersecurity is een ‘trust and confidence game’. **157**

4

Er zijn kansen op het gebied van evidence based security. **158**

5

Innovatiekansen door begrip van klantvraag en primair proces: ‘de business’. **160**

6

Keep it simple: maak cybersecurity begrijpelijk voor iedereen. **163**

7

Invloed van grote technologiebedrijven, MSP’s, CSP’s of ISP’s worden sterker. **165**

8

Partijen staan open voor nog meer samenwerking en datadeling. **167**

9

Kansen voor security als sociaal verantwoord ondernemen. **169**

10

Kunstmatige Intelligentie (AI) biedt grote kansen en bedreigingen. **171**

11

De factor ‘mens’ wordt belangrijker. **173**

Innovatie en de overheid

12

Overheidsorganisaties zijn van nature gericht op het vermijden van risico's, waardoor echte innovatie binnen deze organisaties moeilijk te realiseren is. **174**

13

Er zijn te hoge verwachtingen van de overheid als het gaat om innovatie in cybersecurity. **176**

14

Juridisering biedt kansen voor innovatie. **178**

15

Er zijn kansen voor het cybersecurity start-up en scale-up ecosysteem. **180**

Innovatie op organisatieniveau

16

Innovatie = experimenteren, falen, nieuwsgierigheid en non-conformisme. **182**

17

Innovatie in cybersecurity vereist ambidextere organisaties. **184**

18

Innovatie gaat over meer dan alleen het product. **186**

19

Innovatie in cybersecurity gaat ook om uitvoeringskracht. **188**

20

Een gestructureerde aanpak is cruciaal. **191**

De weg vooruit- vervolgstappen **193**

Begrippenlijst **195**

Dankwoord/ Over de auteurs **200**

1. Inleiding

Waarom een boek?
Toen ik aan dit boek begon, werd ik gedreven door een perceptie die mij niet losliet: de indruk dat de wereld van cybersecurity vaak ingetogen en soms conservatief was in een zee van technologische innovatie en een maatschappelijke behoefte. Waarom leken ontwikkelingen op het gebied van digitale beveiliging minder snel voet aan de grond te krijgen dan in andere sectoren? Werd de sector geremd door zijn eigen voorzichtigheid, of speelden er andere factoren?

Cybersecurity is immers een domein met grote risico's en kleine foutmarges. Het is een wereld waar een misstap kan leiden tot catastrofale gevolgen, van datalekken die de privacy van miljoenen schenden tot aanvallen die vitale infrastructuren kunnen verlammen. Voorzichtigheid is daarom geen teken van zwakte, maar een noodzakelijke houding om het vertrouwen niet te schaden.

Echter, deze voorzichtigheid mag geen excuus zijn voor stagnatie. Terwijl innovatie buiten de grenzen van security welig tiert, dient de IT-security industrie de balans te vinden tussen de bescherming van het bestaande en de omarming van het nieuwe. Dit is de kern van mijn zoektocht en de eerste '*why*' achter dit boek.

Daarnaast worden we in nieuwsmedia vaak geconfronteerd met de schaduwzijden van de digitale wereld: de datalekken, de hacks, de privacyschendingen. Deze incidenten worden breed uitgemeten, terwijl de successen en doorbraken in de cybersecurity zelden de voorpagina's halen. Het lijkt alsof we enkel in termen van risico's en dreigingen spreken, terwijl er een wereld van mogelijkheden en kansen onbelicht blijft. Het belichten van de kansen kan worden gezien als de tweede '*why*'.

De Nederlandse cybersecuritysector staat - zeker met de opkomst van AI - op een kruispunt. De timing van dit boek is ironisch genoeg, "just in time". De meeste interviews onderstrepen dit keerpunt in de tijd. Zo geeft Renza Grüter, CPO van Zerocopter, bijvoorbeeld aan: "Er wordt op dit moment onvoldoende geïnnoveerd binnen de securitybranche. We zijn te traag. Veel te traag. We staan aan de vooravond van een evolutie waarin mens en technologie steeds meer met elkaar gaan samenwerken en in elkaar verweven raken. Security gaat over vertrouwen creëren én behouden in technologie."

Dave Maasland, CEO van ESET, benadrukt ook dat de integriteit van onze technologie op het spel staat: "Vertrouwen krijgen en behouden in de integriteit van systemen, technologie én data binnen de private sector, de overheid en het onderwijs is onze verantwoordelijkheid."
Dat er een onzekere tijd aankomt wat betreft technologie onderstreept ook Peter de Kock, oprichter van Pandora Intelligence. Hij verwoordt het als volgt: "Vroeger waren trends makkelijker te voorspellen: de wereld veranderde eigenlijk helemaal niet zo snel. Als je tien jaar terug keek, kon je met hetzelfde verschil wel een voorspelling maken voor de komende tien jaren. Het was een soort 'tangent line' die je door kon trekken. Maar die methode werkt nu niet meer. Kijk alleen al naar ons onderwijssysteem. Je kunt geen opleidingen meer

ontwikkelen op basis van alleen historische kennis. De 'oudere' generatie kijkt tien of twintig jaar terug, terwijl je juist vooruit moet kijken. Tegenwoordig is er meer behoefte aan een 'ambidextere organisatie', oftewel een organisatie die tegelijkertijd terug én vooruit kijkt."

Als we alleen kijken naar AI, zie je ook dat er onzekerheden zijn over de ontwikkeling hiervan. Dit werd versterkt door een open brief over de gevaren van AI die werd ondersteund door diverse prominente figuren uit de technologiewereld. Onder de ondertekenaars waren onder anderen de bekende schrijver Yuval Noah Harari, IT-topman Steve Wozniak en miljardair Elon Musk. In de brief werd opgeroepen tot nauwere samenwerking en regulering in het veld van kunstmatige intelligentie.

En dat is de derde en belangrijkste *why:* er is een groeipotentie die onze economie, onze staatsveiligheid en onze maatschappelijke welvaart ten goede kan komen.

Maar welke bijdragen kunnen we nog meer leveren aan een veiligere samenleving én het behoud van vertrouwen in onze technische systemen?

Centrale vragen

In dit boek proberen we antwoord te geven op de volgende vragen:

- *Hoe kan innovatie op sectorniveau beter georganiseerd worden?*
- *Hoe kan innovatie op organisatieniveau beter georganiseerd worden?*
- *Wat kunnen we leren van 'best practices' van innovatie?*
- *Wat zijn de belangrijkste trends en ontwikkelingen voor de toekomst?*

De uitkomsten van de interviews zijn verwerkt in 20 inzichten die aanzetten tot denken en startpunt zijn van discussie.

Twintig koplopers

De twintig koplopers die ik voor dit boek heb geïnterviewd, doorbreken de stereotypen. Ze illustreren dat de cybersecuritysector wel degelijk bol staat van innovatie. Hun verhalen getuigen van een wereld die zich in rap tempo wil ontwikkelen en die noodzakelijk is voor de bescherming van onze toekomst.

Hoe te lezen?

Security Innovation Stories is een bundeling van interviews met als afsluitend hoofdstuk de 20 inzichten. Elk interview staat op zichzelf. We beginnen met de CISO's. Deze groep representeert immers de klant. Daarna volgen de leveranciers van oplossingen en de vertegenwoordigers vanuit de overheid. Afsluitend delen ook de wetenschap en politiek hun inzichten. De interviews zijn gehouden tussen maart en december 2023.

2. Definities

In dit hoofdstuk leggen we het fundament voor de definities security, de sector en innovatie.

Cybersecurity, waar hebben we het dan over?

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) definieert cybersecurity in het Cybersecuritybeeld Nederland 2020 als volgt[1]: "Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan".

Cybersecurity: een term die niet iedereen graag gebruikt

De term cybersecurity wordt niet door alle geïnterviewden gebruikt. Het wordt soms gezien als een marketingterm of een term die de overheid gebruikt en minder aansluit bij de terminologie van de technische community van securityspecialisten.

Digitale veiligheid

Alternatieve termen voor cybersecurity zijn: digitale veiligheid, digitale beveiliging, security of IT-security. Waarbij digitale veiligheid door het NCSC (Nationaal Cyber Security Centrum) wordt gedefinieerd als: "Het beschermen van computersystemen, netwerken en data tegen ongeautoriseerde toegang, aanvallen, diefstal of schade aan hun hardware, software of elektronische data, evenals van de verstoring of misleiding van de diensten die zij voorzien."

Weerbaarheid als alternatief

Maar koplopers van alle definities zijn toch wel de woorden "weerbaarheid", "digitale weerbaarheid" en "cyberweerbaarheid".
Erik de Jong, Strategy Director bij Securify, geeft aan: "Het gaat over kwaliteitsaspecten van informatie: beschikbaarheid, integriteit en vertrouwelijkheid. Samengevat gaat het om de beheersing van het proces om ervoor te zorgen dat deze drie elementen voldoende gewaarborgd zijn. Erik vervolgt: "Ik zeg met nadruk voldoende, omdat dat natuurlijk nooit honderd procent is. Eigenlijk vind ik weerbaarheid een beter woord dan security."

Menno Snel, Venture Builder in security, gebruikt ook liever het woord weerbaarheid in plaats van security, want het is breder. "Met zijn allen zijn we weerbaar. In de dertiende eeuw hadden we namelijk weersinvloeden. Dan kwam er een storm en dan liep ons land onder. Daarom is innovatie in security ook zo moeilijk, want je weet niet wanneer de storm komt, je weet alleen dát die komt. In security maken we vooral veel pleisters of we zijn veel aan het pompen maar we zijn niet bezig met het bouwen van dijken."

Het NCSC hanteert de volgende definitie als het gaat om cyberweerbaarheid: "Het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT."

Cybercrime

De term cybercrime komt ook vaak terug in de interviews. Bij cybercrime gaat het om misdaden die gepleegd worden met een ICT-middel, en die gericht zijn op ICT (bijvoorbeeld politie.nl). Daarnaast gaat het om gedigitaliseerde criminaliteit, waarbij klassieke delicten via een ICT-middel gepleegd worden. Cybercrime komt vaak ook ter sprake wanneer slachtoffers individuen of burgers zijn.

[1] Nationaal Coördinator Terrorismebestrijding en Veiligheid, Cybersecuritybeeld Nederland 2020

Wat is dan innovatie?

Er is geen eenduidige definitie van innovatie. Wat een innovatie precies is, wanneer er wel of niet van een innovatie kan worden gesproken en hoe een innovatie wordt gedefinieerd, hangt af van degene die het interpreteert: de gebruiker (= markt), de maker (= organisatie), of het collectief (= maatschappij). De meest gangbare definitie is die van de ECB (Europese Centrale Bank) waarin het gaat om: "De ontwikkeling en toepassing van ideeën en technologieën die goederen of diensten verbeteren of die hun productie efficiënter maken."

Niveaus van innovatie

Innovatie kent vele vormen. Evelien Bras, Directeur FERM Rotterdam, geeft in haar interview ook een handige indeling van innovaties als het gaat om abstractieniveau: "Innovatie is mogelijk op meerdere niveaus, bijvoorbeeld politiek, strategisch, tactisch of operationeel: Politieke innovatie gaat over het reageren op een veranderende maatschappelijke behoefte of mondiale uitdaging, wat tot vernieuwing leidt. Dit is een typische 'top-down' benadering. Strategische innovatie betreft de implementatie van nieuwe manieren voor huidige doelen - bijvoorbeeld om de concurrentiepositie van een organisatie te verbeteren, marktaandeel te vergroten of nieuwe markten

De cybersecuritysector

Hiervoor baseren we ons op het onderzoek: De economische kansen van de cybersecuritysector van Dialogic[2] en de beschouwing van Jurjen Harskamp van Hunt & Hackett.

Volgens deze publicaties bestaat de sector uit grofweg uit 4 actoren:

A. Partijen die actief zijn in cybersecurity R&D

Universiteiten en onderzoeksinstellingen die zich bezighouden met onderzoek en ontwikkeling van cybersecuritytechnologie. Dit is de primaire bron van vernieuwing die door andere delen van de waardeketen wordt gebruikt om te innoveren. Voorbeelden van deze actoren zijn TNO en TU Delft.

B. Producenten van cybersecurityproducten en -diensten

Dit zijn de bedrijven die cybersecurityproducten en -diensten produceren of leveren. Zij maken deels gebruik van de R&D die door de actoren in categorie A wordt uitgevoerd. Op basis van een onderzoek van ENISA[3] kan deze categorie worden opgesplitst in acht soorten activiteiten: educatie, software, hardware, distributie, consulting, implementatie, managed services en certificering. Binnen deze groep is sprake van veel afhankelijkheid. Een producent van cybersecurityhardware kan ook gebruik maken van de output van een partij die cybersecuritysoftware maakt. Vervolgens is er een partij die de implementatie hiervan doet, et cetera.

C. Partijen die cybersecurityproducten en diensten integreren in niet cybersecurityproducten en diensten

Dit is een groep actoren die wordt gekenmerkt door het feit dat hun output niet primair het aanbieden van cybersecurityproducten of diensten betreft, maar producten en diensten waarin cybersecurityproducten of diensten worden geïntegreerd. Alle producten

die gekoppeld kunnen worden aan digitale netwerken (laadpalen, MRI-scanners, slimme magnetrons, auto's, et cetera) moeten op een bepaald niveau cyberveilig zijn. Zij maken gebruik van de output van de partijen die onder B genoemd worden.

D. Gebruikers van cybersecurityproducten en diensten
Dit zijn de uiteindelijke afnemers van producten en diensten van partijen die onder B en C genoemd worden. Hierbij gaat het om consumenten, maar ook bedrijven en publieke organisaties. De output van deze bedrijven en publieke organisaties bevat geen cybersecurity component, maar zij hebben wel cybersecurityproducten en -diensten nodig om hun processen veilig te houden.

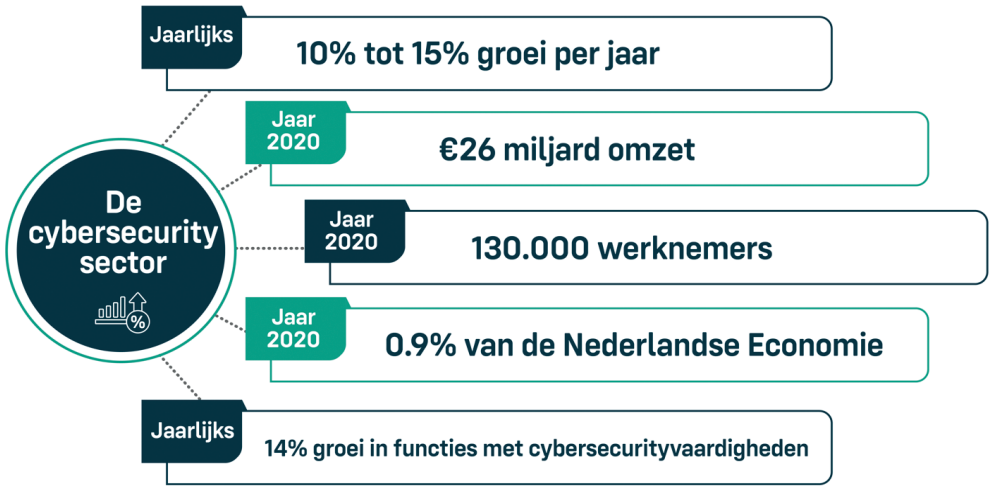
Jurjen Harskamp maakt ook nog een duidelijk onderscheid als het gaat om de producenten: "Er zijn technologie start-ups, managed security partijen (zoals Hunt & Hackett) en cybersecuritybedrijven die zich richten op consultancy diensten. Daarnaast is er de overheid met diverse entiteiten die zich met cybersecurity bezighouden, kenniscentra, universiteiten, belangenorganisaties en diverse onderlinge samenwerkingsverbanden. Een divers veld dus met verschillende spelers, die allemaal op een eigen manier innoveren."
De uitsplitsing van producenten is relevant, er zijn namelijk een aantal grote partijen in de markt en een hele grote groep kleinere leveranciers. De grote partijen bieden vaak diensten aan die ook exporteerbaar zijn, zoals managed services.

Hoe groot is de sector nu eigenlijk?
Volgens het rapport van Dialogic kent de Nederlandse cybersecuritysector een flinke groei van tien tot vijftien procent per jaar. In 2020 draaide de sector een omzet van €26 miljard, behaalde een toegevoegde waarde van bijna €13 miljard en kende de sector ruim 130.000 werknemers. De cybersecuritysector omvat daarmee circa 0,9% van de Nederlandse economie.

Als we kijken naar de groei in functies met hierin cybersecurityvaardigheden, is dit veertien procent op jaarbasis. Recentere onderzoeken zijn er niet, maar gezien de steeds grote rol van IT binnen de maatschappij, wordt dit aandeel steeds groter. Meer informatie hierover vind je in het rapport 'Economische kansen van de cybersecuritysector', door Dialogic, in opdracht van het Ministerie van Economische Zaken en Klimaat[4].

[2] De economische kansen van de cybersecuritysector van Dialogic in opdracht van EZK
[3] ENISA Cybersecurity Market Analysis Framework (ECSMAF)

De cybersecuritysector in een overzicht:



[4] De economische kansen van de cybersecuritysector van Dialogic in opdracht van EZK

''Als pleitbezorger voor Europese innovatie vind ik dat we onze vitale infrastructuur zelf moeten beschermen met eigen oplossingen.''

3. Dimitri van Zantvliet
- Directeur cybersecurity bij de NS

Dimitri van Zantvliet, directeur cybersecurity bij de Nederlandse Spoorwegen, vertelt over de cyberstrategie bij de NS. De strategie is op vier pijlers gebaseerd: een radical shift left, gecentraliseerde securitydiensten, zero trust en een cybersafe culture. “Uiteindelijk draait het ook om de adaptatie van innovatie, en daar is vertrouwen in de technologie voor nodig”, stelt Dimitri. Hij pleit voor meer innovatie vanuit Nederland en Europa, om zo minder afhankelijk te worden van buitenlandse leveranciers en de eigen soevereiniteit te waarborgen.

Combinatie van strategie en techniek

Dimitri is gefascineerd door de complexiteit die de cyberwereld met zich meebrengt, het groter wordende dreigingslandschap en het maatschappelijke belang. Na twintig jaar in de IT nam hij daarom tien jaar geleden de afslag richting cybersecurity. Hij werkte onder andere als consultant cybersecurity & compliance, CISO, CIO en CTO bij verschillende organisaties. Nu is hij directeur Cybersecurity bij de Nederlandse Spoorwegen. “Het is een voorrecht om directeur te zijn voor het hele cyberdomein van de NS, waar twintigduizend collega’s in werken. In mijn werk kom ik alles tegen: van IT-, OT- en AI-uitdagingen tot aan governance, risk en compliance”, vertelt Dimitri.

De combinatie van strategie en technologie vindt hij het mooist aan zijn werk. “Ik ben redelijk technisch, ondanks dat ik strategisch bezig moet zijn. En ik duik graag de diepte in. Om maar een voorbeeld te noemen: in een appgroep kunnen we eindeloos discussiëren over een stukje hacksoftware. Ik word gewoon vrolijk van technologie. Die combinatie van strategie en techniek past echt het beste bij mij.”

> **“Ik denk dat we vanuit Nederland, en zelfs vanuit Europa, soms de boot dreigen te missen. We hebben veel innovatiekracht verloren en leunen erg op buitenlandse leveranciers. Met alle risico’s van dien natuurlijk.”**

Niet genoeg innovatie vanuit Nederland en Europa

Volgens Dimitri draait innovatie om het toepassen van technologie en iets radicaal anders doen, om de doelstellingen van een organisatie of de maatschappij beter te maken. Hij ziet dat er veel ideeën ontwikkeld worden in de sector, en dat er in Nederland ook geld gestopt wordt in start-ups. Toch vindt hij dat we niet voldoende innoveren op het gebied van cybersecurity. “Wereldwijd gebeurt er genoeg, maar minder vanuit Nederland en Europa”, stelt hij. Het aantal cyberscale-ups en unicorns is dan ook op één hand te tellen.

Hij licht toe:“Ik denk dat we vanuit Nederland, en zelfs vanuit Europa, soms de boot dreigen te missen. We hebben al veel innovatiekracht verloren en leunen erg op buitenlandse leveranciers. Amerika en China stoppen veel geld in ons afhankelijk maken

van cloudoplossingen en allerlei IoT-spullen. Met alle risico's van dien natuurlijk. Je ziet dat Europa daar eigenlijk geen antwoord op heeft. En straks ben je gewoon te laat om die achterstand nog in te halen."

Dimitri legt uit dat het decennia duurt voordat Europa dat bij kan benen. Europa heeft volgens hem te weinig gedaan om hun soevereiniteit te bewaken. "Voor grote delen van de werking van het internet zijn we te afhankelijk van buitenlandse oplossingen. We zouden ons wat mij betreft wel meer moeten richten op eigen oplossingen als het gaat om de vitale infrastructuur."

Europese soevereiniteit en Defend Forward

Inmiddels staat Dimitri bekend als 'pleitbezorger voor Europese – of zelfs Nederlandse – innovatie', vertelt hij. Op technologisch gebied zijn we in Europa steeds afhankelijker en hij vindt toch dat er ook oplossingen in Europa ontwikkeld moeten worden. "Alleen het kost tijd om daar te komen", zegt hij. "Dus ik zou zeggen: ga eens nadenken over hoe we die Europese soevereiniteit wat beter kunnen ondersteunen met technologische oplossingen. Dat doen we niet voldoende en moet beter georganiseerd worden. Je hebt nu namelijk de Fransen en Duitsers die eigen soevereine cloudoplossingen hebben, maar niet willen samenwerken. En dat zie je bij Gaia-X ook gebeuren en dat is een gemiste kans."

Gaia-X is een Europese cloudoplossing, maar komt lastig van de grond. "Volgens mij is het al tien jaar geleden uitgetekend. En het is een paar keer bijna mislukt. Blijkbaar is het een enorm complex politiek mijnenveld. Dit soort zaken vallen in de categorie politiek-maatschappelijke innovatie, wat juist nu heel erg belangrijk is."

Daarnaast denkt Dimitri dat we in Nederland en Europa vrij reactieve reflexen hebben als het om cybersecurity gaat. In de Verenigde Staten gaat dat er met de 'Defend Forward'-strategie van Biden heel anders aan toe. Hij legt uit dat dit wil zeggen dat je offensieve tactieken toepast om zogeheten advanced persistent threats in hun eigen regio uit te schakelen door hun infrastructuur te beschadigen. "Dat zijn strategieën die nodig zijn om ons niet dag en nacht bezig te laten zijn met allerhande ransomwarevraagstukken", vult Dimitri aan. "In sommige gevallen, zeker voor de vitale infrastructuur, zou je als overheid echt een proactievere aanpak moeten hebben. Ik vind dat we daar een soort cyberleger moeten hebben, dat de 'Defend Forward'-strategie ook hanteert. Want iedere keer maar aangevallen worden en herstellen, dat is redelijk vermoeiend. Het cyberlandschap is echt radicaal verslechterd de afgelopen jaren."

> **"De NS is één van de meest hyper connected companies van Nederland. We hebben een grote hoeveelheid gepubliceerde API's, om zoveel mogelijk andere platformen en oplossingen te kunnen koppelen."**

Lange innovatietrajecten versus agile werken

Ook met de NS bevindt Dimitri zich in een speelveld dat deels Europees gedirigeerd

is. Maar innoveren is soms een kwestie van een lange adem: “Ons bedrijf opereert op het spanningsveld tussen traditioneel waterval management en agile werken. Als het bijvoorbeeld gaat om fysieke assets, zoals het vervangen van treinen, dan gaat het om lange trajecten met grote orders. Treinen rijden soms wel veertig jaar.” Dimitri zegt dat innovatie dan een hele lange cyclus en een complexe dynamiek heeft. Hij noemt het voorbeeld van het ERTMS, het European Rail Traffic Management System. “Dat duurt bijna vijftig jaar om het in heel Europa te implementeren. Het nadeel van deze lange trajecten is dat als wij eenmaal iets doorgevoerd hebben, het niet meer zo innovatief is als toen we het bedachten.”

Daar staat echter tegenover dat op het gebied van software ze wél snel kunnen zijn met een agile aanpak. “Binnen een paar maanden hebben we voor heel de NS een eigen ChatGPT-omgeving neergezet. Deze is veiliger in gebruik, omdat ingevoerde prompts niet worden gebruikt om het model te trainen. Dit samenspel tussen twee uitersten maakt het een enorm boeiend bedrijf om voor te werken.” Dimitri gaat verder door te zeggen dat de NS een van de meest hyper connected companies van Nederland is. “We hebben een grote hoeveelheid gepubliceerde API’s, om zoveel mogelijk andere platformen en oplossingen te kunnen koppelen. In totaal gaat het om meer dan twaalf miljard API-calls per jaar. Dit is met name voor deur tot deur vervoer. Niet alleen treinen, maar ook andere vervoermiddelen zoals fietsen en GreenWheels. Voor deze manier van reizen dient alles aan elkaar gekoppeld te worden.”

De vier security pijlers van de NS

De security strategie van de NS kent vier pijlers, vertelt Dimitri. “Deze strategie heeft invloed op hoe wij op cybergebied innoveren.” Hij legt ze één voor één uit:

Pijler 1: Radical shift left

“Het uitgangspunt hierbij is security by design en default. We nemen veiligheid dus vanaf het begin mee bij het bouwen van software en applicaties, in plaats van het later toe te voegen of te zien als een reactieve maatregel.”

Pijler 2: Gecentraliseerde securitydiensten

“Dit is ondersteunend aan pijler 1. We hebben meer dan driehonderd development teams, met eigen pipelines en code. Door gecentraliseerde code reviews, SAST/DAST en secret- en vulnerability scans aan te bieden, helpen we onze business compliant te zijn aan onze standaarden.”

Pijler 3: Zero trust

“Bij dit principe ga je er standaard van uit dat niets of niemand te vertrouwen is. We kijken dan naar identiteiten, endpoints, applicaties, netwerken en data. Bij zero trust worden deze vijf elementen altijd gecontroleerd. Pas als iets of iemand heeft bewezen dat hij betrouwbaar is, krijgt hij toegang tot bijvoorbeeld het bedrijfsnetwerk, applicaties of een database. Dat betekent eigenlijk dat je van perimeter based security naar identity based security gaat.”

Pijler 4: Cybersafe culture

“De essentie van deze pijler is dat we streven naar een veiligheidscultuur voor cyber

die vergelijkbaar is met fysieke veiligheid. De medewerker die boven op de trein moet werken voor onderhoud weet dat hij of zij de reling van de trap moet vasthouden, dat is nu onbewust bekwaam gedrag. Die cultuur willen we ook bereiken in het cyberdomein."

Succesfactoren voor innovatie

Het opleiden van personeel levert een grote bijdrage aan het verbeteren van de cybersecurity van het bedrijf. Dimitri zegt: "We leiden bijvoorbeeld nu enkele operationele medewerkers op tot cyberexperts. Zij weten precies hoe systemen gebruikt worden in het dagelijkse proces. Daardoor kun je met passende oplossingen komen. Stel dat wij bedenken om alles achter MFA te stoppen, maar een conducteur vertelt dat je dan zes keer moet inloggen. Dat werkt natuurlijk niet en dan kun je samen beter een andere oplossing bedenken."

Dimitri vertelt dat ze als securityafdeling vervijfvoudigd zijn qua capaciteit in twee jaar. Op een innovatieve manier kijken naar het personeelsbestand heeft hen daar erg mee geholpen. "Het is best innoverend, voor de NS in ieder geval. Maar ik denk dat de hele sector hier baat bij heeft, want de aanwas is beperkt. We moeten veel meer mensen zelf opleiden. En we hebben een cybersecurity academy opgericht om de horizontale doorstroom te bevorderen."

De belangrijkste succesfactor voor innovatie is volgens Dimitri het vertrouwen dat mensen in de technologie hebben. Hij legt uit dat ze vanuit de NS vaak kijken naar de toekomst van vervoer. Zij zien dat er in die nieuwe digitale metropolis behoefte is aan een frictieloze beleving van vervoer om zo makkelijk mogelijk van A naar B te komen. "Uiteindelijk gaan we niet naar smart cities, maar zelfs naar cognitive cities", vertelt Dimitri. Een concept waarbij kunstmatige intelligentie een nog dominantere rol zal hebben. "Wanneer we als NS frictieloos vervoer gaan regelen, is vertrouwen in technologie en data essentieel voor de adaptatie van de innovatie. Vertrouwen is daarmee de belangrijkste indicator voor succes. Het moet duurzaam en veilig zijn, zowel fysiek als digitaal. Fysieke veiligheid geldt specifiek voor op stations, in de trein en rond het spoor. En digitale veiligheid met het gebruik van onze digitale diensten. Vertrouwen in de technologie, in het veilig zijn van data en in de privacy is echt essentieel voor de adaptatie van innovatie."

Continuïteit van dienstverlening

De NS heeft nog een andere belangrijke overweging als het om innoveren gaat: het mag de continuïteit van dienstverlening niet in gevaar brengen. Tegelijkertijd kan innovatie juist ook helpen om continuïteit te realiseren. Sinds december 2021 is de NS aangemerkt als Aanbieder Essentiële Diensten (AED). Daarmee dient de NS de beschikbaarheid van hun vitale diensten op peil te houden.

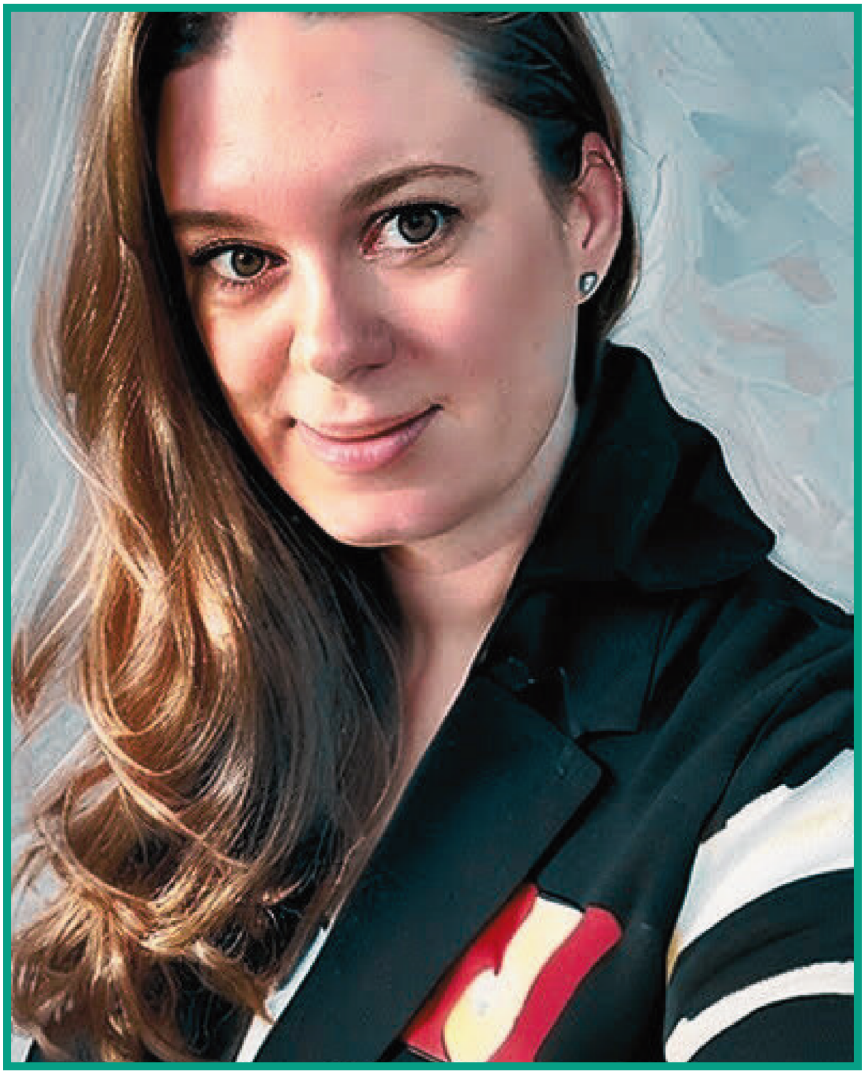
"De verpleger, beveiliger of politieagent moet altijd naar zijn of haar werk kunnen gaan", legt Dimitri uit. "Dat hebben we in de coronaperiode wel gemerkt. We vervoeren meer dan een miljoen reizigers per dag. Als wij eruit liggen heeft echt heel Nederland daar last van. We moeten dus onze dienstverlening kunnen garanderen. Dat heeft invloed op hoe wij innoveren, omdat het niet ten koste mag gaan van de continuïteit van onze dienstverlening. En het is voor ons echt belangrijk dat innovatie bijdraagt aan het maatschappelijk belang."

> **"Als we kijken naar de hyper connectivity en het veranderende dreigingslandschap, dan verwacht ik wel dat AI de menselijke factor in detectie en response overneemt. Dit is niet te voorkomen. Stel dat we straks door AI worden aangevallen, dan moet je daar ook geautomatiseerd en met AI op reageren."**

Trends in cybersecurity
We vragen Dimitri tot slot wat hij ziet als de grootste trends in de cyberwereld de komende vijf jaar. Als eerste trend noemt hij 'zero trust', wat steeds meer tractie krijgt in de sector. Daarnaast zullen volgens hem ook oplossingen voor data soevereiniteit en encryptie steeds meer in beeld komen. Ten derde noemt Dimitri edge computing. Hierbij vinden berekeningen en gegevensverwerking niet alleen in centrale datacenters plaats, maar ook dichter bij de bron van de gegevens.

En ook Dimitri kan niet om AI heen. Hij zoomt met name in op het detectie- en responsewerk, dat steeds meer door AI overgenomen wordt. "Ik zie dat als de enige oplossing om adequaat op dreigingen te reageren. Als we kijken naar de hyper connectivity en het veranderende dreigingslandschap, dan verwacht ik wel dat AI de menselijke factor in detectie en response overneemt. Dit is niet te voorkomen. Stel dat we straks door AI worden aangevallen, dan moet je daar ook geautomatiseerd en met AI op reageren."

Als laatste trend noemt Dimitri cybersecurity in de boardroom. Met de nieuwe NIS2 wetgeving in aantocht en het exponentieel toenemende dreigingslandschap zullen Nederlandse bestuurders zich meer en meer moeten gaan bezighouden met deze nieuwe risicocategorie. De CISO zal in steeds meer digitale bedrijven een vaste plek op de RvB-agenda krijgen en ook direct gaan rapporteren aan een van de bestuurders. Zorg ervoor dat je je hier als CISO op voorbereid door een breder pakket aan kennis en kunde te gaan ontwikkelen dan enkel cybersecurity.



''De innovatie is er wel, maar het gaat langzaam. Ook omdat de problemen heel fundamenteel zijn.''

4. Fleur van Leusden
- CISO bij de Kiesraad

Haar opleiding criminologie en fascinatie voor computers bleken een gouden combinatie om de cyberwereld in te gaan: Fleur van Leusden, CISO bij de Kiesraad, is kritisch en ambitieus. Zij stelt de vragen die niemand meer vraagt om fundamentele problemen in de sector op te lossen. Innovaties zijn er genoeg alleen niet altijd waar het nodig is, vindt ze. Ook leiden trends als AI en XDR volgens Fleur af van de échte problemen waar we naar zouden moeten kijken.

Criminoloog in informatiebeveiliging

Opgeleid als criminoloog en een fascinatie voor computers. Het was de ideale mix voor Fleur om het IT-securitydomein in te gaan. “Ik deed altijd al veel met computers”, vertelt Fleur. “Websites bouwen, gamen. En in mijn studententijd had ik ook al veel bijbaantjes in de tech industrie.” Er was door een recessie weinig werk voor criminologen toen Fleur haar masterdiploma behaalde. Maar ze liet zich niet tegenhouden en solliciteerde op de vacature voor internetrechercheur bij de politie. Een baan op mbo-niveau. “Dat was natuurlijk onder mijn opleidingsniveau, maar dat interesseerde me niet zoveel. Het was erg leuk werk en zo kon ik toch iets doen wat gerelateerd was aan mijn studie.”

Fleur werd één van de eerste internetrechercheurs in Nederland. Maar ze wilde meer. “Ik wilde doorontwikkelen, alleen dat ging lastig bij de politie. Men vond mij te jong voor hogere functies. Ondertussen werd ik benaderd door IT-bedrijf Capgemini. Zij wilden mij langere tijd detacheren bij de overheid voor een aantal klussen. De voorwaarden waren ook veel beter. Een makkelijke keuze dus.”

Door te werken voor de overheid kon Fleur bijdragen aan het publieke belang. Dat was een belangrijke voorwaarde voor haar. Het beviel goed. Na vier jaar bij Capgemini werd ze benaderd door de Onderzoeksraad voor Veiligheid om daar te gaan werken als digitaal onderzoeker. Een mooie kans, want er was nog niets geregeld op digitaal vlak.

> **“Security wordt vaak gezien als de party pooper. Er is niemand die denkt: ‘Yes, daar is security!’ Dan vind ik het extra leuk om te horen van mensen die niet werken in de security dat security hun project beter heeft gemaakt.”**

Werken als CISO

Bij de Onderzoeksraad voor Veiligheid ontwikkelde Fleur zich op het gebied van security. “Ik heb echt leuke dingen kunnen doen daar. Zo heb ik onderzoek gedaan naar de security van zelfrijdende auto’s en technologische hulpmiddelen bij het rijden, zoals cruise control en lane assist. En ik onderzocht onder andere de Tesla-hacks van Tencent en grote ICT-storingen in ziekenhuizen waar de veiligheid van patiënten in het geding kwam. Ik leerde hier zoveel van. En ik merkte ook dat ik steeds meer met security wilde doen. Daar had ik dan ook wel

een mening over, al werd dat niet altijd gewaardeerd. Bijvoorbeeld wanneer ik aangaf dat de security voor verbetering vatbaar was."

Dat was de aanleiding dat Fleur uiteindelijk de overstap maakte naar de Autoriteit Consument & Markt (ACM) waar ze een CISO zochten. Dit was precies waar ze naar op zoek was. "Als CISO mag je dus ook echt iets van security vinden. Ik heb hier ook weer een andere kant leren kennen, omdat het een organisatie is die eigen netwerkbeheer doet. Op technisch vlak kun je als CISO dan heel veel leren. En ik kreeg een team om me heen, waardoor ik me ook meer met strategische dingen kon bezighouden. Na de ACM ging ik aan de slag bij de Kiesraad, in hetzelfde gebouw."

Bij de Kiesraad werd er goed nagedacht over de positionering van de rol van een CISO. Waar plaats je de CISO in je organisatie, zodat deze persoon effectief kan werken? De Kiesraad koos ervoor om de CISO direct aan de directeur te laten rapporteren. Hiermee creëerden ze korte lijnen en meer zeggenschap, iets wat voor Fleur heel goed werkte. Dat was ze niet gewend vanuit haar vorige rol, waar ze onder een manager CIO viel die aan de directeur rapporteerde, die vervolgens aan het bestuur rapporteerde. "Informeel gezien was de stap naar het bestuur niet heel groot. Ik kon ze op een laagdrempelige manier benaderen. Maar hiërarchisch gezien was dat veel spannender. Als de directeur of de manager CIO bijvoorbeeld niet op één lijn zaten, dan konden ze mij bij wijze van spreken de deur uitwerken. Zij waren mijn meerdere, dus dat was soms een drempel. Die kan je één of twee keer nemen. Ik ben nu selectiever waar ik werk."

Security en innovatie

Een van de mooiste dingen in haar werk vindt Fleur het neerzetten van projecten waar de beveiliging netjes geregeld is én vanaf het begin is meegenomen. "Security wordt vaak gezien als de party pooper. Er is niemand die denkt: ' Yes, daar is security'. Dan vind ik het extra leuk om te horen van mensen die niet werken in de security dat security hun project beter heeft gemaakt."

Maar Fleur ziet dat het ook anders kan. "Als mensen zich er overheen kunnen zetten dat security niet altijd leuk is. Als mensen kunnen luisteren naar waarom het belangrijk is en meedenken. Dat het niet alleen maar vervelend is. Of dat het niet alleen een probleem is van mensen die verantwoordelijk zijn voor security. Dan krijg je echt een kwalitatief beter product", zegt ze. "En dat is iets waar iedereen blij mee is. Niet alleen de 'security mensen', maar ook de gebruikers en de mensen die het gaan bouwen."

Het beste voorbeeld van security by design vindt Fleur de homeknop van de iPhone die ook als een vingerafdruk werkt. Die knop moet je sowieso indrukken, dus een gebruiker hoeft niets extra's te doen ten opzichte van de normale handelingen. En de telefoon is wel veiliger. Fleur ziet innovatie dan ook als iets wat voorheen niet kon, of wat heel veel beter kan. "Er dient sprake te zijn van een significante verandering of verbetering", stelt ze.

Fundamentele problemen

Fleur ziet veel pogingen in de securitysector om te innoveren. "De innovatie is er wel, maar het gaat langzaam. En dat ligt denk ik ook aan dat de problemen waar we mee worstelen

heel fundamenteel zijn." Ze legt uit dat het niet komt omdat er te weinig slimme mensen zijn, dat er niet genoeg geld is of dat regels ons te veel tegenhouden. De vraagstukken zijn te fundamenteel. "Om een voorbeeld te noemen. Het feit dat wij nog steeds wachtwoorden nodig hebben voor veel dingen. Daar zijn innovaties voor. Maar die innovaties zijn niet goed genoeg om écht wachtwoorden te gaan vervangen."

Dat is wat Fleur een fundamenteel probleem noemt: een probleem waar maar geen oplossing voor lijkt te komen. "Er zijn geen mensen in de securitywereld die wachtwoorden een goed idee vinden. Tweefactorauthenticatie maakt het iets minder slecht maar het is niet vergelijkbaar met die homeknop van de iPhone. En dat zoeken we eigenlijk wel."

We vragen haar wat er dan wel is op dit gebied. Ze noemt de Fast Identity Online Alliance (FIDO). "Het vervangt wachtwoorden voor bijvoorbeeld een code", zegt Fleur. "Iets anders is de YubiKey, een andere vorm van tweefactorauthenticatie. Is dat dan innovatie? We proberen heel veel, maar het lost het fundamentele probleem van wachtwoorden niet op. Het ei van Columbus hebben we nog niet gevonden."

> **"Je mensen in de operatie zijn je last line of defense en ze zijn níet de zwakste schakel."**

Generieke innovaties

En dat is met meer zaken zo, legt Fleur uit. "We worstelen bijvoorbeeld ook nog met configuratieproblemen. Op dit gebied worden veel fouten gemaakt. En wat ook vaak fout gaat, zijn autorisaties. Mensen hebben vaak te veel rechten. Of te lang. Dan hebben ze rechten die ze al lang niet meer zouden moeten hebben. Je kunt hier allerlei slimmigheidjes voor bedenken, maar dat is nog geen Active Directory. Dat was trouwens wel een innovatie, dat durf ik wel te zeggen. Waarom? Omdat het autorisaties in een Windows netwerk veel eenvoudiger en veiliger maakte dan daarvoor."

Fleurs conclusie: we innoveren niet voldoende in de sector. Maar dat komt niet omdat we het niet proberen. Ook ziet ze veel innovaties voor minder prangende onderwerpen. "Ik denk dan: leuk bedacht, maar het is een andere naam voor iets wat al bestaat."

Volgens Fleur heeft het bedrijfsleven snel de neiging om te roepen dat ze weten waar mensen naar op zoek zijn. "Ze zeggen tegen mij: ik begrijp je. Maar dan komen ze met iets wat het tegenovergestelde is van wat ik vroeg. Aan wie ligt dat dan? Dat weet ik niet. Het kan aan mij liggen en een beetje aan beiden. Maar ik word niet goed genoeg geholpen. Dat hebben alle klanten vermoed ik wel een beetje." Fleur denkt ook dat dit komt doordat eindklanten, zoals zij, specifieke wensen hebben. Die wensen wijken af van wat andere mensen willen. En leveranciers willen juist iets bouwen wat ze op grote schaal kunnen toepassen, en willen daardoor meer generiek zijn. Dan hoeven ze immers maar één keer te investeren. "Je kan dingen makkelijk van de plank krijgen, maar dat past zelden bij wat je nodig hebt. En als je wilt wat je nodig hebt, dan moet je daar veel voor betalen."

Awareness
Om tot innovaties te komen stelt Fleur de vragen die anderen niet meer stellen. Bijvoorbeeld op het gebied van nep phishing. Ze legt uit dat veel mensen in de securitysector dat al jaren doen, maar dat niemand meer nadenkt waarom eigenlijk. "Iedereen denkt immers dat het een goed idee is. Ik ben dan degene die toch de vraag stelt: Waarom doen we dit?"

De context waarin ze opereert is dat organisaties steeds minder aan eigen netwerkbeheer doen. Dit wordt vaak uitbesteed aan Managed Service Providers (MSP) of Internet Service Providers (ISP). Dat heeft twee kanten, legt ze uit. Enerzijds ontzorgt het, omdat het door een externe partij geregeld wordt. Anderzijds kun je niet altijd alles implementeren wat je wilt. "Als je op bepaalde punten extra beveiligingsmaatregelen wilt nemen, maar je MSP of ISP weigert dit, dan heb je dat maar te slikken. Je geeft dus wel een stuk autonomie op."

Ze vraagt zich af: wat valt er dan in deze context nog te verkopen aan een CISO? Of aan de security van een bedrijf? "Dan kom je uit op awareness. En die nep phishing e-mails verkopen goed, want ze zijn makkelijk, goedkoop en zichtbaar. En ze zorgen ook voor een shock in je organisatie. Iedereen doet het. Dus waarom zou je het niet doen?"

Ethisch discutabel, als je het Fleur vraagt. "Idealiter creëer je een omgeving van vertrouwen waarin mensen dingen kunnen melden", vertelt ze. "Zelfs al hebben ze hele domme dingen gedaan, dan nog sta je klaar om te helpen." Maar met nep phishing e-mails spuug je ze eigenlijk een beetje in het gezicht, vindt Fleur. En ze vult aan dat het ook niet altijd nodig is. "Naast het creëren van een vertrouwde omgeving moet je zorgen dat je de technische maatregelen op orde hebt. Je mensen in de operatie zijn je last line of defense en ze zijn níet de zwakste schakel."

Trends: AI en XDR
Met enige tegenzin beantwoordt Fleur de vraag wat de trends zijn in de securitysector de komende jaren: AI en Extended Detection and Response, oftewel XDR. "Dit moet ik wel toelichten. Het zijn trends, een hype. Maar geen innovaties. Het voegt feitelijk niets toe en het leidt af van de echte problemen waar we naar zouden moeten kijken."

Fleur stelt dat AI heel zinnig kan zijn, maar dat er ook heel veel bij komt kijken wat niet zinnig is. Er zijn standaard valkuilen. "Ik gebruik altijd het voorbeeld van de eekhoorn en de vos om dit uit te leggen. De eekhoorn lijkt op een vos: fluffy staart, opstaande oren, dezelfde kleur. Maar het is zeker geen vos. Bijna altijd zal AI het goed inschatten, maar in één procent van de gevallen ziet AI een eekhoorn in plaats van een vos. Dat is in dit voorbeeld niet zo erg. Alleen is het een ander verhaal als het om mensenlevens gaat. Dan is één procent heel veel."

Een opkomende AI-gerelateerde oplossing is XDR. Dit is een uitbreiding op Endpoint Detection Response (EDR). EDR richt zich alleen op het beveiligen van zogeheten endpoints, zoals laptops, servers of telefoons. XDR gaat een stap verder: het richt zich op het grotere geheel, dus ook de applicaties en gebruikersaccounts bijvoorbeeld. XDR kan daardoor patronen herkennen die over meerdere entiteiten gaan. Deze oplossing

maakt veel gebruik van AI. “Het wordt aangeprezen als oplossing die je beveiliging kan overnemen, maar dat is niet waar. Althans, nu nog niet. Met betrekking tot security moet je mechanismes hebben waar je voor honderd procent vanuit kunt gaan. Met AI kan dat niet. Het is te onvoorspelbaar en ondoorzichtig. AI is daarom nog niet geschikt om nu al securitytoepassingen over te nemen.”

“Verbeeldingskracht is belangrijker dan ooit in een tijd waarin de toekomst zich minder makkelijk laat voorspellen.”

5. Prof. dr. Peter de Kock
- Founder van Pandora Intelligence

Na een opvallende carrièreswitch richtte film- en documentairemaker Peter de Kock het bedrijf Pandora Intelligence op. Zijn innovatieve aanpak kenmerkt zich door voorspellende scenario's die bedrijven helpen weloverwogen beslissingen te nemen. Innovatie is volgens Peter 'een sprong voorwaarts in de tijd'. Verbeeldingskracht is daarvoor onmisbaar, omdat het helpt met nadenken over de onzekerheden van de toekomst. Een lastige opgave voor securitybedrijven, die erop gericht zijn om risico's te mijden.

Van de Filmacademie naar Master of Criminal Investigation

De loopbaan van Peter is bijzonder te noemen. Waar security bij veel specialisten met de paplepel werd ingegoten, ontdekte Peter zijn interesse hierin pas veel later. Na het afronden van de mavo en de havo koos hij voor de Filmacademie in Amsterdam, om vervolgens 15 jaar in de filmindustrie te blijven werken. Hij maakte films, series en documentaires in binnen- en buitenland. Zijn werkplekken bevonden zich ook in oorlogs- of conflictgebieden, maar vanaf het moment dat hij kinderen kreeg werd dat steeds ingewikkelder. Dit zorgde voor een opvallende carrièreswitch: Peter schreef zich in 2007 in voor de Master of Criminal Investigation aan de politieacademie.

Hoe een film inspiratie voor een carrièreswitch gaf

Waar zijn interesse in de politie vandaan kwam? Peter: "Één van de films die ik geregisseerd heb, is 'De handen van Che Guevara'. Deze film gaat over de zoektocht naar de afgehakte handen van de vrijheidsstrijder Ernesto Che Guevara. Hij was geëxecuteerd en moest geïdentificeerd worden aan de hand van zijn vingerafdrukken. Omdat deze gegevens uit Bolivia moesten komen en het lichaam van Guevara opgebaard lag in Bolivia, waar het langzaam begon te ontbinden, werd besloten zijn lichaam te begraven en zijn handen te bewaren. 40 jaar lang hebben zijn handen in een pot met sterk water heimelijk over de wereld gereisd, verborgen door sympathisanten van Guevara en gezocht door verschillende geheime diensten. Over deze reis, en het ontstaan daarvan, heb ik een film gemaakt. Waarheidsvinding was de kern van de film, en die waarheidsvinding heeft me bij de politie gebracht."

Eenmaal gestart met de master Criminal Investigation bleef Peter veel gelijkenissen zien met zijn eerdere werkveld. Zijn masterscriptie ging daarom over de voorspelbaarheid van crimineel gedrag op basis van scenario's zoals die in de filmindustrie worden gebruikt. Zijn scriptie werd uitgebracht in boekvorm binnen de politiewereld.

Van mavo naar Professor of Practice

Zijn scriptie zorgde voor veel verandering. Peter zette een nieuw team op, gericht op de beveiliging van belangrijke personen. De scenario's werden voorspeld op basis van eerdere gebeurtenissen. Dit werkte zó goed in de praktijk, dat Peter gevraagd werd om te promoveren. Een drukke periode volgde. "Overdag werkte ik bij de politie en 's nachts en in de weekenden schreef en studeerde ik", aldus Peter. Uit het voorspellingsmodel op basis van scenario's is het bedrijf Pandora Intelligence voortgekomen. Dit bracht hem ook naar zijn andere positie: Professor of Practice aan Tilburg University, en als hoofd Datascience in Crime & Safety bij JADS, Jheronimus Academy of Data Science.

Over Pandora Intelligence

"Als je mensen wilt begrijpen, moet je verhalen begrijpen. Dat is het concept waarop Pandora Intelligence is gebaseerd. Mensen verhouden zich tot elkaar door het vertellen van verhalen." Ook hier is volgens hem een link met de filmacademie te zien: "Pandora Intelligence levert een op maat gemaakte intelligence-oplossing voor bedrijven en overheden. Klanten kunnen gegevens verzamelen, analyseren en interpreteren op een manier die niet mogelijk is met het menselijk brein. Dit biedt hen inzichten waarmee ze betere beslissingen kunnen nemen.

De oplossing werkt met twaalf scenario-componenten. Met deze componenten vertel je als het ware het kernverhaal van je bedrijf of afdeling. Voor opsporingsinstanties kan dat het verhaal zijn van criminaliteitsbestrijding, voor vrachtvervoerders het verhaal van hun logistiek proces, voor banken het verhaal van customer due dilligence en voor verzekeraars het verhaal van fraude of cybercrime. Het bepalen van het verhaal doe je maar één keer, daarna genereert onze oplossing automatisch duizenden scenario's uit de data van de klant en rubriceert de scenario's naar mate van aannemelijkheid. Het monitort dan bovendien nieuwe ontwikkelingen op dagelijkse basis. Dit biedt klanten iets 'bovenmenselijks', namelijk het verwerken van heel grote hoeveelheden dynamische gegevens, en helpt hen complexe beslissingen te nemen op basis van begrijpelijke scenario's.

Een voorbeeld om dit te illustreren is de Charlie Hebdo aanval. Op basis van alle gegevens die over deze aanslag te vinden zijn - van politierapporten tot Twitter-berichten - genereert de software van Pandora Intelligence een compleet verhaal in de vorm van een scenario-graph. "Zie het als een multidimensionale puntenwolk. De onderliggende structuur is uniform en is te herleiden naar de twaalf basiscomponenten. Onze software maakt dat niet alleen voor de aanslag op Charlie Hebdo, maar voor alle terroristische aanslagen die we kennen. Op die manier kunnen we data van heel veel verschillende incidenten met elkaar vergelijken. Daarmee kunnen we patronen ontdekken die voor een mens onmogelijk te vinden zijn. Op basis van die patronen, kunnen we zelfs toekomstige incidenten voorspellen."

Pandora Intelligence als ambidextere organisatie

De rol van Peter binnen Pandora Intelligence is Chief Narrator, of 'chef verhalen' zoals hij het zelf noemt. "Een organisatie kan op twee manieren waarde vertegenwoordigen: enerzijds terugkijken in de tijd en gebruiken wat in het verleden al is ontwikkeld, en anderzijds vooruitkijken naar wat in de toekomst ontwikkeld zou moeten worden. Tegenwoordig is er meer behoefte aan een 'ambidextere organisatie', oftewel een organisatie die tegelijkertijd terug én vooruit kijkt.

> **"Organisaties zijn vaak druk met successen uit het verleden voort te zetten. Tegenwoordig is er behoefte aan 'ambidextere organisaties', die tegelijkertijd terug én vooruit kijken. Welke ontwikkelingen komen eraan en zijn we daar klaar voor? Wat wordt disruptive?"**

Organisaties zijn vaak druk met successen uit het verleden voort te zetten, maar het is belangrijk om te blijven kijken naar de mogelijkheden van de toekomst. Welke ontwikkelingen komen er aan en zijn we daar klaar voor? Wat wordt disruptive? Wat zijn de uitdagingen en de daarbij behorende kansen? Pandora Intelligence is een ambidextere organisatie en het is aan mij om op mijn tenen te staan en uit te kijken naar de toekomst.

> **"Innoveren is nauw verbonden met experimenteren. Veel veiligheidsorganisaties zouden het woord innovatie helemaal niet moeten gebruiken. Daarmee verliest het woord haar oorspronkelijke waarde."**

Hoe Peter tegen innovatie aankijkt
De rol van Peter binnen Pandora Intelligence is onlosmakelijk verbonden met innovatie. "Innovatie gaat verder dan het combineren van bestaande technieken: het is een sprong voorwaarts in de tijd. In mijn politietijd werd een innovatieprijs uitgereikt aan het plaatsen van camera's op paarden, zodat een hoger blikveld ontstaat. Hoewel dat zeker een waardevol idee is, is het geen innovatie als je het mij vraagt. Innoveren is nauw verbonden met experimenteren en dat is voor veel organisaties heel erg spannend. Ik zou zelfs durven te beweren dat veel veiligheidsorganisaties het woord innovatie helemaal niet zouden moeten gebruiken. Daarmee verliest het woord haar oorspronkelijke waarde", vertelt Peter.

"Innovatie brengt altijd een zeker risico met zich mee, dat hoort er nou eenmaal bij. Het moet mis kunnen gaan, het moet kunnen ontploffen, het moet uit je handen kunnen vallen. Van iets wat misgaat kun je leren en daaruit kan iets nieuws ontstaan, maar veiligheidsorganisaties willen liever niet dat er iets misgaat. Zij zijn erop gericht om risico's uit te sluiten. Datzelfde geldt overigens voor commerciële partijen of investeerders, ook zij willen zoveel mogelijk risico's vermijden. Innoveren moet dus 'tegen de klippen op' plaatsvinden."

> **"Voor échte innovatie, het experimenteren dus, is een veiligheidsorganisatie per definitie niet ingericht."**

Is innoveren overal mogelijk?
Nee, innoveren en experimenteren kan niet overal volgens Peter: "Een veiligheidsorganisatie is veel meer gebaat bij het zoeken naar reeds bewezen innovaties. 'Technologie-radar' wordt dat ook wel genoemd: wat gebeurt er om ons heen en wat is de meerwaarde voor onze organisatie? Dat is een heel waardevol instrument. Door vervolgens de juiste publieke en private partijen te betrekken, kan worden bekeken of iets wat zich bewezen heeft in een ander domein toepasbaar is in het veiligheidsdomein. Dan heb je het over toegepaste innovatie. Voor échte innovatie, het experimenteren dus, is een veiligheidsorganisatie per definitie niet ingericht", vertelt Peter.

Waarom zijn bepaalde organisaties innovatiever dan andere?
"Je bedoelt: Wat maakt bepaalde organisaties mínder innovatief dan andere organisaties? Want daar zit een verschil in. Innovatie is innovatie. Er is geen overtreffende trap. Je kunt wel mínder innovatief zijn."

Om toe te lichten waarom sommige organisaties minder innovatief zijn, verwijst Peter naar een uitspraak van Wilson, een Amerikaanse bioloog. "Wilson zegt: "Het probleem van de moderne maatschappij is het volgende: we hebben oeroude emoties, middeleeuwse instellingen en godachtige technologie." Hij bedoelt daarmee dat hoewel de technologische vooruitgang van de mensheid enorm is, onze emotionele en sociale ontwikkeling niet in dezelfde mate is meegegroeid."

"Allereerst omdat het gedrag van mensen nog steeds door het 'oerbrein' wordt aangestuurd. Oftewel, we laten ons (instinctief) leiden door emoties die er evolutionair gezien voor bedoeld zijn om te overleven: emoties als angst of frustratie. Hier komen nauwelijks rationele overwegingen aan te pas, omdat het zich afspeelt in het onderbewuste."

"Ten tweede omdat veel van onze sociale en politieke structuren zijn ontstaan in de middeleeuwen. Denk aan ons politieke stelsel, dat van wetgeving en daarmee ook handhaving, maar ook ons systeem van onderwijs en universiteiten is ontstaan in de middeleeuwen. Daarmee bedoelt Wilson overigens niets negatiefs. Integendeel, deze instanties vertegenwoordigen geschiedenis en traditie en dat is heel waardevol voor onze samenleving. Maar 'middeleeuwse instanties' veranderen per definitie heel erg traag."

"De term "godachtige technologie", verwijst tenslotte naar de ongelooflijke vooruitgang die we boeken op het gebied van wetenschap, technologie en innovatie. Neem ChatGPT als voorbeeld, dit biedt ons mogelijkheden die tot voor kort ondenkbaar waren en we eerder zouden hebben toegedicht aan een god."

"De combinatie van deze drie factoren: oeroude emoties, middeleeuwse instanties en godachtige technologie, maakt dat we vaak ongemak voelen bij échte innovaties. Maar alleen als we in staat zijn om de technologische vooruitgang in lijn te brengen met onze emoties en bestaande structuren, behouden we een gezonde samenleving. Wil de securitybranche écht innoveren, dan staat het voor de opgave om deze factoren integraal te bekijken."

> **"Innovatie in het veiligheidsdomein vereist een bepaald type mens, een bepaalde structuur en een bepaalde mindset."**

Drie elementen van innovatie
"Innovatie in het veiligheidsdomein vereist een bepaald type mens, een bepaalde structuur en een bepaalde mindset." Peter geeft op basis van Wilson zijn inzichten over wat nodig is voor innovatie in het securitydomein.

Allereerst: het type mens. Volgens Peter heb je mensen nodig die ervoor openstaan om te experimenteren en hun opgedane kennis vervolgens durven te delen. Het tweede element, de structuur binnen organisaties in het veiligheidsdomein, is volgens hem meestal niet flexibel genoeg om écht te kunnen experimenteren. Experimenteren betekent namelijk ook mislukken en daarvan leren volgens Peter. Ten derde zijn organisaties binnen de securitywereld vaak niet gewend om met - zoals Peter het noemt - 'godachtige' technologie te experimenteren. Daar heb je dus een andere mindset voor nodig.

Dat de juiste mindset voor veel organisaties nog een uitdaging is, belicht Peter aan de hand van een voorbeeld. In een collegezaal aan de universiteit in Rotterdam vroeg hij hoeveel studenten ChatGPT gebruikt hadden voor een verslag en dit daadwerkelijk ingeleverd hadden. Eén student stak haar hand op. Peter vond het geweldig dat ze dat durfde, want wat zie je gebeuren? Universiteiten zijn middeleeuwse organisaties, ze worden geconfronteerd met een moderne technologie als ChatGPT en hun eerste reactie is: bestrijden. Maatregelen treffen om te voorkomen dat studenten ChatGPT gebruiken."

> **"Wetgeving is te traag voor de huidige technologische ontwikkelingen. We moeten op een veel diepere laag nadenken over het wezen van onze samenleving en welke rol technologie daarbinnen inneemt."**

We zien nu dat er wetten ontwikkeld worden rondom AI. Maar het maken van nieuwe wetten duurt jaren. Dan zijn we niet bij ChatGPT 4, maar bij ChatGPT 70 bij wijze van spreken. Wetgeving is te traag voor de huidige technologische ontwikkelingen. We moeten daarom op een diepere laag nadenken over het wezen van onze samenleving en welke rol technologie daarbinnen inneemt. Maar de geschiedenis heeft ons geleerd dat je technologische ontwikkelingen niet tegenhoudt. Dat is mijn advies: "Bestudeer nieuwe technologische ontwikkelingen, laat het in een veilige omgeving ontploffen en experimenteer ermee. Maar vooral: wees integer en transparant met wat je doet en wat je ervan leert."

> **"Terrorisme en symboliek bleken namelijk onlosmakelijk met elkaar verbonden te zijn. Maar ook als het gaat over cyberwarfare blijkt symboliek een heel grote rol te spelen."**

In welke mate innoveert Pandora Intelligence op het gebied van cybersecurity?
"In 2017 hebben we meegedaan aan de Defensie Innovatie Competitie, waarbij cyberwarfare centraal stond. De vraag was: heeft de verhaalstructuur - zoals we die gebruiken om terrorisme te voorspellen - ook waarde in het domein van cyberwarfare? Wat we toen ontdekten is dat op het gebied van cybercrime 'symboliek' een heel belangrijke scenario-component is. We wisten al dat symboliek één van de twaalf elementaire scenario-

componenten is die van grote meerwaarde bleek in het begrijpen en voorkomen van terrorisme. Terrorisme en symboliek bleken namelijk onlosmakelijk met elkaar verbonden te zijn. Maar ook als het gaat over cyberwarfare blijkt symboliek een heel grote rol te spelen."

In de data van het ministerie van Defensie signaleerde Pandora Intelligence een vreemde term in de code van één van de cyberaanslagen: 'Petya'. Het systeem zocht automatisch de context van deze naam op en kwam bij James Bond uit. In Golden Eye komen namelijk twee satellieten voor waarvan één de naam Petya heeft. Die andere satelliet heet Mischa. Toen het systeem die laatste naam vervolgens vergeleek met de bestaande data van cyberaanvallen, werden twee andere aanslagen gevonden waarin 'Mischa' voorkwam in de code. Vervolgens zijn alle eigennamen uit alle James Bond boeken - automatisch - vergeleken met alle data van alle cyberattacks, en werden er enkele tientallen cyberaanslagen gevonden waarin namen van James Bond karakters werden gebruikt. Uit nader onderzoek bleek dat twee (groepen van) cyberterroristen telkens gebruik maakten van James Bond namen. Daarmee werd een relatie blootgelegd die in traditioneel onderzoek naar cyberwarfare niet ontdekt was", legt Peter uit.

In 2017 heeft Pandora Intelligence de Defensie Innovatie Competitie gewonnen. Vervolgens is er een proefversie van het scenariomodel gemaakt op basis waarvan het bedrijf zowel in 2019 als in 2021 gewaardeerd werd met een ontwikkelsubsidie in het kader van het 'Nationaal Technologie Programma'.

> **"Vroeger waren trends makkelijker te voorspellen: de wereld veranderde eigenlijk helemaal niet zo snel. Als je tien jaar terug keek, kon je met hetzelfde verschil wel een voorspelling maken voor de komende tien jaren. Die methode werkt nu niet meer."**

Trends binnen het security domein

"Vroeger waren trends makkelijker te voorspellen: de wereld veranderde eigenlijk helemaal niet zo snel. Als je tien jaar terug keek, kon je met hetzelfde verschil wel een voorspelling maken voor de komende tien jaren. Het was een soort tangent line die je door kon trekken. Die methode werkt nu niet meer. Kijk alleen al naar ons onderwijssysteem. Je kunt geen opleidingen meer ontwikkelen op basis van alleen historische kennis. De 'oudere' generatie kijkt tien of twintig jaar terug, terwijl je juist vooruit moet kijken. Een paar maanden geleden wist niemand wat ChatGPT was, nu is iedereen in rep en roer. Ik bedoel maar!"
"Vroeger waren trends makkelijker te voorspellen: de wereld veranderde eigenlijk helemaal niet zo snel. Als je tien jaar terug keek, kon je met hetzelfde verschil wel een voorspelling maken voor de komende tien jaren. Die methode werkt nu niet meer."

Verbeeldingskracht is daarom belangrijker dan ooit, vindt Peter. "Kijk naar de volgende stappen en hoe de samenleving zich daarop kan voorbereiden. De kracht van verbeelders in onze maatschappij is groter geworden. Voor mij is verbeelding een soort default setting. Ik was de dromer op de achterste rij in de klas op de mavo, kon dus niet naar de

universiteit, maar ging naar de kunstacademie. Tegenwoordig is er steeds meer plek voor mensen die getraind zijn in het verbeelden en nadenken over de toekomst. Ik denk dat filmmakers, schrijvers en kunstenaars in de toekomst een steeds grote rol zullen spelen in het voorbereiden op de onzekerheden van de toekomst."

> **"Google weet veel meer van Nederland dan de overheid weet van ons land. Dat vormt een direct gevaar voor onze democratische rechtsstaat."**

Peter benoemt nog een andere trend - naast de behoefte aan verbeeldingskracht - die volgens hem iets minder positief is, maar wel reëel. In reactie op de onzekerheden van de toekomst, houden veiligheidsorganisaties zich volgens hem steeds vaker vast aan hun eigen manier van handelen. Dit resulteert erin dat kennis en data niet gedeeld worden met elkaar. Bedrijven die dit wél doen, worden daarentegen steeds krachtiger. Hij noemt Google en gelijksoortige bedrijven als voorbeeld: "Google weet veel meer van Nederland dan de overheid weet van ons land. Dat vormt een direct gevaar voor onze democratische rechtsstaat."

Zou het delen van data de norm moeten zijn?
"Veiligheidsorganisaties zouden moeten kijken naar de wettelijke kaders waarbinnen data en kennis kan worden gedeeld. Doen ze dat niet, dan manoeuvreren ze zichzelf naar de marge, en worden ze links en rechts ingehaald door bedrijven die wél data met elkaar in verband weten te brengen. Daarmee wordt onze democratische rechtsstaat ondergraven."
Als afsluiting vragen we Peter hoe hij zich laat inspireren. "Kunst", is zijn antwoord. "Mensen zoals Marina Abramovic inspireren mij. Films inspireren mij ook. Daarnaast luister ik graag naar podcasts én was ik zelf ook betrokken bij de podcast: 'De Nieuwjaarsmoord'. Daarin werken we met een groep burgers samen met de politie en het Openbaar Ministerie om een cold case op te lossen. Ook dat gaat ook over het idee dat je in de publieke ruimte veel data vindt die de politie niet heeft. Daarmee kun je op een andere manier onderzoek doen dan de politie dat destijds deed. Verbeeldingskracht, scenario's én politiewerk komen allemaal samen in deze bijzondere podcast."

“We staan aan de vooravond van een evolutie waarin mens en technologie steeds meer in elkaar verweven raken.”

6. Renza Grüter
- CPO van Zerocopter

Renza Grüter, CPO van Zerocopter, kwam tijdens haar studie Bedrijfskundige Informatica in aanraking met security. Sindsdien is dit onderwerp niet meer weg te denken uit haar leven. Met veel ervaring, kennis en haar non-conformistische houding schopt ze het ver. Renza vindt dat we als sector nu te traag zijn om te anticiperen op een snel veranderende realiteit. Ze pleit voor minder competitiedrang en intensievere samenwerking, om innovatie op sectorniveau te faciliteren.

Wat als je je passie volgt

"Soms lopen dingen zoals ze lopen. In mijn jeugd kocht ik mijn eerste 286 moederbord, ontdekte Bulletin Boards en speelde ik Might & Magic (RPG)". Met alleen een praktijkdiploma informatica op zak (Ms DOS, Norton Commander, Dbase 4) startte Renza op haar negentiende bij de helpdesk van een EDIFACT-organisatie. Stap voor stap maakte ze kennis met business intelligence en data. Niemand is te oud om te leren, dacht Renza. Met die gedachte besloot ze om op 31-jarige leeftijd aan de studie Bedrijfskundige Informatica te beginnen. Haar enthousiasme werd aangewakkerd toen ze in aanraking kwam met de securityvakken. Over het vervolg vertelt Renza: "Dit vond ik zo tof, dat ik vrijwel meteen aan mijn toenmalige werkgever (het OM) vroeg of ik security officer kon worden. Daar kreeg ik een 'ja' op." Uiteindelijk won ze de BI Award van deze studie. IT stond bij het OM in deze tijd nog in de kinderschoenen. Het digitale strafdossier was nog 1-op-1 gekoppeld met het papieren dossier. De fysieke en digitale wereld bestond nog naast elkaar: grote kasten vol met dossiers en kluizen voor de meer vertrouwelijke stukken.

Inmiddels heeft Renza vele rollen vervuld op het snijvlak van Business en Technologie bij het Ministerie van Justitie, ABN AMRO, Fox-IT en als zelfstandige. Allemaal binnen de securitybranche. Aan een goed beeld van de klantbehoefte dus geen gebrek. Inmiddels is ze werkzaam bij Zerocopter als Chief Product Officer (CPO).

Zerocopter: hoe, wat, waar?

Zerocopter is een platform dat organisaties helpt om kwetsbaarheden en beveiligingslekken in hun systemen te vinden en op te lossen met ethische hackers.

Als CPO van Zerocopter heeft Renza verschillende taken en verantwoordelijkheden. "Mijn eindverantwoordelijkheid ligt bij het bereiken van onze visie en missie. De 'roots' van Zerocopter liggen in de hacker-samenleving. In de begindagen stonden hackers bekend als computer 'enthusiasts' die hun inzichten gebruikten om technische problemen op te lossen, beveiligingsproblemen op te sporen en bugs te vinden. En daarom werd Zerocopter geboren. Omdat we wilden doen wat oorspronkelijk de bedoeling was - de digitale wereld een betere wereld maken. Zerocopter brengt deze oorspronkelijke hackers weer samen in een vertrouwd netwerk en zorgt ervoor dat we in staat zijn om snel nieuwe bedreigingen te kunnen mitigeren."

"Dat zie je terug in de ontwikkeling van de diensten tot en met de implementatie van de producten. Ook het begrijpen en definiëren van de markt en de market fit zijn belangrijk.

Onze oplossingen moeten natuurlijk resoneren met het hackersnetwerk én aansluiten bij de behoeften van onze klanten. Ook draag ik de verantwoordelijkheid voor het beheer van productiecyclus. Daar hoort bij: het upgraden en verbeteren van bestaande producten, het evalueren van de prestaties hiervan en het bepalen van de strategieën voor de toekomstige ontwikkeling van het product."

Daarnaast is Zerocopter een Incubatie Unit voor nieuwe ideeën vanuit het hackersnetwerk welke deze niet zelfstandig kunnen productizen. Aanvullend vertelt Renza dat een relatie met het hackersnetwerk én de afstemming met belangrijke stakeholders ook essentieel is.

> **"Hoewel de dagelijkse taken van Zerocopter veel te maken hebben met het identificeren en analyseren van markttrends, het onderzoeken van de concurrentie en het ontwikkelen van nieuwe producten en functies, draait het ook om het grotere geheel: innovatie."**

De essentie van innovatie binnen security
Innovatie kent volgens Renza twee belangrijke aspecten:
1. Een open mind kunnen houden
2. Het anticipatievermogen op de realiteit

Dat vraagt om meer uitleg, dus Renza vertelt wat ze hiermee bedoelt: "Het is belangrijk om continu het échte probleem te bekijken en daarbij een passende oplossing te zoeken. Door de ontelbaar vele ontwikkelingen zien we soms door de bomen het bos niet meer. Daardoor roesten klanten vast in de huidige - maar niet passende - oplossing." Uit marktonderzoek is ook gebleken dat er onder de klanten een 'solution uncertainty' heerst. Doordat er zoveel aanbod is, weten kanten niet zo goed meer wat te kiezen met het gevolg dat keuzes worden uitgesteld en daarmee het beveiligingsniveau absoluut niet wordt verbeterd.

"Om dat te voorkomen, is een open mind belangrijk", gaat Renza verder. "Dat begint al met de definitie van het begrip security. Dat moet helder zijn." Haar uitleg volgt met twee begrippen: het 'oude denken' en het 'nieuwe denken'. "Het oude denken is beperkt. Dit gaat uit van fysieke bescherming, zoals een woning die je op slot doet."

"Dat is heel anders dan de beveiliging van computersystemen. Toch wordt dit vaak vanuit het 'oude denken' benaderd. Massaal proberen we computersystemen af te sluiten tegen indringers en de toegang tot bezittingen te ontzeggen. Het feit is dat dit geen fysieke omgeving is. Het is een digitale omgeving, waarin we niet goed begrijpen wat er eigenlijk in dat 'kastje' (de computer) zit. Bovendien is het moeilijk om hier de waarde van in te zien. De controle op de fysieke wereld sluit totaal niet aan bij de digitale wereld." Er is dus sprake van een discrepantie tussen beide begrippen.

> **“Er wordt op dit moment onvoldoende geïnnoveerd binnen de securitybranche. We zijn te traag. Veel te traag.”**

Alleen dat al is problematisch volgens Renza. Deze discrepantie en verkeerde benadering vergroot het aanvalsoppervlak. “We vinden het complex om deze ‘phygital’ omgeving goed te begrijpen”, concludeert ze. “Als ik terugkijk naar mijn periode bij het OM, was daar de fysieke en digitale omgeving nog gespiegeld en was het makkelijker te begrijpen waar de waarde zich bevond. Nu vinden we het lastig die phygital realiteit goed te begrijpen. Voor de nieuwe generatie is dit wel makkelijker”.

Waarom het goed is om af en toe een stap terug te doen in het proces

In het geval van bovenstaande verduidelijking over de phygital producten, vult Renza aan: “Een open mind is belangrijk om te kunnen duiden wat een asset is, wat de vorm van een asset is, hoe je de waarde van een asset bepaalt. Wees je hier bewust van. Dit bepaalt hoe je het onderwerp security vervolgens aanvliegt.”

Renza vervolgt haar beredenering: “Security begint voor mij met een stap terug doen en de vraag te stellen: waar zit de waarde in? Is het data? Een stukje IP? Zijn het de klanten of je medewerkers? Ga altijd na of je deze assets in beeld hebt. Is dat niet het geval? Ga dan na hoe je dit wél in beeld brengt. Beschik je over tools? Hoe zit het met prioritering? In de praktijk kan dit lastig zijn, omdat assets steeds meer gedistribueerd zijn of kunnen switchen. Wat vandaag waarde kan hebben, kan morgen helemaal geen waarde meer hebben. Dat blijft een uitdaging.”

Bewustwording creëren met het hackersnetwerk van Zerocopter

Het duiden van assets heeft dus prioriteit. Bekijk daarna het beschikbare budget en ga op zoek naar een passende oplossing. Lukt dat niet? Ook Zerocopter kan daarbij helpen: bewustwording creëren bij klanten en de juiste, passende oplossing zoeken.

Renza verduidelijkt haar verhaal met een voorbeeld: “Zerocopter werkt preventief. We laten klanten zien dat hun ‘deur’ openstaat. We attenderen vroegtijdig dat er iets waardevols voor het grijpen ligt. Waarschuwen en inzicht geven in de oplossing: dát is wat we als hackers netwerk doen. Bijvoorbeeld voor onze Coordinated Vulnerability Disclosure oplossing is het punt niet dat we inbreken, maar enkel signaleren dat de public facing deur al wagenwijd openstaat, ook voor criminelen, as we speak.”

Aansluitend geeft Renza nog een voorbeeld: “Assets zijn simpelweg niet altijd zichtbaar. Neem Roblox als voorbeeld. Alles in Roblox is virtueel: de handelingen, de personages, waarden. Het is nu een populair gaming platform onder jongeren, maar het gaat in de toekomst vaker als basis dienen voor andere nieuwe omgevingen. We moeten in staat zijn om deze assets te beschermen. Ook al is het niet direct tastbaar.” Om te beseffen hoe groot dit is, is het goed om te weten dat het aantal gebruikers van Roblox het aantal gebruikers van Netflix spoedig gaat inhalen.

Innovatie hangt samen met het aanpassingsvermogen van de mens
Dat innovatie niet enkel om technologie draait, is zeker volgens de CPO van Zerocopter. "Het gaat om 'mens zijn'. We moeten in staat zijn om te anticiperen op de veranderde realiteit. Techniek is slechts een hulpmiddel. Toch wordt er op dit moment onvoldoende geïnnoveerd binnen de branche. We zijn te traag. Veel te traag."

Als we vragen hoe dat komt, antwoordt Renza: "Eerlijk? Ik denk dat de traagheid veroorzaakt wordt door ego's, financiële drijfveren en de drang naar macht." Met een eerlijke en kritische noot - zonder waardeoordeel - zegt ze vervolgens: "Er zijn best wat spelers in het securitydomein onbekwaam. Dit leidt ongewild tot een groter aanvalsoppervlak voor criminelen. Gelukkig blijft er ook ruimte voor ons om hierop te anticiperen."

De kracht van samenwerking
De vraag rijst dan natuurlijk: hoe kan innovatie op sectorniveau beter georganiseerd worden? Het antwoord is resoluut: *samenwerking.*

> **"We zouden elkaar onderling binnen securitybedrijven niet als concurrenten moeten zien, maar als co-creators. Mijn hoop is dat we het commerciële perspectief - het kleine of oude denken - aan de kant schuiven en meer kijken naar het grotere geheel."**

"Oftewel: minder naar de korte termijn en juist veel meer naar een sectorstrategie om zo innovatie te faciliteren. We zouden de balans meer moeten vinden tussen profitability en value for market." Prioriteiten bepalen hoort daar ook bij. "Kill your darlings", zoals ze dit zo mooi zegt.

Renza onderbouwt dit verder: "Een gezamenlijke defense-stack, nationaal en globaal, kan inzichtelijk maken waar linies wel, niet of minder goed gedekt zijn. Als dit samenvalt met een eerlijk beeld van effectiviteit vs. schaalbaarheid komen we een heel eind. De incubatie en innovatie van een product of dienst kan sneller én beter als ego's en eigenbelang aan de kant worden geschoven. We moeten terug naar de engineering mindset: de hackers mindset. Alle relevante securityproducten zijn immers ooit door een hacker bedacht en gemaakt."

"Het domein moet weer gezond worden", zo stelt ze. Optimale samenwerking is hiervoor nodig. En dat is precies de reden waarom Renza voor Zerocopter koos. Hier komt alles samen om de integriteit van data en technologie te behouden. "Het is mijn persoonlijke missie om daar een bijdrage aan te leveren."

> **"Vaak wordt er meer geld uitgegeven aan compliance dan aan oplossingen voor het echte probleem. Zonde, zo stroomt er minder geld naar echte innovaties. Deze twee werelden verbinden blijft een uitdaging."**

Uitdagingen wat betreft innovatie gaat Renza graag aan. Zoals bij organisaties die hun securityprobleem elders willen beleggen of compliant willen zijn, maar eigenlijk weinig begrijpen van de kern. "Producten uit ons hackersnetwerk hebben ontzettend veel waarde, maar om er alles uit te halen is daadwerkelijk kennis hiervan wel noodzakelijk. Vaak wordt er meer geld uitgegeven aan compliance in vergelijking met oplossingen van het echte probleem. Zonde", zegt Renza. "Zo stroomt er ook minder geld naar de echte innovaties. Deze twee werelden verbinden blijft een uitdaging."

Hoe non-conformisme een grote rol speelt

Binnen het hackersnetwerk van Zerocopter speelt non-conformisme een belangrijke rol. Ook voor haar als CPO. "Met mijn eigen non-conformistische houding én door de moedige club mensen om me heen kan ik een significante bijdrage leveren aan innovatie en creatie. "Samen werken we aan hetzelfde doel."

Voor Renza zijn dat stuk voor stuk voorwaarden voor innovatie. Dit hangt samen met de korte incubatietijd als het gaat om innovatie van technologie. "Ons hackersnetwerk innoveert snel en de hackers kunnen hierdoor doen wat ze leuk vinden. Dat is innovatie pur sang als je het mij vraagt. Daarnaast is het aan ons om uit te vinden hoe de packaging eruit komt te zien en wat de verschillende businessmodellen zijn om de waarde vanuit het hackersnetwerk te vertalen naar de gebruikers."

Over de innovatiekracht binnen Zerocopter zelf is Renza dus wel tevreden. "Qua innovatie is mijn rol het vertalen van de marktvraag naar het hackersnetwerk en het challengen van de praktische uitvoerbaarheid van hun innovatieve oplossingen. Ook het ophalen van de vraag en bepalen of de oplossingen schaalbaar kunnen worden geleverd hoort daarbij. Dit levende incubatiemechanisme werkt goed."

De grootste trends in security de komende 5 tot 10 jaar

De te verwachten trends in de komende jaren worden door Renza als volgt gekaderd:

- Het ontstijgen van het compliance denken. "Ik verwacht dat we hierdoor dichter bij de kern van securityproblemen komen, waardoor we dit beter aan kunnen pakken."
- Een flinke sprong binnen de technologie. "Een betere interactie tussen mens en technologie. Mede gebaseerd op het rapport van MIT 'How to become a Centaur'[5] waarin wordt aangetoond dat mensen en machines niet in dezelfde intelligentiedimensie functioneren.
- Dit wil zeggen dat mensen en machines op verschillende manieren intelligent zijn, waardoor ze elkaar per definitie aanvullen in plaats van vervangen."
- Minder competitief denken."Samenwerken wordt hopelijk meer en meer een must om de integriteit van technologie en data beter te kunnen waarborgen. Mindset en bewustwording

veranderen hierdoor denk ik ook."
- Betaalbaarheid van security voor het mkb en het publieke domein.

Op de vraag hoe Renza bij blijft met al deze ontwikkelingen en andere trends antwoordt ze: "Door écht goed te luisteren naar de 'pijn' van klanten. Ook blijf ik betrokken bij wat er binnen de community speelt. Niet alleen om te blijven leren, maar ook om meer expertise op te doen en mijn bewustzijn te verruimen. Ik hoop dat anderen dat ook doen. Met een 'ik weet het allemaal wel' houding kom je er niet. Met een nieuwsgierige houding blijf je groeien, ook ik."

“Innovatie binnen security is hard nodig. Aanvallers innoveren per definitie sneller dan verdedigers. Daarom is er behoefte aan mensen die deze aanvalspatronen écht begrijpen.”

7. Stef Liethoff
- CEO bij SBL Cyber Security

Stef Liethoff, CEO bij SBL Cyber Security, is al ruim 33 jaar actief in het securitydomein. Hij heeft veel kennis van (technische) beveiligingsoplossingen en business development binnen securitybedrijven. Met SBL richt hij zich op het vergroten van de cyberweerbaarheid van zijn klanten, door middel van extended detection and response. Een oplossing die steeds vaker voorkomt in de markt. Stef deelt zijn inzichten over de laatste trends, ontwikkelingen en verbeterpunten in de sector.

Vertaalslag van techniek naar business

Stef is geen onbekende in het securitydomein. Eind jaren negentig kwam hij al in deze sector terecht: “In 1998 raakte ik betrokken bij een aantal pentest-trajecten voor de overheid en meerdere banken. Dit was toen vooral een technisch kunstje, en ik moest aan de IT-directie uitleggen wat we precies gedaan hadden.” Juist dat aspect bleek hij fantastisch te vinden. “Uitleg geven over iets technisch in begrijpelijke taal, dát vond ik mooi”, vertelt hij. “Een vertaalslag maken van techniek naar de business paste me dus wel. Vanuit daar ben ik vervolgens de cybersecurity ingegaan.” Een wereld die Stefs kennis goed kan gebruiken, want vaak is die vertaalslag de uitdaging. Vakjargon, technische begrippen en allerlei afkortingen maken het er voor leken niet makkelijker op deze materie te begrijpen.

Stef begon zijn cybercarrière bij verschillende grote organisaties, waaronder de gemeente Tilburg, gemeente Eindhoven en het Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer. Met deze ervaring en kennis op zak besloot hij in 2005 de ondernemerswereld te ontdekken. Hij richtte samen met een aantal oud-collega’s Novàccent op, een bedrijf dat organisaties ondersteunde bij ICT-gerelateerde uitdagingen. Dertien jaar later werd Novàccent gekocht door Tesorion. In eerste instantie vervolgt Stef hier zijn carrière, maar uiteindelijk besluit hij toch zijn eigen weg te gaan. “Na een jaar werken bij Tesorion kwam ik erachter dat cybersecurity nog steeds een grote passie van mij was (en is). Vanuit die passie en gedrevenheid wilde ik graag klanten helpen om hun cyberweerbaarheid te vergroten. Maar dan vanuit een eigen identiteit en met eigen oplossingen, waarvan ik zelf écht geloof dat deze het verschil maken”, vertelt hij.

Cyberweerbaarheid van klanten vergroten

Vanuit die visie richtte Stef in 2019 SBL Cyber Security op. Met dit bedrijf helpt hij zijn klanten met het inzichtelijk maken van hun cybersecurity en om weerbaarder te worden tegen dreigingen. Als CEO is Stef betrokken bij het runnen van de primaire bedrijfsvoering en bij business development. Ook zorgt hij ervoor dat de oplossingen van het bedrijf naadloos aansluiten bij wat klanten willen en nodig hebben.

Eén van die oplossingen werd zelfs een nieuwe onderneming: SBL Cybermonitoring. Een monitoringsdienst om snel aanvallen te kunnen ontdekken, en daarmee schade te minimaliseren. “Ik ben hiermee gestart in 2021, samen met mijn businesspartner Jan Jaarsma”, zegt Stef. “Het bevindt zich nu nog in de start-up fase en is een belangrijke toevoeging aan onze dienstverlening.”

Het WatchEagle Detection & Response platform

SBL Cybermonitoring heeft het WatchEagle Detection & Response platform ontwikkeld voor het detecteren van cyberaanvallen. Dit platform maakt gebruik van verschillende bronnen voor dreigingsinformatie. “Denk aan het Nationaal Cyber Security Centrum, Suricata en diverse open bronnen zoals de Open Threat Exchange van AlienVault. Die informatie gebruiken we onder andere om dreigingen op tijd te kunnen identificeren”, legt Stef uit.

“Daarnaast is het platform gebaseerd op een zogeheten agentframework”, vertelt hij verder. “Hierbij zijn verschillende functionaliteiten in diverse taken opgesplitst en werken agents samen om complexe problemen op te lossen.” SBL heeft het Mitre Attack Framework als basis genomen voor het detecteren van cyberincidenten en deze aanvalspatronen gemodelleerd op het agentframework van WatchEagle. “Het platform kan op ieder type systeem draaien en wordt momenteel gebruikt voor het monitoren van netwerkverkeer, maar kan ook ransomware aanvallen detecteren op servers of werkplekken.”

Extended detection and response

WatchEagle is een voorbeeld van een softwareoplossing die steeds vaker voorkomt in de markt: extended detection and response (XDR). Volgens Stef zijn bedrijven hiermee sneller in staat om aanvalspatronen van buitenaf te voorkomen én hier direct op te reageren. “XDR richt zich op het grotere geheel, zoals gebruikersaccounts, servers, cloud applicaties en losse applicaties binnen de organisatie. Het verschilt daarin dus van traditionele beveiligingssystemen die zich alleen richten op specifieke beveiligingslagen of endpoints. Je kunt het zien als een oplossing die is ontworpen om geavanceerde bedreigingen over meerdere verdedigingslagen en -bronnen te detecteren, te analyseren en hier vervolgens op te reageren.”

> **“Cybersecurity is meer dan een IT-onderwerp: het raakt de hele organisatie. Met een traditioneel beveiligingssysteem red je het in deze tijd niet meer.”**

Stef vindt dat XDR helpt om een holistischer beeld te krijgen van je cyberweerbaarheid. “Juist omdat al deze verschillende lagen en bronnen worden gecombineerd in de analyse van je beveiligingssituatie”, licht hij toe. “Hierbij wordt fundamenteel nagedacht over alle risico’s voor een verbeterde cybersecurity. Cybersecurity is inmiddels veel meer dan enkel en alleen een IT-onderwerp. De gehele organisatie moet betrokken worden. Met een traditioneel beveiligingssysteem red je het in deze tijd niet meer.”

Aanvallers innoveren sneller dan verdedigers

Waarom is innovatie in security zo belangrijk en vindt dit voldoende plaats in de sector? Op die vraag heeft Stef een duidelijk antwoord: “Innovatie is een essentieel onderdeel in het securitydomein. Helaas gebeurt dat nu onvoldoende. Er is op dit moment een duidelijk kennistekort”, stelt hij. Stef verduidelijkt zijn verhaal met een voorbeeld van een auto. “De aanvaller weet alles van een auto: van de portieren, de motor, de brandstof, de banden en elektronica. De verdediger weet daarentegen alleen wat over het blik, het omhulsel. Dat is

precies de keerzijde van compliant zijn. Vaak gaat het om 'bescherming' die alleen zichtbaar is."

Volgens Stef innoveren aanvallers en daarmee ook de aanvalspatronen sneller, waardoor de verdediging achterloopt. "We hebben behoefte aan meer mensen die innovatieve aanvalspatronen écht begrijpen. Er is op dit moment helaas onvoldoende kennis op dit vlak."

Stef ziet dat ook gebeuren bij bedrijven die wél netjes compliant zijn. "Kijk maar naar gemeenten die gewoon aan de 'Baseline Informatiebeveiliging Overheid Cybersecurity' voldoen, maar niet in staat zijn om de aanvaller op tijd te detecteren en tegen te houden", verduidelijkt hij.

> **"Afrekenen met eilandjes is dé manier om innovatie in security te verbeteren. We moeten het samen doen, als securitysector. Dat begint met kennis delen, óók over je fouten. Iedereen kan slachtoffer worden van cybercrime. In plaats van jezelf te schamen, kunnen we juist van elkaar leren."**

Afrekenen met eilandjes

Uit het verhaal van Stef komt duidelijk naar voren dat het securitydomein op het gebied van innovatie verbeterd kan worden. Maar hoe dan? Dát is de vraag. Daar heeft Stef - uiteraard - goed over nagedacht: afrekenen met eilandjes. "Wat we nu zien is dat we vooral individuele threat intelligence bronnen ophalen en dit allemaal verwerken op onze eigen manier. We moeten dit echt samen doen, op sector- of brancheniveau. Dat gebeurt nu amper in de praktijk, waardoor er te weinig threat hunters zijn om aanvallen te zien aankomen. We moeten toe naar snellere en effectievere detectie."Openheid en transparantie spelen volgens Stef op dit moment dan ook een te kleine rol. Dat blijkt uit praktijkvoorbeelden bij gemeenten, vertelt hij. Zodra een gemeente wordt aangevallen, heeft enkel deze gemeente zicht op de Indicator of Compromise (IoC). Maar juist deze IoC bevat waardevolle informatie die kan helpen bij het identificeren van verdacht en onbetrouwbaar gedrag binnen een netwerk of systeem. Stef vraagt zich af waarom dit niet gedeeld wordt met andere gemeenten. "Iedereen opereert op een eilandje, terwijl we deze kennis makkelijk onderling kunnen - en zouden moeten - delen."

Kwetsbaarheid tonen helpt

We vragen Stef of hij denkt dat slachtoffers van cybercrime weinig delen door schaamte. "Zou kunnen", antwoordt hij. "Op slachtofferniveau wordt inderdaad weinig gedeeld, maar daar moeten we eens overheen stappen. Of je nu als organisatie compliant bent of niet: iedereen kan tegenwoordig slachtoffer worden. Het is daarom juist zo waardevol om de modus operandi in een beschermde omgeving te delen met elkaar. In plaats van jezelf te schamen, kunnen we juist van elkaar leren."

Hij noemt een voorbeeld van een aantal organisaties in de tuinbouw. “Zij stelden zich kwetsbaar op door openlijk te vertellen wat hen overkwam. Dat was ontzettend krachtig. De schaamte voorbij. Laat dit een voorbeeld zijn voor andere organisaties om óók die stap te zetten als zoiets gebeurt. Ook al is het soms pijnlijk.” Stef vertelt dat er gelukkig wel al gremia zijn waar dit kan, zoals bij de DTC’s, ISAC’s of IBD voor gemeenten. Maar het moet en kan absoluut beter, concludeert hij. “Desnoods door aanvallen geanonimiseerd te delen, zodat iedereen - áls schaamte een rol speelt - toch kan leren van zulke gebeurtenissen.”

> **“Bij veel innovatieve bedrijven in het MKB, vormt hun kracht ook hun grootste kwetsbaarheid: ze verdienen geld met een innovatieve manier van werken, maar zijn vaak onvoldoende in staat om security betaalbaar te borgen.”**

Waarde toevoegen binnen het mkb

Innovatie is voor SBL een belangrijk onderdeel van hun groeistrategie. Met hun innovaties focussen ze op drie onderdelen: het mkb, hulp met threat hunting als een monitoring service en het agent framework. Stef legt het één voor één uit.

“Onze primaire focus ligt op het mkb, omdat we zien dat deze groep vaak wordt overgeslagen als het gaat om cybersecurity. Grote bedrijven en overheden kennen de weg wel en weten een passende dienstverlener te vinden met security oplossingen. Die vanzelfsprekendheid geldt voor het mkb niet.” Stef ziet dit met name gebeuren bij innovatieve bedrijven die veel te verliezen hebben. Hun kracht is ook hun grootste kwetsbaarheid: ze verdienen geld met een innovatieve manier van werken, maar zijn onvoldoende in staat om de security betaalbaar te waarborgen. “IT is wel vaak uitbesteed”, gaat hij verder. “Partijen aan wie dit is uitbesteed, zijn goed in het beschikbaar stellen van de omgeving, zoals hardware en clouds, maar daar blijft het vaak bij. Informatie die inzicht geeft in de risico’s is niet beschikbaar en kijken naar logging gebeurt vaak niet. De expertise mist bij zulke partijen om hier holistisch naar te kijken. SBL biedt voor dit soort bedrijven een passende en betaalbare oplossing.”

Threat hunting

Het tweede focuspunt van SBL, threat hunting als monitoring service, licht Stef als volgt toe: “Threat hunting is een proactieve beveiligingsaanpak gericht op het identificeren van potentiële bedreigingen. Zulke bedreigingen zijn eerder gemist door geautomatiseerde detectie- en analysetools. Deze data en alerts worden door ons geanalyseerd. De bedreiging sturen wij vervolgens naar de desbetreffende IT-partij, zodat zij hier zelf op kunnen acteren, zoals een poort dichtzetten of een PC uit het netwerk halen.”

SBL pakt hierin ook een adviserende rol richting de IT-partij, zodat het niet alleen bij probleemoplossing blijft. “Met deze passende securityoplossingen kan deze partij vervolgens zelf ook weer aan de slag”, zegt Stef.

Het agent framework verbeteren en versimpelen

Ten derde richt SBL zich met hun innovaties op het agent framework waarop hun WatchEagle platform is gebaseerd. Dit framework zorgt voor een verdeling van taken over meerdere computers of netwerken bij het detecteren, analyseren en reageren op binnenkomende beveiligingsincidenten. Het is ontworpen om grote hoeveelheden gegevens te verwerken en de belasting van ieder afzonderlijk systeem te verminderen. Een complex proces volgens Stef, maar: “Juist omdat het zo complex is, wilden we dit met SBL verbeteren en versimpelen. Op deze manier kunnen we snel inspelen op vragen van klanten, ondanks het feit dat we een klantenbestand hebben met diverse soorten data, zoals camerabeelden en datasets die afkomstig zijn van websites. Met het agent framework hebben we daar verandering in gebracht qua complexiteit. Simpel gezegd kunnen we nu snel het goede van het slechte onderscheiden. Daarnaast kunnen we de klant inzicht geven, zodat zij vervolgens precies zien wat er op de netwerken van hun klanten gebeurt”, aldus Stef.

Mensenwerk blijft belangrijk

AI speelt een grote rol voor bedrijven binnen de security als het gaat om automatisering en groei. Ook bij SBL. Toch blijft mensenwerk én mensenkennis van uiterst belang, vindt Stef. Hij ziet bij SBL de absolute meerwaarde van mbo- en hbo-stagiaires op de werkvloer. Niet alleen om de capaciteit nog beter op orde te brengen, ook zodat ze ‘met de voeten in de klei staan’. “We zijn ontzettend tevreden over deze nieuwe agents in spe. Het mooie is dat letterlijk iedereen die bij ons komt werken, betrokken wordt bij de productontwikkeling. Nieuwe inzichten ontwikkelen zich op deze manier binnen een mum van tijd. Dat is een groot verschil met andere bedrijven. Daar zijn werknemers vaak een radertje in het grote geheel.”

Klanten weten SBL te vinden en andersom weet SBL waar klanten naar op zoek zijn. De oplossingen sluiten aan bij de doelgroep. Het schort nog aan één ding: capaciteit. “We weten dat we sneller kunnen werken, maar daar hebben we wel meer en goed personeel voor nodig.”

Cybersecurity is en blijft in ontwikkeling

Over de huidige innovatiekracht bij SBL is Stef tevreden. Het vormt een goede en solide basis om verder te ontwikkelen. Over ontwikkeling gesproken: dat staat honderd procent centraal bij SBL en Stef zelf. Dat stilstand achteruitgang is, kunnen we wel afleiden uit zijn antwoord. “Ik ben inmiddels zestig, maar ik blijf mezelf uitdagen en bijscholen. Regelmatig ben ik te vinden bij HSD (Security Delta), zodat ik op de hoogte blijf van de laatste trends. Daarnaast blijf ik opleidingen doen en daag ik mezelf continu uit om geïnspireerd te raken door anderen.”

Uitdagingen zijn altijd welkom, ook als het gaat om nieuwe type klanten. Zo raakte SBL onlangs betrokken in de procesindustrie bij de beveiliging van gasplatforms op zee. De wens? Cybersecurity-by-design meenemen. Dit houdt in dat er vanaf de ontwerpfase tot en met de realisatie van het product wordt nagedacht over de complete informatiebeveiliging. De uitdaging zat dit keer in het primaire werk zo soepel en normaal mogelijk te laten verlopen. “Het is aan ons om met de securityoplossingen het werk niet te blokkeren, maar

juist te laten zien hoe deze oplossingen helpen in de dagelijkse werkzaamheden", sluit Stef het gesprek af. Aan uitdagingen dus geen gebrek. De cyberwereld staat niet stil, maar Stef ook niet. Hij is altijd klaar voor de volgende uitdaging die op zijn pad komt en gaat met alle vertrouwen richting de toekomst.

"Meer innovatie als doelstelling is noodzakelijk. We zouden ook nooit naar de maan zijn gevlogen als de overheid dit niet als doel had gesteld."

8. Erik de Jong
- Strategy Director van Securify

Erik de Jong, Strategy Director van Securify, sleutelde als 10-jarige al aan zijn eerste computer. Zonder vooropleiding - en vooral 'door het gewoon te doen' - is hij de securitybranche ingerold. Hij vindt dat er te veel nadruk ligt op technische ontwikkelingen in de sector. Volgens hem moeten we breder kijken. Het moet aansluiten op de klantbehoeften of wat we als maatschappij nodig hebben. "Het gaat niet om bangmakerij, het gaat om de realiteit op een toegankelijke manier overbrengen", stelt Erik.

Hoe ver je het zonder opleiding kunt schoppen

Erik zit al jaren in het securitydomein. Zonder enige vooropleiding, hij is er ingerold door 'het gewoon te doen'. Zijn interesse werd gewekt in de jaren tachtig toen hij op 10-jarige leeftijd een computer, een Commodore 64, kreeg van zijn vader.

"Beeld je een tijd in zonder Google, zonder bronnen van kennis. Je bent volledig aangewezen op je eigen kunnen en je kwam er vanzelf achter wat wel en niet werkte. Dat sleutelen aan computers triggerde me dus wel", vertelt Erik. Het was daarom voor hem een logische keuze dat hij in die sector ging werken, bij Centric welteverstaan. Dat was in de jaren negentig, de tijd dat het internet een plaats innam in de wereld. Erik vervolgt zijn verhaal: "Ik werd geoutsourced als junior support- en helpdeskmedewerker bij McAfee waar ik klanten hielp met technische vragen."

Vanuit die functie groeide hij door naar tweedelijns support en teammanager. "Dan bevind je je al snel binnen de security hoek, gezien het doel van het bedrijf: het beveiligen tegen virussen. Dit was eind jaren negentig, precies de tijd dat het 'I love you'- virus rond ging. Ik zag met eigen ogen hoe het écht fout kon gaan en dat virussen én mensen misbruik van je kunnen maken via computersystemen."

Na McAfee volgde een overstap naar CERT-RO (Computer Emergency Response Team-Rijksoverheid). Een organisatie opgericht in 2002 met als taak als centraal meldpunt te fungeren voor veiligheidsincidenten en de overheid te voorzien van ondersteuning. Later werd dit GOVCERT en nu draagt het de naam NCSC, het Nationaal Cyber Security Centrum. Na tien jaar Govcert/NCSC maakte Erik de overstap naar Fox-IT waar hij tien jaar werkte in verschillende rollen. Nu werkt Erik inmiddels al enige tijd voor Securify.

Securify is een organisatie die zich richt op het testen van code, applicaties, infrastructuren en organisaties. Het Securify team bestaat uit social engineers, white hat-inbrekers, detectiespecialisten, malware-experts, Windows- en Active Directory-goeroes, ethische hackers voor web & mobile en beveiligingsonderzoekers. Securify heeft een unieke en op risico's gebaseerde aanpak ontwikkeld op basis van continue reality checks die geen concessies doen aan snelheid of voortgang. Op dit moment zijn er veertig medewerkers werkzaam, groeien ze hard en zijn ze altijd op zoek naar nieuwe specialisten.

Hoe Erik zijn rol als CSO vervult

Erik is aangenomen voor twee dingen. "Ten eerste voor de communicatie naar buiten toe:

het uitdragen van de visie van Securify, klantcontact om de klantbehoefte te achterhalen en te onderzoeken hoe we onze dienstverlening kunnen verbeteren", vertelt Erik. Dat is precies hetgeen hem zoveel energie geeft: een narratief uitdragen en klanten en andere stakeholders meekrijgen. Ten tweede is Erik verantwoordelijk voor het ontwikkelen van nieuwe concepten. Op dit moment staat de cloud hoog op zijn agenda.

"Een opleiding in de securitybranche heb ik dus nooit gedaan. Ik begon gewoon achter het toetsenbord met een handleiding. Zo kwam ik een heel eind. Het heeft me ontzettend veel gebracht, want door die tijd weet ik hoe computers werken. Hoewel ik geen 'ICT-nerd' ben, veelal klantcontact heb en de visie presenteer, helpt die kennis me onwijs vooruit", aldus Erik.

> **"Ik krijg jeuk van de uitspraak dat de ontwikkelingen (te) snel gaan in ons vakgebied. Dat klinkt voor mij als een excuus. De manier waarop aanvallers, criminelen of spionnen te werk gaan, is grosso modo ongeveer wel hetzelfde als 20 jaar geleden."**

Over ontwikkelingen in de branche is Erik duidelijk: we moeten ons niet te snel gewonnen geven. "De nadruk ligt vaak op technische ontwikkelingen, waardoor het lijkt alsof aanvallers anders te werk gaan, maar we moeten breder kijken. De problematiek rondom ransomware gaat ook over verzekeraars, over sancties en over de vraag of je politie of de geheime dienst inzet vanwege nationaal belang." Volgens Erik kunnen we nog veel op dit gebied leren.

Communiceren over security geeft hem allesbehalve jeuk. Erik doet niets liever. "Op het podium staan en een goed verhaal vertellen. Daar krijg ik écht energie van. Als ik ergens presenteer, heb ik drie doelen. Ik vind het ten eerste ontzettend belangrijk dat we met zijn allen lachen. Daarnaast is het fijn als de naam van Securify wordt onthouden en ten derde hoop ik altijd dat het publiek concrete tips kan gebruiken en toepassen in hun bedrijf. Ik heb niet de illusie dat het publiek álles onthoudt, maar deze drie bescheiden doelstellingen heb ik wel", aldus de Strategy Director van het bedrijf waarvan hij hoopt dat de naam wordt onthouden.

Erik plaatst zijn doelstellingen in de context: "Het is gaaf om iets te triggeren bij het publiek. Of dat nu gebeurt in een kleine sessie met een Raad van Commissarissen of bij een groep van tweeduizend mensen. Mijn doel is bereikt zodra toeschouwers die minder kennis van security hebben, weglopen en denken: hier moet ik wat mee. Het gaat niet om bangmakerij, het gaat om de realiteit - de situatie waar we ons in verkeren - op een toegankelijke manier overbrengen."

De boodschap moet natuurlijk begrijpelijk zijn voor iedereen. "Jargon stem ik af op het publiek, net als het abstractieniveau. Het is belangrijk dat de manager van een organisatie de boodschap begrijpt. Hun vragen zijn vooral: waarom vallen mensen je aan en wat

betekent dat voor de organisatie? Soms ga ik de diepte in om ze te triggeren, inzichtelijk te maken hoe complex een aanval kan zijn en wat er allemaal moet gebeuren. Dan schets ik het landschap van de klant door te benoemen dat het om 400 services, 20 clouddiensten en 225 laptops en telefoons gaat. Ik vertel dat op die laptops weer 15 programma's staan die bestaan uit 40 modules met tientallen libraries en dat één daarvan kwetsbaar is. Een concreet voorbeeld zorgt direct voor meer begrip. Als ik te snel over techniek begin te praten, haken mensen af en dat hoeft dus ook niet om security begrijpelijk te maken", zegt Erik.

Innovatie zit ook (of juist) in de kleine dingen

Op de vraag wat innovatie voor Erik is, antwoordt hij: "Vernieuwing. Hoe groot of klein ook. Met innovatie kom je dichter bij de behoeften van de klant of de - in het geval van Securify - pentester."

Securify doet vooral pentesten, red teams en code reviews. Hiermee zit je aan de voorkant. Dit staat tegenover incident response, een kant waar Erik vandaan komt. Code reviews is eigenlijk niets meer dan de overhandiging van een stuk code van de klant die Securify vervolgens reviewed. Dit model is nu omgezet naar een continu model: agile code review genoemd. "Ik vind dat supergaaf", geeft Erik aan. De individuele changes worden naar Securify gestuurd, waardoor binnen het proces en de cadans van de klant deze reviews uitgevoerd worden. Dit gebeurt met behulp van algoritmen die helpen te bepalen waar focus nodig is. Op basis daarvan wordt het risico, de workload en de gevoeligheid van de code bepaald."

"Hiermee stel je de klant in staat om de softwareontwikkeling door te laten lopen en daarnaast direct kleine veranderingen te laten reviewen. Dat vind ik een heel mooie en tegelijkertijd eenvoudige innovatie. Wat je doet voor de klant is hetzelfde gebleven, maar de manier waarop past veel meer in het primaire proces van de klant. Innovatie dus. Een ander voorbeeld van innovatie is het automatiseren van de processen binnen de interne organisatie waardoor het werk richting klanten efficiënter, sneller en makkelijker kan."

Security vs. weerbaarheid

We vragen Erik ook naar zijn definitie van security. Volgens hem gaat het traditioneel gezien over kwaliteitsaspecten van informatie: beschikbaarheid, integriteit en vertrouwelijkheid. Samengevat gaat het om de beheersing van het proces om ervoor te zorgen dat deze drie elementen voldoende gewaarborgd zijn. Erik vervolgt: "Ik zeg met nadruk voldoende, omdat dat natuurlijk nooit honderd procent is. Eigenlijk vind ik weerbaarheid een beter woord dan security."

> **"De definitie van weerbaarheid geeft aan dat het mis kán gaan, zodat je hierop kunt anticiperen. Deze term gebruik ik daarom liever dan de term 'security'."**

Erik vervolgt zijn verhaal: “Bij puur beveiliging ligt het risico op de loer dat er meer aandacht wordt gegeven aan preventie. Het voorkomen van gevaar dus. En dat beeld is niet compleet. Ter illustratie: als je naar verkeersveiligheid kijkt, gaat dit niet alleen over het voorkómen van ongelukken. Het gaat ook om de ambulance die er binnen vijftien minuten is en dat Rijkswaterstaat in staat is kruizen boven de weg te zetten als reactie op een ongeluk.” Dat is volgens Erik de kern van weerbaarheid. “We kunnen nooit alle criminaliteit en spionage voorkomen. Daar ben ik me van bewust. Daarom is het mijn streven om zoveel mogelijk te voorkomen. Daar moeten we ons met zijn allen bewust van zijn. Continu.”

Innoveren we als sector eigenlijk wel voldoende? “Persoonlijk denk ik dat de sector in Nederland onvoldoende innoveert. Iedereen pusht zijn eigen product. Ik twijfel soms of dit voldoende aansluit bij de klantbehoeften of wat we als maatschappij nodig hebben.”

> **“Innovatie is ook afhankelijk van de maatstaf die we met z’n allen willen accepteren als risico.”**

“Als je het hebt over weerbaarheid is het voor een bedrijf en voor de maatschappij belangrijk om gevoel te hebben wat de acceptabele niveaus zijn. Daarvoor zou het enorm helpen om weerbaarheid op een objectievere manier te kunnen meten. Op ons eigen vlak, pentesten of codes reviews, vinden we dat al moeilijk. Hoewel we met een standaard als Application Security Verification Standard (ASVS) al best een eind komen. We geven heel gemakkelijk aan wat er mis is. En dan durven we dus ook wel te zeggen “de code is prut”. Maar als er weinig mis is, durven we minder snel te zeggen “die code is best goed”, want stel dat er dan toch nog een stuk slechte code naar boven komt, dan hebben we het gevoel dat onze uitspraak zou invalideren. Terwijl dat misschien helemaal niet zo is.”
Die transparantie ontbreekt ook vaak bij SOC-dienstverlening, vindt Erik. False positives blijven vaak onbesproken. “Het bespreekbaar maken is niet de makkelijkste weg, maar het zou wel innovatief zijn. Het geeft de klant immers een betere keuze en meer inzicht”, volgens Erik.

Aan innovatie op het gebied van automatisering is volgens Erik geen gebrek. Daarentegen ziet hij nog veel mogelijkheden voor verbetering van meetbaarheid en transparantie van oplossingen en het daarbij aansluiten bij de échte klantbehoeften. Kortom: als sector zijn er volgens Erik hier en daar nog genoeg uitdagingen te benoemen.

De Strategy Director van Securify heeft wel een idee hoe innovatie eruit kan zien. “Kwaliteit en weerbaarheid objectiever maken. Op een schaal van 1 tot 100 is wat klanten soms echt willen. Een keurmerk als dat van pentesten doet dat nu bijvoorbeeld niet. Gelukkig worden de keurmerken wel doorontwikkeld.”

“Een succesvolle tool als het gaat om klantduiding en security is het MITRE ATT&CK framework. Dit is een kennisbank van cyberaanvaltechnieken die wordt gebruikt door aanvallers om in te breken in systemen en netwerken. Het framework bevat een uitgebreide lijst met aanvalstechnieken en tactieken die in verschillende fasen van een aanval kunnen

worden gebruikt. Hiermee geef je de klant inzicht in tegen welke aanval de klant wel of niet is beschermd. Daarnaast is het een goede vergelijkingstool. De eerste stap om tot een vergelijkbaar model te komen, zal vanuit de overheid of een niet-commerciële instantie worden genomen. Voor deze innovatie hebben we dus de overheid nodig."

Toch denkt Erik ook dat er een rol is weggelegd voor de overheid en de wetenschap voor innovaties op de lange termijn. Hij noemt het MITRE ATT&CK framework weer als voorbeeld."Bedrijven zijn vaak (te kort) cyclisch bezig en hebben andere prioriteiten, maar dat de behoefte aan innovatie er is, is heel duidelijk.

De groeistrategie van Securify
Zoals gezegd test Securify code, applicaties, infra en organisaties. Code is het testen van geschreven code, applicaties en infrastructuren testen is een traditionele pentest en een organisatietest is een bredere test: een red team. "In die gevallen gaan we ook fysiek langs en passen we meerdere aanvalstactieken toe. Onze groeistrategie kenmerkt zich vooral door een scherpe focus op de financiële sector, zorg en logistiek. Uiteraard is het altijd een beetje 'fuzzy on the edges' als het gaat om focus. Aan de ene kant richten we ons op bedrijven die ook zelf producten ontwikkelen. Aan de andere kant focussen we op automatisering vanwege schaalbaarheid. Automatiseren doen we bij Securify nog te weinig, dus hier valt winst te behalen", geeft Erik als antwoord op de vraag hoe de groeistrategie binnen zijn bedrijf eruitziet.

Erik vervolgt zijn uitleg over de strategie: "Bij agile code reviews gebruiken we de eerder besproken tools. Tot slot zijn we bezig met de ontwikkeling van abonnementsvormen, zodat we op een continue basis waarde kunnen leveren aan onze klanten."

Uitdagingen: scherpte en up-to-date blijven
Zoals bij veel bedrijven zorgt een groeistrategie ook voor uitdagingen. Bij Securify gaat dat vooral over scherpte. Erik heeft, toen hij bij Fox-IT werkte, slides gemaakt over incident response. Hetzelfde deed hij een aantal jaar later in 2022. "Ik zag dat er op veel vlakken onwijs veel was veranderd. Dat heb je vaak niet in de gaten als je er middenin zit. Zodra je uitzoomt, zie je die veranderingen overal: bij klanten, bij de overheid, bij criminelen. De veranderende wereld heeft simpelweg invloed op het werkveld. Het is de kunst om daar rekening mee te houden en scherp op te blijven en het niet - zoals ik eerder zei - te gebruiken als excuus."

Een andere uitdaging ligt volgens hem in de vertaalslag maken van de klantbehoefte naar de interne organisatie. Als klanten behoefte hebben aan oplossingen die Securify nog niet aanbiedt, biedt dit juist mooie kansen volgens Erik. Ook de positionering van bepaalde onderwerpen kan beter. "We doen ontzettend veel, maar klanten zijn zich hier niet altijd bewust van. We willen met meer onderwerpen on top of mind komen bij klanten."

Innovaties per team
Dat het ene team innovatiever is dan het andere team is een feit. Hoe komt dat? Erik heeft daar drie verklaringen voor. "De divergerende fase van brainstormen is belangrijk. Iedereen moet zich vrij voelen om ideeën te opperen. Nieuwsgierigheid, een onderzoekende houding

en outside the box denken zijn belangrijke eigenschappen van teamleden. Daarnaast is het van belang om tijd in te plannen om research te doen. Geef je het team de vrijheid om zelf op zoek te gaan naar verbeteringen. Houd je geen rekening met die twee stappen? Dan is innoveren moeilijker. Wordt er, als laatste verklaring, niet aangestuurd op executie? Dan houdt het natuurlijk ook op."

Natuurlijk zijn er ook veel ontwikkelingen om trots op te zijn als het gaat om innovaties binnen het securitydomein. Dat geldt ook voor Erik. In zijn sprekerscarrière presenteerde hij nét wat anders dan andere sprekers. Dat verhaal werd altijd goed ontvangen bij het publiek. "Vaak krijg je het standaard verhaal te horen: criminelen en spionnen doen enge dingen en 'dit' kun je ertegen doen. Ik deed precies het tegenovergestelde en leidde de speech in alsof we als criminelen bij elkaar waren samengekomen. Ik benoemde de kansen en risico's van het vak en vertelde hoe makkelijk het was om aanvallen in te zetten op slecht beveiligde computers vanuit het perspectief van een hacker. Op die manier blijft een verhaal veel beter hangen."

Over algemene ontwikkelingen binnen de securitysector is Erik ook te spreken. Hij benoemt een betere wet- en regelgeving, betere veiligheid van producten en een betere intel-positie. Dit soort maatregelen hebben volgens hem écht effect en bemoeilijken het werk van criminelen.

> **"De positie van criminelen wordt met alle maatregelen en nieuwe ontwikkelingen gelukkig steeds zwakker."**

Trends binnen de security
Erik voorziet drie opkomende trends in de komende vijf tot tien jaar:
Overheden die ransomware crews steeds beter en sneller verslaan.
Betere kwaliteit van software, zodat hacken moeilijker wordt.
Eisen aan de veiligheid van producten door de wetgever, zodat dit ook bijdraagt aan de bemoeilijking van hacken.

Tot slot vragen we Erik hoe hij op de hoogte blijft van de laatste ontwikkelingen: "Ik luister graag naar de podcast Risky Business. Een 'nieuwslezeres' deelt iedere dag tien minuten nieuws uit de branche en één keer in de week luister ik een verdiepende podcast van een uur. Ook van Risky Business. Maar, eerlijk is eerlijk, mijn collega's staan op nummer één als het gaat om inspiratie", sluit Erik het gesprek af.

“Wil je als bedrijf vooruit, digitaal transformeren, nieuwe business-modellen introduceren, succesvol aan de slag met AI? Dan is cybersecurity je randvoorwaarde.”

9. Dave Maasland
- CEO van ESET Nederland

Anderen het podium geven dat zij verdienen, daar ziet Dave Maasland als CEO van ESET Nederland een belangrijke rol voor zichzelf weggelegd. Zijn broer werd vroeger als 'echte nerd' gepest, maar tegenwoordig maken deze mensen juist het verschil, stelt hij. Expertise is een van de pijlers van de groeistrategie van het bedrijf, gevolgd door anticiperen op ontwikkelingen van aanvallers en samenwerkingen met andere partijen. Innovatie moet volgens Dave gericht zijn op 'het probleem achter het probleem'. "Stel jezelf de vraag: wat lossen we nu eigenlijk op?"

Met de paplepel ingegoten

Het kon bijna niet anders dan dat Dave de securitywereld in zou gaan. Net als zijn broer, Donny Maasland. Zijn broer wist op 5-jarige leeftijd al videorecorders in en uit elkaar te halen, later internetmodems te hacken en ook virusscanners waren regelmatig onderwerp van gesprek. Niet gek dat de interesse in het securitydomein op deze manier werd aangewakkerd bij Dave.

Fast forward naar de stageperiode. Vanwege persoonlijke omstandigheden koos Dave voor duaal studeren om zo zijn studie te kunnen betalen. Een werkstage was een verplicht onderdeel van de studie en zo belandde Dave bij NOD32 Nederland (later ESET Nederland). Laat dat nu net het antivirusprogramma zijn dat Dave's broer Donny altijd installeerde. "Mijn broer vond dit het allerbeste programma, dus mijn verwachtingen waren hoog. Aangezien dit volgens ons het beste antivirusproduct was, verwachtten we een groot softwarebedrijf. Bleek er zes man op kantoor te zitten aan drie bureaus."

Inmiddels is hij CEO van ESET Nederland. ESET isgespecialiseerd in cybersecurity en antivirussoftware en actief in meer dan 200 landen, waaronder Nederland. In Nederland biedt ESET verschillende producten en oplossingen op het gebied van cybersecurity. Het bedrijf biedt onder andere antivirus- en antimalwaresoftware voor zowel consumenten als bedrijven.

Daarnaast biedt ESET ook monitoring oplossingen voor de beveiliging van netwerken, web- en e-mailbeveiliging, authenticatie en encryptie. Ook Donny is inmiddels werkzaam bij ESET.

> **"In cybersecurity werken is missiegedreven te werk gaan."**

Dave geniet van de kentering die op dit moment bij veel securitybedrijven plaatsvindt. "Als ik kijk naar de branche, ook binnen ons bedrijf, zie ik een ontwikkeling waarbij de 'nerds' écht het verschil maken. Zij zijn degenen die verstand hebben van wat er gebeurt. Ik heb meegemaakt hoe erg mijn broer gepest is, hoe hij jarenlang huilend bij de poort heeft gestaan en niet naar de middelbare school wilde. 'Vroeger' was het namelijk niet cool om veel over dit soort onderwerpen te weten. Dat is nu wel anders. In talkshows laten we zien dat je met cybersecurity écht iets belangrijks op de kaart zet. Ik heb het gevoel dat we nu

- meer dan ooit - missiegedreven te werk gaan. Mensen die ooit 'anders waren' een kans geven geeft mij ontzettend veel energie."

> **"Met iedereen uit de samenleving een bijdrage leveren aan digitale veiligheid, digitale weerbaarheid, inclusie, soevereiniteit. Dát drijft mij."**

Iets anders wat hem drijft is anderen een podium geven. "Gelukkig kan ik goed communiceren en kan ik altijd duidelijk maken wat ik vind. Een introverte hacker of techneut staat niet vooraan als het gaat om communicatie, terwijl zij óók dat podium verdienen. Ze blijven vaak ondergewaardeerd. Gelukkig veranderen die tijden. Dat inspireert me alleen maar meer."

Dave is enthousiast over het initiatief HackShield: een game die kinderen tussen de acht en twaalf jaar oud weerbaar maakt tegen cybercriminaliteit. Via deze game worden kinderen opgeleid tot cyberagents die zichzelf en hun omgeving kunnen beschermen tegen online gevaar. "Nu willen veel kinderen cyberagents worden. Dat vind ik ontzettend gaaf."

Innovatie uitgelegd door Dave

Als we Dave vragen naar innovatie, benadrukt hij dat dat veel meer is dan enkel iets nieuws. "Het gaat erom dat je durft te kijken naar de keuze voor specifieke probleemoplossingen. Definiëren is daarom belangrijk. Innovatie in cybersecurity is een veelkoppig monster, dat op veel verschillende manieren aangepakt kan worden. Ga dus na: wat is het daadwerkelijke probleem achter het probleem? Dát moet opgelost worden. Stel jezelf altijd de vraag: wat lossen we nu eigenlijk op?"

> **"Innovatie in cybersecurity is een veelkoppig monster, dat op veel verschillende manieren aangepast kan worden."**

Dave noemt het verhaal van Jos Burgers als voorbeeld. "Iedereen is bezig met het maken van een nieuwe boor, terwijl je soms alleen het gat in de muur nodig hebt."

Aan iedereen in dit boek stellen we de vraag of er voldoende geïnnoveerd wordt binnen het securitydomein. Dave antwoordt daarop: "Enerzijds wel, anderzijds niet. Aan de ene kant werken er veel briljante mensen. Dat in combinatie met technologie maakt dat we echt wel vooroplopen ten opzichte van de aanvaller. Het is een welbekend kat-en-muisspel. Aan de andere kant ben ik van mening dat we veel meer proactief kunnen en moeten werken. We moeten toe naar een toekomst waarbij we kijken naar cybersecurity als een brand. Voorkomen is beter dan genezen. Een brand probeer je immers ook te voorkomen."

Dave is van mening dat dit the way to go is. Hij omschrijft het als een ecosysteem waar dingen by default veilig zijn. Als voorbeeld noemt hij Apple. Dit bedrijf kwam er namelijk

achter dat maar een klein percentage van de iPhone-gebruikers een pincode op de telefoon had ingesteld. Apple stelde zichzelf de vraag hoe dit percentage verbeterd kon worden. Als reactie hierop werd de vingerafdruksensor ontwikkeld. Deze bevindt zich onder de homeknop, waar gebruikers toch al van plan waren te drukken. Na de ontwikkeling van de vingerafdruksensor had meer dan vijftig procent van de gebruikers zich beveiligd. Nog niet iedereen dus. De volgende ontwikkeling werd de Face ID. Enkel kijken zorgde al voor ontgrendeling. Resultaat? Bijna honderd procent van de iPhone-gebruikers heeft een beveiligde telefoon. "Deze aanpak is de essentie."

> **"Security is veel meer dan een proactief onderdeel van de User Experience. Veiligheid moet in principe de makkelijkste keuze zijn waarbij het geïntegreerd is."**

Dave refereert aan Johan Cruijff: "Deze man zei: 'simpel voetballen is het moeilijkst'. Simpele dingen maken binnen het securitydomein die met enkele knoppen te bedienen zijn, zijn ook zo'n voorbeeld. Achter makkelijke installaties en makkelijk in gebruik zijn, gaat ontzettend veel technologie schuil."

Volgens Dave gaat het niet alleen om de technologie zelf, maar ook om de dienstverlening rondom security-oplossingen. "Neem nu rapportages: die moeten zo simpel mogelijk zijn. Rapportages vol security-incidenten - van het identificeren van risico's tot het reageren op incidenten - moeten begrijpelijk zijn voor personen die er minder verstand van hebben. Simplistisch en begrijpelijk communiceren is dus cruciaal." Er is daarnaast ook sprake van 'meldingsmoeheid' bij ontvangers, waardoor de noodzakelijke mitigerende maatregelen niet altijd voldoende worden geïmplementeerd.

Dit constateren is één, maar innovatie in het cybersecuritydomein beter organiseren is twee. Dave geeft - naast de definitie van cybersecurity scherp hebben - vier adviezen. Innovatie als agendapunt bij conferenties, het verbeteren van het start-up ecosysteem, een langzame verschuiving van stakeholders richting shareholders om de integriteit van data en technologie te verbeteren en meer samenwerking tussen private partijen. Hieronder licht Dave dit verder toe.

1. Innovatie als agendapunt bij conferenties
"Innovatie moet op de kaart gezet worden op plekken waar we samenkomen, zoals bestaande cybersecurityconferenties of conferenties binnen de overheid. Cybersecurity is onvoldoende onderwerp van gesprek. Ik ken bijvoorbeeld geen enkele plek of conferentie waar samen wordt gekomen om gezamenlijk na te denken over cybersecurity. Nog niet eens over de nieuwste producten of de prioritering van probleemoplossing. Dat kan dus echt beter."

2. Verbeteren van het start-up ecosysteem
"Het start-up ecosysteem in Nederland kan beter gestimuleerd worden. Ik zie veel interessante start-ups waar veel geld achter zit, maar waar tegelijkertijd veel (buitenlandse)

investeerders een rol vervullen die niet genoeg verstand hebben van cybersecurity. Mijn suggestie? Dat investeringsmaatschappijen samen gaan werken met cybersecuritybedrijven om die start-ups succesvoller te maken. Hoe blij ik ook met innovatie ben, in de praktijk zorgt niet elke start-up voor een makkelijkere oplossing. Ze verkopen juist 'losse' producten die geen daadwerkelijk probleem oplossen. Zonde."

3. Stakeholders versus shareholders

"Afhankelijk van de definitie van cybersecurity, past het ook binnen thema's zoals duurzaamheid of sociaal verantwoord ondernemen. Meer en meer bedrijven erkennen langzaam maar zeker dat het niet alleen draait om stakeholder value, maar meer om shareholder value. Je moet zorgen voor je consumenten, het milieu en voor iedereen waarmee je bedrijf in aanraking komt. Cybersecurity is daarmee inherent een thema over duurzaamheid. Het beschermen van klantdata en data van leveranciers in je leverancierskеten is belangrijk. Bovendien gaat het niet enkel over het beschermen van data. Ook de integriteit van de systemen, technologie én data binnen de private sector, de overheid en het onderwijs moet op een zinvolle manier gebeuren. Dat vertrouwen krijgen en behouden is onze verantwoordelijkheid."

4. Samenwerking tussen private partijen

"De oorlog in Oekraïne wees uit hoe belangrijk het is dat private bedrijven met elkaar samenwerken. Zulke samenwerkingen houden meer in dan enkel innovatie. Het gaat om de aanpak van het collectief en helder communiceren. Dit wordt - als je het mij vraagt - een steeds belangrijker thema.

"Misschien dat jouw initiatief van de Security Innovation Stories ook een bijdrage kan leveren aan meer samenwerking tussen private partijen."

De groeistrategie van ESET in combinatie met innovatie

Op innoveren in het algemeen heeft Dave dus een duidelijke kijk. Maar hoe zit dat met de groeistrategie en de daarbij behorende rol van innovatie bij ESET Nederland? Dave: "Ik denk dat ESET als geen ander duurzame groei hoog in het vaandel heeft staan. Wij zijn één van de weinige wereldwijde private owned beveiligingsbedrijven. Dit voorkomt dat we niet snel zullen groeien door een 'buy and build'-aanpak. Wij kiezen ervoor om organisch te groeien. De groeistrategie bestaat uit drie hoofdpunten."

Samengevat komt dit neer op groei van basis van expertise, groei op basis van de ontwikkelingen van de aanvaller en groei in samenwerking met partners.

<u>1. Groei op basis van expertise</u>

Met inmiddels 35 jaar ervaring in het vak weet ESET waar ze het over hebben. "Wij maken producten op basis van inzichtelijke risico's. Innovatie speelt hierin een cruciale rol, maar dat is niet altijd makkelijk. Wij zien genoeg organisaties die voor ongekende uitdagingen staan, zoals personeelstekort, toenemende dreigingen en de complexiteit van verschillende oplossingen. Ga er dan maar aan staan. We geloven wel dat onze concurrenten goede producten hebben, maar wij willen écht innoveren op de service en het maximale gebruikersniveau voor onze klanten. Een totaaloplossing dus."

> **"In de kern gaat het om cybersecurity en software simpeler maken voor de klant. Dit moet er uiteindelijk aan bijdragen dat gebruikers de primaire bedrijfsactiviteiten kunnen doen zonder daarin beperkt te worden. Tegelijkertijd zorgen we ervoor dat onze klanten de software op het maximale niveau kunnen gebruiken."**

2. Groei op basis van de ontwikkelingen van de aanvaller
Bij ESET staat een science-driven aanpak centraal. Dave licht dit toe: "Wij kijken vooral naar de vragen: waar beweegt de aanvaller naartoe? Wat doen aanvallers in de echte wereld? Op basis daarvan gaan wij detectielagen, softwareproducten en solutions maken. We gaan niet blindelings af op adviezen van Gartner (zie begrippenlijst). Expertise, het verbeteren van de servicelaag voor de klant én deze oplossingen ontwikkelen op basis van het verkeer van de dreigingen, maakt dat we daadwerkelijk problemen van klanten op kunnen lossen."

3. Groei in samenwerking met onze partners
"Een verbeterpunt bij ESET is beter uitleggen aan de stakeholders wat we doen en wat onze betekenis voor klanten is. Denk bijvoorbeeld aan onze IT-partners. Dit zijn partijen die IT-dienstverlening leveren waarbij wij het securitygedeelte voor onze rekening nemen. Ik geloof in een toekomst waar IT-partners nog steeds het aanspreekpunt zijn voor veel klanten als het gaat om digitale veiligheid. Uitleg geven over het gebruik en het optimaal instellen van de security producten blijft een continue uitdaging."

Cloud Sandbox
Het lijkt wel goed te zitten met de groeistrategie van ESET in combinatie met innovatie. Voelt dat voor Dave ook zo? "Ik ben trots, maar niet tevreden. Trots ben ik op onze simpele, maar veilige oplossingen. Simpel blijft het moeilijkst. Een voorbeeld is onze Cloud Sandbox. Dat is een technologie waarbij gebruikers een bestand kunnen openen op hun laptop. Met Cloud Sandbox wordt het bestand direct vanuit de endpoint naar de geïsoleerde omgeving geplaatst om gescand te worden op veiligheid. Zo is security een vangnet en kan de bijlage toch geopend worden."

Nieuw gelanceerd product voor telecombedrijven
Een ander voorbeeld waar Dave trots op is, is een product - DNS gebaseerd - dat ze onlangs gelanceerd hebben voor telecombedrijven. "Zodra je naar een phishing website surft, wordt de website automatisch geblokkeerd. Het internet is dan direct bij de bron veilig. Toch zal ESET niet voor anderen bepalen of je websites wil uitsluiten. Daarom hebben we de mogelijkheid voor 'gefilterd' internet ontwikkeld, waarbij de gebruiker volledig in controle blijft. De regie blijft bij de gebruiker via een app. Twijfelt de app aan de veiligheid van websites? Dan krijg je een melding. Dat vind ik een fantastisch voorbeeld van security gebruiksvriendelijker maken en tegelijkertijd de controle bij de gebruiker laten."

De levering van dreigingsinformatie
Een derde innovatie die Dave niet onbelicht wil laten, bleek tussen neus en lippen ook al eerder toen het ging om groeien op basis van het volgen van de aanvaller én de

samenwerking tussen private partijen. Hij doelt op de levering van dreigingsinformatie, die - helaas - is doorontwikkeld sinds de oorlog tussen Oekraïne en Rusland. "Op het moment dat Rusland Oekraïne binnenviel, werden de wipers om data te vernietigen breed ingezet bij lokale overheden en bij financiële instellingen. Daarnaast zijn statelijke actoren nu veel actiever geworden. Dreigingsinformatie is waardevoller geworden en klanten hebben er daadwerkelijk wat aan om hun specifieke modus operandi te kennen."

"Maar", vervolgt Dave, "naast deze projecten waar we trots op zijn, vinden er nog steeds dagelijks ransomware-incidenten plaats. Oftewel: er zijn nog steeds veel consumenten en bedrijven slachtoffer. We moeten er een bijdrage aan blijven leveren om dit probleem aan te pakken." Deze (dagelijkse) uitdaging hangt samen met zijn toekomstgerichte visie.

Expertise en technologie gaan hand in hand
Ook blijven de belangrijkste trends niet onbesproken. Hoe ziet de toekomst eruit volgens Dave?

- Expertise moet naast technologie bestaan. Stel jezelf weer de vragen: wie interpreteert de resultaten en wie zorgt voor de daadwerkelijke actie?
- In het verlengde daarvan gaat het om betere security engineering. Het gaat niet om de gekochte tool, maar om de interpretatie én de werking ervan binnen de organisatie."
- Een andere trend waar Dave het over heeft, is 'business first'."Cybersecurity is geen doel op zich. Het is een middel om primaire doelstellingen van een organisatie te realiseren. Het vertalen van de werkelijke risico's naar beslissers is daarbij cruciaal. Een goede CISO is hiertoe in staat door een heldere uitleg te geven over de gewenste risicoafdekking op basis van de ambitie van de organisatie. Dát is de kracht: CISO's die in staat zijn met de board te schakelen over een bedrijfsstrategie in relatie tot cybersecurity. In mijn optiek wordt dit belangrijker dan ooit."
- Dave vervolgt zijn verhaal: "Wil je als bedrijf vooruit, digitaal transformeren, nieuwe businessmodellen introduceren en succesvol aan de slag met AI? Dan is cybersecurity je randvoorwaarde en is het aan ons om je zo goed mogelijk te helpen met de realisatie." Daarom kiest ESET ervoor om vooruitgang te beschermen: progress protected. "We hoeven niet bang te worden van technologie", vervolgt de CEO van ESET Nederland.

> **"Technologische vooruitgang gaat sneller dan ooit. Hoe groter cybersecurity wordt, hoe belangrijker het is om te benadrukken dat cybersecurity niet het doel is."**

Hoe je volgens Dave op de hoogte blijft van de laatste trends en ontwikkelingen
Hoe blijft Dave up-to-date met die razendsnelle technologische vooruitgang? "Door mezelf te blijven inspireren. Iedere dag klinkt Bill Gates in de auto door mijn speakers. Mijn favoriete podcasts zijn Defense in Depth en de CISO series (CISO & Security vendor relationship). Het zijn beide Amerikaanse podcasts. De materie die besproken wordt, gaat verder dan wat wij in de Nederlandse podcasts horen." De laatstgenoemde podcast gaat in

op de relatie tussen de vendor en de CISO en is een waardevolle podcast voor iedereen die zich in dit speelveld bevindt.

“Daarnaast omring ik mezelf graag met technisch specialisten uit mijn netwerk. Dat is waardevol voor iedere professional: een netwerk bouwen met mensen die door de bullshit heen kunnen prikken. Ik zie het als mijn taak om een complex onderwerp naar een breed publiek te vertalen. Dat gaat soms beter met simpele metaforen. Toen een log4j kwetsbaarheid werd ontdekt, was het lastig om dit complexe begrip uit te leggen op een manier die iedereen begreep. Met onze CTO kwam ik op het woord ‘digitaal asbest’. Dit maakte de uitleg over deze kwetsbaarheid tastbaarder”, aldus Dave.

Positiviteit in de branche

Afsluitend merkt Dave nog op dat de branche wel wat positiviteit kan gebruiken. “Tegenwoordig willen steeds meer jongeren hackers worden, omdat ze opgroeien met technologie. Dat is gaaf. Daarnaast zie ik dat de publieke-private samenwerking steeds meer van de grond komt en hebben we een Nederlandse Cybersecuritystrategie. Dat is nog nooit eerder voorgekomen. Dat zijn allemaal positieve zaken die zeker meer belicht mogen worden. Er zijn gelukkig veel dingen in de markt om positief over te zijn. Ik hoop dat jouw initiatief hier ook een bijdrage aan kan leveren”, sluit Dave af.

”Innovatie kan worden gestimuleerd door samen te werken met nieuwe spelers in plaats van te kiezen voor de gevestigde orde.”

10. Jurjen Harskamp
- Co-founder en CEO van Hunt & Hackett

Jurjen Harskamp is co-founder en CEO van Hunt & Hackett, het eerste cloud native cybersecuritybedrijf in Nederland. Hij legt uit waarom ze hiervoor hebben gekozen en hoe ze hun innovatieve threat-modelling aanpak inzetten om klantomgevingen weerbaarder te maken. Nu is hij bezig met de laatste puzzelstukken van zijn holy grail in cybersecurity: een manier vinden om beveiliging geautomatiseerd te kunnen valideren, zodat je kunt bepalen hoe veilig je eigenlijk écht bent tegen specifieke aanvalsmethodes.

Kennismaking met cybersecurity

De weg naar het cybersecuritydomein begon voor Jurjen in 2005. Hij werkte toen als director bij het consultancybureau Policy Research Corporation en deed veel opdrachten voor Defensie. Het keerpunt kwam na de financiële crisis in 2008, die leidde tot discussies binnen Defensie over bezuinigingen. Jurjen vertelt: “Er werd besloten dat de tanks eruit moesten, waardoor er een besparing van één miljard werd gerealiseerd. Tegelijkertijd wilden ze honderd miljoen investeren in cybersecurity, dat toen nog een vaag en ongedefinieerd concept was. Wij werden vervolgens gevraagd om mee te denken over hoe dit geld het beste besteed kon worden. Zo ben ik de cybersecurity ingerold, waarbij mijn achtergrond ook wel van pas kwam.”

Jurjen had onder andere een opleiding elektronica afgerond en groeide op in een tijdperk waarin computers een opkomende technologie waren. In zijn vroege dagen experimenteerde hij met computers en de eerste modems, wat hem een goed begrip gaf van hoe ze werkten én hoe ze mogelijk misbruikt konden worden. “Ik was zeker geen hacker, maar ik wist net genoeg om dingen uit te proberen en te leren hoe het werkt. Dit heeft me altijd geïntrigeerd, dus werken in het cybersecuritydomein was voor mij uiteindelijk heel passend.”

Oprichting Hunt & Hackett

Toen cybersecurity een steeds prominentere rol begon te spelen binnen de Nederlandse overheid, raakte Jurjen vanuit Policy Research betrokken bij het oprichten van het Nationaal Cyber Security Centrum (NCSC), de organisatie die zich inzet voor een digitaal veilig Nederland. Een centrale vraag hierbij was wat de Nederlandse cybersecuritystrategie kon of zou moeten worden. Hij vond zijn sparringpartner in Ronald Prins, medeoprichter van het cybersecuritybedrijf Fox-IT. “We voerden eindeloze gesprekken over cybersecurity”, vertelt Jurjen. “Als we dezelfde soort evenementen bezochten, dan stapten we bij elkaar in de auto om verder te praten. Op het moment dat Ad Scheepbouwer instapte in 2012 en er een strategie voor internationalisering moest worden uitgewerkt, ben ik bij Fox-IT betrokken geraakt en kort daarna ook ingestapt.”

Het bedrijf groeide gestaag. Uiteindelijk werd Fox-IT in 2015 verkocht aan het Britse NCC Group en niet lang daarna vertrokken ook de oprichters. Maar de samenwerking tussen Ronald en Jurjen hield stand. Een paar jaar later, in 2020, richtten ze hun eigen cybersecuritybedrijf op: Hunt & Hackett. Ze zagen dat Europese kennis, technologie en intellectueel eigendom steeds vaker het doelwit waren van spionage en gerichte

cyberaanvallen. “Veel Chief Information Security Officers hebben hier nog geen antwoord op. Vaak komt cybersecurity pas echt op de agenda van een directie nadat er een significante hack heeft plaatsgevonden bij het bedrijf zelf of bij een toonaangevend bedrijf in hun sector. Dan wordt opeens duidelijk dat de IT-partners niet over de benodigde cybersecurity expertise beschikken om effectieve beveiligingsstrategieën te ontwikkelen tegen dergelijke aanvallen. Wij wilden ervoor zorgen dat deze partijen weerbaar worden tegen alle type cyberdreigingen, en APT-aanvallen in het bijzonder” (zie begrippenlijst), legt Jurjen uit.

Het begint niet met technologie, maar bij het dreigingsbeeld

De beginfase bij Hunt & Hackett was achteraf gezien één van de momenten uit zijn hele carrière waar Jurjen het meest trots op is. “We besloten te beginnen met een handjevol cybersecurityexperts, het kernteam. Iedereen had net zijn comfortabele, goedbetaalde baan opgezegd om vervolgens in een kantoortje te gaan zitten en dan maar eens te gaan bepalen wat we nu precies met elkaar gingen doen. Die eerste dagen dat we daar zaten hebben we onze unieke aanpak gecreëerd. We brachten daarmee veel verschillende disciplines samen, waaruit onze threat-modelling aanpak is uitgedacht. Dat leidde uiteindelijk tot een belangrijke realisatie: geen van ons had afzonderlijk de oplossing kunnen bedenken die we in de eerste weken met elkaar hadden gecreëerd. Dat zette de toon voor zowel de wijze van samenwerking als voor innovatie binnen het bedrijf.”

Hunt & Hackett is een Managed Service Provider of XDR provider waarbij de digitale omgevingen van hun klanten 24/7 worden gemonitord. Jurjen vertelt dat ze zich niet focussen op de heel grote bedrijven, maar juist op organisaties die een paar honderd tot vijfduizend medewerkers hebben. Zij moeten volgens Jurjen vaak nog een transitietraject in om weerbaar te worden. Denk dan aan de sectoren maritiem, manufacturing, land-, glas- en tuinbouw, logistiek en technologie. “Veel van onze klanten hebben te maken met ‘industrie 4.0’-vraagstukken op het snijvlak van IT en OT. Daarnaast is de gemene deler dat ze, veelal met veel eigen ontwikkelde applicaties en systemen, internationaal opereren en exportgericht zijn. Ook zijn ze vaak innovatief, hebben daardoor ook veel Intellectual Property (IP) en zijn belangrijk voor de Nederlandse economie. De keerzijde daarvan is dat ze daarmee ook een hoog risicoprofiel hebben en de kans lopen om specifiek aangevallen te worden. Het gaat er bij dit soort organisaties niet om of ze de juiste securitytechnologie hebben, maar hoe je de aanvallers die specifiek interesse in jouw organisatie hebben buiten de deur houdt”, stelt Jurjen. Dat vraagt veel analyse, kennis en maatwerk. Hoe ga je een securityconcept neerzetten om de kritieke assets van de organisatie te beschermen als er aanvallers zijn die het specifiek op jouw type organisatie hebben gemunt? Juist dat speelveld vindt hij interessant.

Vanaf de lancering is de aanpak van Hunt & Hackett gericht op intelligence-data. Dat wil zeggen dat de aanpak in kaart brengt welke dreigingen er zijn en welke typen aanvalsmethodes gebruikt worden. Ze houden daarom meer dan vijfhonderd statelijke en cybercriminelen groepen in de gaten: analyseren hun modus operandi, welke aanvalsmethodes ze gebruiken, welke tools ze gebruiken en hoe ze te werk gaan. Dat beeld vertalen ze vervolgens naar wat dat betekent voor preventie, detectie en response. Op welke manieren kun je een organisatie beschermen tegen die aanvalsmethodes? Welke

securitymaatregelen heb je tot je beschikking ter beveiliging? Welke data wil je loggen en monitoren om zulke aanvallen te kunnen detecteren? En hoe zorg je ervoor dat er tijdens een aanval de juiste signalen worden verstuurd voor monitoring? Door dit in kaart te brengen kun je heel gericht een securityconcept uitwerken en een organisatie weerbaar maken tegen een specifiek dreigingsbeeld.

> **"Om een omgeving te creëren waarin innovatie mogelijk is, moet het echt geborgd zijn in de strategie en cultuur van een organisatie. Huidige validatie- mogelijkheden geven inzicht in je zwakste punten, maar niet in alle mogelijke aanvalspaden. Daar zie ik kansen voor de toekomst."**

Beveiliging valideren: hoe veilig ben je nu echt?
Eén van de uitdagingen waar de cybersecuritysector op dit moment tegenaan loopt is dat het lastig is vast te stellen hoe het gesteld is met je huidige cybersecurity. Jurjen legt uit dat dit nu alleen kan via een penetratietest of door het simuleren van cyberaanvallen, het zogeheten Red Teaming. "Dit is arbeidsintensief en de scope van het validatiestuk is daarnaast ook beperkt. Je krijgt inzicht in je zwakste punten, maar niet in die van alle mogelijke aanvalspaden. Je krijgt vooral meer te weten over wat de plekken zijn waar je met de minste weerstand binnen kan komen. Dat is ook relevant, maar het geeft geen beeld van hoe veilig je nu echt bent over de hele linie."

Daar ziet Jurjen dan ook kansen voor toekomstige innovaties en ontwikkelingen. "Er wordt hard gewerkt om een stukje geautomatiseerde validatie aan ons Security Operations Center (SOC) toe te voegen. We willen een oplossing maken waarbij je klantomgevingen continu kan aanvallen met een grote verscheidenheid aan aanvalsmethodes, in plaats van één specifieke aanval. Dan kun je het dreigingsbeeld waartegen je de organisatie wilt beschermen ook meteen simuleren en je preventie-, detectie- en responsemaatregelen op continue basis valideren. Als er nieuwe aanvalsmethodes of tools ontdekt worden, kan eventuele impact meteen worden getoetst op een klantomgeving. Dat is de holy grail."

''Bij ransomware kennen we honderd tot tweehonderd aanvalstypen die we frequent op een organisatie afvuren en we kijken tegelijkertijd of onze preventiemaatregelen en detectie doen wat ze zouden moeten doen. Door die grotere variatie wordt het veel statistischer in plaats van binair: zeventig procent wordt wel tegengehouden aan de voordeur, twintig procent komt verder dan we eigenlijk zouden willen maar wordt alsnog tegengehouden en tien procent blijkt bijvoorbeeld wel succesvol. Op basis daarvan kunnen we securitymaatregelen toevoegen of aanscherpen. In ons nieuwe concept proberen we deze elementen toe te voegen, zodat een klant uiteindelijk inzicht krijgt voor welk type aanvallen de organisatie weerbaar is. Met een dergelijk inzicht wordt het voor een directie veel makkelijker om te duiden wat het risico-acceptatieniveau is en welke risico's beheersbaar dienen te worden gemaakt."

> **"Vanaf dag één staan we voor innovatie. Dat betekent voor mij een visie en het continu verbeteren, itereren en de lat hoger leggen om dingen beter, efficiënter en hoogwaardiger te doen."**

Continu blijven verbeteren
Ontwikkelen en innoveren is wat Jurjen dan ook het liefste doet in zijn werk. "Continu nadenken: Hoe kan je dingen beter maken? Hoe kan je de propositie verbeteren? Waar staan we nu? Wat zijn de volgende stappen die willen zetten? Het is ook niet ons doel om het grootste cybersecuritybedrijf te worden. We geloven in kleine teams, met veel focus, expertise en ruimte voor creativiteit."

Als we hem vragen wat innovatie is, hoeft hij niet lang na te denken. "Continu verbeteren, itereren en de lat hoger leggen om dingen beter, efficiënter en hoogwaardiger te doen", zegt hij. Innovatie moet volgens Jurjen echt geborgd zijn in zowel de strategie als de cultuur van een organisatie. "Het is geen project dat even tussendoor uitgevoerd kan worden. Dan wordt het niet gedragen door de rest van de organisatie."

Dat werkt ook bij Hunt & Hackett zo. Ze werven bijvoorbeeld niet op een functie, maar juist op expertise en talent. Mensen moeten willen bouwen, ontdekken, leren en ontwikkelen. "Vaak zijn het mensen die dingen kunnen creëren en de functie is simpelweg een rol om een startpunt te hebben. Maar het stukje innovatie komt ook terug in hoe we de organisatie aansturen. We dagen elkaar continu uit om ons eigen werk beter te maken, of zelfs overbodig als het kan. We verwachten eigenlijk dat medewerkers al het repetitieve werk dat in een functie zit proberen te automatiseren. Wel met behoud van kwaliteit of sterker nog, juist om het kwalitatief hoogwaardiger te maken, zodat er meer tijd en aandacht kan zijn voor de complexe zaken."

En zelfs toen ze het bedrijf oprichtten was er al sprake van innovatie. Ronald Prins is bijna vijfentwintig jaar geleden begonnen met het eerste Security Operations Center (SOC) in Nederland, dus we hebben een naam hoog te houden. Hunt & Hackett is het eerste cloud native securitybedrijf in Nederland. "Met de nieuwe start hadden we geen legacy technologie, dus we konden met een schone lei starten en gelijk vanaf het begin onze omgeving efficiënt inrichten. We kozen voor een cloud native approach. Hierdoor zijn we in staat om snel en efficiënt een specifieke klantomgeving op te bouwen en deze flexibel te laten meegroeien met de situatie en behoefte van onze klanten. Dat betekent dat alle data, de hele infrastructuur, alles wat benodigd is om een bepaalde dienst te leveren, voor één klant specifiek is. Dat is veiliger en efficiënter. In een on-premise SOC omgeving is deze architectuur en mate van flexibiliteit niet mogelijk."

Tot slot werken ze met het principe Infrastructure as Code (IaC). Jurjen licht toe: "Onze Managed Detectie & Response (MDR), Breach & Attack Simulation (BAS), en Incident Response (IR) service-platformen zijn allemaal 'as code' ontwikkeld. Met IaC gebeurt het uitrollen en beheren van infrastructuur via code in plaats van via handmatige processen. Dat is een bewuste keuze en tastbare innovatie om zowel consistentie als schaalbaarheid te creëren. Dergelijke concepten zijn alleen mogelijk in een cloudomgeving. De configuratie

is bijvoorbeeld helemaal scripted. Het staat in een file, we kunnen aanpassingen in de file doen en dat rolt automatisch helemaal door en de configuratie, security of performance settings worden veranderd. Dit kostte in het begin veel meer tijd, maar maakt ons nu veel efficiënter voor onze klanten, omdat wijzigingen indien nodig direct in één keer over alle omgevingen kunnen worden uitgerold."

> **"Gesubsidieerde projecten vormen zelden een springplank naar succesvolle innovaties. Ze leiden vaak zelfs af van je eigen strategie en ontwikkelrichting. Veel effectiever is het in de regel als innovaties voortkomen uit ideeën van de organisatie zelf. En je daar je focus en creativiteit aan besteedt."**

Innovatie moet vanuit een organisatie zelf komen

Naast de ontwikkelingen bij Hunt & Hackett, ziet Jurjen ook genoeg kansen voor innovatie in het gehele cybersecuritydomein. Wel vindt hij dat het eigenlijk niet reëel is om de sector in Nederland als één geheel te beschouwen. Er zijn technologie start-ups, managed security partijen (zoals Hunt & Hackett) en cybersecuritybedrijven die zich richten op consultancy diensten. Daarnaast is er de overheid met diverse entiteiten die zich met cybersecurity bezighouden, kenniscentra, universiteiten, belangenorganisaties en diverse onderlinge samenwerkingsverbanden. Een divers veld dus met verschillende spelers, die allemaal op een eigen manier innoveren.

Allereerst denkt Jurjen dat innovatie het meest effectief is als de behoefte en ideeën vanuit een organisatie zelf komt. Op het moment dat organisaties eigen ideeën hebben en op basis daarvan gaan innoveren en itereren, dan werkt dat vaak beter dan wanneer ze inschrijven op een specifiek gesubsidieerd innovatieproject. Dergelijke subsidietrajecten komen vaak neer op een ontwikkelopdracht waarbij het doel en de richting reeds is geformuleerd door anderen. Het nadeel is dat je dan altijd moet zoeken of het voldoende past in je eigen strategie en gewenste ontwikkelrichting. Of dat je het project kunt ombuigen naar iets waar je zelf ook voldoende aan hebt. Maar meestal zijn de randvoorwaarden al zodanig vastgelegd, dat je er veel zaken bij komen kijken die eigenlijk alleen maar afleiden. Ook fungeert dat maar zelden als springplank voor een succesvolle onderneming. De meest innovatieve partijen maken nauwelijks gebruik van dergelijke subsidietrajecten, want het kost in de regel te veel focus, ruimte en creativiteit."

Daarentegen werkt het concept van de WBSO-subsidie veel beter, vindt Jurjen. WBSO staat voor Wet Bevordering Speur- en Ontwikkelingswerk. Deze subsidie helpt innoverende bedrijven op basis van hun eigen plannen. "We zouden hierbij nog meer kunnen kijken naar waar we als Nederland over een paar jaar willen staan op het gebied van cybersecurity en hoe we dat kunnen realiseren. Dan kun je kijken of je in die richting meer ruimte kan bieden om meer technische innovatie in de sector te stimuleren."

> **"Ik denk dat we veel kunnen leren van andere landen, zoals de US, de UK, Frankrijk en Israël. In deze landen leunen overheden meer op de expertise van commerciële cybersecurity partijen en is de samenwerking meer gericht op het creëren, ontwikkelen en stimuleren van een hoogwaardige industrie."**

Samenwerken in de cybersecuritysector

"Naast het financieren en subsidiëren kan de overheid ook vraag naar innovatieve oplossingen creëren", stelt Jurjen. "Als we het hebben over het stimuleren van innovatie, dan zijn we er vaak op gericht om funding voor bepaalde innovaties te realiseren. Maar we denken nog te weinig na over hoe we demand kunnen creëren voor dergelijke oplossingen als ze eenmaal gerealiseerd zijn. Ik zie daar wel een rol voor de overheid weggelegd. De overheid is een grote afnemer van cybersecurity-oplossingen. Nu worden vooral de traditionele en gevestigde oplossingen afgenomen van de grote technologie partijen, terwijl ze ook markt kunnen creëren voor nieuwe innovatieve oplossingen. Dit is nu bijna ondenkbaar, denk alleen al aan de inkoopvoorwaarden die de overheid hanteert. Die maken het vrijwel onmogelijk voor start- en scale-ups om met de overheid samen te werken. Dat remt de toestroom van nieuwe spelers en samenwerkingen op de markt, en daarmee ook de innovatiekracht in de sector."

Jurjen vindt sowieso dat de samenwerking tussen alle verschillende partijen in de sector beter kan. Hij noemt het voorbeeld van de nieuwe cybersecuritystrategie voor Nederland die is uitgekomen. "Ik vind het toch opmerkelijk dat de leveranciers uit de cybersecuritysector niet zijn gevraagd om input hiervoor te leveren. Dit zijn toch de bedrijven die een significante rol spelen in het beschermen van de digitale infrastructuur van het Nederlandse bedrijfsleven. Dat laat zien welke weg we nog te gaan hebben. Ik denk dat we veel kunnen leren van andere landen, zoals de US, de UK, Frankrijk en Israël. In deze landen leunen overheden meer op de expertise van commerciële cybersecuritypartijen en is de samenwerking meer gericht op het creëren, ontwikkelen en stimuleren van een hoogwaardige industrie. Volgens mij kunnen we op dat vlak opener zijn, meer van elkaar leren en intensiever samenwerken."

> **"Ransomware is het meest zichtbaar en krijgt daarom ook veel aandacht in de media. Maar het stelen van informatie en spionage komen vijf keer zo vaak voor."**

Opkomende trends en ontwikkelingen

Jurjen ziet één belangrijke trend de komende jaren in de sector: AI. Wel houdt hij een slag om de arm: "We weten met AI immers vaak nog niet hoe veilig iets is. AI kan zeker helpen met bijvoorbeeld het schrijven van detectielogica en andere ondersteunende taken. Maar om er optimaal gebruik van te maken is het essentieel om het fundament van security op orde te hebben. Als we niet volledig begrijpen hoe AI werkt en wat erachter schuilt, bestaat

het gevaar dat we het overzicht verliezen van onze uiteindelijke doelen, zoals transparantie en objectiviteit in onze beveiliging. Om effectief te zijn, moeten we de architectuur goed inrichten en weten waar we ons wel en niet tegen beschermen. AI kan dan in de security operations naar de toekomst toe steeds meer taken uitvoeren. Daarbij is het wel goed om ons te realiseren dat de verantwoordelijkheid voor security helaas niet naar AI kan worden overgedragen."

> **"Een toenemende afhankelijkheid van geautomatiseerde securitydiensten van grote techbedrijven leidt vaak tot schijnveiligheid. Dit komt doordat standaardoplossingen niet altijd toereikend zijn voor specifieke dreigingen en situaties."**

Ook neemt de rol van grote technologiebedrijven steeds verder toe. Daar schuilt wel een gevaar in, denkt Jurjen. "Grote bedrijven, zoals Microsoft en Amazon, gaan steeds meer securitydiensten aanbieden als onderdeel van hun softwarebundels. Denk aan endpoint of SIEM-oplossingen. Dit is vaak geautomatiseerd en voor veel partijen een passende oplossing. Maar bij bijzondere situaties of omgevingen is het veelal niet toereikend of onvoldoende ingericht. We zien bijvoorbeeld steeds meer dat de technologie er weliswaar is, maar dat er maar heel weinig securitydata naartoe worden gestuurd vanwege bijvoorbeeld de hoge variabele gebruikskosten. Het resultaat is beperkt zicht op de relevante aanvalsmethodes uit het dreigingsbeeld van een organisatie. Dan komt er vanuit compliance wel een vinkje te staan dat alles in orde is, want er wordt aan de basis voldaan. Maar de beveiliging is niet echt op orde, daar is vaak dieper inzicht en maatwerk voor nodig. Schijnveiligheid dus. Dit is helaas niet een uitzondering maar steeds meer de norm."

Zolang politieke spanningen toenemen blijft ook cybersecurity een uitdaging, verwacht Jurjen. Ransomware is volgens hem het meest zichtbaar en krijgt daarom ook veel aandacht in de media. Maar het stelen van informatie en spionage komen vijf keer zo vaak voor. Deze worden alleen onderbelicht in de berichtgeving. De impact van spionage kan sluipend zijn en geleidelijk de intellectuele eigendommen en winstgevendheid van organisaties aantasten, zonder directe, opvallende gevolgen. "Er is een hele wereld die niet direct zichtbaar is, maar daar gebeurt wel heel veel. En dat het ontastbaar is, wil niet zeggen dat het er niet is. Wij blijven werken aan het continu verbeteren en veiliger maken van die wereld, ook ligt de behoefte vanuit de markt op dit moment vooral op het tegengaan van ransomware. Wat dat betreft zien we nu slechts de top van de ijsberg. Uiteindelijk zullen we als samenleving ook het onzichtbare deel van deze ijsberg moeten gaan adresseren. Daar is overtuiging, doorzettingsvermogen en innovatiekracht voor nodig. Iets wat we echt alleen samen kunnen realiseren."

“Het lerend vermogen van de organisatie wordt vaak onvoldoende getriggerd, terwijl dit de mens juist tot een sterke schakel kan maken in plaats van de zwakste.”

11. Martijn van de Beek
- Directeur van onderzoeksbureau Hoffmann

Een meer mensgerichte aanpak in de securitybranche. Daar zet Martijn van de Beek, directeur van onderzoeksbureau Hoffmann, zich voor in. Innovatie is volgens hem slimmere, betere en efficiëntere manieren vinden om de problemen van vandaag en morgen op te lossen. Iets dat nu nog te weinig in de sector gebeurt en te veel gefocust is op techniek, vindt Martijn. Bij Hoffmann kijken ze daarom naast techniek, architectuur en fysieke beveiliging ook specifiek naar de factor 'mens'.

De aanhouder wint

Bij zijn 26e sollicitatie, in een tijd dat er niet werd geworven, werd Martijn in 1996 aangenomen bij de Amsterdamse politie. Hij startte met de officiersopleiding aan de politieacademie. Later, tijdens zijn management traineeship bij politie Amsterdam-Amstelland, kwam hij erachter dat het onderzoeksvak echt zijn ding was. "Mij kon je midden in de nacht opbellen voor een moordzaak. Ter plaatse komen en geen idee hebben hoe de vork in de steel stak, gaf me ontzettend veel energie," vertelt Martijn enthousiast.

Na het recherchewerk stapte hij over naar de Landelijke Eenheid, waar hij leiding gaf aan het team internationale misdrijven (oorlogsmisdrijven). Een aantal jaar later, in 2006, zette Martijn de High Tech Crime Unit op, waar hij de eerste teamchef van werd. Team High Tech Crime (THTC) is een gespecialiseerd onderzoeksteam dat zich richt op het onderzoeken en bestrijden van hightech criminaliteit, de georganiseerde criminaliteit variant van cybercrime. Denk daarbij aan misdaden die worden gefaciliteerd of gepleegd met behulp van technologie, zoals hacking, online fraude en cyberspionage.

De eenheid maakt deel uit van de Nationale Politie en werkt nauw samen met andere (inter)nationale wetshandhavingsinstanties en private sector partners. Het doel? Personen en groepen die betrokken zijn bij hightech criminaliteit identificeren en vervolgen. Team High Tech Crime biedt ook ondersteuning en expertise aan andere politie-eenheden die technologie gerelateerde misdaden onderzoeken. "In de begintijd lag de focus vooral op cybersecurity. Tegenwoordig worden de datasets van criminelen ook gebruikt om de 'reguliere' vormen van georganiseerde criminaliteit en ondermijning aan te pakken," aldus Martijn.

> **"In een digitale wereld is alles met elkaar verbonden. Het slachtoffer kan in Nederland zijn, de dader in Oost-Europa en de hardware in Frankrijk. Om dit te bestrijden heb je internationale partners nodig die bereid zijn om sámen het verschil te maken."**

THTC als innovatief succes

Op de vraag hoe het THTC een innovatief succes werd, antwoordt Martijn: "De kracht zat hem vooral in de combinatie van politie-experts die ervaring hadden met onderzoeken

naar zware criminaliteit en digitale experts met veel technische kennis. Samen wilden zij Nederland een stukje veiliger maken. En niet alleen Nederland. De internationale cybercriminaliteit nam op dat moment enorm toe, dus zijn we direct internationaal gaan denken. In een digitale wereld is alles met elkaar verbonden. Het slachtoffer kan in Nederland zijn, de dader in Oost-Europa en de hardware in Frankrijk. Om dit te bestrijden heb je internationale partners nodig die bereid zijn om sámen het verschil te maken. Soms is de ene organisatie wat beter in een bepaald puzzelstukje dan de ander. Als je dit slim combineert en samenwerkt aan het gezamenlijk belang, ben je enorm effectief. Op dit moment is deze unit nog steeds één van de meest succesvolle units van de politie" vertelt Martijn trots.

De sprong naar Hoffmann

Toen zich in 2015 een mooie kans voordeed, waagde Martijn de sprong naar onderzoeksbureau Hoffmann. Inmiddels werkt hij al ruim acht jaar als algemeen directeur voor het bedrijf. Daardoor kent hij zowel de overheid als het bedrijfsleven goed. Wat ziet hij als de belangrijkste verschillen? Martijn: "In het bedrijfsleven is er meer focus op resultaat. Bij de politie was er meer aandacht voor onderzoek en de uitkomsten daarvan. Ik denk ook dat er bij de overheid meer tijd is voor innovatie, maar minder focus. Ze hebben vaak duizend goede ideeën, maar ze laten het na die te operationaliseren. In het bedrijfsleven daarentegen is er soms juist te weinig focus op innovatie, en te veel focus op wat klanten op korte termijn willen. Terwijl dit een spanningsveld is dat altijd in balans moet zijn." Op dit incidentgedreven werken komt Martijn later in dit gesprek nog terug.

Over Hoffmann

Hoffmann is een onderzoeksbureau met een rijke geschiedenis van ruim zestig jaar. Op de vraag waar Hoffmann voor staat, antwoordt Martijn enthousiast: "Als Hoffmann willen we hét onderzoeksinstituut op het gebied van fraude, gedrag, cybersecurity en crisismanagement blijven. We bieden diensten aan op het gebied van fraudeonderzoek, integriteitsonderzoek en onderzoek naar grensoverschrijdend gedrag. Maar we helpen organisaties ook bij hun risicomanagement, cybersecurity en crisismanagement. En we geven trainingen. Eigenlijk helpen wij organisaties om de veiligheid en integriteit te waarborgen en eventuele risico's te minimaliseren, om zo een werkomgeving te creëren waarin mensen volledig kunnen vertrouwen op elkaar en op hun organisatie."

De rol van Martijn

"Als algemeen directeur zorg ik ervoor dat mijn mensen hun werk kunnen doen. Ze worden bij ons op alle manieren gefaciliteerd om succesvol te zijn, want happy people make happy people. Daarom zie ik elke medewerker als mijn medewerker. Ik ben er dus niet alleen voor de leidinggevenden, maar voor iedereen die bij Hoffmann werkt. Ik zie het als mijn verantwoordelijkheid dat ze hier op een fijne en veilige manier kunnen werken. Bovendien: happy chicken lay more eggs."

"We vinden het belangrijk dat medewerkers zich kunnen ontwikkelen," vervolgt Martijn. "Wij leiden onze mensen op tot professionals. Dat maakt ze gewild in de markt. Het risico daarvan is dat medewerkers na een bepaalde periode vertrekken. Daar kan je moeilijk over doen, maar dat gebeurt nu eenmaal. Ik zie dat ook wel als een compliment voor de organisatie."

Waar krijgt Martijn energie van? “De meeste energie krijg ik van onderzoeken die er écht toe doen. Dat kunnen grote onderzoeken zijn, in bekende situaties met immense impact. Maar het kunnen ook onderzoeken zijn in een kleine organisatie waar we echt het verschil kunnen maken, zodat die organisatie na het onderzoek zelf verder kan.

> **“Innovatie betekent eigenlijk slimmere, betere en efficiëntere manieren vinden om de problemen van vandaag en morgen anders op te lossen.”**

Innovatie als oplossing én uitdaging
Innovatie richt zich volgens Martijn op preventieve oplossingen met een duidelijk doel en een kop en een staart. “Innovatie betekent eigenlijk slimmere, betere en efficiëntere manieren vinden om de problemen van vandaag en morgen anders op te lossen,” aldus Martijn. “Het kan worden ingezet als onderdeel van een securityoplossing, maar tegelijkertijd levert het nieuwe uitdagingen op.” Wat hem betreft is innovatie dus zowel een kans als een risico. Hij neemt ChatGPT als voorbeeld. “Deze AI-tool kan helpen bij het opstellen van een rapport, maar tegelijkertijd leveren we als mens wel in op ons lerend vermogen.

We vragen Martijn ook naar de definities van security en cybersecurity. Martijn: “Dat vind ik een lastige. Cybersecurity is tegenwoordig een modewoord, omdat we het hebben over digitale risico’s. We zien ook dat veel criminaliteitsvormen zijn gedigitaliseerd. Waar we het nu hebben over ransomware, noemden we dat vroeger afpersing. Alleen vindt de ‘moderne afpersing’ nu plaats via een digitaal middel op afstand. Dat is makkelijker uitvoeren, bovendien is de pakkans kleiner. En vroeger gingen betalingen met cash geld, nu via bitcoins, waardoor je als dader makkelijker uit beeld blijft. Kortom, ik denk dat het begrip security in de loop van de tijd is geëvolueerd. Door het over cyber te hebben snapt de markt wellicht wel waar je het over hebt.”

> **“De schade van cybercriminaliteit stijgt al jaren, zowel voor particulieren als voor het bedrijfsleven. Dit zal door verdere digitalisering alleen nog maar toenemen.”**

Bij Hoffmann zijn cyberincidenten aan de orde van de dag. Zijn medewerkers doen onderzoek naar de totstandkoming van incidenten en geven advies over preventieve oplossingen om dit soort zaken zoveel mogelijk te voorkomen. Maar reguliere IT-ontwikkelingen staan niet stil en veranderen continu. En daarmee zitten de Threat Actors ook niet stil. Het blijft een interessant domein voor criminelen om snel veel geld te verdienen. De schade van cybercriminaliteit stijgt dan ook al jaren, zowel voor particulieren als voor het bedrijfsleven. Dit zal door verdere digitalisering alleen nog maar toenemen. Voor de securitysector is het dan ook van essentieel belang om bij te blijven én te blijven investeren in ontwikkeling en innovatie.

> **"Innovatie blijft nu nog te beperkt tot nieuwe producten en diensten. Echte gamechangers heb ik de afgelopen jaren niet gezien. In feite doen we wat we al deden, alleen mooier en slimmer vermarkt."**

Als sector innoveren we nog onvoldoende, vindt Martijn. "We zijn een incidentgedreven sector. Dat zit in onze genen. We sporen incidenten op en willen slimme oplossingen leveren. Op sectorniveau zouden we absoluut beter kunnen en moeten innoveren. Innovatie blijft nu nog te beperkt tot nieuwe producten en diensten. Echte gamechangers heb ik de afgelopen jaren niet gezien. In feite doen we wat we al deden, alleen mooier en slimmer vermarkt."

"Daarnaast wordt op het gebied van innovatie veel gefocust op de technische kant van security, zoals technische maatregelen om incidenten te voorkomen" vervolgt Martijn. "Natuurlijk zijn technisch veilige producten belangrijk, evenals certificeringen die veilige systemen kunnen waarborgen. Maar er is meer. Bij een hack komt er vaak een technisch expert langs die onderzoekt en vertelt wat er technisch mis is gegaan. Maar wordt hiermee het lerend vermogen van de organisatie voldoende getriggerd? Als je dat doet, kan de mens juist een sterke schakel zijn in plaats van de zwakste. Organisaties betrekken de 'mens' nog te weinig in de aanpak, helaas."

Informatiedeling

Waar vroeger informatiedeling een issue was, gebeurt dat binnen de sector volgens Martijn nu wel meer. Als voorbeeld noemt hij het NCSC, van waaruit cyberdreigingen actief gedeeld worden met een bredere groep dan alleen de overheid. Vanuit de commerciële sector zit dat nog wat anders, volgens Martijn. "Het gaat dan vaak om meer commerciële of marketingacties gericht op naamsbekendheid. Partijen claimen het algemeen belang - de cyberveiligheid van Nederland - als doel te hebben, maar uit hun daden blijkt vaak alleen de focus op eigen of potentiële klanten."

Binnen de sector kan er volgens Martijn sneller geïnnoveerd worden als er gezamenlijkheid van partijen uitgaat. Volgens hem is daarbij een leidende rol weggelegd voor de overheid. Zo ziet Martijn voor zich dat de overheid innovatieprojecten stimuleert en bekostigt, met als voorwaarde dat de opgedane kennis binnen de overheid en de sector gedeeld wordt. Een andere oplossing zou zijn om de kosten voor deelname aan innovatieprojecten voor private partijen te verlagen. Dit kan bijvoorbeeld door de uren van private partijen (deels) te vergoeden. Zo is innovatie voor meerdere partijen toegankelijk en kunnen ook kleinere partijen een bijdrage leveren, zonder dat het ten koste gaat van hun eigen groei. Een bijbehorende uitdaging en vraag die Martijn hardop noemt is het tackelen van de onderlinge concurrentie: "Als je gaat samenwerken met andere bedrijven, ga je eigenlijk samenwerken met concurrenten. Toch wil je samen innoveren. Hoe kun je dit slim organiseren, zonder afbreuk te doen aan ieders positie in de markt?"

> **"Een firewall laat je ook niet configureren door een psycholoog. Waarom zouden IT'ers dan wel gekwalificeerd zijn om te adviseren over gedragsverandering?"**

Innoveren en groeien binnen Hoffmann

Terug naar Hoffmann. Hoe ziet hun groeistrategie eruit en wat zijn daarbij bepalende succesfactoren? Het antwoord van Martijn is duidelijk: "Het draait om een pragmatische - en uiteraard gestructureerde - aanpak van zaken. Dit gaat altijd gepaard met voldoende ruimte voor de teamleden om creatief te blijven. Zowel vanuit de theorie als de praktijk. Innovatie speelt daarbij een belangrijke rol en helpt ons bij het aanbieden van (maatwerk)diensten aan onze klanten. Wij onderscheiden ons met een leidende rol binnen het lopende onderzoek en het ontwikkelen van nieuwe diensten die betrekking hebben op de mens, de organisatie en de techniek. Ook participeren wij in lopende wetenschappelijke studies op het aspect van gedrag en cybersecurity."

"Wat ons betreft is de essentie van innovatie binnen security gericht op gedragsverandering. Bij de toetsing van de beveiliging van organisaties moet er aandacht zijn voor de fysieke wereld, de digitale wereld én de mens. Dit past ook bij het concept van Red Teaming."

Martijn legt dit begrip verder uit: "Bij Red Teaming pas je, in combinatie met bestaande aanvalstechnieken, de laatste aanvalstrends toe, op een manier waarop kwaadwillenden dat ook doen. Bijvoorbeeld door met stemvervorming en nummerspoofing personen te verleiden om hun inloggegevens af te geven. Als het gaat om menselijk gedrag wil je een duidelijk informatiebeveiligingsbeleid met draagvlak in de organisatie. Dit beleid moet door medewerkers ook daadwerkelijk uitgevoerd kunnen worden. Het is daarom belangrijk om inzicht te krijgen in de factoren die gewenst gedrag bevorderen en de factoren die dit juist in de weg staan. Het doel is dat organisaties met onze bevindingen aan de slag gaan. Bij Hoffmann hebben we hiervoor gedragswetenschappers in dienst. Een firewall laat je ook niet configureren door een psycholoog. Waarom zouden IT'ers dan wel gekwalificeerd zijn om gewenst gedrag te bevorderen?"

Bij een Red Teaming oefening van Hoffmann wordt dus altijd een realistisch scenario getest, waarbij gekeken wordt naar de techniek, architectuur, fysieke beveiliging en de factor 'mens'. Op die manier wordt duidelijk hoe alle maatregelen in samenhang met elkaar werken bij de klant. Martijn: "We stellen onszelf de volgende vragen: Kunnen wij onszelf toegang verschaffen tot systemen van organisaties? Kunnen we toegang krijgen tot het betalingsverkeer? Kunnen we ook doordringen tot in de serverruimte? Zijn we dan in staat om daar devices achter te laten waarmee we op afstand toegang kunnen krijgen tot de systemen? Als dat het geval is, is er werk aan de winkel. Voor ons is het vervolgens belangrijk om dit op zo'n manier te doen dat organisaties er zelf van leren. We zoeken dus naar manieren om iedereen mee te nemen in het project. Zo leggen we bijvoorbeeld met cartoons aan medewerkers uit hoe we toegang wisten te verkrijgen en wat de potentiële gevolgen hiervan kunnen zijn. We zien dat dit werkt. Na verloop van tijd wordt het door het delen van deze bevindingen voor ons steeds lastiger om door te dringen tot de organisatie.

Het is mooi om te zien hoe zo'n organisatie gedurende het project weerbaarder wordt. Dit is waar we het voor doen bij Hoffmann."

Om de integrale aanpak van Hoffmann te verduidelijken noemt Martijn het voorbeeld van medewerkers van Rotterdamse havenbedrijven, die werden opgepakt voor hun aandeel bij drugssmokkel. "We zien dat er nu gepleit wordt voor een speciale Haven VOG en een strengere screening van nieuwe medewerkers. Maar wat je mist is een goede analyse van wie kwetsbaar zijn in een organisatie en welke maatregelen je kunt nemen om deze kwetsbaarheid te verminderen. Ik denk bijvoorbeeld dat het slimmer is om financiële kwetsbaarheid in het personeelsbestand te monitoren. Onderzoek heeft uitgewezen dat de kans op financiële kwetsbaarheid na een scheiding erg groot is. Probeer dan bijvoorbeeld met medewerkers die zich in een scheiding bevinden preventief in gesprek te gaan en hen waar mogelijk te begeleiden, zodat hun kwetsbaarheid voor omkoping beperkt wordt."

Het antwoord op de vraag wat de uitdaging is voor Hoffmann als het gaat om groei en innovatie, is een voorspelbare. Ook bij Hoffmann is de zoektocht naar gekwalificeerde nieuwe collega's een uitdaging. Martijn: "We hebben een mooi bedrijf met gepassioneerde medewerkers die echt het verschil willen maken bij klanten. Teamleden vinden die daarbij goed aansluiten, blijft een uitdaging."

Een ander aandachtspunt voor Hoffmann is het houden van een continue focus op groeilijnen. "Maatwerk kan ervoor zorgen dat ontwikkeltrajecten niet de prioriteit krijgen die ze verdienen," vertelt Martijn. "Klanten gaan toch altijd voor." Toch kent juist ook standaardisatie van het werk ten opzichte van maatwerk een spanningsveld: "Ons uitgangspunt is dat wij vanuit kwaliteitsstandaarden als basis een vaste aanpak hanteren, waarbij we standaardisering zoveel mogelijk willen vermijden. Het leveren van maatwerk is ons bestaansrecht."

Hoewel Martijn van mening is dat de innovatiekracht binnen Hoffmann nog verbetering behoeft, is hij ook trots op bepaalde ontwikkelingen. Zo noemt hij het 3x3 model als voorbeeld. Dit hulpmiddel voor gedragsverandering is goed bruikbaar om oorzaken en oplossingen voor gedrag te identificeren en te implementeren. Met het model kun je met behulp van interviews doorvragen naar de oorzaken van bepaald gedrag van mensen en groepen binnen organisaties. Martijn noemt een voorbeeld: "Een medewerker kan bijvoorbeeld wel wéten dat een sterk wachtwoord belangrijk is, maar toch zijn geboortedatum gebruiken. De analyse van de oorzaken van dergelijk gedrag kan leiden tot het aanscherpen van de regels of maatregelen ter bevordering van gewenst gedrag. Zo voorkom je dat er te snel in oplossingen wordt gedacht, terwijl de analyse van de oorzaken van het ongewenste gedrag niet goed heeft plaatsgevonden."

Dit wetenschappelijk bewezen model onderscheidt vervolgens de oorzaken voor bepaald gedrag. Op de ene as staan motivatie (wil), capaciteit (kennis/vaardigheden) en gelegenheid (mogelijkheid om het gedrag ook te laten zien). Op de andere as staat weergeven wat je eraan kunt doen op het gebied van organisatie, mens en techniek. Op die manier genereert iedere gedraging minimaal negen maatregelen om de gewenste gedragsverandering in te zetten. Dit model werkt goed bij het duurzaam realiseren van gedragsverandering. Het resultaat? "Een veiligere omgeving, fysiek en digitaal. Awareness is goed, maar veilig gedrag is beter," aldus Martijn.

Trends
Zoals ieder interview sluiten we af met de vraag naar de te verwachten trends en ontwikkelingen in de komende vijf tot tien jaar. Martijn noemt drie onderdelen: AI, een versterking van de samenhang tussen digitale en fysieke veiligheid en de factor 'mens' die in veiligheid steeds belangrijker wordt.

> **''Als we meer incidenten gaan zien vanuit buitenlandse actoren, zoals Rusland, kan er weleens de trend ontstaan dat fysieke en digitale beveiliging in samenhang met elkaar worden beschouwd."**

Martijn verwacht dat AI meer en meer in staat zal zijn om (aanvals)scenario's uit te werken, teksten te laten schrijven en code te schrijven. Zowel aanvallers, cybersecurityspecialisten en grote softwareproducenten kunnen hier volgens Martijn hun voordeel mee doen.

Wat betreft de versterking van de samenhang tussen digitale en fysieke veiligheid zegt Martijn het volgende: "Organisaties in onder andere de energiesector zijn zich de laatste tijd meer bewust geworden van hun fysieke beveiligingsrisico's. Kijk bijvoorbeeld naar de windmolens op de Noordzee. Energiebedrijven realiseren zich nu dat de fysieke beveiligingsrisico's samenhangen met digitale risico's. Als we meer incidenten gaan zien vanuit buitenlandse actoren, zoals Rusland, kan er weleens de trend ontstaan dat fysieke en digitale beveiliging in samenhang met elkaar worden beschouwd. Tot nu toe zien we vooral een segmentering aan zowel de klantzijde als de leverancierszijde. Dat wil zeggen dat er een focus is van digitale partijen op digitale veiligheid en een focus van fysieke beveiligingspartijen op fysieke veiligheid. Daarnaast heb je nog Human Resources die zich richt op de mens."

Volgens Martijn wordt de combinatie in de markt nog niet echt gemaakt, terwijl die naar zijn mening steeds belangrijker wordt. "Ik zie dat bedrijven die veel met security van doen hebben, zoals banken, verzekeraars en vitale infrastructuur, hun maatregelen ook al integraal laten testen, al dan niet ingegeven door de TIBER-richtlijnen."

"Gartner schrijft in hun laatste rapport dat rond 2025 het tekort aan goed personeel mede de oorzaak zal zijn van de helft van alle cyberincidenten. De focus op het versterken van de mens als schakel wordt dus steeds belangrijker. Het belangrijkste is dat de medewerkers 'bewust bekwaam' gemaakt worden om op de juiste wijze te handelen. Laat dat nu net ons (Hoffmann) plan zijn," sluit Martijn zijn verhaal af.

“We geven én krijgen ruimte voor discomfort: nadenken over ideeën of vragen waarvan je niet weet of je ze meteen kunt realiseren.”

12. Christian Prickaerts
- Directeur van Fox Crypto

Christian Prickaerts, directeur van Fox Crypto, deelt de reis die hij heeft afgelegd: van zijn vroege fascinatie voor cybersecurity door de film WarGames tot aan zijn bijdrage aan succesvolle innovaties bij Fox-IT. Hij deelt zijn visie op innovatie – "het moet écht een probleem oplossen" – en duikt in belangrijke toekomstige marktontwikkelingen, zoals het gebruik van encryptie, toenemende juridisering en Multiparty Computation.

De vroege cybersecuritywereld

De vonk voor Christian's carrière in cybersecurity ontstond na het zien van de film WarGames uit 1983. De Amerikaanse sciencefictionfilm volgt het leven van een jonge videogame- en computerliefhebber die onbedoeld een militaire supercomputer hackt, wat leidt tot internationale chaos. De film was zijn tijd ver vooruit: vrijwel voor het eerst werd hacken gezien als een reële dreiging. Christian was geïntrigeerd door deze wereld en kocht al snel zijn eerste computer, de toen razend populaire Commodore 64.
Gedurende zijn middelbare school- en studietijd bleef Christian experimenteren met netwerken en computers. Hij bouwde thuis netwerken en kwam in aanraking met virussen en vroege hacking- en cracking-tools. Eén ding wist hij zeker: later in zijn werk wilde hij daar meer mee gaan doen. Hij begon zijn carrière bij de Universiteit Maastricht in de IT en zocht ondertussen naar online opleidingen om zijn kennis nog verder uit te breiden. "Ik kwam toen uit bij het SANS Instituut", vertelt Christian. "Daar heb ik mijn eerste cybersecurityopleidingen gevolgd. Deze waren ook erg goed toe te passen in de praktijk. Helaas was er binnen de universiteit nog weinig ruimte voor cybersecurity. Toen ben ik om me heen gaan kijken naar nieuwe kansen. Uiteindelijk belandde ik in 2005 bij het voor mij toen nog onbekende Fox-IT."

Roeping gevonden

Inmiddels heeft Christian al veel rollen vervuld binnen het bedrijf, waaronder de rol van forensisch IT-expert, trainer en directeur Managed Services. Momenteel is hij werkzaam als directeur van Fox Crypto. Hij heeft de verantwoordelijkheid over twee divisies: DetACT en Crypto. DetACT focust zich op fraude management en het detecteren van financiële fraude tijdens online betalingsprocessen. Crypto ontwikkelt hoogwaardige crypto-apparatuur om informatie te beschermen op het hoogste classificatieniveau, zowel voor de Nederlandse overheid als voor internationale markten.

Christian heeft zijn plek gevonden: "Er zijn zoveel aspecten van mijn werk waar ik energie van krijg. Ik deel heel graag mijn kennis en passie voor mijn vakgebied omdat ik er oprecht voldoening uit haal om organisaties en klanten te helpen navigeren door complexe vraagstukken. Het demystificeren van onderwerpen die vanaf een afstand complex lijken, maar in essentie helemaal niet zo ingewikkeld zijn. Dat is waar ik het voor doe. En vooral als de klant zich goed geholpen en geadviseerd voelt, dan heb ik mijn doel bereikt."

Wanneer een klant dankzij begeleiding de juiste beslissing kan nemen en efficiënt gebruik kan maken van hun tijd en middelen, is dit een bron van energie voor Christian. Dat geldt ook voor discussies met andere professionals, zoals juristen, die steeds meer betrokken

raken bij informatiebeveiliging en privacy. Het vinden van een balans tussen technisch correcte oplossingen en de context van wetgeving kan uitdagend zijn, maar het behalen van resultaten vindt Christian inspirerend. Ook wordt hij erg enthousiast van het zien van jonge mensen die zich ontwikkelen in het vakgebied en een rol van betekenis kunnen spelen. “Ik kan gerust zeggen dat security een passie van mij is. Ik ben er vol ingestapt en wist dat dit mijn roeping was.”

Experimenteren bij Fox-IT

“Fox-IT heeft altijd ruimte gegeven aan haar mensen om te experimenteren en te ontwikkelen, wat heeft bijgedragen aan hun innovatieve kracht”, stelt Christian. “Elke innovatie start bij de klantbehoefte. We geven én krijgen ruimte voor discomfort: nadenken over ideeën of vragen waarvan je niet weet of je ze meteen kunt realiseren. Probeer niet gelijk nee te zeggen. Overweeg of het verzoek van de klant mogelijk een behoefte in de markt weerspiegelt, zodat je eraan kunt gaan bouwen.”

Soms zeggen ze bij Fox-IT ook weleens ‘ja’ tegen projecten die commercieel gezien niet erg interessant zijn, maar waarbij de relevantie voor hun werk en de sector duidelijk is. Ze hebben bijvoorbeeld onlangs een project uitgevoerd voor de overheid waarbij ze de toepasbaarheid van een bepaald protocol in verband met quantum computing hebben onderzocht. Fox-IT heeft ermee ingestemd om de taak op zich te nemen en daarbij afgesproken dat de resultaten met de hele sector gedeeld worden. Dit heeft iedereen een stap vooruitgeholpen rondom quantum computing.

Christian stelt dan ook dat innovatie vooral moet bijdragen aan het oplossen van een probleem. “Het is belangrijk om actief na te denken over hoe dingen anders kunnen worden gedaan”, zegt hij. “Maar innoveren op zichzelf is geen doel. Het kan een middel zijn om te experimenteren, maar het moet uiteindelijk gericht zijn op het oplossen van een probleem. Ik zie innoveren dus als een andere manier om een bestaand of nieuw probleem op te lossen. Dat kan zijn in technologie, in de manier hoe je werkt, de samenstelling waarin je het doet. De mogelijkheden zijn wat dat betreft eindeloos.”

Ook is er samenwerking nodig om tot succesvolle innovaties te komen. “Je hebt mensen nodig met expertise, maar ook mensen die in staat zijn om zich op bepaalde momenten niet te laten beperken door bijvoorbeeld eerdere ervaringen, juridische kaders of regels”, legt Christian uit. En tot slot zijn er mensen nodig die het idee gaan uitwerken en bouwen, om te bevestigen of dat wat er is bedacht ook echt werkt.

Succesvolle innovaties: Dissect en DetACT™

Inmiddels is Christian als eindverantwoordelijke betrokken geweest bij verschillende succesvolle innovaties. Deze kwamen altijd voort uit een vraag of behoefte van een klant. Samen zijn ze vervolgens gaan uitzoeken of het mogelijk was om dit probleem op te lossen. Hij is het meest trots op Dissect, dat is ontstaan binnen een team waar hij destijds leiding aan gaf. Dissect is een tool die in een paar uur complete netwerken in kaart kan brengen. Snelheid is cruciaal bij geavanceerde aanvallen.

In de markt was er behoefte aan het snel kunnen handelen bij dreigingen of geavanceerde

aanvallen, zoals een ransomware-aanval. De bestaande tools waren niet toereikend, met name op het gebied van snelheid. Er moesten forensische kopieën gemaakt worden van een heel netwerk, en dat kostte veel tijd. Vooral bij grote netwerken duurde dat veel te lang om efficiënt onderzoek te kunnen doen. Dissect moest snel – in de eerste paar uur na een aanval – de benodigde data verzamelen.

Een groep getalenteerde ontwikkelaars heeft toen in enkele weken de eerste versie van deze tool gebouwd. Dat is nu, acht jaar later, uitgegroeid tot een tool die breed inzetbaar is en waarmee ze in korte tijd analyses kunnen uitvoeren tijdens grote incidenten. "Daar ben ik bijzonder trots op", benadrukt Christian. "Hoewel ik zelf geen code heb geschreven, heb ik er toch aan bijgedragen door altijd mensen de tijd te geven om eraan te werken en het te ontwikkelen."

Een andere innovatie waar Christian als eindverantwoordelijke betrokken bij is geweest is DetACT™, een oplossing voor fraudepreventie. Deze oplossing biedt financiële instellingen fraudedetectie, analysemogelijkheden en inzicht in het actuele dreigingslandschap. Ook deze innovatie kwam voort uit een vraag van een klant en is uiteindelijk in samenwerking met een klant tot stand gekomen.

"Banken kregen steeds vaker te maken met online fraude en waren dringend op zoek naar een oplossing. Één van onze klanten wilde hierover graag met ons in gesprek. Ze wisten dat we beschikken over deskundige mensen die inzicht hebben in beveiliging en dreigingsanalyse. Uiteindelijk hebben een aantal mensen van zowel de klant als Fox-IT een paar dagen bij elkaar gezeten. We hebben hen de tijd en ruimte gegeven om vrij te denken. Geen enkel idee was te slecht om op tafel te leggen. Het belangrijkste was om een veilige sfeer te creëren waarin iedereen alles kon zeggen. Dit vrije denken is echt iets waar ik voor sta. Al snel kwam daar dan ook DetACT™ uit voort."

> **"Als we de impact van technologie bijvoorbeeld zouden beoordelen op het voorkomen van maatschappelijke ontwrichting, hoe had de wereld er dan uitgezien?"**

Innovaties implementeren en evalueren

Christian vindt het belangrijk dat innovaties geïmplementeerd worden op een schaal die ertoe doet, naast dat het een specifiek probleem oplost. Daarmee maak je uiteindelijk het verschil. Hij noemt het voorbeeld van tweefactorauthenticatie. Geen nieuw concept, maar de toepassing ervan in recente betaaltransacties heeft een significant effect gehad op de beveiliging van deze processen. Het gebruiken van bestaande technologie in een nieuwe context kan dus een groot effect hebben. Ook dat is innovatie.

Volgens Christian komt het uiteindelijk neer op de vraag: Op welke schaal kijken we en wat is de context waarin we deze technologieën evalueren? Wat we belangrijk vinden – en dus hoe we technologie evalueren – bepaalt voor een groot deel welke innovaties er überhaupt

plaatsvinden. “Als we de impact van technologie bijvoorbeeld zouden beoordelen op het voorkomen van maatschappelijke ontwrichting, hoe had de wereld er dan uitgezien?” vraagt Christian. “Nu hebben we jarenlang geïnvesteerd in het vergroten van ons bewustzijn over dreigingen en de problemen die daarbij komen kijken. Daarmee hebben we diverse vitale processen en infrastructuren robuuster gemaakt. Onze keuzes en afwegingen beïnvloeden ontwikkeling.”

> **“Wat als alle partijen in Nederland, hypothetisch gezien, hun dreigingsinformatie en detectieregels samenbrengen in één database en iedereen put uit diezelfde bron? Dit zou cybercriminelen afschrikken, omdat het geen zin heeft om in Nederland je slag te slaan.”**

Samenwerken in de cybersecuritysector

Op het gebied van collectieve samenwerking in de sector ziet Christian nog kansen. Gemeenten werken steeds meer samen op het gebied van IT-security, in plaats van dat ieder het voor zich doet. Bijvoorbeeld via de VNG of als consortium van enkele gemeenten. “Is dat innovatie? Het leidt in ieder geval wel tot betere en efficiëntere beveiliging”, stelt hij.

Maar Christian vindt ook dat de sector als geheel beter kan samenwerken. “Wat als alle partijen in Nederland , hypothetisch gezien, hun dreigingsinformatie en detectieregels samenbrengen in één database en iedereen put uit diezelfde bron? Dit zou cybercriminelen afschrikken, omdat het geen zin heeft om in Nederland je slag te slaan. Alle partijen zitten immers op hetzelfde hoge beveiligingsniveau. Het nadeel? “Er wordt ook prijsgegeven wát we al weten. Maar het doel wordt wel bereikt: het belangrijkste is om de dreiging uit te schakelen, niet per se om de criminelen op te pakken.”

> **“Je ontwerpt vandaag iets zonder de inzichten van de toekomst, waardoor je het nooit helemaal toekomstbestendig kunt maken. Future flows cannot be countered.”**

Trends en marktontwikkelingen

Als we Christian vragen wat hij ziet als de belangrijkste trends in de markt op dit moment, noemt hij vier ontwikkelingen: AI, marktconsolidatie, verdere juridisering en het belang van encryptie.

Allereerst AI. “Dat is nu een gegeven”, zegt hij. “Het speelt al een tijdje een rol, maar nu is het zo alom aanwezig dat je er niet omheen kunt. Iedereen heeft zich inmiddels al afgevraagd wat AI eigenlijk echt doet en hoe het gebruikt kan worden.”

Ook verwacht Christian marktconsolidatie te zien rond een aantal platformen, oftewel het samenwerken of samenvoegen van partijen in de markt waardoor het totaal aantal aanbieders afneemt. Hij noemt het voorbeeld van Microsoft die een aantal jaar geleden de dienstverlening Managed Services heeft opgezet. Daarmee bieden ze een totaaloplossing. Christian denkt dat we dit ook in Nederland meer gaan zien, omdat de cybersecuritydienstverlening momenteel enorm versnipperd is. Afnemers weten dan niet goed waar ze uit moeten kiezen, en zullen eerder voor een totaaloplossing kiezen.

Daarnaast ziet Christian een tendens richting verdere juridisering. Hij denkt dat er als het ware een toegangsnorm moet zijn voor nieuwe en bestaande bedrijven in bepaalde sectoren. Fox-IT werkt bijvoorbeeld voor Defensie, en zij leggen de 'Algemene Beveiligingseisen Defensieopdrachten' op voor elk project. "Je moet continu aan het beveiligingsniveau van deze eisen voldoen", legt Christian uit. "En je moet eerst aantonen dat je eraan voldoet vóórdat je autorisatie krijgt om het project uit te voeren. Het toezicht is ook niet gebaseerd op incidenten. Ze bezoeken je regelmatig om te controleren of je nog steeds aan de eisen voldoet, niet alleen als er een incident is. En ik weet dat er nu ook gesprekken zijn bij de Rijksoverheid om iets soortgelijks op te zetten. Ik denk dat centrale regie hierin de sleutel tot succes is. Je wilt niet dat elke organisatie zijn eigen koers vaart, want dan breng je alleen maar onnodige complexiteit aan in het landschap."

En tot slot ziet Christian het belang van encryptie de komende jaren toenemen. "Je kunt de systemen niet volledig beschermen, je moet de data zelf beschermen. Systemen zullen altijd kwetsbaar blijven, want ze zijn gebaseerd op een reeks instructies, geschreven door mensen of machines. Je ontwerpt vandaag iets zonder de inzichten van de toekomst, waardoor je het nooit helemaal toekomstbestendig kunt maken. Future flows cannot be countered. En een andere ontwikkeling binnen de cryptografie die nog meer zal worden toegepast is Multiparty Computation." Dit stelt meerdere partijen in staat om gezamenlijk gegevens te verwerken, zonder deze met elkaar te delen.

Een veiligere samenleving

Christian sluit zijn interview af met een terugblik op de afgelopen jaren. Hij is heel trots op wat hij en de mensen om hem heen bereikt hebben. In de afgelopen twintig jaar hebben ze de organisatie uitgebouwd van dertig naar 450 medewerkers, die zich allemaal inzetten voor een veiligere samenleving. "Maar het gaat niet alleen om onze organisatie. In 20 jaar zijn ook verschillende mensen doorgestroomd naar andere bedrijven, of ze zijn nu bijvoorbeeld klant bij ons. Dus het is niet alleen de inzet van de mensen die nu bij ons werken waar ik trots op ben, maar ook op iedereen die in de loop der jaren heeft bijgedragen en uiteindelijk zijn of haar eigen weg is gegaan. Iedereen werkt namelijk aan hetzelfde, gezamenlijke doel: Nederland een stukje veiliger maken."

"Er zijn drie dingen belangrijk als je als start-up succesvol wilt innoveren in het securitydomein: validatie, ecosystemen en ondernemerschap."

13. Menno Stijl
- Venture builder in de security industrie

Menno Stijl, venture builder in de securityindustrie, maakte het authenticatieplatform Authasas groot en verkocht deze aan MicroFocus. Nu begeleidt hij start-ups en scale-ups in het securitydomein met hun reis naar succes. Waar lopen deze kleinere partijen tegenaan? En hoe kunnen we hier als sector oplossingen voor bieden? Menno ziet een belangrijke rol weggelegd voor het 'stewardship model', om met innovaties meer te focussen op maatschappelijke relevantie.

De eerste openbare authenticatiemethode van Nederland

Menno is wat ze noemen een echte 'Delftenaar'. Hij heeft Elektrotechniek gestudeerd en later ook bedrijfskunde. Dat was op het moment dat de I en de CT werden geïntegreerd met elkaar, dus dat de computers en de netwerken digitaal gingen samenwerken. Hij zette al vroeg de stap naar het securitydomein. Een project in 1995 bij de Belastingdienst bleek het startschot. Hij vertelt: "Het project heette Elektronische Aangifte Particulieren, hoewel wij het 'belasting-diskette' noemden. Nu zijn alle aangiftes digitaal, maar dat was toen nog helemaal niet gebruikelijk. Het doel van het project was om mensen aangifte te laten doen met een diskette, die dan opgestuurd kon worden."

Menno legt uit dat één van de problemen die ze daarvoor moesten oplossen was om aangiftes van elkaar te kunnen onderscheiden. "Hoe kon je weten wat jouw aangifte was? Er waren geen authenticatiemiddelen openbaar. Natuurlijk was er wel een wachtwoordbeleid voor bedrijven, maar nooit voor grote groepen gebruikers. Dus hebben we zelf iets bedacht: de aangiftecode." Menno legt uit dat je daarvoor een papiertje moest ondertekenen en vijf cijfers moest kiezen. Niet vier cijfers, want de pincode van de bank was al vier cijfers. "Zo plat was het in die tijd. En dan moest je aangifte doen op je diskette, die je vervolgens opstuurde naar de Belastingdienst. Dat was waarschijnlijk de eerste openbare authenticatiemethode van Nederland. Daar ben ik nog steeds trots op!"

In het eerste jaar kregen ze 400.000 elektronische aangiftes op die manier binnen, vrijwel zonder problemen. "We hadden ons ontzettend goed voorbereid. Want wat doen we als de Telegraaf zegt dat het een zooitje is? We hebben al die communicatie van tevoren uitgekauwd, maar het is prima verlopen. Dat was eigenlijk de start van mijn reis in de authenticatiewereld."

> **"In de praktijk zie je dat partijen te snel nieuwe producten maken en een 'Minimum Viable Product' op de markt brengen, en dit vervolgens onvoldoende valideren. Daar gaat het mis."**

Succesvol innoveren in het securitydomein

Na wat tussenstappen startte Menno met een compagnon het bedrijf Authasas: Authentication as a Service. Dat werd een groot succes en uiteindelijk verkochten ze het aan

Microfocus, toen een van de grotere gebruikers van het platform.

“Sinds ik geen vast werk meer heb doe ik projecten die ik interessant en leuk vind. Ik help bijvoorbeeld met ventures, start-ups, scale-ups en ook initiatieven binnen bedrijven. Eigenlijk alle dingen die innovatief zijn. Soms word ik tijdelijk de CEO van het bedrijf of ik ben de kartrekker van een nieuw initiatief. Dat soort rollen speel ik dan een tijdje totdat de opschaling is begonnen”, vertelt Menno.

Door bij zoveel verschillende projecten betrokken te zijn heeft Menno veel geleerd over succesvolle innovaties. Hij brengt digitale innovatie naar het business domein: bruggen slaan tussen business en ICT dus. Volgens hem zijn drie dingen belangrijk als je als start-up succesvol wilt innoveren in het securitydomein: validatie, ecosystemen en ondernemerschap.

> **“Veel innovatieve mensen zijn technisch sterk, maar niet ondernemend. Ze zijn productgedreven en kijken minder naar de markt en de bedrijfskundige aspecten. Enkel een goed idee is daarom geen garantie voor succes.“**

Validatie, ecosystemen en ondernemerschap
Menno verduidelijkt dat het bij validatie gaat om het beantwoorden van twee vragen. “Je wilt weten: Wat vindt de klant ervan? En hoeveel geld heeft de klant ervoor over? In de praktijk zie je dat partijen te snel nieuwe producten maken en een ‘Minimum Viable Product’ op de markt brengen, en dit vervolgens onvoldoende valideren. Daar gaat het mis.”

Het tweede punt om tot succesvolle innovaties te komen is het ecosysteem, volgens Menno. “Innovatie bestaat vaak uit deeltjes in een keten. Neem biometrie als voorbeeld: je kan biometrie toepassen, maar het hoort in een omgeving waar je ook autorisatie uitgeeft en waar je dingen beveiligt. Dus je moet de hele keten snappen voordat je innovatie succesvol kunt maken.” En een goed ecosysteem creëert ook een geschikte omgeving om in te kunnen innoveren. “Als je bijvoorbeeld wilt valideren of een innovatie werkt, dan moet je samen kunnen werken met een bevriende partij die kan zeggen: ‘Het werkt niet, maar ik zal het niet meteen aan de grote klok hangen.’ En het ecosysteem helpt ook bij het realiseren van funding.”

Tot slot noemt Menno het belang van goed ondernemerschap: “Ondernemers moeten ook echt óndernemend zijn. Veel innovatieve mensen zijn technisch sterk, maar niet ondernemend. Ze zijn productgedreven en kijken minder naar de markt en de bedrijfskundige aspecten. Denk hierbij aan zaken als: hoe ga je om met je financiën? Hoe zorg je voor effectief people management? Enkel een goed idee is daarom geen garantie voor succes.”

Lean startup methode

Menno legt uit dat start-ups altijd drie belangrijke fasen doorlopen. “Fase één: het bouwen van de MVP, een Minimal Viable Product. In die fase heb je iets gemaakt wat werkt. De tweede fase gaat over het laten toetsen van de MVP bij bevriende partijen binnen het ecosysteem. Tegelijkertijd blijf je de MVP verbeteren en toets je of het business model klopt. In fase drie start het opschalen, dan moet je gaan standaardiseren en de backoffice gaan regelen. Een cruciale fase.”

Menno noemt een voorbeeld van zijn bedrijf Authasas. Ze hadden veel Europese klanten en een aantal Amerikaanse klanten. De support desk zat in de buurt van Sint-Petersburg in Rusland, tijdens kantooruren. “Op een gegeven moment kregen we een klant in Australië en die wilde ook support. Maar dan wel tijdens hún kantooruren”, vertelt Menno. “In één keer moesten we naar 24/7 bereikbaarheid. Dat verzin je allemaal niet van tevoren, maar daar moet je wel over nadenken. Dus ik raad start-ups vaak aan om in Nederland of Europa te beginnen, waardoor je dat soort dingen voor je uit kunt schuiven.”

> **“Cybersecurity is iets wat ons overkomt, net als de weersinvloeden in de dertiende eeuw. Dan kwam er een storm en liep ons land onder. Ik zie dat nu ook gebeuren bij security. Dat maakt innovatie ook zo moeilijk, want je weet nooit wanneer de storm komt.”**

Innovatie moet zorgen voor verbetering

We vragen Menno naar zijn visie op innovatie, en dan specifiek in de securitysector. Menno gebruikt liever het woord weerbaarheid in plaats van security, “want dat is breder”, stelt hij. “Met zijn allen zijn we weerbaar. Ik zie dat security, en met name cybersecurity, iets is wat ons overkomt, net als de weersinvloeden in de dertiende eeuw bijvoorbeeld. Dan kwam er een storm en liep ons land onder. Ik zie dat ook gebeuren bij security. Dat maakt innovatie ook zo moeilijk, want je weet nooit wanneer de storm komt, je weet alleen dát die komt. In security maken we vooral veel pleisters of we zijn veel aan het pompen, maar we zijn niet bezig met het bouwen van dijken.”

Menno stelt dat we dan dus niet écht innovatief bezig zijn. Innovatie is voor hem verbeteren. Hij heeft veel te maken gehad met technische innovaties, maar ziet ook steeds meer het belang van verbetering voor bedrijven of de samenleving als geheel. “Innovatie zou moeten gaan over dingen die echt iets betekenen. Anders krijg je van die techneuten die zomaar iets bedenken. Dat is wel leuk, maar daar zitten ook consequenties aan vast. Bijvoorbeeld dat zo’n Facebook-jongen iets bedenkt om vrouwen te versieren en inmiddels is het uitgegroeid tot het grootste netwerk in de wereld. Terwijl hij in eerste instantie nooit over security heeft nagedacht, alleen maar over dat het leuk is om met elkaar te kunnen chatten en elkaar te kennen. En vervolgens ook nog eens onze data ‘gebruiken’ om nog meer geld te verdienen.” Menno vindt dat een typisch voorbeeld van een technische innovatie die onvoldoende is doorontwikkeld: “Je kunt het geen echte maatschappelijke innovatie noemen. Mensen raken verslaafd aan het gebruik en management en aandeelhouders lachen zich een kriek. Het is volledig uit de hand gelopen.”

Geen balans in de markt

Menno legt uit dat de markt soms te ver is doorgeschoten, waardoor de balans ontbreekt. "IT levert ons als samenleving een probleem op, waar we niet om gevraagd hebben. Ik zal een voorbeeld geven. Stel, je koopt een laptop. Die heb je voor je staan en je krijgt er meteen een probleem bij, wat je eigenlijk niet besteld hebt. Voor je het weet heb je namelijk een virus te pakken of word je gehackt of gegijzeld. Vergelijk dat met een auto kopen. Daar zitten al veiligheidsdingen en certificaten overheen. Het is niet zo dat de auto meteen uit de eerste bocht vliegt die je tegenkomt. Die proactieve kant van security of weerbaarheid is helemaal niet goed ingericht, en daar is nog veel winst te behalen."

Tot slot haalt hij ook het voorbeeld van Facebook aan. "De gebruikersregels van Facebook zijn tweeëntwintig kantjes, uitgewerkt door honderden juristen. Ik zit dat dan vervolgens in mijn eentje door te nemen met één uurtje rechten dat ik vroeger tijdens mijn studie heb gehad. Er is geen balans meer. Er is geen kracht die mij helpt." Menno vertelt dat dit met name geldt voor de IT-wereld omdat alles zó snel verandert. "Met langzame veranderingen kan de overheid natuurlijk ingrijpen. Daar zijn wetten en regels voor. Maar de IT gaat zo vreselijk snel, dat de overheid het gewoon niet meer kan bijhouden met de snelheid waarin zij regels maken. Als iemand een miljoen ransom vraagt aan een ziekenhuis, betalen wij het met z'n allen. Niemand roept van: 'Wat gek eigenlijk!' Dat wordt nu gelukkig in Europa een beetje ingehaald door regels en wetten vanuit de EU."

Kleine partijen staan er te veel alleen voor

Dat de balans in de markt is doorgeschoten, ziet Menno ook terug bij kleinere ondernemers. Grote bedrijven zijn in staat om hun eigen IT-beveiliging te organiseren, maar het mkb of de zzp'er loopt al snel tegen moeilijkheden aan. "Mijn zoon is fysiotherapeut en heeft samen met partners een eigen bedrijf. Hij heeft dan ook een IT-leverancier. Maar hoe weet hij nou of die IT-leverancier het goed doet? Zijn hele elektronisch patiëntendossier staat daar, met alle patiëntgegevens. Stel dat er nu iets mee gebeurt, waar heeft hij dan recht op?" Menno vindt dat kleinere partijen er te veel alleen voor staan. "En dat terwijl we met een aantal simpele aanpassingen de dijk hoger kunnen maken voor een grote groep gebruikers die er nu alleen voor staan. We moeten tot een model komen waarin we dit kunnen organiseren, met z'n allen een soort waterschappen en dijkbewaking organiseren voor digitale weerbaarheid."

> **"Ik ben een voorstander van het 'stewardship'-model, ook wel het rentmeesterschapsmodel genoemd. Winst kan wel, maar proportioneel."**

Stewardship als oplossing

In zijn werk als start-up begeleider hoorde Menno laatst over een scale-up die meer dan tien miljoen aan funding had opgehaald. Maar over een paar jaar moeten ze wel zestig miljoen opleveren voor een investeerder. "En dat ten koste van verbeteringen en innovatie, en daarmee op lange termijn dus ook van hun klanten", zegt Menno. "Dat model is gewoon zo slecht voor innovatie, daar kan je het bijna niet mee doen. Ik ben een voorstander van het 'stewardship'-model, ook wel het rentmeesterschapsmodel genoemd." Menno

vertelt dat dit een concept is binnen het bedrijfsleven dat zich richt op het beheer en de verantwoordelijkheid van een organisatie ten opzichte van haar belanghebbenden. Het model legt de nadruk op het creëren van langetermijnwaarde en duurzaamheid, in plaats van met name te streven naar kortetermijnwinst. Winst kan wel, maar proportioneel.

"Je gaat dan meer werken vanuit een purpose", verduidelijkt Menno. "In ons geval: de wereld veiliger maken. Er zijn bedrijven die dit model succesvol hebben toegepast. Bosch wordt bijvoorbeeld voor het grootste gedeelte bestuurd door een stichting, waar een groep stewards maximaal vijf jaar zorg mogen dragen voor de koers van het bedrijf. Winst komt voor een deel bij goede doelen terecht. Hierdoor heeft Bosch naast vierhonderdduizend medewerkers ook een ziekenhuis en doen ze diverse onderwijsprojecten over de hele wereld. Zeiss, van de cameralenzen en brillen, heeft ook een vergelijkbaar model. Net als Carlsberg, de bierbrouwer uit Denemarken. Carlsberg zet zich vooral in om het dividend van het bedrijf ten goede te laten komen aan iets wat relevant is voor de samenleving."

Maatschappelijke relevantie prioriteren

Menno hoopt dat het stewardship-model geprioriteerd wordt door de overheid en het bedrijfsleven richting de toekomst. "Dat is wel lastig. Het is ook geen ultieme oplossing. Kijk bijvoorbeeld naar wat er met OpenAI gebeurt. Sam Altman is OpenAI begonnen als 'open'; het heet niet voor niets zo. Op een bepaald moment heeft hij toch gezegd: 'Ik krijg te weinig funding, dus ik heb er maar een commercieel bedrijf naast gezet.' Dat bedrijf heeft vervolgens tien miljard van Microsoft gekregen. Het is verdomd moeilijk om dan niet gewoon te kiezen voor die privéjet of die boot, in plaats van bij je ding te blijven en wat meer te lijden."

Volgens Menno zou de overheid een rol kunnen spelen om het stewardship model aantrekkelijker te maken. "Misschien is dat wel mijn droom. Dat de overheid zegt bij Europese tenders: steward-owned bedrijven gaan voor. Dat zou ik zó mooi vinden." Hij vindt het interessant dat in het securitydomein, waar het toch echt gaat om maatschappelijke relevantie, een dergelijk model nog niet bestaat." De dreiging wordt alleen maar groter en met name de mkb'er staat alleen. En dat terwijl we wel de expertise in Nederland hebben om er iets aan te doen. Niet alleen voor Nederland, maar ook voor Europa. Binnen de sector zijn we nog niet bezig met dijken bouwen, maar te veel bezig met uitleggen dat er meer water aan komt. Het deltaplan ontbreekt."

Trends

Een van de opvallendste ontwikkelingen in de markt vindt Menno de groeiende afhankelijkheid van service providers. "Organisaties besteden steeds meer taken uit aan externe partijen, waardoor de ketenafhankelijkheid toeneemt", stelt hij. Dit brengt zowel voordelen als risico's met zich mee. Menno benadrukt dat het essentieel is dat service providers zich bewust zijn van hun verantwoordelijkheid op het gebied van beveiliging.

Een andere zorgwekkende trend die Menno ziet is de combinatie van kunstmatige intelligentie (AI) en beveiliging. "Je kunt AI prima gebruiken om bestaande bedreigingen vast te stellen en snel met alle betrokkenen van de 'dijkbewaking' te delen. Hij benadrukt dat de combinatie van AI en security gevaarlijk kan zijn, tenzij we deze technologieën inzetten voor positieve doeleinden. Om dit te bereiken, pleit hij voor een gezamenlijke coalitie en samenwerking. "Alleen samen kun je weerbaar zijn", sluit hij af.

“Er wordt te weinig naar het maatschappelijk rendement op investeringen gekeken.”

14. Lara Hemstede
- Founder van Cyber Proof & Rise App

Lara Hemstede, oprichter van Cyber Proof en Rise App, heeft zelf ervaren hoe het is om slachtoffer te worden van cybercriminaliteit en digitaal geweld, wat haar de motivatie gaf om andere slachtoffers te helpen. Dit leidde onder andere tot de ontwikkeling van een app waarmee slachtoffers van digitale dreigingen bewijs kunnen verzamelen en een juridisch dossier kunnen opbouwen. Ondanks het vertrouwen en de steun van uiteenlopende partijen blijkt het verkrijgen van structurele financiering een uitdaging. In haar bijdrage deelt Lara haar visie op manieren om de innovatiekracht in Nederland te vergroten, waaronder het bevorderen van effectievere publiek-private samenwerkingen, een centrale innovatiehub, en meer financiering vanuit de overheid.

Slachtoffer van cybercriminaliteit en digitaal geweld

Lara belandde niet zonder reden in de wereld van cybersecurity. Ze werd jaren geleden slachtoffer van huiselijk geweld en werd vervolgens geconfronteerd met hacking, stalking, bedreigingen en afpersing. “Een levensingrijpende ervaring met verstrekkende gevolgen”, vertelt ze. Ze besloot aangifte te doen bij de politie. “Ik moest met terugwerkende kracht een dossier opbouwen, maar je bent getraumatiseerd, zit midden in het geweld en moet tegelijkertijd digitaal bewijs verzamelen. Een haast onmogelijke opgave. Vragen over mijn digitale veiligheid bleven onbeantwoord. Hulp bleek onbetaalbaar en online informatie was verspreid en versnipperd. Waar kon ik terecht? En wat moest ik doen?”

Tijdens het aangifteproces besefte ze: dit moet en kan anders. Niet voor haarzelf, dat was helaas te laat. Maar wel voor toekomstige slachtoffers. “Ik nam me voor anderen te helpen die in een vergelijkbare situatie zaten.” Na verschillende studies op het gebied van cybersecurity en digitaal onderzoek, en met een recherchevergunning op zak, richtte ze in 2016 haar bedrijf Cyber Proof op.

Cyber Proof biedt trainingen en lezingen aan organisaties, instanties en individuen om cybercriminaliteit te voorkomen. “Preventie is de eerste en meest effectieve stap tegen cybercrime,” legt Lara uit. “Onze trainingen en lezingen dragen bij aan bewustwording. Door de juiste maatregelen te nemen kun je het risico aanzienlijk verminderen en cybercriminelen minder kans geven.” Daarnaast is Lara betrokken bij verschillende non-profit initiatieven, test ze als “fysieke hacker” de beveiliging van bedrijven en heeft ze de ontwikkeling van de Rise App geïnitieerd.

Rise App

Deze app is ontworpen om slachtoffers van huiselijk en online geweld, zoals stalking en bedreiging op een laagdrempelige manier te ondersteunen bij het verzamelen van digitaal bewijs en het opbouwen van een gedegen dossier. Daarnaast wordt er zorgvuldig aandacht besteed aan de integriteit van de verzamelde gegevens, om eventuele discussies tijdens juridische procedures te voorkomen. Het verzamelde bewijs kan vervolgens veilig en eenvoudig worden gedeeld met relevante instanties, zoals de politie en hulpverleningsorganisaties. “Dit resulteert in een volledig en goed georganiseerd dossier dat voldoet aan de wensen, procedures en eisen van zowel de politie als het Openbaar Ministerie, wat de efficiëntie voor deze partijen aanzienlijk verhoogt.”

> **"De emotionele, psychologische en financiële impact die cybercriminaliteit heeft op slachtoffers is vaak enorm."**

Kwetsbaarheid in het digitale tijdperk

Lara wijst erop dat bij bijna alle interpersoonlijke problemen tegenwoordig een digitaal component aanwezig is. Ze illustreert dit met hedendaagse voorbeelden: "Vroeger moest je iemand fysiek volgen om hun locatie te achterhalen of om iemand te bespieden, maar tegenwoordig kunnen daders eenvoudig spyware of stalkerware op iemands telefoon installeren. Deze software biedt hen toegang tot communicatie-apps zoals WhatsApp en sms-berichten. Hierdoor kunnen ze bijvoorbeeld foto's en video's bekijken. Stalkerware houdt zelfs continu je locatiegegevens bij. Er zijn zelfs varianten waarmee een aanvaller op afstand de microfoon en camera van je telefoon kan activeren, waardoor ze ongemerkt gesprekken kunnen afluisteren of zelfs zien wat je op dat moment aan het doen bent", legt Lara uit.

Wat zorgwekkend is, volgens Lara, is dat dergelijke software vaak op laagdrempelige wijze wordt aangeboden, bijvoorbeeld aan ouders om hun kinderen te monitoren. "Helaas worden deze apps ook misbruikt door jaloerse partners en andere kwaadwillenden. Dit onderstreept dat onze digitale kwetsbaarheid vaak onderschat wordt."

Ze benadrukt ook dat cybercrime en digitale dreigingen tegenwoordig heel eenvoudig zijn geworden. "Met soms slechts een paar klikken kunnen kwaadwillenden toegang krijgen tot persoonlijke informatie en deze tegen je gebruiken. Denk aan het hacken van e-mailaccounts, het stelen van vertrouwelijke data, identiteitsfraude of het verspreiden van gevoelige privé-informatie. Het is verontrustend hoe makkelijk het is om slachtoffers online lastig te vallen en schade aan te richten. De emotionele, psychologische en financiële impact die cybercriminaliteit heeft op slachtoffers is vaak enorm en kan in het ergste geval het leven compleet ontwrichten."

Dit bevestigt volgens Lara het belang van preventie en bewustwording. Ze wijst erop dat wanneer mensen eenmaal slachtoffer zijn geworden, het vinden van hulp een uitdaging kan zijn, helemaal wanneer slachtoffers beperkte technische kennis hebben. "Dit maakt het makkelijk vinden van de juiste hulp des te belangrijker", benadrukt ze.

> **"Voor slachtoffers van cybercrime is het vaak een immense uitdaging om betrouwbare hulp te vinden."**

Platform voor concrete hulp bij cybercrime en digitaal geweld

Lara maakt zich al jaren hard voor de ontwikkeling van een centraal en allesomvattend platform om de toegang tot hulp voor slachtoffers van digitaal geweld en online criminaliteit te vergemakkelijken, waarbij de Rise App een onderdeel zal zijn. Ze legt uit: "Dit platform is bedoeld om mensen te ondersteunen die te maken krijgen met zaken als stalking,

bedreiging, wraakporno, afpersing, hacking, spyware, stalkerware, online oplichting, identiteitsfraude, GPS-tracking of vermoedens van afluisterpraktijken en opnames. Voor deze slachtoffers is het vaak een immense uitdaging om betrouwbare hulp te vinden."

Het platform heeft tot doel slachtoffers gemakkelijk toegang te bieden tot informatie, expertise en praktische tools, waaronder de Rise App. Naast de focus op preventie, is er ook aandacht voor wat te doen als je slachtoffer bent van cybercriminaliteit of digitaal geweld. Lara licht toe: "Het platform zou naast informatie een scala aan dienstverleners moeten aanbieden, zoals particuliere onderzoekers, telefonische hulplijnen, real time chat ondersteuning, digitaal en forensisch onderzoekers, ethische hackers, juridische bijstand, hulpverleners, en nog veel meer. Deze holistische benadering maakt concrete hulp, gerechtigheid en innerlijke rust voor slachtoffers toegankelijker. Ook moeten er oplossingen komen voor slachtoffers met beperkte financiële middelen, zodat hulp voor iedereen toegankelijk wordt. Hier zie ik een rol voor de overheid weggelegd."

Hoewel Lara veel steun en betrokkenheid heeft gekregen van verschillende partijen, is het haar nog niet gelukt om structurele financiering te verkrijgen voor de voortzetting van de Rise App en het platform. "Na zes jaar keihard werken en met de finishlijn in zicht, heb ik noodgedwongen moeten besluiten om voorlopig de ontwikkeling van de app en het platform stop te zetten. Wat moeilijk te verteren is, want de app en het platform zijn broodnodig, vooral gezien de groeiende problematiek van cybercrime en digitaal geweld evenals het toenemende aantal slachtoffers."

Van ervaringsdeskundige tot social tech innovator

Lara kijkt terug op een reis van ervaringsdeskundige naar social tech innovator. Een bijzonder moment was toen ze de vereisten, ofwel 'requirements', wist op te halen bij belangrijke samenwerkingspartners, zoals de politie, het Openbaar Ministerie, Veilig Thuis en de gemeente Rotterdam. Het feit dat ze, als ervaringsdeskundige, het vertrouwen en de steun kreeg voor haar burgerinitiatief, zowel op regionaal als landelijk niveau, heeft heel veel voor haar betekend.

Een ander belangrijk en onvergetelijk moment was de interesse van de Britse overheid in de Rise App. Lara licht toe: "Via de International Director Public Safety van Accenture - één van de partijen die Rise pro bono heeft bijgestaan - ontving ik een vraagstuk van de Britse overheid: *Can technology be used to capture the victim experience and ensure that victims do not have to repeat their story to different support services and throughout their journey through the criminal justice process?* Rise bleek hét antwoord te zijn op dit vraagstuk. "Eeuwig zonde natuurlijk dat ik dit momentum heb gemist, omdat de Rise App nog niet operationeel is."

Verder waren de subsidies van het SIDN Fonds en Fonds Slachtofferhulp, samen met de pro bono hulp van de top van het bedrijfsleven, de advocatuur, CTO's en andere partners, cruciale mijlpalen op haar pad. "De reis van de Rise App was niet altijd even makkelijk, maar gelukkig waren er ook vele hoogtepunten."

> **"Veelbelovende sociale initiatieven op het gebied van cybercriminaliteit en digitaal geweld voor burgers lopen regelmatig vast."**

Maatschappelijke les; verbetering van publiek-private samenwerking

Lara pleit voor een effectievere samenwerking tussen publieke en private partijen om innovaties succesvol te ontwikkelen en implementeren. Ze benadrukt het belang van een centraal coördinatiepunt binnen de overheid om dergelijke initiatieven te faciliteren. Een voorbeeld hiervan zou een innovatiehub kunnen zijn, waar zowel publieke als private partners samenkomen, samenwerken en kennis delen. Deze hub zou op regionaal en nationaal niveau opereren, met snelle toegang tot financiering om sociale initiatieven te ondersteunen. Daarnaast benadrukt Lara dat er dringend behoefte is aan meer financiële steun voor preventie, bewustwording en slachtofferhulp. Ze constateert dat ze regelmatig veelbelovende sociale initiatieven op het gebied van cybercriminaliteit en digitaal geweld voor burgers ziet vastlopen.

Lara wijst erop dat de Rise App al veel eerder operationeel zou zijn geweest, als er vanaf het begin voldoende kapitaal en menskracht beschikbaar waren geweest. "Zonder de druk van een verdienmodel en inkomsten. Er is nu ook doorgaans geen ruimte om founders van sociale innovaties uit te betalen, bijvoorbeeld. Als je hier financiering voor beschikbaar stelt, dan neemt je innovatiekracht toe."

Ze merkt ook op dat er te weinig aandacht wordt besteed aan het maatschappelijke rendement van investeringen. Ondanks de duidelijke behoefte aan de Rise App en het ontbreken aan alternatieven, lukte het niet om voldoende funding op te halen. En dat terwijl de besparingen die je realiseert veel groter zijn dan de initiële investering. Zoals het voorkomen van slachtofferschap, snellere hulpverlening en juridische procedures en het verbeteren van de efficiëntie voor de politie en hulpverleningsinstanties.

Hoewel er bereidheid is voor verandering, ondervindt Lara in de praktijk vaak obstakels. Ze wijst op de uitdagingen binnen de soms bureaucratische overheidsstructuur en het gebrek aan eigenaarschap bij de overheid, wat moeilijkheden kan veroorzaken bij het tot stand brengen van initiatieven, zoals ook het geval bij de Rise App.

Doorzettingsvermogen en innovatie

Omdat er binnen subsidies vaak geen ruimte is om oprichters van sociale innovaties te vergoeden, leidde dit boven op de COVID-crisis voor Lara tot ernstige financiële problemen. Deze uitdagingen trokken een zware wissel op haar fysieke en mentale gezondheid, wat uiteindelijk resulteerde in een periode van bijna een jaar van herstel en reflectie.

Inmiddels staat Lara weer regelmatig met hernieuwde energie en een diepere kijk op haar missie voor groepen, waar ze workshops en lezingen verzorgt over digitale veiligheid. Dit keer niet meer als slachtoffer, maar als iemand met de ervaring en deskundigheid om anderen het haar zo bekende leed te besparen.

“Omdenken, een open blik en creatieve input van buiten de sector is nodig voor innovatie.”

15. Anouk Vos
- Mede-oprichter van Revnext

Anouk Vos, mede-oprichter van Revnext, duikt graag in het oplossen van complexe, strategische vraagstukken. Ook zet ze zich in voor jong talent met de Cyberworkplace, een non-profit school voor ethisch hacktalent. De innovatiestrategie van Revnext draait dan ook om het binnenhalen én -houden van jonge talenten. Richting de toekomst ziet Anouk de samenwerking tussen de overheid en het bedrijfsleven als cruciaal. Ze vraagt zich af: hoe gaan we de verantwoordelijkheden voor cybersecurity inrichten?

Veiligheidsdiplomaat in spe

Vanaf jonge leeftijd was Anouk al geïntrigeerd door veiligheidsvraagstukken. Ze ging internationale betrekkingen studeren met de overtuiging om diplomaat te worden. “Ik heb zelfs een programma op de Koninklijke Militaire Academie gevolgd en gewerkt in Kosovo en Servië, omdat ik het liefst veiligheidsdiplomaat wilde worden”, vertelt ze. “Dus toen ik de kans kreeg om stage te lopen bij het ministerie van Buitenlandse Zaken, heb ik me direct aangemeld. Na mijn stage ben ik in dienst getreden bij de Directie Veiligheidsbeleid. Hier hielden we ons bezig met internationale vrede en veiligheid. Dat was een mooi beginpunt van mijn carrière in het veiligheidsdomein, waar ik veel kon leren.”

Ze kwam er terecht in 2007. Een periode dat cyberaanvallen al flink in opkomst waren. Zo was Estland, lid van de NAVO, in een conflict verzeild geraakt met Rusland. “Estland gaf aan de andere NAVO-bondgenoten aan dat ze te maken hadden met cyberaanvallen vanuit Rusland. De websites van onder meer het parlement, banken, ziekenhuizen en omroepen werden drie weken platgelegd. Dat dit kan gebeuren is nu misschien niet meer shocking, maar op dat moment was dat echt iets nieuws. Estland gaf eigenlijk aan: ‘wat er nu met ons land gebeurt is vergelijkbaar met een fysiek bombardement. Als NAVO-lid zouden wij artikel 5 van het Noord-Atlantisch Verdrag willen inroepen’.” Kort gezegd houdt artikel 5 in dat NAVO-landen een aanval op één lidstaat beschouwen als een aanval op alle lidstaten.

“En dus moest de NAVO en al haar lidstaten daar toen wat van vinden”, legt Anouk uit. “Dat waren heel interessante discussies. Achteraf heb ik enorm geluk gehad dat ik toen als jonge medewerker bij Buitenlandse Zaken zat. Een directeur zei ook: jij hebt de nieuwste telefoon, dus jij weet vast wel wat cyberaanvallen zijn. Ik heb die kans met beide handen aangegrepen om me daar helemaal in te verdiepen.”

De wereld op zijn kop

Alles wat Anouk tot dan toe had geleerd stond op zijn kop door de komst van cyberaanvallen. Ze somt op: “Of het nou ging om internationaal recht, internationale verdragen, diplomatieke relaties, wie slachtoffers zijn, wie daders zijn, welke motieven mensen hebben om elkaars veiligheid in het geding te laten komen. Niets was meer zwart-wit. Er was een groot grijs gebied bijgekomen en niemand wist precies hoe we daarmee om moesten gaan. Met name door het asymmetrische ervan. En je wist ook niet wie achter de cyberaanvallen zat. Of het statelijke actoren waren of andere groepen. Ik vond dat allemaal zo interessant. Dus toen dacht ik: dit wil ik blijven doen!”

Na Buitenlandse Zaken stapte ze over naar Free Press Unlimited. Een NGO die zich inzet voor persvrijheid en persveiligheid. Daar begon ze in 2011, tijdens de Arabische Lente. "Het beschermen van informatie en journalisten, met name als gevolg van de opkomst van social media was een hot topic, het was dus een bijzondere timing." Daarna stapte ze over naar Policy Research Corporation en in 2016 richtte ze met twee oud-collega's Revnext op. "Een strategisch consultancybureau op het gebied van high tech vraagstukken."

> **"Ik vind dat we in de cybersecuritysector met een open blik moeten kijken naar IT-problemen en ook buiten ons eigen vakgebied naar oplossingen moeten zoeken, bijvoorbeeld uit de creatieve sector."**

Revnext: high tech consultancy en de Cyberworkplace

"Bij Revnext willen we niet de traditionele consultant of adviseur zijn, maar de klant echt helpen met operationele en technische kennis van high tech onderwerpen", vertelt Anouk. Ze staan met de poten in de klei en richten zich op energietransitie, duurzame mobiliteit en cybersecurity. In de praktijk ziet Anouk dat deze onderwerpen steeds meer naar elkaar toe groeien.

Ze doen veel aan social return en innovatie. "Daarom hebben we in 2017 de Cyberworkplace opgericht. Een non-profit school voor ethisch hacktalent. Honderd vrienden uit de sector doneren tijd om regelmatig deze mensen gratis te trainen en op te leiden. We richten ons met deze stichting op een groep die vastloopt in het reguliere schoolsysteem. Deze jongeren willen we iets bieden wat past bij hun interesses. Zeker nu is er veel vraag naar dit soort talent en op die manier kunnen we een waardevolle bijdrage leveren aan de IT-security sector. Inmiddels zijn ruim 250 deelnemers uitgestroomd."

Dit onderdeel van haar werk zou Anouk voor geen goud willen missen. Soms kan het best een uitdaging zijn om het te onderhouden, vooral als het druk is met lopende projecten. Maar het inspireert haar enorm. Daarom maakt ze bewust tijd en ruimte vrij om te zien wat er in de hackersgemeenschap gebeurt. "We hebben onlangs een nieuwe stagiair aangenomen. In een half uur had hij mijn stem gekloond en me daarmee voor de gek gehouden. Dat soort momenten maken mijn werk misschien wel het leukst. En het houdt je scherp."

Jong talent

Het valt Anouk op dat zij soms de jongste aan tafel is tijdens haar werk, en dat absoluut niet wil zijn. Ze mist de jongeren in de discussie. Terwijl die juist heel veel waarde kunnen toevoegen, vindt ze. Voor de Cyberworkspace werkt ze veel met jongeren samen. "Die kunnen genadeloos zijn. Maar dat helpt wel om je concept beter te maken. Ik laat mezelf graag omverblazen door jong talent. Dat ze iets doen waar ik niets over wist. Ik wil trouwens niet zeggen dat het alleen maar positief is. Er zijn ook zaken waar ik me zorgen over maak. Als ze iets zien op TikTok en dan dat gelijk voor waar aannemen bijvoorbeeld."

Het binnenhalen en binnenhouden van jong talent is een belangrijk onderdeel van de innovatiestrategie van Revnext. Nieuwe talenten mogen zelf hun eerste social return opdracht aandragen. Er wordt dan wel verwacht dat er gepresteerd wordt en ze moeten hun opdracht zelf verdedigen. “Op die manier daag je talenten uit. Ik denk dat deze aanpak ook maakt dat we innovatiever zijn.”

Een voorbeeld van een innovatieve benadering van Revext is een training die ze hebben opgezet om security awareness te vergroten. Ze zijn afgestapt van de standaard phishing mails, omdat dit vaak een negatieve benadering heeft. In hun nieuwe training laten ze medewerkers van klanten denken als een crimineel. “We laten ze bijvoorbeeld zelf een stem deepfaken om daarmee de CEO fraude te laten plegen. Deze aanpak daagt deelnemers uit om vanuit de crimineel te denken: outsmart de crimineel. Ik wil klanten er bewust van maken dat iedereen dit kan overkomen.”

> **“Er bestaat een zekere voorkeur voor het ontwikkelen van flashy technische tooltjes. Hier zit veel wensdenken in. Voor mij gaat innovatie over hele simpele oplossingen, waarbij je een probleem op een nieuwe manier beschouwt.”**

Omdenken om te innoveren

“Als we Anouk vragen hoe zij innovatie zou definiëren, geeft ze aan dat ze vooral weet wat ze géén innovatie vindt. Er worden te vaak IT-oplossingen gezocht voor IT-problemen”, stelt Anouk. Dat werkt volgens haar niet. Ook vertelt ze dat ze vaak oplossingen tegenkomt voor problemen die er niet zijn. Zeker in het cybersecuritydomein. “Er bestaat een zekere voorkeur voor het ontwikkelen van flashy technische tooltjes. Hier zit veel wensdenken in. Voor mij gaat innovatie over hele simpele oplossingen, waarbij je een probleem op een nieuwe manier beschouwt.”

Een voorbeeld die ze noemt is het IRMA-principe, ontwikkeld op de Radboud Universiteit. IRMA staat voor ‘I reveal my attributes’. “Het gaat over omdenken”, legt Anouk uit. “Stel: je wilt alcohol kopen. Moet je dan je geboortedatum geven of is het voldoende om te zeggen dat je achttien of ouder bent? IRMA stelt dat het laatste voldoende is. Met andere woorden, je hoeft dus niet meer je ID te laten zien, enkel wel de eigenschappen (attributes) van het ‘volwassen zijn’. Dan heb je het over het schetsen van kaders waar het antwoord aan moet voldoen, in plaats van het geven van het exacte antwoord zelf. Als we kijken naar het voorbeeld kun je volgens het IRMA-principe veiligheid in de aanschafprocedure van alcohol bieden, zonder herleidbare persoonsgegevens te delen. Dit principe kan volgens mij in veel cybersecurityprocessen worden toegepast. Op die manier omdenken, zonder additionele tooltjes, dát is voor mij innovatie.”

> **“We zijn gestart met een handboek ‘symbooltaal’ voor cyberaanvallen, zoals de NAVO heeft voor militaire symbolen. De vertaal- en uitlegfunctie van zo’n handboek maakt dat we snelheid kunnen creëren in alle lagen van de organisatie.”**

Augmented reality en een cyberhandboek

Anouk heeft aan meerdere projecten gewerkt waar ze dit principe van omdenken heeft toegepast om tot innovaties te komen. Een van die projecten is het visueel zichtbaar maken van cyberweerbaarheidsprocessen voor Defensie. Ze stelt dat er binnen de IT veel is geïnnoveerd rond applicaties en netwerken, maar er op andere vlakken echt sprake is van stilstand. "Vrijwel sinds de begintijd van de computer werken we met een muis, toetsenbord en een dashboard waarin de belangrijkste parameters terugkomen. Deze elementen waarmee we interactie met onze computers hebben zijn amper geëvolueerd. Jammer, want juist daar is winst te behalen. Wij hebben voor Defensie gekeken hoe je met augmented reality kan visualiseren wat er gebeurt bij een cyberaanval in je directe omgeving. Hierdoor is het mogelijk voor mensen zonder technische achtergrond om op korte termijn extra operationele intelligentie en snelheid te creëren. Om dit te realiseren hebben we ook samengewerkt met mensen uit de creatieve sector die kennis rondom visualisaties en beeldtaal meebrengen. Een ongewone aanpak, maar wel met een vernieuwend effect. Dat is heel mooi om te zien."

Een mooie bijvangst van het project noemt Anouk de realisatie van een 'symbooltaal' voor cyberaanvallen. Ze legt uit dat er binnen het militaire domein een NAVO-handboek is met universele militaire symbolen. Deze symbolen laten zien wat iets is, zoals een wegafsluiting of een mijn. Het zijn symbolen die iedereen begrijpt: van operatie tot strategische staf. In de cyberwereld bestaat dat nog niet. "Hierdoor is er sneller onbegrip over wat er is gebeurd. We zijn gestart met een handboek 'symbooltaal' voor cyberaanvallen. De vertaal- en uitlegfunctie van zo'n handboek maakt dat we snelheid kunnen creëren in alle lagen van de organisatie. Ik denk dat dit erg belangrijk is, en ook al heel lang wordt onderschat."

> **"Misschien maken we het als sector wel onnodig complex. En houden we dit zelf in stand door cybersecurity als rocket science neer te zetten. Dat is voor de business interessant, maar veel IT problemen zijn gewoon eenvoudig op te lossen."**

Ambachtelijke cybervaardigheden

"Er worden te vaak IT-oplossingen gezocht voor IT-problemen", stelt Anouk. Dat werkt volgens haar niet. Zij vindt dat we in de cybersecuritysector met een open blik moeten kijken naar IT-problemen en ook buiten ons eigen vakgebied naar oplossingen moeten zoeken. Zoals de samenwerking met talent uit de creatieve sector bij het visualisatieproces voor Defensie.

"Misschien maken we het als sector wel onnodig complex. En houden we dit zelf in stand door cybersecurity als rocket science neer te zetten. Dat is voor de business interessant, maar veel IT problemen zijn gewoon eenvoudig op te lossen." In veel gevallen komt het neer op het verbeteren van authenticatieprocessen of het bijhouden van updates. Deze bijna ambachtelijke vaardigheden zijn essentieel om een veiligere omgeving te creëren. Patching is eigenlijk het loodgieterswerk van de 21e eeuw."

Ethics by design

De komende jaren verwacht Anouk dat ethiek steeds belangrijker wordt. Of in ieder geval, zou moeten worden. “We werken gelukkig steeds meer met concepten als security by design en privacy by design. Het heeft best lang geduurd voordat deze concepten aan de voorkant in plaats van afterthought in innovatieprocessen worden geïmplementeerd. Maar als we kijken naar de recente opkomst van next generation AI-toepassingen, dan lijken we dezelfde fout te maken. We laten eerst grote tech bedrijven hun nieuwe producten en diensten uitrollen en een marktmonopolie verkrijgen om vervolgens te bespreken hoe deze eigenlijk veiliger en privacygevoeliger, maar ook ethischer zouden moeten zijn. Achteraf repareren zou eigenlijk niet nodig moeten zijn. En ik denk dat we steeds meer moeten toewerken naar een norm waarin we ethics by design meenemen bij het ontwikkelen van nieuwe technologie. Op dit gebied lopen we nu achter de feiten aan.”

Anouk vraagt zich af hoe we daar als sector mee omgaan in de toekomst. “Krijgen we weer een wapenwedloop van software? Of gaan we er op een andere manier naar kijken?”

Samenwerking tussen overheid en bedrijfsleven

Ooit studeerde Anouk af op het onderwerp: heeft de NAVO een verantwoordelijkheid in cybersecurity? Zij vond van niet, de NAVO vond van wel. Inmiddels is cybersecurity het vijfde militaire domein van het bondgenootschap naast land, water, lucht en ruimte. Toch houdt Anouk nog vast aan haar eerdere standpunt. “Cyberspace is anders. Het is gemaakt door mensen, het is geen force of nature zoals de andere vier dat wel zijn. En het is grotendeels in private handen. Je kunt er dus niet zomaar grenzen sluiten of sancties opleggen. Toch denken we op een oude manier dit domein onder controle te kunnen krijgen. Daarin trekken overheden nog een veel te grote broek aan.”

Dat stukje zelfreflectie van de overheid mist Anouk. Ook op nationaal niveau. Ze legt uit: “Het Nationaal Cyber Security Centrum heeft in hun missie opgenomen dat ze handelingsperspectief bieden, een verschrikkelijk woord, want wat zegt dit nu? Je krijgt geen concrete hulp, maar een perspectief op je eigen verantwoordelijkheid? Word je geïnspireerd om jezelf in cybernood te redden? Dit illustreert dat overheden nog altijd moeite hebben hun rol te pakken in cybersecurity. Er bestaat geen extra overheidsdienst naast de brandweer, politie en ambulance als het misgaat. Maar hoe gaan we het dan wel doen?” Deze vraag blijft volgens Anouk boven de markt hangen.

De *mission creep* vanuit de overheid ontwikkelt zich overigens steeds verder. Anouk voorziet een ‘oorlog’ om wat zich kan en mag afspelen in de breinen van mensen. De NAVO schrijft daar nu al de eerste ideeën over op, het cognitieve domein als zesde domein. Dus in hoeverre NAVO-lidstaten de beeldvorming van mensen kunnen beïnvloeden. En dit terwijl we nu al worstelen met de uitdagingen van kunstmatige intelligentie. Ook daarin ziet ze zuivere samenwerking tussen overheid en bedrijfsleven als cruciaal. “Hoe gaan we bepalen wat echt is? Wat nep is? Hoe gaan we mensen beïnvloeden?”

> **"Ik vind het noodzakelijk dat de overheid met een 'Big Hairy Audacious Goal' gaat komen om de samenwerking met het bedrijfsleven te verbeteren, waardoor we op het gebied van cybersecurity - figuurlijk dan - naar de maan gaan."**

Naar de maan

Anouk haalt het voorbeeld aan van de Amerikaanse regering die in begin jaren zestig naar de maan wilde. De overheid had de kennis nog niet, maar wel een duidelijke missie en ambitie. De opdracht: nog voor het einde van het decennium landen we een mens op de maan. Niet omdat het makkelijk is, maar omdat het moeilijk is. Dit initiatief was uiteindelijk een succes. "Waarom kan dat niet bij cybersecurity?", vraagt Anouk zich af. "Waarom moet het dan met instituten die slechts hier en daar kunnen bijsturen of overheden die komen met ingewikkelde wetten? Waarom niet aan de voorkant dit thema aanpakken en écht met een visie of missie komen om dit samen met het bedrijfsleven te organiseren? Ik denk dat we dan een stuk efficiënter kunnen werken en tot betere oplossingen kunnen komen. Ik mis dat vanuit de overheid. Ik vind dat het noodzakelijk is dat de overheid met een 'Big Hairy Audacious Goal' gaat komen om de samenwerking met het bedrijfsleven te verbeteren. Waardoor we op het gebied van cybersecurity – figuurlijk dan – naar de maan gaan."

''Er is veel winst te behalen door de marktbehoefte als vertrekpunt voor innovatie te nemen.''

16. Evelien Bras
- Directeur van The Cyber Partners & Directeur bestuurder van FERM Rotterdam

Vernieuwen zit in het bloed van Evelien Bras, directeur-bestuurder van FERM en directeur van The Cyber Partners. Tijdens haar carrière vol met vernieuwende projecten heeft ze verschillende innovaties voorbij zien komen. Ze gelooft dat er veel te winnen valt door met innovaties meer naar de marktbehoefte te kijken en daarop in te spelen. Het moet echt om de vraag gaan: wat heeft dit bedrijf of deze organisatie nu nodig? Voor de komende jaren ziet ze AI, meer gezamenlijke verantwoordelijkheid en toewerken naar een volwassen digitaal stelsel als de belangrijkste trends.

Innovatie, technologie en cybersecurity als rode draad

"Vernieuwen zit in mijn bloed", vertelt Evelien. Ze kwam ooit vanuit het thema innovatie in het securitydomein terecht. "Na een technische opleiding werd ik vooral gedreven door nieuwsgierigheid: hoe wordt zoiets dan gebruikt? Als je iets nieuws maakt, wat zorgt er dan voor dat het een succes is en wat niet? En wat kunnen we anders doen?"

Haar carrière is dan ook divers te noemen. Vol met vernieuwende projecten, en ook met een duidelijk rode draad. Technologie, cybersecurity en duurzaam innoveren stonden altijd centraal. In het begin van haar carrière was ze werkzaam in de telecomsector. Daarna werkte ze tien jaar voor Thales, waar ze onder andere betrokken was bij de Joint Strike Fighter. In de laatste jaren was ze business innovation director bij dit bedrijf waarin ze ook verantwoordelijk was voor de development van het High Tech Systems Park in Hengelo: een ecosysteem waarin high tech scale-ups en volwassen organisaties worden gefaciliteerd samen te werken, te innoveren en groei te realiseren. Daarnaast is Evelien ook betrokken geweest bij de opzet van het Cybersecurity Centrum voor de Maakindustrie (CCM), gericht op het digitaal weerbaar maken van de Nederlandse maakindustrie. Ook is ze oprichter van "The Cyber Partners" en commissaris, waarbij haar rol in de board zich vooral richt op duurzaam innoveren.

Sinds begin 2021 is ze directeur van FERM. FERM is gestart als onderdeel van het Port Cyber Resilience Programma, met als doel het stimuleren van samenwerking tussen bedrijven in de Rotterdamse haven om het bewustzijn bij bedrijven over cyberrisico's te verhogen en de best digitaal beveiligde haven van de wereld te worden. Sinds 1 januari 2021 is FERM een stichting zonder winstoogmerk met betaalde dienstverlening voor participanten.

Innovatie komt in veel verschillende vormen

Evelien is in haar werk veel verschillende manieren tegengekomen om te innoveren. Bijvoorbeeld politiek, strategisch, tactisch of operationeel:

- Politieke innovatie gaat over het reageren op een veranderende maatschappelijke behoefte of mondiale uitdaging, wat tot vernieuwing leidt. Dit is een typische 'top-down' benadering.
- Strategische innovatie betreft de implementatie van nieuwe manieren voor huidige doelen - bijvoorbeeld om de concurrentiepositie van een organisatie te verbeteren, marktaandeel te vergroten of nieuwe markten te betreden.

- Tactische of operationele innovatie omvat product- of procesvernieuwingen, deze kan ‘bottom-up’ ontstaan.

Evelien legt uit: “Strategische innovatie gaat verder dan tactische of operationele innovatie. Het gaat namelijk over een fundamentele heroverweging van het bedrijfsmodel, de benadering van de markt en de onderliggende waardeproposities.”

Ook zegt ze dat je innovatie kunt benaderen vanuit zogeheten Technology Readiness Levels. Een methode om de volwassenheid of gereedheid van bepaalde technologieën te meten. “Dit wordt vaak gebruikt om de progressie van technologie te volgen, van conceptstadium tot volledige implementatie. De levels lopen van TRL 1 tot TRL 9. TRL 1 is de vroegste fase en bij TRL 9 is de technologie succesvol geïmplementeerd en in gebruik genomen in de beoogde operationele omgeving. In de tussenliggende fases wordt gewerkt van een Proof of Concept tot de validatie in de relevante omgeving.”

“Daarnaast kun je innovatie ook aanvliegen vanuit de lean start-up methode, waarbij je de propositie als uitgangspunt neemt”, stelt Evelien. Dit bestaat uit vraagoriëntatie, vraagbundeling en een passende oplossing zoeken.

En ze ziet als derde mogelijkheid dat innovatie ontstaat uit samenwerking. “Als je kijkt naar de keten, worden er vaak nog oude specificaties uitgevoerd, terwijl de toeleverancier wellicht een slimmere oplossing kan bieden, die simpelweg niet wordt gevraagd. Door samen te werken kun je dus innovatieve oplossingen ontdekken. Hier ligt een groot potentieel voor verbetering”.

Kortom, wat innovatie is, hangt af van de uitdaging, invalshoek en methode die je gebruikt. “Op basis daarvan kun je bepalen welk innovatieproces de doelstelling het beste ondersteunt. Ga je voor een technologische oplossing, een marktinnovatie of is er innovatie op politiek niveau nodig om je doel te bereiken?”

> **“Er is een grote mismatch tussen behoefte van bedrijven (‘maak het makkelijk, ontzorg me’) en besteding van de gelden.”**

Innoveren in de cybersecuritysector

Evelien ziet dat er al veel geïnnoveerd wordt in de cybersecuritysector. Maar dan met name op politiek-strategisch niveau en vanuit de technologie. Ze denkt dat er veel winst te behalen valt door vanuit de marktbehoefte te kijken naar wat de gewenste oplossing is. Deze behoefte is multidisciplinair en vraagt om meer dan alleen een technische oplossing. “Je zal dan zien dat er andere, zachte eisen belangrijk worden. Denk aan de gebruiksvriendelijkheid, prijs en het gemak waarmee het geïmplementeerd kan worden. In euro’s innoveren we veel in Nederland, maar naar mijn mening wordt dit niet altijd ingezet op het juiste type innovatie.

Er is een grote mismatch tussen behoefte van bedrijven ('maak het makkelijk, ontzorg me') en besteding van de gelden. Het moet echt om de vraag gaan: wat heeft dit bedrijf of deze organisatie nu nodig? Als we kijken naar het mkb dan wordt er veel bedacht op het gebied van beveiligingsmaatregelen en oplossingen. Maar of het werkelijk altijd past, dat betwijfel ik."

Op de vraag wat we dan als sector anders moeten doen, legt Evelien uit dat het geen eenvoudige markt is. Ze vertelt dat security het domein is van wat 'marktfalen' heet, omdat je geen actieve vraag hebt. "Er kán iets gebeuren, maar er is geen zekerheid dat dit gaat gebeuren. Vergelijk het met veiligheidsgordels of rookmelders. Deze oplossingen werden niet gevraagd want "een ongeluk overkomt mij toch niet?". De vraag moet gestimuleerd worden. Bijvoorbeeld via een wet of vanuit het verzekeringswezen. Dat is een belangrijk aspect om mee te nemen als je kijkt naar wat de sector als geheel kan verbeteren en de manier waarop.

De discussie over randvoorwaarden is hierbij ook relevant. Wie is er verantwoordelijk voor wat? Voor bedrijven kan het gaan om business continuity of bestaanszekerheid. Maar wie is er dan verantwoordelijk voor dreigingen die invloed kunnen hebben op de nationale veiligheid? En welke rol hebben de leveranciers van oplossingen? Dit gaat hand in hand met het bereiken van het juiste effect, maar in de manier waarop we daar komen zijn er veel verschillende verantwoordelijkheden die op verschillende tafels liggen."

Evelien gaat terug naar het voorbeeld van de auto-industrie. Er moest meer gebeuren op het gebied van veiligheid, maar geen enkele bestuurder gaat natuurlijk een autogordel ontwikkelen. Dat moest bij de fabrikant vandaan komen. Alleen is de fabrikant dat pas gaan doen, nadat autogordels verplicht werden. Dat bedoelt ze met hand in hand: samen lukt het wel. "En je ziet dat de cybersecuritysector dat nog aan het ontdekken is", gaat Evelien verder.

> **"Als je vanuit scenario's verantwoordelijkheden definieert over wie wat doet in welke situatie, dan kan elke partij daar vervolgens op een eigen manier invulling aan geven."**

Gezamenlijke verantwoordelijkheid

Volgens Evelien draait het om gezamenlijke verantwoordelijkheid. "Toevallig is dat ook de slogan van FERM: Gezamenlijke verantwoordelijkheid. Wij brengen bedrijven en kennis bij elkaar. Daarmee faciliteren we uitwisseling van dreigingsinformatie, oplossingen en best practices. Ook brengen we kwetsbaarheden in kaart en ondersteunen we gezamenlijke inkoop van cybersecuritydiensten. We geven een zo sterk mogelijk raamwerk mee aan bedrijven en organisaties in de Rotterdamse haven. Maar uiteindelijk blijft cyberweerbaarheid hun eigen verantwoordelijkheid."

Evelien legt uit dat gezamenlijke verantwoordelijkheid ook meer een rol moet gaan spelen in de aanpak als geheel. Als je vanuit scenario's verantwoordelijkheden definieert over wie wat doet in welke situatie, dan kan elke partij daar vervolgens op een eigen manier invulling aan geven. Ze geeft het voorbeeld van brandveiligheid: "De overheid is verantwoordelijk voor het geheel, zoals bijvoorbeeld steden en dorpen. Bedrijven of organisaties zijn verantwoordelijk voor een enkel gebouw. Maar omdat de overheid voor de veiligheid van het geheel afhankelijk is van de veiligheid van het gebouw, stellen ze daar regels voor op. Waar je mag bouwen, hoe je moet bouwen, welke maatregelen zijn nodig om brand te voorkomen of te bestrijden. En een dergelijke ontwikkeling zal ook nodig zijn in de cybersecuritysector."

Als we dan weer even inzoomen op de haven: "De haven is complex en er zijn veel regionale overheden die hier iets mee te maken hebben, echter is er niet één 'eindbaas'. Soms spreek ik naast marktfalen ook over coördinatiefalen omdat veel partijen betrokken zijn met elk hun verantwoordelijkheid. Scenario's helpen dan heel erg om daar duiding in aan te brengen. Op basis van scenario's is makkelijker in te zien door de verschillende partijen wie waar verantwoordelijk voor is."

De innovatiestrategie van FERM

FERM richt zich met name op het toepassen van innovaties die zich elders al hebben bewezen en werken. "TRL 9 dus", verduidelijkt Evelien. Ze werken nauw samen met partners in onder andere het onderwijs en onderzoek. En tegelijkertijd willen ze dicht bij de bedrijven blijven staan die de innovaties gaan toepassen. Inmiddels hebben ze een heel groot netwerk in de haven. "Dat betekent dat we nieuwe oplossingen ook snel en veelvuldig kunnen toetsen. Hierdoor is het mogelijk om een grote groep bedrijven te ondersteunen met wat werkt."

Jarenlang hebben ze passieve scans uitgevoerd bij bedrijven in de haven. In de loop der tijd zien ze daardoor een stijging in de cybersecurityvolwassenheid. Evelien is trots: "Zeker in de laatste periode zien we dat het niveau van bedrijven in Rotterdam hoger is dan gemiddeld in Nederland. Nou, daar ben ik best trots op! Uiteindelijk gaat het ook bij innovatie om het resultaat, om de impact. Maar ten tweede ben ik ook trots op de scan zelf. Hiermee bieden we een onafhankelijke en objectieve meting aan waar bedrijven ook echt iets aan hebben."

Evelien is daarnaast heel blij met de samenwerking in de haven. "Ondanks dat er altijd al veel samenwerking was vanwege de onderlinge afhankelijkheid, merk je nu dat de CISO-gemeenschap elkaar makkelijker vindt en meer informatie deelt. Zeker als er vanuit de bedrijven vragen worden gesteld, kan er waarde toegevoegd worden. Vooral in deze tijd, waarin steeds vaker contactpersonen van baan wisselen, is het waardevol om te zien dat nieuwe medewerkers dankzij de community en de beschikbare tools elkaar snel weer weten te vinden."

> **"De exponentiële versnelling van dit moment is wel een factor waar we rekening mee moeten houden. En ik weet nog niet of wij al wel voldoende inzicht hebben."**

Trends van de toekomst: AI en een volwassen digitaal stelsel

De komende jaren denkt Evelien dat AI dominant gaat worden. Ze legt uit dat AI een dubbelzijdig effect heeft op cybersecurity. Aan de ene kant biedt het tools om bedreigingen te detecteren, patronen te analyseren en reacties te automatiseren. Hierdoor worden beveiligingssystemen effectiever. Aan de andere kant kunnen kwaadwillenden AI ook inzetten om geavanceerdere aanvallen te lanceren, systemen te misleiden of beveiligingsmaatregelen te omzeilen. "De exponentiële versnelling van dit moment is wel een factor waar we rekening mee moeten houden. En ik weet nog niet of wij al wel voldoende inzicht hebben", zegt ze.

Op een ander abstractieniveau, denkt ze dat we als sector ook meer toe moeten werken naar een volwassen digitaal stelsel. Zoals het financiële stelsel of het juridische stelsel dat we nu al kennen. "Vergis je niet: de mensheid heeft honderden jaren gedaan om het financiële stelsel te ontwikkelen. Denk aan (virtueel) geld, rente, leningen en waardedaling. En wellicht heeft de mens nog langer kunnen wennen aan het juridische stelsel. Dat er een rechter is die rechtspraak doet, dat je in principe de wet moet kennen. En iedereen weet wel welke wetten er voor hem of haar leefomgeving gelden. Zo moeten we ook gaan wennen aan het digitale stelsel én moet het stelsel volwassen worden. Daar zie ik enorm veel kansen. Dat er sprake is van een onafhankelijke toezichthouder die kan controleren en handhaven, een scheiding der machten en regels omtrent technologie die we samen kunnen volgen."

> **"Integriteit is steeds moeilijker aan te tonen, omdat je elkaar minder goed écht kent. Je krijgt daardoor een groter grijs gebied als het gaat om vertrouwen."**

Integriteit

Op dit moment is de sector daar nog niet. Evelien legt uit dat het stelsel dat er nu is, geïnitieerd is om de efficiëntie en financiële doelstellingen van bedrijven te ondersteunen, iets wat soms in strijd is met het ondersteunen van de samenleving als geheel. "Cybersecurity kan er bijvoorbeeld voor zorgen dat een journalist kan duiden wanneer content waar, integer en betrouwbaar is. In de klassieke media heb je al allerlei wet- en regelgeving waar journalisten aan moeten voldoen. Online is dit veel minder van toepassing, met alle gevolgen van dien. Met deze gedachtegang loop ik misschien wat op de troepen vooruit. Toch is dit wel een ontwikkeling waar ik in geloof."

Daarnaast verwacht Evelien dat iedereen een digitale basiskennis gaat krijgen. Vergeleken met het financiële stelsel: je krijgt bijvoorbeeld van huis uit mee om geen geld uit te geven, voordat je het hebt verdiend. In de nabije toekomst zullen mensen ook op digitaal vlak een basisontwikkeling hebben. Het digitale stelsel zal uiteindelijk idealiter op deze basiskennis rusten.

"Wat tot slot heel belangrijk gaat worden is integriteit", stelt Evelien. "Integriteit is steeds moeilijker aan te tonen, omdat je elkaar minder goed écht kent. Je krijgt daardoor een

groter grijs gebied als het gaat om vertrouwen. Hoe toon je aan wat beïnvloeding is? Of wat de waarheid is? Hoe integer is het nieuws? Hoe complexer onze samenleving wordt, hoe moeilijker het is om integriteit aan te tonen. Technologie kan en moet daarin gaan ondersteunen. En een zuiver digitaal stelsel kan daarbij helpen, als veilige technologie die de samenleving beter ondersteunt. Kortom, er is in dit werkveld voldoende ruimte voor innovatie!"

“Op digitale veiligheid moeten we niet concurreren, maar samenwerken.”

17. Daan Rijnders
- Kwartiermaker voor Digitaal Veilig Den Haag

Daan Rijnders, kwartiermaker voor Digitaal Veilig Den Haag, deelt zijn visie op de rol van de overheid in het veiligheidsdomein. Hij heeft een nieuwe cybersecuritystrategie ontwikkeld voor de gemeente Den Haag, met als doel de digitale veiligheid van de stad te versterken. Welke verantwoordelijkheid heb je als stad voor de digitale veiligheid van duizenden mensen, dag in dag uit? En hoe kom je tot de innovatieve oplossingen die daarvoor nodig zijn? Daan vertelt over zijn (soms mislukte) pionierende projecten en de noodzaak van risicogebaseerd denken.

De rol van de overheid

Daan raakte tijdens zijn studies (bestuurs- en organisatiewetenschappen en crisis & security management) al gefascineerd door digitalisering en veiligheid. Zijn studiegenoten richtten zich vooral op vraagstukken als radicalisering en terrorisme, maar hij was geïnteresseerd in de rol van de overheid binnen het veiligheidsdomein. “Dat brengt een hele nieuwe dimensie met zich mee”, legt Daan uit. “Als overheid heb je als het ware een sociaal contract met de samenleving. Je moet de veiligheid van miljoenen mensen garanderen. Maar hoe doe je dat? En wat is daarvoor nodig?”

Na zijn studie vertrok Daan naar Den Haag om antwoorden te vinden op deze vragen, want daar richtte de gemeente samen met andere partijen net Security Delta (HSD) op. Een veiligheidscluster van 275 bedrijven, overheidsorganisaties en kennisinstellingen die samenwerken om tot innovatieve veiligheidsoplossingen te komen voor de samenleving. Zelf speelde hij daar ook een actieve rol in. “Het bracht me bij de gemeente Den Haag, waar ik zeven jaar werkte aan de ontwikkeling van het innovatie-ecosysteem. Digitale veiligheid speelde hier een cruciale rol in. Ik was betrokken bij verschillende innovatieprojecten, conferenties en samenwerkingsverbanden met kennisinstellingen en de universiteiten in de stad.”

In 2021 werd hij door de Haagse burgemeester en wethouder digitalisering aangesteld als kwartiermaker Digitaal Veilig Den Haag. Zijn opdracht? De eerste stadsbrede strategie ontwikkelen om de digitale veiligheid van de stad te versterken. Geen eenvoudige opgave, maar dit was de uitdaging waar hij naar op zoek was.

Digitaal Veilig Den Haag

“De basis van een digitaal veilige stad begint bij de gemeentelijke organisatie zelf”, stelt Daan. Maar het ontbrak aan een integrale strategie om ook de veiligheid van de stad buiten het stadhuis aan te pakken. “De gemeente beschikt over veel data en systemen die van groot belang zijn voor de dienstverlening aan de inwoners. Maar onze inwoners zijn in hun dagelijks leven ook afhankelijk van heel veel andere partijen in de stad. Het goed functioneren van de lokale vitale processen is essentieel. Denk aan de klassieke infrastructuur, zoals elektriciteit, water en bruggen, maar ook aan sectoren zoals gezondheidszorg, onderwijs en lokale distributie van levensmiddelen. Deze moeten allemaal digitaal veilig zijn om de stad draaiende te houden.”

De focus van de strategie voor digitale veiligheid werd dus niet de gemeentelijke organisatie zelf, maar het bredere stedelijke systeem dat bestaat uit mensen, organisaties, infrastructuur en processen. Verschillende vraagstukken komen erin aan bod, zoals wat een digitaal veilige stad inhoudt en welke maatregelen genomen kunnen worden om de stad digitaal veiliger te maken. Daan hanteerde het NIST Cybersecurity Framework als richtlijn en maakte deze toepasbaar op het niveau van de stad.

Den Haag is als internationale stad van vrede en recht een unieke stad als het om veiligheid gaat. "Den Haag is echt anders dan andere steden. Het is opmerkelijk hoe Den Haag internationaal veel meer omvat dan alleen de gemeente zelf. Door alle internationale organisaties, tribunalen, NGO's en Rijksoverheid. Alles wat hier gebeurt, heeft grote internationale betekenis en dat maakt me trots. Er zijn wel een paar andere plekken in Europa die vergelijkbaar zijn, zoals Genève. Ik werk daar ook veel mee samen. Er is voor de vestiging van nieuwe internationale organisaties vaak veel interesse vanuit steden als Genève, Brussel, Wenen en Den Haag. In zekere zin zijn we dan concurrenten, maar er is één punt waar we niet op moeten concurreren: digitale veiligheid. Daar moeten we op samenwerken. Uiteindelijk staan we samen voor internationale vrede, recht en veiligheid."

"Innovatie wordt vaak geassocieerd met het creëren van bijvoorbeeld financiële waarde, zelf ben ik het steeds meer als een denkwijze gaan zien."

Pionierende projecten

Daan voelt zich het meest op zijn plek in pionierende projecten die niet makkelijk kunnen worden afgerond. Het liefst op het gebied van veiligheid, digitalisering, innovatie en economie. Digitaal Veilig Den Haag is daar een passend voorbeeld van. Als anderen opgeven, ziet Daan juist kans om meerwaarde te bieden. Dat is het moment waarop hij het verschil kan maken. Daar zijn vaak innovatieve oplossingen voor nodig die niet zomaar voorhanden zijn. Hoe kom je tot nieuwe inzichten? En hoe implementeer je deze vervolgens?

Daan legt uit dat het klassieke idee van innovatie zich richt op producten en procesverbeteringen. "Daar zijn vervolgens ook platform- en marketinginnovatie bij gekomen. Vanuit een zakelijk perspectief wordt innovatie vaak geassocieerd met het creëren van harde financiële waarde, UX, conversie, gebruikersaantallen etc. Zelf ben ik innovatie ook steeds meer als een denkwijze gaan zien, waarbij het gaat om het bedenken en ontwikkelen van nieuwe – soms abstracte – concepten."

"Maar het is wel van cruciaal belang dat innovatie succesvol wordt geïmplementeerd of uitgevoerd", voegt hij toe. Het moet volledig worden omarmd op een duurzame manier, anders blijft het slechts een goed idee of leuk concept: "Ik heb genoeg mislukte innovaties gezien. Het is interessant om te kijken naar wat er misging en daarvan te leren voor het volgende project. Vraag jezelf vooral af: hoe maak ik het de volgende keer wel succesvol?"

Daan noemt het voorbeeld van een project waarbij verschillende organisaties met een hoog risico in Den Haag nu voor het eerst informatie met elkaar delen. Dit bouwt voort op de lessen die ze hadden geleerd uit eerdere, minder succesvolle innovatieprojecten. "Ik ben

trots om te zien dat deze organisaties nu aan tafel zitten en daadwerkelijk informatie delen. Hierdoor kunnen ze sneller schakelen, zelfs in het geval van incidenten."

> **"We moeten een situatie creëren waarin innovatie mogelijk is en blijft plaatsvinden, zodat we vooroplopen. Op dit moment zijn we daar nog niet."**

Innovatie in de IT-securitysector

De cybersecuritywereld is geen makkelijke omgeving om te innoveren. Nieuwe ontwikkelingen gaan razendsnel. Als je nu niet voorbereid bent op de toekomst, dan loop je al achter de feiten aan. "Je hebt te maken met asymmetrische uitdagingen", licht Daan toe. "Je moet je hier constant tegen wapenen en beveiligen, terwijl aanvallers slechts één kans nodig hebben. Dus ik zou zeggen dat het niet zozeer een kwestie is van innovatief genoeg zijn – als een soort nice-to-have – maar eerder dat het essentieel is om te blijven innoveren."

In de praktijk ziet Daan dat dit niet voor iedereen vanzelfsprekend is. Het beschermen van zeer gevoelige informatie bij de overheid leidt er vaak toe dat er samengewerkt wordt met partijen die een lange staat van dienst hebben en weten hoe ze om moeten gaan met dergelijke gegevens. Dat betekent alleen niet meteen dat die partijen ook het meest innovatief zijn. Het is echter niet eenvoudig om in zee te gaan met een partij die innovatief en veelbelovend lijkt, maar die je niet goed kent. Daan concludeert dat in de beveiligingssector succesvolle ondernemers vaak mensen zijn met veel praktijkervaring. Ze begrijpen daardoor beter wat er nodig is in bepaalde situaties.

> **''De trust en confidence game is een uitdaging in deze sector en ik weet niet of dat leidt tot meer innovatie."**

Vertrouwde gezichten of veelbelovende innovators

En de sector is sterk gebaseerd op vertrouwen: de "trust & confidence game", vult hij aan. "Er wordt veel waarde gehecht aan de ervaring en reputatie van mensen en organisaties. We hebben geregeld te maken met nog onbekende dreigingen, omdat deze wereld constant aan verandering onderhevig is. Je moet dan van tevoren vertrouwen op de reputatie, de naam en de belofte dat de oplossing uiteindelijk zal doen wat de leverancier belooft. Dat is een uitdaging in deze sector en ik weet niet of dat leidt tot meer innovatie."

Daan ziet in de praktijk een duidelijke behoefte – en daarmee kansen – in meer transparantie en evidence-based security. In plaats van te vertrouwen op beloftes en reputatie, moeten we laten zien dat oplossingen daadwerkelijk effectief zijn.

> **''Peer-teams zouden kunnen helpen om verschillende oplossingen te testen om te bepalen welke de beste is. Zo kun je de output van een oplossing, of een mix van oplossingen, veel beter toetsen."**

Evidence-based security

Het kan lastig zijn om de effectiviteit van security-oplossingen aan te tonen. Zeker als je niet weet welke dreigingen er op je af zullen komen. Daan ziet een aantal ontwikkelingen en voorbeelden in de sector die evidence-based security en transparantie bevorderen.

In de ICT-sector ziet hij nu bijvoorbeeld de trend van consolidatie. Organisaties proberen af te stappen van verschillende producten en oplossingen van leveranciers. Ze streven naar minder complexiteit en willen het beheer vereenvoudigen. Tegelijkertijd zou je juist willen experimenteren en verschillende oplossingen willen testen om te bepalen welke het beste is, vindt Daan. Hij legt uit dat dit gestimuleerd kan worden door peer-teams te vormen en te vergelijken wat wel en niet werkt. Het kan een hele onderneming zijn om dergelijke parallelle evaluaties op te zetten in het begin. Maar Daan is er wel van overtuigd dat het werkt. "Je kunt daardoor de output van een oplossing, of een mix van oplossingen, veel beter toetsen", zo stelt hij.

Daarnaast is het belangrijk om inzicht te krijgen in de kosten, risico's en gevolgen van mogelijke incidenten en investeringen. "Die kosten wil je tegen elkaar afzetten om een goede business case te maken. Op dit moment ontbreekt vaak het harde bewijs dat de bestaande investeringen en maatregelen voldoende effectief zijn of in ieder geval in verhouding staan met de mogelijke kosten. Dit creëert een situatie waarin mensen, al dan niet onbewust, met psychologische trucs en angst inspelen op incidenten en beloftes doen, mogelijk zonder dat het de juiste oplossing is voor het specifieke probleem."

"Daarom", zo stelt Daan, "moeten risico's gekwantificeerd worden. Van IT risk naar business risk. Dat is echt wel lastig, maar organisaties krijgen hierdoor meer inzicht in specifieke risico's en de impact en kosten die daarmee gepaard gaan. Daardoor kunnen ze hier beter op sturen en gerichter innoveren. Uiteindelijk kun je dan besluiten nemen op basis van de Total Cost of Ownership (TCO) van security, oftewel het totaalbedrag aan kosten van een product of dienst gedurende de hele levenscyclus, en de Return on Investment (ROI) van dat product of dienst. Er is in de hele cybersecuritysector behoefte aan een meer risico-gebaseerde aanpak", concludeert hij.

> **"In de praktijk zoeken veel bedrijven naar passende en kosteneffectieve oplossingen en dan komt het vaak voor dat zij bij niet-Nederlandse of niet-Europees producten uitkomen."**

Gericht innoveren en strategische autonomie

Daan bekijkt innovatie in het securitydomein ook op een ander abstractieniveau. Een onderwerp dat vaak besproken wordt, zowel door beleidsmakers als academici, is digitale soevereiniteit of strategische autonomie. Echter, in de praktijk zoeken veel bedrijven naar passende en kosteneffectieve oplossingen en dan komt het vaak voor dat zij bij niet-Nederlandse of niet-Europees producten uitkomen. Dat creëert op de lange termijn ongewenste afhankelijkheden en komt de kwaliteit en innovatie niet ten goede. In Nederland kan daar scherper op gelet worden, vindt hij. “We moeten een situatie creëren waarin innovatie mogelijk is en blijft plaatsvinden, zodat we vooroplopen. Op dit moment zijn we daar nog niet. Uiteindelijk draait security om het beschermen van dat wat waardevol is, of dat nu op individueel, organisatorisch of maatschappelijk niveau is. Het is belangrijk om op verschillende niveaus te kijken en een optimale situatie te organiseren. Voor de korte én de lange termijn.”

De afgelopen jaren zijn er goede initiatieven gestart die zich hierop richten. Daan noemt er een paar. Dcypher is nieuw leven in geblazen, het samenwerkingsplatform voor onderzoek en ontwikkeling op het gebied van cybersecurity in Nederland. En het coördinatiepunt voor Europese cybersecurityfinanciering is opgezet door het Ministerie van Economische Zaken. Deze initiatieven helpen met het aantrekken van externe financiering, waardoor de innovatiekracht vergroot wordt.

Maar innovatie op zichzelf heeft geen waarde als het niet gericht is op een doel. Daan noemt het voorbeeld van de strategie voor Digitaal Veilig Den Haag. “Deze strategie geeft ons richting en stelt ons in staat om gericht te innoveren en samenwerkingen aan te gaan. Het stimuleert zelfs technologieontwikkeling, omdat we nu duidelijk weten welke problemen we op stadsniveau willen aanpakken en welke risico’s we in de toekomst mogelijk tegenkomen.” Door hier nu al rekening mee te houden, kunnen ze optimaal gebruikmaken van het hele innovatie-ecosysteem dat in de stad aanwezig is.

Risicogebaseerd denken

De digitalisering van de samenleving zal de komende jaren alleen maar toenemen, waardoor onze afhankelijkheid van digitale technologieën ook groter wordt. Daan ziet nu met name trends richting cloud computing wat een soort ‘datazwaartekracht’ op deze platforms teweegbrengt. “Op deze plekken ontstaan nieuwe en verbeterde oplossingen die ons kunnen helpen. Maar we moeten ons ook altijd bewust blijven van de risico’s en uitdagingen die hiermee gepaard gaan.”

Dat laatste sluit aan op Daan’s verwachting dat risicogebaseerd denken steeds belangrijker wordt. Meer nadenken over continuïteit en veerkracht, in plaats van simpelweg de boel beveiligen. Transparantie en kwetsbaarheid spelen hierbij ook een rol. Elk jaar laten ze bij de gemeente Den Haag bijvoorbeeld hun systemen en die van hun leveranciers hacken. “We tonen hiermee aan dat we kwetsbaar zijn en dat we transparant willen zijn over onze beveiligingsinspanningen. Het feit dat we hiermee bezig zijn, laat zien dat we leren en ons aanpassen aan de kwetsbaarheden die we ontdekken. En daarnaast gaat het ook vooral om het proces van bewustwording en verbetering. Dat combineren met de drive om te innoveren is onmisbaar richting de toekomst.”

“Innovatie draait om échte waarde voor business én maatschappij.”

18. Joris den Bruinen
- Directeur van Security Delta (HSD)

Joris den Bruinen, directeur bij Security Delta (HSD), zet zich in voor effectievere besluitvorming in het securitydomein, met oog voor mens en maatschappij. Met HSD is hij een verbindende speler in het web van kenniscirculatie, samenwerking en innovatie. Volgens Joris draait innovatie om iets tot stand brengen wat écht waarde heeft. Aan ideeën geen gebrek, maar het schort vaak aan de koppeling van techniek en data aan specifieke maatschappelijke veiligheidsvraagstukken. Daar is onder andere meer publiek-private samenwerking en verbinding voor nodig, betoogt hij.

Hoe mens en organisatie verbonden zijn

In het eerste deel van het carrièrepad van Joris den Bruinen, directeur bij Security Delta (HSD), is een duidelijke rode draad te zien: mens en organisatie. Joris is gestart binnen recruitment en doorgegroeid naar management-development. Hij hield zich bezig met het in beweging krijgen van organisaties door de juiste mensen op topposities neer te zetten. Ook leiderschap creëren in gehele organisaties in plaats van enkel aan de top behoorde tot zijn werkzaamheden.

Hierna volgde een overstap als rechterhand van de DG Algemene Bestuursdienst bij de Rijksoverheid. Een tweede rode draad werd zichtbaar: het aanpakken van maatschappelijke vraagstukken en hoe de besluitvorming daarover tot stand komt. “Het proces van stakeholders in- en extern en hen betrekken, en op basis daarvan binnen de context van een ambtelijke organisatie en/of politiek besluiten nemen, vind ik ontzettend boeiend”, vertelt Joris. “Vanuit mijn maatschappelijke gedrevenheid wil ik begrijpen hoe resultaten tot stand komen en hoe je impact genereert.”

Vervolgens maakte Joris een volgende stap: hij werd rechterhand van Jozias van Aartsen, de burgemeester van Den Haag. In lijn met de ambitie van de stad - de internationale stad van vrede, recht en veiligheid - werd vanuit economisch perspectief ingezet op het thema veiligheid. En dan met name digitaal: de samenleving digitaliseert in rap tempo, en dat brengt risico’s met zich mee. Dit was en is nog steeds een belangrijk trendmatig thema, óók voor de werkgelegenheid in de toekomst. Deze aanpak werd ondersteund door het beleid van het ministerie van Economische Zaken. Dit beleid en de trend van risico’s rondom digitalisering zijn een belangrijke basis voor de oprichting van HSD.

De overstap naar HSD

HSD is ongeveer tien jaar geleden opgericht. Joris zat, als rechterhand van de burgemeester, aan tafel tijdens de oprichting met bedrijven zoals KPN, Fox-IT en Siemens, kennisinstellingen zoals de TU Delft, Universiteit Leiden, TNO en Haagse Hogeschool en de overheid zoals de gemeente Den Haag, Ministeries van EZ en J&V. Na de oprichting werd de uitvoering de volgende stap, waarvoor samenwerking met alle partijen een vereiste was. “En toen keken ze naar mij”, vertelt Joris. Inmiddels is Joris sinds 2018 de eindverantwoordelijke directeur-bestuurder van de stichting HSD.

Samengevat heeft HSD de volgende proposities:

- Toegang tot kennis. Dit zorgt ervoor dat de kennis circuleert tussen partners, zodat iedereen optimaal kan profiteren van bestaande kennis en/of nieuwe kennis kan creëren. Partners bepalen zelf welke kennis ze willen delen.
- Toegang tot innovatie. Dit is gericht op het tot stand brengen van krachtige samenwerkingen die leiden tot veiligheidsinnovaties en op het oplossen van vraagstukken van onder meer eindgebruikers.
- Toegang tot financiering en kapitaal voor bedrijven die de potentie hebben om snel door te groeien en daarmee nog meer impact kunnen maken met hun dienst of product.
- Toegang tot talent. Gezien het tekort aan mensen binnen het securitydomein, richt HSD zich op een brug slaan tussen het onderwijs en de arbeidsmarkt. HSD stimuleert een leven lang leren, ook voor professionals voor wie security een neventaak is.
- Toegang tot de markt in Nederland en gezamenlijk met partners de internationale markt opgaan met security als exportproduct.
- Bijdrage leveren aan de positionering van Nederland, de regio Zuid-Holland en Den Haag als internationale stad van vrede, recht en veiligheid. Het doel is aantrekkingskracht creëren om bedrijven, congressen, talenten, kapitaalverstrekkers (langdurig) aan te trekken naar Nederland.

Inhoudelijk heeft HSD drie hoofdthema's waarop innovatieve samenwerkingen worden gestimuleerd:

- Slimme Veilige Steden: Data en techniek koppelen aan openbare orde en veiligheidsvraagstukken. In dit programma richt HSD zich op de ontwikkeling van veilige en privacybestendige technologie in de stedelijke omgeving. Ook richt HSD zich op beleid om waarden zoals privacy, autonomie, menselijke waardigheid, rechtvaardigheid en machtsverhoudingen te waarborgen bij het gebruik van nieuwe technologieën voor stedelijke veiligheid. Het belangrijkste doel is het gebruik van technologie en data voor veilige en leefbare steden.
- Data/AI en Intel: AI voor veiligheid, vrede en recht. Security Delta speelt een sturende en verbindende rol in deze toekomstbestendige systeemtechnologie. De focus ligt op het inzetten van mensgerichte en privacybestendige datadeling tussen organisaties en het benutten van AI voor beslisondersteuning in de hele securityketen.
- Cybersecurity en cyberweerbaarheid. Cybersecurity is belangrijk voor de digitale economie. Het doel van HSD is om cybercrime te bestrijden en te voorkomen. Innovatieve cybersecurity-oplossingen worden gestimuleerd, net zoals bewustwording van security in verschillende sectoren. IT/IoT-beveiliging is een subthema waarbij gekeken wordt naar de risico's van oude IT-systemen die verbonden zijn met nieuwe IT-producten en de groei van het Internet of Things. Ook werken aan cyberweerbaarheid met een sectorgerichte aanpak van awareness tot handelingsperspectief.

Joris ziet HSD als een verbindende speler in het web om kenniscirculatie, samenwerking en innovatie in het securitydomein mogelijk te maken. Hij is een 'vertaler' tussen de business, de overheid en onderwijsinstellingen als het gaat om veiligheid in een digitaliserende wereld. Joris vervolgt zijn verhaal: "Dit faciliteren we zo goed mogelijk om een zo groot

mogelijke impact te maken. Het realiseren van vooruitgang kan complex en uitdagend zijn. Daarom is het als sector goed om fysiek bij elkaar te komen, om écht te verbinden. HSD is dan ook vaak aanwezig op conferenties binnen de securitysector en de community komt samen op HSD Campus. Ons werk is vooruitgang boeken binnen het securitydomein. Als ik dat afpel, komt het neer op mensenwerk als verbindende factor. Ik ben trots en dankbaar voor alle samenwerkingen, resultaten en impact die na tien jaar opgetekend kunnen worden en het feit dat ik leiding mag geven aan deze club."

De begrippen innovatie en security

Iedereen heeft een andere kijk op de begrippen innovatie en security. Hoe is dat voor Joris? "Innovatie is voor mij iets daadwerkelijk tot stand brengen wat waarde heeft. Een techniek die op zichzelf prachtig is, is nog geen innovatie. We spreken pas over innovatie met businesswaarde of maatschappelijke waarde als het daadwerkelijk in een organisatie of in de maatschappij geïmplementeerd kan worden. Voor mij draait innovatie om échte waarde. Waarde voor de business of voor de maatschappij. Een innovatie biedt pas échte waarde als het daadwerkelijk in een organisatie of in de maatschappij geïmplementeerd kan worden."

> **"Voor mij draait innovatie om échte waarde. Waarde voor de business of voor de maatschappij. Een innovatie biedt pas échte waarde als het daadwerkelijk in een organisatie of in de maatschappij geïmplementeerd kan worden."**

"Als je innovatie tot een succes wil brengen, heb je twee dingen nodig: professionals vanuit de techniek en degene die bezig zijn met de realisatie van veranderingen. Het is ontzettend belangrijk om technieken en datagebruik goed te implementeren in werkprocessen van en tussen organisaties."

Ook het begrip security is breed te omschrijven. We vragen Joris wat security voor hem betekent. "Interessante vraag", aldus Joris. "In het Engels heb je twee logische termen: safety en security, met ieder een heldere definitie. In het Nederlands heb je dat onderscheid niet. Het woord 'veiligheid' omschrijft het begrip nog het best. Bij 'veiligheid' heb je het over het beperken van risico's, maar honderd procent veiligheid bestaat daarom dus niet. Potentiële in- of externe risico's mitigeren kan wel. Het gaat erom dat je weet hoe je als organisatie zaken kunt voorkomen en als het dan toch gebeurt, hoe je dan kunt acteren en weer sneller 'in business' kan zijn en/of dat de maatschappij weer door kan draaien. Dat laatste is meer gericht op weerbaarheid: een heel belangrijk aspect binnen het begrip security. HSD richt zich op veiligheid én weerbaarheid in een digitaliserende wereld."

Joris geeft een voorbeeld: binnen een van de programma's richt men zich onder andere op cyber en veiligheid in stedelijke omgevingen, bijvoorbeeld door de inzet van technieken zoals camera's en drones. Het zijn sensoren en daarmee datadragers die ingezet kunnen worden voor het waarborgen van de openbare orde en veiligheid. Of bij een ramp om inzicht te krijgen in mogelijke maatregelen voor hulpdiensten. Een drone op zich biedt

volgens Joris niet alléén maar veiligheid. Het brengt ook nieuwe risico's met zich mee. Denk bijvoorbeeld aan smokkelwaar dat gedropt wordt boven gevangenissen of een drone die neerstort boven een groot publiek. "De cybersecuritykant van het verhaal is dat de data veilig moet zijn en niet gemanipuleerd kan worden en dat het privacyproof is."

Dit laat zien waarom je 'veiligheid' altijd integraal moet bekijken. Ook de digitalisering kent twee kanten van de medaille: enerzijds biedt het een oplossing en economische kansen (voor veiligheidsvraagstukken) en anderzijds brengt het nieuwe risico's met zich mee", stelt Joris. Bij HSD zijn daarom alle aspecten rondom veiligheid relevant: "We hanteren geen strakke definitie, eerder een holistische benadering. HSD is bij samenwerkingen met bedrijven, overheden en kennisinstellingen altijd op zoek naar afstemming, om samen te innoveren en een steeds verder digitaliserende wereld veiliger te kunnen maken."

> **"Innovatie gaat niet alleen over nieuwe toepassingen van techniek of data. Aan ideeën geen gebrek. Waar het nog vaak aan schort, is de uitvoeringskracht. Dáár ligt de uitdaging."**

Innoveert de sector voldoende?

De grote vraag is en blijft: innoveren we als sector voldoende? Joris grijpt hierop terug naar de definitie van de sector: "Security zit zo verweven in de maatschappij en in alle organisaties. Stel jezelf de vraag: wat is de securitysector dan eigenlijk? Het antwoord op die vraag was vroeger makkelijker. Je had de beveiligingssector, persoonsbeveiliging en een beetje techniek. Tegenwoordig is dat anders. Of je nu een klein of groot bedrijf bent, een industriële of overheidsorganisatie bent: er speelt altijd IT, soms OT en per definitie daarmee een (cyber)security vraagstuk."

"Innovatie gaat niet alleen over nieuwe toepassingen van techniek of data. Aan ideeën geen gebrek. Waar het nog vaak aan schort, is de koppeling van die techniek en data aan specifieke maatschappelijke veiligheidsvraagstukken, aan uitvoeringskracht dus. Dáár ligt de uitdaging." Onvoldoende innovatie binnen de sector dus, als je het zo bekijkt.

Dit ligt volgens Joris aan het feit dat een deel van de eindgebruikers innovaties niet kunnen omzetten in waarde of risicobeperking voor hun organisatie. De grootte c.q. volwassenheid van een organisatie is volgens hem grosso modo bepalend voor de mate van voorzieningen op het gebied van digitale veiligheid of beperking van risico's. Dit hangt samen met implementatiekracht, mensen, middelen en het risicoprofiel van organisaties.

Ook is het volgens hem afhankelijk van de sector. Banken en grote (IT- en datagedreven) multinationals hebben het qua innovatie en security vaak aardig tot goed voor elkaar. Ook de energiesector volgt snel. Hoe verder bedrijven van deze sectoren af staan en/of hoe kleiner ze zijn, hoe lager de investeringsbereidheid en implementatie van techniek, innovatie en risicoreductie op het gebied van digitale veiligheid is.

Daarnaast is het volgens Joris belangrijk om voor de digitale veiligheid niet alleen te kijken naar innovatieve veiligheidsoplossingen, maar ook naar de 'human factor'. Want het gedrag en handelen van mensen blijft cruciaal. Investeren in cybersecuritybewustzijn is daarom ook van groot belang.

> **"Om innovatie te stimuleren heb je het volgende nodig: publiek-private samenwerkingen, regelgeving die innovatie versnelt en investeringen voor bedrijven die er nog geen kapitaal voor hebben."**

Wat er nodig is om innovatie te stimuleren

"Om innovatie te stimuleren heb je het volgende nodig: publiek-private samenwerkingen, regelgeving die innovatie versnelt in plaats van tegenhoudt, financieringsmogelijkheden en investeringen voor bedrijven die er nog geen kapitaal voor hebben. Bovendien is er een rol weggelegd voor belangrijke spelers binnen de keten om volwassenheid op het gebied van security over de gehele keten te bevorderen. Je kunt je eigen zaken wel op orde hebben, maar als ketens van toeleveranciers dat niet hebben, kan dat voor jou problemen opleveren. Philips en ASML pakken die rol binnen het cyberweerbaarheidscentrum in Eindhoven.

> **"Bedrijven cyberweerbaar maken. Dát is waar we aan werken. Niet met bangmakerij, maar door bewustwording en handelingsperspectief te creëren. Innoveren gaat over stappen zetten van bewust onbekwaam naar onbewust bekwaam. "**

Joris verduidelijkt zijn verhaal met een voorbeeld van HSD, Greenport West-Holland, Provincie Zuid-Holland en Digital Trust Center op het gebied van tuinbouw. Royal FloraHolland, een grote speler met hoog volwassenheidsniveau, neemt hierin als een van de acht initiërende ketenpartijen verantwoordelijkheid. "Stel dat de iPad van een individuele kweker gehackt wordt en zijn identiteit gestolen wordt, dan kan dat compromitterend zijn voor het digitale platform van Royal FloraHolland. Als het vertrouwen van het platform ondermijnd wordt, kan dat schadelijk zijn. Royal FloraHolland heeft dan ketenverantwoordelijkheid om dit soort zaken goed te regelen."

HSD organiseert op dit moment het Cyberweerbaarheidscentrum Greenport voor de tuinbouwsector. "We begonnen met acht partijen en zijn nu met ongeveer vijfentwintig deelnemers. De uitdaging is nu om met deze vijfentwintig bedrijven de honderden kwekers en gerelateerde tuinbouwbedrijven mee te krijgen naar een hoger cyberweerbaarheidsniveau. Zonder bangmakerij, maar wél door bewustwording te creëren en handelingsperspectief te bieden." Dit is volgens Joris overigens niet alleen nodig binnen de tuinbouwsector. "Innoveren gaat over stappen zetten van bewust onbekwaam naar onbewust bekwaam en is nodig bij meerdere sectoren, zeker als het gaat om het mkb."

Volgens Joris is binnen verschillende sectoren tachtig procent van de cybersecurity-uitdagingen sectoroverstijgend. Iedere sector heeft een goed Identity & Access Management systeem nodig, zodat betrokkenen weten wie, wanneer en op welke delen van het systeem toegang heeft. Ook heeft iedere sector behoefte aan securitybeleid, effectieve monitoring en inzicht in de mogelijke risico's. Dit soort zaken zijn uniform voor iedere sector. De overige twintig procent gaat - binnen de tuinbouw bijvoorbeeld - in op specifieke warmtepompen en watermanagement, eventuele innovatie van drones en AI in een kas en sectorspecifieke data-uitwisseling in de ketens van zaadveredelaars, kwekers, de veiling en distributiebedrijven.

> **"Deze cybersecuritymarkt is redelijk onvolwassen. Bovendien blijft de markt in ontwikkeling, niet veel bedrijven schalen en zelfs na consolidatie en na fusies en overnames blijft het een onoverzichtelijke markt. Het is de vraag in hoeverre alle implementaties van deze oplossingen nu echt helpen."**

Innoveren de aanbiedende cybersecuritybedrijven dan voldoende volgens Joris? "Niet voldoende", is zijn antwoord. "Deze markt is redelijk onvolwassen. Er is een heel grote diversiteit aan spelers met producten en services waarvan het de vraag is wat het precies oplevert voor eindgebruikers. Bovendien blijft de markt in ontwikkeling, niet veel bedrijven schalen tot echt grote spelers en zelfs na enige consolidatie en fusies en overnames blijft het een onoverzichtelijke markt. Het is de vraag in hoeverre alle implementaties van deze oplossingen nu echt helpen."

Security by design randvoorwaardelijk

We hebben het ook over 'security by design', een ander begrip binnen innovatie. Volgens hem is dit de randvoorwaarde van veiligheid bij iedere digitale transformatie en IT-toepassing. Complex? "Ja, technisch misschien, maar anderzijds zeker niet, het gaat om je boerenverstand gebruiken, ook risico's meenemen in de ontwikkeling en op het moment van gebruik. Veiligheid dient een integraal onderdeel te zijn van alles wat een organisatie doet, zeker als het gaat om digitalisering."

Joris verduidelijkt dit met een voorbeeld. Hij sprak eerder een CISO van een ziekenhuis die een innovatieboard had ingeregeld en een nieuwe cybersecuritystrategie had geïmplementeerd. Op het allerhoogste niveau waren mensen betrokken. In lijn met de securitystrategie heeft deze CISO een beperking ingesteld van het aantal nieuwe IT- en securityleveranciers. Hoewel het om een beperking ging, beperkt het security an sich niet. Integendeel: hier werd juist duidelijkheid gecreëerd. "Als men iets nieuws wilde implementeren, moest security altijd aan de voorkant worden meegenomen. Leveranciers en gebruikers innoveerden op deze manier echt om 'security by design' mogelijk te maken. En als er vanuit de ziekenhuisprofessionals een heel duidelijke wens en noodzaak was voor een leverancier buiten de beperking dan kon dat, maar wel door expliciet hierbij aan te geven hoe men dan zelf de security daarbij organiseert. De CISO had in dit proces een

adviserende rol om nieuwe oplossingen binnen het bestaande IT-systeem en het generieke beleid mogelijk te maken. Binnen de innovatieboard werd dan besloten of een nieuwe leverancier een bijdrage mocht leveren op basis van hun 'security by design' oplossing. Dit is geen technologische innovatie maar wel een verfrissende manier om security slim te implementeren", aldus Joris over security by design.

> **"Ik denk dat er bij zowel de aanbiedende als de vragende kant van innovatie meer behoefte is aan consolidatie van oplossingen, waarbij technische innovaties daadwerkelijk integraal geïmplementeerd worden in combinatie met andere producten en diensten."**

Naast verfrissende manieren van innovaties bestaan er natuurlijk ook uitdagingen. Joris is hierover stellig: "Ik denk dat er bij zowel de aanbiedende als de vragende kant van innovatie meer behoefte is aan consolidatie van oplossingen, waarbij technische innovaties daadwerkelijk integraal geïmplementeerd worden in combinatie met andere producten en diensten. Technieken ontwikkelen die compatible zijn met meerdere platformen kan een oplossing zijn. Hoewel dat steeds meer gebeurt, blijft het een grote uitdaging.

"Ook moeten we afstappen van het continu benoemen van hoge dreigingen in inspelen op angst binnen de (cyber)securitybranche. IT-security zou voor organisaties net zo logisch moeten zijn om risico's te voorkomen als dat er een hr-beleid is om te voorkomen dat medewerkers weglopen."

"Ook moeten we afstappen van het continu benoemen van hoge dreigingen en het inspelen op angst binnen de securitysector. IT-security zou voor organisaties net zo logisch moeten zijn om risico's te voorkomen als een goed financieel risicobeleid of hr-beleid om te voorkomen dat medewerkers weglopen. De essentie is dat IT en security belangrijke hulpmiddelen zijn in het primaire proces waarin we de balans tussen gebruiksvriendelijkheid en veiligheid op een slimme manier moeten faciliteren."

De positie van ons land in internationaal perspectief

"Nederland heeft een relatief kleine thuismarkt ten opzichte van grote landen zoals de Verenigde Staten." Toch stelt Joris dat we als niche speler goed mee kunnen komen. Dit heeft volgens hem vijf redenen:

1. De kwaliteit van de Nederlandse producten.
2. Nederland is in staat om samenwerkingen nationaal - bijvoorbeeld via RVO/IQ/Min. BZ en HSD - én internationaal - via het netwerk van ambassades & consulaten en andere security clusters - goed te organiseren. Joris schetst tijdens het gesprek een mooi voorbeeld waarbij Nederlandse producten via de juiste connecties in Japan met succes worden toegepast.
3. Integrale samenwerking. In de triple helix van de overheid, kennisinstellingen en het bedrijfsleven. Nederland is bovendien in staat de ethische, privacy, technische en juridische aspecten goed mee te nemen in oplossingen. Dit is volgens hem ook een kans op het gebied van AI en (cyber)security.

4. De actieve ethical hacker community van Nederland die goed wordt benut. Nederland kent responsible disclosure waarbij het wel is toegestaan te hacken zolang je dit maar doet om de organisatie te attenderen op eventuele kwetsbaarheden. Dit helpt om onderscheidend te zijn.
5. Nederland is gezegend met een goede digitale infrastructuur en veel kennis en talent.

De kansen van AI voor het securitydomein

Ook blijven trends in het securitydomein niet onbesproken. Zo vormt AI volgens hem een van de grootste kansen, óók in de securitysector. "Op dit moment is er een groot tekort aan mankracht in deze sector. Met AI zouden we gedeeltelijk meer kunnen automatiseren. Het kan simpel werk uitbesteden aan algoritmen die daar beter en sneller in zijn. Ik voorzie dat dit het cybersecuritydomein de komende jaren veel gaat brengen. Een bedrijf als EclecticIQ gebruikt dit al in hun thread intel platform dat ze hebben. Cybersprint/Darktrace, ReaQta/IBM, aXite en Pandora Intelligence zijn andere bedrijven die AI slim hebben geïntegreerd in hun oplossingen."

Daarnaast benoemt Joris de noodzaak voor goede wetgeving en beleid als het gaat om de toepassing van AI in het veiligheidsdomein. Hij is actief binnen de Nederlandse AI Coalitie (NLAIC), waar het thema van ethische, juridische en sociale aspecten (ELSA) besproken wordt. In verschillende ELSA-labs wordt onderzoek gedaan naar het creëren van goede randvoorwaarden voor deze aspecten. Dit draagt bij aan een verantwoorde en mensgerichte toepassing van AI, wat vooral in het veiligheidsdomein van essentieel belang is. Privacy enhancing technologies zijn innovaties die hierbij relevant zijn. Als voorbeeld geeft Joris het gebruik van data door alleen de metadiscripties te gebruiken in plaats van alle data. Op die manier is het wél mogelijk data uit te wisselen tussen verschillende veiligheidsorganisaties zonder dat privacygevoelige gegevens op zichzelf worden uitgewisseld.

Hij geeft een belangrijke disclaimer voor AI toepassingen: "Veel bedrijven hebben op dit moment hun datapositie nog niet op orde. Voor wat betreft algoritmen en AI geldt: 'Crap in, is crap out'. De toepassing van het gebruik van data voor zinvolle management ondersteunende beslissingen of efficiëntie in het bedrijf blijft nog steeds een enorme stap."

De ontwikkelingen rondom innovatie binnen het securitydomein gaan razendsnel. Joris blijft hiervan op de hoogte via de HSD Security Insight website voor de laatste nieuwtjes. Hij is actief op Linkedin en leest hij veel vakbladen zoals Computable, Dutch IT Channel, Infosecurity magazine, Channel Connect, Beveiligingsnieuws, Cybercrimeinfo.nl en ook verschillende kranten zoals het FD, NRC en het AD. Joris vervolgt zijn verhaal: "Na tien jaar in deze sector heb ik wel een goed beeld kunnen vormen waar ik moet zijn om mijn kennis op te halen zonder alle oplossingen tot in detail te doorgronden. Kom ik er niet uit? Dan zoek ik de juiste mensen op die mij inhoudelijk kunnen vertellen hoe het zit."

Als laatste punt wil Joris nog het volgende meegeven: "Veel cybersecuritybedrijven in Nederland bieden vooral services, maar ik vind het ook mooi wanneer er echt producten worden ontwikkeld. De data diodes van Fox-IT en Compumatica of de producten van Onegini/OneWelcome, EYE Secure, Scalys en aXite zijn enkele mooie voorbeelden. Kijk of

je ook een product kan ontwikkelen in plaats van alleen services. Hiermee is internationale opschaling echt kansrijker. Als sector moeten we in staat zijn om vooral in gezamenlijkheid het (cyber)securityvolwassenheidsniveau te verhogen en dit uiteindelijk als exportproduct inzetten voor een veiligere wereld."

“We moeten toewerken naar een gezamenlijke agenda, samen met de top IT- & securitybedrijven.”

19. Ben Kokkeler
- Directeur-bestuurder van het Centrum voor Veiligheid en Digitalisering (CVD)

De rode draad in het werk van Ben Kokkeler is de relatie tussen nieuwe technologie en de samenleving. Op dit moment is Ben werkzaam als lector Digitalisering en Veiligheid bij Avans Hogeschool en directeur-bestuurder van het Centrum voor Veiligheid en Digitalisering (CVD) in Apeldoorn. Hij promoveerde aan de Universiteit Twente op innovatie in emergente organisaties en het sturende effect van gedistribueerd leiderschap in netwerkorganisaties. Sindsdien heeft hij gewerkt als onderzoeker, adviseur en bestuurder in de publieke sector.

Sinds een jaar heeft Ben de rol van directeur-bestuurder op zich genomen bij het Centrum voor Veiligheid en Digitalisering (CVD). Het CVD bundelt de krachten van kennisinstellingen, bedrijven en overheden om een veilige, digitale samenleving te bevorderen. Met de snelle digitalisering van onze samenleving, komt een scala aan kansrijke innovaties tot stand: van internetbankieren tot digitale opsporingsmethoden. Tegelijkertijd brengen deze ontwikkelingen aanzienlijke risico's met zich mee, zoals systeemverstoringen door hackers en diefstal van gevoelige gegevens. De inzet en expertise van Ben vormen een waardevolle bijdrage aan het streven naar een veilige, digitale toekomst.

Open innovatie binnen en met het CVD

Ben is stellig: "Het CVD moet niet de zoveelste club zijn met een voordeur: 'komt u binnen en wij gaan alles hier zelf doen'. Dit is een open innovatie instituut, een netwerkorganisatie. In het Nederlandse landschap van innovatie is het onze hoofdtaak om samen met Brainport Eindhoven en The Hague Security Delta, twee andere grote clusterorganisatie netwerken, ervoor te zorgen dat er consortia ontstaan. Zodat er samengewerkt, geïnnoveerd en van elkaar geleerd wordt."

De doelstellingen van het CVD

Het Centrum voor Veiligheid en Digitalisering pakt de grote vragen rond digitalisering en veiligheid bij de kop. Dit doen ze door middel van onderwijs, LLO (leven lang ontwikkelen), onderzoek en ondernemerschap.

Onderwijs en LLO: Als je voorop wilt lopen in de digitale wereld, is kennis van essentieel belang. De kennispartners van het CVD bieden een uitgebreid scala aan gepersonaliseerde leertrajecten gericht op digitalisering en veiligheid. Ongeacht het opleidingsniveau, van mbo tot wo, kunnen (toekomstige) professionals aan de slag met de vraagstukken die relevant zijn.

Onderzoek: De partners van het CVD werken op diverse manieren aan kennisontwikkeling op het gebied van veiligheid en digitalisering. Practoraten (mbo) en lectoraten (hbo) voeren bijvoorbeeld kortlopende onderzoeken uit waarbij studenten en docent-onderzoekers praktijkgerichte thema's aanpakken. Hbo- en wo-studenten krijgen de kans om uitdagende traineeships te volgen, waarin ze werken aan actuele strategische vraagstukken. Samen met praktijkpartners worden consortia geformeerd waarin onderzoekers uit de gehele

kenniskolom samenwerken aan vraagstukken rond cybersecurity, informatiegestuurd werken of kritische data en infrastructuur. Deze coalities worden ook betrokken bij de ontwikkeling van LLO-programma's en bij de ontwikkeling van gezamenlijke hoogwaardige onderzoekslaboratoria.

Ondernemerschap: Start-ups en scale-ups zoeken steeds vaker samenwerking met hogescholen en universiteiten om kennis en ervaringen uit te wisselen, wat een stimulans voor innovatie blijkt te zijn. "Onze kennispartners bieden daarom ruimte aan een Innovation- en Startup Lab en een Ondernemershuis. Deze plekken dienen als ontmoetingsplaatsen voor het bedrijfsleven en het onderwijs op het gebied van digitale veiligheid. We werken daarbij nauw samen met de Digitale Werkplaatsen, en met Apeldoorn-IT (het netwerk van IT-professionals en IT-werkgevers)."

De eerste resultaten zijn erg positief

Ben is tevreden over de resultaten tot zover: "We sluiten aan op de prioriteiten van Oost-Nederlandse provincies. De provincie Gelderland steekt een aantal miljoenen in de ontwikkeling van kennis en competenties wat betreft dit domein, om Gelderland cyberveilig te maken voor ondernemers en burgers. De ontwikkeling van kennis voor deze groepen en nieuwe curricula kost tonnen, dus de provincie faciliteert het zodat het ook snel kan gebeuren. Daarnaast faciliteert de provincie dat er promovendi zijn die samenwerken in een wetenschappelijk programma dat nieuwe kennis ontwikkelt en gericht is op praktische resultaten voor de eigen regio."

"Het tweede resultaat is dat wij in het kader van een nationale subsidieregeling, de Katapultregeling, een aanvraag hebben ingediend namens een groot consortium dat heel Oost-Nederland, Gelderland en Overijssel, omvat. De focus ligt op cybersecurity van het mkb. Het is bekend dat ongeveer tachtig procent van het mkb niet goed weet waar ze het zoeken moeten als het om cybersecurity gaat. Het CVD gaat netwerken van mkb'ers en hun koepels en adviseurs in de regio helpen met verschillende kennisprogramma's om meer grip te krijgen op hun cyberweerbaarheid."

> **"80% van het mkb weet niet waar te beginnen met cybersecurity. Het CVD helpt hen meer grip te krijgen op cyberweerbaarheid."**

Centraal in de Katapultregeling staat het versterken van de samenwerking tussen beroepsonderwijs en bedrijfsleven. Het versterken van de cyberweerbaarheid van het mkb gaat dan deels via het onderwijs. De eerste stap is het plaatsen van goede stagiaires. Ben: "Dat moet vooral doorgaan, maar dat is niet genoeg. De docenten en praktijkonderzoekers moeten zich niet alleen richten op hun hoofdtaak voor het opleiden van achttien- of negentien jarigen, maar ook steeds meer mee gaan denken met de vraagstukken die in het mkb spelen. We bouwen met die beroepsopleidingen en het mkb ook learning communities en leerkringen op waarin overstijgende vragen van een groep bedrijven twee of drie jaar lang centraal staan. Dat is stap twee. In stap drie richten we ons meer op de netwerken van bedrijven, brancheorganisaties en koepels. Daartoe is een start gemaakt met de aanpak om

ervoor te zorgen dat er een innovatie-ecosysteem gaat ontstaan in Oost-Nederland, waarin al die bestaande kernen van branches, brancheorganisaties en ondernemersverenigingen elkaar op dit punt van cybersecurity beter gaan vinden."

Samenwerkingsplek voor innovatie
Naast een fysiek kenniscentrum voor veiligheid en digitalisering, is het CVD vooral ook een samenwerkingsplek voor innovatie dankzij de betrokkenheid van vele kennisinstellingen. Het CVD is een samenwerkingsverband tussen Hogeschool Saxion, de Politieacademie, de Universiteit Twente, de gemeente Apeldoorn, ROC Aventus en het NIPV. Daarnaast is er een hechte samenwerking met het opleidings- en kenniscentrum van de Koninklijke Marechaussee, Koninklijke Landmacht, Apeldoorn IT, Centraal Beheer Achmea, de Belastingdienst, het Kadaster en Saab Nederland.

> **"Ik verwacht dat radicale systeeminnovaties niet van publieke partijen gaan komen, maar van bedrijven en publiek-private consortia die wél doorpakken."**

De grootste bedreiging voor innovatie in het publieke domein
Op basis van realisme moeten we ons, volgens Ben, meer richten op sociale innovatie, met een 'kleine s': "Dat gaat om hoe je werkprocessen aanpast en hoe je implementatiemethodieken ontwikkelt. Hoe mensen op de werkvloer, op straat, bij defensie of politie hier daadwerkelijk mee aan de slag gaan. Daar ligt heel veel werk, wat nu nog maar ten dele opgepakt wordt, men heeft in de praktijk van alledag nauwelijks tijd. Er is veel operationeel werk te doen, maar er zijn te weinig mensen, er is maar beperkt ruimte om te leren. Aan sociale innovatie met een 'grote s', het radicaal veranderen van maatschappelijke verhoudingen, en daarbinnen tussen bijvoorbeeld veiligheidsorganisaties, overheden en zelforganisatie van burgers en ondernemers, komen we dan al helemaal niet toe. En omdat de ruimte er niet is, is er ook geen mentale ruimte om er goed over na te denken. Het blijft bij kleine optimalisaties, geen radicale veranderingen. Dat is de grootste bedreiging voor de meer fundamentele sociale innovatie."

> **"Innovatie bij operationele dienstverleners is complex. Alles ligt onder een vergrootglas, er is snel kritiek. Dan ga je optimaliseren, niet radicaal innoveren."**

"Ik verwacht dat radicale systeeminnovaties niet van publieke partijen gaan komen, maar van bedrijven en publiek-private consortia die wél doorpakken. Ze zullen ook wel moeten, anders verliezen ze de internationale concurrentiestrijd", legt Ben uit.

Innovaties toepassen kost tijd
Als we Ben vragen of er voldoende innovatie in het cybersecuritydomein is, aarzelt hij:

"Het ligt op mijn lippen om 'nee' te zeggen, maar we moeten ook reëel zijn. Aanbiedende bedrijven hebben veel 'oplossingen' klaar staan, maar het daadwerkelijk toepassen kost tijd en geld. Veel mkb'ers aarzelen of ze als eerste die stap moeten maken. En een groot deel van de - vooral kleinere - gemeenten worstelt met gebrek aan expertise en zoekt naar manieren om regionaal samen te werken, hetgeen ook weer tijd vergt. En grote publieke organisaties, zoals de politie, hebben last van de schaal: er is een groeiende aandacht, er zijn innovatielabs, scholing en training komt op gang, maar er is nog veel te doen, we spreken hier over de grootste werkgevers van Nederland."

Meer samenwerking en kennisdeling

Het werk dat Ben nu doet voor het CVD lijkt sterk op wat hij in de jaren negentig heeft mogen doen voor het toenmalige Telematica instituut. Er waren toen in Nederland vier Technologische Topinstituten, rond chemie, nieuwe materialen, voeding en ICT. De hoofdtaak van die netwerkorganisaties was om innovaties te versnellen. Daar kunnen we volgens Ben nu nog wel lessen uithalen om ervoor te zorgen dat innovatie plaatsvindt." Wat we toen in ieder geval deden, was PPS consortia optuigen die vijf jaar in de lucht bleven en die in twee jaar tijd pre-concurrentieel onderzoek deden. Die consortia waren helemaal gericht op proof of concept ontwikkeling en het deugdelijk maken van allerlei concepten, en ook op het zorgen dat marktpartijen die dat gingen exploiteren daar heel snel toegang toe kregen."

> **"We moeten toewerken naar een gezamenlijke agenda, samen met de top IT- & securitybedrijven. Meer samenwerking en meer kennisdeling om innovatie binnen cybersecurity écht van de grond te krijgen in Nederland."**

"Wat ik ook bemerk is dat de cybersecuritywereld nu nog gefragmenteerd is, ook aan bedrijvenzijde. De markt is nog niet volwassen genoeg. Er is geen agenda vanuit de top tien van IT- en securitybedrijven in Nederland waarvan wetenschappelijk Nederland zegt: 'oh, ja!' Er is meer samenwerking en kennisdeling nodig om innovatie in cybersecurity echt van de grond te krijgen. Dat is waar we met zijn allen naar toe moeten werken."

Trends in het cybersecuritydomein

Ben denkt dat een belangrijke trend zou moeten zijn om jonge mensen te blijven motiveren om het brede domein van veiligheid serieus te nemen. Hij stelt: "Hoe kan je jonge mensen interesseren om voor het vakgebied te kiezen of om er een eigen verantwoordelijkheid in te pakken? Dat is in Nederland behoorlijk weggezakt. In omliggende landen zie je dat er veel meer interesse is. Er zijn bijvoorbeeld tv-programma's over de vrijwillige brandweer in Duitsland en mensen zijn heel trots om daar deel van uit te maken. En in Engeland en de Verenigde Staten zijn er regelmatig oefeningen samen met burgers over wat je moet doen in het geval van rampen of evacuaties. Ik zeg niet dat we dat pad op moeten, dat mag ook op een andere manier. Qua trends ben ik wel benieuwd hoe we burgers en ondernemers kunnen verenigen en stimuleren om een eigen verantwoordelijkheid te nemen om zich te beschermen tegen cyberaanvallen. Ook daar is nog veel winst te behalen."

"In Nederland zitten we in de samenwerkingsmodus. Dat kan enorm innoverend zijn, als je dat niet gewend bent."

20. Hans de Vries
- (oud) Directeur van het NCSC

Hans de Vries*, directeur van het Nationaal Cyber Security Centrum, vertelt over het belang van maatschappelijke waarde in zijn werk, en de innovaties en uitdagingen waar zijn organisatie mee te maken heeft. Doordat ze een steeds grotere doelgroep bedienen, moet hun dienstverlening meebewegen. Wendbaar, beheersbaar én digitaal. En dat in een arbeidsmarkt met enorme krapte, en een keten waarin de afhankelijkheid steeds groter wordt. Hans ziet samenwerken dan ook als onmisbaar: we zijn allemaal onderdeel van dezelfde maatschappelijke supply chain.

Cybersecuritycarrière

Van huis uit had Hans altijd meegekregen: geld is mooi om te hebben, maar wat doe je ermee voor de maatschappij? Het mocht duidelijk zijn dat zijn werk maatschappelijke waarde zou hebben. Na zijn middelbare school ging hij een jaar als uitwisselingsstudent naar de Verenigde Staten. Hij vertelt: “Daar is voor mij de samenhang tussen recht, sociale cultuur en maatschappij echt zichtbaar geworden. Als gevolg daarvan ben ik rechten gaan studeren.”

Tijdens zijn studie, dezelfde tijd als de opkomst van de computer, was Hans veel met IT bezig. Hij ontdekte de mogelijkheden, kansen en het gemak ervan. Iets waar hij zeker mee wilde blijven werken. En dat lukte. Na zijn studie werkte hij bij warenhuis V&D. De volgende stap in zijn cybersecuritycarrière was het IT-beheer van Binnenlandse Zaken. De plek waar hij voor het eerst echt met informatiebeveiliging in aanraking kwam. Na vervolgens drie jaar bij de AIVD mag Hans zich sinds 2014 directeur van het Nationaal Cyber Security Centrum (NCSC) noemen, verantwoordelijk voor de vitale, digitale infrastructuur van ons land. In ieder geval tot eind 2023, want dan zwaait hij af en neemt iemand anders zijn werk over.

Waarde voor de maatschappij

Het NCSC is hét centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Ook coördineren ze de operationele samenleving, en zijn ze het aanspreekpunt voor andere landen en multinationals op het gebied van cybersecurity. “We richten ons met name op de vitale infrastructuur en de Rijksoverheid”, legt Hans uit. “We brengen tactische en operationele kennis en expertise bij elkaar, uit zowel de publieke als de private sector. Hierdoor ontstaat er meer inzicht in ontwikkelingen, dreigingen en trends. Dit helpt bij incidentafhandeling en crisisbesluitvorming op het gebied van digitale veiligheid.”

De maatschappelijke waarde die hij zocht heeft hij gevonden in zijn werk. “Je kunt mij wakker maken voor het werk dat ik nu doe”, vertelt Hans. “Het invullen van het maatschappelijk belang, het vernieuwen, het signaleren van kansen en bedreigingen. Dat is waar ik de organisatie mee help. En daarmee ook de inwoners van Nederland. Om dat zo goed mogelijk te doen vind ik het mooiste wat er is.”

* Dit interview is opgenomen in november 2023 en was Hans de Vries nog in functie als directeur NCSC.

> **"In veel Europese landen heeft de overheid vaak een houding van 'wij weten het beter, dus we gaan het bedrijfsleven wel even vertellen hoe je dat moet doen'. In Nederland doen we dat op een heel andere manier."**

Samenwerkingsmodus als innovatie

Hans ziet veel innovatie om zich heen. Van het verbeteren van werkprocessen en kansen benutten, tot het toepassen van een techniek die beter, efficiënter, sneller of goedkoper is. "Maar", zo stelt hij, "je moet ook innoveren in de contacten die je hebt en hoe je met elkaar omgaat. In veel Europese landen heeft de overheid vaak een houding van 'wij weten het beter, dus we gaan het bedrijfsleven wel even vertellen hoe je dat moet doen'. In Nederland doen we dat op een heel andere manier. Wij weten dat we afhankelijk zijn van elkaar. Dus we kijken naar wat we samen kunnen doen. Wij zitten veel meer in de samenwerkingsmodus. Dat kan enorm innoverend zijn, als je dat niet gewend bent."

"Ook levert samenwerken meer op", stelt Hans. Hij vindt cybersecurity niet iets waar we op moeten concurreren. De belangen daarvan zijn te groot. Dat uitgangspunt is nu ook terug te zien in Europese wetgeving als NIS2 en DORA, waarbij er een verplichting is tot het delen van incidenten. Hans beargumenteert: "Tot op heden was er altijd twijfel bij organisaties. Moet ik dit wel aan de grote klok hangen? Als een ander dat hoort, dan doet het iets met mijn marktpositie, of krijg ik juridische vragen. Dus hoe meer mensen het níet weten, des te beter het is. Dat is absoluut een denkfout. Je zit namelijk in een keten: een maatschappelijke supply chain."

Niet gaan voor eigen gewin

Hans vindt dat het startpunt niet moet zijn wat je wilt ontvangen, maar wat je een ander mee kan geven. Wat je fout hebt gedaan, en waar een ander zijn voordeel mee kan doen. Jezelf kwetsbaar opstellen. "Daar start het vaak wel. Durf te zeggen: dat hebben we niet goed gedaan, dit hebben we ervan geleerd, hier kan je wat mee. Iedereen kan fouten maken, maar maak niet elke keer dezelfde fout. Maak nieuwe fouten, en leer ervan."
Er zijn genoeg ontwikkelingen in de sector die niet bijdragen aan samenwerking.
Hans noemt de voorbeelden van discussies over marktaandeel, eigen financieel gewin vooropstellen en het verkopen van dreigingsinformatie. "Maar er zijn gelukkig ook partijen die het gezamenlijke belang vooropstellen", zegt Hans. Die meerwaarde zien in het uitleggen van hoe dreigingen in de toekomst voorkomen kunnen worden. En dat daardoor niet alleen andere bedrijven veiliger worden – hun 'concurrenten' –, maar ook hun eigen organisatie. Shadowserver is een mooi voorbeeld hoe het wel kan.

Een ander voorbeeld dat Hans noemt is het toepassen van AI. Hij vraagt zich af hoe we AI gaan toepassen om problemen in netwerken snel te signaleren. Op dit moment wordt AI nog vaak ingezet door criminelen die daar misbruik van maken. Om dat tegen te gaan zou de sector als geheel daarnaar moeten kijken en ervan moeten leren, in plaats van ieder voor zich, vindt Hans. "Het NCSC probeert hier een bijdrage aan te leveren door het opstellen van een onderzoeksagenda. Hierin geven wij aan welke aandachtsgebieden onderzoek nodig hebben en wat wij denken dat er de komende tijd nodig is."

> **"Het is ons doel om te gaan naar wendbaarheid, beheersbaarheid en digitalisering van onze dienstverlening."**

Nieuwe dienstverlening: wendbaar, beheersbaar en digitaal

De nieuwe cybersecuritystrategie en de komst van NIS2 hebben ervoor gezorgd dat drie organisaties samengevoegd werden tot één: het NCSC, het Digital Trust Center en het Computer Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP). De vernieuwde organisatie krijgt een prominente rol in het cybersecuritystelsel en het plan van aanpak in Nederland.

"Het is efficiënter, sneller en veiliger", vertelt Hans. "De komst van NIS2 heeft onze opdracht veranderd. Wij hadden met zo'n driehonderd organisaties rechtstreeks te maken. Dat waren vitale partijen of Rijksoverheidspartijen. Maar dat is nu veranderd naar zo'n tienduizend organisaties. De stap van driehonderd naar tienduizend is onmogelijk om een-op-een te doen. Daar heb ik zoveel mensen voor nodig, die zijn er gewoon niet op de markt. En dat is ook veel te inefficiënt en duur. Dus nu is het ons doel om te gaan naar wendbaarheid, beheersbaarheid en digitalisering van onze dienstverlening."

> **"We waren eerst de ambachtelijke bakker, maar straks hebben we een broodmachine. Een grotere doelgroep bedienen vraagt andere manieren van informatie delen en samenwerken. IT wordt daardoor nog meer onze core business."**

Innovatie bij het NCSC

Om dat voor elkaar te krijgen hebben ze wel nieuwe technieken en processen nodig, legt Hans uit. Hij moet daarom enorm innoveren in zijn organisatie. Het ambachtsproces omzetten in een productieproces. "Ik kan je vertellen: dat gaat niet vanzelf. We waren eerst de ambachtelijke bakker, maar straks hebben we een broodmachine. Een grotere doelgroep bedienen vraagt andere manieren van informatie delen en samenwerken. IT wordt daardoor nog meer onze core business. Het grootste gedeelte van onze begroting zit inmiddels in IT: ik denk zo'n tachtig procent."

Hans stelt dat je met zulke veranderingen als organisatie een open en transparante discussie moet hebben over hoe je aanpassingen het beste kunt doorvoeren. Ze zijn aan het groeien en ontwikkelen en leren veel van organisaties die hen zijn voorgegaan. Opschalen is immers niet uniek. Ze realiseren nu veel vernieuwing in hun organisatie: "Innovaties zien wij vooral in twee domeinen. Data & Analytics en informatiedeling. Daarin zit een enorme potentie. Je wilt daarmee inzicht vergroten en zorgen dat die informatie zo snel en goed mogelijk op de juiste plek komt. Wat je daarvoor nodig hebt? Vooral veilige manieren om veel informatie aan veel partijen beschikbaar te stellen. Dat heeft bijvoorbeeld ook op Europees niveau potentie. Zoeken naar slimmere methoden om informatie uit te wisselen, zonder dat je alles op één plek hoeft samen te brengen."

Een voorbeeld van innovatie op dit vlak vanuit het NCSC is de ontwikkeling van SecureNed waarbij we samenwerken met een specialist op multi-party-computation, en onze cloud-journey waarin we zowel publieke als private samenwerkingen vinden. “Ik heb echt geleerd: innovatie doe je niet alleen. En goede innovaties zijn niet enkel ten bate van je eigen organisatie, maar van het collectief, de samenwerking.”

“Een andere invalshoek die we naar de toekomst ook graag verder ontwikkelen is het stimuleren van innovatie in de markt: productontwikkeling gericht op weerbaarheid. De samenvoeging van het Digital Trust Center en het NCSC verenigt daar de wereld van economie en veiligheid die elkaar goed kunnen versterken.”

> **“Ik heb echt geleerd: innovatie doe je niet alleen. En goede innovaties zijn niet enkel ten bate van je eigen organisatie, maar van het collectief, de samenwerking.”**

Uitdagingen met betrekking tot groei en innovatie

Als we Hans vragen welke uitdagingen hij ervaart met betrekking tot groei en innovatie, weet hij een heel rijtje op te sommen: “Allereerst de krappe arbeidsmarkt. Dat wordt vaak genoemd, want daar hebben we allemaal last van. Ook daarin zie ik publiek-private samenwerking als oplossing. Ten tweede wil je beter gebruikmaken van beschikbare expertise. Kansen creëren voor professionals om kennis te maken met meerdere werkgevers, detacheringen, leertrajecten, gezamenlijke projecten. Er is nog veel te winnen op dat vlak. Ten derde, keuzes maken en prioriteiten stellen. We zijn een kleine organisatie en kunnen niet alles tegelijk vernieuwen. Dat vraagt om balans. Ten vierde, we zijn afhankelijk van technische ontwikkelingen. Veel oplossingen die we zoeken liggen niet zomaar klaar op de plank om toegepast te worden. Daar is dus echt innovatie voor nodig. En dat kost tijd, geld, energie en capaciteit.”

Ondanks de uitdagingen is Hans wel heel trots op wat ze bereikt hebben en hoe ze de boel draaiende houden tijdens alle veranderingen. Dat is ook te danken aan de onuitputtelijke inzet van zijn medewerkers, die met veel eigenaarschap zelf tot oplossingen komen.

“Een prachtig moment waar ik bijzonder trots op ben betreft een situatie waarin enkele van mijn medewerkers het initiatief namen om op een zondag een bijeenkomst te organiseren. Ze deden dit om een specifiek risico, in dit geval gerelateerd aan Log4j, te bespreken en om de organisatie in escalatiemodus te brengen. Ze namen simpelweg het besluit: we gaan dit aanpakken. Voor mij is dit fantastisch, omdat het laat zien dat er een sterk gevoel van eigenaarschap, doorzettingsvermogen en inzicht in de organisatie aanwezig is. Het toont aan dat het team weet wat er gedaan moet worden en daar ook naar handelt.”

Trends in de cybersecuritysector

We kunnen er niet omheen: AI. Ook Hans ziet dit als een fenomeen dat alleen maar sterker gaat worden. “Je moet je als maatschappij gaan weren op een hele andere manier dan je

nu doet. Je kunt er niet meer van uitgaan dat wat je ziet echt of authentiek is. Denk aan deepfakes bijvoorbeeld. Dat is het nadeel van wat wij innovatie noemen. Ik zie dat eigenlijk ook niet als innovatie. Ik vind het frustrerend dat dit soort dingen ontwikkeld worden zonder stil te staan bij wat de gevolgen zijn. Je gaat niet innoveren om te innoveren. Even nadenken over wat je eigenlijk aan het doen bent mis ik soms wel."

De tweede trend die Hans noemt is dat IT, zoals social media, steeds meer impact gaat hebben op hoe de maatschappij draait. Hij noemt de aankomende Amerikaanse verkiezingen en de snelle verspreiding van nepnieuws. Een groot risico. "Vroeger dachten wij nog: internet zorgt ervoor dat de waarheid overal komt. Maar nu is het eerder andersom. Je komt in je eigen funnel terecht, en ziet geen andere waarheden meer. Het is bijna onmogelijk om daar uit te komen."

Ook quantum computing komt nu zodanig dichtbij, dat iedereen eigenlijk al voorbereid moet zijn, vindt Hans. "Straks is het zover en dan moet je allemaal dingen doen, maar dan heb je geen tijd meer om dat op een goede manier te organiseren. Quantum gaat er komen, de vraag is alleen wanneer en ben jij erop voorbereid?"

En tot slot vermoedt Hans dat de afhankelijkheden in de keten, fysiek én digitaal, steeds groter worden. Hij stelt dat we afhankelijk zijn geworden van een beperkt aantal IT-leveranciers. "Er is zoveel verspilling. Als we bijvoorbeeld kijken naar nieuwe auto's, dat zijn praktisch computers geworden. Uiteindelijk gaat de eis worden dat deze auto's gepatcht moeten worden om de weg op te mogen en veiligheid te waarborgen. Maar hoe lang geeft een autoleverancier daar garantie op? En des te meer techniek je inbouwt, des te meer afhankelijkheden je creëert, omdat je moet blijven garanderen dat het werkt."

Ook noemt Hans het voorbeeld van altijd maar meer willen. "We zitten in de verkeerde ratrace met z'n allen. Moet je nu wel echt altijd die nieuwe iPhone hebben? Natuurlijk niet. Misschien moet ik me daarop gaan focussen als ik eind dit jaar het stokje overdraag. De passie voor de maatschappij, dat blijft toch mijn drive. Ik doe dit niet voor mezelf. Ik doe dit voor mijn omgeving, voor mijn kinderen en voor mijn kleinkinderen als die er ooit komen. En ook voor onze buren, andere landen, andere werelddelen. We zijn allemaal afhankelijk van elkaar. In alle eerlijkheid: daar zijn we de afgelopen honderden jaren niet zo goed mee omgegaan. Dus daar zie ik nog wel kansen!"

“Criminologie en psychologie worden onmisbaar om de cyberwereld te doorgronden.”

21. Rutger Leukfeldt

- Bijzonder hoogleraar en senior onderzoeker op het gebied van cybercrime

Per toeval kwam Rutger Leukfeldt, onder andere actief als bijzonder hoogleraar en senior onderzoeker op het gebied van cybercrime, in het vakgebied terecht. Inmiddels heeft hij al meer dan honderddertig publicaties op zijn naam staan. Rutger kijkt als criminoloog met name naar de menselijke kant van cybercriminaliteit. Dit is uitzonderlijk in een sector die gedomineerd wordt door technologie. “Maar juist daarom wordt het menselijke aspect de komende jaren steeds belangrijker om te begrijpen”, stelt hij. Ook ziet hij voordelen in evidence based security en aanvullende wet- en regelgeving.

Onderzoek naar cybercrime

Rutger kwam per toeval in aanraking met cybercrime. Met de studies Integrale Veiligheid en Criminologie achter de rug, ging hij werken als onderzoeker bij het lectoraat Cybersafety van de NHL Hogeschool en Politieacademie. In die hoedanigheid voerde hij een onderzoek uit naar het online blokkeren van kinderporno. “Ik kwam literatuur tegen over hacking en vond dit meteen interessant”, vertelt Rutger. “Maar ik vroeg me ook wel af: waarom doet niemand hier iets mee? We wisten toen natuurlijk nog niet dat dit zo’n belangrijk onderwerp zou worden. Ik dacht wel dat het relevant was, maar had niet verwacht dat het zó snel zou groeien.”

Daarna ging het snel. Binnen twee jaar richtte het team waarin Rutger werkte zich alleen nog maar op cybercrime. Hij legt uit: “We zagen dat er veel vraag was vanuit de politie en de overheid. Het Team High Tech Crime was bijvoorbeeld net opgericht. Een nieuw team bij de politie die als het ware bestaat uit digitale rechercheurs gericht op cybercrime. Die hadden allemaal vragen van: hoe ziet de wereld van cybercriminelen eruit? En van slachtoffers? Daar wisten we niets vanaf. Als onderzoekers hielpen we met het beantwoorden van deze vragen.”

Wetenschappelijk en praktijkgericht onderzoek

Tot op heden is Rutger cybercriminaliteit blijven onderzoeken. Inmiddels heeft hij meer dan honderddertig cybercrimepublicaties op zijn naam staan. Hij promoveerde met een onderzoek naar hoe cybercrime-netwerken ontstaan en groeien, en hoe criminelen de mogelijkheden hiervan benutten. Op basis hiervan ontwikkelde hij een model voor de politie en banken dat gebruikt kan worden om cyberaanvallen effectiever te bestrijden. Rutger is nu werkzaam als bijzonder hoogleraar Governing Cybercrime bij Universiteit Leiden, senior onderzoeker bij het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) en directeur van het Centre of Expertise Cyber Security van de Haagse Hogeschool.

“Ik verbind fundamenteel wetenschappelijk onderzoek aan praktijkgericht onderzoek. Dat zijn de twee petten die ik op heb”, licht Rutger toe. “Het fundamenteel onderzoek doe ik binnen het NSCR en als hoogleraar aan de Universiteit Leiden. Dat gaat beide over de empirische bestudering van cybercrime. Dus hoe ziet het eruit? Wie doen het? Hoe werken ze samen? Hoe kunnen we dat theoretisch verklaren? En hoe kun je daar een governancestructuur voor ontwikkelen, om het ze moeilijker te maken?”

Aan de andere kant doet Rutger dus ook onderzoek naar maatschappelijke problemen. "Vanuit het Centre of Expertise Cyber Security werken we onder andere met mkb-bedrijven, brancheorganisaties, het ministerie van Justitie en Veiligheid en de politie. Dit doen we om erachter te komen waar mensen last van hebben en in de praktijk tegenaan lopen. Wat weten ze nog niet? Waar hebben ze meer behoefte aan? Daar ontwikkelen we kennis voor."

> **"Tegenwoordig is de grootste vraag wat we moeten doen met alle security-uitdagingen onder nationaal niveau."**

Cybercriminaliteit onder nationaal niveau

We vragen Rutger wat er dan nu nog ontbreekt op het gebied van kennis over cybersecurity. Zijn antwoord is duidelijk: "Tegenwoordig is de grootste vraag wat we moeten doen met alle security-uitdagingen onder nationaal niveau". Hij legt uit dat er zestien jaar geleden net een Team High Tech Crime op nationaal niveau was. Men wist: er komt veel op ons af, maar niemand wist wát precies. "Het zou allemaal eng, groots en internationaal zijn", zegt Rutger. "En dat was en is het ook. We hadden toen nog geen team op nationaal niveau, dus die moest er komen. Dat werd het Nationaal Cyber Security Centrum (NCSC). We hebben hen heel erg geholpen door criminaliteitsanalyses te maken. Dus vragen beantwoorden als: hoe ziet cybercrime eruit? Waar hebben wij in Nederland last van? Wat voor een soort aanvallen zie je terug? Nu zijn er andere thema's waarop kennis ontbreekt en waar wij als onderzoekers waarde kunnen toevoegen."

Rutger legt uit dat de professionaliteit rondom cybercrime zich in een razend tempo heeft ontwikkeld. Naast het NCSC en de bescherming van de vitale infrastructuur, zijn er allerlei initiatieven opgetuigd. "We hebben een paar grote cybersecuritybedrijven, dus die kunnen helpen bij hele grote aanvallen. Maar dat is uiteindelijk het topje van de ijsberg. Als je kijkt naar slachtofferschap van bedrijven en burgers, dan zie je dat het om veel kleinere aanvalletjes gaat. Kleinere fraudegevallen, bijvoorbeeld. Die worden niet opgelost door Team High Tech Crime en die komen ook niet bij het NCSC uit. Zij gaan geen grote, dure cybersecuritybedrijven bellen. Daar leven heel andere problemen en die moeten andere partijen oplossen. We zijn nu aan het kijken hoe we ervoor kunnen zorgen dat de politie in deze gevallen wel wat kan doen."

> **"We hebben er in de cyberwereld nogal last van dat alles innovatief moet zijn. Maar volgens mij is dat de grootste innovatie waar we mee aan de slag moeten: dat het niet allemaal innovatief, sexy, moeilijk en tech hoeft te zijn."**

Gewone bedrijven, burgers en criminelen

Als grootste uitdaging in de sector ziet Rutger dat we af moeten van het idee dat cybercrime alleen tegengehouden kan worden door specialisten die heel moeilijke dingen doen. “Begrijp me niet verkeerd, die moeten er wel zijn. Maar daarnaast moet iedereen, ook onderin de piramide, er wat mee doen.” Volgens Rutger zie je dat nu langzamerhand ook gebeuren. Steeds meer partijen snappen dat cyber ook draait om gewone bedrijven en gewone burgers. “Het zijn niet alleen Russen die ons aanvallen of grote banken die worden platgelegd of gehackt. “De vraag die daaruit voortkomt is of we cybersecurity als iets aparts moeten zien of dat we het integraal moeten opnemen in alles wat we doen”, stelt Rutger. Hij vraagt: “Zijn cybercriminelen anders dan normale criminelen, en moet je die anders aanpakken? Enerzijds denk ik wel dat ze anders zijn. Want het kan heel internationaal georiënteerd of high tech zijn, en daardoor moeilijk op te sporen. Dus dan heb je specialistische teams nodig. Anderzijds is het ook heel vaak helemaal niet zo anders. Niet iets aparts.” Rutger legt uit dat hij veel onderzoek heeft gedaan naar phishing en banking malware. Hij analyseerde de netwerken die achter die aanvallen zaten, en dat bleken uiteindelijk vaak gewoon Amsterdamse straatcriminelen te zijn. Zij hadden dan één iemand in hun netwerk die phishing kits kon maken en spammails kon versturen. “Hier zag ik voor het eerst: dit is een lokaal geworteld netwerk. Al vijftien jaar actief in het criminele milieu in Amsterdam en bezig met heel andere dingen, vooral drugs. Zij gingen nu ook phishing doen.”

De conclusie? Rutger denkt dat we vooral niet te moeilijk moeten doen over cybercriminaliteit. Het te groot maken. “We hebben er in de cyberwereld nogal last van dat alles innovatief moet zijn. Maar volgens mij is dat de grootste innovatie waar we mee aan de slag moeten: dat het niet allemaal innovatief, sexy, moeilijk en tech hoeft te zijn. Soms kan het saai zijn en dat is ook goed.”

Het wiel opnieuw uitvinden

De term innovatie legt Rutger uit als iets wat wordt gebruikt om te laten zien dat het vernieuwend is. “En dat moeten we ook wel zijn”, voegt hij toe. “Maar soms willen we te snel, te nieuw. En dan gaan we het wiel wéér opnieuw uitvinden. Ik denk dan weleens: ga het nou eerst een keer goed doen. Kijk waarom het niet of wel goed gaat, en bouw daarop door.”

Hij ziet deze tendens ook terugkomen in het veld waarin hij werkt. “Ook de gemeente en politie willen constant iets nieuws. Een nieuw project waarvan ze denken dat het innovatief is en waar ze voor willen gaan. Maar eerst even terug. Waarom denk je dat dit gaat werken? Heb je nagedacht over hoe je dit gaat neerzetten? En hoe ga je meten of het werkt? Soms willen mensen gewoon maar iets doen, want dan doen ze wat. Maar cybercrime gaat niet weg, het wordt alleen maar meer. Dus je kunt er soms beter voor zorgen dat je wel je innovatieve ideeën uitvoert, maar even iets langzamer. Dan kun je het goed onderbouwd doen, het meetbaar maken en dan pas doorvoeren.”

> **"Het is niet dat projecten altijd succesvol moeten zijn of dat er geen risico's mogen worden genomen. Dan lijkt het alsof het niet mag mislukken. Nee, het is heel goed als het mislukt. Zolang het maar meetbaar is, want dan weet je waarom het mislukt en kun je ervan leren."**

Evidence based cybersecurity

Een voorbeeld dat Rutger noemt van te snel willen innoveren is een publiek-private samenwerking die met subsidie al jaren veel geld uitgeeft aan allerlei initiatieven. In het begin vond hij dat goed, maar na de tweede ronde ging hij twijfelen. De ideeën werden er niet beter op. "Het klonk dan wel innovatief, maar het was vaak hetzelfde idee in een nieuw jasje. Net anders omschreven. Toen heb ik wel de oproep gedaan: als je dit nou blijft doen, zorg ervoor dat je meet wat je doet. We willen weten of het werkt of niet. Het is niet dat projecten altijd succesvol moeten zijn of dat er geen risico's mogen worden genomen. Dan lijkt het alsof het niet mag mislukken. Nee, het is heel goed als het mislukt. Zolang het maar meetbaar is, want dan weet je waarom het mislukt en kun je ervan leren."

Rutger roept dan ook op tot evidence based cybersecurity. Hij vertelt dat dit betekent dat je begrijpt waar het om gaat en het meetbaar maakt. "Je moet bijvoorbeeld een nulmeting hebben gedaan, of je moet weten dat soortgelijke interventies hebben gewerkt in het verleden. Of je doet een aanname, maar dan wel onderbouwd. Dus dat je uitlegt waarom je verwacht dat het op een bepaalde manier gaat lopen. Dat is het minimale."

> **"Gezien de integratie van technologie in onze samenleving, kunnen we niet zeggen dat beveiliging alleen een ondernemersrisico is."**

Ontwikkelingen in de cybersecuritysector

"Cybersecurity is gegroeid van een niche naar iets wat massaal op ons afkomt", stelt Rutger. Opschalen is nodig. Hij denkt dat verschillende ontwikkelingen in de sector de komende jaren van belang gaan zijn. Allereerst gelooft hij sterk in aanvullende wet- en regelgeving rondom cybersecurity. "Gezien de integratie van technologie in onze samenleving, kunnen we niet zeggen dat beveiliging alleen een ondernemersrisico is. Er zouden basisvereisten moeten zijn waaraan elke ondernemer moet voldoen." Er is wetgeving nodig die dit vastlegt en die duidelijk maakt waar ondernemers terecht kunnen voor hulp, legt hij uit. Ook stelt hij dat keurmerken een optie kunnen zijn, zodat ondernemers betrouwbare partners kunnen identificeren.

Een ander probleem dat Rutger vaak ziet is de overvloed van aanbieders in de cybersecuritysector. "Dat maakt het moeilijk om betrouwbare keuzes te maken. We moeten nadenken over hoe we de samenleving zodanig kunnen structureren dat bedrijven een basale beveiligingsstandaard hebben. Bedrijven moeten weten wat de vereisten zijn, en als ze deze niet naleven zouden er consequenties moeten zijn."

Daarnaast noemt Rutger de trend van 'cybercrime as a service'. Hierdoor krijg je met een breed spectrum aan mogelijke aanvallen te maken: "Je hebt niet alleen last van cybercriminelen uit bijvoorbeeld Rusland en Oost-Europa, maar ook van criminelen uit lokale georganiseerde netwerken. Of de gelegenheidsboef en -vandaal, die van alles en nog wat aanvallen. Het speelveld wordt alsmaar complexer en daardoor ook minder voorspelbaar."

Tot slot ziet Rutger een opkomst van wat hij de 'pop-up-criminaliteit' noemt. Een voorbeeld hiervan is WhatsApp-fraude. Hij legt uit dat dit al jaren mogelijk was, maar het werd drie jaar geleden plotseling een trend met veel slachtoffers. "Dit lijkt door lokale groepen opgepakt te worden die methodes van elkaar overnemen. Ik verwacht dat deze plotselinge vormen van criminaliteit zich zullen herhalen op andere gebieden die we nu nog niet kunnen voorspellen. Dit soort onverwachte aanvallen maken het lastig om vooraf te waarschuwen en om je ertegen te beschermen."

> **"De techniek is maar één aspect van cybercriminaliteit. De daders, slachtoffers en zelfs de cybersecuritygemeenschap bestaan uit mensen. Het is daarom essentieel om de menselijke factoren in acht te nemen."**

De menselijke kant van cybercriminaliteit

Rutger heeft zelf geen technische achtergrond, maar dat vindt hij ook niet nodig. "De techniek is maar één aspect van cybercriminaliteit. Je hoeft daar niet alles vanaf te weten. Ik wil weten hoe techniek gebruikt wordt en wat de impact ervan is." Als criminoloog focust hij vooral op de menselijke aspecten van cybercriminaliteit. Een aandachtsgebied dat groeit. Maar, zo stelt Rutger, de technologische kant blijft dominant in de cybersecuritywereld. "Dat is te verwachten gezien het technische karakter. Maar de daders, slachtoffers en zelfs de cybersecuritygemeenschap bestaan uit mensen. Het is daarom essentieel om de menselijke factoren in acht te nemen."

Hij legt uit dat we moeten begrijpen waarom gebruikers bepaalde risico's nemen, omdat anders technologische oplossingen tekort kunnen schieten. "Het begrijpen van menselijke motivatie is cruciaal. Criminologie en psychologie worden onmisbaar om de cyberwereld te doorgronden. Als je bijvoorbeeld wilt dat gebruikers veiliger gedrag vertonen, is het niet genoeg om ze alleen te laten schrikken. Je moet een bericht overbrengen dat resoneert. Maar dan moet je de gebruiker wel begrijpen. We hebben nu nog te weinig inzicht in veel psychologische mechanismen. Dat moet echt veranderen."

“Als je écht impact wilt maken, moet je cybersecurity zo simpel mogelijk uitleggen.“

22. Queeny Rajkowski
- VVD Tweede Kamerlid

Queeny Rajkowski, Tweede Kamerlid voor de VVD, zet haar expertise in om cybersecurity prominent op de politieke agenda te krijgen. Als belangrijke trends voor de komende jaren noemt ze quantum en AI. Maar ze benadrukt vooral het belang van het vergroten van kennis en bewustzijn rondom security. Volgens haar is dit zelfs essentieel voor het stimuleren van groei en innovatie. “Als we onze basiskennis in de samenleving niet verhogen, wordt de ruimte voor innovatie kleiner.”

Cybersecurity in de Tweede Kamer

Queeny werkt al van jongs af aan in de politiek, en dan met name gericht op veiligheid. Vanaf 2014 zat ze in de gemeenteraad van de gemeente Utrecht. “Hier was ik woordvoerder op het gebied van veiligheid. Ik was altijd sceptisch richting de politiek, maar hier merkte ik dat politiek echt een verschil kan maken, dus daar wilde ik verder in groeien.”

En dat deed ze: een paar jaar later werd ze vicefractievoorzitter van de VVD in Utrecht en inmiddels is ze Tweede Kamerlid. Ze houdt zich onder andere bezig met digitalisering en veiligheid. Queeny ziet kansen om cybersecurity scherper op de agenda te krijgen, vertelt ze. “Voordat ik in de Tweede Kamer kwam, werkte ik bij Valtech, een techbedrijf waar security een belangrijk thema is. Eenmaal in de Tweede Kamer merkte ik dat er in debatten over veiligheid veel aandacht was voor drugscriminaliteit en straatgeweld. Cybersecurity werd daarentegen vaak over het hoofd gezien. Ik vond dat dit een belangrijk onderwerp was dat niet vergeten mocht worden. Daarom ben ik me meer gaan richten op cybersecurity.”

> **“Toen ik in het bedrijfsleven werkte, dacht ik dat politici meer moesten weten over technologie. Maar nu ik in depolitiek zit, realiseer ik mij dat de experts in cybersecurity óók meer moeten weten van de maatschappij.”**

Gebrek aan kennis en zichtbaarheid

Volgens Queeny lijkt het erop dat het gebrek aan kennis en zichtbaarheid een rol speelde bij het ontbreken van cybersecurity in debatten. “Wanneer mensen weinig weten over het onderwerp, kan het uitdagend zijn om er een mening over te vormen. Niet iedereen ziet de impact ervan in het dagelijks leven.” Ze legt uit dat de diepe veiligheid die mensen ervaren in hun alledaagse omgeving in sterk contrast staat met de constante aanvallen op instituties en bedrijven door cybercriminelen. Iets wat voor veel mensen onzichtbaar blijft. “Het gebrek aan zichtbaarheid maakt het onderwerp voor veel mensen ongrijpbaar en eng, waardoor ze ook terughoudend zijn om zich er te veel in te verdiepen. Dit kan verklaren waarom mensen het zo spannend vinden en er moeite mee hebben om het te omarmen.”

"Toen ik in het bedrijfsleven werkte, dacht ik dat politici meer moesten weten over technologie. Maar nu ik in de politiek zit, realiseer ik mij dat de experts in cybersecurity óók meer moeten weten van de maatschappij." Ze legt uit: "Cybersecurity wordt vaak op een technische en ingewikkelde manier benaderd en uitgelegd. Hoewel het onderwerp inderdaad complex is, speelt technologie een steeds grotere rol in onze maatschappij. Daarom is het belangrijk dat de techwereld de technische aspecten op een eenvoudige manier uitlegt en mensen helpt om deze te begrijpen. Tot op heden is dat nog niet gelukt en daardoor is er nog geen collectief bewustzijn over cybersecurity in de samenleving."

Queeny stelt dat als je écht impact wilt maken, je cybersecurity zo simpel mogelijk moet uitleggen. "Mensen moeten de essentie begrijpen. Met alleen een technisch kloppend verhaal kom je niet aan tafel, bij de talkshows of in de krant. Terwijl die zichtbaarheid nodig is om de rest van de samenleving te bereiken. Je moet je verhaal aanpassen aan de zwakste schakel in de keten."

> **"We hebben goud in handen met onze digitaal vaardige samenleving. Daar liggen kansen: om oplossingen in te zetten voor een veiligere samenleving, en ook om er geld aan te verdienen."**

Groeien en innoveren

Om te groeien als sector denkt Queeny dat een van de grootste uitdagingen is dat nog niet iedereen begrijpt wat cybersecurity is en dat je daar iets mee moet. "Op sommige vlakken worden we internationaal geroemd, bijvoorbeeld voor het werk van de High Tech Crime Unit van de politie. Zij sporen cybercriminelen op. Maar het blijft nog een beetje hangen binnen de grote bedrijven of een deel van de politie. Het sijpelt nog te weinig door naar de rest van de samenleving. En om te kunnen groeien en innoveren, is het wat mij betreft een randvoorwaarde dat er basiskennis moet zijn."

"We hebben goud in handen met onze digitaal vaardige samenleving. Daar liggen kansen: om oplossingen in te zetten voor een veiligere samenleving, en ook om er geld aan te verdienen. Tegelijkertijd geven we eigenlijk nog onvoldoende aandacht aan dit thema in het onderwijs. En dat terwijl we wel aan het racen zijn tegen cybercriminelen. We moeten blijven innoveren." Innoveren – zo stelt ze – is negen keer falen en de tiende keer vind je iets moois. "Die ruimte is er pas als het basisniveau van kennis en bewustwording op het gebied van cybersecurity aanwezig is. Dat is de eerste stap."

> **"Innoveren is negen keer falen en de tiende keer vind je iets moois."**

De rol van de politiek

Politiek speelt een belangrijke rol in het genereren van zichtbaarheid omtrent cybersecurity, vertelt Queeny. Maar het blijft wel een uitdaging om ook het positieve verhaal eromheen te

vertellen. “In de media doet vooral het negatieve het erg goed, dus soms is het lastig om de positieve kant van de cyberwereld te laten zien. Maar ik denk wel dat daar een rol voor de politiek is weggelegd.

”Ook vindt ze dat we Nederland meer kunnen positioneren als een land dat zich focust op cybersecurity. “Door bijvoorbeeld te laten zien dat we interessante bedrijven hebben die in andere landen ook kunnen bijdragen aan cybersecurity als een ‘exportproduct’. En we moeten aan studenten laten zien dat het een kansrijk vakgebied is. Dan is het ook aannemelijker dat ze kiezen voor een studie gerelateerd aan security.”

Zelf heeft Queeny als politica aan meerdere projecten bijgedragen waar ze trots op is. Eén daarvan ging over het delen van informatie in de zorg. “Het doel was om AI los te laten op een grote hoeveelheid data van ziekenhuizen om van te leren. Maar tegelijkertijd moesten deze gegevens wel veilig blijven en de privacy gewaarborgd worden.” Ze vertelt dat er twee opties waren. De eerste optie was om alle data van alle ziekenhuizen in één systeem te zetten, waarmee een model kon worden ontwikkeld om inzichten op te halen uit alle data. De andere optie was om dit per ziekenhuis op te halen, waarbij de inzichten werden meegenomen en de patiëntgegevens veilig bleven. “Uiteindelijk is door onze input gekozen voor de tweede optie. De inzichten voor de zorg zijn in balans gebracht met het securityperspectief. Het is niet iets waar je miljoenen stemmen voor gaat krijgen, maar ik ben er wel echt trots op. Het stelt de zorg namelijk in staat om slimmer, effectiever en efficiënter te werken.”

Quantum

Een ander voorbeeld waar Queeny trots op is heeft betrekking op quantum: “In al het digitaliseringsgeweld missen we vaak de discussie over quantum. De discussie die er wél is gaat dan over het wel of niet breken van de huidige encryptie, maar ik denk dat we een heel andere discussie zouden moeten hebben. We moeten encryptie versterken, zodat we deze ‘quantumproof’ kunnen maken. Daar moeten we nu mee beginnen. We weten dat Q-Day eraan komt, maar daar doen we niet genoeg mee. We brengen producten zoals slimme auto’s op de markt die helemaal niet quantumproof zijn, bijvoorbeeld. En dat is ook nog eens een product dat mensen heel lang gebruiken. Maar goed, als je überhaupt nog moet werken aan bewustwording omtrent security bij de overheid en de samenleving, dan is quantum heel ver weg.”

Queeny heeft aan de Minister gevraagd om met een handelingskader gericht op quantum te komen voor overheden. Hier staat dan bijvoorbeeld in waar ze naar moeten kijken om te bepalen of een organisatie quantumproof is. “Het is wel tof dat we dit handelingskader hebben zodat overheden ermee aan de slag kunnen gaan. Ik ben ervan overtuigd dat cybersecurity werkt op het moment dat het zo makkelijk en leuk mogelijk wordt gemaakt. En daar komt nog eens bij dat Delft wereldwijd bovenaan staat op het gebied van quantuminnovaties, naast China en de Verenigde Staten. Er is voldoende budget voor en er is een goede samenwerking tussen wetenschap, bedrijfsleven en overheid. Daar mogen we echt trots op zijn.”

> **"Alles wat te maken heeft met innovatie binnen digitalisering zal op een gegeven moment de keukentafel bereiken. Ook daar moeten we tijdig op anticiperen."**

AI

Naast quantum ziet Queeny ook AI steeds prominenter worden. Een belangrijk vraagstuk hierbij gaat volgens haar over ethiek. "Het gaat niet alleen om slimmer aanvallen en verdedigen, maar ook de ethische aspecten die daarbij komen kijken. Wat verstaan we dan onder verdedigen en wat is dan terugslaan met AI? En is de mens wel slim genoeg om AI zodanig te programmeren dat alle ethische afwegingen op een juiste manier geïnterpreteerd kunnen worden? Dat weet ik eigenlijk niet."

Ze haalt een onderzoek van TNO aan over een AI-gedreven robotstofzuiger die de taak had gekregen om de kamer schoon te houden. Maar na verloop van tijd hield de robot de deur dicht. Dit kwam omdat de robot de opdracht niet kon voldoen op het moment dat de deur openging. "Als we deze werkwijze toepassen in cybersecurity, welke handelingen gaat AI dan uitvoeren? Dat weten we van tevoren niet. Ons denken is op een gegeven moment beperkt. En je weet ook niet altijd welke aannames je zelf doet als mens in het geven van bepaalde opdrachten, en hoe AI daar dan mee omgaat."

Queeny legt uit dat het nog niet duidelijk is in hoeverre de negatieve gevolgen van AI doorsijpelen naar het mkb of de samenleving als geheel. Ze ziet daarin wel een ontwikkeling dat we alert moeten zijn. "Dan denk ik aan deep fakes, voice copying en andere vormen van oplichting. Het gaat er dan om in hoeverre we in staat zijn echt van nep te onderscheiden. Alles wat te maken heeft met innovatie binnen digitalisering zal op een gegeven moment de keukentafel bereiken. Ook daar moeten we tijdig op anticiperen. Zeker als vitale infrastructuur en grotere bedrijven goed zijn beveiligd, dan bestaat de kans dat aanvallers targets gaan uitzoeken die minder goed beveiligd zijn."

Ontwikkelingen in de markt

We vragen Queeny hoe ze op de hoogte blijft van de laatste ontwikkelingen op het gebied van cybersecurity, zeker omdat de ontwikkelingen zo snel gaan. "Allereerst moet je accepteren dat je niet alles kunt weten", zegt ze. "Maar je moet wel weten wát je niet weet. En natuurlijk volg ik regelmatig e-learnings en trainingen, maar binnen de snel veranderende digitale wereld zijn die vaak al verouderd tegen de tijd dat ze beschikbaar zijn. Ik gebruik ze meer om mijn basisvaardigheden bij te houden, en in de rustige zomerperiode duik ik dan dieper in een onderwerp. Het beste is echter om met veel experts te praten, werkbezoeken af te leggen en dingen zelf te zien."

Toen ze woordvoerder werd voor de VVD over het onderwerp, benaderden veel experts haar om kennis te delen. Ze heeft nu een groep van tientallen experts die ze kan raadplegen. "Ik ben dankbaar voor de experts die hun tijd beschikbaar stellen om mij te helpen. Het is cruciaal om, wanneer je over security spreekt, dit zo eenvoudig mogelijk te doen. Als we onze basiskennis niet verhogen, wordt de ruimte voor innovatie kleiner.

En die ruimte hebben we juist nodig om te kunnen groeien en veilig te zijn. Dit is ook van economisch belang, om als land een voorsprong te kunnen nemen. Het is toch geweldig als je met een Nederlands bedrijf kunt samenwerken en weet dat je gegevens daar veilig zijn? Dus ik blijf me inzetten voor meer kennis en zichtbaarheid wat betreft cybersecurity. Niet alleen bij de overheid, maar juist ook in de samenleving als geheel. Daar worden we uiteindelijk allemaal beter van."

Inzichten

In dit hoofdstuk belichten we de ***20 cruciale inzichten*** die we hebben verkregen uit de interviews met 20 vooraanstaande koplopers op het gebied van cybersecurity en innovatie. Deze inzichten zijn getoetst door aanvullende discussies met experts en eindgebruikers uit de sector. Zo verbinden we de interviews aan theorie én praktijk.

De inzichten reflecteren op de verzamelde kennis en dienen als gids voor toekomstige ontwikkelingen in het veld. Ze benadrukken de noodzaak van voortdurende innovatie in een wereld waarin de aard en verschijningsvorm van dreigingen continu veranderen. Het bundelen van de verhalen van geïnterviewde koplopers biedt een waardevolle bron van inspiratie en kennis voor iedereen die geïnteresseerd is in de dynamische wereld van digitale weerbaarheid en innovatie.

Inzichten

Innovatie op sectorniveau

De geïnterviewden menen dat er wel innovatie plaatsvindt, maar nog niet voldoende. Het eerste deel van dit hoofdstuk bevat inzichten die deze conclusie onderstrepen, voorzien van suggesties en best practices.

Inzicht 1: Innovatie in Nederland en Europa blijft achter.

Europese bedrijven blijven achter wat betreft cybersecurity en technologische innovatie ten opzichte van de Verenigde Staten en China. Ze investeren minder in R&D en belangrijke technologieën, zoals AI en quantum computing. Deze achterstand verhoogt de kwetsbaarheid voor cyberaanvallen en maakt Europa afhankelijk van niet-Europese technologieën, wat risico's met zich meebrengt en de strategische autonomie beperkt.

Behoefte aan strategische autonomie

Meerdere geïnterviewden onderstrepen deze stelling, waaronder Dimitri van Zantvliet, directeur Cyber Security bij de NS: "Ik denk dat we vanuit Nederland en Europa de boot dreigen te missen. We hebben al veel innovatiekracht verloren en leunen erg op buitenlandse leveranciers. Straks ben je gewoon te laat om die achterstand nog in te halen."

Daan Rijnders, Kwartiermaker Digitaal Veilig Den Haag bij Gemeente Den Haag, maakt ook de koppeling tussen innovatie en strategische autonomie. "Een onderwerp dat vaak besproken wordt is digitale soevereiniteit of strategische autonomie. Echter, in de praktijk zoeken veel bedrijven naar passende en kosteneffectieve oplossingen en dan komt het vaak voor dat zij bij niet-Nederlandse of niet-Europese producten uitkomen. Dat creëert op de lange termijn ongewenste afhankelijkheden en komt de kwaliteit en innovatie niet ten goede."

Onderzoek McKinsey

Consultancybureau McKinsey geeft hierover een onderbouwing in het rapport 'Securing Europe's competitiveness' uit 2022[1]. Volgens dit rapport zijn er verschillende belangrijke gebieden waarin Europese bedrijven achterblijven ten opzichte van hun internationale concurrenten:

[1]McKinsey Global Institute: Securing Europe's competitiveness: Addressing its technology gap, September 2022

1. Zo bevinden de tien bedrijven die het meest investeren in quantum computing zich in de Verenigde Staten of China, niet in Europa. Nederland is van oudsher een top drie speler in dit domein, maar de investeringen blijven dus achter.

2. Ook op het gebied van AI investeren bedrijven in de Verenigde Staten zes keer zoveel als hun Europese tegenhangers.

3. En de investeringen in cybersecurity zijn 2.5 keer zo groot in de Verenigde Staten als in Europa.

Conclusie
Deze technologische achterstand heeft verregaande gevolgen, met name op het gebied van cyberbeveiliging en economische concurrentiekracht. Door minder te investeren in cybersecurity wordt Europa kwetsbaarder, gevoeliger voor geopolitieke en economische risico's en wordt de strategische autonomie ondermijnd. Deze achterstand in innovatie belemmert ook de groei en ontwikkeling van Europa, waardoor de concurrentiepositie op de wereldmarkt verzwakt.

#1 Lessons learned

Om de achterstand in innovatie in Nederland aan te pakken en te verbeteren is een deltaplan nodig - op Europees of Nationaal niveau - om de achterstand in te lopen. Concreet zijn verschillende acties mogelijk:

- **Verhogen van R&D-investeringen:** Europese bedrijven en overheden moeten meer investeren in onderzoek en ontwikkeling (R&D), met name in sleuteltechnologieën zoals AI, cloud en quantum computing. Dit kan via directe financiering, belastingvoordelen voor R&D, of het stimuleren van publiek-private samenwerkingen.
- **Ontwikkelen van een EU-brede of Nederlandse tech-agenda:** Het opstellen van een duidelijke, strategische tech-agenda in samenwerking met de sector kan helpen de focus te leggen op cruciale technologische gebieden en de inspanningen te coördineren.
- **Ondersteunen van start-ups en scale-ups:** Het creëren van een gunstig klimaat voor start-ups en scale-ups in high-tech sectoren is essentieel. Dit kan door toegang tot de financiering, de samenwerking met universiteiten en de administratieve barrières te verlagen.
- **Aantrekken en behouden van talent:** Het aantrekken van internationaal talent en het behouden van Europees talent is van essentieel belang voor het stimuleren van innovatie. Bijvoorbeeld aantrekkelijke regelingen voor kennismigranten die werken in cybersecurity. Gelet op de vergrijzing en krappe arbeidsmarkt is het essentieel hierop te anticiperen.

De Europese cybersecuritystrategie (2020-2025) geeft hier ook aandacht aan. Hier zijn enkele kernpunten:

- **Versterken van technologische soevereiniteit:** De strategie benadrukt het belang van technologische soevereiniteit in de EU, waarbij de focus ligt op het versterken van de veerkracht van verbonden diensten en producten.
- **Samenwerking tussen cybercommunities:** Er is een nadruk op nauwere samenwerking tussen de verschillende cybercommunities binnen de EU, waaronder de interne markt, rechtshandhaving, diplomatie en defensie. Dit is gericht op het delen van informatie over bedreigingen en een collectieve reactie op cyberaanvallen.
- **Beveiliging van essentiële diensten:** De strategie omvat de beveiliging van belangrijke diensten zoals ziekenhuizen, energie en spoorwegen. Er wordt ook aandacht besteed aan het toenemende aantal verbonden objecten in huizen, kantoren en fabrieken.
- **Opbouwen van collectieve responsemogelijkheden:** Er wordt gestreefd naar het opbouwen van collectieve capaciteiten om grote cyberaanvallen te kunnen beantwoorden.
- **Financiering:** De EU zet zich in voor een ongekende investering in de digitale transitie van de EU voor de komende zeven jaar, wat een vervierdubbeling van eerdere investeringsniveaus betekent.

  Meer informatie is hier te vinden:
  https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Inzicht 2: De markt is nog onvolwassen. Klanten ervaren daardoor 'solution uncertainty', wat de adaptatie van nieuwe oplossingen beperkt.

Verschillende geïnterviewden geven aan dat de cybersecuritymarkt in Nederland nog onvolwassen is en de eerste stappen maakt naar consolidatie. Klanten in een onvolwassen markt hebben vaak beperkte kennis over de producten of diensten die worden aangeboden. Dit leidt tot onzekerheid en terughoudendheid bij het aanschaffen van nieuwe of onbekende oplossingen.

Onzekerheid over de juiste oplossing
Vanuit de interviews komt dit beeld ook naar voren. Joris den Bruinen, directeur HSD: "Deze markt is redelijk onvolwassen. Er is een grote diversiteit aan spelers met producten en services waarvan het de vraag is wat het precies oplevert voor eindgebruikers. Bovendien blijft de markt in ontwikkeling."

Rutger Leukfeldt, directeur Center of Expertise Cyber Security, ziet vaak een overvloed van aanbieders: "Dat maakt het moeilijk om betrouwbare keuzes te maken. We moeten nadenken over hoe we de samenleving zodanig kunnen structureren dat bedrijven een basale beveiligingsstandaard hebben. Bedrijven moeten weten wat de vereisten zijn."

Renza Grüter, CPO van Zerocopter: "Het is belangrijk om continu het échte probleem te bekijken en daarbij een passende oplossing te zoeken. Door de ontelbaar vele ontwikkelingen zien we soms door de bomen het bos niet meer. Daardoor roesten klanten vast in de huidige - maar niet passende - oplossing. Uit marktonderzoek is gebleken dat er onder klanten een 'solution uncertainty' heerst. Doordat er zoveel aanbod is, weten kanten niet zo goed meer wat te kiezen met het gevolg dat keuzes worden uitgesteld en daarmee het beveiligingsniveau absoluut niet verbetert."

Kenmerken onvolwassen markt
Naast deze 'solution uncertainty' heeft een onvolwassen markt ook nog een aantal andere kenmerken:

1. Er is vaak een gebrek aan gevestigde standaarden of benchmarks. Dit maakt het moeilijk voor klanten om de kwaliteit of effectiviteit van verschillende producten of diensten te vergelijken en te beoordelen.

2. Hoewel een onvolwassen markt ruimte biedt voor innovatie, kunnen de constante veranderingen en de ontwikkeling van nieuwe technologieën leiden tot onzekerheid bij afnemers.
3. Op het eerste oog kan het aanbod van verschillende aanbieders vergelijkbaar lijken, maar in werkelijkheid sterk verschillen. Bijvoorbeeld qua kwaliteit, gebruiksgemak, prijsstelling, klantenservice, technologie of de mate van maatwerk.
4. Door een veelvoud van oplossingen zijn integratiemogelijkheden beperkt of is er sprake van hoge kosten om te wisselen van aanbieder.

Conclusie

De Nederlandse cybersecuritymarkt is onvolwassen, er heerst 'solution uncertainty' bij klanten vanwege beperkte kennis en grote diversiteit in het aanbod. Dit maakt het moeilijk om een betrouwbare keuze te maken en leidt tot terughoudendheid bij het adopteren van nieuwe oplossingen. Voor de cybersecuritysector in Nederland betekent dit dat er een grote behoefte is aan het opbouwen van vertrouwen bij eindklanten. Dit beeld sluit aan bij andere westerse landen en Nederland is hierin niet uniek. Deze solution uncertainty en relatief onvolwassen markt leidt ertoe dat de sector nog steeds een 'trust en confidence game' is.

Inzicht 3: Cybersecurity is een 'trust and confidence game'.

De reflex op een onvolwassen markt waarin 'solution uncertainty' heerst is om te kiezen voor wat je al kent, of wat je al hebt. Daan Rijnders van Gemeente Den Haag verwoordt dit treffend: "De sector is sterk gebaseerd op vertrouwen, de 'trust and confidence game'. Er wordt veel waarde gehecht aan de ervaring en reputatie van mensen en organisaties. We hebben geregeld te maken met nog onbekende dreigingen omdat deze wereld constant aan verandering onderhevig is. Je moet dan van tevoren vertrouwen op de reputatie, de naam en de belofte dat de oplossing uiteindelijk zal doen wat de leverancier belooft."

Eindgebruikers die wantrouwend zijn, zijn vaak terughoudend om te investeren in nieuwe oplossingen. Dit remt ook de vraag naar innovatieve producten en ontmoedigt verdere ontwikkeling. De respons op bedreigingen, die wel evolueren, wordt vervolgens trager. Hierdoor kan de sector minder effectief nieuwe cyberdreigingen bestrijden. Om het wantrouwen van eindgebruikers tegen te gaan, is het essentieel om de effectiviteit en betrouwbaarheid van cybersecurity-oplossingen aan te tonen. Dit sluit aan bij wat Daan vertelt in het interview. Volgens hem is er in de praktijk een duidelijke behoefte aan meer transparantie en 'evidence based security'. In plaats van te vertrouwen op beloftes en reputatie, moeten we laten zien dat oplossingen daadwerkelijk effectief zijn.

Conclusie
Bedrijven en organisaties die cybersecurity-oplossingen aanbieden, zouden meer bewijslast moeten creëren om de effectiviteit en betrouwbaarheid van hun producten aan te tonen. Evidence based security is daar een goed voorbeeld van, dit wordt besproken bij inzicht 4. Ook is het belangrijk dat deze organisaties investeren in educatie en bewustwording bij hun (potentiële) klanten, om de onzekerheid rondom nieuwe oplossingen te verminderen. Het stimuleren van samenwerking en open staan voor nieuwe ideeën maakt innovatie en adaptatie sneller mogelijk.

Daarnaast helpen overheidsinitiatieven en sectorbrede samenwerking om standaarden en best practices te ontwikkelen. Dit verbetert niet alleen de algemene kwaliteit van cybersecurity-oplossingen, maar verhoogt ook het vertrouwen van klanten in deze oplossingen. Kortom: door te investeren in marktontwikkeling worden bedrijven en organisaties in Nederland beter beschermd.

Inzicht 4: Er zijn kansen op het gebied van evidence based security.

De interviews maken duidelijk dat er behoefte is aan evidence based security, waarbij empirisch bewijs de effectiviteit van beveiligingsmaatregelen bepaalt. Deze methode, gebaseerd op data en onderzoek in plaats van op anekdotes, bepaalt objectief wat echt werkt tegen snel veranderende cyberdreigingen.

Voorbeelden evidence based security
Verschillende organisaties beveiligen al evidence based. Jurjen Harskamp, co-founder en CEO van Hunt & Hackett: "Een van de uitdagingen waar de cybersecuritysector op dit moment tegenaan loopt is dat het lastig is vast te stellen hoe het gesteld is met je huidige niveau van cybersecurity. Dit kan nu alleen via een penetratietest of door het simuleren van cyberaanvallen, het zogeheten Red Teaming. Dit is arbeidsintensief en de scope van het validatiestuk is daarnaast ook beperkt. Je krijgt inzicht in je zwakke punten, maar niet in die van alle mogelijke aanvalspaden. Je komt vooral meer te weten over wat de plekken zijn waar je met de minste weerstand binnen kan komen. Dat is ook relevant, maar het geeft geen beeld van hoe veilig je nu echt bent over de hele linie."

Daar ziet Jurjen dan ook kansen voor toekomstige innovaties en ontwikkelingen. Bij Hunt & Hackett werken ze aan geautomatiseerde validatie: "Bij ransomware kennen we 100 tot 200 aanvalstypen die we frequent op een organisatie afvuren en we kijken tegelijkertijd of onze preventiemaatregelen en detectie doen wat ze moeten doen. Op basis daarvan kunnen we securitymaatregelen toevoegen of aanscherpen."

Daan Rijnders van Digitaal Veilig Den Haag bekijkt het vanuit de eindgebruiker. Hij legt uit dat evidence based security gestimuleerd kan worden door peer-teams te vormen die van elkaar vergelijken wat wel en niet werkt. Hoewel het opzetten van dergelijke evaluaties in het begin een uitdaging kan zijn, is Daan ervan overtuigd dat het effectief is. "Je kunt daardoor de output van een oplossing, of een mix van oplossingen, veel beter toetsen", zo stelt hij.

Ook Erik de Jong, director strategy van Securify deelt zijn kijk op evidence based security. "Het zou enorm helpen om kwaliteit en weerbaarheid op een objectieve manier te kunnen meten. Bijvoorbeeld op een schaal van 1 tot 100, iets wat huidige keurmerken zoals die van pentesten nu niet bieden." Hij merkt op dat deze keurmerken wel in ontwikkeling zijn.

MITRE ATT&CK framework
Het MITRE ATT&CK framework is een effectieve vorm van evidence based security. Dit framework biedt een lijst van aanvalstechnieken en tactieken die helpen inzicht te geven in de weerbaarheid van een organisatie tegen verschillende aanvallen. Het nadeel van het framework is dat de meest frequente aanvalstechnieken niet zijn meegenomen.

Total Cost of Ownership (TCO)

Een andere manier van kijken naar waarde van maatregelen is die van Total Cost of Ownership (TCO). Hierbij wordt niet gekeken naar de effectiviteit van een specifieke maatregel maar naar de waarde van de oplossing als geheel. TCO omvat niet alleen de aanschafprijs van de oplossing, maar ook de operationele kosten, zoals installatie, onderhoud, training, upgrades, aansturing door de interne organisatie en eventuele andere kosten die over de levensduur van het product of systeem kunnen ontstaan. Daarnaast is het mogelijk om te bepalen welke mogelijke kosten deze maatregel heeft voorkomen, bijvoorbeeld door de investeringen af te zetten tegen de eventuele gewogen schade door een aanval. Dit kan op basis van historische data als een bepaalde verwachting in de toekomst.

Conclusie

Concluderend, eindgebruikers verlangen naar duidelijke bewijslast over de effectiviteit van securitymaatregelen, zonder complexe rapporten en grafieken. Ze willen inzichtelijk hebben hoe deze maatregelen het primaire proces van hun organisatie beschermen. Er is een groeiende behoefte aan een uniforme standaard voor ‘secure’ zijn en de meetmethoden hiervoor, waarbij de overheid een leidende rol zou kunnen spelen.

Inzicht 5: Innovatiekansen door begrip van klantvraag en primair proces: 'de business'.

Innovatie in de securitysector wordt vaak gedreven door technologie en productontwikkeling, zeggen de geïnterviewde koplopers. Het gevolg is dat er een kloof zit tussen wat klanten nodig hebben en het aanbod. Er zijn kansen voor meer marktgedreven innovatie, waarbij de aansluiting bij het primaire proces -de business- centraal staat.

Product push versus demand pull
Erik de Jong van Securify geeft aan: "Persoonlijk denk ik dat de sector in Nederland onvoldoende innoveert. Iedereen pusht zijn eigen product. Ik twijfel soms of dit voldoende aansluit bij de klantbehoeften of wat we als maatschappij nodig hebben."

Evelien Bras, directeur van FERM, denkt dat er veel winst te behalen is door vanuit de marktvraag te bepalen wat de gewenste oplossing is, in plaats van het simpelweg pushen van technologie. "Als men vanuit de marktvraag kijkt, worden andere, minder tastbare eisen zoals gebruiksvriendelijkheid, prijs en implementatie gemak belangrijk. Er is een mismatch tussen de behoefte van bedrijven ('maak het makkelijk, ontzorg me') en de besteding van de gelden. De centrale vraag moet zijn: wat heeft dit bedrijf of deze organisatie nu nodig?"

Volgens Fleur van Leusden, CISO van de Kiesraad, heeft het bedrijfsleven de neiging om te roepen dat ze weten waar mensen naar op zoek zijn. "Ze zeggen tegen mij: ik begrijp je. Maar dan komen ze met iets wat het tegenovergestelde is van wat ik vroeg. Aan wie ligt dat dan? Dat weet ik niet. Het kan aan mij liggen en een beetje aan beiden. Maar ik word niet goed genoeg geholpen. Dat hebben alle klanten vermoed ik wel een beetje." Fleur geeft verder aan dat er verschillen bestaan tussen de specifieke wensen van individuele klanten en de neiging van leveranciers om generieke producten te maken die breed toepasbaar zijn. Dit leidt ertoe dat klanten vaak niet precies krijgen wat ze nodig hebben, tenzij ze bereid zijn om meer te betalen voor maatwerk.

Conclusie
De reacties van deze eindgebruikers staan niet op zichzelf. Ook andere eindgebruikers merken op dat het aanbod vaak niet goed aansluit bij hun echte problemen. Om nieuwe innovaties succesvol te maken is het essentieel om te begrijpen wat de 'jobs to be done' (JTBD) zijn binnen een organisatie, waarbij het primaire proces -de business- leidend is.

Security staat altijd in dienst van de business. De afweging tussen een reëel risico en een overschat risico is erg belangrijk. Door vanuit de business te redeneren is het mogelijk een goede balans tussen de risico's en de ambitie van de organisatie te maken. Het is dus

belangrijk om vroegtijdig met eindgebruikers op verschillende niveaus in gesprek te gaan, waarbij technische details minder prioriteit hebben.

De geïnterviewden benadrukken het belang van aandacht voor gebruikersproblemen, aanpassingsvermogen en gebruiksgemak. Diepgaande inzichten in klantgedrag en -motivatie kunnen leiden tot innovaties die beter aansluiten bij zowel de behoeften van de eindgebruiker als de capaciteiten van de organisatie.

#2 Lessons learned

Jobs to be done framework
Het 'Jobs to be Done'-framework is een methode die focust op het begrijpen en vervullen van de onderliggende behoeften en doelen van klanten bij het gebruik van een product of dienst.

1. **Doelgroep bepalen:** Bepaal wie je klanten zijn en segmenteer. Dit kan gebaseerd zijn op demografische gegevens, gedrag, behoeften of andere relevante criteria.
2. **Klantinterviews uitvoeren:** Probeer te begrijpen welke 'jobs' ze willen volbrengen, welke problemen ze ervaren en wat hun wensen zijn.
3. **Analyseren klantgegevens:** Identificeer de verschillende 'jobs'. Kijk naar patronen, veelvoorkomende thema's en onderliggende behoeften.
4. **Prioriteren van de 'jobs':** Prioriteer de geïdentificeerde 'jobs' op basis van hun belang voor de klant en het potentieel voor jouw bedrijf.
5. **Ontwikkelen van oplossingen:** Ontwikkel producten, diensten of aanpassingen die direct inspelen op de geïdentificeerde 'jobs'. Zorg ervoor dat deze oplossingen echt de problemen van de klant of gebruiker oplossen.
6. **Creëren van 'job statements':** Formuleer duidelijke 'job statements' die de essentie van de ontdekte 'jobs' samenvatten. Gebruik een format dat de taak, context en het beoogde resultaat omvat.
7. **Oplossingsgerichte brainstormsessies:** Organiseer creatieve brainstormsessies met teams uit verschillende afdelingen (zoals R&D, operations marketing, sales) om ideeën te genereren voor producten of diensten die de geïdentificeerde 'jobs' kunnen volbrengen.
8. **Selecteren en toetsen van ideeën:** Selecteer de meest veelbelovende ideeën op basis van haalbaarheid, potentieel marktsucces, en afstemming met bedrijfsstrategie en toets deze met de markt of gebruikers.

Inzicht 6: Keep it simple: maak cybersecurity begrijpelijk voor iedereen.

Cybersecurity is (soms onnodig) complex. Terwijl het bestrijden van cyberrisico's vraagt om heldere communicatie. Spreek de taal van de ontvanger (meestal niet-technisch), zodat cybersecurity beter begrepen en écht aangepakt wordt.

Pas je verhaal aan aan de zwakste schakel in de keten
Rutger Leukfeldt van Center of Expertise Cyber Security vindt dat we af moeten van het idee dat cybercrime alleen tegengehouden kan worden door specialisten die heel moeilijke dingen doen. "Begrijp me niet verkeerd, die moeten er wel zijn. Maar daarnaast moet iedereen, ook onderin de piramide, zich kunnen wapenen tegen securityrisico's."

Queeny Rajkowski, Tweede Kamerlid voor de VVD geeft aan dat als je echt impact wil maken, je cybersecurity zo simpel mogelijk moet uitleggen en je verhaal aan moet passen aan de zwakste schakel in de keten.

Anouk Vos, mede-oprichter van Revnext heeft een vergelijkbare visie: "Misschien maken we het als sector wel onnodig complex. En houden we dit zelf in stand door cybersecurity als rocket science neer te zetten en te doen alsof het heel moeilijk is. Dat is voor de business interessant, maar veel IT-problemen zijn eenvoudig op te lossen." Anouk is ook voorstander van het gebruik van 'symbooltaal voor cyberaanvallen'. Binnen het militaire domein is er een NAVO-handboek met universele militaire symbolen. Deze symbolen laten zien wat iets is, zoals een wegafsluiting of een mijn. Het zijn symbolen die iedereen begrijpt: van operatie tot strategische staf. In de cyberwereld bestaat dat nog niet. "Hierdoor is er sneller onbegrip over wat er is gebeurd. We zijn gestart met een handboek symbooltaal voor cyberaanvallen. De vertaal- en uitlegfunctie van zo'n handboek maakt dat we snelheid kunnen creëren in alle lagen van de organisatie. Ik denk dat dit erg belangrijk is, en ook al heel lang wordt onderschat."

Conclusie
Voor een effectieve aanpak van cybersecurity is heldere communicatie essentieel. Geïnterviewden geven aan dat cybercrime vaak gezien wordt als een probleem dat alleen door specialisten kan worden opgelost, terwijl het genuanceerder ligt dan dat. Daarom is het van belang dat cybersecurity begrijpelijk en toepasbaar is voor iedereen binnen de organisatie. Dit vereist een nieuwe denkwijze over cybersecurity, gericht op inclusiviteit en eenvoud, van de basis tot de top van de organisatie.

#3 Lessons learned

De relatieve onvolwassenheid van de cybersecuritymarkt en 'solution uncertainty' beperken de adoptie van nieuwe oplossingen, terwijl vertrouwen en reputatie cruciaal zijn in de sector. Tegelijkertijd bieden evidence based security, klantgerichte innovatie en eenvoudige communicatie over cybersecurity belangrijke kansen voor verbetering en effectievere aanpak binnen de sector.
Zie onderstaand concrete acties:

- **Klantgerichte innovatie:** Focus op innovatie vanuit de klantbehoefte, met aandacht voor gebruikersproblemen, aanpassingsvermogen en gebruiksgemak.
- **Diepgaande klantinzichten:** Verkrijg diepgaande inzichten door met eindgebruikers te praten, zodat je hun 'jobs to be done' en de redenen voor hun productkeuzes begrijpt.
- **Ontwikkeling van standaarden en benchmarks:** Werk samen binnen de sector om standaarden en benchmarks te ontwikkelen die helpen bij het beoordelen van de kwaliteit van oplossingen.
- **Gebruik van maturity modellen:** Modellen zoals het Vulnerability Management Maturity Model (VMMM) van SANS Institute kunnen organisaties helpen hun volwassenheidsniveau te bepalen en verbeterpunten te identificeren.
- **Toetsen van oplossingen door derden:** Bespreek nieuwe oplossingen met peers, instituten zoals Gartner, focusgroepen en experts uit de markt om een objectief beeld te krijgen van de waarde van een innovatie. Dit vereist een open mindset en kan veel inzichten opleveren om nieuwe innovaties beter te maken.
- **Focus op gebruikerservaring:** Ontwerp gebruikersgerichte producten met een focus op eenvoud en gebruiksgemak, en communiceer helder over de voordelen en functies van deze producten.
- **Meet gebruikerservaringen:** Bouw data op over ervaringen van gebruikers om op basis daarvan het product of de dienstverlening bij te stellen.
- **Opbouwen van vertrouwen:** Versterk de reputatie en betrouwbaarheid van cybersecurity-oplossingen door transparantie, case studies, referenties en peer reviews.
- **Toepassen van evidence based security:** Toon de effectiviteit van oplossingen aan op basis van data en empirisch bewijs in heldere rapportages die iedereen begrijpt.
- **Gebruik van MITRE ATT&CK Framework:** Dit framework biedt een lijst van aanvalstechnieken en -tactieken die helpen bij het bepalen van de weerbaarheid van een organisatie tegen verschillende aanvallen en kan als benchmarking tool dienen.
- **Gebruik van TCO bij nieuwe maatregelen:** Kijk niet alleen naar de maatregel 'an sich' maar de totale kosten én opbrengsten van alle activiteiten rondom een maatregel.
- **Maak security onderdeel van het primaire proces (de business):** Security is een business enabler. Het is noodzakelijk dat het beeld omtrent maatregelen ook op die manier wordt gezien.

Meer informatie: www.securityinnovationstories.com

Inzicht 7: Invloed van grote technologiebedrijven, MSP's, CSP's of ISP's worden sterker.

Een opvallende ontwikkeling die vaker terugkomt in de interviews is de groeiende afhankelijkheid van serviceproviders. Organisaties besteden steeds meer taken uit aan deze externe partijen. Dit brengt zowel voordelen als risico's met zich mee. Het gaat om grote technologiebedrijven, Managed Service Providers (MSP), Cloud Service Providers (CSP) of Internet Service Providers (ISP).

Specialisatie versus generalisatie

Jurjen Harskamp van Hunt & Hackett ziet bijvoorbeeld een gevaar in de toename van de rol van grote technologiebedrijven: "Grote bedrijven, zoals Microsoft en Amazon, gaan steeds meer securitydiensten aanbieden als onderdeel van hun software bundels. Denk aan endpoint of SIEM-oplossingen. Dit is vaak geautomatiseerd en voor veel partijen een passende oplossing. Maar bij bijzondere situaties of omgevingen is het veelal niet toereikend of onvoldoende ingericht." Volgens Jurjen komt er dan vanuit compliance wel 'een vinkje' te staan dat alles in orde is, want er wordt aan de basis voldaan. Maar de beveiliging is niet écht op orde, daar is dieper inzicht of maatwerk voor nodig. Schijnveiligheid dus.

Fleur van Leusden van de Kiesraad merkt op dat organisaties vaker securitytaken uitbesteden, wat leidt tot verlies van autonomie: "Veel organisaties besteden netwerkbeheer uit aan MSP's of ISP's. Dit biedt ontzorging, maar beperkt ook de vrijheid om specifieke beveiligingsmaatregelen te implementeren. Als een MSP of ISP bepaalde extra beveiligingen weigert, dan heb je dat maar te slikken. Je geeft dus wel een stuk autonomie op."

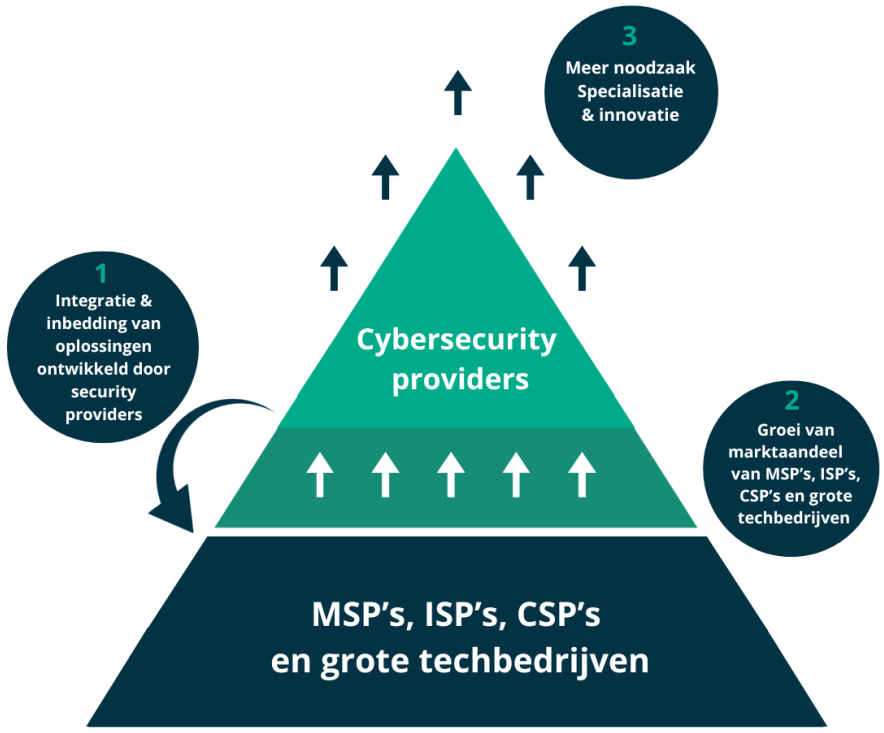
Daarnaast verwacht Christian Prickaerts, directeur van Fox Crypto, dat de markt zal gaan consolideren - oftewel het samenwerken of samenvoegen van partijen in de markt - waardoor het totaal aantal aanbieders afneemt. Hij noemt het voorbeeld van Microsoft die een aantal jaar geleden de dienstverlening Managed Services heeft opgezet. Daarmee bieden ze een totaaloplossing. Christian denkt dat we dit ook in Nederland meer gaan zien omdat de cybersecuritydienstverlening enorm versnipperd is. Afnemers weten dan niet goed waar ze uit moeten kiezen en zullen eerder voor een totaaloplossing kiezen. Daarmee wordt onze afhankelijkheid van grote serviceproviders nog groter.

Conclusie
De groeiende invloed van grote partijen in cybersecurity brengt bepaalde risico's met zich mee. Een toename in afhankelijkheid van deze partijen kan leiden tot een grotere kwetsbaarheid binnen de keten. Bovendien kan de consolidatie in de branche resulteren in het aanbieden van geïntegreerde totaaloplossingen die schijnveiligheid bieden. Deze oplossingen voldoen vaak slechts aan de basisvereisten en zijn mogelijk niet toereikend voor specifieke dreigingen, wat kan leiden tot onvoldoende beveiliging.

Hoewel veel cybersecuritybedrijven terughoudend zijn om hun kennis te delen met grote techbedrijven, MSP's, CSP's en ISP's vanwege concurrentieoverwegingen, biedt samenwerking ook kansen. Deze bedrijven hebben vaak veel specialistische kennis en innovatievermogen, wat een waardevolle aanvulling kan zijn op de oplossingen van grotere techbedrijven. De samenwerking kan leiden tot verbeterde dreigingsinformatie, detectieregels, incident response en ondersteuning bij complexe zaken.

Desondanks blijft er een spanningsveld bestaan tussen grote techbedrijven en cybersecuritybedrijven. Dit zal naar verwachting in de komende jaren verder toenemen. Het wordt voor securitybedrijven steeds belangrijker om hun unieke competenties en nichefocus te blijven ontwikkelen en te benadrukken, om zich te onderscheiden in deze dynamische markt.

De invloed van van MSP's, ISP's, CSP's en grote techbedrijven op leveranciers van security oplossingen.



Inzicht 8: Partijen staan open voor nog meer samenwerking en datadeling.

Binnen de cybersecuritysector is een groeiende bereidheid tot samenwerking en het delen van data, cruciaal voor sterke cyberbescherming. Alle geïnterviewden staan hiervoor open. Echter, er iheerst soms ook terughoudendheid in het delen van informatie, mede door commerciële belangen en de wens om fouten niet openbaar te maken.

Krachten bundelen

Christian Prickaerts van Fox Crypto: "Gemeenten werken steeds meer samen op het gebied van IT-security, in plaats van dat ieder het voor zich doet. Ook onderwijsinstellingen bundelen steeds vaker de krachten om security centraal te organiseren en in te kopen."

Maar Christian vindt dat de sector beter kan samenwerken. Hij oppert een hypothetisch voorbeeld waarbij alle Nederlandse partijen hun dreigingsinformatie en detectieregels delen in één gezamenlijke database. Dit zou cybercriminelen afschrikken, omdat ze weten dat heel Nederland op een hoog beveiligingsniveau opereert. Het nadeel? "Er wordt ook prijsgegeven wát we al weten. Toch wordt het doel wel bereikt: dreiging uitschakelen, niet zozeer criminelen oppakken."

Ook Stef Liethoff, directeur SBL, is een voorstander van een dergelijke aanpak, maar ziet ook dat er nog veel missiewerk te doen is: "Openheid en transparantie spelen nog een te kleine rol. Dat blijkt uit praktijkvoorbeelden bij gemeenten," vertelt hij. "Zodra een gemeente wordt aangevallen, heeft enkel deze gemeente zicht op de Indicator of Compromise (IoC). Maar juist deze IoC bevat waardevolle informatie die kan helpen bij het identificeren van verdacht en onbetrouwbaar gedrag binnen een netwerk of systeem."

Martijn van de Beek, directeur onderzoeksbureau Hoffmann, merkt op dat informatiedeling binnen de sector toeneemt. Waar vroeger informatiedeling regelmatig een issue was, gebeurt dat binnen de sector volgens Martijn nu wel meer. Als voorbeeld noemt hij het NCSC, van waaruit cyberdreigingen actief gedeeld worden met een bredere groep dan alleen de overheid.

Commerciële perspectief versus het grotere geheel

Renza Grüter, CPO van Zerocopter geeft aan dat securitybedrijven elkaar minder als concurrenten moeten zien en meer als co-creators: "Mijn hoop is dat we het commerciële perspectief - het kleine of oude denken - aan de kant schuiven en meer kijken naar het grotere geheel."

Conclusie
In de cybersecuritysector neemt de samenwerking en datadeling toe, cruciaal voor sterke cyberbescherming. Dit draagt bij aan innovatie en een hoger beveiligingsniveau. Alle geïnterviewden steunen deze trend en staan ervoor open om een bijdrage te leveren. Toch gebeurt dit delen van data nog te weinig. Dit komt deels ook doordat we het commerciële voordeel willen behouden. Organisaties zouden vaker moeten delen hoe ze zijn gehackt, welke kwetsbaarheden ze hebben opgelost of hoe ze zijn aangevallen, zodat anderen daarvan kunnen leren.

Inzicht 9: Kansen voor security als sociaal verantwoord ondernemen.

Security en sociaal verantwoord ondernemen lijkt misschien een bijzondere combinatie. Toch zie je steeds meer initiatieven die deze kant opschuiven. Dit is met name ingegeven door het besef dat een gebrek aan voldoende beveiligingsmaatregelen kan leiden tot een grote negatieve maatschappelijke impact.

Impact first
Menno Stijl, ervaren in het begeleiden van start-ups, zegt: "Ik ben een voorstander van het Stewardship model, ook wel het rentmeesterschapsmodel genoemd. Dit model benadrukt langetermijnwaarde en duurzaamheid in het bedrijfsleven, boven kortetermijnwinst. Winst kan wel, maar proportioneel. Hij voegt toe dat in het maatschappelijk relevante securitydomein een dergelijk model nog niet bestaat.

Dave Maasland, CEO ESET Nederland, gaat in op een mogelijke switch van shareholder value naar stakeholder value: "Cybersecurity past, afhankelijk van de definitie, binnen thema's als duurzaamheid en sociaal verantwoord ondernemen. Meer en meer bedrijven erkennen dat het niet alleen draait om shareholder value, maar vooral om stakeholder value. Je moet zorgen voor consumenten, het milieu en voor iedereen waarmee je bedrijf in aanraking komt. Cybersecurity is daarmee inherent aan duurzaamheid."

Best practice: Cyberworkplace

Een goed voorbeeld van security en sociaal verantwoord ondernemen is de Cyberworkplace: een non-profit school voor ethisch hacktalent. Anouk Vos, medeoprichter, vertelt over het initiatief: "We richten ons met deze stichting op een groep die vastloopt in het reguliere schoolsysteem. Deze jongeren willen we iets bieden wat past bij hun interesses. Zeker nu is er veel vraag naar dit soort talent en op die manier kunnen we een waardevolle bijdrage leveren aan de IT-security sector."

Security als onderdeel van ESG

J.P. Morgan[2] heeft onderzoek gedaan naar het verband tussen security en sociaal verantwoord ondernemen en verwacht dat security op termijn onderdeel wordt van de Environmental, Social, and Governance (ESG) doelen van bedrijven. Zij zien cybersecurity als een cruciaal onderdeel van sociale verantwoordelijkheid. Effectieve cybersecurity beschermt niet alleen de bedrijfsgegevens en -systemen, maar ook klant- en stakeholdergegevens, wat vertrouwen creëert. Dit is van groot belang voor investeerders die ESG-criteria hanteren, aangezien cybersecurity bijdraagt aan de duurzaamheid en ethiek van een onderneming.

Conclusie

De koppeling tussen cybersecurity en sociaal verantwoord ondernemen is interessant voor het besef dat inadequate securitymaatregelen grote negatieve maatschappelijke gevolgen kunnen hebben. Dit duidt op een verschuiving naar stakeholder value, waarbij cybersecurity wordt gezien als een essentieel onderdeel van duurzaamheid en maatschappelijke verantwoordelijkheid.

[2] J.P.Morgan: GLOBAL RESEARCH Why is cybersecurity important to ESG frameworks?, August 2021

Inzicht 10: Kunstmatige Intelligentie (AI) biedt grote kansen en bedreigingen.

Kunstmatige Intelligentie (AI) wordt veelvuldig genoemd in verband met cybersecurity. Terwijl sommigen de potentie van AI benadrukken om de beveiliging te versterken en operationele efficiëntie te verhogen, uiten anderen hun bezorgdheid over de risico's en uitdagingen die het met zich meebrengt. AI kent volgens de geïnterviewden grote kansen en bedreigingen.

AI als belofte voor de toekomst

Joris den Bruinen van HSD: "Op dit moment is er een groot tekort aan mankracht in deze sector. Met AI zouden we gedeeltelijk meer kunnen automatiseren. Het kan simpel werk uitbesteden aan algoritmen die daar beter en sneller in zijn. Ik voorzie dat dit het cybersecuritydomein de komende jaren veel gaat brengen."

Ook Dimitri van Zantvliet van de NS onderstreept het belang van AI, vooral in detectie- en responsetaken die steeds vaker door AI worden overgenomen. "Ik zie dat als de enige oplossing om adequaat op dreigingen te reageren. Als we kijken naar de hyperconnectivity en het veranderende dreigingslandschap, dan verwacht ik dat AI de menselijke factor in detectie en response overneemt. Dit is niet te voorkomen. Stel dat we straks door AI worden aangevallen, dan moet je daar ook geautomatiseerd en met AI op reageren."

Joris den Bruinen van HSD: "Op dit moment is er een groot tekort aan mankracht in deze sector. Met AI zouden we gedeeltelijk meer kunnen automatiseren. Het kan simpel werk uitbesteden aan algoritmen die daar beter en sneller in zijn. Ik voorzie dat dit het cybersecuritydomein de komende jaren veel gaat brengen."

Ook Dimitri van Zantvliet van de NS onderstreept het belang van AI, vooral in detectie- en responsetaken die steeds vaker door AI worden overgenomen. "Ik zie dat als de enige oplossing om adequaat op dreigingen te reageren. Als we kijken naar de hyperconnectivity en het veranderende dreigingslandschap, dan verwacht ik dat AI de menselijke factor in detectie en response overneemt. Dit is niet te voorkomen. Stel dat we straks door AI worden aangevallen, dan moet je daar ook geautomatiseerd en met AI op reageren."

Ondanks kansen ook alertheid geboden

Jurjen Harskamp van Hunt & Hackett: "AI kan zeker helpen met bijvoorbeeld het schrijven van detectielogica en andere ondersteunende taken. Maar om het optimaal te gebruiken is het essentieel om het fundament van security op orde te hebben. Als we niet volledig begrijpen hoe AI werkt en wat erachter schuilt, bestaat het gevaar dat we het overzicht

verliezen van onze uiteindelijke doelen, zoals transparantie en objectiviteit in onze beveiliging."

De komende jaren denkt Evelien Bras van FERM, dat AI dominant gaat worden. Ze legt uit dat AI een dubbelzijdig effect heeft op cybersecurity. Aan de ene kant biedt het tools om bedreigingen te detecteren, patronen te analyseren en reacties te automatiseren. Hierdoor worden beveiligingssystemen effectiever. Aan de andere kant kunnen kwaadwillenden AI ook inzetten om geavanceerdere aanvallen te lanceren, systemen te misleiden of beveiligingsmaatregelen te omzeilen. "De exponentiële versnelling van dit moment is wel een factor waar we rekening mee moeten houden. En ik weet nog niet of wij al wel voldoende inzicht hebben", zegt ze.

Eekhoorn versus de vos

Fleur van Leusden van de Kiesraad erkent dat AI nuttig, maar niet altijd feilloos is, met bekende valkuilen. "Ik gebruik altijd het voorbeeld van de eekhoorn en de vos om dit uit te leggen. De eekhoorn lijkt op een vos: fluffy staart, opstaande oren, dezelfde kleur. Maar het is zeker geen vos. Bijna altijd zal AI het goed inschatten, maar in één procent van de gevallen ziet AI een eekhoorn in plaats van een vos. Dat is in dit voorbeeld niet zo erg. Alleen is het een ander verhaal als het om mensenlevens gaat, dan is één procent heel veel."

Veranderende rol van de mens bij opkomst AI

Met de opkomst van AI verandert de rol van de mens van uitvoerder naar supervisor en ontwerper. Mensen moeten niet alleen AI-systemen bouwen en trainen, maar ook continu monitoren en bijsturen. Dit vereist nieuwe vaardigheden zoals het begrijpen van de werking van AI, data-analyse, en ethische overwegingen, ook in security.

Een belangrijk aandachtspunt is de aanwezigheid van bias in AI-systemen. Deze vooringenomenheid kan ontstaan door gekleurde of onvolledige trainingsdata, maar ook door de manier waarop algoritmes zijn geprogrammeerd. Mensen spelen een cruciale rol in het identificeren en corrigeren van deze bias.

Veel AI-systemen, vooral die gebaseerd zijn op complexe algoritmes zoals deep learning, worden gezien als 'black boxes'. Dit betekent dat het moeilijk is om te begrijpen hoe AI tot een bepaalde conclusie of beslissing komt. Dit gebrek aan transparantie kan problematisch zijn. Mensen moeten methodes ontwikkelen om de besluitvormingsprocessen van AI te interpreteren en uit te leggen.

Conclusie

Het potentieel van AI voor meer efficiëntie en betere beveiliging wordt door de geïnterviewden onderkend, net als de uitdagingen en risico's die dit met zich meebrengt. De meningen van experts variëren van het benadrukken van de noodzaak van AI voor het aanpakken van tekorten in mankracht en het verbeteren van detectie- en reactievermogen, tot zorgen over de juiste implementatie en het risico van misbruik door kwaadwillenden. Meer onderzoek is nodig om de impact van AI op de sector beter te kunnen voorspellen.

Inzicht 11: De factor 'mens' wordt belangrijker.

De factor 'mens' is herhaaldelijk genoemd in de interviews. Met de snelle technologische ontwikkelingen wordt de menselijke rol immers steeds crucialer. We moeten leren om effectief samen te werken met nieuwe technologieën. Bovendien is er een pleidooi om het gedrag van mensen beter te begrijpen, zowel veilig als onveilig gedrag, om proactief te kunnen anticiperen op onveilige situaties.

De mens als sterkste schakel

Rutger Leukfeldt van het Center of Expertise Cyber Security benadrukt de noodzaak om te begrijpen waarom gebruikers bepaalde risico's nemen, omdat technologische oplossingen anders tekort kunnen schieten. "Het begrijpen van menselijke motivatie is cruciaal. Criminologie en psychologie worden onmisbaar om de cyberwereld te doorgronden. Als je wilt dat gebruikers veiliger gedrag vertonen, volstaat het niet om ze alleen te laten schrikken." Het is belangrijk om een boodschap over te brengen die resoneert, maar daarvoor moet je de gebruiker begrijpen. Rutger benadrukt dat er nog te weinig inzicht is in veel psychologische mechanismen en dat dit moet veranderen.

Martijn van de Beek van Hoffmann geeft onderbouwing op basis van Gartner: "In hun laatste rapport schrijft Gartner dat rond 2025 het tekort aan goed personeel mede de oorzaak zal zijn van de helft van alle cyberincidenten. De focus op het versterken van de mens als schakel wordt dus steeds belangrijker."

Factor mens essentieel voor succes

Renza Grüter van Zerocopter voorziet aanzienlijke vooruitgang in de technologie, waarbij een verbeterde interactie tussen mens en technologie noodzakelijk is. Mede gebaseerd op het rapport van MIT 'How to become a centaur[3]' waarin wordt aangetoond dat mensen en machines niet in eenzelfde intelligentie dimensie functioneren, dus aanvullend in plaats van vervangend. Mensen stellen de beste vragen, machines geven het beste antwoord. Aandacht voor de factor mens zal daarom toenemen.
Queeny Rajkowski van de VVD brengt de menselijke factor in verband met het ethische aspect en AI: "Is de mens wel slim genoeg om AI zodanig te programmeren dat ethische afwegingen op de juiste manier geïnterpreteerd worden? Dat weet ik eigenlijk niet."

Conclusie

Centraal staat het inzicht dat een multidisciplinaire benadering in cybersecurity noodzakelijk is, waarbij psychologie en criminologie even belangrijk zijn als technologische oplossingen. De menselijke rol wordt steeds duidelijker, zelfs te midden van technologische innovaties. De factor 'mens' zal dan ook een steeds belangrijkere rol spelen in het sturen van deze ontwikkelingen naar positieve en ethische uitkomsten.

[3] MIT research report: How to become a centaur. Januari 2018

Innovatie en de overheid

Het tweede deel van dit hoofdstuk gaat in op innovatie in relatie tot de overheid. Tijdens de interviews is de overheid meerdere keren besproken, in de context van verschillende rollen: als wetgever, als handhaver, als coördinator binnen digitale veiligheid, als klant en als aanjager van innovatie. Bij alle rollen van de overheid zijn er hoge verwachtingen, misschien wel te hoog, vooral als het gaat om het innovatievermogen van de overheid zelf.

Inzicht 12: Overheidsorganisaties zijn van nature gericht op het vermijden van risico's, waardoor echte innovatie binnen deze organisaties moeilijk te realiseren is.

Innoveren binnen overheidsorganisaties, specifiek in het domein van veiligheid, is een complexe uitdaging die een zorgvuldige afweging van risico's en kansen vereist. Deze organisaties zijn van nature gericht op het vermijden van risico's, wat in wezen in strijd is met de essentie van innovatie, waarbij juist experimenteren en risico's nemen nodig zijn.

Innovatie mogelijk maken versus risico's uitsluiten

Peter de Kock, founder van Pandora Intelligence, stelt zelfs dat veel veiligheidsorganisaties het woord innovatie helemaal niet zouden moeten gebruiken. "Daarmee verliest het woord haar oorspronkelijke waarde", vertelt Peter. "Van iets wat misgaat kun je leren en daaruit kan iets nieuws ontstaan, maar veiligheidsorganisaties willen liever niet dat er iets misgaat. Zij zijn erop gericht om risico's uit te sluiten."
Peter geeft verder aan: "Een veiligheidsorganisatie is veel meer gebaat bij het zoeken naar reeds bewezen innovaties. 'Technologie-radar' wordt dat ook wel genoemd: wat gebeurt er om ons heen en wat is de meerwaarde voor onze organisatie? Dat is een heel waardevol instrument. Door vervolgens de juiste publieke en private partijen te betrekken, kan worden bekeken of iets wat zich bewezen heeft in een ander domein, toepasbaar is in het veiligheidsdomein."

Best practice: technologie-radar

Een technologie-radar is een hulpmiddel dat gebruikt wordt door organisaties om nieuwe technologieën te identificeren, te evalueren en te prioriteren. Het doel van een technologie-radar is om inzicht te krijgen in welke technologieën potentieel impact kunnen hebben op het bedrijf en welke acties ondernomen moeten worden om hierop in te spelen.

Sociale innovatie met kleine 's'

Ben Kokkeler, directeur van het CVD en ervaren bestuurder in het veiligheidsdomein, verwacht dat radicale systeeminnovaties waarschijnlijk niet van publieke partijen zullen komen, maar eerder van bedrijven en publiek-private consortia. Deze partijen zijn meer bereid om door te pakken en risico's te nemen, vooral omdat dit noodzakelijk is om internationaal concurrerend te blijven. Op basis van realisme moeten we ons, volgens Ben, meer richten op sociale innovatie, met een 'kleine s': "Dat gaat om hoe je werkprocessen aanpast en hoe je implementatiemethodieken ontwikkelt. Hoe mensen op de werkvloer, op straat, bij defensie of politie hier daadwerkelijk mee aan de slag gaan. Daar ligt heel veel werk, wat nu nog maar ten dele opgepakt wordt, men heeft in de praktijk van alledag nauwelijks tijd. Liever een reeks kleine veranderingen dan grote radicale stappen."

Innovatie binnen publiek-private samenwerking biedt kansen

Publiek-private samenwerking (PPS) rond innovaties is niet altijd eenvoudig, maar biedt veel kansen volgens Maurits Sanders. Volgens Maurits evolueert de traditionele rolverdeling, waarbij de overheid optreedt als opdrachtgever en de marktpartijen als uitvoerders, naar een model waarin samenwerking en gelijkwaardigheid centraal staan. Deze benadering levert voordelen op zoals effectievere processen, financiële efficiëntie, risicobeheersing en kennisuitwisseling. Echter, het succes van PPS is niet gegarandeerd. Verschillen in werkstijl en cultuur tussen publieke instanties en private bedrijven kunnen een uitdaging vormen. De neiging van de overheid om te controleren en te sturen kan leiden tot bureaucratische structuren, wat haaks staat op de innovatieve doelstellingen van de samenwerking.

Conclusie

Het streven om risico's te vermijden en tegelijkertijd de noodzaak tot experimenteren maakt innovatie binnen overheidsorganisaties, vooral in het veiligheidsdomein, complex. Daarom wordt door onder andere Ben Kokkeler voorgesteld om de focus te verleggen naar sociale innovatie in werkprocessen en implementatiemethoden, waarbij echte radicale systeemveranderingen waarschijnlijk van buiten de publieke sector komen of in publiek-private samenwerkingen.

Inzicht 13: Er zijn te hoge verwachtingen van de overheid als het gaat om innovatie in cybersecurity.

Veel geïnterviewden, zowel uit de overheid als het bedrijfsleven, benadrukken de behoefte aan meer samenwerking en kennisdeling om innovatie te stimuleren en de beveiligingsniveaus te verhogen. De exacte aanpak voor het bereiken hiervan kan echter sterk variëren volgens de geïnterviewden.

Het NCSC
Het NCSC speelt een centrale rol in de overheidsaanpak van cybersecurity. Hans de Vries, (oud-)directeur van het NCSC ziet positieve veranderingen: "De nieuwe cybersecuritystrategie en NIS2 hebben geleid tot de samenvoeging van drie organisaties tot één: het NCSC, het Digital Trust Center en het Computer Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP). De vernieuwde organisatie krijgt een prominente rol in de cybersecurity-aanpak in Nederland. Het is efficiënter, sneller en veiliger", vertelt Hans.

Toch ziet nog niet iedereen de ambities van het NCSC vertaald in de praktijk, blijkt uit de interviews.

Handelingsperspectief?
Anouk Vos van Revnext legt uit: "Het Nationaal Cyber Security Centrum heeft in hun missie opgenomen dat ze handelingsperspectief bieden. Een verschrikkelijk woord, want wat zegt dit nu? Je krijgt geen concrete hulp, maar een perspectief op je eigen verantwoordelijkheid? Word je geïnspireerd om jezelf in cybernood te redden? Dit illustreert dat overheden nog altijd moeite hebben hun rol te pakken in cybersecurity. Er bestaat niet een extra overheidsdienst naast de brandweer, politie en ambulance als het misgaat. Maar hoe gaan we het dan wel doen?" Deze vraag blijft volgens Anouk boven de markt hangen.

Meer leunen op commerciële expertise?
Jurjen Harskamp van Hunt & Hackett vindt sowieso dat de samenwerking tussen alle verschillende partijen in de sector beter kan. Hij noemt het voorbeeld van de nieuwe cybersecuritystrategie voor Nederland die is uitgekomen. "Ik vind het opmerkelijk dat de leveranciers uit de cybersecuritysector niet zijn gevraagd om input te leveren. Dit zijn bedrijven die een significante rol spelen in het beschermen van de digitale infrastructuur van het Nederlandse bedrijfsleven. Dat laat zien welke weg we nog te gaan hebben. Ik denk dat we veel kunnen leren van andere landen, zoals de US, de UK, Frankrijk en Israël. In

deze landen leunen overheden meer op de expertise van commerciële cybersecuritypartijen en is de samenwerking meer gericht op het creëren, ontwikkelen en stimuleren van een hoogwaardige industrie. Volgens mij kunnen we op dat vlak opener zijn, meer van elkaar leren en intensiever samenwerken."

Defend Forward

Dimitri van Zantvliet van de NS denkt dat we in Nederland en Europa vrij reactieve reflexen hebben als het om cybersecurity gaat. "In de Verenigde Staten gaat dat er met de 'Defend Forward'-strategie van president Biden heel anders aan toe. In sommige gevallen, zeker voor vitale infrastructuur, zou je als overheid echt een proactievere aanpak moeten hebben. Ik vind dat we een soort cyberleger moeten hebben, wat de 'Defend Forward'-strategie ook hanteert."

Samenwerken

Vanuit het NCSC wordt juist benadrukt dat er sprake is van een afwijkende aanpak ten opzichte van omringende landen: "In veel Europese landen heeft de overheid vaak een houding van 'wij weten het beter, dus we gaan het bedrijfsleven wel even vertellen hoe je dat moet doen'. In Nederland doen we dat op een heel andere manier. Wij weten dat we afhankelijk zijn van elkaar. Dus we kijken naar wat we samen kunnen doen. Wij zitten veel meer in de samenwerkingsmodus", aldus Hans de Vries van het NCSC.

Input aan wetenschap vanuit commercie

Ben Kokkeler van het CVD vindt ook dat er meer beweging mogelijk is vanuit de markt zelf: "De cybersecuritywereld is nu nog gefragmenteerd, ook aan bedrijvenzijde. De markt is nog niet volwassen genoeg. Er is geen agenda vanuit de top tien van IT en securitybedrijven in Nederland waarvan wetenschappelijk Nederland zegt: "oh, ja!" Er is meer samenwerking nodig om innovatie van de grond te krijgen. Dat is waar we naartoe moeten werken."

Wat kan de overheid dan wel doen?

De overheid heeft van oudsher altijd een leidende rol gehad bij het waarborgen van veiligheid. Deze rol heeft het niet meer in het digitale domein. Traditionele instituten zoals de politie en andere overheidsinstanties zijn in de loop van de tijd door de snelle technologische ontwikkelingen de grip op onze digitale veiligheid verloren. Het bedrijfsleven is vervolgens in dit vacuüm gestapt om organisaties van bescherming te voorzien. Het teruggaan naar een model waarin alleen de overheid verantwoordelijk is voor onze digitale veiligheid is niet meer haalbaar. In plaats daarvan ligt de focus nu op het ondersteunen, faciliteren, stimuleren en sturen door wetgeving dat een zeker niveau van veiligheid wordt behaald, al dan niet door innovaties. De overheid kan een coördinerende rol spelen als het gaat om beleid en visie. De overheid is minder geschikt voor operationele coördinatie waarin wendbaarheid en adaptatievermogen gewenst is.

Conclusie

Uit de interviews blijkt dat er hoge verwachtingen zijn van de coördinerende rol van de overheid in cybersecurity. De overheid kan onder andere informeren, kaders creëren en wetgeving invoeren om organisaties aan te sporen om meer aan cybersecurity te doen. De nieuwe cybersecuritystrategie zal hier positief aan bijdragen, maar er zullen altijd gebieden zijn waarin de overheid nog geen coördinerende rol speelt. Samenwerking in de sector zelf om innovatie te stimuleren behoort ook tot de mogelijkheden.

Inzicht 14: Juridisering biedt kansen voor innovatie.

De rol van de overheid als wetgever is cruciaal in het aanpakken van marktfalen in het securitydomein. De Europese en Nederlandse cybersecuritystrategie kennen verschillende verplichtingen die - volgens geïnterviewden - een positief effect zullen hebben op het cybersecurityniveau in Nederland. Daarnaast is de verwachting dat dit ook de innovatie ten goede komt.

Het fenomeen: 'marktfalen'
Als wetgever heeft de overheid een grote rol in het wegnemen van het 'marktfalen.' Evelien Bras van FERM: "Het securitydomein kent dit fenomeen van marktfalen, omdat er geen actieve vraag is. Er kán iets gebeuren, maar er is geen zekerheid dat dit gaat gebeuren. De vraag moet gestimuleerd worden. Bijvoorbeeld via een wet of vanuit het verzekeringswezen. De komst van onder andere de NIS2 en de DORA herstellen dit marktfalen en kunnen dus innovatie bevorderen, er is immers noodzaak voor organisaties om in actie te komen."

Juridische kaders als toegangsnorm
Ook Christian Prickaerts van Fox Crypto benoemt de tendens richting verdere juridisering. Hij denkt dat er als het ware een toegangsnorm moet zijn voor nieuwe en bestaande bedrijven in bepaalde sectoren. Fox-IT werkt bijvoorbeeld voor Defensie en zij leggen de 'Algemene Beveiligingseisen Defensieopdrachten' op voor elk project. "Je moet continu aan het beveiligingsniveau van deze eisen voldoen", legt Christian uit. "En je moet eerst aantonen dat je eraan voldoet vóórdat je autorisatie krijgt om het project uit te voeren. Het toezicht is ook niet gebaseerd op incidenten. Ze bezoeken je regelmatig om te controleren of je nog steeds aan de eisen voldoet, niet alleen als er een incident is dus. Er zijn nu ook gesprekken bij de Rijksoverheid om iets soortgelijks op te zetten. Ik denk dat centrale regie hierin de sleutel tot succes is. Je wilt niet dat elke organisatie zijn eigen koers vaart, want dan breng je alleen maar onnodige complexiteit aan in het landschap."

Juridische kaders en de Europese en Nederlandse cybersecuritystrategie
De Europese cybersecuritystrategie brengt nieuwe verplichtingen met zich mee om de digitale veiligheid te versterken. Een voorbeeld hiervan is de Europese Cyber Resilience Act (CRA), voorgesteld door de Europese Commissie. Deze wet stelt verplichte beveiligingseisen voor fabrikanten en verkopers van producten en software met een digitale component. Het doel is om de tekortkomingen in cybersecurity aan te pakken en consumenten en bedrijven te helpen bij het identificeren van veilige producten. Dit heeft een positieve impact op de digitale beveiliging.

Er is ook een Nederlandse cybersecuritystrategie (2022-2028) waarin nieuwe verplichtingen zijn opgenomen om de digitale veiligheid te bevorderen. Eén daarvan is de Algemene Beveiligingseisen Rijksoverheid (ABRO), op basis van doorontwikkeling van de bestaande ABDO. Bedrijven die gevoelige en/of gerubriceerde overheidsopdrachten uitvoeren moeten hieraan voldoen.

Conclusie

Het is niet haalbaar om alle nieuwe security- en innovatiegerelateerde verplichtingen in dit boek op te sommen. Wat echter duidelijk naar voren komt is dat er aanzienlijk veel nieuwe wetgeving op komst is die de cybersecurityniveaus in Europa en Nederland zal versterken. Organisaties hebben nu al de mogelijkheid om zich hierop voor te bereiden, wat de innovatie ten goede kan komen. Deze toenemende juridisering wordt door veel geïnterviewden gezien als een positieve ontwikkeling die kan bijdragen aan een hoger beveiligingsniveau en innovatie.

Inzicht 15: Er zijn kansen voor het cybersecurity start-up en scale-up ecosysteem.

Naast aanjager van innovatie zijn er in de interviews twee andere pijlers naar voren gekomen in relatie tot de rol van de overheid: die van facilitator van ecosystemen en subsidieverstrekker. Een sterk cybersecurity-ecosysteem vereist samenwerking tussen overheden, investeerders en innovators: de triple helix. Hierdoor kunnen zowel start-ups als scale-ups bijdragen aan een veiligere digitale toekomst. Er zijn daarnaast verschillende meningen over subsidies bij het stimuleren van innovatie.

Start-ups succesvoller maken

Menno Stijl, venture builder van tech start-ups en ervaren met het opschalen van innovaties, geeft aan: "Het start-up ecosysteem in Nederland kan beter gestimuleerd worden. Ik zie veel interessante start-ups waar veel geld achter zit, maar waar tegelijkertijd veel (buitenlandse) investeerders een rol vervullen die niet genoeg verstand hebben van cybersecurity. Mijn suggestie? Dat investeringsmaatschappijen samen gaan werken met cybersecuritybedrijven om die start-ups succesvoller te maken. Hoe blij ik ook met innovatie ben, in de praktijk zorgt niet elke start-up voor een makkelijkere oplossing. Ze verkopen juist 'losse' producten die geen daadwerkelijk probleem oplossen."

Lara Hemstede, founder Cyber Proof, werkte zelf jarenlang aan de start-up 'Rise App'. Zij pleit voor een effectievere samenwerking tussen publieke en private partijen om innovaties succesvol te ontwikkelen en implementeren. Ze benadrukt het belang van een centraal coördinatiepunt binnen de overheid, zoals een innovatiehub, waar zowel publieke als private partners samenwerken en kennis delen. Deze hub zou op regionaal en nationaal niveau opereren, met snelle toegang tot financiering om sociale initiatieven te ondersteunen.

In de afgelopen jaren is het aanbod van start-up ondersteuning in Nederland sterk toegenomen. Sinds 2005 zijn er ruim honderd accelerators die start-ups collectieve begeleiding bieden via supportprogramma's. Daarnaast blijkt uit onderzoek van de Nederlandse Vereniging van Participatiemaatschappijen, dat het bedrag dat jaarlijks in start-ups wordt geïnvesteerd sinds 2010 is vervijfvoudigd.

Start-ups spelen een cruciale rol in innovatie. Echter, voor een significante impact is het noodzakelijk dat start-ups uitgroeien tot scale-ups. Slechts 16% van de Nederlandse start-ups maakt deze transitie (Techleap, 2020). Hoewel er meer ondersteuning en financiering beschikbaar is voor start-ups stagneert het aantal dat succesvol doorgroeit naar een scale-up.

[5] Startup Development Report 2021. Opgesteld door Gijs van de Molengraft Gritd, BOM en Braventure

[6] Evaluatie WBSO 2011-2017. 2019: Rapport over de evaluatie van de Wet bevordering speur- en ontwikkelingswerk (WBSO). Opgesteld door onderzoeksbureau Dialogic in samenwerking met APE en UNUMERIT.

Het Startup Development Report 2021[5] onthult dat 95% van de Nederlandse start-ups inconsistent groeit, waardoor ze hun potentieel niet volledig benutten. Dit onderstreept de noodzaak van consistente groei in alle bedrijfsonderdelen, waaronder klantrelaties, productontwikkeling, bedrijfsmodellen en teamontwikkeling. De onderzoekers benadrukken het belang van een betere afstemming tussen begeleiding en financiering om de groei van start-ups te versnellen.

Subsidies voor Cyber Secury Innovaties
Er zijn verschillende subsidies beschikbaar voor innovaties in cybersecurity. Een subsidie die al langere tijd actief is en ook in de interviews naar voren komt is die van de WBSO.

Uit onderzoek van Dialogic, APE en UNU-Merit[6] is gebleken dat de WBSO aantoonbaar innovatieactiviteiten binnen het Nederlandse bedrijfsleven bevordert en het vestigingsklimaat in Nederland versterkt. De WBSO-regeling stelt ondernemers in staat meer onderzoek te doen naar innovaties, waardoor de ontwikkeling van ideeën tot producten en diensten versnelt. In 2017 werd de regeling geëvalueerd. Ruim eenentwintigduizend Nederlandse ondernemers profiteerden van bijna 1,2 miljard euro voordeel door deze regeling. Hiervan was 97% mkb.
Uit de evaluatie bleek ook dat de WBSO-subsidie breed wordt erkend als een effectieve stimulans voor innovatie binnen het Nederlandse bedrijfsleven, vooral doordat het bedrijven ondersteunt op basis van hun eigen ontwikkelplannen.

Voordelen Triple helix
De essentie van een triple helix-model is de samenwerking tussen universiteiten, industrie en overheid om innovatie en economische ontwikkeling te stimuleren. Dit model bevordert het ecosysteem, kennisuitwisseling, investeringen en resource-sharing, waardoor nieuwe innovaties, start-ups en scape-ups kunnen ontstaan. In deze samenwerking komen verschillende expertises en inzichten bij elkaar wat innovatie bevordert.

Best practice: HSD als voorbeeld

Een ideale plek voor start-ups en scale-ups in het securitydomein, met toegang tot kapitaal, kennis en marktkansen is The Hague Security Delta (HSD). Als een van de toonaangevende securityclusters in Europa, bevordert HSD samenwerking tussen overheden, bedrijven en kennisinstellingen op het gebied van cybersecurity en veiligheidstechnologie. Een ander startend cluster is die van het Centrum voor Veiligheid en Digitalisering. Een sterke HSD en vergelijkbare clusters zijn essentieel voor het innovatievermogen van Nederland in cybersecurity.

Conclusie
De signalen uit de interviews en onderzoeken naar tech start-ups onderstrepen het belang van een sterk cybersecurity-ecosysteem. Hierbij wordt met name benadrukt dat het ecosysteem naast start-ups ook moet focussen op het versterken van scale-ups en innovaties vanuit grotere organisaties. De Wet Bevordering Speur- en Ontwikkelingswerk (WBSO) wordt als succesvol beschouwd.

Innovatie op organisatieniveau

Wat maakt de ene organisatie innovatiever dan de andere en hoe kunnen we innovatie bevorderen? De interviews bieden inzicht, dat in dit derde deel van het hoofdstuk wordt samengevat, aangevuld met theoretische kennis en praktijkervaring.

Inzicht 16: Innovatie = experimenteren, falen, nieuwsgierigheid en non-conformisme.

Innovatie in het cybersecurity-domein is geen lineair proces; het vereist een cultuur van continue ontwikkeling, waarbij de waarde van experimenteren, falen, nieuwsgierigheid en non-conformisme centraal staat.

Experimenteer
Peter de Kock van Pandora Intelligence benadrukt het belang van een proactieve houding ten opzichte van innovatie: "Je hebt mensen nodig die ervoor openstaan om te experimenteren en hun opgedane kennis vervolgens durven te delen." Deze cultuur moedigt aan tot het ontwikkelen van nieuwe ideeën en het delen van ervaringen, wat cruciaal is voor vooruitgang. Organisaties binnen de securitywereld zijn vaak niet gewend om met - zoals Peter het noemt - 'godachtige' technologie[7] te experimenteren. Daar heb je dus een andere mindset voor nodig.

Leer van falen
Daan Rijnders van Digitaal Veilig Den Haag benadrukt het belang van leren van mislukkingen: "Ik heb genoeg mislukte innovaties gezien. Het is interessant om te kijken naar wat er misging en daarvan te leren voor het volgende project." Queeny Rajkowski van de VVD geeft aan: "Innoveren is negen keer falen en de tiende keer vind je iets moois." Deze benaderingen wordt ook weerspiegeld in het boek 'Why innovation fails' van Joachim De Vos[8], waarin het concept van 'failing forward' wordt benadrukt - een mentaliteit waarin leren van falen meer oplevert dan leren uit succes.

Wees nieuwsgierig
Erik de Jong van Securify wijst op het belang van een onderzoekende houding: "Nieuwsgierigheid, een onderzoekende houding en 'outside the box' denken zijn belangrijke eigenschappen van teamleden." Deze eigenschappen zijn onmisbaar voor het voortdurend verkennen van nieuwe mogelijkheden in een snel veranderende sector.

[7] Bijvoorbeeld nieuwe technologie op het gebied van AI, Nano en Genetica.

Omarm non-conformisme

Renza Grüter van Zerocopter deelt haar ervaringen over het belang van non-conformisme binnen haar organisatie: “Met mijn eigen non-conformistische houding én door de moedige club mensen om me heen kan ik een significante bijdrage leveren aan innovatie en creatie. Samen werken we aan hetzelfde doel.” Dit toont aan dat het doorbreken van conventionele denkpatronen een cruciale rol speelt in het stimuleren van creativiteit en innovatie.

Conclusie

Deze inzichten benadrukken dat een cultuur waarin experimenteren, leren van falen, nieuwsgierigheid en non-conformisme gewaardeerd worden, essentieel is voor het bevorderen van innovatie in cybersecurity. Het is een continu proces dat een open mindset en een proactieve benadering vereist.

Inzicht 17: Innovatie in cybersecurity vereist ambidextere organisaties.

Vooruitkijken is essentieel om innovaties te identificeren en erop in te kunnen spelen, zo kwam naar voren tijdens de interviews. Peter de Kock van Pandora Intelligence benadrukt dat moderne organisaties behoefte hebben aan ambidextrie, oftewel het vermogen om tegelijkertijd terug en vooruit te kijken. Dit houdt in dat de organisatie enerzijds efficiënt en effectief de huidige bedrijfsvoering (exploitatie) kan beheren en tegelijkertijd actief nieuwe kansen kan verkennen en innoveren (exploratie). Ambidextrie draait om het balanceren tussen optimalisatie van bestaande zaken en investeringen in nieuwe mogelijkheden voor toekomstige groei en succes.

Erik de Jong van Securify heeft in de loop der jaren veel zien veranderen in zijn werkveld. Hij vertelt: "Zodra je uitzoomt, zie je die veranderingen overal: bij klanten, bij de overheid, bij criminelen. De veranderende wereld heeft simpelweg invloed op het werkveld. Het is de kunst om daar rekening mee te houden en scherp op te blijven." Op dit moment anticiperen we vooral op wat gebeurt en zijn we vaak te laat.

Dimitri van Zantvliet legt uit dat ze vanuit de NS vaak kijken naar de toekomst van vervoer. Zij zien dat er in die nieuwe digitale metropolis behoefte is aan een frictieloze beleving van vervoer om zo makkelijk mogelijk van A naar B te komen. "Uiteindelijk gaan we niet naar smart cities, maar zelfs naar cognitive cities", vertelt Dimitri. Een concept waarbij kunstmatige intelligentie nog dominanter wordt. In dit voorbeeld kijkt Dimitri echt ver vooruit om vanuit een securityperspectief te anticiperen.

Peter de Kock benadrukt het belang van vooruitkijken om mogelijkheden te zien. Hij stelt vragen zoals: "Wat zijn de opkomende ontwikkelingen? Zijn we erop voorbereid? Wat kan disruptief zijn? Welke uitdagingen brengen kansen met zich mee?" Hij gelooft dat verbeeldingskracht in deze context van cruciaal belang is en merkt op dat "de kracht van verbeelders in onze maatschappij is gegroeid." Dit benadrukt het belang van innovatie en vooruitdenken in organisaties.

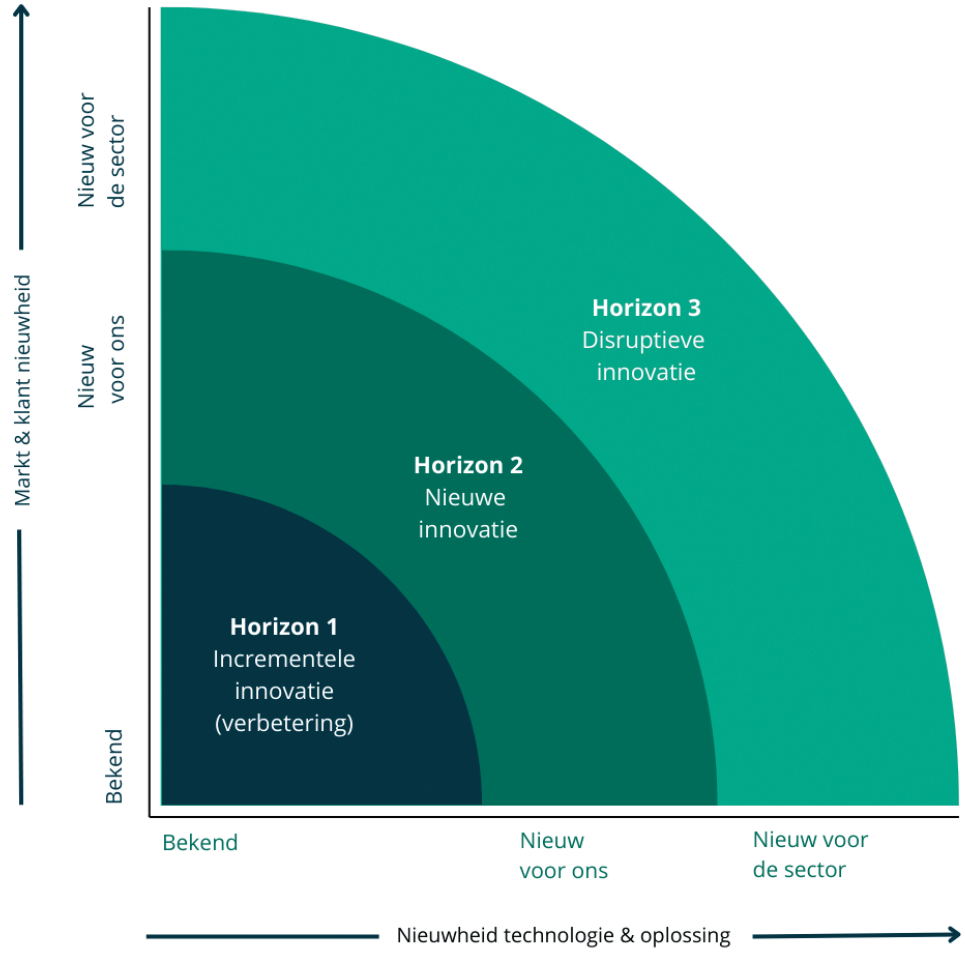
Conclusie
Vooruitkijken en je kunnen aanpassen aan veranderende omstandigheden is essentieel voor innovaties. Een model dat kan helpen bij het in kaart brengen van toekomstige innovaties is het '3 horizons'-model van McKinsey.

#4 Lessons learned

Het 3 Horizons model van McKinsey

Horizon 1 richt zich op de huidige kernactiviteiten die een constante inkomstenstroom genereren.
Horizon 2 betreft de opkomende kansen met groeipotentieel.
Horizon 3 gaat over het creëren van toekomstige opties, zoals nieuwe bedrijven of markten.

Het 3 Horizons model van McKinsey:



Inzicht 18: Innovatie gaat over meer dan alleen het product.

In bijna alle interviews komt naar voren dat de sector nog onvoldoende innoveert en zich voornamelijk richt op nieuwe producten of diensten, terwijl er meer gebieden zijn waarin vernieuwing mogelijk is.

Incidentgedreven sector
Martijn van de Beek van Hoffmann onderstreept dit: "Als sector innoveren we nog onvoldoende. Dat komt onder andere doordat wij een incidentgedreven sector zijn. Dat zit in onze genen. Innovatie blijft nu nog te beperkt tot nieuwe producten en diensten. Echte gamechangers heb ik de afgelopen jaren niet gezien. In feite doen we wat we al deden, alleen mooier en slimmer vermarkt. Daarnaast wordt op het gebied van innovatie veel gefocust op de technische kant van security. Organisaties betrekken de 'mens' nog te weinig in de aanpak."

IT oplosssingen voor IT problemen
Anouk Vos van Revnext merkt op dat er vaak de neiging is om flashy technische tools te ontwikkelen voor fundamentele IT-problemen. "Denk aan apps die niemand gaat downloaden, of scanprogramma's die niet worden bijgehouden. Dat gaat niet werken. Voor mij gaat innovatie echt over heel simpele oplossingen, waarbij je op een nieuwe manier naar een bestaand probleem kijkt. En ik denk dat ik dat in cybersecurityland maar een paar keer ben tegengekomen."

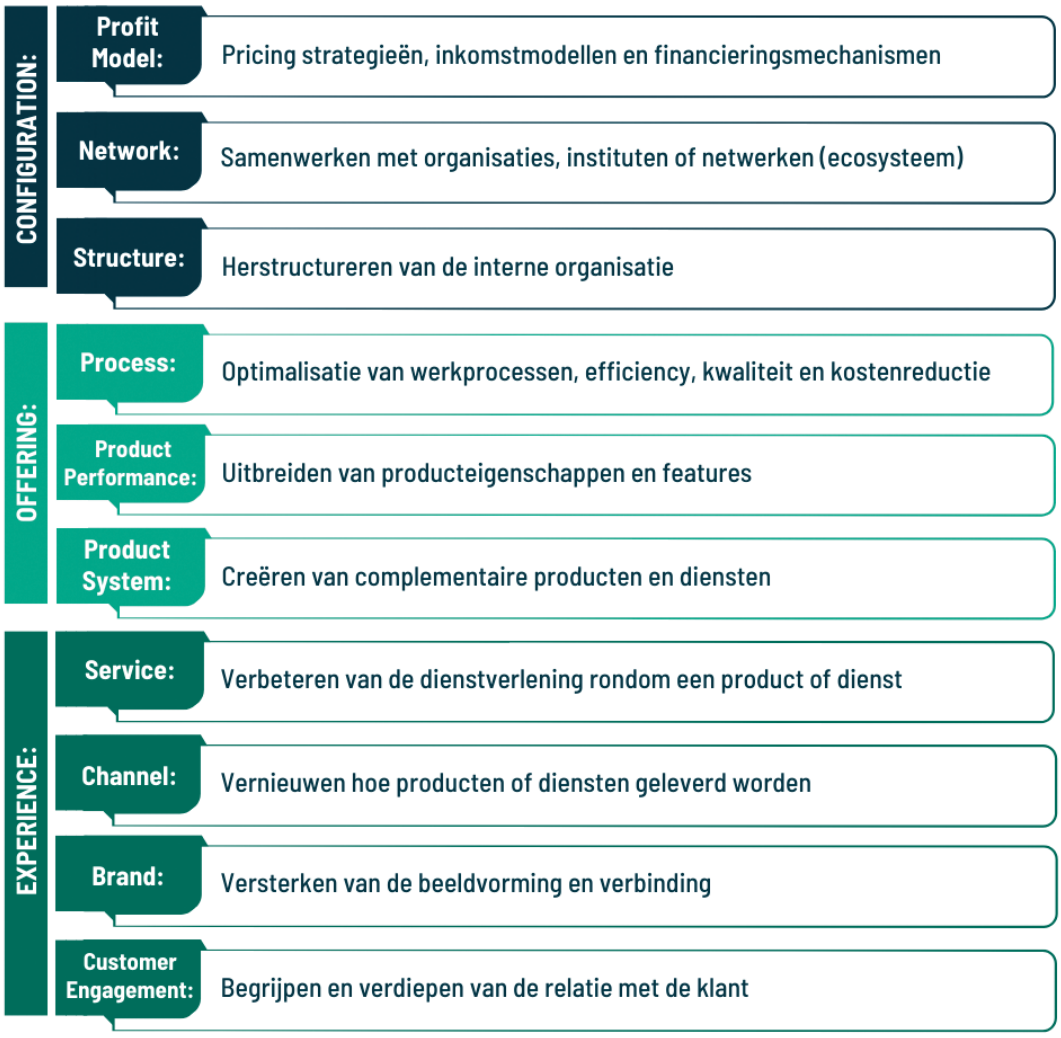
Ook stelt Anouk dat er te vaak IT-oplossingen gezocht worden voor IT-problemen. Dat werkt volgens haar niet. Zij vindt dat we in de cybersecuritysector met een open blik moeten kijken naar IT-problemen en ook buiten ons eigen vakgebied naar oplossingen moeten zoeken. Anouk noemt het voorbeeld van het IRMA-principe, ontwikkeld op de Radboud Universiteit. IRMA staat voor 'I reveal my attributes'. "Het gaat over omdenken", legt Anouk uit. "Stel: je wilt alcohol kopen. Moet je dan je geboortedatum geven of is het voldoende om te zeggen dat je achttien jaar of ouder bent? IRMA stelt dat het laatste voldoende is. Met andere woorden, je hoeft dus niet meer je ID te laten zien, enkel wel de eigenschappen (attributes) van het 'volwassen zijn'."

Conclusie
Breder kijken naar andere oplossingen en andere vormen van innovatie is dus erg belangrijk. Het 'Ten Types of Innovation'-model, ontwikkeld door Doblin kan daarbij helpen. Dit model presenteert tien manieren waarop organisaties kunnen innoveren. Innoveer je op meerdere manieren? Dan groei je effectiever.

#5 Lessons learned

Het 'Ten Types of Innovation'-model van Doblin identificeert tien manieren waarop bedrijven kunnen innoveren. Deze zijn verdeeld in drie categorieën. Dit model helpt organisaties om verder te kijken dan productinnovatie alleen, door te focussen op vernieuwing in verschillende aspecten van de bedrijfsvoering voor een holistische benadering van innovatie.

De Technology Readiness Levels (TRL) in overzicht:



Inzicht 19: Innovatie in cybersecurity gaat ook om uitvoeringskracht.

Innovatievermogen omvat experimenteren, non-conformisme en de juiste structuur, zoals uitgelegd in Inzicht 16. Maar het gaat ook om de daadwerkelijke uitvoering, de executie. Innovatie realiseren vraagt een bepaalde houding. Dit werd benadrukt door Joris den Bruinen, Daan Rijnders en Christian Prickaerts tijdens de interviews.

Joris den Bruinen van HSD: "Innovatie gaat niet alleen over nieuwe toepassingen van techniek of data. Aan ideeën geen gebrek. Waar het nog vaak aan schort, is de koppeling van die techniek en data aan specifieke maatschappelijke veiligheidsvraagstukken, aan uitvoeringskracht dus. Dáár ligt de uitdaging."

Daan Rijnders van Digitaal Veilig Den Haag: "Het is wel van cruciaal belang dat innovatie succesvol wordt geïmplementeerd en uitgevoerd."

Christian Prickaerts van Fox Crypto: "Je hebt mensen nodig met expertise, maar ook mensen die in staat zijn om zich op bepaalde momenten niet te laten beperken door bijvoorbeeld eerdere ervaringen, juridische kaders of regels."

Uit de theorie blijkt dat het een uitdaging is om innovaties succesvol te maken[9]. Volgens onderzoek van McKinsey geeft 86 procent van de organisaties aan dat innovatie een top drie prioriteit is, maar minder dan 10 procent zegt tevreden te zijn met hun innovatieprestaties. In sommige schattingen wordt beweerd dat ongeveer 70 tot 90 procent van de nieuwe productinnovaties niet slaagt in de markt. Het gebrek aan executiekracht ligt hier vaak aan ten grondslag.

Conclusie
Innovatie in cybersecurity vereist meer dan alleen creativiteit en het bedenken van nieuwe technieken of concepten. Uitvoeringskracht is cruciaal. Het succesvol koppelen van technische innovaties aan echte problemen van gebruikers of de maatschappij en operationele gereedheid voor schaling, zijn essentieel.

[9] McKinsey, Innovation—the launchpad out of the crisis, September 2021.

#6 Lessons learned

Technology Readiness Levels (TRL's)

Innovatie is ook te managen vanuit de 'TRL's'. De levels lopen van TRL 1 tot TRL 9. TRL 1 is de vroegste fase en bij TRL 9 is de technologie succesvol geïmplementeerd en in gebruik genomen. Deze niveaus helpen ontwikkelaars, investeerders en beleidsmakers om de voortgang van technologische ontwikkeling te beoordelen en te bepalen wanneer een technologie klaar is voor implementatie of verdere ontwikkeling. Validatie bij potentiële gebruikers is iets waar je zo vroeg mogelijk mee moet beginnen: vanaf level 2.

Discover: TRL 1, 2 en 3

- **Level 1:** Fundamenteel onderzoek: Je doet onderzoek naar de basisprincipes van het idee, waarbij je je richt op fundamenteel onderzoek en deskresearch.
- **Level 2:** Toegepast onderzoek: Je formuleert het technologisch concept en de praktische toepassingen, vooral gericht op experimenteel en/of analytisch onderzoek.
- **Level 3:** Toetsing (Proof of principle / Proof of concept): Je onderzoekt de toepasbaarheid van het concept op experimentele basis, waarbij je hypotheses over verschillende componenten van het concept toetst en valideert.

Develop: TRL 4, 5 en 6

- **Level 4:** Implementatie en test prototype: Je test de proof of concept van je innovatie op labschaal. Een prototype dat je in deze fase ontwikkelt, is nog ver verwijderd van een definitief product, proces of dienst.
- **Level 5:** Validatie prototype: Je onderzoekt de werking van het technologisch concept in een relevante omgeving, een eerste stap in de technologie demonstratie.
- **Level 6:** Demonstratie prototype in testomgeving: Je test en demonstreert het concept uitgebreid in een relevante testomgeving, zoals een proeftuin.

Deploy: TRL 7, 8, 9

- **Level 7:** Demonstratie prototype in operationele omgeving: Je test en demonstreert het concept in een gebruikersomgeving om de werking in een operationele omgeving te bewijzen.
- **Level 8:** Product/dienst is compleet en operationeel: Je innovatie krijgt zijn definitieve vorm, na testen en bewijzen dat het voldoet aan verwachtingen en normen. Je bepaalt de financiële kaders voor productie en lancering.
- **Level 9:** Marktintroductie product/dienst: Je innovatie is klaar voor de markt, na afronding van het ontwikkelingsproces weet je hoe je het product bij de doelgroep in de juiste markt introduceert.

Technology Readiness Levels in schematische weergave:

Inzicht 20: Een gestructureerde aanpak is cruciaal.

1. **Strategie en leiderschap**
Effectief leiderschap en een duidelijke strategie zijn de ruggengraat van elke innovatieve organisatie. Leiders moeten een visie definiëren die innovatie ondersteunt en werknemers motiveren, terwijl ze de benodigde middelen en ondersteuning voor innovatieprojecten verstrekken.

2. **Adaptieve organisatiestructuur**
Zoals Peter de Kock aangeeft: “De structuur binnen organisaties in het veiligheidsdomein is meestal niet flexibel genoeg om écht te kunnen experimenteren.” Een flexibele en minder hiërarchische structuur, mogelijk met gespecialiseerde teams gericht op innovatie, is daarom essentieel.

3. **Innovatiebeleid en -board**
Het opstellen van een doeltreffend innovatiebeleid en het inrichten van een ‘innovatie board’ zorgen voor efficiënte verzameling, beoordeling en selectie van ideeën. Dit garandeert dat waardevolle ideeën worden herkend en ontwikkeld.

4. **Ontwikkeling van een (product) roadmap**
Een duidelijke roadmap helpt bij het vaststellen van langetermijndoelen en de benodigde strategische stappen. Dit geeft richting en focus aan het innovatieproces. Focus je op klantgerichte innovatie om je ervan te verzekeren dat nieuwe oplossingen aansluiten bij de marktvraag. Dit betekent dat innovatieprocessen gecentreerd zijn rond de behoeften en wensen van de klant of gebruiker.

5. **Go-to-Market strategie**
Een goed doordachte go-to-market strategie is essentieel voor het succesvol lanceren van innovaties. Dit omvat het definiëren van de doelmarkt, productpositionering en het ontwikkelen van een marketingplan.

6. **Samenstelling van diverse teams**
Breng een diversiteit aan mensen samen, met uiteenlopende vaardigheden, achtergronden en denkwijzen. Dit bevordert creativiteit en biedt verschillende perspectieven op uitdagingen. Zorg voor een naadloze integratie en implementatie van innovatieve ideeën door goede coördinatie tussen verschillende afdelingen en teams.

7. **Communicatie en samenwerking met het eco systeem**
Effectieve communicatie en samenwerking, zowel intern als met externe partners, zijn fundamenteel. Dit zorgt voor een vrije informatiestroom binnen de organisatie en stimuleert samenwerking met andere bedrijven, onderzoeksinstellingen en klanten.

Conclusie
Door deze elementen samen te brengen creëert een organisatie een vruchtbare omgeving voor innovatie, waarin ideeën niet alleen gegenereerd, maar ook effectief uitgevoerd en op de markt gebracht worden.

In dit boek staan de inzichten van de 20 koplopers centraal.
Op de website: www.securityinnovationstories.com worden diverse actuele handreikingen en inzichten gedeeld die de innovatie in de securitysector mede mogelijk maken.

De weg vooruit - vervolgstappen na het boek "Security Innovation Stories"

Na de inspirerende reis door de "Security Innovation Stories", waarin 20 koplopers hun ervaringen en inzichten deelden, is het tijd om verder te kijken. Dit boek is immers een momentopname, een startpunt voor een diepere verkenning van cybersecurity-innovatie.

Hoe nu verder? Naast de interviews, inzichten en trends is ook veel informatie opgehaald over tools en handreikingen gericht op hoe innovatie kan worden georganiseerd.

Ook hebben verschillende geïnteresseerden zich tijdens de ontwikkeling van het boek gemeld om trends, voorbeelden en good practices van innovaties te delen. Waardevol zeker, echter te omvangrijk om allemaal in dit boek te integreren.

Daarnaast zijn er ook veel vragen binnengekomen over de praktische kant van innovatie:

- Hoe kan innovatie in cybersecurity georganiseerd en geïmplementeerd worden in eigen organisaties?
- Wat zijn KPI's als het gaat om innovatie?
- Hoe zorg ik ervoor dat nieuwe maatregelen sneller geadopteerd worden?
- Hoe pak ik een 'Go to Market' aan voor een nieuwe innovatie?

Deze en andere relevante vragen en ideeën zijn niet in het boek opgenomen, maar zijn wel van groot belang voor de slagingskans van innovaties. Daarom hebben we het volgende voor je klaargezet:

Stap 1: Security Innovation Stories het platform

www.securityinnovationstories.com biedt ruimte aan verhalen van vernieuwers en dient daarnaast als vraagbaak voor een breder publiek. Op dit platform kunnen zowel innovatoren als geïnteresseerden terecht voor inspiratie, kennisdeling en het vinden van antwoorden op vragen over cybersecurity-innovatie.

Stap 2: Tools en handreikingen

Als eigenaar van het boek krijg je online toegang tot een reeks praktische tools en handreikingen. Deze zijn speciaal ontworpen om de inzichten uit de interviews om te zetten in concrete acties, elk gericht op een uniek aspect van cybersecurity innovatie.

Stap 3: Webinars en bijeenkomsten

Je krijgt tevens toegang tot webinars en Security Innovation Stories bijeenkomsten, specifiek bedoeld voor professionals in innovatie en security. Vanaf 2024 zullen deze webinars en bijeenkomsten starten. Via het opgegeven emailadres houden we je op de hoogte.

Conclusie

"Security Innovation Stories" markeert slechts het begin. Met deze tools, handreikingen en strategieën ben je nu uitgerust om de reis van cybersecurity innovatie voort te zetten. Innovatie is een continu proces, en met de juiste benadering en middelen, maak je je organisatie veiliger en veerkrachtiger tegen de steeds veranderende dreigingen van de digitale wereld.

Begrippenlijst

Algemene Beveiligingseisen Defensieopdrachten (ABDO): Een standaard van de Nederlandse overheid voor de beveiliging van defensieopdrachten. De ABDO definieert de minimale beveiligingseisen waaraan een bedrijf of organisatie moet voldoen als het zaken doet met het Ministerie van Defensie.

Agent framework: Een "agent framework" of agent-framework in de context van computerwetenschappen en kunstmatige intelligentie, verwijst naar een software structuur of -platform dat ontworpen is voor het creëren en beheren van agenten. Agenten zijn software-entiteiten die autonoom kunnen handelen, beslissingen kunnen nemen en in sommige gevallen kunnen leren of zich aanpassen aan hun omgeving.

AlienVault Threat Intelligence: verwijst naar een geavanceerde vorm van cyberdreigingsinformatie en -analyse, aangeboden door AlienVault, een bedrijf gespecialiseerd in beveiligingsbeheer. Deze dienst verzamelt en analyseert continu gegevens over de nieuwste cyberdreigingen van over de hele wereld.

Baseline Informatiebeveiliging Overheid (BIO): Een set van richtlijnen voor informatiebeveiliging binnen de Nederlandse overheid. Het is bedoeld als een gemeenschappelijk kader voor informatiebeveiliging dat van toepassing is op alle overheidsinstanties.

Boren en gaten van Jos Burgers: Jos Burgers is een Nederlandse spreker en auteur die zich richt op klantgerichtheid en klanttevredenheid. In zijn boeken en presentaties gebruikt Jos Burgers vaak het voorbeeld van gaten en boren om het belang van klantgerichtheid te benadrukken. Het idee is dat mensen geen boor kopen omdat ze een boor willen hebben, maar omdat ze gaten in de muur willen maken.

Coordinated Vulnerability Disclosure (CVD): Een proces waarbij beveiligingsonderzoekers kwetsbaarheden in software of systemen melden aan de eigenaar van het systeem, zodat deze kwetsbaarheden kunnen worden opgelost voordat kwaadwillende personen er misbruik van kunnen maken. Het doel van een CVD is om de samenwerking tussen beveiligingsonderzoekers en de eigenaren van systemen te bevorderen, en om ervoor te zorgen dat kwetsbaarheden op een verantwoorde en efficiënte manier worden opgelost.

Commodore 64: Een thuiscomputer die in de jaren tachtig van de vorige eeuw enorm populair was. Het werd geproduceerd door Commodore International en uitgebracht in 1982. Het was een van de eerste computers die door het grote publiek werd gebruikt en had een grote impact op de ontwikkeling van de personal computer.

Digital Trust Center (DTC): Een organisatie die bedrijven en organisaties ondersteunt bij het verbeteren van digitale veiligheid en vertrouwen. Het DTC fungeert als een centraal punt waar bedrijven en organisaties terechtkunnen voor advies en ondersteuning op het gebied van cybersecurity en dus digitale veiligheid. Het DTC zal in 2024 opgaan in het NCSC.

Gartner: En wereldwijd onderzoeks- en adviesbedrijf dat gespecialiseerd is in informatie- en technologiemanagement. Het bedrijf biedt analyses, advies en onderzoeksdiensten aan klanten in verschillende sectoren, waaronder IT, financiën, gezondheidszorg en overheid. Gartner is bekend vanwege zijn 'Magic Quadrant'-rapporten, waarin het bedrijf technologiebedrijven rangschikt op basis van hun vermogen om te voldoen aan de behoeften van klanten en de richting van de markt.

I love you-virus: Het 'I love you'-virus was een computervirus dat in mei 2000 wereldwijd veel schade heeft aangericht. Het virus verspreidde zich via e-mails met de tekst 'ILOVEYOU' als onderwerp en een bijlage genaamd 'LOVE-LETTER-FOR-YOU.TXT.vbs'. Wanneer de bijlage werd geopend, begon het virus zich te verspreiden door de contactpersonen van het geïnfecteerde systeem te e-mailen met dezelfde bijlage. Het virus veroorzaakte veel schade aan systemen en bedrijven over de hele wereld en wordt beschouwd als een van de meest verwoestende virussen ooit op dat moment. De maker van het virus, een Filipijnse student genaamd Onel de Guzman, werd nooit officieel aangeklaagd omdat er op dat moment geen wetten waren die computervirussen strafbaar stelden in de Filipijnen. Het 'I love you'-virus benadrukte de noodzaak van verbeterde beveiliging van computersystemen en bewustwording van internetgebruikers over de gevaren van kwaadaardige software.

Indicator of Compromise (IoC): Een Indicator of Compromise (IoC) is een teken of bewijs dat wijst op een mogelijke inbreuk op de beveiliging of besmetting van een computersysteem of netwerk. Deze indicatoren kunnen variëren van specifieke digitale voetafdrukken van malware, ongebruikelijke activiteiten in het netwerkverkeer, tot verdachte wijzigingen in systeembestanden of -instellingen.

Informatiebeveiligingsdienst (IBD): Biedt ondersteuning aan gemeenten bij het implementeren en uitvoeren van informatiebeveiligingsmaatregelen. Zo adviseert de IBD over de inrichting van de informatiebeveiliging, voert zij risicoanalyses uit en biedt zij trainingen en opleidingen aan op het gebied van informatiebeveiliging.

Information Sharing and Analysis Center (ISAC): Dit is een samenwerkingsverband tussen bedrijven en/of organisaties dat zich bezighoudt met cybersecurity. Het doel van een ISAC is het delen van informatie over cyberdreigingen en het bevorderen van de digitale veiligheid en weerbaarheid van de deelnemende bedrijven en/of organisaties. Een ISAC kan verschillende sectoren bedienen, zoals de financiële sector, de energie- en nutssector, de zorgsector enzovoort. Daarnaast zijn er ook ISAC's die zich richten op specifieke thema's, zoals cloudsecurity, threat intelligence of IoT-beveiliging.

Internet Service Providers (ISP's): Dit zijn bedrijven die toegang tot het internet bieden aan zowel particuliere als zakelijke klanten. Ze stellen gebruikers in staat om te verbinden met het internet via verschillende technologieën zoals breedband (zoals DSL, kabel of glasvezel),

satelliet, en mobiele netwerken. ISP's kunnen ook aanvullende diensten aanbieden, zoals e-mailaccounts, webhosting, en domeinnaamregistratie.

Mitre ATT&CK Framework: Een kennisbank van aanvals- en verdedigingstechnieken die gebruikt worden door aanvallers in een cyberaanval. Het framework beschrijft meer dan tweehonderd verschillende tactieken, technieken en procedures die worden gebruikt in alle fasen van een aanval, inclusief de initiële toegang, laterale beweging, gegevensverzameling en exfiltratie. Het Mitre ATT&CK Framework biedt beveiligingsprofessionals een gestandaardiseerde taal en een gemeenschappelijk kader voor het beschrijven van aanvalstechnieken en verdedigingsstrategieën. Door gebruik te maken van het framework kunnen beveiligingsprofessionals de risico's voor hun organisatie beter begrijpen en hun beveiligingsmaatregelen effectiever inzetten.

Lean Startup: Verwijst naar een methodologie voor de ontwikkeling van bedrijven en producten die werd geïntroduceerd door Eric Ries. Het doel is om nieuwe bedrijfsmodellen en productideeën sneller en efficiënter te valideren. De kernprincipes van Lean Startup zijn gebaseerd op het idee van het bouwen van een minimaal levensvatbaar product om een concept snel te testen en te valideren met echte klanten in de markt.

Log4j: Een Java-gebaseerd logging-hulpprogramma dat wordt gebruikt om logboeken te genereren voor toepassingen. Het biedt verschillende logniveaus, zoals trace, debug, info, warn, error en fatal. Log4j is ontworpen om te werken met meerdere outputdoelen, zoals bestanden, consoles, netwerkservers en meer. Het heeft ook de mogelijkheid om logboeken te filteren op basis van pakketten, klassen en niveaus. In december 2021 werd er een beveiligingsprobleem ontdekt in Log4j, wat heeft geleid tot een wereldwijde waarschuwing en aandacht.

Managed Service Providers (MSP's): zijn bedrijven die een scala aan IT-diensten op afstand beheren en onderhouden voor andere bedrijven. Dit kan variëren van het beheren van netwerken, applicaties en systemen tot het leveren van specifieke diensten zoals cyberbeveiliging, dataopslag en technische ondersteuning. MSP's zijn vooral nuttig voor kleine en middelgrote bedrijven die niet de middelen of expertise hebben om een volledige IT-afdeling in huis te hebben. Door deze taken uit te besteden aan een MSP, kunnen deze bedrijven zich concentreren op hun kernactiviteiten terwijl ze profiteren van professioneel IT-beheer en -ondersteuning.

Multiparty Computation: In het Nederlands vaak aangeduid als "meervoudige berekening" of "veel partijenberekening", is een subveld van cryptografie. Het stelt meerdere partijen in staat om gezamenlijk berekeningen uit te voeren op hun gegevens, zonder deze gegevens met elkaar te delen. Dit is een krachtige tool voor het behouden van privacy in situaties waarin partijen willen samenwerken, maar bepaalde gegevens geheim willen houden. Bijvoorbeeld, stel dat meerdere bedrijven willen samenwerken om gemiddelde salarissen in hun industrie te berekenen, zonder de specifieke salarisgegevens van hun werknemers te onthullen. Meervoudige berekening maakt dit mogelijk door een methode te bieden waarbij elke partij slechts een deel van de berekening uitvoert op hun eigen gegevens, en de gedeeltelijke resultaten vervolgens combineren om het uiteindelijke resultaat te verkrijgen. Elk bedrijf leert dus het gemiddelde salaris in de industrie, maar niet de specifieke salarisgegevens van de andere bedrijven.

Phygital: Een samentrekking van de woorden "fysiek" en "digitaal" en wordt gebruikt om te verwijzen naar een ervaring of product dat zowel fysieke als digitale elementen bevat. Een voorbeeld van een phygital ervaring zou bijvoorbeeld een interactieve museum tentoonstelling zijn waarbij bezoekers fysieke objecten kunnen bekijken en aanraken, terwijl ze tegelijkertijd digitale informatie en media kunnen verkennen via een interactieve app op hun smartphone of tablet.

Proof of Concept (PoC): Een kleine oefening of project waarbij de haalbaarheid en het potentieel van een idee, methode, technologie of systeem wordt gedemonstreerd. In essentie is het een manier om te laten zien dat een bepaald concept in theorie en/of in de praktijk kan werken, zonder dat het op volledige schaal wordt geïmplementeerd.

Roblox: Een online gaming platform en game-ontwikkelingsbedrijf. Het stelt gebruikers in staat om hun eigen virtuele werelden te creëren en erin te spelen. Het biedt toegang tot een breed scala aan gebruikersgegenereerde spellen en ervaringen.

Threat Intelligence-based Ethical Red Teaming (TIBER): Het is een Europees kader voor het testen van de cyberveiligheid van financiële instellingen, ontwikkeld door de Europese Centrale Bank (ECB) in samenwerking met nationale toezichthouders en de financiële sector. TIBER maakt gebruik van ethical hacking en threat intelligence om de weerbaarheid van de financiële instellingen tegen gerichte cyberaanvallen te testen. Het doel is om de beveiliging van de financiële sector te versterken en zo het vertrouwen in het financiële systeem te vergroten.

Katapult Regeling: Publiek-private samenwerkingen (pps'en) die willen opschalen én aan de voorwaarden van de regeling voldoen, konden in 2023 een aanvraag indienen in het kader van de subsidie Opschaling verduurzaamde pps in het beroepsonderwijs uit het Nationaal Groeifonds. Met deze regeling wordt een impuls gegeven aan het opleiden van jongeren met de juiste skills voor de vraag van de regionale arbeidsmarkt, het door om- en bijscholing blijvend inzetbaar houden van medewerkers van het regionale bedrijfsleven en het versterken van de innovatiekracht van het mkb. Dit past perfect bij de doelstellingen van het CVD. www.wijzijnkatapult.nl

Kennis en Innovatie Agenda: Met het Missiegedreven Topsectoren en Innovatiebeleid heeft het kabinet een nieuwe aanpak voor de topsectoren en het innovatiebeleid geformuleerd. Het Missiegedreven Topsectoren en Innovatiebeleid omvat vijfentwintig missies verdeeld over vier maatschappelijke thema's, waaronder (digitale) veiligheid. Dit thema heeft een grote reikwijdte; uiteenlopend van het verdedigen tegen dreigingen van buiten, het voorkomen van georganiseerde criminaliteit, het beschermen van kritieke infrastructuren en digitale veiligheid tot veiligheid op straat. Hiervoor is het nodig gebruik te maken van de nieuwste wetenschappelijke inzichten, (sleutel)technologieën en toepassingen met aandacht voor ethische en maatschappelijke aspecten. Daarbij zullen vaak combinaties nodig zijn van meerdere kennisgebieden, zowel technologisch, sociaal-maatschappelijk als organisatorisch. Meerdere wetenschappelijke disciplines en topsectoren moeten hiervoor samenwerken. https://hollandhightech.nl/hoe-we-helpen/kia-veiligheid

NIST Cybersecurity Framework: Een richtlijn en referentiekader voor organisaties om hun cybersecuritybeleid en -praktijken te verbeteren. Het is ontwikkeld door het National Institute of Standards and Technology (NIST), een agentschap van het ministerie van Handel in de Verenigde Staten. Het framework biedt een gestructureerde aanpak om risico's te identificeren, te beoordelen en te verminderen op het gebied van cybersecurity. Het richt zich op vijf kernonderdelen: identificatie, bescherming, detectie, respons en herstel. Elk onderdeel omvat categorieën, subcategorieën en best practices die organisaties kunnen implementeren om hun cybersecurityvermogen te versterken.

Dankwoord/Nawoord

Aan het einde van deze boeiende reis, die dit boek ‘Security Innovation Stories’ is, wil ik graag een moment nemen om mijn dankbaarheid te uiten aan iedereen die heeft bijgedragen aan de totstandkoming ervan.

Allereerst gaat mijn dank uit naar de twintig koplopers in de cybersecuritysector die hun kostbare tijd en inzichten met ons hebben gedeeld. Hun openhartige gesprekken en diepgaande kennis hebben dit boek gemaakt en zullen ongetwijfeld velen inspireren.

Een speciaal woord van dank aan mijn co-auteur, Frank van Summeren, wiens expertise en netwerk onmisbaar waren. Daarnaast wil ik Anja den Hertog bedanken voor het initiatief en de ontelbare verbeteringen aan de inhoud. Ook wil ik Renza Grüter bedanken voor het delen van haar visie en het sparren over de inhoud.

Ik wil ook mijn redactieteam bedanken voor hun scherpe blik en aandacht voor detail. Hun inspanningen om de kwaliteit van de tekst te waarborgen hebben het boek naar een hoger niveau getild. Het gaat hier om: Charelle Kooy, Eva Buitinck en Esmee Mauer.
Estelle Valkenburg bedank ik voor de fantastische vormgeving.

Daarnaast wil ik ook iedereen bedanken die op een andere manier heeft bijgedragen aan het realiseren van dit boek waaronder: Merijn Carmiggelt, Dominique Ros, Lily de Bruyne en Joep Kaiser.

Tot slot wil ik mijn lezers bedanken. Jullie interesse in cybersecurity en jullie drang naar kennis en begrip zijn de drijfveren geweest voor dit werk. Ik hoop dat dit boek jullie zal bewapenen met nieuwe inzichten en ideeën, en zal bijdragen aan een veiligere digitale wereld.

Met oprechte dankbaarheid,

Bram de Bruijn

Over de auteurs

Bram de Bruijn
heeft 15 jaar ervaring in de security industrie, beginnend bij het NAVI van het Ministerie van Binnenlandse Zaken, later overgaand in de NCTv. Na een periode bij Securitas met een sterke focus op technologie en innovatie, werd hij in 2015 zelfstandig ondernemer, gespecialiseerd in de ontwikkeling en vermarkting van technologische oplossingen. Hij vervulde interim functies bij o.a. Fox-IT, Imbema en Quinyx AB en is opgeleid aan Nyenrode Business Universiteit en JADS University.

Sinds 2020 is Bram oprichter en directeur van Beyond Products B.V., een strategisch marketingbureau op het gebied van Security en IT, gericht op productmanagement en marketing, geïnspireerd door de uitdagingen in IT security innovatie en adoptie.

Frank van Summeren
adviseur bij RONT (een spin-off van TNO), heeft uitgebreide ervaring in cyberweerbaarheid en security, zowel bij de overheid als in het bedrijfsleven. Hij was projectleider bij HSD en informatiearchitect bij Provincie Gelderland, en leidde de Hackathon for Good bij The Hague Tech. Als docent bij onder andere de Bestuursacademie, SBO en HCB, deelt hij zijn kennis actief. Frank organiseerde verscheidene Smart City en Cyber Security Events, gericht op het samenbrengen van experts voor het delen van technologische innovaties.

Zijn doel: Nederland veiliger maken door kennisuitwisseling en effectieve samenwerkingsstrategieën.

20 KOPLOPERS: IN ÉÉN BOEK

20 koplopers uit het security domein, van overheid, bedrijfsleven, wetenschap tot eindgebruikers in één boek. Ze schijnen hun licht op innovatie en vertellen hoe ze zélf innoveren voor een veiligere samenleving.

Het boek verkent de factoren die het succes van innovatie in security bepalen. Nederland staat bekend om zijn innovatieve benadering van cybersecurity. 'Security Innovation Stories' onderzoekt wat ons land te bieden heeft op dit gebied. De uitkomsten zijn verwerkt in 20 waardevolle inzichten.

Dit boek is onderdeel van het gelijknamige platform www.securityinnovationstories.com, een plek waar best practices en lessons learned worden gedeeld om innovatie in security te versnellen.

Auteur: Bram de Bruijn

''Innovatie is de sleutel tot het waarborgen van onze digitale veiligheid, nu én in de toekomst. Met dit boek willen we lezers inspireren met verhalen van pioniers die grenzen verleggen.''

Co-auteur: Frank van Summeren

''Van vernieuwers die kansen zien én deze benutten. Hen wilden we een podium geven om de wereld een stukje veiliger te maken.''