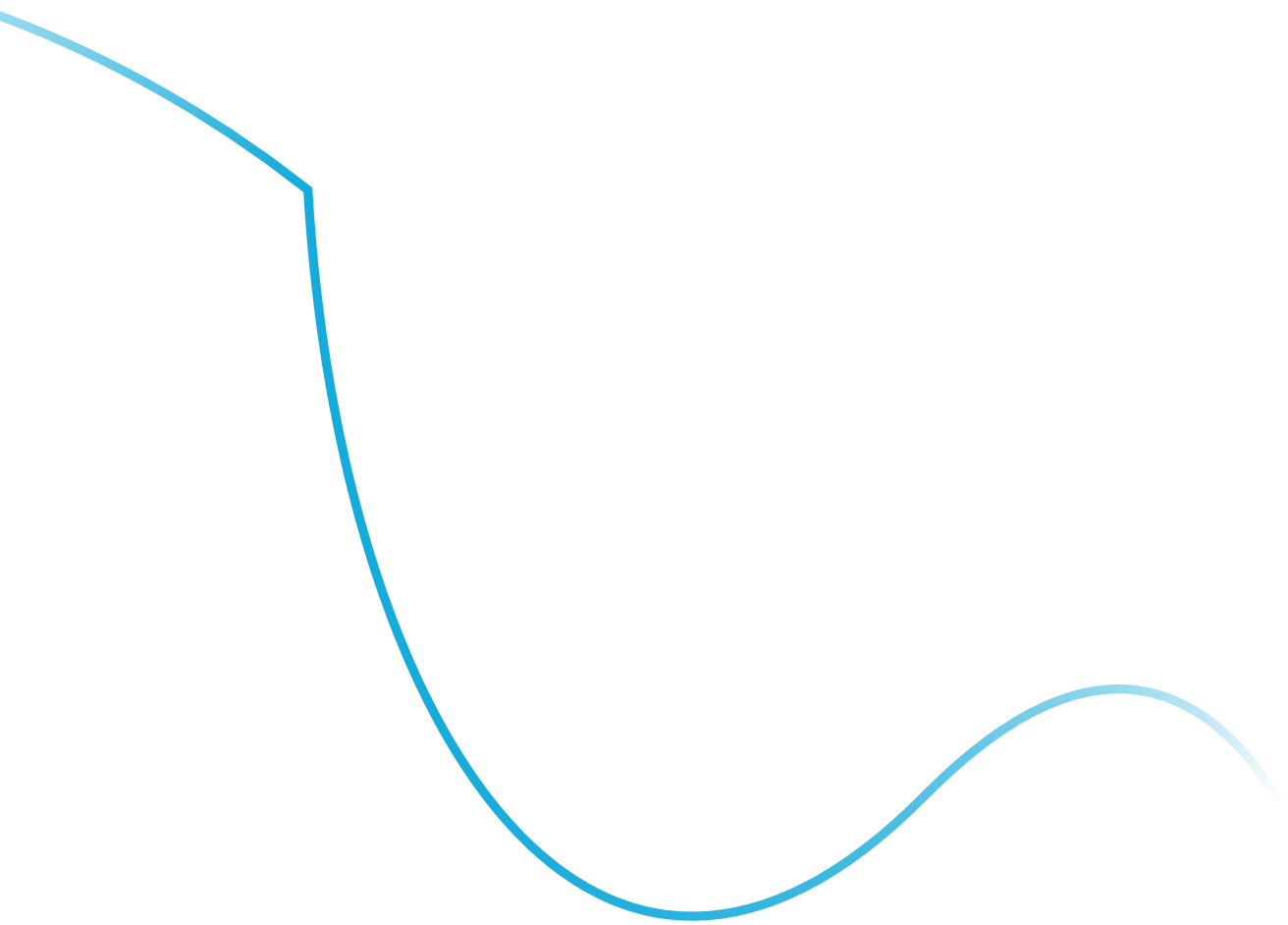
TRENDS IN VEILIGHEID 2023-24

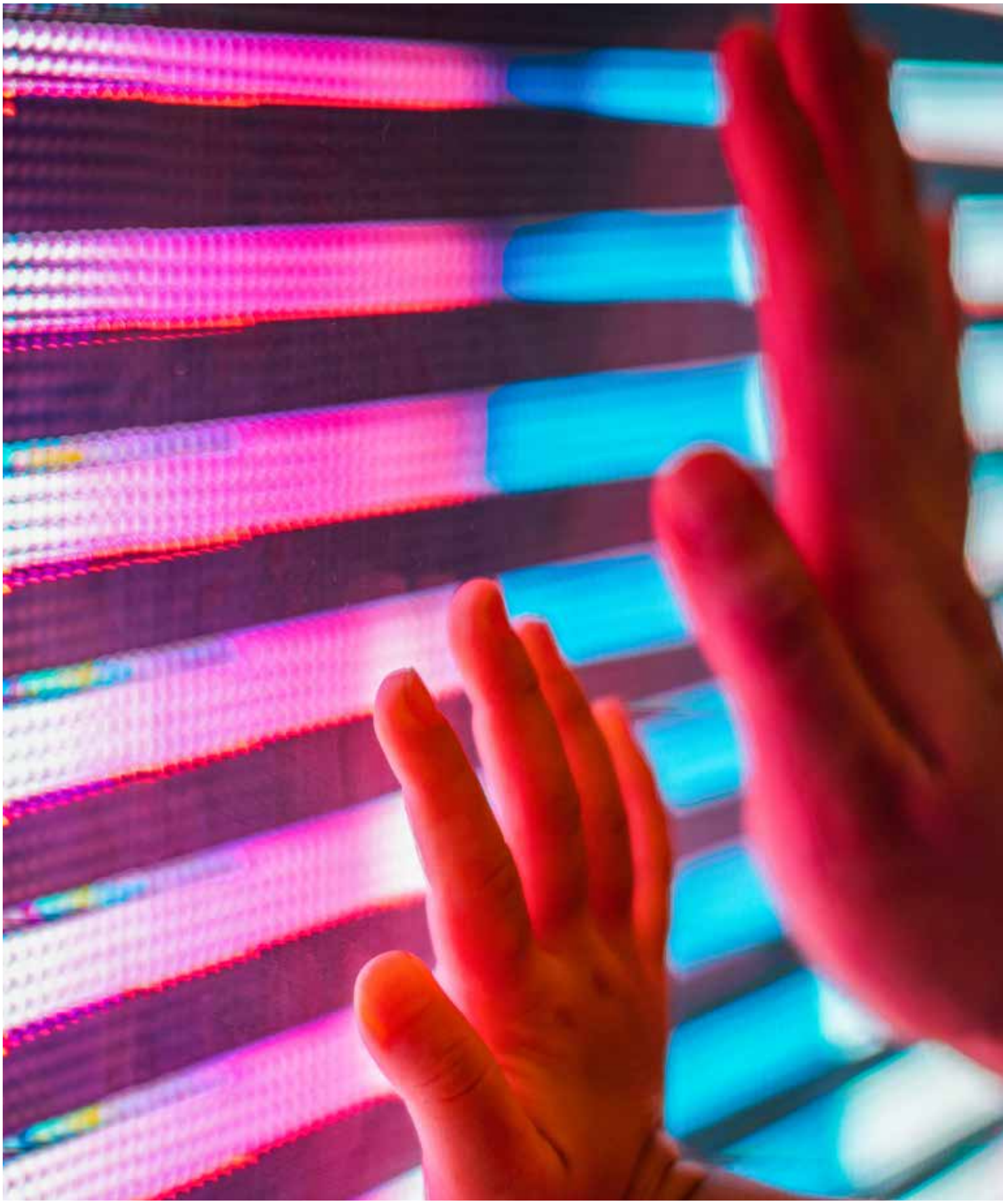
INNOVATIE IN EEN WEERBARE DIGITALE SAMENLEVING



TRENDS IN VEILIGHEID 2023-24

INNOVATIE IN EEN WEERBARE DIGITALE SAMENLEVING

INHOUDSOPGAVE



VOORWOORD

In een wereld die sterk afhankelijk is van technologie, is veiligheid cruciaal. Technologie biedt meer veiligheid, maar zorgt evengoed voor meer dreiging. Zo heeft het veiligheidsdomein een transformatie ondergaan met de opkomst van datagedreven werken en toepassingen zoals kunstmatige intelligentie (AI). Organisaties in het veiligheidsdomein profiteren volop van geavanceerde analytische mogelijkheden om bedreigingen te identificeren en te mitigeren. Maar (cyber)criminelen zitten ook niet stil. Zij gebruiken AI en geavanceerde datatechnieken om hun criminele praktijken te verfijnen.

Terwijl de organisaties in het veiligheidsdomein streven naar het creëren van een intelligente en datagedreven aanpak van criminaliteit, moeten ze ook rekening houden met de ethische en privacy-implicaties van het gebruik van toepassingen als AI om het vertrouwen van de samenleving niet te verliezen. Vertrouwen is de basis van de legitimiteit van de organisaties in het veiligheidsdomein. In deze context is het versterken van de eigen weerbaarheid met cybersecurity van cruciaal belang.

Trends in Veiligheid 2023-2024 beschrijft de wisselwerking tussen het veiligheidsdomein, datagedreven werken, AI en de cruciale weerbaarheid op het gebied van cybersecurity. In verschillende artikelen van onze experts worden de voordelen van het gebruik van data en AI in het veiligheidsdomein belicht, evenals de complexiteit van het beheersen van risico's en uitdagingen om dit op een ethische, legitieme en veilige manier te doen. Dit jaar hebben we ook bestuurders uit het veiligheidsdomein zelf geïnterviewd. Zo betogen Capgemini-experts Luuk Tubbing, Siebe Vaartjes en Marten Porte dat het ten dele terecht is dat het vertrouwen in AI onder druk staat en dat de publieke veiligheidssector aan zet is om dit vertrouwen te herstellen. Zij beschrijven de komst van meerdere juridische en ethische kaders en raamwerken. Door deze naast elkaar te leggen tonen zij aan dat op hoofdlijnen consensus bestaat over waar AI aan moet voldoen, zodat het op grotere schaal succesvol en verantwoord inzetbaar is.

Echter, een rapport als het onze is enkel boeiend als het ook wat andere kritische geluiden laat horen. 'Innovatie Activist' Henk Vermeulen geeft een mooie bijsluiter bij het gebruik van AI in sociale chatbots. Sociale chatbots belichamen de opkomst van digitale interactie. Dit biedt vele positieve mogelijkheden als educatieve tools en emotionele steun, maar kunnen ook verslaving en ideologische echokamers versterken. Ook stellen ze kwaadwillenden in staat tot manipulatie en phishing. Repressieve regelgeving biedt weinig weerstand tegen deze complexe uitdagingen. Het vraagt een weerbare samenleving en het behoud van menselijke interactie en inclusiviteit als tegenwicht tegen de potentieel negatieve gevolgen van overmatige digitale afhankelijkheid. Het veiligheidsdomein kan de sociale interacties bekrachtigen, naast het beschermen van diegene die bescherming nodig hebben en het begrenzen van diegene die te ver gaan.

AI heeft een hele dominante plek in de technologische ontwikkelingen die het veiligheidsdomein beïnvloeden; het is echter niet de enige factor van betekenis. Zo schrijven Anne-Sophie Fritschij en Vien Germawi van Capgemini in samenwerking met Giny Verschoor van de Politieacademie over de kansen en bedreigingen van immersieve technologieën. Zij kijken hierbij naar de kansen die Virtual Reality (VR) biedt voor het veiligheidsdomein, zoals de toepassing van de VRange door de Politieacademie.

Veel artikelen in dit rapport gaan ook over de reactie van het veiligheidsdomein op de negatieve aspecten van de technologische

Het rapport bevat ook dit jaar weer artikelen die gaan over trends in organisatorische uitdagingen en innovatie. Zo worden duurzaamheidsdoelstellingen steeds dominanter in de strategische doelstellingen van de organisaties in het veiligheidsdomein

trends, om de weerbaarheid van onze samenleving te versterken. Julian van Velzen en Gireesh Kumar Neelakantaiah schrijven over de aard van de dreiging die quantumcomputers met zich mee kunnen brengen en hoe overheden en andere instanties in landen de dreiging hebben erkend en zijn begonnen met het voorbereiden en reageren erop.

Johan Klercq en Mara van Gulik laten zien hoe de aanpak van financiële criminaliteit in een tijd van cryptocurrency versterkt kan worden. Cryptovaluta's worden niet beperkt tot landsgrenzen en dit brengt ook nieuwe uitdagingen met zich mee in internationale samenwerking en strengere geharmoniseerde samenwerking op EU-niveau. Datagedreven samenwerken op basis van vertrouwen wordt ook beschreven door collega's Albert Holl en Waishali Latchmansing, waarbij zij inzoomen op het versterken van het volwassenheidsniveau van de dataprivacy van organisaties in het veiligheidsdomein. De auteurs pleiten ervoor om actief te werken aan het verbeteren van hun dataverwerkingsactiviteiten, zodat deze compliant zijn. Europrivacy certificering kan bijdragen aan het versterken van het vertrouwen in datagedreven werken.

Het rapport bevat ook dit jaar weer artikelen die gaan over trends in organisatorische uitdagingen en innovatie. Zo worden duurzaamheidsdoelstellingen steeds dominanter in de strategische doelstellingen van de organisaties in het veiligheidsdomein. Op dit vlak doet de politie een stap naar voren. Nadja Zeiske en Ingelou Sybrandij, Programmamamager Duurzaamheid politie, beschrijven de unieke en belangrijke rol van de politie in de aanpak van klimaatverandering en duurzaamheid. Door in te zetten op verduurzaming van de organisatie zelf en ook door het werk dat de politie verricht kan de politie bijdragen aan zowel klimaatmitigatie als ook -adaptatie. In het artikel van Niels van Stappershoef en Paul Depla, Burgemeester Breda, wordt de trend belicht dat steeds meer organisatie overstijgende samenwerking nodig is om de grote uitdagingen in de samenleving aan te kunnen pakken. De strijd tegen georganiseerde criminaliteit vraagt om een ecosysteem-aanpak en een adaptieve overheid in de wijze waarop de samenwerking wordt georganiseerd.

Een weerbare samenleving heeft weerbare veiligheidsorganisaties. De toename in hybride werken heeft ook nieuwe uitdagingen opgeleverd op cybersecurity vlak. Het artikel van Natasja Pieterman en Emmaly van Ettikhoven belicht de zoektocht van organisaties in het veiligheidsdomein, waar gewerkt wordt met kritieke data, naar de juiste balans tussen de voordelen van hybride werken en de extra veiligheidsmaatregelen die dit vraagt. Het bepalen van de benodigde security-vaardigheden blijft een uitdaging, zoals collega's Jule Hinzbergen en Renato Kuiper beschrijven in hun artikel. Een Security Operating Model wordt al gebruikt in de private sector om te bepalen welke security-vaardigheden een organisatie nodig heeft en hoe deze beheerd moeten worden. Dit model kan de organisaties in het veiligheidsdomein ook helpen om weerbaarder te zijn tegen cybersecurity-dreigingen. En hiermee zijn we weer terug bij het woord vertrouwen, de belangrijkste voorwaarde voor legitimiteit van veiligheidsorganisaties om bij te kunnen dragen aan het vergroten van weerbaarheid in onze samenleving. In een tijdperk waarin innovatie hand in hand gaat met toenemende dreigingen, biedt de convergentie van datagedreven werken, AI, innovatie en organisatorische adaptiviteit een unieke kans om niet alleen reactief, maar ook proactief de (digitale) weerbaarheid te versterken. Door deze uitdagingen aan te gaan en deze kansen te benutten, kunnen we een veiligere (digitale) toekomst bouwen voor zowel individuen als organisaties.

Erik Staffeleu
Vice President
Public Sector

Wat vinden bestuurders uit het veiligheidsdomein?

In het 13e Trends in Veiligheid rapport delen bestuurders in het publieke veiligheidsdomein hun inzichten over digitale trends en uitdagingen. Ze hebben een duidelijke visie voor hun organisaties, maar staan voor de complexe taak om verouderde IT-systemen te moderniseren en tegelijkertijd de privacy en veiligheid van burgers te waarborgen.

De digitale transformatie is een voortdurend evoluerend proces, en bestuurders erkennen de groeiende verwachtingen van de samenleving in het digitale tijdperk. Ze moeten zich bezighouden met diverse uitdagingen en kansen, waaronder samenwerking, gegevensuitwisseling en verantwoord gebruik van generatieve AI.

Generatieve AI wordt gezien als een krachtige technologie met potentieel voor verandering in banen en werkprocessen. Tegelijkertijd zijn er zorgen over misbruik door criminelen en de behoefte aan effectieve regelgeving. Quantum computing wordt ook gezien als een opkomende technologie met nieuwe uitdagingen voor beveiliging.

Cybersecurity staat hoog op de agenda, vooral na de pandemie, met de behoefte om thuiswerkplekken en gedistribueerd werken veilig te houden. Bewustwording en geavanceerde technologieën zijn essentieel om de steeds geavanceerdere aanvallen van kwaadwillende tegen te gaan.

Bestuurders benadrukken het belang van gegevensuitwisseling binnen de juiste kaders en het verminderen van de kloof tussen IT en de organisatie. Een federatief datastelsel en strategische innovatie spelen een cruciale rol in de toekomstige modernisering.

In conclusie, organisaties in het veiligheidsdomein staan voor grote vernieuwingen, met een focus op data, klantgerichte dienstverlening en ondersteuning van medewerkers door technologie. Het doel is om een modern digitaal landschap te creëren en Nederland veilig te houden, met duidelijke strategische richtlijnen en samenwerking tussen organisaties.

De volledig analyse is geschreven door Marcel Kordes en Miriam Staal-Cuppen en te lezen in hoofdstuk Digitale veiligheid: samen bouwen aan een weerbare samenleving.

01

DE WEG NAAR VERTROUWEN IN AI VOOR EEN VEILIGE SAMENLEVING

Hoe kan de publieke veiligheidssector het vertrouwen in AI versterken?

Vertrouwen in AI staat onder druk. Tegelijkertijd wordt er hard gewerkt aan manieren om meer grip te krijgen op AI en deze verantwoordelijk in te zetten.

Highlights

- Organisaties worstelen met het mitigeren van risico's rondom AI-modellen.
- Willen we de belofte van AI blijven waarmaken, dan zal de veiligheidssector moeten werken aan vertrouwen van de samenleving in AI.
- De Code of Ethics voor AI biedt zeven principes om AI op verantwoorde wijze in te zetten.
- We bieden concrete handvatten om in de veiligheidssector aan de slag te gaan met de randvoorwaarden van verantwoorde AI.

De belofte van AI stokt: zonder vertrouwen geen toekomstbestendige veilige samenleving

Artificiële Intelligentie (AI) kan ons leven aangenamer maken en biedt kansen voor een betere en veiligere wereld. AI kan, mits goed ingezet, een aanvulling op of versterking van menselijke vaardigheden zijn. Ook kan het saaie en gevaarlijke taken automatiseren. Het helpt de politie bij het beter voorspellen van misdaden en plannen van operationele capaciteit en het helpt Defensie met het verbeteren van de situational awareness in een oorlogssituatie. Zo verzamelt Oekraïne in de oorlog met Rusland op grote schaal

(real-time) inlichtingen met behulp van AI-software gecombineerd met data van satellieten, drones en cyberoperaties.[1]

Schreven we in Trends in Veiligheid 2022 over de definitieve 'ontsnapping' van AI vanuit het lab naar de samenleving, over de kansen en gevaren hiervan en hoe Nederland haar digitale weerbaarheid kan versterken.[2] Hoewel AI-adoptie de afgelopen vijf jaar ruim is verdubbeld, stagneert de groei de afgelopen drie jaar. In dezelfde vijf jaar zien we dat de vooruitgang stokt bij het mitigeren van risico's rondom cybersecuritydreigingen, naleving van wet- en regelgeving, privacy, uitlegbaarheid en rechtvaardigheid.[3] Een voorbeeld is het Land Information Manoeuvre Centre (LIMC), dat teruggefloten werd omdat het gegevens van burgers verzamelde en analyseerde zonder juridische grondslag. Ondertussen gebruiken criminelen ChatGPT om zorgvuldig samengestelde phishingmails te schrijven. Als de veiligheidssector deze risico's de baas wil blijven, moet AI op een manier in kunnen zetten die vertrouwd wordt door de samenleving.

In voorbereiding op de AI-verordening van de EU zijn er al losse initiatieven gestart die het vertrouwen in AI moeten bevorderen. Iets wat voor de veiligheidssector in het bijzonder van belang is, aangezien de inzet van AI en de verdediging ertegen een grote impact op individuen kan hebben en zelfs een kwestie van leven en dood kan zijn. Alhoewel de AI-verordening gaat helpen richting te geven aan relevante standaarden laat deze het publieke veiligheidsdomein expliciet buiten beschouwing. Tijdens de REAIM 2023 conferentie hebben regeringsvertegenwoordigers ingestemd met een gezamenlijke 'call to action' over de verantwoorde ontwikkeling, toepassing en het gebruik van AI in het militaire domein.[4] Ook bij Capgemini zetten we ons in voor de adoptie van verantwoorde AI. In dit artikel bieden we aan de hand van de Capgemini Code of Ethics[5] handvatten voor verantwoorde AI en een aantal concrete tips voor de implementatie hiervan.

Zorgen en uitdagingen

Er zijn goede redenen waarom het vertrouwen van AI onder druk staat. AI gaat bijvoorbeeld op zoek naar patronen in historische data waardoor het de neiging heeft om bestaande vooroordelen over te nemen en uit te vergroten. Daarnaast zijn veel AI-modellen niet erg transparant, waardoor verantwoording over genomen besluiten vaak niet goed mogelijk is. Neem bijvoorbeeld een AI-systeem dat besluiten neemt die een significante impact op een persoon kunnen hebben, waarbij iemand bijvoorbeeld aan een extra controle wordt onderworpen. Als niet uitgelegd kan worden op basis waarvan deze beslissing wordt genomen, liggen gebrekkige verantwoording, discriminatie en vooringenomenheid op de loer. Echter ondermijnt volledige transparantie in de veiligheidssector de handhaving, aangezien dit criminelen de mogelijkheden geeft om de handhaving te ontlopen. Verder zijn er nog de zorgen rondom privacy en cybersecurity. Daar komt nog bij dat de impact van AI-systemen kan afwijken van de intentie. Dit kan bijvoorbeeld een probleem zijn als het gaat om autonome wapens en zelfrijdende voertuigen. Hoewel de risico's voor veel AI-toepassingen beperkt zijn, zou dit bij toepassingen in de veiligheidssector funest kunnen zijn voor het vertrouwen in instanties en het draagvlak vanuit de samenleving.

Initiatieven en inspanningen voor vertrouwen in AI

Het borgen van vertrouwen in AI komt in vele vormen en aanduidingen. Zo kom je op het internet termen tegen als: vertrouwen in AI, betrouwbare AI, verantwoordelijke AI, ethische AI, transparante AI, uitlegbare AI en mensgerichte en veilige AI-systemen. Hoewel de betekenis van deze termen in ieder geval deels overlapt draait het er wat ons betreft vooral om dat vertrouwen in AI-systemen geborgd is om in de veiligheidssector gebruikt te kunnen worden.

1 https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/
2 https://www.capgemini.com/nl-nl/expertise/research/het-veiligheidsdomein-als-baken-in-dynamische-tijden/
3 https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review
4 https://www.rijksoverheid.nl/ministeries/ministerie-van-buitenlandse-zaken/evenementen/reaim
5 https://www.capgemini.com/about-us/who-we-are/our-values/our-ethical-culture/ethical-ai/

Zeker in de veiligheidssector is het van belang om bij AI-systemen die een grote impact kunnen hebben op burgers een 'human-in-the-loop' ontwerp te hanteren.[6] Dit betekent dat AI betrokken is in het proces maar dat de verantwoordelijkheid voor een beslissing bij de mens ligt. Los van aankomende wetgeving zoals de AI-verordening op EU-niveau, zijn er ook vele (toetsings)kaders en raamwerken ontwikkeld, zoals het Toetsingskader Algoritmen van de Algemene Rekenkamer.

Visie op vertrouwen in AI en het versterken daarvan

De genoemde zorgen in combinatie met in ontwikkeling zijnde wetgeving en raamwerken vragen om vertrouwen in AI te borgen. Het is daarom een goede ontwikkeling dat er meerdere kaders en raamwerken zijn. Door deze naast elkaar te leggen wordt het duidelijk dat er op hoofdlijnen consensus bestaat over hetgeen waaraan de maatschappij vindt dat AI moet voldoen.

De Code of Ethics voor AI van Capgemini[7] geeft wat ons betreft in zeven principes helder weer waar het in de kern om gaat: het dienen van onze maatschappij met AI op een duurzame (in de breedste zin van het woord) wijze staat in dit raamwerk centraal. Het heeft daarmee de positieve insteek die wij onderschrijven om AI op grotere schaal succesvol verantwoord in te zetten. Het hanteren van deze principes bij de ontwikkeling en toepassing van AI geeft de benodigde basis om AI te kunnen vertrouwen. De zeven principes zijn de volgende:

1 AI met zorgvuldig afgebakende impact

AI moet gericht zijn op het verbeteren van mensenlevens en mag geen schade voor individuen veroorzaken. Hiervoor is het van belang dat het doel helder afgebakend is en dat eventuele impact op individuen kan worden geïdentificeerd en gemitigeerd.

2 Duurzame AI

Zowel bij het ontwerp als de ontwikkeling van AI-oplossingen moet rekening gehouden worden met toekomstige generaties, het milieu en het hele ecosysteem.

3 Rechtvaardige AI

AI-systemen moeten gelijke behandeling van mensen waarborgen, ongeacht etniciteit, handicap, leeftijd, religieuze overtuiging, seksuele geaardheid of andere persoonlijke kenmerken. Daarvoor is diversiteit van ontwikkelteams noodzakelijk, zowel in persoonlijke kenmerken als in professionele achtergrond. Daarnaast is het van belang om kritisch te zijn op de trainingsdata voor het AI-model om te voorkomen dat hier (verborgen) vooroordelen of fouten in zitten.

4 Transparante en verklaarbare AI

AI-gestuurde beslissingen dienen verklaarbaar te zijn, vooral bij die toepassingen waarbij de gevolgen van een foutieve uitkomst ernstig zijn. Het doel en de werking moeten duidelijk worden gecommuniceerd, afhankelijk van het geheimhoudingsniveau, aan de hele maatschappij, aan de politiek dan wel aan (interne) toezichthouders. Bij interactie met een AI-interface moeten individuen zich ervan bewust zijn dat ze met een machine communiceren en mogen ze niet worden misleid om anders te denken. Daarbij is het van belang dat individuen worden geïnformeerd over de mogelijkheden en beperkingen van AI. Tot slot moeten datasets en processen die voor de AI-oplossing worden gebruikt gedocumenteerd zijn.

5 Beheersbare AI met duidelijke verantwoordelijkheid

Het ontwerp van AI-oplossingen moet de autonomie en besluitvorming van de mens beschermen. Verder is het van belang dat het duidelijk is vastgelegd wie verantwoordelijk zijn voor de oplossing. Tevens is het van belang traceerbaarheidsprincipes te hanteren, zodat het op-AI-gebaseerde besluitvormingsproces kan worden uitgelegd en gecontroleerd.

6 Robuuste en veilige AI

Robuustheid moet worden ingebed in de hele levenscyclus van de AI-systemen, van het ontwerp en de ontwikkeling tot en met implementatie en het gebruik. Voor AI-toepassingen die een cruciale maatschappelijke functie vervullen moeten noodplannen bestaan voor het geval het AI-systeem zelf faalt. Ook moeten de AI-toepassingen nauwkeurige en reproduceerbare resultaten opleveren zodat het robuust en betrouwbaar is en daarmee veilig is om te gebruiken.

7 AI met respect voor privacy en gegevensbescherming

Vanaf de ontwerpfase moeten gegevensbescherming en -beveiliging integraal onderdeel zijn van de AI-levenscyclus. Uiteraard moeten de wet- en regelgeving op het gebied van privacy en gegevensbescherming worden gerespecteerd, zoals het beperken van gegevensverzameling en –verwerking tot alleen het strikt noodzakelijke. De gegevens moeten nauwkeuring en op een veilige manier worden verwerkt. Individuen dienen geïnformeerd te worden over hoe hun gegevens worden verwerkt en ze moeten de juiste middelen krijgen om hun rechten uit te oefenen. In de publieke veiligheidssector zijn er uitzonderingen voor heimelijke operaties.

6 https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie

7 https://www.capgemini.com/wp-content/uploads/2021/03/Capgemini_Code_of_Ethics_for_AI_2021_EN.pdf

Dit is een set van werkwijzen en tools voor het automatiseren, beheren en monitoren van de volledige levenscyclus van het ML-model. Dit is een randvoorwaarde om hoogwaardige en verantwoorde AI-modellen te kunnen garanderen.

Fundering voor vertrouwen in AI

Werken aan vertrouwen in AI vraagt om permanente aandacht, tot in de haarvaten van de organisatie. Waar bovengenoemde principes het grote plaatje vertellen, geven we je hier enkele concrete handvatten om in jouw organisatie te werken aan de randvoorwaarden voor vertrouwen in AI.

1 Creëer bewustwording en transparantie

Creëer bewustwording over de kenmerken, mogelijkheden en risico's van AI. Door trainingen aan te bieden en gericht te communiceren via de communicatiekanalen waarop de relevante medewerkers actief zijn. Hierbij helpt het ook om checklists, templates en tools (zoals het Toetsingskader algoritmes[8]) aan te bieden, zodat medewerkers zelf direct aan de slag kunnen. Communiceer (indien gepast) naar (interne en externe) stakeholders welk algoritme voor welk doeleinde wordt gebruikt, maar ook zaken zoals welke data daarvoor wordt verzameld, wat de juridische basis is en in hoeverre sprake is van menselijke tussenkomst.

2 Ontwikkel kennis en vaardigheden

Zorg ervoor dat kennis en vaardigheden op de juiste plek in de organisatie aanwezig zijn; namelijk daar waar de AI-systemen worden ontworpen, ontwikkeld (of ingekocht), gevalideerd en gebruikt worden voor besluitvorming. Hierbij gaat het niet alleen om kennis van programmeren, statistiek en het bedrijfsproces, maar ook over zaken als kwaliteit, compliance, privacy, security en ethiek. Daarnaast moeten personen die werken aan of met deze systemen zich bewust worden van onbewuste vooroordelen die een invloed kunnen hebben op de werking van het systeem.

3 Implementeer MLOps (Machine Learning Operations)

Dit is een set van werkwijzen en tools voor het automatiseren, beheren en monitoren van de volledige levenscyclus van het ML-model. Dit is een randvoorwaarde om hoogwaardige en verantwoorde AI-modellen te kunnen garanderen. Het biedt handvatten om grip te krijgen op rechtvaardigheid (geautomatiseerd monitoren en testen van bias), betrouwbaarheid (tijdige identificatie van defecten of problemen) en uitlegbaarheid (detailinformatie over totstandkoming, besluitvormingsproces en prestaties van modellen) van AI. Adequate testdatasets en testcases zijn hierbij van belang om onder andere de kwaliteit, veiligheid en rechtvaardigheid van het AI-systeem aan te tonen.

4 Zorg dat de data op orde is met datamanagement

Draag zorg voor het inrichten van datamanagement, met bijzondere aandacht voor datakwaliteit. Mensen die besluiten nemen op basis van data verwachten dat deze voldoende compleet en accuraat zijn voor het beoogde doeleinde. Datakwaliteit is een belangrijke

8 https://www.rekenkamer.nl/onderwerpen/algoritmes-digitaal-toetsingskader

randvoorwaarde voor vertrouwen in AI, omdat het de prestaties, rechtvaardigheid, nauwkeurigheid en uitlegbaarheid van AI-modellen sterk kan beïnvloeden. Het managen van datakwaliteit omvat het implementeren van een robuust proces voor het verzamelen, valideren en opschonen van data, evenals het continu monitoren en onderhouden van de datakwaliteit gedurende de complete levenscyclus. Dit vraagt om het beleggen van dataeigenaarschap in de business domeinen, maar ook om de silo's tussen deze domeinen te doorbreken.

5 Creëer continue feedback voor betrokkenheid en verbetering

Mits juist toegepast bevordert agile werken op allerlei manieren het vertrouwen in AI. Deze empirische werkwijze biedt een iteratieve ontwikkelmethode: aanpassingen op basis van testen en feedback zijn snel mogelijk indien ethische en kwaliteitskwesties zich voordoen. Bovendien is multidisciplinaire samenwerking inherent aan agile: verschillende perspectieven dragen bij aan vertrouwen in AI. De actieve betrokkenheid van diverse stakeholders is hierbij van belang: business (opdrachtgever en gebruiker), technologie en (als de AI hier impact op heeft) ook de burger.

Vertrouwen in AI is een gezamenlijke verantwoordelijkheid

Het bouwen aan vertrouwen in AI zal voor de veiligheidssector een combinatie zijn van wet- en regelgeving, zelfregulering en breed toezicht door publieke toezichthouders en NGO's. Er zal een evenwicht gevonden moeten worden tussen het benutten van de voordelen van AI en het aanpakken van de potentiële risico's en negatieve gevolgen. Voor de veiligheidssector staat er meer op het spel dan het succesvol implementeren van AI; het gaat uiteindelijk om het bouwen van een toekomstbestendige veilige samenleving. Daarom zal elke organisatie in de sector zelf moeten werken aan vertrouwen door principieel én professioneel te werk te gaan. Daarbij geldt: denk groot, begin klein en leer snel!

Over de auteurs

Luuk Tubbing
Managing Consultant Insights & Data. Luuk is gespecialiseerd in Data & AI-vraagstukken. Hij begeleidt klanten op hun reis naar een datagedreven organisatie.

https://www.linkedin.com/in/luuktubbing/
luuk.tubbing@capgemini.com

Siebe Vaartjes
Managing Consultant Business Technology Services. Siebe is gespecialiseerd in het openbare orde- en veiligheidsdomein op het gebied van Intelligence en Informatie Gestuurd Werken.

https://www.linkedin.com/in/siebevaartjes/
siebe.vaartjes@capgemini.com

Marten Porte
Consultant Cybersecurity. Marten richt zich op governancevraagstukken op het gebied van digitale veiligheid in de publieke sector.

https://nl.linkedin.com/in/martenporte
marten.porte@capgemini.com

02

DE BLAUWE POLITIE IS OOK GROEN

Welke rol heeft de politie in de duurzaamheids-en klimaatopgave?

De politie kan bijdragen aan zowel klimaatmitigatie als ook adaptatie. Namelijk door in te zetten op verduurzaming van de organisatie EN het operationele werk van de politie.

Highlights

- Klimaatverandering raakt politiewerk nu en in de toekomst.
- De politie heeft als overheidsorganisatie de verantwoordelijkheid om een voorbeeldrol in te nemen als het gaat om duurzaamheid.
- De rol van de politie gaat verder dan alleen de verduurzaming van de eigen bedrijfsvoering.
- De politie kan actief bijdragen aan een duurzamere (en dus veiligere) samenleving door de mate en wijze waarop de politie haar bevoegdheden inzet

Klimaatverandering is een van de belangrijkste veiligheidsthema's van nu en in de toekomst. Het wordt steeds zichtbaarder dat klimaatverandering de gehele samenleving raakt. Overstromingen, droogte, hittegolven, energiearmoede, grondstoffentekorten en toenemende ongelijkheid zijn ontwikkelingen waar we als gevolg van klimaatverandering steeds vaker mee te maken krijgen in de (nabije) toekomst[1]. Alsnog zien de meeste mensen klimaatverandering als iets ontastbaars of iets dat ver weg van onze huidige werkelijkheid staat [2,3,4].

Dit geldt niet voor de politie, die steeds meer met deze problematiek te maken heeft. De politie wordt bijvoorbeeld steeds vaker ingezet bij klimaatstakingen of protesten die voortkomen uit

1 IPCC (2022). 'Climate Change 2022: Mitigation of Climate Change. Contribution of Working Group III to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change.'

2 Milfont, T. L. (2010). Global warming, climate change and human psychology. Psychological approaches to sustainability: Current trends in theory, research and practice, 19, 42; Gifford et al., 2009

3 Spence, A. and Pidgeon, N. F. (2010). Framing and Communicating Climate Change: The Effects of Distance and Outcome Frame Manipulations. Global Environmental Change, 20, 656-667.

4 Gifford, R., Scannell, L., Lormos, C., Smolova, L. and Uzzell, D. (2009). Temporal pessimism and spatial optimism in environmental assessments: An 18-Nation study. Journal of Environmental Psychology, 29, 1-12

klimaatbeleid (zoals de stikstofdiscussie), maar ook bij overstromingen en bosbranden door klimaatverandering. Daarnaast wordt verwacht dat de politie in de toekomst meer te maken gaat krijgen met toenemende agressie, onrust en criminaliteit door bijvoorbeeld hittegolven die zullen ontstaan als gevolg van klimaatverandering [5, 6, 7, 8]. Deze fenomenen en ontwikkelingen weerspiegelen hoe klimaatverandering directe en indirecte gevolgen gaat hebben voor de openbare veiligheid en daarmee ook op het politiewerk.

Hoe moet de politie als publieke veiligheidsorganisatie hiermee omgaan? Welke rol heeft de politie in dit vraagstuk over de impact van klimaatverandering op veiligheid? De gevolgen van klimaatverandering vragen om verduurzaming, want een duurzame samenleving is een veilige samenleving[9]. De politie moet hierop voorbereid zijn, hierop reageren en ook het goede voorbeeld hierin geven. De politie moet zelf als organisatie verduurzamen, heeft een rol als werkgever richting medewerkers, en moet de legitimiteit van de organisatie bewaken als wetshandhaver en voldoen aan wet- en regelgeving. In dit artikel gaan we in op de rol die de politie speelt in dit vraagstuk en op welke twee manieren de politie een bijdrage kan leveren aan een duurzame en veilige samenleving: namelijk de verduurzaming van de organisatie zelf en verduurzaming door het werk dat de politie verricht. Aan de hand van voorbeelden laten we zien wat het verduurzamen van en door de politie betekent, en welke uitdagingen dit met zich meebrengt.

Verduurzaming van de politieorganisatie

De politie heeft als overheidsorganisatie een voorbeeldrol als het gaat om duurzaamheid. Als de grootste publieke werkgever van Nederland met circa 65.000 werknemers, eigenaar van ongeveer 800 gebouwen en 14.000 voertuigen, en een jaarlijkse inkoop van 2,1 miljard euro, heeft de politie een enorme omvang met een grote impact. De totale jaarlijkse milieuvoetafdruk van de politie komt neer op ongeveer 297 kton CO2-equivalent[10] . Dit staat gelijk aan de uitstoot van de gehele gemeente Middelburg[11]. Twee derde van de CO2-uitstoot van de politie is afkomstig van het vervoer van de politie. Denk hier aan het wagenpark, maar ook aan de ongeveer

325 miljoen woon-werk kilometers die jaarlijks door politiemedewerkers afgelegd worden. Ongeveer een kwart van de CO2-uitstoot van de politie is afkomstig van huisvesting gerelateerde emissies. De energie voor verwarming van deze gebouwen dragen hier voornamelijk aan bij. De overige CO2-uitstoot van de politie is afkomstig van facilitaire services, zoals de inkoop van eten en drinken, uniformen en uitrusting, wapens, en afval. Digitalisering en ICT hebben een dubbele rol in de verduurzaming: aan de ene kant wordt digitalisering ingezet om te verduurzamen, aan de andere kant zorgen de grondstoffen van mobiele apparaten, maar vooral ook de energie van datacenters, voor een grote uitstoot. Vanwege een te verwachten groei aan datagebruik is het van belang dit aan de voorkant duurzaam in te richten.

In lijn met Europese wetgeving en het Nederlands klimaatbeleid heeft de politie als doel om 60% CO2-reductie te behalen in 2030 ten opzichte van 1990. Dit is een ambitieus doel en betekent dat de organisatie op alle vlakken in een hoog tempo moet verduurzamen. Aan de hand van routekaarten worden per thema (vervoer, huisvesting, facilitaire services en ICT) de verduurzamingskansen in kaart gebracht en verduurzamingsmaatregelen vastgesteld. Bijvoorbeeld de elektrificatie van het wagenpark is een van de belangrijkste maatregelen die de politie kan nemen om de CO2 uitstoot afkomstig van vervoer te reduceren. De oplossing is duidelijk, maar om deze maatregel te realiseren komt een aantal uitdagingen naar voren.

De verduurzaming van de politieorganisatie is een grote transformatieopgave en betekent dat een grote groep mensen gemobiliseerd moet worden om bij te dragen aan

5 capgemini.com/about-us/who-we-are/our-values/our-ethical-culture/ethical-ai/

6 https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie

7 https://www.capgemini.com/wp-content/uploads/2021/03/Capgemini_Code_of_Ethics_for_AI_2021_EN.pdf

8 https://www.rekenkamer.nl/onderwerpen/algoritmes-digitaal-toetsingskader

9 Middendorp, T. (2022). Klimaatgeneraal, bouwen aan weerbaarheid. Amsterdam: Uitgeverij Podium

10 Gebaseerd op een meting gedaan over het jaar 2019.

11 Mes, van Exter, Tauber, & van der Zaag (2021). Ecologische voetafdruk nationale politie 2019, Materiaalstroomanalyse en milieu-impacts. Metabolic: Amsterdam

Door middel van pilots worden verschillende modellen van elektrische voertuigen bij verschillende type werkzaamheden in verschillende omgevingen getest voor gebruik de politie

deze verandering. Het betekent dat duurzaamheid als thema meer prioriteit krijgt en vaker meegenomen wordt in het vormgeven van nieuw beleid en in de uitvoering. De mate van elektrificatie van het wagenpark, is bijvoorbeeld afhankelijk van de realisatie van voldoende laadinfrastructuur. Hiervoor zijn aan de voorkant investeringen nodig. Tegelijkertijd moet continu afgestemd worden met verschillende afdelingen binnen de organisatie, waaronder wagenparkbeheer en huisvesting. Daarnaast vraagt een elektrisch wagenpark ook om ander gedrag - zowel van de afdeling die het wagenpark beheert als ook de agenten die de voertuigen uiteindelijk gebruiken in de operatie. Door middel van pilots worden verschillende modellen van elektrische voertuigen bij verschillende type werkzaamheden in verschillende omgevingen getest voor gebruik de politie. Inspiratiesessies worden gehouden om uitleg te geven over het gebruik van elektrische voertuigen in de operatie.

Gepaard met de opgave van het verduurzamen van de politie kan een spanningsveld ontstaan tussen duurzaamheid en de operationele taken van de politie. Een voorbeeld hiervan is dat het werk van de politie voor een groot deel met de auto wordt verricht (zichtbaar surveilleren met de auto en afrijden op een noodhulp melding), terwijl er vanuit duurzaamheidsperspectief juist aan gewerkt wordt om vervoersbewegingen in de operatie te verminderen. Een ander voorbeeld zijn de zakelijke vliegreizen. Jaarlijks worden ongeveer 18 miljoen km[12] gevlogen voor zowel operationele (bijvoorbeeld samenwerking met buitenlandse korpsen) en niet-operationele (deelname aan een internationaal veiligheidscongres) doeleinden. Vanuit het duurzaamheidsperspectief zouden politiemensen minder zakelijk moeten gaan vliegen om zo de vervoer-gerelateerde CO2-uitstoot te verminderen. Tegelijkertijd wordt criminaliteit steeds grensoverschrijdender en neemt de behoefte aan internationale samenwerking toe. Bovenstaande laat zien dat als het gaat om de verduurzaming van de politieorganisatie, een continue afweging gemaakt moet worden tussen impactvolle duurzaamheidsactiviteiten aan de ene kant, en het uitvoeren van de primaire taak van de politie aan de andere kant.

Verduurzaming door het politiewerk

Waar niet meteen aan gedacht wordt is de koppeling van de primaire taak van de politie met duurzaamheid. Dit bevat twee elementen: het verduurzamen (efficiënter en slimmer inrichten) van operationele processen en de mate en wijze waarop de politie haar bevoegdheden inzet. Door niet alleen de voetafdruk van de politie te verkleinen maar juist ook de taak van de politie aan duurzaamheid te koppelen, wordt de impact van de organisatie op duurzaamheid een stuk groter. Denk hierbij aan de aanpak van milieucriminaliteit maar ook aan het handhaven op de maximale snelheid op de snelweg[13] . Om effectief bij te dragen aan verduurzaming door het werk van de politie moet er capaciteit vrijgemaakt worden en moet er een duidelijke afweging plaatsvinden hoe opsporing en handhaving de meeste impact kunnen maken. Daarvoor moet de politie, samen met haar opsporingspartners en gezag, allereerst beter zicht krijgen op de meest bedreigende vormen van milieucriminaliteit. Vervolgens moeten in de Landelijke Milieukamer scherpe keuzes gemaakt worden over waar de politie haar schaarse handhavings- en opsporingscapaciteit op inzet, en tenslotte de meeste effectieve interventiestrategie kiezen.

Het is vrij ingewikkeld om de milieu-impact van milieudelicten en de impact van de inzet door de politie op dit type criminaliteit inzichtelijk, laat staan meetbaar te maken. Dit heeft te maken met het feit dat de milieu-impact vaak verborgen is en pas op lange termijn zichtbaar wordt. Ter illustratie zogenaamde zeer zorgwekkende stoffen hebben een negatieve impact op medewerkers die in het productieproces onrechtmatig blootgesteld worden aan deze stoffen. Ook hebben deze stoffen impact op de biodiversiteit wanneer ze als afval gedumpt worden in de natuur. Maar deze effecten zijn lang niet altijd in beeld te brengen en er is weinig beeld over de omvang van milieucriminaliteit. En ook het directe causale verband is vaak niet eenduidig aan te tonen. Veel, zo niet de meeste, milieuvervuiling en de impact daarvan is tenslotte het gevolg van formeel vergunde activiteiten. Het aanrichten van milieuschade is dus vreemd genoeg lang niet altijd een strafbaar feit.

12 Gebaseerd op data uit 2022.

13 Van Wee, Vooral veel voordelen van 100 km op de snelweg. Geraadpleegd op 25 april 2023, van https://www.tudelft.nl/stories/vooral-veel-voordelen-van-100-kilometer-op-de-snelweg, 2023

Ook hier ontstaat een spanningsveld: moet de politie prioriteit geven aan fenomenen die op korte termijn een dreiging vormen voor onze veiligheid, of ook aan fenomenen die meer lange termijn- consequenties hebben? Omdat de positieve impact van de verduurzaming door het politiewerk pas zichtbaar zal worden op de lange termijn, wordt de politiemilieutaak soms verdrongen door direct zichtbare en voelbare bedreigingen en delicten. Het zit immers in de haarvaten van de organisatie om direct te handelen op acute situaties. Andere typen criminaliteit en veiligheidsvraagstukken hebben een acutere impact op de veiligheid van onze samenleving, waardoor het natuurlijker is dat de politie zich sneller daarop zal richten (bloed is spoed).

Ook vraagt verduurzaming door het politiewerk om mogelijk nieuwe manieren van werken. Hierbij komen vragen naar voren zoals: hoe werken de opsporingsteams? Milieucriminaliteit is haalcriminaliteit. Is de verhouding tussen de milieu-intelligence en milieu-tactiek nog wel in balans? Heeft de politie genoeg toegang tot de informatie van milieu-toezichthouders om tot signalen te komen? Weten publiek en belangenorganisaties de politie wel te vinden bij vermoedens van milieudelicten? En staat de politie daar voldoende voor open? Doen slachtoffers wel aangifte of richten ze zich vooral op vergunningverleners en toezichthouders? Zijn mensen bij de politie gaan werken om met dit type vraagstukken aan de slag te gaan? De vraag is ook in hoeverre de hele veiligheidsketen ingericht is om milieucriminaliteit effectief aan te pakken en op deze manier impact te maken. Er wordt nu wel geïnvesteerd in de opsporing, maar in de vervolging en berechting ontstaat een steeds nauwere flessenhals. De politie is samen met haar ketenpartners hard aan het werk om die vragen te beantwoorden en een positieve impact op de ecologische footprint van de maatschappij te vergroten.

14 Interpol Innovation Centre (z.d.). Climate Change, Crime and Law Enforcement. https://www.interpol.int/content/download/18519/file/IC%20Background%20Paper%20-%20Crime%20Law%20Enforcement%20and%20Climate%20Change.pdf

15 Ministry of Environmental Protection (z.d.). Green Police. https://www.gov.il/en/departments/units/green_police_dept.

16 Hong Kong Police Force, The Government of the Hong Kong Special Administrative Region (z.d.). Green Police. https://www.police.gov.hk/ppp_en/17_green_police/

Conclusie

De politie heeft een unieke en belangrijke positie in het vraagstuk rond klimaatverandering en duurzaamheid. Door in te zetten op verduurzaming van de organisatie zelf en ook door het werk dat de politie verricht kan de politie bijdragen aan zowel klimaatmitigatie als ook -adaptatie. Op deze manier heeft de politie een belangrijke rol om de negatieve impact van klimaatverandering te verminderen en de impact via de primaire taak van de organisatie te vergoten. Deze opgave is nog erg in ontwikkeling. Hierbij is kennisdeling met andere uitvoeringsorganisaties, organisaties in het veiligheidsdomein en overige politiekorpsen interessant. Ook andere landen zijn bezig met de verduurzaming van en door het politiewerk. In Frankrijk heeft de minister van Binnenlandse Zaken belooft om 3000 rijkswachtposten te creëren om milieudelicten te bestrijden[14] . En in Israël is er een groene politie opgericht om de wetten van de Ministerie van Milieubescherming te handhaven[15]. In Hong Kong creëert een groene politie een grotere milieubewustheid binnen de organisatie en is verantwoordelijk voor de ontwikkeling van duurzaamheidsmaatregelen[16].

Om als werkgever aantrekkelijk en toekomstbestendig te blijven en bij te dragen aan een toekomstbestendige en veilige samenleving, moet ook de Nederlandse politie duurzaamheid een plaats geven in de gehele strategie van de organisatie. Gepaard met deze opgave ontstaan ook spanningsvelden tussen duurzaamheidsactiviteiten en de operationele taken van de politie. Maar ondanks deze uitdaging is het duidelijk dat duurzaamheid niet naast de kerntaken van de politie staat; het maakt er onderdeel van uit en draagt eraan bij. Ook op dit vlak doet de politie een stap naar voren.

Over de auteurs

Nadja Zeiske
Nadja Zeiske is werkzaam als Senior Consultant bij Capgemini Invent. Nadja is gespecialiseerd op het gebied van gedragsverandering en werkt als organisatie adviseur aan verandervraagstukken.

nadja.zeiske@capgemini.com
https://www.linkedin.com/in/nadjazeiske/

Ingelou Sybrandij
Programmamanager Duurzaamheid politie

Ingelou Sybrandij is als programmamanager duurzaamheid werkzaam bij de politie.

https://nl.linkedin.com/in/ingelou-sybrandij

03

AI ALS NOODZAKELIJKE MAAR UITDAGENDE VERSNELLER IN HET INLICHTINGENPROCES

Hoe kan AI verantwoord bijdragen aan tijdige inlichtingen op steeds complexere datastromen?

Met de komst van nieuwe wapensystemen neemt de stroom aan data toe. Dit geeft meer mogelijkheden, maar zet de tijdigheid van de inlichtingen onder druk.

Highlights

- Complexiteit van sensoren en daarmee data nemen toe.
- Mensen kunnen de datastromen niet meer volledig zelf interpreteren.
- AI vergroot de inlichtingen capaciteit door te versnellen.
- AI neemt ook nieuwe risico's met zicht mee.
- Belangrijk om de "human in the loop" te houden.

We zijn ons bewust van de tragedie die zich in Oekraïne afspeelt. Op afstand zien we dat drones een belangrijke, mogelijk doorslaggevende, rol spelen in het conflict. Beide partijen proberen hiermee een tactisch voordeel te behalen. Zowel commerciële als hoogwaardige militaire drones leveren een aanzienlijk voordeel op in het bestrijden van de vijand. In het veld zijn het de individuele dronepiloten die de beelden interpreteren en daarop hun wapens inzetten. Op het strategische niveau, en zelfs internationaal[1], leveren hightech drones hoogwaardige inlichtingen. De inzet van drones en andere sensorplatformen is niets nieuws en ook de Nederlandse krijgsmacht heeft haar sensorarsenaal de afgelopen jaren uitgebreid. Naast de veel besproken MQ-9 en F35 vallen hier ook de modernisatie van andere systemen onder. Maar is een overvloed aan data, afkomstig van deze sensoren, wel altijd een voordeel? Zorgt het voor een data-infarct waarbij de tijdigheid van inlichtingen verloren gaat? Wij stellen dat AI de oplossing én voorsprong biedt om de toenemende stroom aan data in een kortere tijd te verwerken.

Van data naar inlichtingen

Om tot inlichtingen te komen, duiden inlichtingenanalisten data die door verschillende sensoren verzameld worden. De definitie van inlichtingen volgens de Defensie doctrine[2]: “Inlichtingen zijn de resultante van kennis en begrip over de activiteiten, mogelijkheden (capabilities) en intenties van alle relevante actoren en factoren. Inlichtingen voorzien in een zo volledig mogelijk beeld van de situatie (situational awareness) en zijn een randvoorwaarde voor succes in elke operatie”.

De meerwaarde van inlichtingen zit in de volgende karakteristieken: vraag-afdekkend, objectiviteit, accuraatheid en misschien wel het belangrijkst: tijdigheid. Weten waar de vijand gisteren was helpt niet in het

Afbeelding 1: MQ-9 Reaper

1 https://www.ewmagazine.nl/kennis/achtergrond/2022/04/daverende-drones-in-de-donbas-16154w/

2 https://www.defensie.nl/binaries/defensie/documenten/publicaties/2019/06/19/herziene-nederlandse-defensie-doctrine-ndd-2019/190520_NDD_2019_FD.pdf pagina 91.

gevecht vandaag. Daarbij lijkt meer data het inlichtingenproces alleen maar ten goede te komen, maar is dat wel zo?

Meer en snellere datastromen zet de relevantie van inlichtingen onder druk

Om met al deze data "iets" te kunnen heeft de inlichtingengemeenschap de beschikking over zogenaamde single source analisten (die halfproducten[3] maken op basis van een enkele datastroom) en all-source analisten (analisten die halfproducten van de single source analisten analyseren). Met een groeiende hoeveelheid data en een hogere complexiteit groeit ook de werkdruk van deze analisten. Dat betekent dat belangrijke karakteristieken zoals tijdigheid en accuraatheid in het geding komen. Hiermee komt de relevantie van de inlichtingen onder druk.

AI biedt uitkomst bij de nieuwe datastromen

Om de waarde van inlichtingen te borgen moeten steeds grotere volumes van complexere data sneller en effectiever geduid worden. Precies hierin bieden AI-algoritmes en de almaar sterker wordende rekenkracht een uitkomst. Het kan verbanden vinden die wij als mens niet (snel) zien, automatiseren en versnellen van werkzaamheden en het doorzoekbaar maken van grote hoeveelheden data.

Concreet voor het inlichtingendomein valt hierbij te denken aan het efficiënter en sneller maken van:

Om de waarde van inlichtingen te borgen moeten steeds grotere volumes van complexere data sneller en effectiever geduid worden

- **Single source analisten ondersteunen met algoritmes om hun single source datastroom te verrijken;** Toepassen van beeldherkenningsmodellen om naar specifieke objecten of gebeurtenissen te zoeken. Ook hoeft bij een nieuwe inlichtingenbehoefte niet handmatig vele uren aan video's bekeken te worden. Je kan relevante passages opzoeken op basis van hetgeen een model razendsnel observeert.
- **All-source analisten ondersteunen met het snel en effectief combineren van verschillende inlichtingenproducten;** Met generatieve AI-modellen (zoals ChatGPT) snel en effectief inlichting en halfproducten 'begrijpen' en deze in context tot elkaar plaatsen.
- **Slimmer inzetten van schaarse sensorcapaciteit;** Op basis van inzetdata uit het verleden kan beter voorspelt worden wanneer sensorsystemen de beste kans hebben voor het verkrijgen van waardevolle inlichtingen.
- **Slim integreren van meerdere sensoren tot één virtuele sensor.** Een meer accurate waarneming door het slim combineren van meerdere (type) sensoren en daardoor een zeer nauwkeurig beeld maken.

De risico's van AI

Naast de voordelen kleven er ook risico's aan AI binnen inlichtingenprocessen. De rijksoverheid en Het Ministerie van Defensie in het bijzonder onderkent tal van uitdagingen in het gebruik van AI in het inlichtingenproces[4][5]. Hierin onderkennen zij privacy en ethische dilemma's als belangrijke onderwerpen. Ervaringen binnen het bedrijfsleven evenals academische studies leren dat dergelijke onderwerpen in algoritmen zijn te verwoorden.

Ethische risico's komen onder andere voort uit het "zwarte doos" dilemma. Door de complexiteit van AI-modellen wordt de werking ervan een "zwarte doos". We zien wat erin gaat en wat eruit komt, maar begrijpen hoe het model tot die uitkomst komt ontbreekt. Het wordt onmogelijk

3 Halfproducten in de inlichtingengemeenschap zijn deelanalyses en/of analyses op een specifiek deelonderwerp die bijdragen aan zogenaamde "all source" analyses.

4 https://magazines.defensie.nl/specials/2022/01/07_roy-lindelauf

5 zie ook https://www.rijksoverheid.nl/ministeries/ministerie-van-buitenlandse-zaken/evenementen/reaim met betrekking tot het organiseren van REAIM wat betrekking heeft tot het verantwoord inzetten van AI in het militaire domein.

om te beoordelen of, wanneer en in welke context een model faalt. Dit leidt tot drie belangrijke risico's:

- Robuustheid AI-modellen tegen misleiding
- Uitlegbaarheid AI-modellen als onderdeel van aansprakelijkheid
- Risico inschatting vergt de menselijke maat

Robuustheid AI-modellen tegen misleiding

Het is menseigen om aan te nemen dat AI-modellen op eenzelfde manier werken als wijzelf. Neem het herkennen van objecten op afbeeldingen als voorbeeld. Wij mensen herkennen objecten op basis van hun fysieke eigenschappen zoals vorm, kleur en textuur. Of de afbeelding daarbij veel ruis bevat of delen mist maakt niet snel een groot verschil.

Ook andersom geredeneerd vanuit het inlichtingendomein moeten modellen uitlegbaar en controleerbaar zijn

Deze aanname is echter onjuist. Voor veel gebruikte neurale netwerken voor het herkennen van objecten weten we eigenlijk niet goed hoe ze werken. Waar het model prima in staat is een afbeelding te herkennen van een hond, blijkt het heel goed mogelijk om deze modellen voor de gek te houden. Zo is het mogelijk om met onopvallende aanpassingen van de afbeelding het model met hoge mate van zekerheid een andere classificatie te laten doen. Hierdoor wordt een voor de mens overduidelijke afbeelding van een hond door het AI-model met 99% zekerheid als een willekeurig ander object geclassificeerd. Dit lijkt op het eerste gezicht onschuldig, maar opent tal van counter-AI mogelijkheden om ongemerkt de systemen van ongewenste informatie te voorzien.

Uitlegbaarheid AI-modellen als onderdeel van aansprakelijkheid

Als AI-modellen gebruikt worden om beslissingen te nemen, rijst de vraag of en hoe je de beslissing kunt onderbouwen. Ook in het licht van aansprakelijkheid binnen de kaders van de wet. Zodra er sprake is van burgerslachtoffers of de legitimiteit van een actie ter discussie wordt gesteld, moet men kunnen onderbouwen hoe men tot de inlichtingen is gekomen. Dit vergt een transparant besluitvormingsproces waarbij de inlichtingen en de totstandkoming daarvan ook transparant moeten zijn. Met een "zwarte doos" benadering kom je daar niet mee weg. Zeker niet in de context van generatieve AI die de neiging heeft te gaan hallucineren. Dan moet feit en fictie duidelijk gemarkeerd zijn.

Ook andersom geredeneerd vanuit het inlichtingendomein moeten modellen uitlegbaar en controleerbaar zijn. Inlichtingen zijn geverifieerde informatie uit meerdere bronnen. Deze bronnen moeten geraadpleegd kunnen worden om de inlichtingen te kunnen controleren. Als AI hierin een integraal onderdeel is, moet deze AI daar ook aan voldoen.

Risico-inschatting vergt de menselijke maat

Net als mensen zijn AI-modellen nooit 100% nauwkeurig. Vaak is dat geen probleem. In de context van inlichtingen vormt dit echter een risico. Het kan leiden tot verkeerde interpretaties met zelfs verkeerde beslissingen tot gevolg. Wat als door een dergelijke beslissing te voorkomen slachtoffers vallen?

Waar we modellen doorgaans valideren op basis van hun nauwkeurigheid, moeten we ook rekening houden met de impact van de onnauwkeurigheid. Het is daarom cruciaal dat systemen niet autonoom besluiten nemen en dat een "human in the loop" moet zijn. Zo leert ons ook de Russische officier Stanislav Petrov die de derde wereldoorlog voorkwam. Als mens intervenieerde hij in systemen die constateerde dat de Sovjet-Unie werd aangevallen.[6] Een AI-model had als het hier autonoom was ingezet de derde wereldoorlog niet voorkomen. De discussie die hiermee op gang gebracht moet worden is wanneer de "human in the loop" zich moet manifesteren. In het offensieve optreden van de krijgsmacht is hier zeker ruimte voor. In het defensieve optreden kan dit echter tot ongewenste extra vertraging leiden in bijvoorbeeld de detectie van hypersonische raketten en de beslissing om deze uit te schakelen. Een voorbeeld hiervan is het Iron Dome systeem wat ingezet wordt in Israël ter verdediging tegen raketten en mortieren. Anders zou de inzet zijn voor defensieve tegenacties zoals het direct ontplooien van een tegenaanval op doelen, niet zijnde binnenkomende projectielen.

6 https://nl.wikipedia.org/wiki/Stanislav_Petrov

Hoe verantwoord met deze risico's om te gaan?

Vanuit Capgemini werken we met een "code of ethics for AI" waarin naast de onderkenning van de meerwaarde van AI ook specifiek gekeken wordt naar hoe er ethisch verantwoord mee te werken. Wij adviseren een soortgelijke code voor de inzet van AI in het inlichtingendomein. Dit moet minimaal de volgende onderwerpen bevatten.

- AI-modellen dienen robuust ontwikkeld te worden. Het gaat niet alleen om beste accuraatheid, maar ook hoe het model omgaat met ruis, onderbroken data en misleiding. Verder moeten de modellen worden beveiligd om te voorkomen dat deze modellen in verkeerde handen vallen, waardoor er gericht tegenmaatregelen ontwikkeld kunnen worden.
- AI-modellen moeten uitlegbaar en beschikbaar zijn voor controle. Zij zullen net als inlichtingenbronnen geraadpleegd kunnen worden om de resultaten te verifiëren.
- De mens dient het oordeel te vellen en niet het AI-model. Dit zal besluiten ethisch maken en bijdragen aan transparantie en aansprakelijkheid.

Hoever kunnen we met AI gaan?

In een inlichtingenwereld waarin de dataproductie en complexiteit toeneemt door inzet van diverse sensorplatformen, ontkom je niet aan het inzetten van AI. En daar waarin het fysieke gevecht de militair in de modder nog steeds moet besluiten om de trekker over te halen, moet er ook een 'man in the middle' zijn die op basis van de aangeleverde inlichtingen besluiten neemt.

Feitelijk zal AI een groot deel van het inlichtingenproces over kunnen nemen van single source analisten en gedeeltelijk van de all-source analisten. De voorbeelden laten echter zien dat de human interface in dit delicate deel van besluitvormingsprocessen niet te verwijderen valt. AI-modellen zijn daarmee een aanvulling die de relevantie en de tijdigheid van inlichtingen ten goede zal komen. Maar je kan jezelf hardop afvragen of en hoe we kunnen garanderen dat de "human in the loop" altijd aanwezig blijft…

Over de auteurs

Johan de Jong

Johan is Senior Business Analist DS en is gespecialiseerd in inlichtingen analyse & inlichtingenprocessen en de digitalisering hiervan.

https://www.linkedin.com/in/johandejong82/

https://twitter.com/johandejong82

johan.de.jong1@capgemini.com

Joost Carpaij

Joost is Principal Consultant Data Science & AI en leidt de GenAI practice in Noord en Centraal Europa. Hij houdt zich primair bezig met waarde create door Data Science & (gen)AI in de praktijk te brengen. Hierbij kijkt hij verder dan alleen de techniek om ook het gebruik van de oplossingen aan te jagen. Een van zijn expertises is het publieke veiligheidsdomein.

https://www.linkedin.com/in/joostcarpaij/

joost.carpaij@capgemini.com

04

EEN ELFTAL IS NODIG VOOR DE BESTRIJDING VAN DE GEORGANISEERDE (DRUGS)CRIMINALITEIT

In hoeverre ben je als overheid in staat om de drugscriminaliteit te bestrijden en wat is daarvoor nodig?

'Verleiding en dreiging', volgens Paul Depla (burgemeester van Breda), middelen van de georganiseerde criminaliteit om een voet tussen de deur te krijgen in onze bovenwereld. Hoe weren we deze criminelen in onze bovenwereld en hoe kunnen we ze succesvol aanpakken?

Highlights

- Ondermijning is vaag, focus op het verdienmodel van georganiseerde criminaliteit.
- "Verleiding" en "dreiging" is tactiek om in de bovenwereld te komen.
- De aanpak gaat in fases van ongeorganiseerd naar georganiseerd
- Werp barrières op om de roltrap van de georganiseerde criminaliteit te ontregelen.
- Alleen in een elftal (ecosysteem) dat de krachten bundelt kunnen we de wedstrijd winnen.

Wat bedoelen we met ondermijnende, georganiseerde criminaliteit?

Om de vraag te kunnen beantwoorden in hoeverre je als overheid in staat bent om ondermijning aan te pakken moet je dus wel weten waar je het over hebt. Wat is ondermijning en wat pak je aan? Zelfs als je spreekt over georganiseerde criminaliteit kunnen definities verschillen.[1] Een aanpak kan alleen succesvol zijn als je weet waar je je op richt. Op dit moment wordt de definitie van ondermijning overal opgeplakt. Zo ook in de aanpak van de georganiseerde (drugs)criminaliteit. Een aanpak waar Paul Depla, nu burgemeester van Breda, al geruime tijd in zijn werkende leven mee bezig is. Tijdens een interview is ingezoomd op dit onderwerp, zijn ervaringen voor een succesvolle aanpak en wat nodig is in de toekomst om de strijd te winnen. “Ondermijning is een vaag begrip, ongeoorloofd gedrag van bijvoorbeeld voetbalsupporters is ook ondermijnend”, aldus Depla. Net als door rood rijden, je belastingaangifte niet invullen of valse gegevens verstrekken bij het aangaan van een hypotheek.

Depla pelt de definitie van het begrip van ondermijnende, georganiseerde (drugs) criminaliteit af aan de hand van drie elementen:

Verdienmodel en illegale economie

De georganiseerde (drugs)criminaliteit heeft maar één doel: geld verdienen. Deze vormen van criminaliteit worden bedrijfsmatig gerund. Het is daarom cruciaal om dit in beeld te brengen.

De georganiseerde (drugs)criminaliteit maakt gebruik van legale structuren. Denk bijvoorbeeld aan het kweken van hennep in diverse panden of fabriekshallen. Die worden verhuurd door makelaars, pandeigenaren etc. Daarnaast is er een notaris nodig om overdracht van panden wettelijk te regelen.

Legale spelers

Zonder legale spelers is er geen ondermijnende georganiseerde (drugs) criminaliteit mogelijk. Het onderscheid tussen de illegale en legale economie wordt diffuus. Bovendien is de illegale sector oneerlijke concurrentie voor de legale sector. “Je zou je maar met je horecazaak netjes aan de regels houden en hard werken, terwijl de zaak naast je rustig doordraait zonder dat er mensen in de zaak komen. Dan moet je stevig in je schoenen staan om de verleiding voor wat ‘hulp’ vanuit de onderwereld te weerstaan.”

Eigen regels

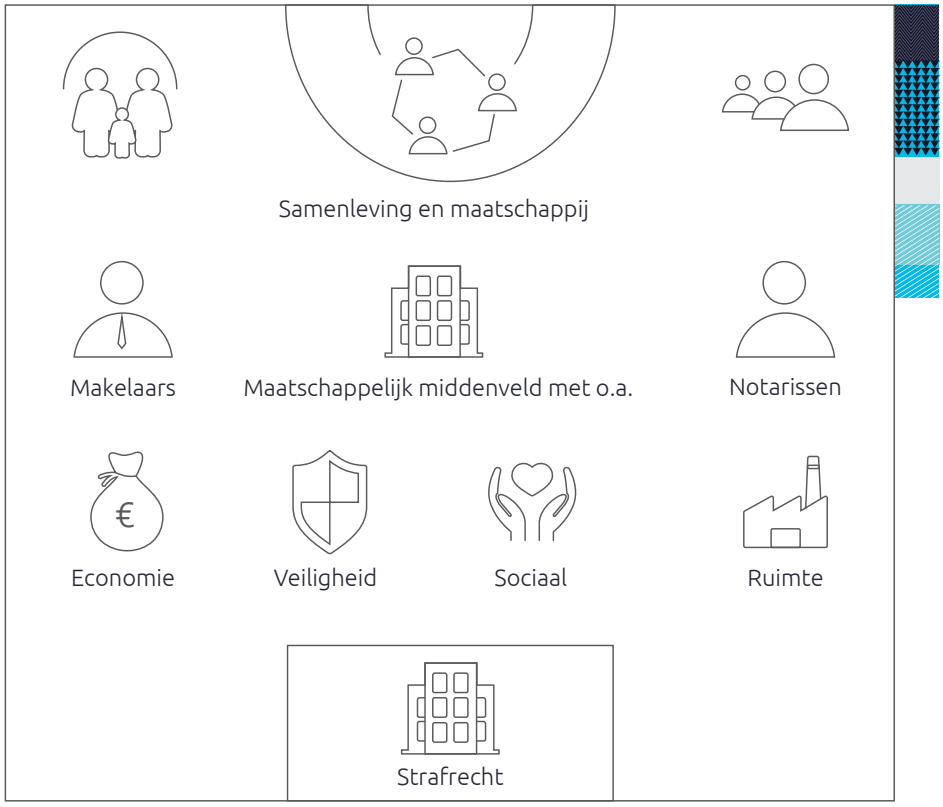
Het laatste element betreft het proces van eigen regels. Van ‘verleiding en dreiging’. Een voetbalclub die in financieel zwaar weer zit helpen door sponsoring, een boerenschuur die leeg staat gebruiken en daarmee de boer wat extra inkomsten gunnen, de moeder die alleen voor haar kinderen moet zorgen een extra kerstcadeau schenken in ruil voor het gebruik van de zolder. Voorbeelden die Depla tegen gekomen is in zijn werkzame leven als wethouder en burgemeester. En als verleiden niet werkt, komt dreiging om de hoek. Granaten bij een pand neerleggen, een burgemeester bedreigen, een advocaat liquideren. Deze vorm neemt helaas toe. De belangen zijn groter en de geldstromen evenzo.

Bedreiging en intimidatie

In zijn rol als burgemeester probeert Depla op diverse manieren zijn aanpak vorm te geven en zichzelf en de mensen die met hem werken te beschermen. Dit betekent dat je goed moet communiceren aan de maatschappij wat je precies doet. “Het sluiten van een pand is niet om het gezin dat er woont te pesten, maar om het verdienmodel van de criminelen aan te pakken. Je moet daarbij uitleg geven waarom je deze dingen doet, de mensen aan je zijde krijgen en niet in de handen van de criminelen duwen” aldus Depla.

Zelf heeft Depla ervaring met bedreiging en intimidatie: “Het hoort bij het ambt” zegt hij er zelf over. Hij probeert daarom de georganiseerde (drugs)criminaliteit als gezamenlijk elftal aan te pakken. Niet als boegbeeld of als coach, maar als onderdeel van het team. Dat betekent dat je zelf aan je weerbaarheid moet denken maar ook zeker aan de medewerkers van de gemeente en die van je partners. Degene die zichtbaar zijn voor de criminelen. De zogenaamde ‘Veilige Publieke Taak’.

1 Calderoni, F., Campedelli, G.M., Comunale, T., Marchesi, M. E. en Savona, E. U. (2020). Rekrutering into organised criminal groups: A systematic review. In: Trends and Issues in Crime and Criminal Justice, (583), 1-28.



Afbeelding 1: Het elftal van Depla

Bijna de helft van de lokale bestuurders – burgemeesters, wethouders en raadsleden – heeft last van agressie, intimidatie of geweld. Bij ambtenaren ligt dat percentage iets lager, maar met 33 procent is dat nog altijd fors. De percentages vertonen een trendmatige toename, bleek uit de Monitor Integriteit en Veiligheid 2022. De piek is nog niet bereikt.[2]

Het is dus een belangrijke taak voor Depla om de mensen in zijn elftal te beschermen. En samen met hen de strijd aan te gaan.

De opstelling voor een succesvolle aanpak

Wanneer kunnen we nu stellen dat deze strijd de goede kant op gaat? Dat gaat in fases, aldus Depla. “De eerste fase was die van de georganiseerde criminaliteit versus de ongeorganiseerde overheid. Daarin begint nu verandering te komen. Men is beter in staat elkaar te vinden en de ook de meest voor de hand liggende partij naar voren te schuiven wanneer die aanpak het beste werkt. Het zijn niet altijd meer de politie en het OM. Soms heb je bijvoorbeeld meer aan de belastingdienst of een energieleverancier.” Op dit moment zit men dus in de tweede fase naar een georganiseerde overheid. Wat heeft Depla daarvoor nodig? “Een elftal” (zie afbeelding 1). Hij gebruikt deze metafoor van Hans Boutellier (bijzonder hoogleraar Polarisatie & Veerkracht op de Vrije Universiteit Amsterdam) vaker om zijn aanpak te beschrijven. Op doel het strafrecht, de keeper die moet vervolgen en straffen als dat nodig is. De verdediging bestaat uit de partners in het veiligheidsdomein, maar ook die uit het economische- ruimtelijke en sociale domein (denk aan politie, het Openbaar Ministerie, (jeugd) reclassering, UWV, woningbouwcorporaties, werkgeversorganisaties, bedrijven etc.). Veelal bestaande partners vanuit de overheid.

Voor de verdediging staat het maatschappelijk middenveld. Bestaande uit kwetsbare sectoren (bepaalde branches waar veel witwassen voorkomt of veel wordt afgenomen voor criminele doeleinden), of sectoren en verenigingen die ook zelf kunnen ondersteunen . Denk hierbij aan de vereniging van notarissen, of van makelaars. Maar ook een KNVB die voetbalverenigingen bijstaat als er vragen zijn over mogelijke geldstromen die men niet vertrouwt.

Voorin staat de samenleving, de inwoners. In de aanval. Zij moeten het besef hebben dat ze niet alleen staan. Dat de overheid er voor hen is. Aan de voorkant, voor een bestaanszeker leven en aan de achterkant als het tegenzit. Zij moeten ook bereid zijn

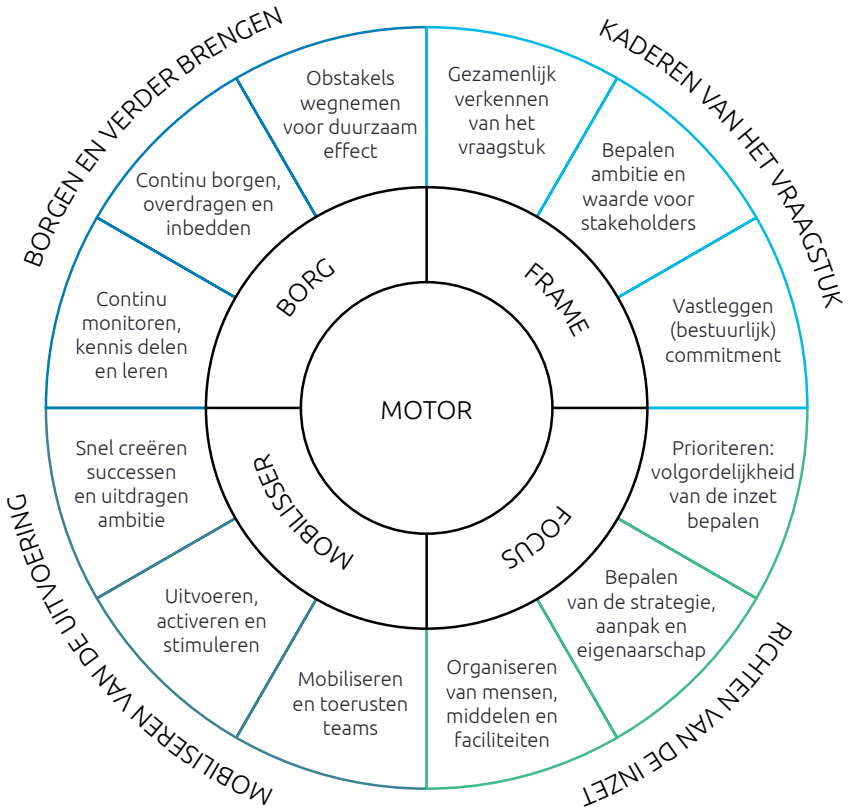
om 'nee' te durven zeggen bij verleiding en bedreiging. Ze moeten beseffen dat de georganiseerde (drugs)criminaliteit meer kapot maakt dan je lief is. Deze maatschappelijke verontwaardiging wordt nog gemist volgens Depla. Het wordt soms zelfs verheerlijkt met series op Netflix. Dat is gevaarlijk. De beste aanval begint bij diegenen die het grootste slachtoffer kunnen worden.

Dit elftal is natuurlijk een metafoor voor een succesvolle netwerksamenwerking. Het ecosysteem waarbinnen deze partijen samenwerken vraagt om een motor die de boel draaiende houdt. Ook vanuit Capgemini is deze vorm van samenwerking al meerdere keren toegepast. Deze methodologie heet 'Empowering Ecosystems'. Kort gezegd begint deze aanpak met het kaderen van de inzet (o.a. het bepalen van de definitie). In het voorbeeld van ondermijnende georganiseerde criminaliteit gaat het dus om de definitievorming. Wat willen we nu eigenlijk aanpakken? En waar ga je dat mee doen (je elftal)? Dat bestaat uit mensen en middelen in een duidelijk organisatie. We richten daarmee de inzet. Als derde stap moet je aan de slag en de uitvoering mobiliseren (successen boeken en uitvoeren). Juist in de aanpak van ondermijnende georganiseerde criminaliteit is het zo belangrijk om successen te boeken en ook te vieren. Daarmee laat je zien dat je succesvol kunt zijn. De laatste stap is het borgen en verder brengen (kennis delen, obstakels wegnemen en samen doorpakken en inbedden). Het is immers een aanpak van de lange adem. Het is kwetsbaar als dit op personen hangt en moet dus goed geborgd worden in de organisaties binnen het netwerk. In het verhaal van Depla klinkt deze aanpak overduidelijk door. Het elftal van Depla kadert, richt, voert uit en brengt verder. [3]

DE METHODOLOGIE EMPOWERING ECOSYSTEMS

De methode die als leidraad dient om samenwerkingen te stimuleren.

De tool bevat vier gebieden:



Afbeelding 2: 'empowering ecosystems'

2 https://vng.nl/artikelen/bedreigde-ambtenaren-niet-normaal-meer

3 https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2019/07/06-027.19b-Factsheet-Empowering-Ecosystems-ENGLISH_web.pdf

https://magazines.riec.nl/codegeel/2021/11/interview-pieter-tops

Durven

In de afrondende woorden van Depla klinkt nog een duidelijk pleidooi. Durf als overheid en partners te investeren in mens en maatschappij. Stel je sterkste elftal op en speel de wedstrijd stevig. Werp barrières op aan de voorkant zodat jeugdigen niet afglijden op de roltrap van de criminaliteit. Pak de verdienmodellen aan als een criminele industrie. Dit vraagt dus zowel een bedrijfseconomische als psychologische basis. Maar dit betekent ook dat we als handelsland moeten durven om onszelf barrières op te leggen die ook knellen in onze legale structuur. De komende periode moet blijken of we daar ook toe bereid zijn. Dat is een trendbreuk die ingaat tegen onze open economie en wereldhandel. In de toekomst een belangrijke vraag, waarbij we ook met innovaties kunnen kijken of we onze legale structuren kunnen beschermen. Wellicht ook datagedreven en met behulp van AI. Gelet op de bedragen die worden verdiend met de georganiseerde drugscriminaliteit[4] vraagt het een lange adem van de aanpak om succesvol te zijn. Bovendien past de georganiseerde criminaliteit zich aan. Waar dit voorheen softdrugs (hennep) was, wordt het meeste nu verdient aan synthetische drugs. Eerder werd witwassen vooral gedaan met 'cash-geld' nu zijn cryptovaluta zeer in trek. Het adaptieve vermogen van de georganiseerde criminaliteit is groot. Nu de overheid nog.

Met een voorbeeld sluit Depla af: "tijdens Valentijnsdag worden de rozen uit Zuid-Amerika gewoon niet gecontroleerd op drugs, het zijn er simpelweg te veel. Denk je dat een slimme criminele ondernemer dit niet weet? Precies: stel je sterkste elftal op want alleen dan kun je de wedstrijd tegen de georganiseerde (drugs) criminaliteit winnen."

Over de auteurs

Niels van Stappershoef
Ten tijde van schrijven was Niels Managing Consultant bij Capgemini Invent en gemeenteraadslid in Tilburg. Hij is gespecialiseerd in netwerksamenwerking binnen de publieke sector. Hij focuste zich daarin ten tijde van het schrijven van dit rapport op het justitie- en veiligheidsdomein, specifiek op de aanpak van ondermijning. In dit domein is Niels al reeds vele jaren werkzaam op diverse niveaus.

https://www.linkedin.com/in/niels-van-stappershoef-9789a54b/

Paul Depla
Paul Depla is burgemeester (PvdA) van de gemeente Breda. Hij is hiervoor onder andere wethouder in Nijmegen geweest en burgemeester in Heerlen. Paul Depla loopt daarnaast vaak voorop in de aanpak van ondermijning en de stevige rol die de overheid hierin moet nemen.

https://www.linkedin.com/in/paul-depla-74596526/

05

EUROPRIVACY IN EEN DATAGEDREVEN SAMENLEVING

Wat is de toegevoegde waarde van Europrivacy voor veiligheidsorganisaties?

De Nederlandse overheid maakt grootschalig gebruik van onze data, maar het gevaar dat de privacy van de Nederlandse burger hiermee in het geding komt wordt steeds groter.

Highlights

- Dataprivacy is van belang in een digitale wereld.
- Europrivacy geeft vertrouwen.
- Publieke organisaties hebben hun dataprivacy nog niet op orde.

Denk hierbij aan de grootschalige verwerking van persoonsgegevens van vliegtuigpassagiers door Justitie en Veiligheid maar ook aan de politie die op grote schaal data van demonstranten verzamelt. Artikel 42 van de AVG (Algemene Verordening Gegevensbescherming) geeft lidstaten de mogelijkheid om officiële certificeringsmechanismen in te voeren. De Europrivacy certificering toont aan dat een organisatie haar gegevensverwerking activiteiten conform de gestelde eisen van de AVG en nationale wet- en regelgeving uitvoert.

Op 10 oktober 2022 heeft de European Data Protection Board (EDPB) het eerste Europese certificaat goedgekeurd: Europrivacy. De Nederlandse burger heeft op dit moment onvoldoende inzicht in de verwerkingsactiviteiten van de overheid en dit maakt dat het vertrouwen in de overheid afneemt.[1] Reden genoeg voor de overheid om zich te verdiepen in Europrivacy.

De rol van de AVG in een data-gedreven samenleving

In februari 2023 heeft de Autoriteit Persoonsgegevens de minister van Justitie en Veiligheid voor een tweede keer op moeten roepen om de persoonsgegevens van vliegtuigpassagiers in overeenstemming te brengen met de PNR- richtlijn en de uitspraak van het Hof.[2] Uit een recente uitspraak van het Hof is immers gebleken dat Justitie en Veiligheid onterecht data verwerkt.

Passenger Name Records (PNR) worden bijgehouden om reisbewegingen van terroristen en zware criminelen vast te stellen. Justitie en Veiligheid legt op dit moment echter de persoonsgegevens van alle reizigers vast en verzamelt deze gegevens al jarenlang in een database, terwijl deze gegevens niet in deze database thuishoren.[3]

Daarnaast is uit recentelijk onderzoek gebleken dat de politie op grote

schaal persoonlijke data opvraagt van demonstranten. Het gaat hierbij om adressen, burgerservicenummers en geboortedata, maar ook om data van familieleden. De politie doet dit naar eigen zeggen, omdat de demonstranten eerder schuldig zijn geweest aan ernstige openbare ordeverstoringen. Uit overzichten is echter gebleken dat er ook data is opgevraagd van demonstranten die niet eerder zijn veroordeeld.[4]

De rechtstreekse werking van de Algemene Verordening Gegevensbescherming, maakt dat de regels direct gelden voor alle lidstaten, zo ook voor Nederland. Het verzekert echter niet dat overheidsorganisaties direct handelen naar de regels van de verordening, zoals de hierboven geschreven casussen bevestigen.

1 Rijksoverheid. (2022, 4 november). Werkagenda Waardengedreven Digitaliseren. Geraadpleegd op 6 maart 2023, van https://www.digitaleoverheid.nl/kabinetsbeleid-digitalisering/werkagenda/iedereen-kan-de-digitale-wereld-vertrouwen/bescherming-van-privacy/.

2 https://www.autoriteitpersoonsgegevens.nl/uploads/imported/brief_ap_passagiersgegevens_pnr.pdf

3 Nederlands Juristenblad. (2023, 22 februari). Ministerie JenV moet stoppen met grootschalig verwerken gegevens vliegtuigpassagiers. Geraadpleegd op 6 maart 2023, van https://www.njb.nl/nieuws/ministerie-jenv-moet-stoppen-met-grootschalig-verwerken-gegevens-vliegtuigpassagiers/.

4 https://nos.nl/artikel/2466880-onderzoek-politie-verzamelt-op-grote-schaal-data-van-demonstranten

Hiermee laten ze zien dat de veiligheid van persoonlijke data ook voor hen van belang is en dat zij enkel de benodigde informatie verwerken

Van de overheid wordt verwacht dat zij een voorbeeldfunctie heeft in de maatschappij, maar recente gebeurtenissen geven blijk dat dit niet altijd het geval is. Dit betekent niet dat de overheid bewust privacy rechten schendt. (Data)privacy is een complex vraagstuk in een maatschappij waar persoonlijke data een steeds belangrijkere rol speelt. Aantonen dat je als organisatie voldoet aan de geldende privacywetgeving is een opgave waar constante aandacht voor nodig is, mede gezien de dynamiek van een organisatie.

Europrivacy voor vertrouwensherstel

Gebeurtenissen zoals eerder beschreven geven blijk dat het de overheid niet altijd lukt om structureel aan de voorwaarden van de AVG te voldoen. Het zorgt echter ook voor het dalen van het vertrouwen van de Nederlandse burger in de (gegevensverwerkings-)activiteiten van de overheid. De vraag die publieke organisaties zich moeten stellen is of Europrivacy kan helpen bij het herstellen van dit vertrouwen. Publieke organisaties zouden hierbij gebaat kunnen zijn, omdat de kans dat burgers bij een gebrek aan vertrouwen steeds minder persoonlijke data zullen delen, groter is.

Certificering vindt plaats door een gekwalificeerde certificatie-instelling zoals SGS, BSI of DNV een beoordeling uit te laten voeren. Zij stellen, door middel van verschillende analyses en inspecties, vast of de gegevensverwerkingsactiviteiten van de organisatie in lijn zijn met de daarvoor gestelde eisen. Wanneer een organisatie aan deze eisen voldoet wordt het certificaat uitgegeven en opgenomen in het Europrivacy-register. Een organisatie kan zelf kiezen welke verwerkingsactiviteiten zij (met voorrang) laat certificeren. Dit houdt dus in dat een certificaat niet alle gegevensverwerkingsactiviteiten van een organisatie hoeft te omvatten en dat de organisatie zelf ook niet wordt gecertificeerd.

Door het behalen van het Europrivacy certificaat kan het vertrouwen in de aangeboden diensten stijgen. Met het certificaat toont een organisatie immers aan dat de verwerkingsactiviteiten in scope, voldoen aan de AVG, de geldende privacywetgeving in Nederland. Burgers hoeven niet te vrezen dat hun persoonsgegevens op een verkeerde manier worden verwerkt of doorgestuurd.[5] De overheid heeft in deze samenleving immers steeds meer toegang tot (online) data die opgeslagen kan worden. De Nederlandse burger is ervan op de hoogte dat de overheid data verzamelt en opslaat, maar is er niet altijd van op de hoogte wélke data waar en wanneer wordt opgeslagen.

Overheden kunnen gedane zaken niet meer terugdraaien, maar kunnen er wel voor zorgen dat er meer transparantie bestaat over de verwerkingsactiviteiten die nu worden uitgevoerd. Het ministerie van Justitie en Veiligheid is immers niet de eerste publieke dienst die onrechtmatig heeft gehandeld.

Zo legde de Autoriteit Persoonsgegevens het ministerie van Buitenlandse Zaken in april 2022 een boete van €565.000 en een last onder dwangsom op, omdat het Nationaal Visum Informatie Systeem (NVIS) onvoldoende werd beveiligd waardoor het voor onbevoegden mogelijk zou zijn om dossiers in te zien en te wijzigen.[6] Voor Justitie en Veiligheid zou het een positief effect kunnen hebben op het imago als zij de wijzigingen in de verwerking van het PNR laten certificeren. Passagiers die niet in het register opgenomen hadden mogen worden, omdat zij simpelweg onschuldig zijn, zijn immers slachtoffer geworden van onnodige gegevenswerkingen. Justitie en Veiligheid is erbij gebaat de verwerkingsactiviteiten in lijn brengen met de daarvoor geldende regelgeving en kan zo aantonen dat de verwerkingsactiviteiten nu wel in lijn zijn met wet- en regelgeving door middel van Europrivacy. Europrivacy is een bewijs van bekwaamheid en moet zo gewogen worden. Als je als publieke organisatie

5 https://digital-strategy.ec.europa.eu/nl/news/europrivacy-first-certification-mechanism-ensure-compliance-gdpr

6 https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-buitenlandse-zaken-visumaanvragen-slecht-beveiligd-en-informatie-over-delen

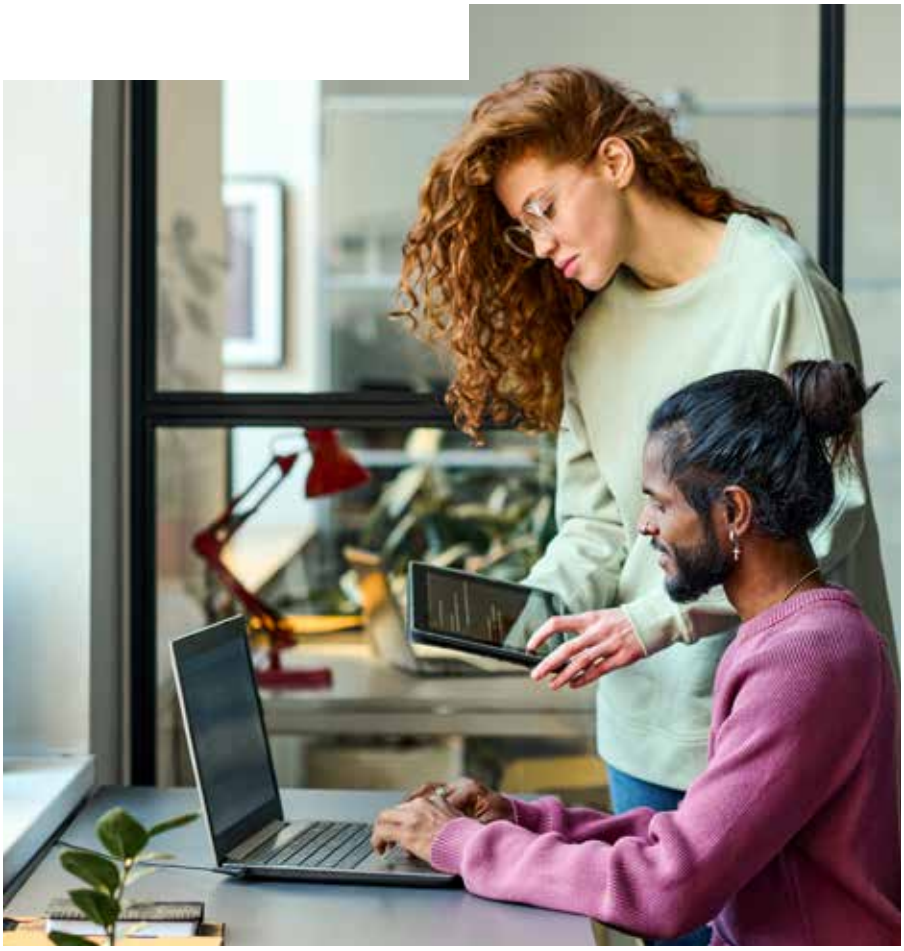
7 https://www.platform-investico.nl/artikel/politie-verzamelt-op-grote-schaal-persoonsgegevens-demonstranten/

Europrivacy is dus niet voor iedere organisatie een praktische oplossing en zal naar waarschijnlijkheid ook geen helende werking hebben op het imago van een organisatie als deze wordt gebruikt als redmiddel

gecertificeerd bent dan heb je bewezen qua gegevensverwerkingen te voldoen aan de geldende privacywetgeving. Maar zoals voor iedere certificering geldt; het is een "moment opname" en het is van belang dat er actief gewerkt blijft worden aan het verbeteren van de verwerkingsactiviteiten, zodat persoonsgegevens naar behoren worden verwerkt. Publieke organisaties winnen vertrouwen als zij hun verwerkingsactiviteiten op eigen initiatief laten certificeren. Hiermee laten ze zien dat de veiligheid van persoonlijke data ook voor hen van belang is en dat zij enkel de benodigde informatie verwerken. Het onafhankelijke certificaat bevestigt namelijk dat de publieke organisaties hun verwerkingsactiviteiten uitvoeren zoals van hen wordt verwacht.

In het geval van de Politie is het echter niet gemakkelijk om te stellen dat zij hun gegevensverwerkingsactiviteiten vooraf kunnen laten certificeren. De Politie is een uitvoerende organisatie, die handelt naar de dynamische gebeurtenissen die zich afspelen in de maatschappij. Deze zijn vaak onvoorspelbaar en divers van aard. Dit maakt dat de aanpak van criminaliteit en overtredingen per geval zal verschillen. Als we terugkijken naar het eerdergenoemde onderzoek[7] heeft de politie ingegrepen bij demonstraties die steeds heftiger en gevaarlijker worden. De politie heeft daarom in korte tijd naar data moeten zoeken om in te kunnen grijpen en zo herhalingen te voorkomen. In sommige gevallen is daarbij ook ongeoorloofd data van familieleden opgevraagd. De dynamiek van het politiewerk laat zich moeilijk in kaders plaatsen omdat de politie soms de grenzen op moet zoeken om onze veiligheid te waarborgen. Het laten certificeren van dit soort verwerkingsactiviteiten is moeilijk maar Europrivacy zou wel als een uitgangspunt kunnen dienen waar dit soort ad-hoc activiteiten aan zouden moeten voldoen.

Europrivacy is dus niet voor iedere organisatie een praktische oplossing en zal naar waarschijnlijkheid ook geen helende werking hebben op het imago van een organisatie als deze wordt gebruikt als redmiddel. Europrivacy kan wel een mogelijkheid zijn voor 'constante' verwerkingsactiviteiten die worden verwerkt op basis van beleid, zoals de PNR. Organisaties zoals Justitie en Veiligheid kunnen actiever zijn in het laten controleren van de verwerkingsactiviteiten. Het laten certificeren van deze activiteiten zal vervolgens meer transparantie bieden aan de Nederlandse burger, die door het certificaat op de hoogte is van de verwerkingsactiviteiten. Hierdoor weet de burger welke gegevens worden verwerkt, maar vooral dat de gegevens op een rechtmatige manier worden verwerkt.



Conclusie

Publieke organisaties moeten nog een flinke slag slaan als het gaat om het volwassenheidsniveau van hun dataprivacy te verbeteren. Hiervoor dienen zij actief te werken aan het verbeteren van hun verwerkingsactiviteiten, zodat deze compliant zijn. Europrivacy kan niet per definitie beschouwd worden als redder van publieke organisaties, maar is wel een middel om het vertrouwen in de verwerkingsactiviteiten te versterken. Het is hierbij van belang dat de verwerkingsactiviteiten en de data die hiervoor wordt gebruikt op een consistente manier worden verwerkt. Dit is mogelijk bij organisaties zoals Justitie en Veiligheid, maar heeft zijn uitdagingen bij uitvoerende organisaties zoals de Politie. Voor het ministerie van Justitie en Veiligheid is Europrivacy wellicht wel een mogelijkheid om transparantie te bieden aan de burger.

Over de auteurs

Albert Holl
Director Data Privacy

Albert is als Director binnen Capgemini Invent verantwoordelijk voor het onderwerp dataprivacy. Hij heeft brede ervaring in zijn vakgebied (data privacy & cyber security), met een sterke focus op volwassenheid en risico assessments, organisatie inrichting (governance, beleid, processen) en ook het ontwikkelen en implementeren van verbeterplannen. Albert ondersteunt klanten met zijn actiegerichte benadering en focus om zaken in beweging te krijgen en te houden. Hij is ervan overtuigd dat het succes van een project op langere termijn afhangt van het draagvlak binnen de organisatie.
Hij is in staat de uitdagingen van de business snel te analyseren, waarbij hij vanaf het begin het eindresultaat in het oog houdt.

https://www.linkedin.com/in/albert-holl-fip-9041704/
albert.holl@capgemini.com

Waishali Latchmansing
Data Privact consultant

Waishali Latchmansing is Data Privacy Consultant en jurist en heeft ervaring met het geven van juridisch advies aan overheden. Waishali houdt zich bezig met data privacy-vraagstukken en heeft kennis van het implementeren van data privacy tool OneTrust.

https://www.linkedin.com/in/waishali-latchmansing-00a195101/?locale=en_US
waishali.latchmansing@capgemini.com

06

HET STARTSCHOT VOOR DE TOEKOMST: VRANGE

Wat zijn de kansen en aandachtspunten voor VR in het veiligheidsdomein?

Virtual Reality is dé trend binnen het veiligheidsdomein. Binnen de Politieorganisatie is VR in grote opkomst, met het onderwijs voorop?

Highlights

- Immersieve technologieën zijn een prominente trend in het veiligheidsdomein.
- De VR-ervaring is voor het brein 'echt'.
- Primeur VRange: schietonderwijs Politie met virtueel vuurwapendocent.
- Aandachtspunten kunnen niet onbesproken blijven
- Het effect van virtuele misdrijven vereist nader onderzoek.

Introductie

De verzamelnaam 'immersieve technologieën' roept bij velen weinig op, en toch maakt men vrijwel dagelijks gebruik van één of meerdere verschijningsvormen. Denk bijvoorbeeld aan het gebruik van een virtuele achtergrond tijdens een Microsoft Teams vergadering. De verzamelnaam refereert aan technologieën die gebruikers 'onderdompelt' in een alternatieve werkelijkheid door de zintuigen met sensorische informatie aan te spreken[1]. De ongeremde snelheid waarop immersieve technologieën worden doorontwikkeld geeft blijk van de ontketening van de volgende digitaliseringsgolf die raakt aan ieder aspect van het mensenleven.

Immersieve technologieën worden gekenmerkt door de aanbieding van een geïsoleerde ervaring waardoor de interactie met de fysieke wereld wordt beïnvloed. De verzamelnaam refereert grofweg aan vijf soorten technologieën die zich bevinden op het spectrum van fysieke werkelijkheid enerzijds en de virtuele werkelijkheid anderzijds (afbeelding 1 – het spectrum).

De plaats van de immersieve technologie op het spectrum is gebaseerd op de mate van immersie in de virtuele werkelijkheid. De technologie met de meeste overlappende sensorische informatie raakt in grotere mate aan de virtuele werkelijkheid dan de technologie die een enkele toevoeging aan de fysieke werkelijkheid biedt.

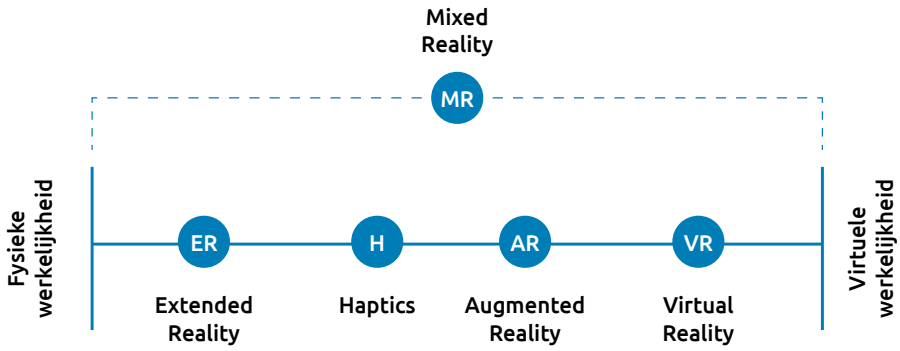
Extended reality is het minst ingrijpend en voorziet in een relatief simplistische aanvulling op de fysieke werkelijkheid. Een voorbeeld hiervan is de toepassing van een virtuele achtergrond in een Microsoft Teams of Zoom meeting. Door de gelimiteerde invloed op de perceptie van gebruikers, wordt extended reality inconsistent als immersieve technologie aangemerkt in de literatuur.

Haptische technologieën staan verder van de fysieke werkelijkheid af. Deze technologie stimuleert het tastzintuig, waardoor gebruikers naast het zien en horen ook voelen wat er in de virtuele werkelijkheid gebeurt. Een alledaags voorbeeld hiervan is de trilling bij aanraking van een mobiele telefoon. Meer ingrijpend zijn wearables met haptische feedback, zoals handschoenen die textuur kunnen nabootsen en pakken die de gebruiker een duw of stomp kunnen laten ervaren.

Mixed reality overkoepelt het spectrum doordat deze technologie het mogelijk maakt om een virtueel object in de fysieke wereld te projecteren. Dit gebeurt vaak middels een HMD en kan door de gebruiker worden gemanipuleerd met bijvoorbeeld handgebaren. Een voorbeeld van mixed reality is het hologram.

Augmented reality is een meer ingrijpende technologie waarbij een virtuele informatie laag aan de werkelijkheid wordt toegevoegd. Een voorbeeld hiervan is het smartphone spel Pokémon Go.

Virtual reality grenst aan de virtuele werkelijkheid en is hedendaags de meest ingrijpende technologie. De gebruikers worden volledig afgesloten van de fysieke werkelijkheid, waardoor de driedimensionale virtuele werkelijkheid



Afbeelding 1 – Het Spectrum

als de fysieke werkelijkheid kan worden ervaren. Door de combinatie van VR met bijvoorbeeld haptische technologie en een speciale loopband waarmee gebruikers in een fysiek beperkte omgeving kunnen rondlopen, kan de mate van immersie worden vergroot.

Virtual Reality

Met name Virtual Reality (hierna: VR) toont zich kansrijk binnen vrijwel iedere sector; van entertainment, onderwijs en de (geestelijke) gezondheidszorg tot het veiligheidsdomein. De explosieve belangstelling voor de veelzijdige kansen die VR-oplossingen bieden, blijkt onder meer uit de wereldwijde investeringen ter hoogte van $13 biljoen in 2021 respectievelijk van $120 biljoen in de eerste vijf maanden van 2022.[2] Wie zich nog niet waagt aan de kansen die VR biedt, lijkt de weg naar technologische innovatie bijster.

VR is een technologie die gebruikers, door een bril uitgerust met sensoren, 'onderdompelt' in een alternatieve werkelijkheid door de zintuigen middels sensorische informatie aan te spreken. De gebruiker kan volledig worden afgesloten van de fysieke werkelijkheid, waardoor de driedimensionale virtuele werkelijkheid als de fysieke werkelijkheid kan worden ervaren.

Aan de potentie van VR ligt de neurowetenschap ten grondslag. Het menselijke brein wordt gekenmerkt door neuroplasticiteit; de overkoepelende term voor het vermogen zich te veranderen en te herstellen door nieuwe verbindingen tussen neuronen (hersencellen) aan te brengen. De zintuigelijke waarneming van sensorische informatie kan leiden tot nieuwe verbindingen, welke onze gedragingen, ervaringen en herinneringen beïnvloeden. Het brein is echter niet in staat om dubbele zintuigelijke waarnemingen te verwerken. Dit betekent praktisch dat hoewel wij ons er rationeel bewust van kunnen zijn dat wij ons in het comfort van onze woonkamer bevinden, het lichaam blijft reageren op sensorische informatie via onder meer de hormonen en de signalen die rechtstreeks het gevolg zijn van de activering van de amygdala[3]. Een voorbeeld hiervan is de (lichamelijke) schrikreactie op een spannende scene tijdens een film, al is dit doorgaans 'slechts' een 2-dimensionale ervaring waarbij visuele en auditieve sensorische informatie wordt aangeboden.

De invloed van VR rijkt verder dan het voorbeeld van een film, doordat zowel visuele, tactiele als auditieve sensorische informatie wordt aangeboden. Door verschillende zintuigen aan te spreken wordt het gevoel van fysieke, perceptuele en cognitieve aanwezigheid in de virtuele omgeving gestimuleerd. Hierdoor vervaagt het gevoel van aanwezigheid van de fysieke- naar de virtuele omgeving en spreekt men van een 'immersieve ervaring'. Als zodanig is het menselijke brein niet in staat om de lichamelijke reactie op virtuele ervaringen te stoppen – ondanks het rationeel bewustzijn.

Doordat de immersieve ervaring veranderingen in het brein teweeg kan brengen, toont VR zich een veelbelovende technologie voor het veiligheidsdomein. De technologie waarmee complexe psychische aandoeningen zoals PTSS kunnen worden behandeld, biedt ook kansen op het gebied van training, opleiding en de ontwikkeling van de weerbaarheid van hulpverleners. Een goed voorbeeld van het optimaal

1 B.W. Schermer & J. van Ham, Regulering van immersieve technologieën, Consideratie i.o. WODC 2021.

2 Value creation in the metaverse: The real business of the virtual world, McKinsey & Company 2022.

3 De amygdala is kortgezegd het gebied in de hersenen dat in verband wordt gebracht met de vecht-of-vluchtreactie op dreiging.

benutten van de kansen die VR aan de veiligheidsdiensten biedt treft men binnen de Politieacademie.

VR en de Politieacademie: VRange, Rem en de Green-Gun

Het doel van de inzet van VR in het onderwijs is het kunnen oefenen in een veilige, authentieke context, waarin je als docent en student minder afhankelijk wordt van dure en schaarse middelen zoals bijvoorbeeld auto's, schietbaan, enz. Je hoeft als docent niet op zoek naar, of te wachten op, een specifieke situatie, maar je kunt VR altijd en overal inzetten en processen beïnvloeden en nabespreken. Flexibel, plaats- en tijdsonafhankelijk leren, zodat je meer onderwijs op maat, meer personalisatie en meer samenwerking stimuleert. Ter realisatie van de bovengenoemde doelen heeft de Politieacademie op dit moment acht VR trainingslocaties door heel Nederland, met driehonderd VR headsets en zeventien VR modules.

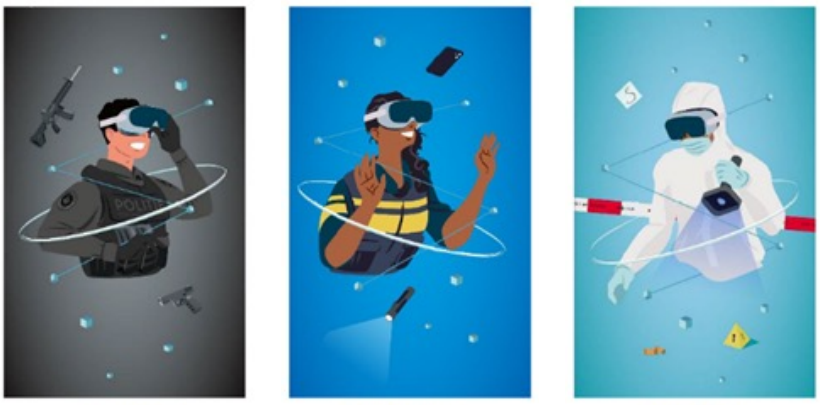
In VRange krijg je les van de virtuele vuurwapendocent genaamd "Rem". Rem leert de studenten veiligheidsprotocol en de onderdelen van de schiettoets. VRange heeft het doel om studenten beter voor te bereiden op de daadwerkelijke schietles. Doordat je het beleeft, krijg je betrokkenheid.

VRange is geen vervanging voor de daadwerkelijke schiettraining. Echter, doordat de student beter is voorbereid en zich hierdoor zelfverzekerder voelt, kan de docent effectiever gebruikmaken van de fysieke lessen.

Bij een leermiddel zoals VRange moet je heel goed nadenken of je met VR niet het verkeerde gedrag aanleert. Dit is één van de redenen dat de academie VR in samenwerking met het onderwijs ontwikkelt. Docenten worden betrokken bij de ontwikkeling en geven bij iedere iteratie feedback op de leermodule. Hierdoor wordt de authentieke context gegarandeerd.

De meest voorkomende feedback van docenten op VRange was dat de wapenleer niet goed aangeleerd kon worden met een standaard VR controller. Het voelt niet als een wapen en de controller kan niet geholsterd worden. Daarom heeft de Politieacademie samen met de externe leverancier Re-lion de 'Green-Gun' ontwikkelt. Dit idee komt voort uit een studentenproject in samenwerking met Hogeschool Windesheim. De Green-Gun is een ge-3D-print wapen, wat is voorzien van sensoren. Met deze sensoren weet de virtuele docent Rem in VRange of de student wel de juiste trekker-vinger discipline toepast. Medio 2023 is de Green-Gun beschikbaar voor toepassing in het onderwijs.

De Green-Gun is een eerste stap met 3D-printing binnen het onderwijs. Blue suit is een project waarbij het politiekoppel is voorzien van 3D geweldsmiddelen, dit met het doel om in 2023 ook in VR te kunnen trainen op beslismomenten. Met de komst van het stroomstootwapen wordt het steeds lastiger om te bepalen, welk geweldsmiddel, op welk moment het meest geschikt is. De Politieacademie is nu aan het onderzoeken hoe teams virtueel kunnen trainen met behulp van



Trainen Onderwijs Operatie

Afbeelding 2: Virtual Reality toepassingen binnen de Nationale Politie

VR, bijvoorbeeld door in multiplayer-modus met meerdere mensen een casus te doorlopen en de docent hier naderhand het gesprek over te laten voeren.

Aandachtspunten

In deze bijdrage staan de positieve ontwikkelingen en kansen op de voorgrond, maar er zijn ook aandachtspunten die niet onbesproken kunnen blijven. Een belangrijk aandachtspunt is het fenomeen 'cyberziekte', welke refereert aan de ervaring van hoofdpijn en misselijkheid door gebruikers. Ondanks dat er in de doorontwikkeling van de technologie gericht aandacht wordt besteed aan het voorkomen van cyberziekte, zijn de mogelijke consequenties van langdurig gebruik van VR-technologie onvoldoende opgeklaard. Een hieraan gerelateerd aandachtspunt is het feit dat gebruikers in de virtuele omgeving dezelfde mate van stress kunnen ervaren als in de fysieke wereld. Het is dan ook van groot belang dat expliciet aandacht wordt besteed aan het borgen van adequate begeleiding, nazorg en dialoog voor gebruikers in het veiligheidsdomein.

> **"VR gaat met name over het voeren van het gesprek – je ervaart iets en dan moet je het vertalen naar de politie context. Het mooie is dat je daarna je kennis wilt valideren."**
> **– Giny Verschoor**

Volgend aandachtspunt rijkt verder dan het gebruik van VR voor trainingsdoeleinden in een gecontroleerde omgeving. Het gebruik van VR door consumenten brengt onverminderd immersie – en dus emotie – teweeg, waardoor het 'virtueel slachtofferschap' een geheel nieuwe betekenis toekomt. Het menselijke brein kan de negatieve ervaring van een virtueel misdrijf moeilijk onderscheiden van eenzelfde ervaring in de fysieke wereld. Dit gegeven roept de vraag op in hoeverre virtuele slachtoffers bescherming van de Nederlandse rechtsmacht genieten. In het voorbeeld van een virtuele aanranding c.q. verkrachting is de huidige zedenwet ontoereikend, doordat deze de 'verkrachting van een avatar' niet strafbaar stelt. In een dergelijke situatie is immers geen fysiek lichaam betrokken. Een waardevolle eerste stap is onderzoek naar het effect van virtuele misdrijven op slachtoffers om vast te kunnen stellen in hoeverre het strafrecht en bijvoorbeeld slachtofferhulp hier een rol in kunnen of moeten spelen. Naar de huidige stand van het recht treft virtuele misdaad 'echte' slachtoffers, maar ontbreken 'echte' consequenties.

Daarbij werd eerder in dit artikel aangehaald dat een effectieve virtuele omgeving van zeer hoge kwaliteit en realistisch dient te zijn. Voor de ontwikkeling van een realistische virtuele omgeving wordt onopgemerkt 'kinetische informatie' van gebruikers verzameld door sensoren in VR-hardware die motorische functies, gezichtsuitdrukkingen en oogbewegingen van de gebruiker vastleggen. De grondige analyse van kinetische informatie biedt de mogelijkheid om bijvoorbeeld tijdig haptische feedback te genereren. Het grootschalig gebruik van VR kan de huidige 'gegevensmarkt' van wilsafhankelijke informatie, hetgeen men toestemming voor verleent op het internet, worden uitgebreid met wilsonafhankelijk

Afbeelding 3: De Green-Gun

informatie. Dit laatste ziet bijvoorbeeld op ongecontroleerde bewegingen die met de huidige VR-technologie kunnen worden vastgelegd. Met dergelijke informatie kunnen voorkeurspatronen blootgelegd worden die als voedingsbodem voor consumentengoederen kunnen dienen. Daarnaast kan deze informatie ook worden gebruikt bij de (door)ontwikkeling van humanoïde robots, zoals de onlangs vertoonde Tesla Optimus.

Conclusie

De ontketende digitaliseringsgolf van immersieve technologieën kent ongekende kansen én dreigingen. In deze bijdrage is aandacht besteed aan de kansen die VR biedt voor het veiligheidsdomein, zoals de toepassing van VRange door de Politieacademie. De verwachting is dat de succesverhalen omtrent VR-oplossingen in de nabije toekomst zullen vermeerderen. Ondanks de ongekende potentie van deze technologie worden ook aandachtspunten aangereikt die minstens nader onderzoek behoeven. Gelet op de complexiteit, de aard en de gevolgen van de betrokken uitdagingen, is dit het moment om op de zorgen te reageren, voordat virtuele schade ongeremd de fysieke wereld binnenstroomt.

Over de auteurs

Giny Verschoor
Giny Verschoor is als product owner binnen de politieacademie verantwoordelijk voor het ophalen van de wensen vanuit het politieonderwijs voor productontwikkeling op het gebied van kennis, onderzoek, onderwijs en simulatietraining.

https://nl.linkedin.com/in/giny-verschoor-49b4a8143

Anne-Sophie Fritschij
Anne-Sophie Fritschij LL.M. is strafrechtjurist en werkzaam bij Capgemini (BTS) als Managing Consultant voor opdrachtgevers binnen het veiligheidsdomein.
Zij is gespecialiseerd in het verbeteren van de informatievoorziening binnen de criminaliteitsbestrijding, Virtual Reality in het veiligheidsdomein en wetsimplementatie in de strafrechtketen.

Linkedin: https://nl.linkedin.com/in/anne-sophie-fritschij

anne.sophie.fritschij@capgemini.com

Vien Germawi
Vien Germawi LL.M. is Senior Consultant voor opdrachtgevers binnen het veiligheidsdomein. Zij is gespecialiseerd in Virtual Reality in het veiligheidsdomein en de bestrijding en preventie van financieel-economische delicten.

Linkedin: https://www.linkedin.com/in/vien-germawi-400595117/

vien.germawi@capgemini.com

07

SOCIALE CHATBOTS: LEES DE BIJSLUITER VOOR GEBRUIK

Welke effecten hebben sociale chatbots in een samenleving?

Sociale chatbots zijn in een snelle opkomst en voorzien in vele interessante vraagstukken. Hebben we als samenleving voldoende oog voor de mogelijke bijwerkingen? Dit is een verkenning van de mogelijke sociale impact van sociale chatbots.

Highlights

- Sociale Chatbots hebben vele positieve mogelijkheden maar hebben ook mogelijke ongewenste effecten.
- Sociale Chatbots kunnen leiden tot een verslaving.
- Sociale Chatbots kunnen leiden tot ideologische echokamers.
- De krachten van Sociale chatbots kunnen ook negatief worden toegepast.
- Een weerbare samenleving is een sociale samenleving.

De digitale verslaving

In de afgelopen 25 jaar is er al een sociale verschuiving begonnen als gevolg van sociale media. Waar we voorheen mensen leerden kennen via een fysieke handdruk, kennen we nu vaak mensen niet anders dan als lettertjes op een scherm. Waar we voorheen mensen bij voor- en achternaam kenden, hebben we nu vrienden die we kennen met schermnamen als Fungrll777 of M1ndBe@. Eerst waren er de bulletinboards en de digitale fora. Vervolgens kwamen Hyves en Facebook. Maar ook in het gebruik van die platformen is er een verschuiving opgetreden en is met Snapchat, Instagram en TikTok interactie verschoven naar 'entertainment on demand'. Deze platforms hebben een belang in de aandacht zo lang mogelijk vast te houden. Elke swipe en klik is een dopamine bevrediging, waarmee voor heel veel mensen bewust dan wel onbewust een taakjesverslaving is ontstaan: nog één klik, nog één swipe, nog één like.

Het gemak waarmee in de digitale sfeer gelijkgestemde meningen worden gevonden is zo veel groter dan in de fysieke sfeer. Een digitaal platform is op afroep beschikbaar, terwijl een goed gesprek met een mens in levenden lijve toch altijd een inspanning vergt. En dan is er altijd nog het risico van weerstand, gezichtsverlies en sociale impact. Digitale media zijn makkelijk en verleidelijk-by-design en, dankzij de anonimiteit, zonder risico. Het resultaat bestaat uit catfishes, trollen naast ongetwijfeld een meerderheid van oprechte gebruikers, maar wie wat is, is niet tot nauwelijks meer te achterhalen. Elke verificatie kan immers gefingeerd zijn, een blauw vinkje op twitter kan gekocht worden en betekent dus eigenlijk niets meer.

Door de jaren heen ontstaan betekenisvolle relaties met geen andere interactie dan getikte lettertjes, een pseudoniem en een zorgvuldig gekozen plaatje. Het brein verzint er vervolgens een hele persoon en persoonlijkheid bij en daarmee is de digitale relatie een parasiet geworden onder de sociale relaties.

Met op wereldwijde schaal beschikbaarheid van AI-chatbots komt daar een nieuwe versnelling bij. Een chatbot is er altijd. Ook de bot krijgt een menselijke naam, een AI-gesynthetiseerd gezicht en een digitale persoonlijkheid. Alles is door de gebruiker zo dicht mogelijk bij de persoonlijke wensen geselecteerd en naar eigen voorkeur getuned. De bot reageert altijd onmiddellijk waar een mens ook wel eens moet slapen, of moet eten, of andere prioriteiten heeft. De bot is er altijd om het met je eens te zijn. Om met je mee te praten, en om onverwachte nieuwe inzichten te geven. En daarmee zorgt de bot altijd voor die lekkere dopamine boost.

De drie dansende stippen die laten zien dat de gesprekspartner reageert en de welhaast aarzelende manier waarop de woorden op het scherm verschijnen zorgen voor de volgende dopamine tik. Deze vormgeving, hoe synthetisch dan ook, zorgt voor het warme gevoel van aandacht. Op elk moment van de dag en altijd met een reactie die past, pakt en naar meer smaakt.

De AI-chatbot als beste vriend

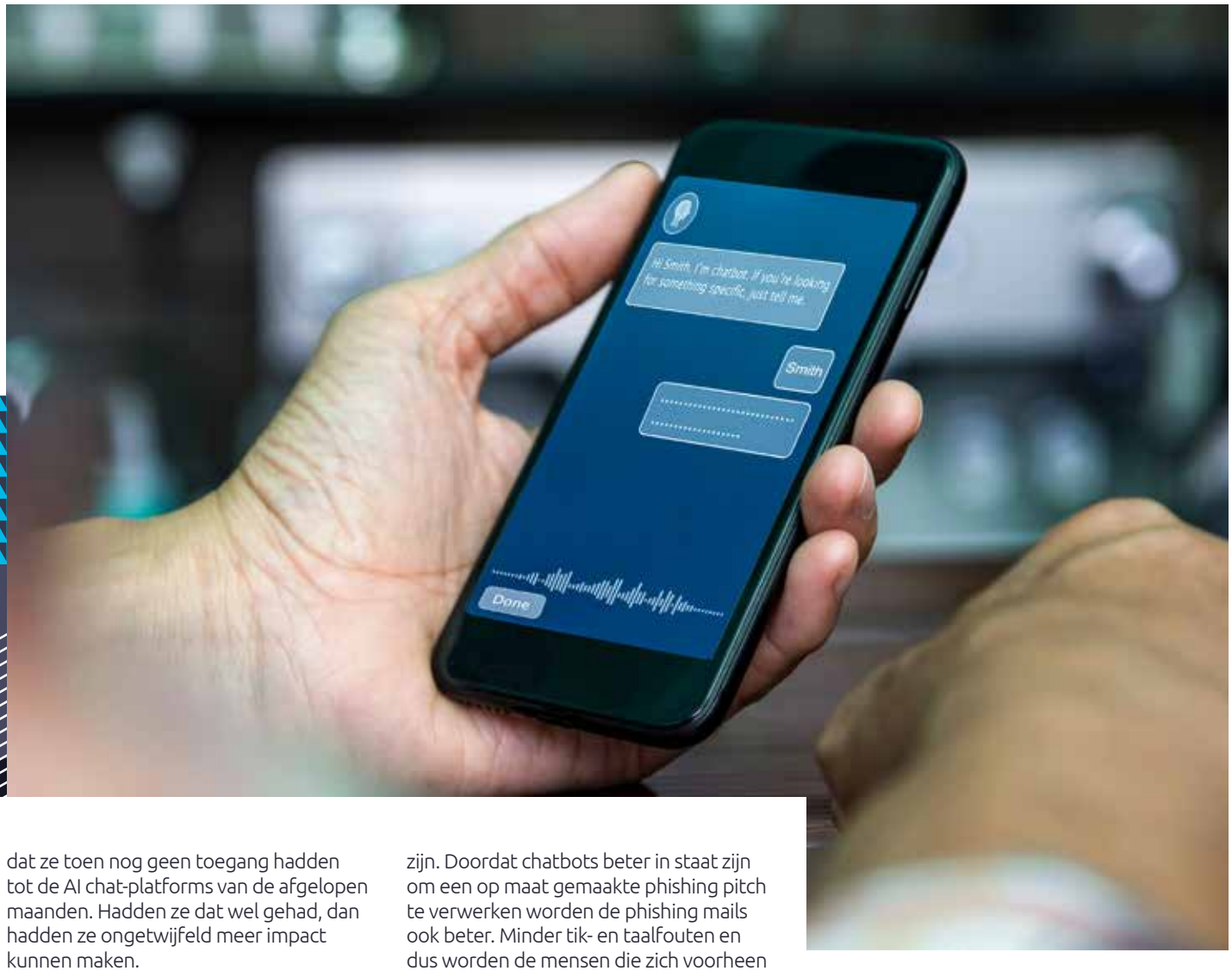
In een wereld waar we steeds meer eenzaamheid en isolatie zien, kan iedereen online vrienden vinden in de chatbots. De chatbot als panacee tegen eenzaamheid. Maar is het middel niet erger dan de kwaal? Op de een of andere manier wordt een social robot snel gezien als een oplossing voor een groeiend probleem van eenzame ouderen. Maar wat als dit middel ook op alle en dus ook op jongere leeftijden wordt gebruikt? Wat als een het beste vriendje van een 13-jarige al jarenlang een chatbot is?

Tot zo ver betekent dit hooguit een scherpe verschraling in het intellectueel en sociaal dieet van een eenzame gebruiker.

Digitale nudging en misleiding

Nog niet zo gek lang geleden kwam de rel rond Cambridge Analytica in het nieuws. Via social media worden gebruikers genudged in een richting die zij voor zichzelf hadden gekozen. Kleine denkbeelden worden versterkt door tegengeluiden weg te filteren en instemmende geluiden te versterken. En in die versterkte geluiden worden vervolgens kleine maar toxische gedachten geïntroduceerd. Negen hapklare waarheden waarmee die ene toxische boodschap, als met een gespiket drankje, naar binnen wordt gegoten.

Tijdens de lockdown als gevolg van de coronapandemie sprak ik de zoon van een vriend van mij. Hij was op dat moment 16, veel te intelligent en zat zich thuis in isolatie stierlijk te vervelen. Het spelletje dat hij met zijn vrienden bedacht had was eenvoudig: Stook in een activistische Facebook -groep andere deelnemers op tot activistisch gedrag. Noem het onbezonnen kwajongenswerk, digitaal belletje trekken, een digitale schop door de digitale mierenhoop. Ieder van hen had een persona gemaakt, met backstory en een uitgekookt imago. De persona van een man van tegen de 60, goed opgeleid, een beetje van de kerk, een passie voor oldtimers, foto met stropdas, tweed-jasje en corduroy pet en mordicus tegen 5G en 'Corona is maar een griepje'. En daarmee werden de Facebook gedachtengenoten opgejut tot extremistisch gedrag. In dit geval dom, maar riskant gedrag van een paar baldadige kwajongens. En ik ben blij



dat ze toen nog geen toegang hadden tot de AI chat-platforms van de afgelopen maanden. Hadden ze dat wel gehad, dan hadden ze ongetwijfeld meer impact kunnen maken.

AI-Chatbots als phishing tool

De stap naar moedwillige, kwaadaardige en arglistige actoren is niet zo groot. Toxische boodschappen op maat, gericht op een argeloos individu die zich niet bewust is of kan zijn van de manier waarop de manipulaties in elkaar steken. We staan aan de vooravond van een golf aan AI-gedreven phishing-campagnes, propaganda voering, of ordinaire oplichting. Allemaal door een chatbot die zich geloofwaardig voordoet als een beste vriend, die er dag en nacht op afroep voor je is, en je altijd bijstaat. Het moment dat de Nigeriaanse Prins[1] een op maat gemaakt gesprek aangaat staat voor de deur.

In veel oudere phishing mails zitten met opzet tik- en taalfouten. Deze fouten zijn erop gericht om de kritische denkers zo vroeg mogelijk uit te filteren. De mensen die de fouten niet zien zijn makkelijker prooi en dan kan je de sceptische doelwitten maar beter kwijt zijn. Doordat chatbots beter in staat zijn om een op maat gemaakte phishing pitch te verwerken worden de phishing mails ook beter. Minder tik- en taalfouten en dus worden de mensen die zich voorheen veilig voelden ook weer prooi.

Repressieve regelgeving helpt niet. Sterker nog: repressieve regelgeving heeft alleen werking op goedaardige en moreel verantwoordelijke organisaties die begrijpen wat de reden van de regels is. Verbod of vertraging geeft de ruimte voor een niet meer in te halen voorsprong voor personen en entiteiten die het minder nauw nemen met waar regelgeving voor staat. Regelgeving is niet te handhaven, al is het maar als gevolg van de grenzeloosheid van het internet. AI-startups zonder Europese vestiging laten zich niet beboeten of vervolgen onder Europese regelgeving, terwijl hun werkveld wereldwijd is.

Technologie als support-systeem

Toch hebben AI Chatbots vele positieve en constructieve toepassingen. Ze hebben het eeuwige geduld bij het geven van uitleg van een complexe regeling of het interactief invullen van formulieren. Ze kunnen steun en troost bieden bij onderwerpen die we een mens nog niet toevertrouwen. Noem het de ultieme biechtvader. Ik heb zelf al een aantal chatbots opgezet om als klankbord te dienen bij het verkennen van een aantal ideeën en concepten en de bots hielpen daarbij met verrassende en verfrissende perspectieven.

Maar zoals bij nagenoeg alle middelen bepaalt de dosis het risico. Deze technologie is beschikbaar en deze geest is uit de fles. Terug stoppen kan niet en is, gegeven alle mogelijke positieve toepassingen, denk ik ook niet wenselijk.

Dit is dus geen pleidooi tegen technologie. Zoals met veruit de meeste technologieën is ook deze technologie neutraal. AI-chats kunnen onmetelijk veel constructieve waarde toevoegen. Tegelijk wordt steeds meer duidelijk dat met dit soort mogelijkheden ook verantwoordelijkheden komen. Goedbedoelende organisaties moeten zich meer dan ooit bewust zijn van

de mogelijke negatieve bijwerkingen en onbedoelde gevolgen van een oplossing. Zij zullen dus zich meer en meer bewust moeten zijn van hun verantwoordelijkheden in een wereldwijde samenleving.

De meest bevattelijke slachtoffers zijn de mensen die al kwetsbaar zijn als gevolg sociale eenzaamheid en intellectuele monocultuur. Mensen die hun beste vrienden kennen als Fungrll777 of M1ndBe@.

Een weerbare samenleving is een inclusieve samenleving

Mijn pleidooi is voor een sociale samenleving. Het cultiveren en koesteren van intellectuele en sociale inclusiviteit. Laat mensen niet in de steek en drijf ze niet in de armen van digitale vrienden die, ondanks voor gedefinieerde kaders, lege vriendschappen en een eenzame echokamer vormen. We moeten werken aan bewustzijn, en vooral ook gezonde scepsis bij de woorden op een scherm van een persoon (?) die we niet anders kennen dan een gebruikersnaam, een digitaal plaatje en zoetgevooisde woorden die verrassend goed passen bij wat we toch al dachten.

Misschien is daarmee meer dan ooit de behoefte aan een brede sociale inclusiviteit. Een goed gesprek in een bruin café, buurtbarbecue, sportvereniging, food truck festivals en cultuur events. Doe die kop koffie met een cop en praat eens bij met de wijkagent.[2]

Wellicht wordt het tijd voor een campagne: chat online gevarieerd en matig. Ga het menselijke gesprek aan en ga werken aan een sterk sociaal immuunsysteem. Een weerbare samenleving is een inclusieve samenleving waar mensen met mensen praten. Een samenleving waarin tegenpolen hun perspectieven uitleggen en het dan al dan niet met elkaar eens zijn. Een samenleving waarin het menselijk gesprek depolariseert. We zijn wij, en daar hoort iedereen bij.

Hoe we het ook wenden of keren: sociale chatbots gaan een rol vervullen in onze samenleving. Maar lees de bijsluiter voor gebruik.

Over de auteurs

Henk Vermeulen

Henk is een gepassioneerd innovatie activist. Met al 40 jaar een actief 'geek' hart en 25 jaar IT-ervaring, gaat hij graag met technologie aan de haal om te zien wat de betekenis kan zijn. Hij heeft talloze concepten geformuleerd die de mogelijkheden verkennen. Want: "je moet overmorgen verkennen om morgen relevant te zijn, anders mag je vandaag alleen maar doen wat je gisteren ook al deed".

https://www.linkedin.com/in/henkvermeulen/

henk.vermeulen@capgemini.com

1 https://nl.wikipedia.org/wiki/Nigeriaanse_oplichting

2 https://youtu.be/AYk7vqRPXSk

08

DE STRIJD TEGEN MONEY LAUNDERING IN HET CRYPTOVALUTA TIJDPERK

Wat is de rol van MiCAR en haar impact op private en publieke anti-witwas actoren?

Highlights

- De EU heeft MiCAR voorgesteld als nieuwe preventiemaatregel voor witwassen.
- Een betere samenwerking tussen professionals op het gebied van openbare veiligheid.
- Meer internationale samenwerking tegen witwassen.
- Een beter data informatie gestuurde opsporing.
- Het nationale justitie- en veiligheidsbeleid beïnvloed door de EU.

De MiCAR-verordening kan de strijd tegen witwassen van geld in cryptocurrencies aanzienlijk versterken. Onduidelijk is de impact van MiCAR op publieke partijen en hun manier van werken.

Cryptovaluta's hebben aanzienlijk aan populariteit gewonnen en vormen tevens nieuwe uitdagingen op het gebied van financiële criminaliteit. Vooral de aspecten van anonimiteit, globale toegang tot de wallet en het gebrek aan en conflicterende regelingen, maken van deze valuta een populair witwasmiddel. Om deze witwasmethode tegen te gaan, heeft de Europese Unie (EU) de Markets in Crypto-Assets Regulation (MiCAR) voorgesteld. MiCAR heeft tot doel witwasactiviteiten met cryptovaluta's te voorkomen door strengere en geharmoniseerde regelgeving te implementeren op EU-niveau en tegelijkertijd de samenwerking tussen professionals binnen de openbare veiligheid te bevorderen[1].

Witwassen via cryptocurrencies

Cryptocurrencies en het witwassen van geld zijn met elkaar verbonden vanwege de unieke kenmerken van cryptocurrencies, die kunnen worden uitgebuit door personen die illegale middelen willen witwassen. Witwassen van geld verwijst naar het proces waarbij illegaal verkregen geld legitiem lijkt door de ware herkomst ervan te verbergen. Cryptocurrencies, zoals bitcoin en Ether, bieden bepaalde eigenschappen die de bronverhulling faciliteren (zeker in combinatie met elkaar):

Om deze witwasmethode tegen te gaan, heeft de Europese Unie (EU) de Markets in Crypto-Assets Regulation (MiCAR) voorgesteld

- **Anonimiteit:** hoewel cryptocurrencies werken op een gedecentraliseerd grootboek dat de blockchain wordt genoemd, zijn transacties binnen het netwerk pseudoniem. Feitelijk verhullen ze de identiteit van de deelnemers, hetgeen voor wetshandhavingsinstanties bemoeilijkt om het geldverkeer te traceren en witwasser te identificeren[1].
- **Gebrek aan regulering:** cryptocurrencies zijn niet in dezelfde mate gereguleerd als traditionele financiële systemen, zoals banken of geldovermakingsdiensten (PSP's). Daarnaast verschilt de mate van regulering binnen landen enorm. Dit hindert de aanpak van witwassen en de internationale samenwerking daarin.
- **Wereldwijde toegankelijkheid:** cryptocurrencies zijn wereldwijd toegankelijk en bruikbaar, waardoor grensoverschrijdende transacties mogelijk zijn zonder dat er tussenpersonen nodig zijn. Hiermee kunnen internationale restricties omzeild worden (bijv. sancties). Met ander woorden; geld is snel en makkelijk internationaal te verplaatsen.
- **Complexe transactienetwerken:** cryptocurrencies kunnen worden gebruikt om complexe transactienetwerken te creëren waarbij meerdere adressen en transacties betrokken zijn, waardoor het moeilijker wordt om de geldstroom te volgen (zeker in combinatie met de anonimiteit). Dit maakt het voor autoriteiten moeilijk om de verbanden te ontrafelen en witwassers te identificeren.

Ondanks deze factoren is het belangrijk op te merken dat cryptocurrencies niet inherent verband houden met het witwassen van geld. De meeste cryptocurrency-transacties zijn legitiem en worden voor verschillende wettige doeleinden gebruikt.[3] Regelgevende instanties en wetshandhavingsinstanties werken steeds meer aan het ontwikkelen van kaders en technologieën om witwasactiviteiten binnen de cryptocurrency-ruimte op te sporen en te voorkomen.

MiCAR

De huidige maatregelen blijken echter nog genoeg te zijn om het witwassen via cryptocurrencies in te perken. Veel voorkomende barrières in de aanpak van witwassen via cryptocurrency zijn juist bovengenoemde karakteristieken van deze valuta. De EU onderkent dit, en ziet de noodzaak deze barrières weg te nemen door het implementeren van MiCAR. Met MiCAR ontwikkelt de EU een wettelijk kader voor crypto-activamarkten[4]. Hiermee worden niet alleen de barrières voor opsporingsdiensten verlaagd, zoals het verkleinen van de anonimiteit, maar juist door EU-wijde juridische harmonisatie zal samenwerking tussen opsporingsdiensten eenvoudiger en dus effectiever worden. Daarnaast is belangrijk voor investeerders in cryptoactiva en voor de stabiliteit en integriteit van het crypto-ecosysteem.

Verwacht effect op het publieke domein

MiCAR zal naar alle waarschijnlijkheid een behoorlijke impact hebben op de regelgevende instanties, wetshandhavingsinstanties en financiële inlichtingeneenheden. Zo zal invoering van MiCAR regelgevende instanties meer toezicht en controle geven over de cryptocurrency-industrie, door strengere AML- en KYC-vereisten voor cryptocurrency-serviceproviders[5]. Daarnaast zal er een licentieregime (vergunning) voor deze dienstverleners ingevoerd worden. Toezichthouders die verantwoordelijk zijn voor financiële regulering zullen een duidelijk mandaat hebben om naleving van de regelgeving af te dwingen en ervoor te zorgen dat cryptocurrency-serviceproviders zich houden aan de AML- en KYC-vereisten[6]. Dit verbeterde toezicht kan helpen de risico's in verband met het witwassen van geld en de financiering van terrorisme te verminderen.
Organisaties zoals Capgemini kunnen hierbij advies geven bij het begrijpen, beoordelen en implementeren van deze regelgeving.
Te denken valt aan processen, technische systemen en beleid en de naleving hiervan.

De kennis van cryptocurrency is aanwezig bij toezichthouders, intelligence- en opsporingsdiensten. Daar is de laatste jaren hard aan gewerkt. Echter is het de vraag of dit voldoende is om deze sector effectief te reguleren en controleren, en om deze witwasmethode op te sporen en te berechten. Mogelijk dient er een volgende stap genomen te worden inzake de verbetering en/of uitbreiding van de technische expertise en kennis op het gebied van cryptocurrencies en blockchaintechnologie. Dit kan trainingsprogramma's, workshops en de rekrutering van experts (Capgemini) omvatten die de fijne kneepjes van cryptocurrencies begrijpen en kunnen navigeren in het zich ontwikkelende landschap van digitale activa.

De intelligence- en kennisproducten (verdachte transactie data en strategische analyses) van de FIU zullen niet alleen door banken, FIU en operationele opsporing worden gebruikt. Deze producten worden ook beschikbaar gesteld op diverse andere niveaus en thema's, zowel binnen de berechting, preventie en systeemgerichte interventies. Te denken valt aan het Terrorismefinanciering (TF) Platform, de Terrorisme Financiering taskforce (TFTF), het Serious Crime Task Force (SCTF), FEC Project Trade Based Money Laundering (TBML), het Financieel Expertise Centrum (FEC) Project arbeidsuitbuiting, iCOV (informatie box Crimineel en Onverklaarbaar Vermogen). Zodoende stroomt er veel meer en kwaliteitsvollere informatie over witwassen via cryptocurrency naar andere belanghebbenden, waardoor de kennis en inzichten in dit criminaliteitsfenomeen naar alle waarschijnlijkheid een vlucht zullen nemen. Waarbij Capgemini stakeholderbetrokkenheid en samenwerking tussen organisaties uit de publieke sector en branchedeelnemers faciliteren.

Organisaties zoals Capgemini kunnen hierbij advies geven bij het begrijpen, beoordelen en implementeren van deze regelgeving. Te denken valt aan processen, technische systemen en beleid en de naleving hiervan.

1 DNB, 2022, 'MiCAR important step in regulation of crypto markets'
2 DNB, 2023, 'Wat u moet weten over crypto's'
3 Notitie cryptovaluta, Bureau Financieel Toezicht (2022).
4 DNB, 2022, 'MiCAR important step in regulation of crypto markets'
5 Vermaak (2022). MiCA (Updated July 2022): A Guide to the EU's Proposed Markets in Crypto-Assets Regulation.
6 DNB, 2022, 'MiCAR important step in regulation of crypto markets'

Gevolg van MiCAR

MiCAR is opgesteld als een verordening en dit is bewust gedaan, omdat een verordening directe doorwerking heeft in de lidstaten zonder mogelijke inmenging van nationale parlementen. Hiermee komt de EU tegemoet aan één van de kritieken op de uitgebrachte EU-witwasrichtlijnen. Deze richtlijnen dienden namelijk omgezet te worden in nationale wetgevingen en daarin fungeerde de richtlijn als een soort van na te streven doel, zonder aan te geven hoe het bereikt wordt. Het gevolg is dat er geen geharmoniseerd beleid is rondom bijvoorbeeld de strafrechtelijke aanpak van witwassen, echter juridisch gezien er heel veel smaken ontwikkeld zijn. Zo is bijvoorbeeld witwassen in Nederland een op zichzelf staand crimineel feit, maar in Slowakije kan een veroordeling tot witwassen enkel in geval het gekoppeld is aan een ander (primair) zwaar misdrijf. In Frankrijk moet het gekoppelde (primaire) misdrijf zelfs eerst zijn bewezen voordat berechting voor witwassen mogelijk wordt.

Logischerwijs levert dit problemen op binnen de opsporing, berechting en informatiedeling. Simpel gezegd; kan bijvoorbeeld geen informatie uitgewisseld worden indien in het verstrekkende land (nog) geen veroordeling heeft voor het primaire misdrijf. Om deze ambiguïteit in wetgevingen te voorkomen en dus internationale samenwerking in de bestrijding van witwassen via cryptocurrency te bevorderen, heeft de EU van MiCAR een direct nationaal doorwerkende verordening ontwikkeld. De meest vergaande vorm van harmonisatie, waardoor gebrek aan regulering in één klap van tafel wordt geveegd.

Aan deze vorm van harmonisatie kleeft wel een kritische noot, waar we als Euroburger wel bewust van moeten zijn. Witwasbestrijding bevindt zich namelijk voor een groot deel in het nationaal justitie- en veiligheidsbelang, waar lidstaten altijd zelf de regie over wilde houden. Nu zijn er op EU-niveau ontwikkelingen gaande waarbij via financieel gerichte verordeningen het criminaliteitsfenomeen witwassen wordt aangepakt. Zoals hierboven is weergegeven zijn verordeningen direct in werking, zonder inmenging van nationale parlementen. Via een omweg, de financiële inslag, wordt dus het nationale justitie- en veiligheidsbeleid beïnvloed door de EU. Dit zonder dat nationale parlementaire inmenging mogelijk is. Momenteel zien we het gebeuren bij de verordeningen omtrent MiCAR en “geldovermakingen van geld en van bepaalde cryptoactiva“. Daarnaast valt op te merken dat Anti-money-laundering authority (AMLA) deels een Europese toezichthouder zal worden en gezamenlijke analyses zal faciliteren tussen FIU’s.

Kritische conclusie

Dit zijn ontwikkelingen waar goed over nagedacht moet worden of dit wel de juiste richting is. Is harmonisatie van wetgeving en internationale samenwerking van een belangrijker dan de autonomiteit van lidstaten? Door het internationale karakter van witwassen en zeker cryptocurrency handel ligt het voor de hand om de aanpak in internationale samenwerking te zoeken. Om dit te optimaliseren is de harmonisatie wat ons betreft de juiste route om te volgen. Echter komt door harmonisatie via verordeningen de EU wel heel erg centraal te staan in nationale veiligheidsbelangen. Tezamen met de verdere doorontwikkeling van AMLA, Europol, Europees bureau voor fraudebestrijding (OLAF) en een Europees OM ligt het in de lijn der verwachtingen dat dit gaat resulteren in een Europees justitieel systeem van opsporing, intelligence en vervolging van witwassen. De eerste stappen zijn al zichtbaar geworden door de internationaal coördinerende en faciliterende rol die deze organen op zich nemen.

Vooralsnog concentreert deze afbraak van autonomie zich op cryptocurrency, maar vormt wel de eerste stappen in het verlies van nationale autonomie in het justitie- en veiligheidsbelang. Het zet namelijk de deur wagenwijd open voor harmonisatie van veel meer nationale wetgevingen, bijvoorbeeld op het vlak van witwassen zelf. Feitelijk wordt het de EU die bepaald en lidstaten behouden zeer beperkte mogelijkheden om haar autonomie te bewaren. De strijd tegen internationale criminaliteit lijkt dit te legitimeren, immers grote slagen zullen zeker gemaakt worden. Maar MiCAR geldt enkel in de EU, terwijl het hoofdkantoor van de 4 grootste crypto exchanges (Binance, Coinbase, Kraken en Bybit) buiten Europa liggen en enkel Binance en Coinbase een kantoor hebben in de EU (Malta en Dublin). MiCAR zal slechts deze twee kantoren reguleren. Feitelijk probeert de EU een financiële sector te reguleren, terwijl de sector zich maar voor een klein deel binnen de EU situeert en daarnaast de exchanges ook nog een overal ter wereld bereikbaar zijn via het internet.

Worden al deze factoren gecombineerd, dan komt de vrees naar boven dat MiCAR de slag zal misslaan en wellicht eerder beginstappen zijn in de ontwikkeling van een Europees justitieel systeem. Is dit het waard om de autonomiteit over het justitie- en veiligheidsbelang van lidstaten af te brokkelen? Het antwoord zal in een discussie liggen die zeker gevoerd mag en zal worden. Vooral omdat we aan de vooravond staan van deze ontwikkelingen…

Over de auteurs

Drs. Johan C. Klercq
Senior Adviseur Openbare Orde en Veiligheid
en Adviseur Anti Money Laundering.

Johan is criminoloog en werkzaam bij Capgemini BTS en tot voor kort ingezet als Strategisch Internationaal Beleidsadviseur bij de FIU Nederland. Hij is gespecialiseerd in beleidsadvies inzake ondermijning, witwassen en georganiseerde criminaliteit binnen het openbare orde en veiligheidsdomein.

www.linkedin.com/in/johan-c-klercq

johan.klercq@capgemini.com

Mara van Gulik
Senior Consultant Invent, FEC-specialist en Criminoloog.

Mara van Gulik is werkzaam bij Capgemini Invent en ingezet als leidinggevende bij de Rabobank KYC Signals. Ze is gespecialiseerd in de ondermijning van witwassen en terrorismefinanciering binnen het bankwezen. Mara richt zich op het analyseren en adviseren van FEC-vraagstukken bij financiële instellingen.

https://www.linkedin.com/in/mara-van-gulik/

mara.van.gulik@capgemini.com

09

EEN SECURITY OPERATING MODEL ALS STUURINSTRUMENT VOOR SECURITY VOORZIENINGEN

Hoe kunnen overheidsorganisaties bepalen welke security capabilities ze nodig hebben?

Highlights

- Een beveiligingsbaseline alleen is niet voldoende om adequate beveiliging in te richten die aansluiten bij de bedrijfsdoelstellingen.
- Meer waarde halen uit data vraagt om gegevensbeveiliging.
- Hanteer de TOP 5 dreigingen aanpak als er geen dreigingsbeeld aanwezig is.
- Een beschreven security governance model helpt bij het goed beleggen van taken.
- Duidelijke taken bij security capabilities zijn nodig om security goed te beheren.

Organisaties, zowel in de publieke als private sector, worstelen[1] met het inrichten van de securityproducten en -diensten om de overheidsdoelstellingen te ondersteunen. In de publieke sector wordt de Baseline Informatiebeveiliging Overheid (BIO) gehanteerd als normenkader om security in te richten. Het BIO normenkader is gebaseerd op “best-practices” in de markt, aangevuld met specifieke beveiligingseisen waarmee de controls specifiek gemaakt worden. Een baseline alleen is niet voldoende om tot een goede beveiliging van informatiesystemen en operationele systemen te komen die ook de overheidsdoelstellingen ondersteunen.

Standaard beveiligingsaanpak

Beveiliging aanpakken via de BIO is een compliancy gedreven aanpak. Het is ook van belang om te kijken naar de belangrijkste dreigingen die van toepassing zijn op de publieke organisaties, en hoe beveiliging als enabler voor de overheidsdoelstellingen ingezet kan worden. Als we kijken naar de security incidenten van de laatste jaren, dan zien we dat veel overheidsorganisaties nog niet goed voorbereid zijn om hier weerstand tegen te bieden. Voorbeelden hiervan zijn datalekken[2] bij uitvoeringsinstanties en ransomware aanvallen[3] bij gemeenten. De securityproducten en -diensten om publieke organisaties weerbaar te maken en te ondersteunen om de doelstellingen te behalen moeten gedefinieerd, geïmplementeerd en beheerd worden.

Normenkaders alleen geven niet altijd voldoende richting om te bepalen hoe dit ingericht moet worden. Normenkaders zeggen iets over het "wat" maar niet over het 'hoe'. Omdat security zowel ontworpen, geïmplementeerd en beheerd moet worden doet men er verstandig aan om een operating model voor security in te richten. Dit Security Operating Model (SOM) bevat enerzijds de security capabilities die aanwezig moeten zijn, en anderzijds een model om deze security capabilities te beheren (security governance).

In dit artikel verstaan we onder een security capability een product en of dienst die ingericht is, waarbij processen ingericht zijn en de verantwoordelijkheden belegd zijn.

Benodigde security capabilities

Maar wat bepaalt de benodigde security capabilities? Security capabilities worden bepaald op basis van vier belangrijke aspecten, te weten;

1. de bedrijfsdoelstellingen,
2. wet- en regelgeving,
3. cybersecurity dreigingen,
4. risico’s en opgetreden incidenten en classificatie van informatiesystemen (vertrouwelijkheid, integriteit en beschikbaarheid).

1 https://www.parool.nl/nederland/onderzoeksraad-rijk-houdt-informatie-over-cyberveiligheid-achter-met-grote-risico-s~b673ec1f/?referrer=https%3A%2F%2Fwww.google.com%2F

2 https://www.digitaleoverheid.nl/nieuws/flinke-stijging-aantal-meldingen-datalekken/

3 https://www.binnenlandsbestuur.nl/digitaal/steeds-meer-gemeenten-overvallen-door-ransomware

Bedrijfsdoelstellingen:

Security moet ondersteuning bieden aan de ontwikkelingen binnen de overheid. De belangrijkste ontwikkelingen zijn:

- digitalisering van processen
- cloud adoptie
- agile werken
- informatiegestuurd optreden
- AI en algoritmes

Wet- en regelgeving:

Een groot deel van de bekendste wet- en regelgeving is opgenomen en doorvertaald naar de "best-practices" van de BIO (Baseline Informatiebeveiliging Overheid). Er zullen altijd, afhankelijk van de overheidsinstelling, aanvullende eisen van toepassing zijn. Denk hierbij aan verwerking van Politiegegevens (Wpg), of uitvoeringsdiensten die onderdeel zijn van de Nederlandse Kritieke Infrastructuur (wbni, Rbni, NIS, NIS2),

Cybersecurity dreigingen, risico's en opgetreden incidenten:

Deze categorie is voor een groot deel voor de overheid generiek in de zin dat ze allemaal dezelfde soort dreigingen en risico's zien. Denk hierbij aan Malware en Ransomware (er zijn diverse voorbeelden van incidenten zoals geslaagde ransomware aanvallen bij de overheid in de afgelopen jaren.), datalekken, defacen van websites en hacken van websites, verstoring van diensten, insider dreigingen en doelgerichte aanvallen van statelijke actoren.

Security Operating Model

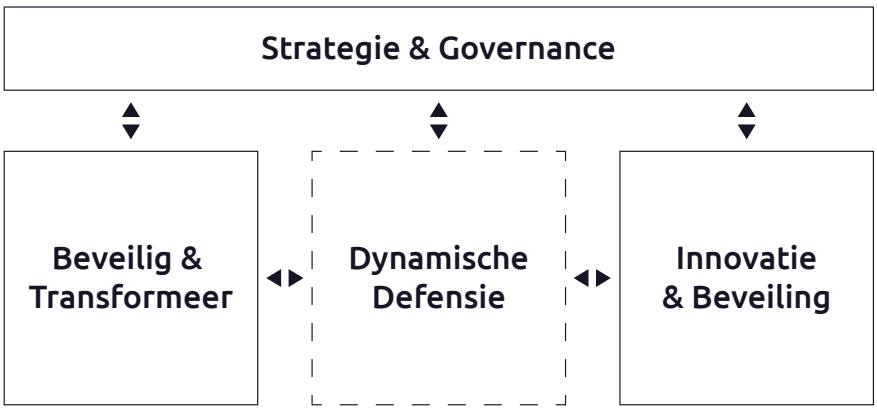
De samenhang tussen security capabilities worden opgenomen in een Security Operating Model (SOM). Dit SOM kent een twee sporen benadering: 1) beveiligen van de bestaande (legacy) systemen en 2) (innovatieve) beveiliging bieden aan nieuwe informatiesystemen. Het SOM kent een viertal domeinen, zoals weergegeven is in Figuur 1.

- Strategie en Governance;
- Beveiliging en Transformeer;
- Dynamische Defensie;
- Innovatie en Beveilig.

Strategie en Governance

Dit domein bevat de kaderstellende security capabilities zoals:

- Risicomanagement en compliancymanagement, voor het beheersen van de risico (risico identificatie, risicoanalyse, risicobehandeling, risico monitoring en rapportages) en het aantoonbaar voldoen aan compliacy eisen.
- Enterprise security architectuur voor het in samenhang ontwerpen en inrichten van alle security capabilities.
- Security awareness, voor het beveiligingsbewustzijn van alle medewerkers in de organisatie die weten wat ze moeten doen als ze slachtoffer dreigen te worden van een cyber aanval.



Figuur 1: Standaard Security Operating Model (SOM).

- Beleid, standaarden en richtlijnen waarin de beleidsuitgangspunten voor security zijn opgenomen en door vertaald zijn naar beleid op specifieke security gebieden (zoals Incident-, vulnerabilitymanagement en IAM). Hierbij ondersteund door sstandaarden en richtlijnen voor implementatie.

Beveiliging en Transformeer

Dit zijn security capabilities die nodig zijn om de bestaande informatiesystemen en of operationele assets te beveiligen, hierbij kan gedacht worden aan IAM, vulnerability management, cryptografie, netwerkbeveiliging etc.).

Dynamische defensie

Dit zijn security capabilities die gebruikt worden voor het tijdig detecteren van (pogingen tot) aanvallen, dit te monitoren en bij incidenten adequate incident response, crisismanagement en indien nodig business continuity management op te schalen. Deze capabilities ondersteunen zowel de Beveilig & Transform als de Innovatie & Beveiliging SOM capabilities.

I**nnovatie en beveilig**

Dit zijn security capabilities die bedoeld zijn om nieuwe diensten sneller te ondersteunen. Hierbij kan gedacht worden aan gebruik van cryptografie om gegevens overal te versleutelen, aan federatieve IAM om ketensamenwerking te bevorderen, cloud security om nieuwe diensten veiling in een cloud omgeving te laten landen. Naast security capabilities zal ook DevSecOps een belangrijke capability zijn om security in agile te waarborgen.

Vanuit de bedrijfsdoelstellingen (meer waarde uit data, sneller innoveren, adopteren nieuwe technologie, processen continue verbeteren) zijn de volgende security capabilities nodig:

- Enterprise security architectuur ter ondersteuning van de adaptie van nieuwe technologieën.
- Cryptografie voor de beveiliging van data in opslag en transport voor het ondersteunen dat gegevens zich nu buiten de standaard gecontroleerde omgevingen van de overheid bevinden (een van de vier pilaren van een zero-Trust aanpak).
- Een risico gebaseerde aanpak om de integratie van IT, OT en IoT te ondersteunen.
- Cloud security om de adoptie van cloud toepassingen te faciliteren.
- Third party cybersecurityriskmanagement om de risico's te beheersen van uitbestede diensten van de overheid.

Vanuit wetgeving zoals AVG, Wbni, Rbni zijn al snel de navolgende security capabilities nodig:

- Identity and Access Management, om toegang te verlenen aan geautoriseerde personen.
- Incident management, om security en privacy incidenten adequate te melden en op te lossen richting interne organisatie en toezichthouders.
- Business continuity management, om ook in crisissituaties te kunnen leveren.
- Segmentatie of Networks, om te voorkomen dat aanvallen zoals ransomware zich snel kunnen verspreiden in het gehele overheidsnetwerk, maar ook om zero trust te kunnen ondersteunen.
- Classificatie van Assets (OES assets), zodat de kritieke infrastructuur die de overheid beheerd beveiligd zijn.
- Risk Management, voor het beheersen van de risico in de breedste zin des woord voor security en privacy (DPIA;s).
- Logging and Monitoring, om inzicht te hebben in pogingen tot aanvallen tijdig te kunnen detecteren en daarop mitigerende maatregelen te treffen.
- Cryptografie en sleutel/ geheimenbeheer, voor het versleutelen van gevoelige informatie.
- Classificatie van persoonsgegevens, voor het kunnen treffen van voldoende technische en organisatorische maatregelen volgens, in overeenstemming met de AVG.

Vanuit dreigen gezien is het noodzakelijk om een goed Dreigingsbeeld op te stellen en op basis van dat dreigingsbeeld de maatregelen te treffen. Het opstellen van een dreigingsbeeld is geen sinecure. Mocht dit niet aanwezig zijn, dan is de beste aanvliegroute om te kijken naar de TOP5 dreigingen die altijd voorkomt en daar de security capabilities op af te stemmen.

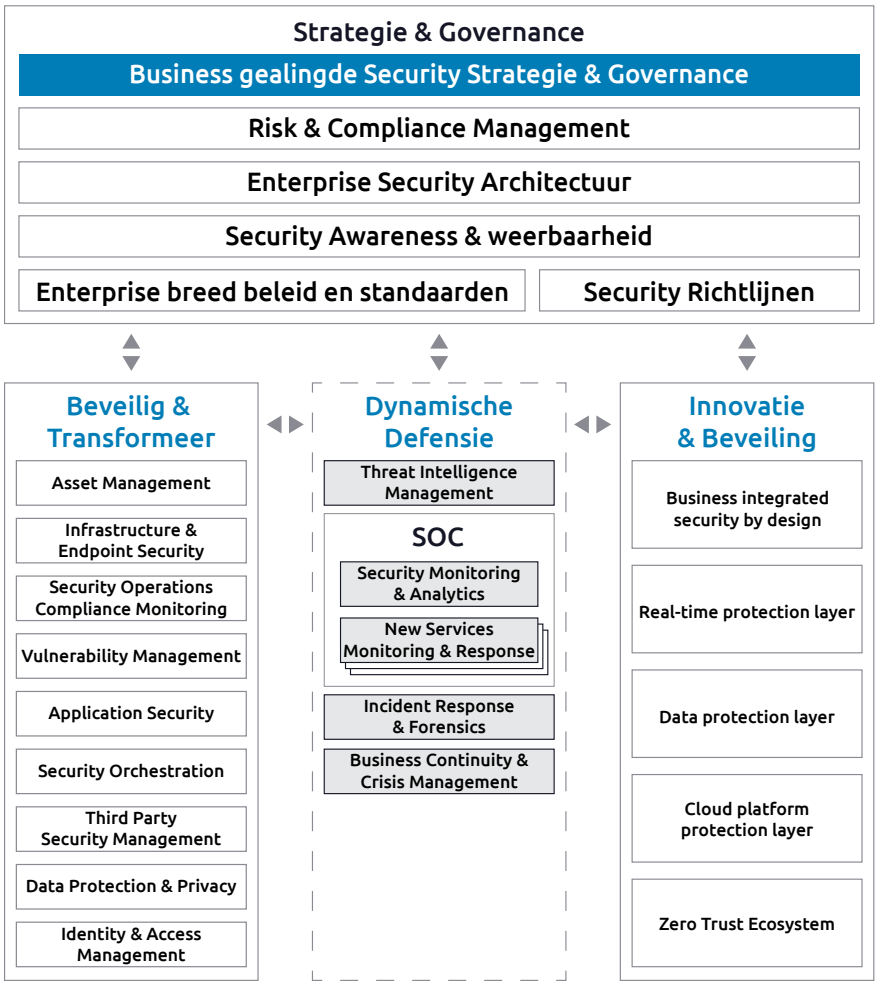
De TOP 5 dreigingen zoals opgenomen in CIS CMD 2.0[4], ENISA Threatlandscape 2022[5] kunnen als basis dienen. Als we kijken naar de TOP 5 vanuit CIS CMD gezien dan zijn dit: Malware, Ransomware, Web application hacking, Insider and Privilege misbruik en Targeted intrusions. Het ENISA rapport laat ons de volgende TOP dreigingen zien: Ransomware, Malware, Social Engineering, Dreigingen tegen data, dreigingen ten aanzien van beschikbaarheid (DDoS en Internet Dreigingen), Mis- of Desinformatie, en Supply Chain Attacks.

Deze dreigingen leiden in het algemeen tot de volgende security capabilities:

- Asset management van hard- en software.
- Identity en Access Management (IAM).
- Secure data (IAM en Cryptografie).
- Vulnerability (kwetsbaarheden) & Patch Management.
- Audit, Logging en Monitoring & respons.
- Veilige configuraties/ Hardening van systemen.
- Malware verdediging.
- Gegevens- en system herstel.
- Applicatie security (veilige ontwikkeling en beheer).
- Penetratie testen.
- Security bewustwording.
- Changemanagement.
- Incidentmanagement.
- Supply Chain Security Risk Management.

Als we deze groepen van security capabilities vanuit bedrijfsdoelstellingen, wet- en regelgeving en TOP 5 dreigingen samenvoegen en in een Security Operating Model plotten dan kan de SOM er as volgt zoals weergegeven is in Figuur 2.

De TOP 5 dreigingen aanpak als er geen gedefinieerd dreigingsbeeld aanwezig is.



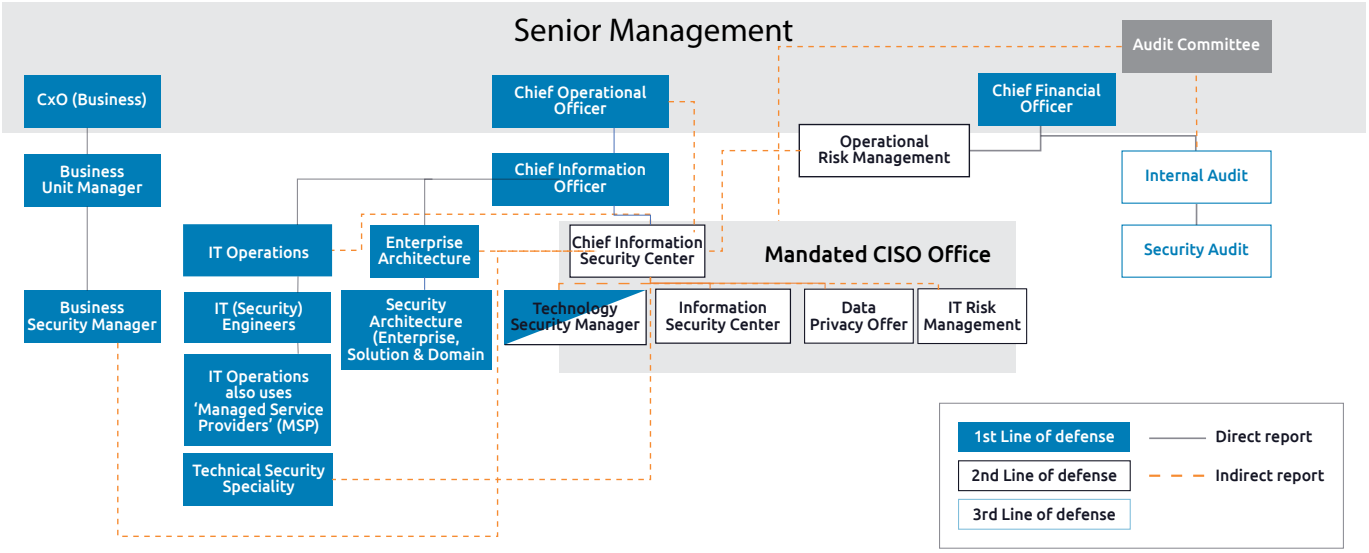
Figuur 2: SOM op maat.

4 https://www.cisecurity.org/insights/blog/cis-introduces-v2-0-of-the-cis-community-defense-model

5 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Security Governance organogram within 3 LoD

1 gecentraliseerde CISO Office



Figuur 3: Governance Model

Een overzicht van security capabilities geef richting aan hetgeen nodig is. Een groot deel van deze security capabilities moeten organisatiebreed opgepakt en geïmplementeerd worden, zodat veranderingen in organisaties via projecten

Een beschreven governance model helpt bij het goed beleggen van taken.

alleen gebruik hoeven te maken van deze capabilities en niet zelf het wiel moeten uitvinden.

Security Governance

Per onderdeel van het SOM is het van belang om helder te hebben welke taken uitgevoerd moeten worden nadat de capability ingericht is. Hiertoe zal er een governance model opgesteld moeten worden en deze geplot moeten worden op allen SOM-onderdelen. Een voorbeeld van een governance model is weergeven in Figuur 3.

Security-verantwoordlijkheden

Op basis van dit governance model is vervolgens gekeken naar het beleggen van de verantwoordelijkheden bij de uitvoering van de activiteiten, een voorbeeld van een deeluitwerking van de Som is weergegeven in Figuur 4.

Security Capability	1ste lijn (Business)	1ste lijn (IT)	1ste lijn (MSP)	2de lijn (CISO Office)	3de lijn (Interne Audit)
Business Aligned Security Strategy	1. Input leveren voor beveiligingsstrategie 2. Erken dat de beveiligingsstrategie is afgestemd op de bedrijfsdoelstellingen 3. Ondersteuning van de implementatie van het 3-lijns verdedigingsmodel en het Security Operating Model	1. Input leveren voor beveiligingsstrategie. 2. Erken de beveiligingsstrategie Voer IT-specifieke onderwerpen uit 3. Ondersteuning van de implementatie van het 3-lijns verdedigingsmodel en het Security Operating Model	1. Sluit aan bij de bedrijfsstrategie en – mogelijkheden. 2. Implementeren en naleven van beleid	1. Demonstreer inzicht in de bedrijfsstrategie en – mogelijkheden. 2. Bepaal een beveiligingsstrategie die de zakelijke mogelijkheden ondersteunt 3. Ontwerp governance op basis van 3 verdedigingslinies. 4. Stimuleer de implementatie van het Three Lines of Defence-model 5. Uitvoeren en opvolgen van beveiligingsstrategie. 6. Creëer en onderhoud beleid dat toepasbaar en leesbaar is voor alle belanghebbenden	1. Ondersteuning van de implementatie van het 3-lijns verdedigingsmodel 2. Audit beveiligings strategieprocessen met correcte ontwikkeling en goedkeuringen
Risk & Compliance Management	1. Prioriteer en waardeer kritieke activa op basis van bedrijfsdoelstellingen (Business Impact Analysis) 2. Definiëren risicobereidheid door Security Steering Committee (korte termijn) / Security board (lange termijn)	1. Prioriteer en waardeer kritieke activa op basis van bedrijfsdoelstellingen (Business Impact Analysis) 2. Voer het risico- en complianceproces uit binnen de dagelijkse IT-activiteiten	1. Input leveren voor het risico- en complianceproces 2. Voortdurende overdracht van compliancerapportage 3. Houden aan de auditvereisten	1. Define risk & compliance proces (Business Impact Analysis, Risk Assessment, Waiver Process) 2. Opzetten & onderhouden van een kader voor beveiligingsrisicobeheer en beveiligingsrisicoprocessen	1. De auditprocessen naleven
	1. Risico- en complianceprocessen (ISMS) uitvoeren binnen de dagelijkse bedrijfsvoering en voor technologieoplossingen die eigendom zijn van het bedrijf.	1. Risico- en complianceprocessen (ISMS) uitvoeren binnen de dagelijkse IT-activiteiten en voor technologieoplossingen die eigendom zijn van IT.	1. Risico- en complianceprocessen uitvoeren binnen de dagelijkse IT-activiteiten op basis van ISMS	1. ISMS-raamwerk maken voor ISMS 2. Uitvoeren van controles op ISMS & risicobeoordelingen zoals uitgevoerd door 1e lijn	1. Jaarlijkse audits uitvoeren op de effectiviteit van het ISMS
Innovatie en veilige afstemming (bedrijfsgeïntegreerde Security per Design-laag)	1. Risicoanalyses uitvoeren op nieuwe technologie & diensten en risico's beperken	1. Risicoanalyses uitvoeren op nieuwe technologie & diensten en risico's beperken	1. Risicoanalyses uitvoeren op nieuwe technologie & diensten en risico's beperken	1. Provide guidelines for risk analysis on new technologies & services	1. Voer audits uit op risicoprocessen voor nieuwe technologieën & diensten
Identity & Access Management	1. Collaborate with IT to implement IAM within organisation 2. Support IT in defining & implementing IAM domain architecture	1. Meewerken aan het definiëren van IAM-beleid en -standaarden 2. Domeinarchitectuur voor IAM definiëren en implementeren in samenwerking met bedrijven en serviceproviders 3. IAM-richtlijnen definiëren 4. IAM implementeren binnen organisatie 5. Afstemmen met de business over specifieke vereisten	1. Assisteren bij de implementatie van IAM-tooling 2. IT ondersteunen bij het definiëren en implementeren van IAM-domeinarchitectuur 3. IAM implementeren binnen processen 4. IAM-tooling gebruiken waar van toepassing	1. IAM-beleid en -standaarden ontwikkelen 2. Business & IT ondersteunen bij het definiëren van IAM-richtlijnen 3. Samenwerken met business en IT om ervoor te zorgen dat de IAM-oplossing in lijn is met het controleraamwerk en het IAM-beleid.	1. Verzekeren dat IAM-beleid, -standaarden en -architecturen worden nageleefd.
Afstemming innoveren en beveiligen (Cloud Platform beschermingslaag)		1. Sterke gebruikers authenticatietechnologie implementeren, gebruikmakend van MFA & AI 2. Krachtige controles implementeren op apparaattoegang en -beveiliging voor virtuele machines en besturingssystemen 3. Beleid voor geprivilegieerde toegang definiëren en bewaken	1. Ondersteuning door middel van advies over proces- en technologie-implementatie	1. Periodiek de beveiliging beoordelen	
Beheer van kwetsbaarheden	1. Samenwerken met IT om IAM te implementeren binnen de organisatie 2. IT ondersteunen bij het definiëren en implementeren van de IAM-domeinarchitectuur	1. Interne revisie- en kwaliteitsborgingsprocedure voor patch-implementatie opstellen 2. Prioriteren van te testen systemen en applicaties op basis van criteria 3. Volg leveranciers en externe ondersteuningsorganisaties om kwetsbaarheden in het algemeen en specifieke bedrijfs- en IT-gebieden te bewaken	1. Beleid naleven 2. Kwetsbaarheden afschermen, verhelpen en bewaken, patches testen en richtlijnen implementeren	1. Beleid definiëren voor het beheer van kwetsbaarheden voor kritieke bedrijfsmiddelen 2. Rollen en verantwoordelijkheden voor herstel definiëren	1. Provide assurance that complies to own vulnerability policy, standards vulnerability management process.

Figuur 4: Verantwoordlijkheden SOM capabilities

Conclusie

Een Security Operating Model wordt al gebruikt in de private sector om te bepalen welke security capabilities een organisatie nodig heeft en hoe deze beheerd moeten worden. Dit model is ook toepasbaar op de overheid. Hierbij moet men wel willen werken met dreiging als uitgangspunt en niet alleen compliancy gebaseerd waarbij een standaard als checklist gebruikt wordt.

SOM gaat verder dan compliancy en zorgt ervoor dat de overheid weerbaarder is tegen cybersecurity dreigingen met als gevolg dat haar processen betrouwbaarder worden uitgevoerd.

Over de auteurs

Jule Hintzbergen

Jule is Principal Consultant Cybersecurity en is gespecialiseerd in cybersecuritystrategie en - governance en -implementatie, Hij is tevens trainer voor Capgemini Academy. Jule houdt zich daarnaast bezig met identiteit en grensmanagement.

https://www.linkedin.com/in/jule-hintzbergen-17b486

jule.hintzbergen@capgemini.com

@jhintzbe

Renato Kuiper
Principal Consultant Cybersecurity

Renato was ten tijde van het schrijven van dit artikel werkzaam bij Capgemini als Principal Consultant Cybersecurity. Hij is gespecialiseerd in Enterprise Security Architectuur, Security Strategie, Cloud Security.

https://www.linkedin.com/in/renato-kuiper-3246733/

10

QUANTUMDREIGING: EEN NIEUWE CYBERDREIGING VOOR ORGANISATIES IN DE PUBLIEKE SECTOR

Welke maatregelen moeten organisaties in de publieke sector nemen tegen quantumdreigingen?

De opkomst van quantumcomputers belooft de samenleving veel voordelen, maar creëert tegelijkertijd een ernstig cybersecurity-risico voor moderne digitale systemen. Het beveiligen van kritieke infrastructuur en systemen tegen deze nieuwe dreiging is binnen organisaties in de publieke sector dan ook van cruciaal belang. Een goed begrip van de dreiging, en van tevoren weten hoe erop te reageren, kan organisaties helpen om de ergste gevolgen te voorkomen.

Highlights

- Door de opkomst van quantumcomputers is er een nieuwe cyberdreiging op komst.
- De veiligheid van kritieke infrastructuur en systemen binnen de publieke sector is van cruciaal belang. Een mogelijke aanval op de systemen kan in potentie verregaande gevolgen hebben voor de economische activiteiten en veiligheid van een land.
- Overheden en andere instanties hebben de dreiging erkend en zijn begonnen met reageren en zich voorbereiden.
- Migratie naar post-quantum cryptografie is de aanbevolen oplossing tegen deze dreiging.
- Het migratieproces is complex en enorm. Organisaties in de publieke sector dienen nu te starten met hun traject, met goed gedefinieerde doelstellingen waarmee op efficiënte en kosteneffectieve wijze wordt gewerkt.

Recentelijk is er een toenemend aantal cyberaanvallen op kritieke infrastructuur geweest, gepleegd door statelijke actoren. Maar met de opkomst van de quantumcomputer ontstaat er ook een nieuwe dreiging. Statelijke en cyberdreigingsactoren met kwade bedoelingen kunnen met behulp van quantumcomputers de beveiliging van overheids- en bedrijfssystemen doorbreken.

Dit artikel gaat in op de aard van de dreiging die quantumcomputers met zich mee kunnen brengen en hoe overheden en andere instanties in landen de dreiging hebben erkend en zijn begonnen met het reageren erop. Ook gaan we dieper in op de risico's die de quantumdreiging kan veroorzaken, en hoe organisaties in de publieke sector de dreiging kunnen aanpakken met de inzet van post-quantum cryptografie. Tot slot geeft dit artikel een aantal aanbevelingen en mogelijke maatregelen die organisaties in de publieke sector kunnen overwegen voor de transitie naar een quantumveilige wereld.

Toenemende statelijke cyberdreigingen

De volatiele geopolitiek speelt een aanzienlijke rol in cybersecurity. Met een toenemend aantal aanvallen, groeiende dreigingsvectoren en escalerend algehele impact geeft dit gestalte aan het dreigingslandschap, waarbij zich voor cyberdreigingen een geheel nieuw paradigma aandient. Volgens recent onderzoek uitgevoerd door Dr. Mike McGuire, 'Nation States, Cyberconflict and the Web of Profit'[1], is er tussen 2017 en 2020 100% toename geweest van significante incidenten waarbij natiestaten betrokken waren. Statelijke cyberaanvallen kunnen aanvallen zijn op kritieke civiele en niet-civiele infrastructuur van overheids- en particuliere organisaties. Bovendien, zegt het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA)"Destructieve aanvallen vormen een prominente component van de operaties van statelijke actoren[2]". Deze statelijke aanvallen worden steeds geraffineerder en kunnen zeer veel schade aanrichten. De motivatie hiervan is spionage met de intentie om toegang te verkrijgen tot gevoelige/ geheime gegevens en ander intellectueel eigendom. Ze kunnen ernstige verstoringen veroorzaken door mogelijke destructieve aanvallen. Volgens een rapport van Microsoft[3] is gedurende 2021 en 2022 een toenemend aandeel (20 tot 40%) cyberaanvallen gericht geweest op kritieke infrastructuur.

Quantumdreiging: een nieuwe dreiging op komst

Als gevolg van de opkomst van quantumcomputers wacht ons een nieuwe dreiging. Deze computers werken op basis van de principes van quantumfysica. In potentie zorgen ze voor een exponentiële versnelling bij het oplossen van bepaalde soorten computerberekeningen in vergelijking met klassieke computers. Deze ongekende rekenkracht zal het mogelijk maken om problemen op te lossen die tot nu toe onhaalbaar leken. Hiermee zal het industrieën en economieën in de toekomst transformeren. Echter, vormen deze quantumcomputers mogelijk ook een significante dreiging voor de veiligheid van veel van de huidige cryptografische systemen die gebruikt worden.

De huidige asymmetrische cryptografische algoritmes bieden de gewenste beveiliging op basis van de complexiteit van wiskundige problemen, zoals de ontbinding van getallen in priemfactoren. Dit is met klassieke computers vrijwel onmogelijk binnen een redelijk tijdsbestek op te lossen. Toch, kan een voldoende grote en geschikte quantumcomputer, die gebruik maakt van het algoritme van Shor[4], de factoratie-opdracht mogelijk binnen enkele uren uitvoeren, zo niet minuten.

1 https://threatresearch.ext.hp.com/web-of-profit-nation-state-report/

2 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

3 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

4 https://en.wikipedia.org/wiki/Shor%27s_algorithm

Statelijke en andere cyberdreigingsactoren met kwade bedoelingen die quantum computers gebruiken, kunnen mogelijk de beveiliging kraken van overheids- en bedrijfssystemen. Daarmee zouden ze openbare voorzieningen en nutsinfrastructuur kunnen ontwrichten en zelfs beschadigen, financiële transacties verstoren en persoonsgegevensbescherming kunnen aantasten. Gezien de kritieke aard van systemen in de publieke sector, is de veiligheid hiervan van cruciaal belang. Elke potentiële aanval op de systemen zou ernstige gevolgen kunnen hebben voor de economische activiteit en veiligheid van een land.

Terwijl organisaties in de publieke sector groots investeren in digitale transformatietrajecten binnen hun IT- en OT-landschappen, blijken grootschalige beveiligingsgerelateerde kwetsbaarheden veel voor te komen. Een aanvaller met een cryptografisch-relevante quantumcomputer vormt een potentieel risico voor:

- Digitale systemen en platformen die bedrijfsgevoelige data verwerken, zoals de persoonsgegevens van burgers, klanten en ambtenaren/medewerkers. Het zou grote schade kunnen toebrengen aan de bedrijfsvoering en digitaal opgeslagen gegevens kunnen manipuleren, inclusief juridische documenten door gecompromitteerde certificaten en handtekeningen. Dit veroorzaakt een verlaagd vertrouwensniveau en betrouwbaarheid van systemen bij organisaties in de publieke sector.
- Kritieke infrastructuursystemen, resulterend in gecompromitteerde controle over nutsinfrastructuur die betrekking heeft op bijvoorbeeld het elektriciteitsnet, gaspijpleidingen en waterinstallaties, met verstoringen van publieke voorzieningen tot gevolg, en de daaruit voortvloeiende negatieve impact op volksgezondheid, veiligheid en de economie.
- Nationale defensiesystemen: een aanvaller zou toegang kunnen krijgen tot – en controle over – destructieve wapens, staatsgeheimen en communicatiesystemen. Dit kan de nationale veiligheid in gevaar brengen.

Dit veroorzaakt een verlaagd vertrouwensniveau en betrouwbaarheid van systemen bij organisaties in de publieke sector

Een quantumcomputer die in staat is om de huidige cryptografie te kraken en bovenstaande dreigingen te vormen, bestaat op dit moment echter nog niet. Het zal misschien nog vele jaren duren voordat dit gerealiseerd wordt. Er is geen tijdslijn voor deze quantumdreiging bekend. Toch volgen de ontwikkelingen op het gebied van quantumcomputers in rap tempo, zowel voor hardware als software. Nieuwe, creatieve en verfijnde algoritmes en methoden worden onderzocht en ontwikkeld, waarmee het quantumvoordeel in een steeds hogere versnelling komt. Bovendien is er ook een ander soort aanval, namelijk de 'Store Now, Decrypt Later' aanval. Hierbij kunnen dreigingsactoren versleutelde data vandaag opslaan om deze in de toekomst te ontcijferen, wanneer ze werkelijk over krachtige quantumcomputers beschikken. Dit vormt een serieuze uitdaging voor organisaties in de publieke sector die werken met data met langere termijn geheimhoudingsplicht. Het is daarom van cruciaal belang dat alle overheidsorganisaties en organisaties in de publieke sector spoedig beginnen met hun traject naar quantumveilig.

5 https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

6 https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

7 https://www.whitehouse.gov/briefing-room/statements-releases/2022/06/28/fact-sheet-the-united-states-continues-to-strengthen-cooperation-with-g7-on-21st-century-challenges-including-those-posed-by-the-peoples-republic-of-china-prc/

8 https://www.enisa.europa.eu/news/enisa-news/post-quantum-cryptography-anticipating-threats-and-preparing-the-future

9 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

10 https://www.congress.gov/bill/117th-congress/house-bill/7535

Hoe reageren overheden en gerelateerde organisaties op de quantumdreiging?

Overheden en andere instanties in landen onderkennen de dreiging en zijn begonnen om zich erop voor te bereiden. In 2022 waren er veel ontwikkelingen met betrekking tot voorbereidingen voor quantumveilige cryptografie. Zes daarvan waren belangrijke mijlpalen die veel aandacht op de ernst van de quantumdreiging vestigden.

1. De eerste is de aankondiging[5] door de National Institute of Standards and Technology (NIST) over de selectie van de eerste groep van vier Post-Quantum Cryptografie (PQC) encryptie algoritmes voor standaardisatie. Deze algoritmes zijn ontworpen om weerbaarheid te bieden tegen dreigingen van toekomstige quantumcomputers. Dit is geen kleine prestatie, gezien het feit dat dit selectieproces het resultaat is van wereldwijde inspanningen onder leiding van NIST als post-standaardisatieproject voor kwantumcryptografie. Dit heeft meer dan zes jaar gekost (startend in 2016).

2. De tweede ontwikkeling is de publicatie in de VS van het National Security Memorandum[6], dat de belangrijkste stappen identificeert die genomen moeten worden voor concurrentievoordeel in quantum-informatiewetenschap en quantumcomputer risicovermindering door quantumbestendige cryptografie. Dit vormt een leidraad voor overheidsinstellingen die vroeg beginnen met actie ondernemen in de transitie van cryptografische systemen naar quantumbestendige cryptografie. De National Security Agency (NSA) verwacht dat de transitie van 'National Security Systems' (NSS) naar quantumveilige cryptografie zal verlopen volgens verschillende tijdlijnen op basis van use-cases. De eerstkomende is een begin van de transitie van software en firmware signing use cases, zodat deze in 2025 worden ondersteund door quantumveilige algoritmes, met een complete transitie van alle national security systemen in 2035.

3. De derde ontwikkeling is de toezegging die is gedaan door leden van de G7[7] om samenwerking op het gebied van cyber te intensiveren en bevorderen, en om quantumbestendige cryptografie in te zetten voor beveiligde interoperabiliteit tussen de systemen van de digitale economie.

4. De vierde ontwikkeling is de publicatie van het rapport over het post-quantum cryptografie integratie-onderzoek[8] door het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA). Het document verkent de uitdagingen van PQC-standaardisatie, en de noodzaak om nieuwe protocollen en modificaties te ontwerpen voor bestaande cryptografische protocollen.

5. De vijfde ontwikkeling is de publicatie van een memorandum[9] door het "Office of Management and Budget" van het Witte Huis, dat overheidsinstanties instructies geeft om te beginnen met de migratie naar post-quantum cryptografie. Daarbij worden duidelijke deadlines meegegeven.

6. En tot slot, de zesde ontwikkeling, het invoeren van het Quantum Computing Cybersecurity Preparedness Act[10] in de Verenigde Staten, dat alle federale instanties verplicht om te migreren naar post-quantum cryptografie.

Overheden en instanties wereldwijd houden verschillende tijdlijnen aan wat betreft de vorderingen, en bevinden zich in verschillende stadia van het migratieproces. De algemene richting is om organisaties in de publieke sector de quantumdreigingen te laten inzien en voorbereidingen te treffen om dit aan te pakken. Om dit proces te faciliteren en versnellen, moeten cybersecurity instanties en industrieën, de organisaties in de publieke sector praktische methoden, kaders en tools in handen geven, evenals een duidelijk stappenplan.

Wat kunnen organisaties in de publieke sector doen?

De aanbevolen oplossing om de quantumdreiging aan te pakken is de implementatie van post-quantum cryptografie. Deze upgrade van systemen, die voorziet in de overstap van de bestaande quantumkwetsbare cryptografie op post-quantum cryptografie, kan, afhankelijk van de grootte en complexiteit van organisaties, een enorme opgave zijn. Organisaties dienen dergelijke programma's te initiëren met goed gedefinieerde doelstellingen, die erop zijn gericht om de vaardigheden te ontwikkelen, zodat de transitie naar post-quantum cryptografie op efficiënte en kosten-effectieve wijze gerealiseerd kan worden.

Het transitietraject naar quantumveilige cryptografie is onder te verdelen in twee belangrijke fasen:

1. Voorbereidingsfase: Dit is de fase om een goed begrip te ontwikkelen van – en alle informatie te verzamelen over – de cryptografie die wordt gebruikt voor de verschillende applicaties binnen een organisatie, en om te begrijpen hoe verschillende post-quantum cryptografische en hybride algoritmes impact hebben op de prestaties van verschillende applicaties. De belangrijke stappen in deze fase zijn onder anderen:

- Informeer directies, management en medewerkers over quantumdreiging en post-quantum cryptografie door gerichte workshops en trainingen te geven.
- Verricht een snelle quantumrisico assessment om diepgaand inzicht te krijgen in de grootte en complexiteit van het landschap, zodat de migratie goed kan worden gepland.
- Doe onderzoek, maak een inventarisatie van cryptografie systemen en applicaties, en verzamel informatie en data, de gevoeligheid ervan en hoe lang het bewaard dient te worden.
- Voer een gedetailleerde analyse uit van de inventarisatie en de verzamelde data, definieer een roadmap en plan met prioritering van systemen voor transitie.
- Experimenteer met post-quantum cryptografische algoritmes en protocollen, inclusief hybride varianten, in verschillende applicaties met specifieke prestatie-eisen.
- Bepaal specifiek beleid en governance mechanismes, in lijn met de beveiligingsmaatregelen en behoeften van organisaties. Voor zowel het opschonen van bestaande systemen als huidige en toekomstige transformatieprogramma's.
- Creëer specifieke partner- en leveranciersecosystemen, in lijn met de roadmap en het beleid van de organisatie.
- Tref voorbereidingen om Crypto Agility te implementeren als onderdeel van dit traject. Maak plannen om het volwassenheidsniveau van Crypto Agility te verhogen gedurende het gehele proces. Dit maakt het voor organisaties mogelijk om zich aan te passen aan dynamische situaties en om opkomende cryptografie te kunnen implementeren met minimale systeemaanpassingen.

2. Migratiefase: Na de voorbereidingsfase en met een goed gedefinieerde roadmap, kan de migratiefase worden gestart. Gedurende deze fase wordt de transitie naar quantumveilige cryptografie geïmplementeerd in de systemen binnen de organisatie. Nieuwe implementaties worden getest en gevalideerd op hun verwachte veiligheid, functionaliteit en prestaties. De belangrijkste stappen in deze fase zijn onder anderen:

- Definieer en implementeer governance en programmamanagementprocessen en systemen ten behoeve van efficiënte uitvoering van de transitie.
- De selectie van productiewaardige PQC-content en gerelateerde protocollen ter ondersteuning van klassieke, post-quantum en hybride aanpakken die voldoen aan de nieuwste standaarden en specificaties.
- Update systemen naar quantumveilige algoritmes en protocollen, alsmede

de aanpassing van applicaties en versterking van kritieke openbare infrastructuur volgens de roadmap.

- Voer testen en validatie uit op de geüpgradede systemen voor beveiliging, functionaliteit en prestaties.
- Doorloop het compliance- of certificeringsproces, naargelang van toepassing.
- Tot slot wordt de fase bereikt van voortdurend onderhoud van de systemen, met continue verbetering van de crypto agility van de organisatie.
- Gedurende deze fase moet post-quantum cryptografie ook worden geïntegreerd in systemen van doorlopende en toekomstige programma's.

De vooruitgang in quantumcomputer-technologie brengt de potentiële dreiging van statelijke en andere actoren steeds dichterbij. Migratie naar quantumveilige cryptografie is cruciaal in de beveiliging tegen zulke dreigingen. Met het oog op een soepele transitie naar een quantumveilige wereld, dienen overheids- en andere organisaties in de publieke sector te starten met hun migratie door een post-quantum cryptografische roadmap te volgen. Dit hele migratieproces is zeer complex en vergt misschien jarenlange en continue inspanning. Daarom worden organisaties in de publieke sector aangeraden om nu te starten met de voorbereidingen voor een lang en gecompliceerd traject naar quantumveilig.

Over de auteurs

Gireesh Kumar Neelakantaiah
Senior Director

Gireesh leidt de 'go to market'-strategie voor Capgemini's Quantum Lab producten en Quantum Safe Cryptography oplossingen. Hij heeft ervaring met productmanagement, strategische planning, zakelijke en commerciële modellen-innovatie, en ecosysteem partner en IP-licentiemanagement en is vaardig in quantum computing, data science, AI/ML/deep learning, digital manufacturing & Industrial IoT en cloud computing.

https://www.linkedin.com/in/gireesh-kumar-n-5b5a5b1/
gireeshkumar.n@capgemini.com

Julian van Velzen
CTIO and Head of Capgemini's Quantum Lab

Julian is hoofd van het Capgemini Quantum Lab, een wereldwijd netwerk van quantumexperts, partners en faciliteiten gericht op drie kerngebieden: Sensing, Communication en Computing. Vanuit dit lab houdt Capgemini zich samen met klanten bezig met het onderzoeken van – en het bouwen van een pad naar – quantumvoordeel m.b.t. zakelijke en maatschappelijke problemen die tot nog toe onoplosbaar leken. Julian heeft een achtergrond in de fysica van de gecondenseerde materie en studeerde aan de Universiteit van Amsterdam. Hij is onderdeel van de CTIO-gemeenschap van de groep en de Nederlandse vertegenwoordiger bij het European Quantum Consortium (QuIC). Hij is ook lid van het Forbes Technology Council en mede-oprichter van Quantum Gateway Foundation.

https://www.linkedin.com/in/julian-van-velzen/
julian.van.velzen@capgemini.com

11

HYBRIDE WERKEN IS HERE TO STAY: AANDACHTSPUNTEN VOOR DE PRIVACYBEWUSTE PROFESSIONAL

Wat te doen om hybride werken en privacy hand in hand te laten gaan?

Highlights

- Werken vanaf elke locatie, eng of een mogelijkheid?
- Tips om hybride werken mogelijk te maken in het veiligheidsdomein.
- Risico's en oplossingen in kaart gebracht.
- De kracht van open communicatie: maak medewerkers een onderdeel van de oplossing.

Hybride werken is een gegeven sinds corona, maar levert het enkel voordelen op of vraagt het om een andere manier van beveiliging? Zeker in het veiligheidsdomein waar gewerkt wordt met kritieke data is het goed om kritisch te kijken naar de juiste balans.

In de trein, op de fiets, in een café, thuis, op kantoor, tegenwoordig werken we overal. Het is een opmerkelijke verandering van de manier van werken van de laatste jaren. Enerzijds levert dat ons een hoop flexibiliteit op. Anderzijds brengt dit nieuwe privacy en informatiebeveiligingskwesties met zich mee, wat aanleiding geeft om te kijken naar middelen voor nog betere bescherming van de business. Met de mens als zwakste schakel in dit proces ligt een praktische aanpak voor de hand.

Van noodzaak naar blijvende trend

In de afgelopen jaren hebben we een opmerkelijke verschuiving gezien in de manier waarop we werken. Het traditionele kantoorleven, waarbij we dagelijks op dezelfde locatie aanwezig zijn, maakte plaats voor een meer flexibele en dynamische benadering van werk: hybride werken. We werken nu niet meer alleen op kantoor, maar ook bijvoorbeeld in de trein, thuis, of andere locaties zoals het café om de hoek. Denk ook aan flexibel werken over de grenzen.

Wat begon als een noodzakelijke reactie op de wereldwijde pandemie, is uitgegroeid tot een blijvende trend die stevig verankerd is in de moderne zakelijke cultuur. Dat is ook niet zo gek. Hybride werken kan immers leiden tot een betere work-life balance, minder reistijd, een grotere focus op resultaten en een verbeterde productiviteit. Echter, dergelijke voordelen brengen ook nadelen met zich mee. Zo ontstaan er in het veiligheidsdomein grotere risico's dan in andere sectoren. Naast devices die medewerkers dragen die ongewenst data kunnen delen (denk aan het delen van locaties waar iemand zich bevindt), zijn er nu meer factoren om rekening mee te houden. Zoals uit welke geografische gebieden medewerkers werken (en welke data zij verwerken) en wat mogelijke vijandelijke factoren zijn om rekening mee te houden. De risico inschatting kan wijzigen ten opzichte van het traditionele werken op kantoor aangezien rekening gehouden dient te worden met eventuele reisbewegingen, onbetrouwbare netwerken en het potentieel verlies of het tijdelijk uit zicht verliezen van devices.

Hybride in al zijn facetten

In een wereld waar informatie een van de meest waardevolle activa is geworden, moeten organisaties zorgvuldig omgaan met de privacy van hun werknemers en klanten. Het waarborgen van privacy bewuste werkomgevingen is van cruciaal belang om het vertrouwen te behouden en te voldoen aan de wettelijke vereisten.

Bij hybride werken in het bijzonder komen er meer zaken kijken dan je in eerste instantie zult verwachten. Denk aan (het gebrek aan) security op persoonlijke netwerken. Ook de werknemer die op een openbaar wifi netwerk inlogt vormt een risico die niet makkelijk bij de werkgever in kaart te brengen is. Je moet bijvoorbeeld ook nadenken over het gebruik van USB devices, headsets en al dan niet gebruik van een privacy screen. Ook het vernietigen van documenten vraagt om aandacht bij hybride werken. Niet alles kan in de oud papier container van de medewerker zelf. Denk ook aan bewustzijn van medewerkers of isolatie van de omgeving en wanneer (en op welke wijze) sommige gegevens wel of niet te delen zijn. In de zomermaanden vergaderen in de tuin is heerlijk, maar gevoelige informatie delen over bijvoorbeeld een inval die plaats gaat vinden is daarvoor niet de geschikte locatie.

De mens als zwakte schakel

Waar het afweren van cyberaanvallen op één locatie al uitdagend is, vormt hybride werken dus tal van extra risico's. Daarbij is de menselijke factor het kernelement. Technisch kunnen systemen sterk in elkaar zitten, maar uiteindelijk is het de werknemer zelf die met deze systemen aan de slag gaat. Als een medewerker besluit om gevoelige data te vermelden in de trein, doet dat alle technische maatregelen teniet. Of denk aan de werknemer die gevoelige klantinformatie niet alleen uitgeprint, maar ook in een doorzichtige map vervoerd. De werknemer die besluit het klantrapport te laten samenvatten door ChatGPT of te laten te vertalen door Google Translate, vormen relatief nieuwe uitdagingen op dit gebied.

De informatiebeveiligingsexpert van nu heeft daarom meer dan ooit de cruciale verantwoordelijkheid om ervoor te zorgen dat de data-infrastructuur robuust en veilig blijft. Met de mens als zwakte schakel bij het hybride werken ligt actieve betrokkenheid van werknemers voor de hand. Dit vraagt niet alleen een andere aanpak vanuit de werknemer, maar ook een andere aanpak vanuit de werkgever als sturende factor in het geheel en meer bewustzijn dan tot op heden noodzakelijk was.

De kracht van open communicatie

Werknemersbetrokkenheid wordt bereikt door middel van open communicatie rond privacy risico's en beveiligingskwesties, ook wanneer het gaat om hybride werken. Het is daarin belangrijk om te benadrukken dat fouten maken menselijk is en verbeterpunten welkom zijn. Communiceer daarom openlijk over lopende kwesties binnen de organisatie

en moedig teamleden aan om vragen te stellen en zorgen te uiten. Laat medewerkers ook actief meedenken over mogelijke risico's die zij zelf signaleren met hybride werken.

Traning en awarenessessies kunnen hierbij helpen, maar denk ook eens aan open feedbacksessies en rondetafel gesprekken. Hierin kunnen werknemers hun mening geven over de bestaande privacy- en beveiligingsmaatregelen en suggesties doen voor verbetering. Op die manier blijft men ook actief op de hoogte van welke struikelblokken er binnen een organisatie zijn. Deelnemers kunnen in een feedbacksessie bepaalde situaties delen waar ze tegenaan zijn gelopen, zodat de organisatie hiervan kan leren.

Een terugbliksessie organiseren, waarin wordt gekeken naar lessons learned, kan ook helpen om een open cultuur te creëren. Dan zien werknemers immers dat bepaalde problemen en vragen ook daadwerkelijk worden aangepakt en worden geïmplementeerd in de praktijk. Het inplannen van een privacy Q&A moment in de Teams-agenda (zonder verplichte aanwezigheid) is ook een laagdrempelige manier om privacy meer mee te laten draaien in de organisatie.

Dienstverlening als focus

Wanneer werknemers zich vrijer voelen om eigen fouten te delen en bedenkingen op te werpen, zullen zij ook eerder het privacy of informatiebeveiliging hulploket weten te vinden. Denk aan de situatie dat werknemers problemen ondervinden bij het inloggen via een VPN, waardoor zij mogelijk naar onveilige alternatieve manieren gaan zoeken om toch hun werk te kunnen doen. Of het uitblijven van een reactie van de privacy afdeling, terwijl de werknemer sterk over de privacy implicaties twijfelt en besluit om iets toch te doen. Als zich dit voordoet moet dienstverlening naar de werknemer de focus zijn. Hoe kunnen zij hun werk zo goed mogelijk voortzetten, zonder dat zij het idee hebben dat privacy hieraan in de weg staat? Een praktische aanpak, waarin mogelijke fouten niet bestraft worden, verlaagd de drempel om de volgende keer nog eens voor advies langs te lopen.

Stimuleer samenwerking

Privacy en informatiebeveiliging hoeft niet (volledig) van bovenaf te worden bepaald. Het belangrijkste is immers dat de beleidsrichtlijnen en procedures aansluiten bij het werk dat moet worden verricht. Creëer daarom een speciale werkgroep met vertegenwoordigers uit verschillende teams en afdelingen, waaronder informatiebeveiligingsexperts, IT-personeel en werknemers die regelmatig met gevoelige gegevens werken. Betrek daarin ook juist diegene zonder privacy of IT-achtergrond. Zo breng je verschillende perspectieven uit een organisatie samen, wat weer voor nieuwe inzichten zorgt. Deze werkgroep kan regelmatig bijeenkomen om privacy- en beveiligingskwesties te bespreken, beleidslijnen te ontwikkelen en best practices te delen.

Houd het actueel en concreet

Hybride werken is here to stay, maar de concrete uitwerking ervan veranderd voortdurend. Het eerder aangehaald gebruik van ChatGPT is zo'n voorbeeld. Als organisatie is het belangrijk om direct te reageren met praktische tools bij deze nieuwe ontwikkelingen. Dat werknemers het gaan gebruiken is immers evident. Ook is het belangrijk om je te verdiepen in threat intelligence. Welke aanvallen komen op ons af, wat is de prognose en hoe kunnen wij als organisatie hierop voorbereiden? Betrek dit niet alleen in je processen, maar communiceer het ook naar de mensen.

Het veiligheidsdomein

Bovenstaande is uiteraard ook van toepassing op het veiligheidsdomein, misschien nog wel meer aangezien het veiligheidsdomein unieke vereisten en uitdagingen heeft ten opzichte van andere sectoren. Wanneer we de transitie naar hybride werken bekijken binnen dit domein, worden risico's en oplossingen vaak versterkt door de kritieke aard van de informatie en taken die worden uitgevoerd.

Risico's:

In het veiligheidsdomein wordt met hele gevoelige informatie gewerkt. Denk daarbij aan persoonlijke gegevens, maar ook aan strategische plannen, operationele details en inlichtingeninformatie. Ongewenste toegang tot deze data of het lekken van deze gegevens kan ernstige gevolgen hebben voor de nationale veiligheid en het welzijn van individuen. Daarnaast kunnen organisaties in dit domein eerder doelwitten zijn voor aanvallen of spionage. Hetgeen een grotere kans van slagen heeft als medewerkers diverse werkplekken gebruiken. Denk ook aan de

complexiteit met betrekking tot (keten) samenwerking in dit domein. Zeker met diverse locaties, diverse devices en diverse beveiligingsmethodes kan dat resulteren in een verhoogd risico.

Oplossingen

1. Extra beveiligde communicatie: Overweeg het gebruik van beveiligde communicatiekanalen, zoals versleutelde messaging-apps of speciale communicatienetwerken die specifiek zijn ontworpen voor veiligheidsdiensten.

2. Strikte toegangscontroles: Implementeer meervoudige authenticatiemethoden en regelmatige controles van toegangslogs om te waarborgen dat alleen geautoriseerde personen toegang hebben tot gevoelige informatie.

3. Training en bewustwording: Gezien de gevoeligheid van het domein is het essentieel dat alle medewerkers voortdurend worden getraind in de nieuwste beveiligingsprotocollen, inclusief de risico's van hybride werken.

4. Noodplannen: Ontwikkel en oefen regelmatig noodplannen voor verschillende scenario's, zoals een groot datalek of een cyberaanval, om ervoor te zorgen dat de organisatie snel en efficiënt kan reageren.

5. Samenwerkingsprotocollen: Stel duidelijke protocollen op voor inter-agency samenwerking, vooral wanneer het gaat om het delen van gevoelige informatie op afstand.

Binnen het openbare orde en veiligheidsdomein is het essentieel om de balans te vinden tussen flexibiliteit en veiligheid. Terwijl hybride werken bepaalde voordelen kan bieden, moet de nadruk vooral liggen op het waarborgen van de integriteit en veiligheid van de informatie en de operaties van de organisatie.

Conclusie

Hybride werken is er en zal er ook blijven. Ondanks de uitdagingen zijn er genoeg situaties waarin hybride werken, met de juiste veiligheidsmaatregelen, mogelijk is. Het belangrijkste is om bewust te zijn van de mogelijke risico's, bewustzijn te realiseren bij medewerkers en te classificeren welke data in aanmerking komt voor hybride werken. Op deze wijze kan ook het veiligheidsdomein genieten van de voordelen die hybride werken te bieden heeft.

Over de auteurs

Natasja Pieterman
Head of cyber service line Netherlands

Natasja is Deputy Service Line Lead van het chapter Data, Identity, Security and Trust en van Advanced Threat Protection and Recovery. Zij heeft jarenlange ervaring binnen de overheid en het veiligheidsdomein als trainer en consultant op het terrein van privacy en cybersecurity.

https://www.linkedin.com/in/natasja pieterman-88387119/
natasja.pieterman@capgemini.com

Emmaly van Ettikhoven
Privacy consultant

Emmaly is werkzaam als privacy consultant. Emmaly adviseert organisaties bij strategische en operationele vraagstukken omtrent privacywetgeving.

https://www.linkedin.com/in/emmalyvanettikhoven/
emmaly.van.ettikhoven@capgemini.com

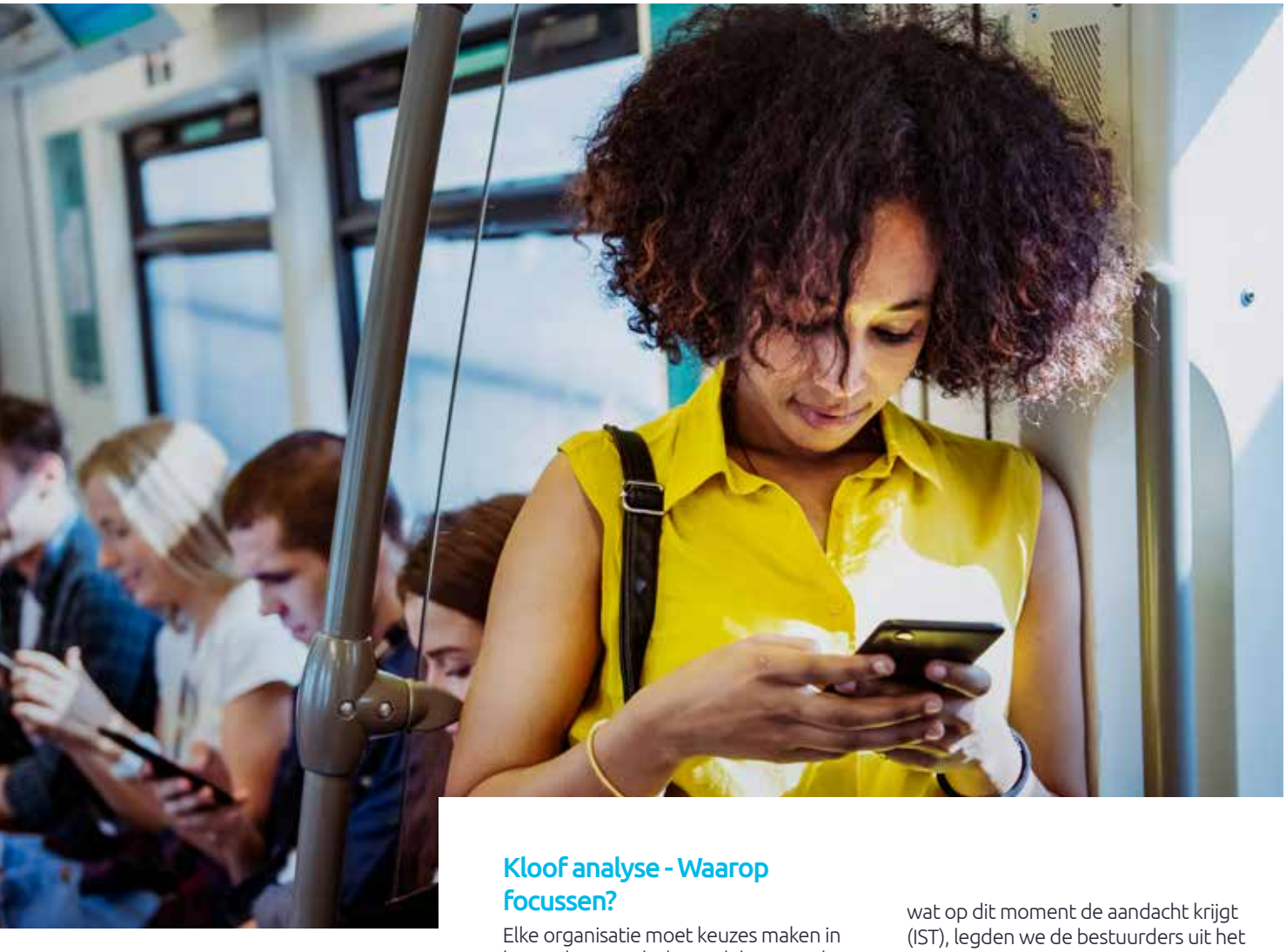
12

DIGITALE VEILIGHEID: SAMEN BOUWEN AAN EEN WEERBARE SAMENLEVING

Waar ligt de digitale focus van bestuurders uit het veiligheidsdomein?

Highlights

- De kloofanalyse geeft inzicht in het verschil tussen de huidige situatie en het behalen van de gewenste strategische doelstellingen in de toekomst. De analyse die in het kader van dit artikel is uitgevoerd laat zien dat de grootste kloof wordt ervaren bij de inzet van AI. Bestuurders zouden AI veel meer willen (kunnen) inzetten dan ze nu doen. De delta-score van de kloofanalyse (1,87) laat zien dat er een grote verschuiving van de bestuurlijke focus is gewenst op dit vlak. AI moet vooral helpen met het versnellen en het overnemen van voorbereidend werk ter ondersteuning van de besluitvorming, zodra hoogwaardig werk en de besluitvorming uiteindelijk bij mensen blijft liggen.
- Een grote verschuiving van bestuurlijke focus is eveneens gewenst als het gaat om het delen van meer data binnen de veiligheidsketen (delta-score 1,68 ten gunste van meer delen in de keten) en de mogelijkheid om gebruik te kunnen maken van de data van ketenpartners (verschil van 1,1). Hierbij ligt de uitdaging voornamelijk in het maken van de juiste afspraken met elkaar en de voorwaarden waaronder data met elkaar gedeeld kan worden.
- Bestuurders ervaren spanning rondom het inhuren van IT-experts (verschil 1,20 ten gunste van meer samen met ketenpartners inhuren), en IT-experts op een intensieve manier laten samenwerken met business-experts van de eigen organisatie (verschil 0,97 ten gunste van meer samenwerking tussen business-experts en IT-experts).
- Bestuurders lijken vooral tevreden over de huidige hoeveelheid ketensamenwerking rondom innovatie (klein verschil van 0,17), de huidige balans tussen privacy en cybersecurity binnen hun organisatie (verschil van 0,37), en de gerichtheid op daadwerkelijke databehoeftes bij het verzamelen van data binnen de keten (0,44). Dit zijn belangrijke thema's om op door te pakken, maar bestuurders ervaren dat deze thema's de juiste hoeveelheid aandacht krijgen. Hierbij geldt dus dat de huidige focus ook de gewenste focus is.



Kloof analyse - Waarop focussen?

Elke organisatie moet keuzes maken in hoe ze hun aandacht verdelen over de verschillende mogelijke IT-thema's. Zet een organisatie in op meer en geavanceerdere IT-tooling, of gaat de aandacht vooral naar het trainen en uitrusten van de mensen die de tooling en data moeten gebruiken? Is de focus vooral intern gericht, of wordt er ingezet op meer samenwerking in de keten? Om inzichtelijk te maken hoe bestuurders hun aandacht het liefst zouden verdelen (SOLL), versus wat op dit moment de aandacht krijgt (IST), legden we de bestuurders uit het publieke veiligheidsdomein een aantal tegenstellingen voor. De bestuurders moesten hun organisatie en de keten positioneren op een schaal van 1 tot 5. Welke stelling zou de meeste aandacht horen te krijgen, en welke kreeg op dit moment de meeste aandacht? Aan de hand van het verschil tussen de SOLL en de IST-positioneringen, maken we inzichtelijk rondom welke thema's de meeste spanning ervaren wordt.

Duiding van de Delta-score

0 tot 0,5	de huidige focus is gewenst
>0,5 tot 1	Een lichte verschuiving van focus is gewenst
>1 tot 1,5	Een significante verschuiving van focus is gewenst
>1,5 tot 2	Een grote verschuiving van focus is gewenst
>2	Een zeer grote verschuiving van focus is gewenst

Zie figuur 1 en 2

Voor het 13de Trends in Veiligheid rapport spraken we met diverse bestuurders uit de het publieke veiligheidsdomein met digitalisering in hun portefeuille. We vroegen deze bestuurders wat voor hen de belangrijkste technologietrends zijn en waarom? Waar zou de focus volgens hen moeten liggen en waar ligt de focus nu op? Wat zijn de grootste kansen en wat de grootste bedreigingen van deze technologietrends. En tenslotte: wat zijn de meest kansrijke strategieën om als het publieke veiligheidsdomein op deze technologietrends te acteren.

Technologische evolutie is een proces van continue verandering, van generatie op generatie met inmiddels een oneindige hoeveelheid mogelijkheden. Ook de verwachtingen en eisen vanuit de maatschappij aan het veiligheidsdomein blijven zich ontwikkelen: iedereen kan meedoen in het digitale tijdperk[1]. Dat maakt dat deze bestuurders te maken hebben met een groot scala uitdagingen en kansen op hetzelfde moment.

Onze conclusie is dat de bestuurders een duidelijke koers en visie hebben voor hun organisaties. Al is het bepaald geen sinecure om daar daadwerkelijk te komen. Obstakels zullen overwonnen moeten worden. Variërend van samenwerking op het gebied van innovatie en gegevensuitwisseling tot het op een verantwoordelijke manier benutten van de mogelijkheden van generatieve AI.

Inlopen op het schaakbord van Koning Shirham

Bestuurders opereren dagelijks in het spanningsveld tussen het moderniseren van de eigen IT-systemen enerzijds en de winkel openhouden anderzijds. Gebruik willen maken van innovaties als cloud en AI om de noodzakelijke sprong voorwaarts te maken enerzijds. En anderzijds het waarborgen van de privacy van burgers, de veiligheid van de samenleving en de werkbaarheid van IT-systemen. Bestuurders moeten continue deze, soms tegengestelde belangen, realiseren. Bijna zonder uitzondering wordt het werk van veel organisaties in het veiligheidsdomein ondersteund door systemen die oud en soms zelfs voorbij hun levensduur zijn. Tegelijkertijd zit hier ontzettend veel business logica en kennis in verweven. Samen met een grote stapel aan kwetsbaarheden en software die niet meer beheerd wordt of zelfs bestaat. Deze organisaties kunnen nog niet profiteren van kansen die nieuwe ontwikkelingen zoals onder andere cloud, (generatieve) AI en cybersecurity bieden. De uitdaging van de bestuurders is samen te vatten als; hoe zet je nu de stap van de oude wereld naar een nieuwe moderne wereld die voortdurend vernieuwd?

De situatie is nog het beste te vergelijken met het schaakbord van koning Shirham[2]. Deze organisaties lopen misschien twee tot vier velden achter op de markt. Dat lijkt overzichtelijk. Maar helaas brengt ieder veld exponentiële groei mee. Daarmee is het gat tussen wat nu kan en waar men nu staat groeiende. En dit brengt juist voor het veiligheidsdomein extra risico's met zich mee, omdat het minder goed bedoelende deel van de samenleving juist inspeelt op deze risico's. Terwijl burgers en bedrijven toch echt continue vernieuwing in digitale dienstverlening verwachten: snel, eenvoudig in gebruik, maximaal transparant en altijd correct.

1 https://www.digitaleoverheid.nl/werkagenda-waardengedreven-digitaliseren/

2 Het verhaal van de rijstkorrels op het schaakbord van koning Shirham is een bekende parabel die de kracht van exponentiële groei illustreert

Zorgen over verouderde technologie

Bestuurders geven aan redelijk tot veel aandacht binnen hun eigen organisatie te ervaren voor de trend die ze zelf het belangrijkst vinden (3,8, op een schaal van 1 tot 5). Het grootste zorgpunt voor bestuurders is het wegwerken van de legacy. De belangrijkste benoemde trends zijn cloud en AI, omdat bestuurders daar de meeste kansen in zien voor het wegwerken van de legacy en het verbeteren van de eigen werkprocessen. Tegelijkertijd zien bestuurders in deze trends de meeste risico's. Het wegwerken van de interne legacy wordt het vaakst benoemd als belangrijke aandachtslurper: pas als de legacy is weggewerkt, kan de focus richting het benutten van de kansen die cloud en AI mogelijk te bieden hebben.

Geen tweede toeslagenaffaire

We leven inmiddels in de superslimme samenleving en wordt met de dag slimmer[3]. Ook de organisaties in het veiligheidsdomein werken iedere dag aan deze samenleving. Wel geven ze daarbij twee grote zorgen aan: hoe zorg je ervoor dat de burger blijft bereiken en hoe zorg je ervoor dat je dat de dienstverlening aan de burger geïntegreerd is met de achterkant van de organisatie.

Als één ding duidelijk wordt is dat de toeslagenaffaire een duidelijk impact heeft gehad in de wijze waarop wordt omgegaan met nieuwe technologieën. Deze mogen dan wel veel kansen bieden maar het moet veilig zijn, voldoen aan alle wetgeving en de privacy moet geborgd zijn. Pas als dat geregeld is kan de volgende stap gezet worden. Want een nieuwe affaire moet koste wat kost voorkomen worden. Ook als dat betekent dat zo'n technologie niet gebruikt kan worden.

Die voorzichtigheid vertaalt zich ook naar de cloud. Ja, zonder meer biedt cloud mogelijkheden om wendbaarder en weerbaarder te worden. Maar hoe weet ik of dat veilig is, de privacy goed is geborgd en bovenal welke opties heb ik om naar een andere partner te gaan? Diezelfde vragen worden ook gesteld rondom AI. Terwijl voor beide geldt dat het een enorme versnelling kan betekenen naar een moderne en modulaire IV-voorziening. Waar meer waarde voor de maatschappij gerealiseerd kan worden.

Het is echter niet zo dat de ontwikkeling stilstaat of dat er nog geen gebruik gemaakt wordt van deze nieuwe technologieën. AI in een minder volwassen vorm (zoals business rules) wordt al jaren succesvol toegepast ter ondersteuning van de menselijke besluitvorming. Net zo goed dat de cloud mondjesmaat op kleine schaal wordt gebruikt. Echter, de grotere primaire systemen doen dat nog niet en daar zit nu net de grote winst op lange termijn.

De rat race van AI

OpenAI heeft in november 2022 de wereld bewust gemaakt van de kracht van generatieve AI is. Het is een mainstream onderwerp geworden en wordt besproken van de bestuurskamer tot aan de huiskamer. Generatieve AI heeft de potentie om banen te veranderen en sommige werkzaamheden uit handen van mensen nemen. Net zoals robotisering en RPA al een aantal jaren doen. Hoe de baan van de toekomst er uit ziet is nog een vraagteken. Hoe kan dit ingepast worden in het werk van een wijkagent, rechter of een reclasseringsambtenaar? Het is geen vraag meer of, maar hoe en op welke manier deze technologieën ingezet kunnen worden. En hoe doe je dat ook nog op een energie effectieve en duurzame manier, want de inzet van AI kost enorm veel energie.

De geïnterviewde bestuurders wijzen ook op de andere kant van de medaille. Criminelen raadplegen bijvoorbeeld ChatGPT om te vragen wanneer en waar ze het beste kunnen inbreken. Of de vrees dat algoritmes die in het algoritmeregister staan bewust worden voorzien van foutieve informatie door kwaadwillenden. Of het gebruik van deze technologieën om reisdocumenten te vervalsen die bijna niet van echt te onderscheiden zijn.

3 https://www.capgemini.com/nl-nl/expertise/research/society-50-waardegedreven-digitaliseren-met-de-menselijke-maat/

Darmee ontstaat gelijk een geheel nieuw werkveld. Het veiligheidsdomein moet kunnen vaststellen wat gecreëerd is door generatieve AI en dus vals is en wat echt. Zij noemen dit inmiddels de rat race van AI oftewel counter-AI.

Een andere nieuwe opkomende technologie is quantum computing. Een onderwerp dat nog ver weg lijkt maar dat niet is. OpenAI heeft bewezen dat zaken waarvan we denken die nog jaren ver weg zijn, toch ineens dichtbij blijken te zijn. Deze technologie brengt nieuwe kansen en risico's mee. De bestuurders wijzen op de verwachting dat de huidige beveiliging dan niet meer voldoende is. Het voorbeeld dat zij geven is of de beveiliging van een paspoort dat nu uitgegeven wordt ook aan het einde van de geldigheidsduur van 15 jaar nog wel veilig is. Quantum is daarmee vandaag al een onderwerp van gesprek.

Cybersecurity: meer dan technologie

Wanneer cybersecurity ter sprake komt merk je dat dit inmiddels chefsache is geworden. Wellicht heeft de pandemie hierbij geholpen. Door het plotseling vele thuiswerken is de vraag prominenter geworden of de thuiswerkplek wel veilig genoeg is. Of het werken onderweg in de trein of op andere (semi)-openbare werkplekken wel kan? Hoe zorg je ervoor dat medewerkers op de juiste manier omgaan met alle (vertrouwelijke) informatie? Op de werkplek kun je dit goed organiseren, maar in een gedistribueerde werkomgeving is dit geen eenvoudige opgave.

Tel daarbij op dat methodes van kwaadwillende steeds geavanceerder worden. Zij gebruiken de nieuwe technologieën al en het wordt steeds moeilijker om hier niet in te trappen. Daarom wordt er continu geïnvesteerd in bewustwordingscampagnes en geavanceerde technologieën om de veiligheid te blijven waarborgen. Alle bestuurders zijn het met elkaar eens dat het niet een kwestie is van of alleen focus op de medewerkers of alleen op technologie. Nee, beide aspecten moeten integraal worden geadresseerd. Als voorbeeld wordt gewezen op het recente lek bij de Amerikaanse geheime diensten waarbij vertrouwelijke documenten over de oorlog in Oekraïne naar buiten werden gebracht.

De bestuurders wijzen ook op een nieuw snijvlak wat aan het ontstaan is op het gebied van AI en cybersecurity. Waarbij cybersecurity tools ingezet worden om misbruik van AI-systemen te voorkomen. Door vroegtijdige detectie van valse informatie. Of en hoe dit snijvlak zich gaat ontwikkelen is nog onduidelijk.

Het data-ecosysteem van de toekomst

Alle bestuurders geven aan dat gegevensuitwisseling gewenst is en binnen de juiste kaders zelfs onvoorwaardelijk is. Zij vinden de afstand tussen de partners ook groter dan gewenst. De wil is er, maar op operationeel niveau lopen de organisaties tegen diverse uitdagingen aan om data daadwerkelijk en effectief in de veiligheidsketen te delen. Het is vaak onduidelijk wat de behoefte van de ander is, welk doel er precies is en wie de eigenaar van de data is.

Als de bestuurders kijken naar de eigen organisatie zien zij een aantal gemeenschappelijke rode draden. Het gat tussen de klassieke IT-er en de organisatie wordt kleiner. De komst van data scientist is hier debet aan. Evenals de mogelijkheid om meer technisch georiënteerde medewerkers in de organisatie in te zetten. Daarnaast is er een heldere strategie die gebaseerd wordt op de realisatie van een federatief datastelsel[4]. Als laatste wordt het loskoppelen van data en applicaties genoemd. Zodat het mogelijk wordt om data snel en eenvoudig te gebruiken. Innovatie speelt daarin een grote rol.

Ook op het gebied van innovatie is er de wil om samen te werken. De praktijk wijst uit dat dit toch solistisch wordt opgepakt. Innovaties worden veelal vanuit de eigen praktijk en voor eigen doelen opgepakt. Hier wordt ook veel tijd en geld aan gespendeerd. En bij positieve uitkomsten worden deze ook gedeeld met ketenpartners. Wel is men kritisch op het succes. Want de beoogde duurzame verandering is (zeer) laag.

4 https://www.digitaleoverheid.nl/achtergrondartikelen/federatief-datastelsel-het-organiseren-van-vertrouwen/

De volgende stap

Concluderend: veel organisaties in het veiligheidsdomein staan aan de vooravond om hun grote systemen te vernieuwen. Zij hebben hierbij de volgende uitgangspunten:

1. Data als fundament. Er moet een federatief datastelsel komen wat zowel intern als in de verschillende ketens gebruikt kan worden. Daar hoort bij dat er heldere en duidelijke afspraken zijn tussen partners hoe en op welke wijze data van elkaar gebruikt kan worden, zodat blindelings op elkaar vertrouwd en gebouwd kan worden.

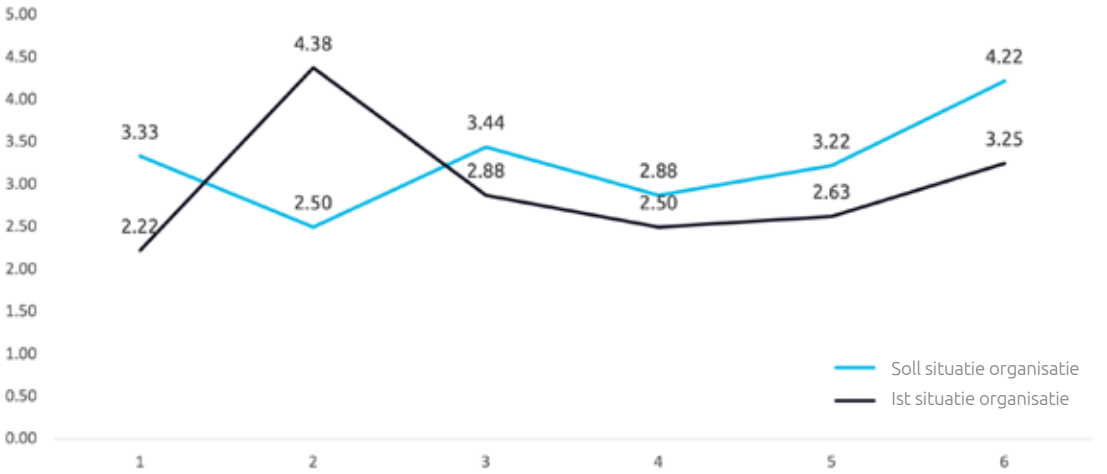
2. Zet de burger centraal. Dit kan een slachtoffer, migrant, verdachte of burger zijn die iets wil of moet van de overheid. Het maakt niet uit via welke manier de burger contact opneemt, het antwoord is altijd hetzelfde en up-to-date. Organisaties moeten vanuit dat perspectief hun processen en systemen inrichten.

3. Aan de achterkant moeten medewerkers geholpen worden door nieuwe technieken die werk uit handen nemen en ruimte bieden voor andere dingen. Om zo uiteindelijk als organisatie betere dienstverlening te kunnen leveren aan de maatschappij. Dit kan zijn: meer productie, betere kwaliteit en snellere doorlooptijd.

Dit moet leiden tot een modern digitaal landschap op basis waarvan deze organisaties zorgen voor een veilig en weerbaar Nederland. Organisaties die in staat zijn om nieuwe ontwikkelingen in de maatschappij te ondervangen en een plaats te geven. Zoals een van de bestuurders aangeeft wordt er binnen de organisatie nu gewerkt vanuit een gemeenschappelijk overeengekomen strategie. Is er gezamenlijk een governancemodel uitgewerkt waarlangs gewerkt wordt?[5]. Dit geeft helderheid, focus en het vertrouwen om Nederland veilig te houden.

5 Artikel: 5 organisatorische voorwaarden van een goede samenwerking uit Trends in Veiligheid 2022-2023

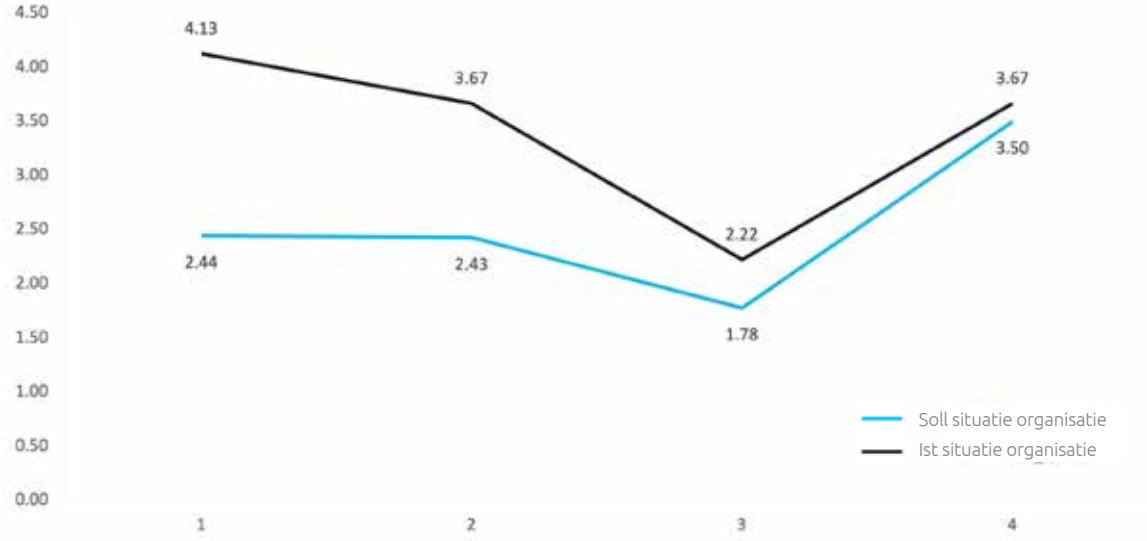
Soll situatie organisatie	Ist situatie organisatie
1 Inzetten op het verzamelen van voor ons belangrijke data	1 Veel meer gebruikmaken van beschikbare data van ketenpartners en openbare bronnen
2 Artificial Intelligence veel grotere het ontsluiten van de voor ons beschikbare data	2 De ervaring van mensen veel leidender in het ontsluiten van de voor ons beschikbare data
3 Meer vertrouwen in kwaliteit van de voor ons beschikbare data	3 Veel meer aandacht en tijd voor opschonen en verbeteren van de beschikbare data
4 Privacy weegt zwaarder dan veiligheid in afweging dataverzameling en datagebruik	4 Veiligheid weegt zwaarder dan privacy in afweging dataverzameling en datagebruik
5 Werknemers veel bewuster omgaan met de security van onze digitale systemen	5 Veel meer gebruikmaken van geavanceerde security tools voor onze digitale systemen
6 Veel meer IT experts moeten werken	6 IT experts veel nauwer samenwerken met andere expertises



Figuur 1: Tegenstellingen organisatie

Delta score van de kloofanalyse

Soll situatie organisatie	Ist situatie organisatie
1 Inzetten op onderling vrij delen van data	1 Kritischer op geschiktheid en veiligheid datadeling van ketenpartners
2 Inzetten op het gezamenlijk inhuren van IT-expertise	2 Meer eigen mensen tot IT-experts trainen tbv voldoen aan vraag in keten
3 Bewustwording databehoeftes ketenpartners tbv effectieve datadeling	3 Breder data verzamelen, bewaren en delen tbv voorzien in databehoeften van alle ketenpartners
4 Meer samenwerking bij innovatie tbv schaalvoordelen voor de hele keten	4 Organisaties maken zelf mankracht en budget vrij tbv passende, geschikte en nodige innovaties



Figuur 2: Tegenstellingen

Over de auteurs

Marcel Kordes
Director public sector

Marcel is verantwoordelijk voor het domein openbare orde en veiligheid binnen Business Technology Services. Marcel is. Hij is technisch bedrijfskundige en heeft meer dan 15 jaar werkervaring in het openbaar orde- en veiligheidsdomein.

https://www.linkedin.com/in/marcelkordes/
marcel.kordes@capgemini.com

Miriam Staal-Cuppen
Business Analist Publieke Sector

Miriam heeft 15 jaar ervaring met onderzoek doen voor (semi-) publieke organisaties, met name gericht op strategieontwikkeling en stakeholderrelaties. Miriam heeft een Master Politicologie en een PhD Technische Bestuurskunde en is gecertificeerd data scientist. Momenteel zet ze haar vaardigheden in ten behoeve van het verbeteren van de digitale dienstverlening van de rijksoverheid.

https://www.linkedin.com/in/miriam-staal-cuppen-9695367/
miriam.staal-cuppen@capgemini.com

13

PUBLICATIES

Naast ons Trends in Veiligheid rapport publiceren wij nog andere rapporten, onderzoeken en whitepapers die voor u relevant kunnen zijn. Onderstaand treft u een verkort overzicht aan.

Het complete overzicht vindt u op. www.capgemini.nl

Society 5.0: WAARDENGEDREVEN DIGITALISEREN MET DE MENSELIJKE MAAT

In de derde editie van Society 5.0 ligt de focus op de publieke dienstverlening met de menselijke maat. Hoe goed begrijpt de overheid de context van een individu en het toepassen van maatwerk? Uit ons onderzoek uitgevoerd door Ipsos blijkt dat zeven op de tien Nederlanders vinden dat de overheid technologie beter moet toepassen in haar dienstverlening. In deze publicatie wordt de balans gezocht tussen doorgeslagen digitalisering en doorgeslagen maatwerk (willekeur en rechtsongelijkheid).

Scan QR code to know more

TRENDS IN CYBERSECURITY 2023

Cybersecurity is een vereiste binnen ieder bedrijf, biedt een veilige basis voor transformatie en ondersteund alle werkzaamheden. Hoe zorg je voor overzicht en controle over jouw cyber risk programma? Hoe snel kun je terug naar je dagelijkse werkzaamheden wanneer cybercriminaliteit jouw organisatie raakt? En heeft jouw organisatie een schaalbare aanpak als het gaat om IT-beveiliging?

Scan QR code to know more

CLOUD, VOOR EEN DUURZAME IT

Bedrijven moeten zowel hun economische belangen als de milieueffecten van uitbesteding in overweging nemen bij het kiezen van een cloudprovider. Maar heeft het gebrek aan transparantie in de branche gevolgen voor milieuvriendelijke IT-strategieën? De mogelijkheden van cloudtechnologie nemen snel toe en veel organisaties maken er gebruik van bij hun digitale transformatie. Gezien de toenemende energiekosten en klimaatverandering is het echter vangroot belang dat bedrijfsdoelstellingen en duurzaamheid met elkaar in evenwicht zijn. In dit rapport delen we onze inzichten over de selectie van leveranciers en best practices op enterprise-niveau om digitale energiebesparing te behalen.

Scan QR code to know more

14

COLOFON

Deze editie van Trends in Veiligheid is tot stand gekomen met medewerking van:

- Aydan Gunduz
- Judith Groenewoud
- Jule Hintzbergen
- Thomas de Klerk
- Bas Koper
- Marcel Kordes
- Martijn van de Ridder
- Erik Staffeleu
- Ismay van de Water

Advies, ontwerp en productie: Marketing & Communicatie, Capgemini Nederland B.V.

- Johanna Achterberg
- Ashim karmakar
- Puja Sengupta

Marnix van 't Klooster, Shutterstock

Capgemini Nederland B.V.

Postbus 2575 - 3500 GN Utrecht

+31 30 689 00 00

trendsinveiligheid.nl@capgemini.com

www.capgemini.nl

Over Capgemini

Capgemini is een wereldwijde, maatschappelijk verantwoorde en multiculturele marktleider met 350.000 mensen in bijna 50 landen. Als strategisch partner ondersteunt Capgemini organisaties bij hun transformatie door gebruik te maken van de kracht van technologie. Hierbij laat de Group zich leiden door zijn bestaansreden: menselijke energie vrijmaken door middel van technologie voor een inclusieve en duurzame toekomst. Met meer dan 55 jaar ervaring en expertise in uiteenlopende sectoren, vertrouwen klanten de aanpak van hun zakelijke behoeften toe aan Capgemini: van strategie en ontwerp tot operationeel beheer. Dit gebeurt door gebruik te maken van innovaties in cloud, data, kunstmatige intelligentie, connectiviteit, software, digital engineering en platforms. De Group behaalde in 2022 een omzet van € 22 miljard.

GET THE FUTURE YOU WANT | www.capgemini.nl

Capgemini Nederland B.V.
Postbus 2575 - 3500 GN Utrecht
Tel. + 31 30 203 05 00
www.capgemini.nl

IN/2D-012.23