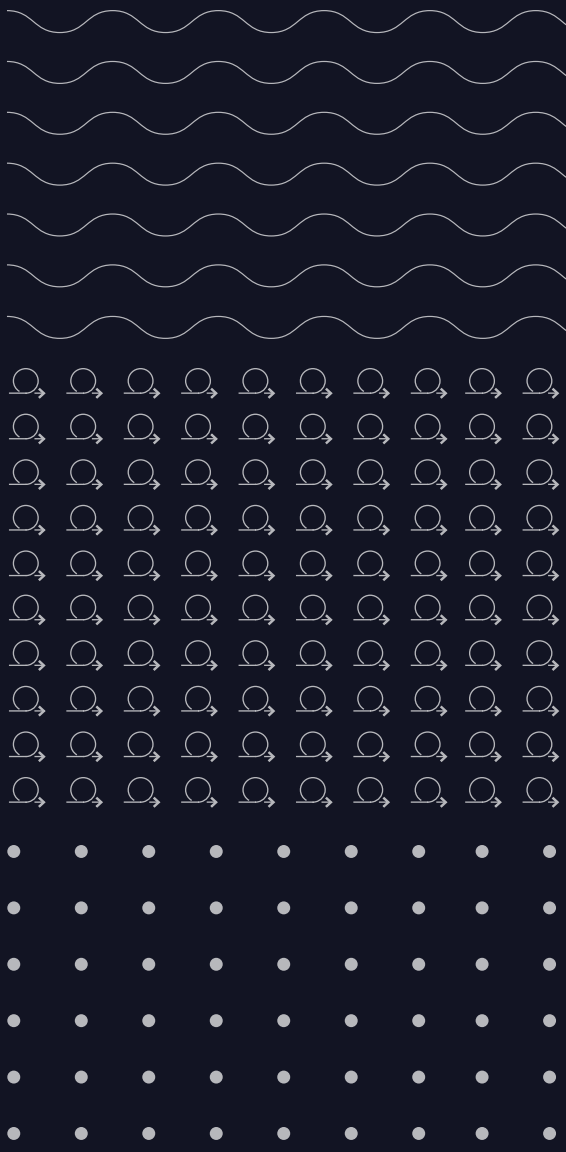
Trends in Veiligheid 2024-2025

Veiligheid in Society 5.0

Capgemini

Trends in Veiligheid 2024-2025

Veiligheid in Society 5.0



Inhoudsopgave

Burger centraal

Toekomst van werk

Management samenvatting Trends in Veiligheid 2024 - 2025: *Veiligheid* in Society 5.0

In een wereld die sterk afhankelijk is van technologie is veiligheid cruciaal. Daarom brengen wij voor de 14de keer het Trends in Veiligheid rapport uit. Dit rapport is speciaal samengesteld voor het publieke veiligheidsdomein, waarin we waardevolle inzichten beschrijven om jouw organisatie te beschermen, te ontwikkelen en te innoveren; met als thema dit jaar: 'Veiligheid in Society 5.0'.

Om ons heen krijgt Society 5.0 steeds meer vorm: een superslimme samenleving, waarin we technologie inzetten om ons welzijn en onze welvaart te bevorderen. Altijd met de menselijke maat, en altijd met oog voor transparantie en privacy. En: met oog voor veiligheid, want Society 5.0 heeft twee kanten: aan de ene kant biedt technologie ons de kans de veiligheid van ons land en onze burgers beter de garanderen, maar aan de andere kant levert die technologie juist nieuwe uitdagingen op voor die veiligheid – en daarbinnen voor de bescherming van onze ethische normen en waarden. In deze nieuwe editie van Trends in Veiligheid gaan onze experts in op de verschillende verschijningsvormen van veiligheid in het tijdperk van Society 5.0. Dat doen ze aan de hand van vijf thema's. Voor elk van de 5 thema's laten we bovendien een aantal leidinggevenden van organisaties uit het publieke veiligheidsdomein aan het woord. Hieronder geven we een kort overzicht van wat u kunt verwachten.

Verantwoord gebruik van AI

De politie ziet het speelveld door digitalisering sterk veranderen. Geavanceerde cybercrime, decryption door quantum technology, deep fakes door AI: het is maar een greep uit wat Society 5.0 met zich meebrengt; “Wendbaarheid is voor de politie meer dan ooit essentieel.”

Aan het woord is Joop van der Born. Als Chief Technology Officer is hij onder meer verantwoordelijk voor de ontwikkeling, het beheer en onderhoud van de IT-infrastructuur, het applicatielandschap en de rekencentra van de politie. Een geheel dat steeds complexer wordt, met de intrede van technologieën als Artificial Intelligence (AI), Data Science of Big Data en quantum technologie.

Van belang zijn transparantie, proportionaliteit en een sterk ontwikkeld ethisch kompas. De politie wil geen ‘big brother-maatschappij’. Belangrijk is dat het publiek begrijpt wat de politie doet, zegt Van der Born. “Als je niet goed uitlegt aan het publiek hoe je AI inzet, waarom en met welke waarborgen, dan ontstaat er wantrouwen. We hebben AI hard nodig voor de rechtshandhaving, maar wel ingezet volgens de spelregels van de rechtsbescherming.”

Het is een perspectief dat vaker terugkomt in dit rapport. Bijvoorbeeld in het artikel van Quido de Zwart en Mirjam Smid. Alleen door technologie in te zetten voor het goede, ben je echt in staat burgers te beschermen tegen minder goedbedoelde uitingen ervan: “Ontwikkelingen als generatieve AI hebben hun weerslag op de veiligheid van de burger. Draai het om en het kan ingezet worden in gerichte mogelijkheden die de burger een veiliger gevoel geven en veiligheid bieden in een digitale omgeving.”

Forensisch onderzoek

Digitale data ontsleutelen en AI-modellen ontwikkelen: het is dagelijks werk voor de digitaal forensisch onderzoekers van het NFI. De grenzen van technologie én ethiek bewaken is een interessante uitdaging voor Society 5.0 en het NFI.

“Het gaat bij DBS vooral om analyses en visualisaties voor politie, OM en andere partners in de veiligheidsketen. Digitale sporen zijn te vinden in bijvoorbeeld auto’s, telefoons en computers. We zeggen ook wel: als het een geheugen heeft, dan is het fair play.” Het zijn de woorden van Erwin van Eijk, Hoofd divisie Digitale en Biometrische Sporen (DBS) en Chief Data Officer bij het Nederlands Forensisch Instituut (NFI). Zijn divisie houdt zich bezig met forensisch onderzoek binnen geautomatiseerde systemen, en biometrisch onderzoek zoals vergelijkend vingersporen-, spraak- en beeldonderzoek.

Van Eijk: “Wij zoeken naar patronen. Om onderzoek te kunnen doen over zaken heen, wil je niet alleen data uit één specifieke zaak toepassen. Je wilt ook voorgaande sporen analyseren, maar dat kan niet anoniem. Als wetenschapper heb je een ander doel en perspectief dan een beleidsmaker. Hoe kunnen we binnen de bestaande wet- en regelgeving optimaal ons werk doen? Dat vind ik een buitengewoon interessante en belangrijke vraag.”

Hoe ziet dat er dan concreet uit, de toepassing van technologie en innovatie in het forensisch domein? Dat leest u bijvoorbeeld in het artikel van Athena van den Busken, Anne-Sophie Fritschij en Vien Germawi. Hun onderwerp: Virtual Reality. Hun conclusie: “VR belooft een diepere en meer gedetailleerde exploratie van de waarheid in forensische en juridische contexten.”Waarbij ze aantekenen dat dat altijd gepaard moet gaan met oog voor uitdagingen op het gebied van acceptatie, realisme, toepasbaarheid, technische infrastructuur en data-veiligheid.

De digitale defensie

De toekomst van onze samenleving is de toekomst van de arbeidsmarkt. Society 5.0 verandert de bestaande arbeidsstructuren ingrijpend. In een wereld van mondiale spanningen moet het personeelsbestand van Defensie flexibel en schaalbaar zijn. “In vredestijd moet je je arbeidsmarktstrategie ontwikkelen. Onze rol als werkgever verandert sterk.”

Paul van der Touw is brigadegeneraal en souschef Personele Gereedheid bij de Defensiestaf. Hij noemt de opkomst van technologie in het veiligheidsdomein als een van de uitdagingen bij het vinden van gekwalificeerde nieuwe medewerkers. Dat is een uitdaging. Zeker in de huidige, krappe arbeidsmarkt waarin extreem veel vraag is naar goede IT-mensen: “Overal waar je technologische innovaties succesvol integreert in militaire concepten ontstaat een groeimarkt en een tekort aan mensen. Zo hebben we veel ICT-ers en cybertechnici nodig want we verdedigen Nederland ook in het

informatiedomein. In dat domein wordt gevochten, 365 dagen per jaar."

Ziedaar de uitdaging van ons defensie-apparaat. Het hervonden belang dat ons land hecht aan een goed uitgeruste defensie kan niet zoals vroeger volledig worden ingevuld met fysieke capaciteiten. Het digitale domein is minstens zo belangrijk – want de digitale dreigingen zijn aanzienlijk.

Een landmacht die zich steeds meer beweegt in het digitale domein moet ook de manier waarop het apparaat wordt aangestuurd herijken. De aansturing verandert totaal. Governance krijgt een nieuwe dimensie: data governance. Jeroen Jeschke schreef er een artikel over, dat u in dit rapport terugvindt. Concreet: als steeds meer van je materieel zelfdenkend, zelfsturend en zelf-beslissend is (denk aan gerobotiseerde drones), dan kun je er maar beter voor zorgen dat de data waarop zulk materieel haar beslissingen baseert, in orde is.

Society 5.0 in de meldkamer

Om burgers in nood efficiënt en snel te helpen én hulpdiensten goed te faciliteren in noodsituaties, moeten meldkamers altijd beschikbaar zijn. Altijd, dus ook met oog op de toekomst. Dat betekent een nieuwe inrichting met een flinke digitaliseringsslag.

In 2010 waren er nog meer dan 25 meldkamers, nu zijn dat er twaalf. "En dat moeten er uiteindelijk tien worden in 2025 met één gestandaardiseerde dienstverlening", legt Melvin Doorn uit. Hij is hoofd functionele meldkamervoorzieningen Landelijke Meldkamer Samenwerking. Naast de continue vernieuwing en doorontwikkeling heeft LMS ook te maken met aanzienlijke veranderingen, zoals door de ontwikkeling van Artificial Intelligence. Society 5.0 en specifiek 'de burger centraal' doet ook steeds meer zijn intrede. Zo zal de ontwikkeling van slimme devices de komende jaren het werk van de meldkamer beïnvloeden."Dan ontvang je veel meer informatie dan alleen uit een belletje", aldus Doorn."Vanuit de techniek kunnen we de gekste dingen bedenken. Maar de centralisten moeten ook digitaal vaardig genoeg zijn, én onze wetgeving moet voldoende afgestemd zijn op dit soort ontwikkelingen zodat we deze technologische mogelijkheden ook kunnen benutten."

Wat het in deze context precies betekent om de burger centraal te stellen, daarop gaan Chèr van Slobbe, Inge Koning en Teddy van Eijk in hun artikel dieper op in. Aan de hand van het concept van de 'burgerreis' laaten ze zien hoe publieke organisaties – zoals meldkamers! – zich een helder beeld kunnen verschaffen van de weg die burgers bewandelen, van melding tot oplossing. In hun woorden: "Door deze benadering kunnen organisaties proactief reageren op de behoeften van burgers en oplossingen bieden die daadwerkelijk aansluiten bij hun dagelijkse realiteit."

Onder druk van toenemende maatschappelijke complexiteit wordt de asielketen in Nederland geconfronteerd met verschillende uitdagingen. De toenemende instroom van asielzoekers, de druk op de woningmarkt en een veranderend politiek klimaat brengen nieuwe vraagstukken met zich mee voor organisaties zoals het Centraal Orgaan opvang asielzoekers (COA). De rol van technologie wordt in deze context steeds belangrijker om de efficiëntie van besluitvorming te vergroten. "Door nauwkeurige data kunnen we als organisatie kalm blijven in chaos" aldus Rogér Pellemans Directeur Opvang & Begeleiding COA

Digitale weerbaarheid

De technologie in Society 5.0 ontwikkelt zich razendsnel. Daar profiteert het veiligheidsdomein van, maar criminelen ook. De gevallen van cybercrime die werden gemeld bij de politie stegen in 2020 met 132% en groeiden in 2021 door met nog eens 33%.

Het is al met al geen wonder dat cybersecurity een van de belangrijkste agendapunten is binnen het Ministerie van Justitie en Veiligheid en haar taakorganisaties. De naïviteit erover is inmiddels wel verdwenen, meent Ric de Rooij. Hij is als plaatsvervangend secretaris-generaal van het Ministerie van Justitie en Veiligheid eigenaar van 28 taakorganisaties, waaronder het COA, NFI, DJI en NCSC, en verantwoordelijk voor de continuïteit van de dienstverlening. De Rooij: "We zijn ons steeds meer bewust van de risico's, dreigingen en gevaren. Cybersecurity is chefsache geworden."

Nederland staat er gelukkig niet alleen voor. Ook voor de Europese Unie is digitale veiligheid topprioriteit. Prioriteit die bijvoorbeeld tot uiting komt in NIS2: de nieuwe versie van het Network and Information Security Directive, die later dit jaar van kracht wordt. De Rooij: "We voorzien grote consequenties voor de inrichting daarvan, maar de noodzaak is duidelijk. Zeker in een tijd van geopolitieke spanningen moeten we ons voorbereiden op nieuwe technologieën en dreigingen."

De urgentie die De Rooij bepleit leest u ook elders in dit rapport terug. Bijvoorbeeld in het artikel van Ana-Isabel Llacayo. Wat haar betreft is de adoptie van richtlijnen als NIS2 de eerste prioriteit: "Door samenwerking, innovatie en strikte naleving van regelgeving, kan de Nederlandse publieke sector niet alleen toekomstige cyberdreigingen effectief het hoofd bieden, maar ook de voordelen van generatieve AI optimaal benutten voor een veiligere samenleving."

In vogelvlucht hebben we laten zien dat het digitale aspect een steeds grotere rol speelt binnen alle subdomeinen van het veiligheidsdomein. Digitale dreigingen vragen om een digitaal antwoord. En dat antwoord moet hand in hand gaan met een sterk ethisch besef, en respect voor de menselijke maat. Ziedaar een van de voornaamste uitdagingen van Society 5.0.

Erik Staffeleu
Marcel Kordes
Natasja Pieterman
Martijn de Ridder
Aydan Gunduz

Interview:

“Digitale weerbaarheid is topprioriteit, en er moet meer gebeuren”

Cybersecurity is een van de belangrijkste agendapunten binnen het ministerie van Justitie en Veiligheid en haar taakorganisaties. Maar nieuwe uitdagingen vereisen ook overheidsbreed een nauwere samenwerking. “Informatiebeveiliging stopt nooit.”

De gevallen van cybercrime die werden gemeld bij de politie stegen in 2020 met 132% en groeiden in 2021 door met nog eens 33%[1]. Cyberaanvallen waren in de periode 2022-2023 volgens de NCTV[2] vooral afkomstig van statelijke en criminele actoren. Ook vielen digitale processen relatief vaak uit. Cyberincidenten, bijvoorbeeld door ransomware bij organisaties als ziekenhuizen en zorgplatformen en niet-vitale bedrijven van de overheid, maakten duidelijk hoe breed de pijlen worden gericht en hoe groot de kwetsbaarheid is.

Naïviteit is verdwenen

De naïviteit is inmiddels wel verdwenen, meent Ric de Rooij. Hij is als plaatsvervangend secretaris-generaal van het Ministerie van Justitie en Veiligheid eigenaar van 28 taakorganisaties, waaronder het COA[3], NFI[4], DJI[5] en NCSC[6], en verantwoordelijk voor de continuïteit van de dienstverlening. De Rooij: “We zijn ons steeds meer bewust van de risico’s, dreigingen en gevaren. De maatschappelijke opgave vereist ook dat we ons beter voorbereiden op de gevolgen. Weerbaarheid is als taak dan ook breed verankerd in onze organisatie.”

De Rooij: “De afgelopen jaren heeft onze organisatie vooral gewerkt aan ‘de basis op orde’. Dat begint bij simpele zaken als het voorkomen dat mensen vrijelijk van het ene naar het andere gebouw wandelen. Daarnaast is er veel aandacht voor trainingen, opleidingen en cursussen op het gebied van cyber- en gedigitaliseerde criminaliteit. Het onderwerp vereist echter een verandering van mindset over het gebruik van alles wat digitaal is. Herhaling is cruciaal. We moeten blijven vertellen wat het belang is. Maar uiteindelijk is het mensenwerk. Samenwerking is essentieel als je stappen wilt maken. Niet alleen als organisaties onderling maar ook met onze partners uit het bedrijfsleven.”

Cybersecurity is ‘chefsache’

De Rooij zag het besef over digitale veiligheid de afgelopen jaren groeien. “Als overheid zijn we ons steeds meer bewust van en gewend aan de dreiging. Weerbaarheid gaat echter niet alleen om digitale veiligheid maar ook om economische weerbaarheid, weerbaarheid in grote ketenafhankelijkheden en, zeker in onze tak van sport zeer relevant, de fysieke weerbaarheid. Mensen worden zich steeds bewuster van hun fysieke kwetsbaarheid als gevolg van digitale zichtbaarheid. Het is onze prioriteit te zorgen voor een veilige werkomgeving. Daar ligt een verantwoordelijkheid bij de werkgever en de werknemer. Medewerkers gebruiken daarom geen TikTok meer en houden rekening met de implicaties van buitenlandse reizen. Ik ben ook steeds meer een voorstander van managed devices en de inzet van een public én private cloud.”

Voor het ministerie is cybersecurity inmiddels een ‘chefsache’ geworden. De Rooij: “De informatie die wij ontvangen, ontdekken en opsporen is uitermate belangrijk in veel strafzaken maar heeft ook implicaties voor onze nationale veiligheid. Informatiebeveiliging is voor ons dan ook prioriteit één, twee endrie. Wij hebben er fors geld ingestoken. Dat is noodzakelijk als jeveiligheid vooropstelt.”

Ric de Rooij
Plaatsvervangend secretaris-generaal
Ministerie Van Justitie en Veiligheid

Versnippering tegengaan

Toch moet er meer gebeuren, meent De Rooij: "Informatiebeveiliging stopt nooit. Wat vandaag relevant is, blijkt morgen alweer verouderd. Het is belangrijk dit onderwerp structureel in te bedden in de organisatie. Dat begint bij de verantwoordelijkheid; bij wie ligt die? Moeten we de positie van de CISO (Chief Information Security Officer – doorgaans werkzaam onder de CIO) bijvoorbeeld upgraden? Ook zie ik nog steeds te veel versnippering binnen de overheid. Binnen onze eigen organisatie hebben we zaken steeds beter afgestemd en weten we welke informatie naar buiten gaat en hoe die beveiligd is. Maar overheidsbreed zou meer uniformering een volgende, noodzakelijke stap zijn. Ik zou willen pleiten voor één SOC (security operations centre, red.) voor de rijksoverheid."

Een belemmering is echter een gebrek aan bekwame mensen, erkent De Rooij. "We zoeken vaak naar techneuten maar naar mijn overtuiging hebben we vooral verbinders nodig. Het gaat om samenwerking en zorgen dat de issues op de bestuurderstafel komen." Want er liggen verschillende uitdagingen in het verschiet.

Afhankelijkheid van risico's verminderen

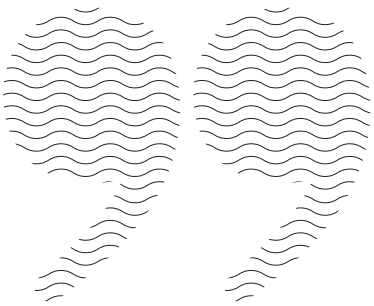
Zo gaat ook de NIS2[7] veel impact hebben op de organisatie. De Rooij: "We voorzien grote consequenties voor de inrichting daarvan. We zijn nu de benodigde bedragen aan het optellen, en die zijn fors. Het gaat ook iets betekenen voor de verantwoordingslijn en het toezicht. We zijn ermee bezig maar staan nog aan het begin. Ook daarbij geldt dat wij eerst de basis op orde moeten hebben. Bij sommige instanties is nog niet alles gedigitaliseerd. Dat is relatief veilig maar niet wat we willen. De strafrechtketen is daarentegen in rap tempo aan het digitaliseren. Dat levert ook nieuwe vraagstukken op, bijvoorbeeld over detectie. Is een stuk onderweg niet gecorrumpeerd? Ook NFI en WODC[8] zijn bezig om data- en gegevensdeling op een zeer veilige manier te organiseren. Veilig gegevens delen vraagt echter om heldere kaders: wat heb je echt nodig, kan het en mag het? Door verschillende incidenten is de organisatie nu wat kopschuw geworden, maar dit zijn wel de vraagstukken die wij voor de toekomst moeten beantwoorden met elkaar."

Daarnaast zullen er keuzes gemaakt moeten worden. Geopolitieke veranderingen vragen om voorbereiding op verschillende scenario's. Van Rooij: "We zijn in toenemende mate afhankelijk van IT, stabiele netwerken, internet en elektriciteit. Door die afhankelijkheid nemen de risico's toe. Zeker in een tijd van geopolitieke spanningen moeten we ons voorbereiden op nieuwe technologieën en dreigingen. We moeten onder meer bepalen hoe we ons willen voorbereiden op storingen of black-outs, maar ook bepalen welke keuzes we willen maken. Wat doen wij als het actueel wordt? Wat krijgt voorrang?"

Cybercriminaliteit is schaalbaar geworden

Cybersecurity is dan ook topprioriteit, meent De Rooij. "Er wordt door criminelen voortdurend, op geautomatiseerde wijze gekeken of er ergens een ingang kan worden ontdekt. Cybercriminaliteit is schaalbaar geworden. Een onoplettend moment kan voldoende zijn om een cyberlawine te veroorzaken. We moeten altijd alert zijn en blijven."

Tegelijkertijd leveren nieuwe technologieën ook oplossingen. De Rooij: "Onze taakorganisaties zoals het NFI onderzoeken bijvoorbeeld hoe we tools als AI kunnen inzetten om sneller malware, DDoS-aanvallen of phishingmails te ontdekken en aanvallen te onderscheppen. Ook wordt door het NFI en de politie AI ingezet voor het herkennen van patronen, beelden of stemmen. Daarmee worden ook onze defensiemechanismen, het verzamelen van bewijslast, opsporingsmechanismen en dossiervorming schaalbaar. We hebben echter wel de dure plicht om dat goed te blijven beveiligen."



1. Openbaar Ministerie - Het OM in cijfers | Jaar in verhaal (openbaarministerie.nl)
2. Nationaal Coördinator Terrorismebestrijding en Veiligheid
3. Centraal Orgaan opvang Asielzoekers
4. Nederlands Forensisch Instituut
5. Dienst Justitiële Inrichtingen
6. Nationaal Cyber Security Centrum
7. Network and Information Security (NIS2) directive: richtlijn gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten. De NIS2-richtlijn richt zich op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. De komst van de richtlijn moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties. (bron: NCSC)
8. Wetenschappelijk Onderzoek- en Datacentrum

Weerbaarheid

01
Weerbaarheid

Navigeren door het landschap van AI en informatiebeveiliging voor de Nederlandse publieke sector

Hoe moeten organisaties in het publieke veiligheidsdomein zich aanpassen aan ontwikkelingen op het gebied van AI en beveiliging?

In het tijdperk van digitale transformatie worden publieke instellingen voortdurend geconfronteerd met de uitdaging om hun cyberbeveiligingsstrategieën te herzien en aan te passen. De snelle ontwikkeling van generatieve kunstmatige intelligentie (GenAI) biedt zowel revolutionaire mogelijkheden als nieuwe veiligheidsrisico's. Deze dynamiek vereist een diepgaand inzicht in hoe de nieuwste AI-capaciteiten kunnen worden benut om de openbare veiligheid te versterken en tegelijkertijd kritieke infrastructuur te beschermen tegen geavanceerde cyberdreigingen.

Highlights

- Dreigingsactoren hebben AI ontdekt als nieuw gereedschap in hun arsenaal om organisaties aan te vallen.
- De NIS2-richtlijn stimuleert het gebruik van AI als onderdeel van een cyberbeveiligingsstrategie.
- Cyberbeveiligingsorganisaties bieden praktische richtlijnen van generatieve AI en cybersecurity
- De Europese AI Act zal een cruciale rol spelen om te zorgen dat entiteiten die AI-oplossingen gebruiken en ontwikkelen, voldoen aan de normen voor gegevensbescherming en naleving van intellectuele eigendomsrechten en auteursrecht.
- Generatieve AI kan worden ingezet ten voordele van informatiebeveiliging, inclusief het beoordelen van logboeken, het nemen van monsters voor malware-detectie en het analyseren van dreigingsinformatie.

Digitale Transformatie in de Publieke Sector

De aanstaande digitale transformatie binnen de Nederlandse publieke sector vereist een proactieve benadering van informatiebeveiliging. Met de toenemende afhankelijkheid van Cloud technologieën, IoT-apparaten en opkomende Zero Trust-architecturen wordt AI een steeds belangrijker instrument voor het beschermen van kritieke infrastructuren en gevoelige informatie.

In het laatste decennium heeft de publieke sector een explosieve toename gezien in het omarmen van technologische trends zoals de migratie naar de cloud, het gebruik van IoT-apparaten, en Zero Trust architectuur voor veilige en moderne hybride werkomgevingen. Op dezelfde manier heeft AI al een belangrijke rol gespeeld in digitale transformaties, met de opkomst van Big Data en Analytics die een steeds grotere rol spelen in data-gedreven organisaties. Met de recente ontwikkelingen in generatieve AI beginnen we nu pas de impact van deze technologie voor de publieke sector te ontdekken.

Generatieve AI: een zegen en een vloek voor informatiebeveiliging

Dreigingsactoren hebben generatieve AI als een nieuw instrument in hun arsenaal verkregen om kwetsbare organisaties aan te vallen. Generatieve modellen kunnen misbruikt worden om data te leren en zo informatiebeveiligingscontroles te omzeilen. Bijvoorbeeld, een model kan getraind worden om normaal netwerkverkeer te evalueren en vervolgens vijandige data te creëren om Inbraakdetectiesystemen (IDS) te ontwijken. Kwaadwillenden kunnen ook proberen iemands stem na te bootsen of nepvideobeelden te genereren en een aanval met social engineering te ondernemen. Een nietsvermoedend slachtoffer is zich mogelijk niet bewust dat de persoon met wie zij spreken niet een vertrouwde vriend of familielid is die om geld vraagt, maar een kwaadwillende die genoeg data heeft verzameld om die persoon digitaal na te bootsen. Nieuwe kwetsbaarheden worden ontdekt in generatieve AI-modellen. Sommige gebruikers hebben aangetoond dat ze data uit een groot taalmodel (LLM) kunnen extraheren dat vergrendeld zou moeten zijn met controles door een misleidend rollenspel tussen de gebruiker en het LLM. Het uitbreiden van deze kwetsbaarheid naar organisaties die LLMs ontwikkelen en in productie nemen, kan ernstige gevolgen hebben voor modellen die getraind zijn op gevoelige data, zoals persoonsgegevens of bedrijfsgeheimen.

De wijdverbreide adoptie van generatieve AI door zowel kwaadwillende als het publiek zal nieuwe risico's introduceren voor het domein van de openbare veiligheid. Publieke instellingen die AI intern ontwikkelen, moeten ervoor zorgen dat ze voldoende beveiligd zijn en het publieke belang in gedachten houden. Sommige organisaties kunnen profiteren van het defensief gebruiken van generatieve AI om informatiebeveiligingsteams te ondersteunen bij het beveiligen van een organisatie. Om deze recente ontwikkelingen aan te pakken, worden nieuwe regelgevingen ontwikkeld voor veilig en eerlijk gebruik van AI. Diverse organisaties ontwikkelen beveiligingskaders en richtlijnen om beveiligingsteams in organisaties te ondersteunen. Dit alles maakt deel uit van het veranderende landschap van AI en cyberbeveiliging, en dit artikel is bedoeld om organisaties te informeren en hen in staat te stellen vandaag nog te handelen.

Wetgeving en strategie

De adoptie van AI binnen de publieke sector wordt nauwlettend gevolgd door regelgevende instanties, met de NIS2-directive en de AI Act die een kader scheppen voor veilig en ethisch gebruik van AI-technologieën. Deze wetgevingen benadrukken het belang van gegevensbescherming, transparantie en de bescherming van intellectueel eigendom, waardoor organisaties worden aangemoedigd om AI op een verantwoorde manier te integreren in hun cyberbeveiligingspraktijken.

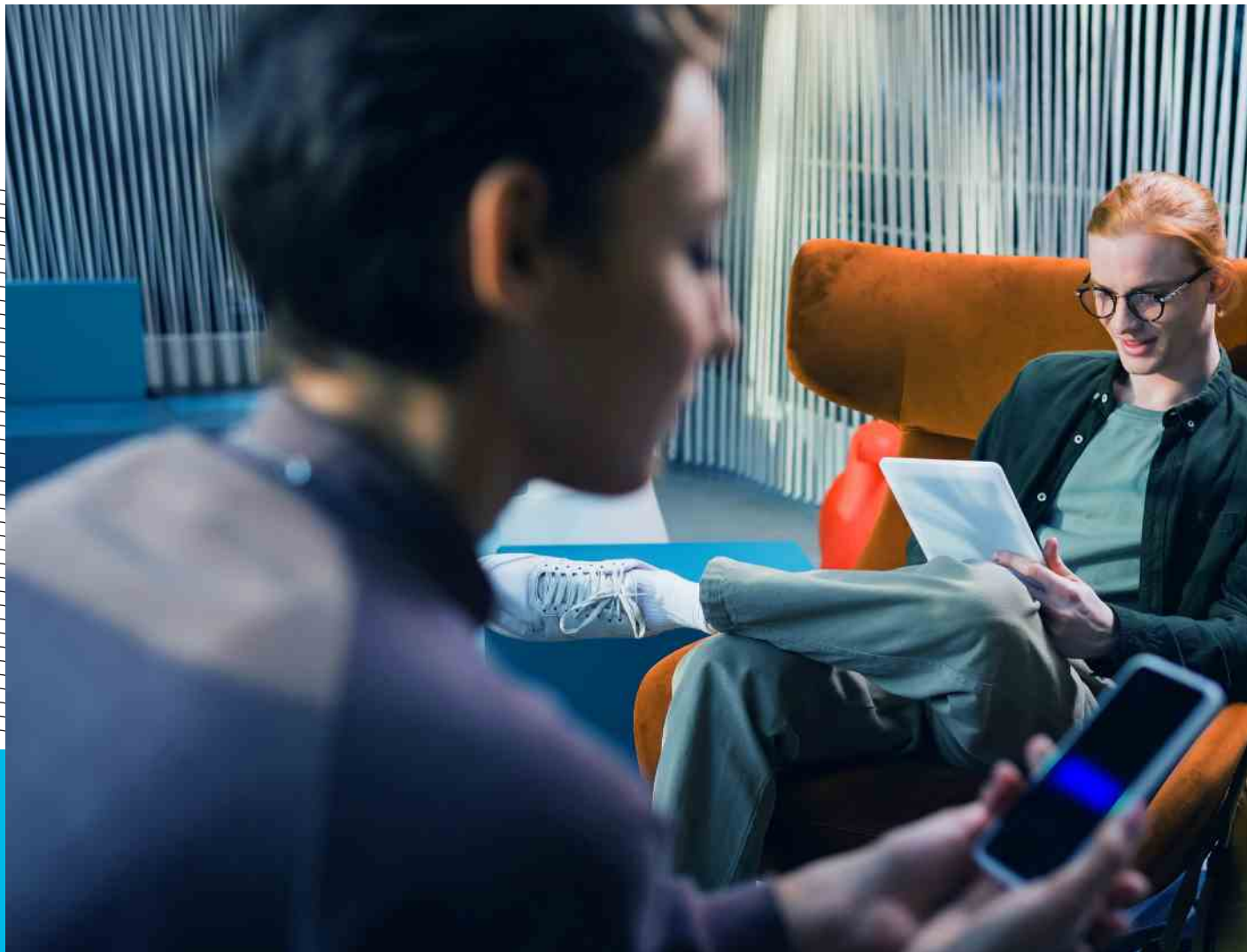
Naast het naleven van deze regelgeving, is het cruciaal dat organisaties binnen de publieke veiligheidssector proactieve strategieën ontwikkelen om de specifieke uitdagingen die generatieve AI met zich meebrengt, aan te pakken. Dit vereist niet alleen een technische heroverweging van beveiligingsprotocollen, maar ook een culturele verschuiving binnen organisaties om de kennis en vaardigheden te ontwikkelen die nodig zijn om deze nieuwe technologieën effectief te beheren.

NIS2-richtlijn en AI

De NIS2-richtlijn (Network and Information Security) vertegenwoordigt een omvangrijk pakket aan wetgevingen dat specifiek van toepassing is op organisaties die actief zijn binnen cruciale sectoren in de Europese Unie, waaronder de Nederlandse publieke sector. Deze richtlijn benadrukt het belang van robuuste cyberbeveiligingspraktijken voor 'vitale' sectoren zoals energie, gezondheidszorg, vervoer en openbaar bestuur, om zo te waarborgen dat kritieke infrastructuur veerkrachtig blijft tegen cyberaanvallen en de persoonlijke gegevens van burgers beschermd worden.

Om te voldoen aan de NIS2, dienen organisaties effectieve strategieën te implementeren die gericht zijn op risicobeheer. Dit omvat niet alleen het opstellen van plannen voor het geval van informatiebeveiligingsincidenten, maar ook het waarborgen van een heldere procedure voor het onderzoek naar en de oplossing van dergelijke incidenten. Een cruciaal aspect van naleving is de zekerheid dat partners, leveranciers en dienstverleners die bijdragen aan de levering van de Nederlandse vitale infrastructuur, eveneens voldoen aan strenge beveiligingseisen. Goed bestuur binnen een organisatie is essentieel. Het zorgt ervoor dat iedereen binnen de organisatie zijn of haar rol, verantwoordelijkheid en verantwoording kent in het garanderen van veiligheid.

Interessant is dat de NIS2 specifieke instructies bevat over het gebruik van AI, met als doel het detecteren en voorkomen van cyberaanvallen te bevorderen. Door AI te integreren in verschillende aspecten van een beveiligingsstrategie, zoals het detecteren en blokkeren van afwijkend netwerkverkeer, kunnen beveiligingsmaatregelen aanzienlijk worden geautomatiseerd. Het is echter van cruciaal belang dat het gebruik van AI in overeenstemming is met wetten omtrent gegevensbescherming en privacy, zoals de Algemene Verordening Gegevensbescherming (AVG). AI-systemen dienen nauwkeurige gegevens te leveren zonder grote hoeveelheden openbare data te verzamelen, te verwerken of op te slaan en moeten vrij zijn van vooroordelen die burgers kunnen discrimineren op basis van ras of



sociaaleconomische status.

Parallel aan de NIS2 wordt de AI-wetgeving binnen de Europese Unie ontwikkeld, met als doel een veilig, ethisch en eerlijk gebruik van AI te garanderen. Deze wet zal, eenmaal gefinaliseerd, een fundamentele rol spelen in het waarborgen dat entiteiten die AI-oplossingen gebruiken en ontwikkelen voldoen aan normen op het gebied van gegevensprivacy en naleving van intellectuele eigendoms- en auteursrechten. Verwacht wordt dat de AI-wet de GDPR-wetgeving aanvult om de veiligheid van de digitale economie binnen de EU te garanderen, gebruikmakend van een risico gebaseerde benadering.

Generatieve AI biedt talrijke voordelen voor de beveiliging, zoals de detectie van anomalieën en het genereren van synthetische data voor toepassingen waarin privacy van gegevens van groot belang is. Bovendien worden nieuwe technieken ontwikkeld waarmee modellen specifieke datapunten kunnen 'vergeten', wat bijdraagt aan de naleving van de GDPR.

Best practices en richtlijnen van de kennisleiders

Vooraanstaande organisaties op het gebied van cybersecurity, zoals OWASP, MITRE, NIST en CISA, hebben onmisbare bijdragen geleverd aan de bestrijding van de uitdagingen die generatieve AI met zich meebrengt. Zij bieden praktische richtlijnen en raamwerken die organisaties helpen bij het veilig navigeren door het complexe landschap van AI en cyberbeveiliging. Deze inspanningen benadrukken het belang van continue educatie, samenwerking en aanpassingsvermogen binnen de sector om zowel de huidige als toekomstige dreigingen effectief het hoofd te bieden.

In de context van de snelle ontwikkelingen binnen het domein van AI en cyberbeveiliging, staat de Nederlandse publieke sector voor zowel uitdagingen als kansen. De implementatie van de NIS2-richtlijn en de in ontwikkeling zijnde AI-wetgeving bieden een raamwerk voor het veilig en ethisch gebruik van AI-technologieën, gericht op het versterken van de cyberweerbaarheid van kritieke sectoren en het beschermen van persoonsgegevens. Het is essentieel dat organisaties proactief zijn in het adopteren van deze richtlijnen, het investeren in AI-competenties en het bevorderen van een cultuur van veiligheid en voortdurende verbetering. Door samenwerking, innovatie en strikte naleving van regelgeving, kan de Nederlandse publieke sector niet alleen toekomstige cyberdreigingen effectief het hoofd bieden, maar ook de voordelen van generatieve AI optimaal benutten voor een veiligere samenleving.

Over de auteurs

Jean de Smidt | Senior Security Consultant

Jean heeft een brede achtergrond in informatiebeveiliging, die zowel het testen, de engineering en architectuur omvat. Hij benut zijn ervaring op het gebied van informatiebeveiliging om raakvlakken te onderzoeken met opkomende onderwerpen zoals AI en cloudtechnologieën.

jean.smidt@capgemini.com

https://www.linkedin.com/in/jean-de-smidt/

Ruben Tienhooven | Stream Lead Cloud Security

Als jurist en IT-specialist weet Ruben de twee werelden van het cyberdomein samen te brengen. In zijn werk weet Ruben de eisen van wetten, regelgeving en het bedrijfsleven te vertalen naar concrete acties en maatregelen die in de praktijk geïmplementeerd kunnen worden.

ruben.tienhooven@capgemini.com

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

Omgaan met NIS2: Een veranderende rol voor het Ministerie van Justitie en Veiligheid

Wat is de impact van NIS2 op de borging van nationale weerbaarheid door het Ministerie van Justitie en Veiligheid?

NIS2 zorgt voor een Europese transformatie in cyber security governance. Het Nederlandse Ministerie van Justitie en Veiligheid heeft een breed mandaat om de nationale weerbaarheid te versterken. Dit artikel bespreekt de verschillende facetten van NIS2, en de gevolgen ervan voor het ministerie.

02
Weerbaarheid

Highlights

- Mandaat van het ministerie: Het Ministerie van Justitie en Veiligheid heeft een politiek mandaat voor de implementatie van de NIS2-richtlijn in Nederland.
- Interne compliance: Het Ministerie van Justitie en Veiligheid geeft het goede voorbeeld door intern de nieuwe eisen omtrent cybersecurity te implementeren.
- Incidentrapportage naar het NCSC: Het NCSC heeft een spilfunctie in de vormgeving van een national kader voor incidentrapportage rond dreigingen en incidenten.
- Rol in Europese samenwerking: De EU versterkt informatie-uitwisseling en situational awareness, met als doel de lidstaten voor te bereiden op grootschalige, grensoverstijgende incidenten of crises.
- Conclusie: Het ministerie heeft een aanzienlijk mandaat binnen de diverse geopolitieke ontwikkelingen.

Een politiek mandaat in Nederland voor de NIS2-richtlijn

Cybersecurity lijkt soms een vaag begrip. Voor velen is het niet meer dan het zoveelste bureaucratische buzz word. Toch komen steeds meer stakeholders erachter dat cybersecurity een stevige impact heeft op hun kernactiviteiten – en dat ze er zelf een rol in hebben. Op BNR luidden brancheverenigingen recent nog de noodklok: duizenden bedrijven lopen het gevaar klanten kwijt te raken en omzet mis te lopen, omdat ze niet goed op de hoogte zijn van de nieuwe cybersecurity-eisen van de EU[1]. In dit alles heeft het Nederlandse Ministerie van Justitie en Veiligheid een belangrijke rol te vervullen. Een rol met verschillende facetten. Dat is een flinke uitdaging, waar dit artikel dieper op ingaat.

Deze Nederlandse Cybersecurity Strategie (2022-2028) zoomt in op het belang van weerbaarheid voor overheden, bedrijven en samenleving.[2] De Network and Information Security Directive (NIS) vormt hiervoor de basis. Deze Europese wetgeving heeft als doel het niveau van digitale veiligheid te verhogen en (inter-)nationale samenwerking te versterken. In 2022 nam de EU NIS2 aan; een herziene versie van NIS die de tekortkomingen van de originele wetgeving adresseert. Vitale sectoren werden in de eerste versie bijvoorbeeld onvoldoende beschermd, en er ontstonden onevenredigheden tussen lidstaten. De herziene NIS2 stelt aanvullende eisen aan organisaties als het gaat om veiligheid, gaat in op veiligheid in supply chains, stelt striktere regels voor audits en implementeert uniforme sancties voor alle EU-lidstaten. NIS2 vormt al met al een flinke uitdaging voor een groter aantal entiteiten en sectoren, als het gaat om verantwoordelijkheid nemen voor cybersecurity en het voldoen aan de baseline voor cybersecurity-maatregelen.

Het is de taak van het Ministerie van Justitie en Veiligheid om de binnenslandse cybersecurity te bewaken en versterken. Het ministerie is daarmee ook verantwoordelijk voor de implementatie van NIS2. Dat doet het door NIS2 te vertalen naar Nederlandse wetgeving, en die wetgeving vervolgens te bekrachtigen. NIS2 wordt op 17 oktober 2024 van kracht in de EU. De Nederlandse versie van NIS1 - Wbni[3] zal dus moeten worden aangepast, net als het besluit (Bbni[4]). Dit process heeft overigens inmiddels al vertraging opgelopen.[5] Sectoren als energie, transport en watermanagement waren al gedekt door NIS1; NIS2 breidt de scope uit naar 18 sectoren, waaronder de Rijksoverheid, overheidsdiensten, ruimtevaart, onderzoek, manufacturing, managed security service providers (MSSP) en cloud-diensten. Deze bredere scope vereist een reorganisatie bij de

overheid, en nauwe afstemming met verschillende stakeholders. Daarbij moet in ogenschouw genomen worden dat er van lidstaat tot lidstaat verschillende interpretaties kunnen bestaan van NIS2; dat kan internationaal zakendoen voor Nederlandse bedrijven bemoeilijken.

Er dragen verschillende stakeholders bij aan de beleidsvorming rond de Nederlandse omzetting van NIS2, waaronder het National Cyber Security Centre (NCSC), de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), het Digital Trust Center, verschillende sectorale toezichthouders zoals de Rijksinspectie Digitale Infrastructuur, andere ministeries (om het ecosysteem in kaart te brengen) en duizenden Nederlandse bedrijven.

De voorbeeldrol van het Ministerie van Justitie en Veiligheid

Het ministerie is in de NIS2-richtlijn aangewezen als een 'essentiële entiteit'. Dit betekent dat ook het ministerie zich zal moeten aanpassen, om te kunnen voldoen aan de nieuwe regels. Dat begint met onderkenning en begrip op board level (en politiek) niveau van de cybersecurity-risico's. Dat begrip moet vervolgens een integrale plek krijgen in de algehele governance. Aangezien het bestuur van het ministerie verantwoordelijk is voor de mitigatie van (strategische) cybersecurity-risico's, moet het toezien op de compliance van het ministerie met NIS2. De publieke sector is uitgezonderd van de persoonlijke aansprakelijkheid die NIS2 voorschrijft omtrent het niet afdoende investeren in maatregelen die nodig zijn om cybersecurity te borgen.[6] Dat wil niet zeggen dat een veiligheidsincident zonder gevolgen zou blijven voor het ministerie. Nog afgezien van de reputatieschade die zou ontstaan, zou een dergelijk incident ook politieke gevolgen kunnen hebben. Als onderdeel van de Rijksoverheid is het Ministerie van Justitie en Veiligheid immers verantwoordelijk voor de veiligheid van de Nederlandse burgers en van persoonlijke en andere gevoelige gegevens. Het ministerie is bovendien verantwoordelijk voor de nationale cybersecurity.

Welke maatregelen moet het bestuur dan treffen? Zonder uitputtend te willen zijn: Ten eerste moeten huidige processen voor risicomanagement worden uitgebreid met beleid op cyber-dreigingen. Ten tweede moeten kritieke assets en applicaties grondig in kaart gebracht worden. Ten derde moeten zowel ambtenaren als managers worden getraind in cybersecurity en -awareness. En ten slotte moet 'cyber hygiene' een plek krijgen in de dagelijkse activiteiten binnen de organisatie.

De nadruk op veiligheid binnen de supply chain is een van de belangrijkste verschillen tussen NIS1 en NIS2. De onderlinge digitale afhankelijkheden tussen leveranciers staan hierbij centraal. Ook buiten de eigen 'hekken' moet het ministerie robuust risicomanagement rond cybersecurity inrichten, en zich meer bewust zijn van de kwetsbaarheden binnen externe diensten. Bij het uitschrijven van overheidsopdrachten moeten veiligheidsrisico's – en de omgang daarmee - een integrale plek krijgen.

Als het gaat om incident response moet het ministerie ervoor zorgen dat het, in geval van een vermoeden van een significant incident, binnen 24 uur een early warning afgeeft. Het gaat dan om incidenten die zijn gericht tegen de eigen organisatie, en die het gevolg zijn van onwettige, kwaadwillende activiteiten. Binnen 72 uur nadat het incident is opgemerkt, moet het ministerie bovendien officieel melding doen. Deze melding omvat details over de ernst en de impact van het incident, en een inschatting van de mate waarin de organisatie is gecompromitteerd – voor zover zulke gegevens voorhanden zijn. Om aan dergelijke eisen en krappe tijdslijnen te kunnen

voldoen zal het ministerie haar interne rapportagemechanisme wellicht moeten aanpassen. De organisatie moet kunnen beschikken over robuuste monitoring en threat intelligence en heldere communicatie- en rapportagelijnen tussen alle stakeholders die in verbinding staan met het security office van het ministerie. Ook van belang is continue communicatietraining, waarbij alle strategische en technische teams die verantwoordelijk zijn voor crisisbeheer worden betrokken.

In veel gevallen zijn de assets al beveiligd. Ook risicomanagement maakt al onderdeel uit van de governance – hetzij operationeel, hetzij financieel. De uitdaging voor het ministerie zit hem vermoedelijk vooral in de integraliteit die NIS2 voorschrijft. In juridisch opzicht is digitale veiligheid niet langer enkel de verantwoordelijkheid van IT, van de Chief Information Officer (CIO) of de Chief Information Security Officer (CISO). Het is de collectieve verantwoordelijkheid van alle leiders binnen de organisatie. Het zwaartepunt zal voor het ministerie dan ook vooral liggen in de afstemming tussen verschillende afdelingen en stakeholders, die elk hun eigen structuren hebben, en met het uitrollen binnen dat geheel van de NIS2-richtlijnen van het ministerie.

De zwaardere rol van de NCSC in NIS2

De aanstaande implementatie van NIS2 in Nederland heeft grote gevolgen. Vooral voor het National Cyber Security Centre (NCSC), dat opereert onder de verantwoordelijkheid van het Ministerie van Justitie en Veiligheid.

Onder NIS1 voert het NCSC de Computer Security Incident Response Team (CSIRT) taken uit voor vitale infrastructuren. Het fungeert bovendien als nationaal contactpunt voor cybersecurity-meldingen. Onder NIS2 groeit het mandaat van het NCSC. Om te voldoen aan de extra verantwoordelijkheden die daarmee gepaard gaan, heeft het centrum aanvullende resources nodig – zowel qua bemensing als qua financiën.[7] Het NCSC is bijvoorbeeld verantwoordelijk voor incident responses en voor het faciliteren en stimuleren van nationale en internationale samenwerking. Het NCSC treedt ook op als informatie- en kennispartner voor andere stakeholders. Een voornaam verschil met NIS1 is dat NIS2 niet langer onderscheid maakt tussen verleners van 'vitale diensten' en digitale dienstverleners. Dit kan voor bepaalde entiteiten gevolgen hebben voor de rol die het NCSC inneemt als CSIRT.[8]

De NCSC zal daarnaast haar diensten moeten uitbreiden naar de aan NIS2 toegevoegde sectoren – sectoren die tot nu toe geen onderdeel uitmaakten van de regelgeving. Het NCSC moet daarmee de slagkracht hebben om ondersteuning te bieden bij een (potentieel) groter aantal incidenten, en – samen met andere betrokken autoriteiten – toezicht te houden op een bredere reeks van entiteiten. Het is daarmee een uitgelezen kans voor het NCSC om haar vitale rol zichtbaarder te maken.

Onder NIS1 kregen nationale CSIRT's een belangrijke rol in de uitgifte van early warnings, aankondigingen en de verspreiding van informatie naar vitale en belangrijke entiteiten, autoriteiten en relevante partijen over cyber-dreigingen, kwetsbaarheden en incidenten. NIS2 introduceert nieuwe, pro-actieve en reactieve taken voor het nationale CSIRT, die moeten worden doorvertaald in het verder uitgebreide mandaat voor het NCSC in de Nederlandse omzetting van de regelgeving.[9] Die bredere scope omvat bijvoorbeeld: forensische data verzamelen en analyseren voor risk assessment, ondersteuning bieden aan entiteiten bij het reageren op incidenten, het scannen van netwerken of publiek toegankelijke systemen op kwetsbaarheden, of de openbaarmaking van kwetsbaarheden (Coordinated Vulnerability Disclosure, CVD) coördineren.

EU-samenwerkingsorganen voor informatiedeling en situational awareness

De rol van het NCSC, in samenwerking met het Ministerie van Justitie en Veiligheid, strekt zich uit tot ver buiten de landsgrenzen. Het NCSC vertegenwoordigt Nederland in Europese samenwerkingsorganen die sinds 2016 bestaan. De kern van deze samenwerking wordt gevormd door het Europese Agency for Cybersecurity (ENISA), dat fungeert als secretariaat voor het beheer van grensoverschrijdende incidenten, de coördinatie tussen de verschillende CSIRT's in het CSIRT-netwerk, en het beheer van het Information Sharing and Analysis Centers (ISACs)-ecosysteem. NIS2 zorgt voor nog sterkere samenwerking tussen lidstaten, bijvoorbeeld in het Europese cyber crisis liaison organization network (EU-CyCLONe).[10] Voor Nederland is het NCSC aangesloten op dit netwerk, als de bevoegde Nederlandse autoriteit op het gebied van crisismanagement, informatiedelen en situational awareness.

CyCLONe heeft een operationele rol. Door te focussen op de impact en gevolgen van een crisis, slaat CyCLONe een brug tussen technische aspecten en politieke besluitvorming. Op die

1. Brancheorganisaties luiden noodklok om nieuwe cyberveiligheidsregels | BNR Nieuwsradio, Accessed on 23 April 2024.
2. The Netherlands Cybersecurity Strategy 2022-2028 | Publication | National Cyber Security Centre (ncsc.nl)
3. wetten.nl - Regeling - Wet beveiliging netwerk- en informatiesystemen - BWBR0041515 (overheid.nl)
4. wetten.nl - Regeling - Besluit beveiliging netwerk- en informatiesystemen - BWBR0041520 (overheid.nl)

manier faciliteert CyCLONe goed onderbouwde beslissingen in geval van veiligheidsincidenten en crises.

In 2016 werd de NIS Cooperation Group opgericht. Hierin hebben ENISA, de Europese Commissie en de lidstaten zitting, waarbij het NCSC Nederland vertegenwoordigt. De implementatie van NIS2 heeft flinke gevolgen voor de herstructurering van nationale ecosystemen voor cybersecurity. De NIS Cooperation Group fungeert als forum voor het delen van nationale inzichten en best practices omtrent potentiële risicogebieden zoals 5G.[11] Daarnaast maakt NIS2 het lidstaten mogelijk om peer reviews uit te voeren, en zo inzichten op te doen uit gedeelde ervaringen. Op basis van NIS2[12] zouden nationale CSIRT's deelnemen aan zulke peer reviews. Dat geeft onder andere het NCSC een belangrijke rol in het delen met andere lidstaten van de Nederlandse aanpak en Nederlandse sectorale best practices. Vooral voor landen met een afwijkende benadering kan dit relevant zijn. Frankrijk kiest bijvoorbeeld een zeer gecentraliseerde aanpak voor het eigen cybersecurity-agentschap (ANSSI). Dit agentschap heeft een rol als auditor voor alle betrokken sectoren en biedt operationele ondersteuning bij veiligheidsdiensten. Het vertrouwt daarbij op een netwerk van gecertificeerde, 'trusted' leveranciers,

Een aanzienlijk mandaat binnen de huidige geopolitieke ontwikkelingen

De NIS2-richtlijn wordt geïntroduceerd in een tijd van flinke geopolitieke veranderingen. Die veranderingen vormen duidelijk een uitdaging voor de veiligheid en welvaart in Europa. Het is daarom van belang dat lidstaten en hun overheden blijven samenwerken, en beleid op cybersecurity implementeren dat onderling goed is afgestemd. In dit artikel heb ik laten zien hoe Nederland dit proces kan helpen vormgeven en de Nederlandse veiligheid kan borgen, vanuit de bepalende rol van het Ministerie van Justitie en Veiligheid.

Over de auteur

Ana-Isabel Llacayo | Senior Manager Data Security

Ana-Isabel is NIS2 Lead Advisor bij Capgemini Invent Nederland. Zij ondersteunt publieke overheden en vitale infrastructuren bij organisatievraagstukken die het gevolg zijn van ontwikkelingen in cybersecurity. Als expert draagt ze regelmatig bij aan Europese projecten die bijdragen aan beleidsvorming omtrent cybersecurity.

ana.isabel.llacayo@capgemini.com

https://www.linkedin.com/in/ana-isabel-llacayo/

5. Beslisnota bij Kamerbrief over stand van zaken implementatie NIS2 en CER richtlijnen | Beleidsnota | Rijksoverheid.nl
6. Art (32) EU NIS2 Directive 2022/2555
7. "Computer Security Incident Response Teams in the reformed Network and Information Security Directive: good practices"
8. Idem
9. Idem
10. EU CyCLONe — ENISA (europa.eu)
11. NIS Cooperation Group | Shaping Europe's digital future (europa.eu)
12. Art (10) EU NIS2 Directive 2022/2555

Interview:

“Mijn droom is dat onze mensen alle hightech tools ter wereld snel kunnen inzetten”

De politie ziet het speelveld door digitalisering sterk veranderen. Geavanceerde cybercrime, decryption door quantum technology, deep fakes door AI: het is maar een greep uit wat Society 5.0 met zich meebrengt. “Wendbaarheid is voor de politie meer dan ooit essentieel.”

Joop van der Born
Chief Technology Officer
Politie Nederland

Joop van der Born is sinds september 2023 Chief Technology Officer bij de politie. Hij is onder meer verantwoordelijk voor de ontwikkeling, het beheer en onderhoud van de complexe IT-infrastructuur, het applicatielandschap en de rekencentra van de politie. Hij maakt deel uit van de dienstleiding van de Dienst Informatievoorziening (IV).

De belangrijkste nieuwe technologieën voor de politie zijn Artificial Intelligence (AI), data science of big data en quantum technology. Van der Born: “Onze leefomgeving digitaliseert razendsnel. Overal hangen camera’s, zoals de vele deurbelcamera’s en ook onze smartphone is niet meer weg te denken. Denk bijvoorbeeld ook aan de cryptodata op de smartphones van criminelen. Als gevolg daarvan wordt de politie overladen met data van burgers en bedrijven, veel meer dan wat politiemensen handmatig kunnen verwerken. Met AI kunnen we beelden razendsnel scannen en vergelijken, bijvoorbeeld bij de bestrijding van kindermisbruik. Ook vingerafdrukherkenning gebeurt in een milliseconde. Daar komt geen mens meer aan te pas, behalve voor het nemen van de definitieve beslissing, dat zal altijd een menselijke beslissing zijn. Inmiddels ontwikkelen we zelf ook algoritmen voor bijvoorbeeld nummerplaatherkenning op digitaal bewijsmateriaal.”

Zorgvuldigheid en proportionaliteit

Technisch kan er al veel, maar wil de politie al deze algoritmes ook toepassen? Zorgvuldigheid en proportionaliteit zijn hierbij altijd belangrijke criteria zegt Van der Born. “Toepassing van dit soort technologische mogelijkheden moet worden afgewogen tegen het misdrijf dat je aan het onderzoeken bent. Onze opdracht is te zorgen voor veiligheid in een complexe maatschappij. Draagvlak is belangrijk evenals de balans tussen privacy en veiligheid. En natuurlijk begrip over het feit dat we niet in alles transparant kunnen zijn. Digitalisering en de inzet van nieuwe technologie en datagedreven werken zijn essentieel voor de politie. Je hebt geen keus als je effectief wilt blijven. Zo is voor onze opsporingspraktijk het ‘gouden uur’ cruciaal: binnen het eerste uur wil je zoveel mogelijk informatie rond hebben. Lukt dat niet, dan gaat het onderzoek veel langer duren. Maar je kunt niet overal camera’s ophangen. We willen geen ‘big brother’-maatschappij. We gebruiken bijvoorbeeld gezichtsherkenningstechnologie op basis van een algoritme om in een grote database te zoeken naar specifieke gezicht(en). Dat systeem helpt ons om grote hoeveelheden afbeeldingen van gezichten zeer snel te kunnen doorzoeken.”

Snel toetsen en testen

Van der Born: “We vinden het heel belangrijk om transparant en zorgvuldig met AI om te gaan. Voordat we het inzetten, denken we na over de juridische en ethische kaders en de operationele meerwaarde van AI. We zorgen uiteraard dat we altijd binnen de kaders van de wet blijven.” Ethiek is dan ook een belangrijk toetsingskader, vindt Van der Born: “Daarom testen en toetsen we zoveel voordat het

dagelijkse praktijk wordt. Dit doen we met steeds meer agile teams. Wendbaarheid is cruciaal. Willen we als politie onze rol kunnen pakken in Society 5.0, dan moeten we de snelheid van technologische veranderingen op een zorgvuldige wijze kunnen bijbenen. Of beter nog: proactief aan het roer staan. We moeten zeker nastreven dat de politie kennis heeft van technologieën die nu en in de toekomst door criminelen worden ingezet."

Exponentiële groei van data

Belangrijk is dat het publiek begrijpt wat de politie doet, zegt Van der Born. "Als je niet goed uitlegt aan het publiek hoe je AI inzet, waarom en met welke waarborgen, dan ontstaat er wantrouwen. We hebben AI hard nodig voor de rechtshandhaving, maar wel ingezet volgens de spelregels van de rechtsbescherming. De politie mag niet zomaar over data beschikken; er moeten waarborgen zijn voor het gebruik van data." Data groeit echter ook exponentieel. De enorme hoeveelheid data waarover de politie beschikt, moet verzameld, geanalyseerd, gearchiveerd en opgeschoond worden. Dat is voor een mens eigenlijk niet meer mogelijk. Hulp van AI is hierbij noodzakelijk. Van der Born: "De snelheid waarmee computers data kunnen analyseren neemt nog steeds sterk toe. Dat gaat in de toekomst door quantum computing nog veel meer versnellen. Dat staat nu nog in de kinderschoenen maar als die rekenkracht wordt ontketend, dan ontstaan ongekende mogelijkheden om snel data te analyseren. Tegelijkertijd moeten we ook voorbereid zijn op ongewenste consequenties. De huidige versleutelingen en cryptografie van bestanden en data zullen niet meer zo veilig zijn: quantum computers kunnen de huidige ingewikkelde encryptiesleutels blootleggen. Post-quantumcryptografy is daarom nu al iets om aandacht voor te hebben."

Veranderingen met impact op het veiligheidsdomein

Naast AI en kwantumtechnologie ontwikkelt ook cybercriminaliteit zich voortdurend. Van der Born: "Cybercriminaliteit is een miljardenbedrijf. En het is lastig wedijveren met miljardenbedrijven die wereldwijd opereren. Wij kunnen veel, maar cybercriminelen hebben het geld en de tijd om steeds weer een nieuwe aanvalsmethoden te creëren. We moeten continu alert zijn. Een 100% veilig systeem is een illusie; we moeten vooral heel snel kunnen detecteren en reageren. Digitale technologieën als AI maken dat mogelijk."

Eigenaarschap vanuit de praktijk

Het Nederlands politiekorps geldt als een van de meest digitale korpsen ter wereld. Veel zaken kunnen via apps op de smartphone worden geregeld. De politie heeft bovendien een speciaal programma ingericht: Hier hebben gespecialiseerde medewerkers eigenaarschap over wat er wordt ontwikkeld. Dat gebeurt veelal op basis van vragen uit de praktijk. Van der Born: "De maatschappij is onze maatstaf voor de meerwaarde van onze oplossingen. Product owners in onze agile teams zijn vaak 'blauw'; ze komen uit de operatie. Wat hun collega's nodig hebben, wordt direct ontwikkeld. Daar zit ontzettend veel snelheid in. We hebben een platform waar agile teams veel zelfstandig kunnen regelen; ze hoeven bijvoorbeeld geen changes meer in te schieten. Het is een soort PaaS wat we aanbieden. De basis ligt in de succesvolle samenwerking tussen IV-specialisten en de operatie. We hebben vier jaar succesvol een pilot gedraaid en gaan deze nu uitbreiden."

Innovatie mits schaalbaar

Dit soort pilots zijn de essentie van innovatie, meent Van der Born. "Ons netwerk van pionierende innovatieteams en innovatiemakelaars ontwikkelen allerlei innovaties voor urgente vraagstukken. Voorwaarde is dat innovaties schaalbaar zijn; er moeten 75.000 mensen mee aan de slag kunnen. Dat betekent ook dat er potentieel veel vraag kan komen naar die oplossingen. Daar zit de uitdaging voor snelle innovaties. Je wilt snel kunnen opschalen qua organisatie, beheer en serverruimte. Dat maakt onze cloud journey ook zo belangrijk voor snelle innovaties. Als we echt wendbaar willen zijn, dan kunnen we niet alles on-premises doen. Mijn taak is te zorgen dat we de juiste keuzes maken; hoe maken we optimaal gebruik van de slagkracht van cloud providers, en wanneer is data dermate gevoelig dat we het op eigen infrastructuur moeten zetten?"

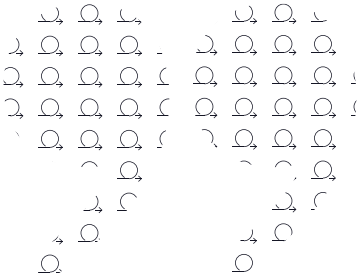
Voorwaarden voor wendbaarheid

De cloud first strategie kent twee sporen vertelt Van der Born. “Als het niet politie-specifiek is, dan is onze lijn ‘SaaS first’. Grote cloudleveranciers innoveren voor ons en bieden nieuwe technologie, toepassingen en services als eerste aan in hun SaaS-omgevingen. Die willen we hebben. Bovendien hebben zij gekoppelde datacenters met miljoenen servers. Dat biedt schaalbaarheid. Ze leveren ook een hogere kwaliteit en ze beschikken over veel innovatiekracht. De professionele cloud is bovendien veiliger dan wij kunnen bieden on-premises. We maken nu de overstap naar Microsoft 365. Niet zozeer vanwege de kosten maar vanwege veiligheid en snelheid. Ons Cloud Competence Center is hierbij een belangrijke speler. Zij denken mee over ons cloudbeleid, onze aanpak, ons databeleid en -architectuur. We moeten kritisch blijven. Snappen wij wat er in de cloudwereld kan en hoe we dit goed kunnen managen? En kunnen we dat vertalen naar onze wereld?”

Voor gevoelige politie-specifieke data is public cloud nog geen optie, vindt Van den Born. “Vertrouwelijke data moeten afgeschermd worden. Mogelijkheden als de private soevereine cloud maken je baas van je eigen data en dat schept weer nieuwe mogelijkheden om naar de cloud te gaan, maar dat duurt nog zeker vijf jaar. Cloud is wat mij betreft het juiste antwoord, mits drie zaken op orde zijn: 1) ik wil weten welke data naar de cloud gaat; 2) ik wil weten waar het staat en wat ze ermee doen en 3) ik wil weten of ik nog steeds eigenaar ben van die data en dat ik het kan terughalen. Dit vereist een uitstekende relatie met je leverancier. Je moet je leverancier kunnen regisseren op basis van een goed contract. Wij moeten doen waar wij verstand van hebben; de rest moet je durven overlaten aan de markt.”

Dromen van AI-capaciteiten en cloud

Over vijf jaar wil Van der Born dat de politie alle AI-capaciteiten op een intelligente en sociale manier inzet, evenals de mogelijkheden van cloud. “Een groot deel van onze on-premises infrastructuur zal dan gemigreerd moeten zijn naar cloud. Ik droom ervan dat onze collega’s op straat en rechercheurs alle tools kunnen inzetten die gebruikt worden door de beste beveiligingsorganisaties ter wereld. Applicaties kan men dan naar een beveiligde omgeving halen in een eigen sandbox en zelf onderzoeken. Werkt het goed? En voldoet de kwaliteit en transparantie aan onze eisen? Dan kunnen ze het vervolgens snel opschalen. Tools die niet handig zijn, verwijderen we weer. Zo houden we het applicatielandschap beheersbaar. De eerste stappen zijn gezet: we gaan onze innoverende platforms samenbrengen. Hiermee kunnen onze mensen ultrasnel gebruikmaken van nieuwe ideeën, vindingen of apps. Dat gaat een enorme snelheid geven aan onze werkzaamheden en resultaten, zodat we ook in de digitaliserende toekomst Nederland veilig kunnen houden.”



Wendbaarheid

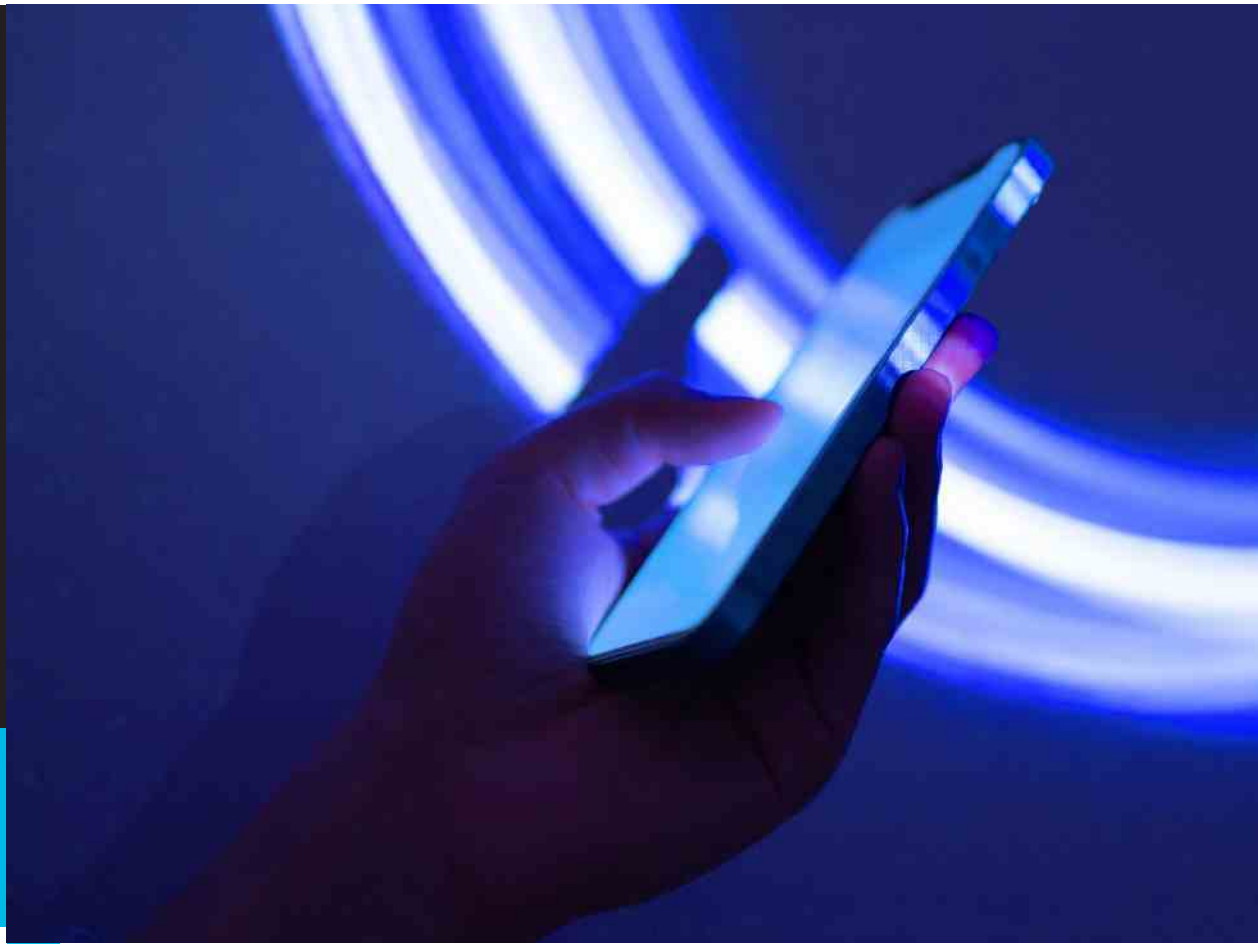
Weerbaarheid tegen aanvallen op de logistieke keten van toeleveranciers

Hoe kunnen risico's van aanvallen op de logistieke keten van toeleveranciers: worden verkleind?

Veiligheidsinstanties hebben onvoldoende zicht op de risico's binnen de logistieke ketens. De vraag is niet óf, maar wanneer zij hierdoor worden geraakt. Grip krijgen op de risico's ten aanzien van toeleveranciers binnen de logistieke keten kan door passende maatregelen te nemen.

Highlights

- Behoud up-to-date overzicht en inzicht ten aanzien van leveranciers.
- Vraag leveranciers om relevante certificeringen (bijvoorbeeld ISO 27001) en het uitvoeren van (IT) audits om inzicht te krijgen in hun eigen weerbaarheid.
- Voer proactief screenings uit ten aanzien van potentiële leveranciers, en stel beveiligingsmaatregelen als eis binnen contracten.
- Verzamel (geautomatiseerd) up-to-date data over relevante dreigingen (threat intelligence).



Aanvallen op logistieke ketens met betrekking tot toeleveranciers vormen grote risico's voor veiligheidsinstanties waaronder de Nationale Politie en Defensie. Het is algemeen bekend dat zowel reguliere bedrijven als overheidsinstanties gebruik maken van diverse leveranciers. Van het faciliteren van bedrijfskantines tot het inrichten en beheren van IT-omgevingen, of zelfs voor het gereedmaken en onderhouden van militaire voertuigen (Defensie). Veiligheidsinstanties hebben onvoldoende zicht op de risico's binnen de logistieke ketens. De vraag is niet óf, maar wanneer zij hierdoor worden geraakt. Grip krijgen op de risico's ten aanzien van toeleveranciers binnen de logistieke keten kan door passende maatregelen te nemen.

Het recente rapport van de Autoriteit Persoonsgegevens over de ruim 25.000 gemelde datalekken in 2023 is alarmerend. Veelvuldig worden (succesvolle) cyberaanvallen uitgevoerd tegen ingehuurde bedrijven waaronder ICT-leveranciers. Hierbij worden direct meerdere organisaties getroffen door hetzelfde incident. Vanuit de sector openbaar bestuur waren in 2023 in totaal 183 meldingen gemaakt van cyberaanvallen. Bij maar liefst 145 (79%) van deze meldingen waren ingehuurde bedrijven betrokken bij de cyberaanval. Organisaties die verantwoordelijk zijn voor de nationale veiligheid lopen dan ook grote risico's. In 2021 hebben hackers data gestolen bij ICT-leverancier Abiom, dat onder meer werkzaam is voor Defensie, de Nationale Politie en het Ministerie van Justitie en Veiligheid. Het zou gaan om interne documenten, waaronder gevoelige en vertrouwelijke communicatie met overheden, persoonsgegevens van leidinggevenden bij de politie, kopieën van paspoorten en verschillende overeenkomsten met buitenlandse overheden en bedrijven. Details van apparatuur die bij politie- en defensieonderdelen is geplaatst zou ook zijn gecompromitteerd. Een forensisch onderzoek is uitgevoerd om duidelijkheid te krijgen over het voorval, echter kan dit worden beschouwd als mosterd na de maaltijd.

De voordelen van samenwerking met (gespecialiseerde) leveranciers is evident, echter brengt dit ook risico's met zich mee, namelijk de kans op (cyber) aanvallen ten aanzien van de logistieke keten (supply chain attacks). Bij een dergelijke aanval lopen organisaties risico's omdat externe partijen waarmee wordt samengewerkt, zoals leveranciers, het doelwit worden van (cyber) aanvallen. Denk bijvoorbeeld aan dreigingsactoren die toegang krijgen tot systemen van de Nationale Politie of Defensie via een externe partij. Het kan voorkomen dat een externe partij minder goede maatregelen heeft genomen om de cyberweerbaarheid te waarborgen dan de eigen organisatie. Hierdoor kan een cybercrimineel de keuze maken om eerst een leverancier aan te vallen alvorens de stap naar het echte doelwit te maken – de weg van de minste weerstand. Het nemen van maatregelen en een goede samenwerking tussen partijen is van belang om de risico's en de eventuele impact van een incident te beperken.

Een ander voorbeeld waarbij het, voor zover bekend, niet fout is gegaan maar de impact van een potentieel incident bij de toeleverancier wel significant kan zijn is het volgende: in 2022 heeft Defensie een nieuwe overeenkomst afgesloten voor het vervangen van de commerciële 4x4 voertuigen, waaronder de Volkswagen Amarok. Bij de introductie van de Amarok is er meer aandacht gekomen voor optimalisatie van processen binnen de logistieke keten van Defensie en toeleveranciers. De Amarok werd destijds geassembleerd in de Volkswagenfabriek in Duitsland en als civiel voertuig naar Pon Logistics vervoerd, de Nederlandse leverancier van deze Amaroks. Vervolgens werden de specifieke delen voor Defensie (zoals bijvoorbeeld een wapenrek) op de voertuigen gemonteerd voordat deze aan Defensie werden overhandigd. Pon Logistics kreeg deze Defensie specifieke delen weer van andere leveranciers. De betreffende Amaroks werden vervolgens geleverd aan Defensie. Het onderhoud van de voertuigen gebeurde bij Volkswagen dealers, waardoor Defensie geen eigen voorraad reservedelen nodig had. Een voordeel, máár er zitten ook nadelen aan vast.

Inzicht in uw leveranciers geeft inzicht in uw risico's

Het vertrouwen in leveranciers is dan ook van groot belang. Kunt u zich voorstellen wat de nadelige gevolgen voor veiligheidsinstanties zouden kunnen zijn wanneer één of meerdere van haar leveranciers (bijvoorbeeld de dealers) zijn gehackt? Het saboteren van apparatuur of het vertragen van leveringen aan de

veiligheidsinstanties behoren zeker tot de mogelijkheden. Daarnaast zijn de risico's tevens van toepassing op de digitale wereld, bijvoorbeeld wanneer leveranciers ondersteuning bieden bij het ontwikkelen van software of het beheren van systemen en applicaties. Het beperken van risico's voor organisaties zoals de Nationale Politie en Defensie, maar ook breder kijkende naar de vitale infrastructuur, verdient dan ook voldoende aandacht te krijgen.

Om grip te krijgen op risico's is inzicht een belangrijke factor. Informatie die binnen de organisatie (interne bronnen) beschikbaar is kunnen over het algemeen relatief eenvoudig en vlot worden verzameld en benut. Naast interne informatie die van belang is, bijvoorbeeld tot welke interne systemen leveranciers toegang hebben en of die systemen van cruciaal belang zijn voor de organisatie of niet, is ook informatie van buitenaf (externe bronnen) van belang. Zo biedt interne informatie vaak beperkt inzicht in (nieuwe) risico's, zoals nieuw ontdekte kwetsbaarheden in software gebruikt door de leveranciers, of bijvoorbeeld gelekte data van leveranciers dat een indicatie kan zijn van potentiële (cyber) inbraak. Het verzamelen van up-to-date dreigingsinformatie (threat intelligence) kan organisaties waardevolle nieuwe inzichten verschaffen in risico's ten aanzien van de logistieke keten. Threat intelligence kan ondersteuning bieden om aandacht te geven aan specifieke zaken, bijvoorbeeld door accounts van leveranciers nauwlettend te monitoren en daarbij te focussen op technieken die door dreigingsactoren worden misbruikt. Dit biedt kansen om eventuele incidenten vroegtijdig te detecteren en hier adequaat op te reageren (incident response).

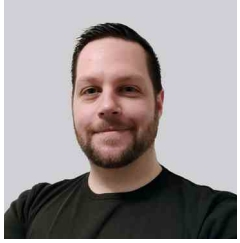
Externe bronnen, zoals bijvoorbeeld (semi)publieke informatie op het internet, helpen een vollediger beeld te krijgen van ontwikkelingen en dreigingen. Het verkrijgen van relevante informatie van deze bronnen kan handmatig worden gedaan, maar ook met behulp van geautomatiseerde tooling. Dit biedt de mogelijkheid om risico's omtrent leveranciers en andere relevante externe partijen automatisch te detecteren en zelfs hier op te acteren. Door bijvoorbeeld gebruik te maken van geautomatiseerde tools om het (dark)web te doorzoeken naar gelekte inloggegevens van leveranciers is het mogelijk om maatregelen te nemen die een eventuele stap naar de klantorganisatie voorkomen door de betreffende accounts direct, al dan niet geautomatiseerd, te blokkeren. Wanneer een dergelijke inbraak bij een leverancier bekend wordt gemaakt is het van belang hier zo snel en zo goed mogelijk op te reageren. Een goede samenwerking met de leverancier waarbij de veiligheidsinstanties, die gebruik maken van hun diensten, direct op de hoogte worden gebracht bij een potentieel incident (al voordat deze publiek wordt aangekondigd) verkleint de reactietijd en daarmee de potentiële impact.

Tot slot kunnen ook proactief maatregelen worden genomen, bijvoorbeeld bij het selecteren van een passende leverancier. Het vragen naar certificeringen van leveranciers (waaronder de ISO27001 certificering), het uitvoeren van screenings en het opleggen van de verplichting tot het uitvoeren van (IT) audits helpt om inzicht te krijgen in het vertrouwen en/of het beveiligingsniveau van de leverancier. Het opleggen van beveiligingsmaatregelen als eis aan de leverancier en het opnemen van de verantwoording van schriftelijke en periodieke rapportage in contracten kan tevens risico's beperken en geeft de leverancier de mogelijkheid om vertrouwen te winnen. Dit kan ondersteuning bieden bij het selecteren van nieuwe leveranciers en het kaf van het koren scheiden. Al deze zaken dienen te worden beschouwd als doorlopende processen, en heldere procedures zijn vereist om alles in goede banen te (blijven) leiden.

Bescherm uw logistieke keten

Sleutelwoorden om risico's ten aanzien van het werken binnen een logistieke keten aan te pakken zijn 'inzicht', 'samenwerking' en 'continu'. Effectieve samenwerking met leveranciers en het toepassen van automatisering, kan helpen de weerbaarheid tegen aanvallen binnen de logistieke keten continu te verbeteren en tegelijkertijd tijd- en kostenefficiënt te blijven.

Over de auteur



Alex Verbiest | Managing Consultant Cybersecurity – Read Team Lead

Alex Verbiest is verantwoordelijk voor het leiden van Capgemini's Red Team in Nederland, het opbouwen van het portfolio en het coördineren van projecten op het gebied van IT-security zoals pentesting, Red Teaming en phishing simulaties.

alex.verbiest@capgemini.com

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

1. https://www.rtlnieuws.nl/tech/artikel/5272070/hacken-ransomware-defensie-justitie-politie-losgeld
2. https://autoriteitpersoonsgegevens.nl/documenten/rapportage-datalekken-2023

Nederland veiliger door capability gedreven innoveren in veiligheidsorganisaties

Hoe zorgt innoveren in veiligheidsorganisaties dat Nederland veiliger wordt in de superslimme samenleving?

Veiligheidsorganisaties staan voor de grote uitdaging om Nederland veilig te houden in een context die digitaliseert, verhardt en polariseert. Capability gedreven innoveren stelt veiligheidsorganisaties in staat gericht en flexibel te innoveren.

04
Wendbaarheid

Highlights

- Effectief innoveren zorgt voor een wendbare organisatie om Nederland veiliger te maken.
- Innoveren gaat niet over technologie implementeren maar over het oplossen van problemen in de organisatie.
- Capability gedreven innoveren zorgt voor een strategische richting om innovatie te kanaliseren.
- In de superslimme samenleving is het cruciaal dat veiligheidsorganisaties wendbaar en flexibel blijven innoveren.

Technologie helpt steeds vaker in effectief optreden

22 februari 2022, Amsterdam schrikt op van het nieuws dat een gijzelnemer meerdere burgers in gijzeling heeft genomen in de Apple store op het Leidseplein in Amsterdam. De man, uitgerust met een bodycam, eist 200 miljoen euro aan cryptovaluta. Eén man wordt voortdurend onder schot gehouden door de gijzelnemer terwijl de politie het gebouw omsingelt. Na enkele uren komt een politierobot water brengen waarna de gijzelaar weet te ontsnappen. Hij rent de straat op als de deur opengaat, de gijzelnemer rent hem achterna. Op dat moment reageert de DSI adequaat en rijdt de gijzelnemer doelbewust aan. Nadat de man, die explosieven bij zich draagt, grondig is geïnspecteerd door een politierobot eindigt op deze manier de urenlange gijzeling.[1]

De casus laat zien dat (nieuwe) technologie steeds vaker zijn enorme meerwaarde aantoont in een operatie terwijl klassiek menselijk ingrijpen altijd nodig blijft. Waar technologie en menselijk handelen wordt gecombineerd, leidt dit tot een succesvolle interventie. Het laat zien dat de context waarin de politie haar kerntaak vervult, het handhaven van de rechtsorde en het verlenen van hulp aan hen die deze behoeven, complexer wordt. Dit geldt niet enkel voor de gijzeling in de Apple store, ook de ransomware aanval op een ziekenhuis en de ruim 3,6 miljoen ontsleutelde PGP-berichten door de politie zijn voorbeelden van de toenemende complexiteit van de verwevenheid van digitaal en fysiek en van mensen en technologie. Effectief optreden van veiligheidsorganisaties in een superslimme samenleving (Society 5.0) kan niet zonder inpassing van technologische innovatie. Om deze nieuwe technologie ten volle te kunnen omarmen zullen deze organisaties steeds adoptiever (sneller) en adaptiever (wendbaarder) moeten worden. Alleen dan zijn deze organisaties instaat om een passend antwoord te formuleren op de veiligheidsbehoefte die vanuit de samenleving wordt gesteld.

Wendbaarheid is noodzakelijk om effectief te blijven als veiligheidsorganisatie

In het interview over wendbaarheid met Joop van der Born, de CTO van de politie, eerder in dit rapport lezen we: "De belangrijkste nieuwe technologieën voor de politie zijn artificial intelligence, data science of big data en quantum technologie. Het gaat razendsnel. Wendbaarheid is cruciaal. Willen we als politie onze rol kunnen pakken in Society 5.0, dan moeten we de snelheid van technologische veranderingen kunnen bijbenen. Of beter nog: proactief aan het roer staan."

Uitzoomend vanuit bovenstaande casus kunnen we ons afvragen: Hoe zorgen veiligheidsorganisaties ervoor dat Nederland veilig blijft in de steeds vernieuwende context? Welke vermogens, of wel capabilities zijn nodig om wendbaar en flexibel de samenleving veiliger te maken? Kun je deze gerichte behoefte naar specifieke capabilities leidend laten zijn voor innovatie? Technologie en innovatie wordt vaak gezien als een relevante oplossing voor een probleem, maar op welke manier? Het voorbeeld van de Apple Store laat zien dat technologie (de politierobots) bij kan dragen, maar dat in dit geval menselijk handelen (een adequate respons van de DSI) essentieel was voor het vermogen om slagvaardig te kunnen optreden. Het inzetten van technologie en innovatie alleen is dus niet voldoende, het gaat er om dat technologie je in staat stelt je primaire taak slagvaardig en doelbewust uit te voeren in de context; "ben je instaat om innovatieve technologie en wetenschappelijke inzichten te vertalen naar de realisatie van nieuwe werkende concepten waarmee de wendbaarheid van de politie wordt vergroot", aldus Wim-Pieter Huijsman, gedelegeerd portefeuillehouder Innovatie bij de politie.

Innoveren als gestructureerd proces om Nederland veiliger maken

Veel organisaties hebben met succes een innovatiemotor ontwikkeld om nieuwe ideeën te genereren en uit te broeden, van innovatiecentra tot complete innovatie-ecosystemen met diverse organisaties en het bedrijfsleven. Het succesvol implementeren en opschalen van de ontwikkelde innovaties blijft echter nog steeds een uitdaging en belemmert daarmee het verhogen van de wendbaarheid. Wanneer we kijken naar de toepassing van AI heeft slechts 13% van de organisaties in verschillende sectoren[2] AI-gebruiksscenario's met succes binnen productie geïmplementeerd waarmee opschaling in productie mogelijk werd. In het hier aangehaalde eerdere onderzoek van het Capgemini Research Institute wordt beschreven dat de inspanningen tot opschalen worden ondermijnd door een groot aantal problemen, variërend van een te grote afhankelijkheid van technologie tot een gebrek aan focus op wat de operatie/gebruikers eigenlijk willen.

In gesprek met Olof Schuring, Programmamanager Innovatie en adviseur binnen het Ministerie van Justitie en Veiligheid, over effectieve innovatie maakt hij duidelijk dat de afdeling 'X' van het ministerie meer de nadruk legt op het proces van 'innoveren' en niet op de (technologische) innovatie als uitkomst. Een van de belangrijkste aspecten van duurzame innovatie is een innovatie cultuur. "De cultuur van de organisatie moet creativiteit stimuleren en innovatie ondersteunen als een geplande en gemanagede activiteit. Innovatie zal daarmee een kernfunctie van de organisatie worden en innoveren op alle niveaus en met meer impact en effect mogelijk maken".

Daarnaast benadrukt Olof het belang van design principes. "Het is de uitdaging om tot de kern van het probleem te komen en niet de technologie te laten leiden. Innoveren is er om problemen op te lossen, niet om technologie te pushen. Als je in het innovatieproces tot conclusie komt dat je zonder technologie het probleem oplost, dan is er ook sprake van een succesvolle innovatie." Daarom begeleiden binnen het Ministerie van Justitie en Veiligheid mensen met een 'design achtergrond' innovatie in Justitie en Veiligheid organisaties. Uit onderzoek van het Capgemini Research intituut van een aantal jaar geleden in 'What's the Big Idea? Why most innovations fail to scale and what to do about it'[3], blijkt dat naast een innovatiecultuur, de juiste schaalgrootte voor innovatie, het behandelen van innovatie als een specifieke en unieke discipline en de juiste governance die stuurt op deze elementen ingrediënten zijn organisaties om innovaties op schaal bereiken.

Capability gedreven innoveren als verbinder tussen technologie en organisatiebehoefte

Het op de juiste manier inzetten van een robot en gebruik maken van open data of sensoren in de openbare ruimte; wat helpt om bijvoorbeeld een politietaak uit te voeren? Effectief kunnen innoveren

is een belangrijke voorwaarde om met innovatieve manieren van werken en nieuwe technologie een significante bijdrage te leveren aan het veilig houden van Nederland (zonder daar garanties voor te kunnen geven). Succesvol innoveren kijkt naar het oplossen van problemen voor de organisatie en stelt de organisatie in staat om flexibel en wendbaar in te spelen op nieuwe ontwikkelingen in Society 5.0.

Een heldere innovatiestrategie en een goed ingericht innovatielandschap met bijbehorende innovatiecultuur stelt organisaties in staat om zowel wendbaar te reageren op plotselinge ontwikkelingen, als proactief en strategisch hun innovatiebehoeften vast te stellen en te richten. Welke ambities heeft de organisatie, waartoe moet het instaat zijn, welke vermogens zijn daarvoor nodig en welke (innovatieve) functionaliteiten gaan die mogelijk maken?

Er is bijvoorbeeld behoefte aan het vermogen om bij een melding bij de politie z.s.m. een volledig beeld van de situatie te krijgen, zodat de juiste interventie/reactie kan worden uitgevoerd. Hiervoor is minimaal een aantal functionaliteiten nodig zoals: real time inzicht in de situatie, handelingsruimte voor leidinggevenden om de juiste actie in te zetten en de verbinding tussen uitvoerder, meldkamer en leidinggevenden zodat actie kan worden bijgestuurd. Een drone is een technisch hulpmiddel om real time inzicht te krijgen in de situatie, maar ook bijvoorbeeld 'Google glasses'. Een beveiligde smartphone is vervolgens de verbinding tussen agent en meldkamer.

Op deze manier nadenken over specifieke onderwerpen en welke technologie er nodig is om de benodigde vermogens (de capabilities) van een organisatie te realiseren noemen we capability gedreven innoveren. Ook binnen de politie wordt innoveren steeds vaker gestuurd op basis van deze benodigde 'vermogens', aldus Wim-Pieter Huijsman, "Vanuit onze strategische thema's (e.g. Digitale Transformatie) wordt vastgesteld welke vermogens moeten worden (door) ontwikkeld, om vervolgens te bepalen welke innovatiebehoefte daarbij kan worden vastgesteld; op welke vermogens hebben we innovaties nodig om onze ambitie te realiseren?".

Capability gedreven innoveren legt de verbinding tussen technologie en de (benodigde) capabilities van een organisatie. Het verschuift de focus van technologisch gedreven innoveren naar praktische organisatievermogens; hoe draagt innoveren bij aan het versterken van de 'kerncapabilities' van de organisatie? Innoveren is hierbij geen doel op zich. Het is een middel om de organisatie te versterken en relevant te houden in de continu veranderende context. Wim-Pieter maakt in een gesprek over capability gedreven innoveren duidelijk dat: "Innoveren moet leiden tot vernieuwing van werkconcepten. Als innoveren ons kan helpen om nieuwe, betere, effectievere werkwijzen te ontwikkelen, betekent dit dat we verouderde, minder efficiënte, werkwijzen kunnen aanpassen en/of afschaffen op basis van validatie in de praktijk".

Samen innoveren met onderzoeksinstellingen, onderwijs, bedrijfsleven en andere overheden

Steeds vaker wordt in veiligheidsorganisaties de 'capability' vraag gesteld: Hoe zorgen we ervoor dat innoveren bijdraagt aan het vergroten van de 'vermogens'? Deze wijze van denken vraagt om gecoördineerde sturing op verschillende niveaus in de organisatie. Dit zien we ook binnen de politie. De portefeuille Innovatie heeft als taak om vanuit de 'visie op de innovatiefunctie van de politie' de benodigde organisatie en besturing in te richten. "Dat betekent naast het beleggen van verantwoordelijkheden ook actief innovatiemanagement, dus ook het oormerken van budgetten en het monitoren of aan de vastgestelde innovatiebehoeften wordt voldaan". Aldus Wim-Pieter.

Vanuit de strategische leiding wordt doormiddel van 'een innovatie- en Science & Technology agenda', nut en noodzaak aangegeven zodat het innovatiebudget ook echt bijdraagt aan de gewenste vernieuwing en verbetering van de operationele slagkracht van de organisatie. Een Science & Technology Agenda is cruciaal voor de kennisopbouw in samenwerking met onderzoeksinstellingen, onderwijs, bedrijfsleven en overheden. Gezamenlijk worden onderzoek en experimenten uitgevoerd".

"In een tijd waarin de wereld en technologie voortdurend evolueren, is het van belang om strategische koers te bepalen om deze veranderingen bij te kunnen houden. Ter voorbereiding

op toekomstige taken is het nodig te analyseren, experimenteren en kennis op te bouwen.", benadrukt Sven Hamelink, hoofd Science & Technology van politie. In samenwerking met ondernemers, onderzoekers en andere overheden wordt de relevante kennis opgebouwd. "Onze missie is om de politie voor te bereiden op de kansen en bedreigingen van nieuwe technologie voor zowel de rol, inrichting en taakuitvoering. Werken aan een verandervaardige politie die continu vooruitkijkt en technologie integraal opneemt in nieuwe oplossingen."

Tegelijk ziet de operatie vanuit hun expertise het beste wat direct te verbeteren is door het toepassen van de laatste technologieën en werkconcepten. Capability gedreven innoveren betekent niet dat innoveren top-down wordt opgelegd, in tegendeel. De 'ideatie' kracht en creativiteit vanuit de operatie wordt hiermee juist nóg belangrijker. De operatie heeft namelijk het beste beeld bij de middelen en oplossingen die waarde toevoegen in de operatie en is daarmee zeer geschikt om te werken aan innovatieve ideeën die voor mensen in de operatie het werk beter maakt. Wim-Pieter hierover: "Het is belangrijk dat we collega's die met inventieve ideeën komen om hun werk te verbeteren serieus nemen, dat we kunnen inschatten of en hoe dat idee een bijdrage levert aan de doorontwikkeling van de politie, zodat we ze kunnen helpen zo'n idee uit te werken en op een gedegen manier te toetsen. Dit klinkt heel vanzelfsprekend, maar onderzoek heeft aangetoond dat|in verschillende organisaties veelbelovende innovaties door het uitblijven van aanmoediging en waardering nooit aan de oppervlakte komen. Dat is eeuwig zonde"[4].

Het op basis van capabilities richting geven aan innoveren zorgt ervoor dat de 'ideatie-' en innovatiekracht van de operatie wordt gericht op de meest belangrijke ontwikkelopgaven van de organisatie. Richting geven zorgt ervoor dat de waarde van innovatieve ideeën toeneemt zodat het niet enkel in een specifieke casus probleemoplossend werkt, maar bijdraagt aan de grotere ontwikkeldoelen en 'kerncapabilities' van de organisatie. Capability gedreven innoveren werkt faciliterend en zorgt

voor de link tussen de operatie en het bereiken van de strategische ambities van de organisatie.

Veiligheid door wendbaarheid en innovatie

We willen allemaal een veilige samenleving, maar ook vrijheid en vertrouwen in een leefbare Society 5.0. Dit betekent dat veiligheidsorganisaties wendbaar en flexibel moeten kunnen zijn om hun veranderende taak en rol goed uit te blijven voeren. Daarbij moet ook altijd de ethische vraag gesteld worden en binnen de kaders van de wet worden gehandeld. Veiligheidsorganisaties hebben een voorbeeldfunctie hierin. Essentieel is een goede innovatiefunctie, ingericht als een vermogen waarin de organisatie zowel top down als bottom-up faciliteert. Verandering zal altijd plaatsvinden vanuit de noodzaak om effectiever en efficiënter de juiste bijdrage te leveren aan de door de samenleving gewenste veiligheid. Laten we ervoor zorgen dat innovatie en technologie daarbij als hulpmiddel kunnen worden ingezet.

Onze dank gaat uit naar de mensen die beschikbaar zijn geweest voor het delen van hun inzichten en kritische review: Olof Schurink, Joop van der Born, Sven Hamelink en Wim-Pieter Huisman. Een speciaal dank je wel aan onze collega's Teddy ven Eijk en Guus Kok voor hun inspiratie, review en samenwerking op het onderwerp van Capability Driven Innovation.

Over de auteurs

Roeland de Koning | Director Public Security

Roeland heeft meer dan 20 jaar ervaring in het adviseren van nationale overheden en de Europese Commissie op het gebied van Veiligheid. Afgelopen jaren is hij veelvuldig actief in het Politie domein op het onderwerp van kennis en innovatiemanagement.

roeland.de.koning@capgemini.com
https://www.linkedin.com/in/roeland-de-koning-5536482

Ivo de Boer | Senior Management Consultant Strategic Innovation & Transformation

Ivo is senior managementconsultant Strategische Innovatie & Transformatie (SI&T) binnen frog, Part of Capgemini Invent. Ivo heeft 2,5 jaar ervaring in het bijstaan van managementlagen in zijn of haar transformatie uitdagingen op het gebied van strategie & innovatie binnen de (semi-) publieke en financiële sector.

ivo.de.boer@capgemini.com
https://www.linkedin.com/in/ivowimdeboer/

1. https://www.ad.nl/amsterdam/de-selfie-van-de-apple-store-gijzelnemer-onthulde-dat-de-bom-nep-was-maar-dat-stelde-nog-niet-gerust~a9fe5a5e/213035616/
2. https://prod.ucwe.capgemini.com/wp-content/uploads/2022/08/Conversations_Edition_5_Report_20220921_Web.pdf
3. https://www.capgemini.com/insights/research-library/scaling-innovation/
4. https://www.uu.nl/nieuws/ondergrondse-innovatie-een-niet-te-missen-kans

Interview:

“Heeft het een geheugen? Dan is het fair play”

Digitale data ontsleutelen en AI-modellen ontwikkelen: het is dagelijks werk voor de digitaal forensisch onderzoekers van het NFI. De grenzen van technologie én ethiek bewaken is een interessante uitdaging voor Society 5.0 en het NFI. “Als wetenschapper heb je een ander doel en perspectief dan een beleidsmaker.”

Erwin van Eijk
Divisiehoofd Digitale en Biometrische Sporen
Nederlands Forensisch Instituut (NFI)

Erwin van Eijk is Hoofd divisie Digitale en Biometrische Sporen (DBS) en Chief Data Officer bij het Nederlands Forensisch Instituut (NFI). Hij deed zelf zo’n twintig jaar forensisch onderzoek. Zijn divisie houdt zich bezig met forensisch onderzoek binnen geautomatiseerde systemen, en biometrisch onderzoek zoals vergelijkend vingersporen-, spraak- en beeldonderzoek. Daarmee ondersteunt DBS onderzoek in complexe nationale zaken, maar werkt ook samen met internationale instituten op digitaal gebied.

Van Eijk: “Het gaat bij DBS vooral om analyses en visualisaties voor politie, OM en andere partners in de veiligheidsketen. Digitale sporen zijn te vinden in bijvoorbeeld auto’s, telefoons en computers. We zeggen ook wel: als het een geheugen heeft, dan is het ‘fair play’.”

Toch kan deze taak schuren met de beleidseisen, want hoe ga je om met persoonsgegevens op inbeslaggenomen goederen of middelen? Van Eijk: “Stel, we treffen in die data een kopie paspoort of rijbewijs aan, dan ben je feitelijk persoonsgegevens aan het verwerken volgens de AVG. Maar wij kunnen niet ‘stoppen met verwerken’: je kunt niet dat ene specifieke stuk data uit een kopie halen. Daar wordt het interessant. Ons werk vereist namelijk het de-anonimiseren van data. Ons ultieme doel is te zorgen dat wij data aan een naam of persoon koppelen. Dat was niet direct bedacht toen het beleid werd opgesteld.”

Ethische dilemma’s

Het forensisch laboratorium is zich zeer bewust van de ethische dilemma’s. Van Eijk: “Wij zoeken naar patronen. Om onderzoek te kunnen doen over zaken heen, wil je niet alleen data uit één specifieke zaak toepassen. Je wilt ook voorgaande sporen analyseren, maar dat kan niet anoniem. Als wetenschapper heb je een ander doel en perspectief dan een beleidsmaker. Hoe kunnen we binnen de bestaande wet- en regelgeving optimaal ons werk doen? Dat vind ik een buitengewoon interessante en belangrijke vraag.”

Van Eijk legt uit waardoor de NFI-praktijk afwijkt: “De grote datacollecties die noodgedwongen ontstaan door ons werk zijn atypisch. Het zijn geen relationele databases. We verwerken bijvoorbeeld geen gegevens als het land van herkomst. Toch gaat de huidige wetgeving veelal uit van het relationele model als mentaal model voor gegevensverwerking. Die assumptie heeft invloed op onze onderzoeken. Het bemoeilijkt bijvoorbeeld de uitwisseling tussen internationale databanken maar heeft ook invloed op onderzoek dat we middels Large Language Models (LLM) willen doen.”

AI-modellen moeten data leren herkennen

LLM worden door het NFI vooral getraind voor toekomstige zaken. Het NFI wil die modellen bijvoorbeeld inzetten om: entiteitsextracties uit te voeren op basis

van beschikbare data uit diverse zaken. Van Eijk: “Onze modellen moeten data leren herkennen en herleiden over zaken heen om zo betekenisvolle patronen van criminaliteit te identificeren. Denk aan berichten tussen criminelen over op handen zijnde delicten. Dan wil je weten wie wat zegt en wat dat precies betekent. Daarvoor heb je context nodig. Je kunt een model eigenlijk alleen goed trainen als het exact weet wie wat zegt, en hoe dat te interpreteren. Die data kunnen dan eenvoudigweg niet anoniem zijn.”

Wetgeving en doelbinding moeten daarom beter op elkaar worden afgestemd, meent Van Eijk. “Het is lastig om voor ons type industrie precies te formuleren hoe we moeten omgaan met het synthetiseren van data[1]. We kennen veel ‘geschreven’ data, zoals kranten, Wikipedia, etc., maar criminelen zetten hun onderlinge correspondentie niet in publieke domeinen. Daardoor is er weinig data voorhanden. Door wetgeving en doelbinding breder te maken en af te stemmen, kunnen we voorwaarden stellen waarmee we onze data beter kunnen synthetiseren. Dat betekent bijvoorbeeld dat we strenge classificaties hanteren voor het algoritme dat we inzetten. Het herkennen van gezichten of het koppelen van individuen aan een bepaald gedrag krijgt een hogere classificatie dan bijvoorbeeld het volgen van een blauwe regenjas in een menigte.”

Uitlegbaar bewijs

Voor de aan te voeren bewijslast is het ook cruciaal dat een rechter kan volgen hoe het bewijs tot stand is gekomen, zegt Van Eijk. “We moeten kunnen uitleggen hoe we het algoritme gebruiken. Daardoor kiezen we soms voor het inzetten van een simpeler algoritme omdat beter uitlegbaar is welke route het algoritme heeft gevolgd. Dat kan leiden tot minder hoogwaardig bewijs. Maar als het algoritme niet goed te verifiëren valt, is het bewijs veel minder goed bruikbaar in de rechtszaal.”

Toepassing AI

Artificial Intelligence (AI) wordt door het NFI inmiddels op verschillende manieren toegepast. Van Eijk. “Die blauwe regenjas wil je bijvoorbeeld koppelen aan beelden van CCTV-camera’s. Door AI alleen te laten zoeken op een specifieke donkerblauwe regenjas, is de hoeveelheid data die je moet veiligstellen veel minder. En daarmee ook proportioneler voor de mogelijke inbreuk op de privacy van andere mensen op die beelden. Of denk aan het onderzoek naar kruitsporen. Wij kijken naar AI-modellen om de chemische stoffen uit dit soort sporen te detecteren en te analyseren om zo het type munitie te identificeren en te matchen aan een bepaald wapen en ultimo aan een persoon. AI scheelt veel onderzoekswerk door onze mensen. Die kunnen zich daardoor richten op meer complexe vraagstukken.”

Deze werkwijze kan ook een ander belangrijk vraagstuk oplossen. Van Eijk: “Ook wij zoeken naar goede techneuten. We willen mensen boeien en binden met aantrekkelijk werk. Standaardonderzoek of routinematige activiteiten proberen we daarom te automatiseren. Dat mes snijdt aan twee kanten. Dankzij automatisering kunnen we onze activiteiten opschalen omdat opsporingsdiensten en politie zelf bepaalde taken kunnen uitvoeren. Dat scheelt logistiek, tijd en kosten. Met onze forensische zoekmachine Hansken kan de politie bijvoorbeeld efficiënt zoeken in grote hoeveelheden data van beslaggenomen computers en telefoons. Onze mensen hebben dan weer tijd voor complexe zaken die meer handwerk vereisen: het werk dat wij het meest interessant vinden.”

Digitaal plaats delict

Aan uitdagingen geen gebrek bij het NFI. Van Eijk: “Digitale sporen worden steeds belangrijker om misdrijven te reconstrueren. Daarom zijn we nu bezig een equivalent van een digitale Plaats Delict (PD) te creëren. Aan een gehackte telefoon zie je weinig aan de buitenkant. Als onderzoeker wil je weten wat ermee is gebeurd. Welke scenario’s kunnen erbij horen? Digitaal onderzoek is niet alleen complex maar ook uitermate veranderlijk; software verandert iedere dag. Referentieonderzoek naar sporen in bijvoorbeeld Whatsapp wordt een jaar na dato heel lastig. Daarom willen we digitale sporen direct veiligstellen voor referentieonderzoek. Dat kan niet handmatig met die enorme hoeveelheid data. Dat moet je automatiseren.”

Verstevigen van robuustheidsideaal

Ook voor fysieke sporen zijn data science en AI steeds belangrijker. Van Eijk: “Ook analoge sporen willen we beter kunnen analyseren, sneller en minder biased onderzoeken om zo betere ondersteuning te bieden in de strafrechtketen. Dat verstevigt ons robuustheidsideaal: je wilt kennis en kunde zoveel mogelijk objectiveren en borgen. Het moet uit de ‘analoge geheugens’ van onze experts en opgeslagen worden in een collectief digitaal geheugen. We kunnen pas zeggen of iets wel of niet uitzonderlijk is als we het verifiëren met data. Uitspraken als ‘Ik kan me niet herinneren dat ik zoiets ooit heb gezien’, gaan tot het verleden behoren. Wetenschap is geen mening. We moeten onze uitkomsten staven met data en onze uitspraken kunnen objectiveren. Dat vereist data; data maken onze bewijskracht veel sterker.”

Over het NFI

Het NFI is een internationaal kennis- en expertisecentrum voor forensisch onderzoek. Het instituut heeft bijna veertig verschillende forensische deskundigheidsgebieden onder één dak en houdt zich bezig met onder andere DNA-onderzoek, het verrichten van gerechtelijke secties, het onderzoeken van vezels of het openmaken, uitlezen en ontsleutelen van digitale informatie uit telefoons van verdachten. Met deze onderzoeken, met de overdracht van kennis en door te innoveren levert het NFI een bijdrage aan de opsporing en waarheidsvinding in strafrechtelijke onderzoeken, zowel nationaal als internationaal. Dat doet het NFI op basis van de laatste wetenschappelijke inzichten. De missie van het NFI is dan ook: 'Gericht op waarheid. Geleid door wetenschap. Voor een veiligere samenleving.'

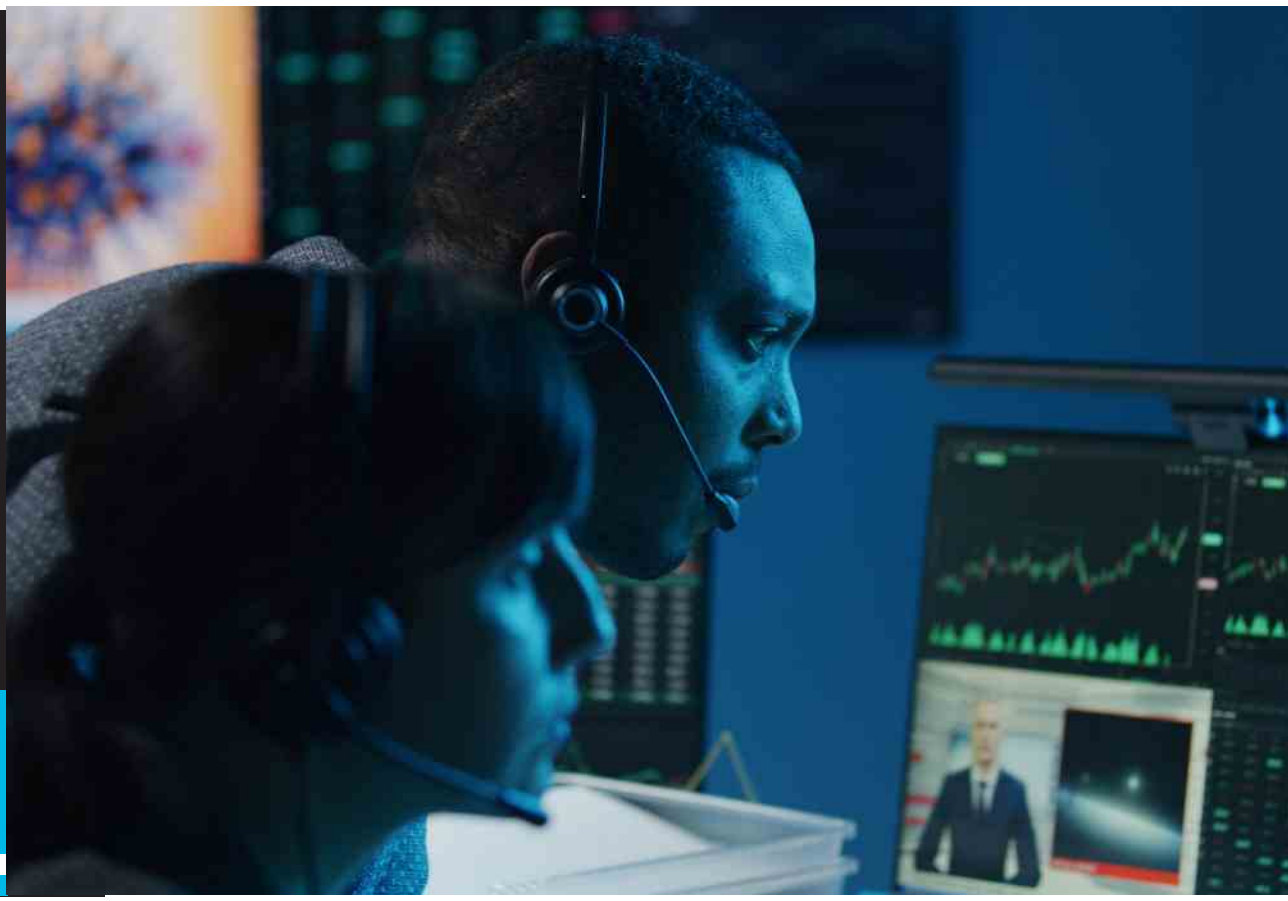
Welke digitale middelen het NFI heeft ontwikkeld

- De hoeveelheid te onderzoeken data en databronnen in strafzaken neemt razendsnel toe. Om de effectiviteit en snelheid van onderzoek te vergroten, heeft het NFI de forensische zoekmachine Hansken ontwikkeld.
- Telefoons zijn vaak beveiligd met toegangscodes, gegevens kunnen (deels) zijn verwijderd of de telefoon zelf kan beschadigd zijn. De Memory Toolkit van het NFI kan het geheugen uitlezen van apparaten zoals mobiele telefoons, satellietnavigatie-apparatuur, auto-elektronica en USB-sticks.
- Ook biedt het NFI overheden en gerechtelijke instanties wereldwijd de Mobile Data Recovery Service aan. Hierbij wordt de geheugenchip uit de telefoon gehaald en de data gekopieerd.
- Forensische big data analyse (FBDA) richt zich op technieken voor intelligente data-analyse om essentiële informatie te halen uit grote hoeveelheden digitale gegevens.
- Digitale afbeeldingen en video's uit mobieltjes worden steeds belangrijker in politieonderzoeken. Maar met welke camera is een foto of video gemaakt? En zijn verschillende foto's met dezelfde camera gemaakt? Het NFI geeft met PRNU Compare Professional software een antwoord hierop.
- Sieve kan 24 uur per dag geautomatiseerd zoeken door (porno)grafisch materiaal. Dat scheelt digitale rechercheurs veel tijd maar ook minder confrontatie met (kinder)pornografisch materiaal.
- DNAxs is software ontwikkeld om veel en complexe DNA-profielen met elkaar te vergelijken. Met de software kan ook meteen de bewijskracht worden berekend.
- De software Defraser kan verwijderde of beschadigde multimediabestanden terugvinden en repareren. Ook complete verwijderde videobestanden en bestanden die deels al zijn overschreven met andere data.
- Vingersporen en handpalmsporen van slechtere kwaliteit of partiële afdrukken werden gezien als onbruikbaar. Dankzij de Wetenschappelijke Onderbouwing Vingersporenindividualisatie (WOVI) zijn ook deze sporen te gebruiken als bewijsmateriaal in de rechtbank. Via de probabilistische benadering wordt gekeken naar de aanwezige karakteristieken en naar hoe vaak ze voorkomen in de populatie. Het NFI gebruikt daarvoor een geanonimiseerde referentiedatabase met vingerafdrukken.

1. Synthetische data simuleren kenmerken van relaties tussen personen en objecten. Daardoor kan de realiteit worden nagebootst zonder dat de persoon of het object geïdentificeerd wordt. Synthetische data kunnen worden gegenereerd door een algoritme of een computersimulatie. Synthetische data worden gebruikt voor privacybescherming en gecontroleerde openbaarmaking. Bron: CBS

Data

05
Data



Generatieve AI in politiewerk

Is het gebruik van generatieve taalmodellen in politiewerk een geschenk of zonde?

Generatieve AI om informatievoorziening binnen politiewerk te versnellen. Hoe kan de politie Generatieve AI op een betrouwbare manier inzetten?

Highlights:

- LLM's: revolutionair in diverse sectoren.
- LLM's: gebruikt door zowel criminelen als politie.
- Risico's LLM's: auteursrecht, desinfo, deepfakes en dataveiligheid.
- Maatregelen tegen LLM-risico's: EU AI Verordening.
- Meer effectief politiewerk en minder kansen voor criminaliteit.

In de afgelopen jaren zijn Large Language Models (LLM's) uitgegroeid tot krachtige AI-modellen met een enorm potentieel om revolutionaire veranderingen aan te brengen in verschillende sectoren. ChatGPT werd na de lancering in 2022 een van de meest besproken onderwerpen van 2023. Vooral omdat dergelijke modellen snel antwoord kunnen geven op een groot scala aan vragen waarbij de teksten niet of nauwelijks te onderscheiden zijn van door mens geschreven teksten. LLM's kunnen specifieke context meenemen en tekst in een desgewenste stijl schrijven; van Shakespeare tot Shakira. Niet alleen in de media was er veel belangstelling voor, ook op Europees niveau, waar de eerste wetgeving rondom AI (de Europese AI Verordening of de AI Act) in ontwikkeling was. Op het laatste moment werden nog artikelen en hoofdstukken toegevoegd met aan dit soort modellen te stellen regels. Generatieve AI-systemen, zoals ChatGPT zijn een specifieke vorm van 'General Purpose AI' (GPAI) en dit was eerder niet expliciet meegenomen in de verordening.

Deze modellen kregen in het veiligheidsdomein veel aandacht door het misbruik wat criminelen hiervan maken. Met behulp van LLM's kunnen criminelen snel en op grote schaal online fraude plegen met gegenereerde content. Daarnaast kan het ook gebruikt worden voor een groot aantal criminele activiteiten om de belangrijkste stappen van een modus operandi te leren. Dit kan variëren van hoe in te breken in een huis, tot terrorisme, cybercriminaliteit en seksueel misbruik bij kinderen[1].

Niet alleen voor criminelen zijn LLM's kansrijk, ook binnen de rechtshandhaving biedt het ongekende mogelijkheden voor het ondersteunen, onderzoeken en opsporen van misdaden. Er zijn enorme capaciteitsproblemen bij de politie die langer aan zullen houden dan gedacht; in de basisteams, bij de recherche, de informatie-afdelingen en bij sommige specialistische diensten[2]. Deze tekorten in capaciteit kunnen ondersteund worden met verschillende systemen die mede een LLM gebruiken:

- Binnenkomende meldingen automatisch labelen en omschrijven naar een concept proces verbaal;
- Verhoortranscripten automatisch samenvatten;
- Digitaal beslag snel doorzoeken en linken;
- Online (sociale) media doorspitten om intelligence te verzamelen;
- Verschillende informatiebronnen (tekst, audio, beeld) koppelen en met behulp van een chatbotassistent inzichten over deze data verschaffen.

Large Language Models kunnen politiewerk op verschillende vlakken versnellen. Ondanks de potentiële voordelen kunnen LLM's echter ook significante risico's met zich meebrengen op het vlak van auteursrechten, desinformatie en dataveiligheid.

Auteursrechten en persoonlijke gegevens

Er zijn veel voorgetrainde LLM's beschikbaar voor het publiek om te gebruiken. LLM's zijn getraind op een enorme hoeveelheid data. Het is echter vaak niet duidelijk wat er precies in deze data zit en hoe deze verkregen zijn. Hierdoor kunnen er persoonlijke gegevens of auteursrechtelijk beschermd materiaal in zitten. Gezien de voorbeeldfunctie van de overheid kunnen dit soort modellen niet zomaar gebruikt worden. Voor het zelf trainen van een dergelijk model is ontzettend veel data en rekenkracht nodig. De Nederlandse overheid heeft niet de beschikking over een dergelijke infrastructuur en de vraag is ook of dat voor alle mogelijke toepassingen wel nodig is.

Het gebruik van voorgetrainde modellen is niet altijd uit den boze voor partijen in het veiligheidsdomein. We zien steeds meer kleine (Europese) AI-bedrijven ontstaan die focus leggen op databeveiliging, transparantie en uitlegbaarheid van AI-modellen; kijk bijvoorbeeld naar het Duitse Aleph Alpha of het Franse Mistral AI[3]. De kwaliteit van de modellen van deze bedrijven doet niet veel onder voor het populaire OpenAI, maar zij spelen wel in op de noodzaak van compliancy en betrouwbaarheid van AI. Bovendien investeert de Nederlandse overheid in de ontwikkeling van GPT-NL; een Nederlands LLM. Ook Europol is na het eerder verkennen van de initiële impact van LLM's op het werk van de politie in het Europol Innovation Lab (EIL) actief op zoek naar manieren om gebruik te maken van LLM-technologie om een 'politie ChatGPT' te bouwen voor rechtshandhaving.

Het verspreiden van desinformatie

LLM's staan bekend om het hebben van hallucinaties: het concept van het genereren van foutieve informatie die wel plausibel lijkt. LLM's genereren, statistisch gezien, het meest voor de hand liggende antwoord op de vraag die het model gesteld wordt. Hoe goed de antwoorden zijn, is afhankelijk van de data waarop het model getraind is. Voor ChatGPT is het onmogelijk te zeggen of de trainingsdata correct en volledig is. Hierdoor kan het model biased zijn en desinformatie verspreiden. Bij het samenvatten van een verhoor kan een LLM een andere conclusie trekken uit de transcriptietekst dan een rechercheur zou doen; wie van de twee heeft gelijk? Wanneer besluiten door agenten of rechercheurs worden genomen op basis van verkeerde informatie, kan dit grote (rechts)gevolgen hebben. Het gebruik van LLM's ter ondersteuning zorgt er echter wel voor dat veel sneller en op grotere schaal informatie wordt verwerkt.

Dataveiligheid

Het zelf doortrainen van LLM's op de vragen die gesteld worden, kan 'lekkage' van trainingsdata voorkomen. Het terugkrijgen van letterlijke passages uit trainingsdata kunnen ongewenst zijn vooral bij (privacy) gevoelige

data zoals processen-verbaal. Dit is te voorkomen door trainingsdata te anonimiseren (ook in deze taak is een LLM erg goed) of alleen data uit de kennisbank te gebruiken waarvoor de gebruiker geautoriseerd is. Trainingsdata lekkage is overigens het belangrijkste argument voor de politie om in geen geval LLM's te gebruiken vanuit online API's, maar zelf een LLM te hosten om compliant te blijven[4]. Wanneer getrainde politiemodellen of data uitlekken kunnen modus operandi, privacygevoelige en vertrouwelijke gegevens op straat komen te liggen.

Risico's beperken en de mogelijkheden maximaliseren

Om de risico's die aan LLM's zijn verbonden te beperken, moeten proactieve maatregelen worden genomen, waarbij gebruik wordt gemaakt van regelgevingskaders, technologische oplossingen en best practices uit de sector.

Europese AI-verordening

De Europese AI Verordening[5] is de allereerste uitgebreide AI-wet ter wereld die vereist dat organisaties binnen de EU zich houden aan de verplichtingen afhankelijk van hun rol en de risicocategorie van het AI-systeem en/of model, zie afbeelding 1.

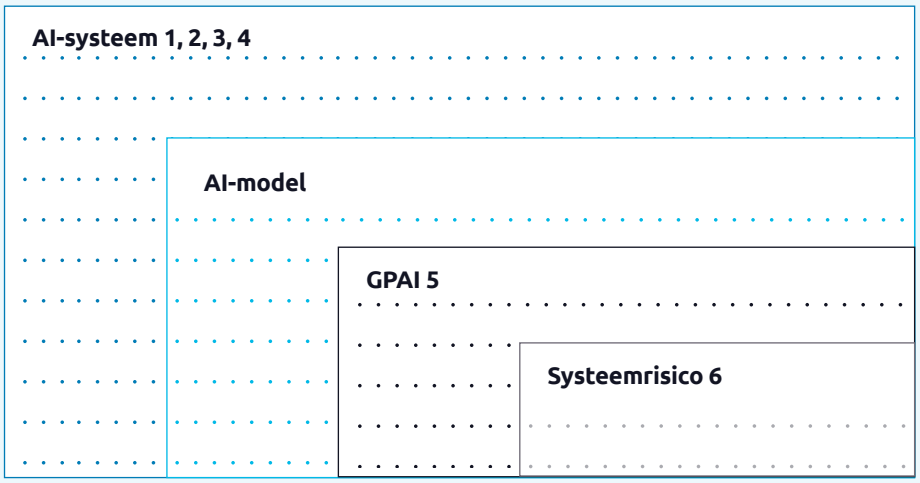
In ons scenario vallen modellen die informatie uit diverse bronnen combineren onder GPAI-systemen met risico's. Afhankelijk van de rol die de organisatie aanneemt in de AI-waardeketen zullen er meer of minder verplichtingen zijn. Wanneer het model wordt aangepast voor eigen systeemgebruik, zal de organisatie zowel de rol van aanbieder als gebruiker aannemen. De volgende eisen zullen dan van toepassing zijn:

- Voor GPAI-modellen gelden de transparantievereisten, waaronder het up-to-date houden van de technische documentatie en het bieden van een samenvatting van de inhoud die wordt gebruikt voor modeltraining, en aan het doen van auteursrechten[6].
- Voor GPAI-modellen met systeemrisico's gelden meer transparantievereisten, waaronder modelevaluaties, documentatie en rapportages over incidenten en corrigerende maatregelen. Ook moet er gezorgd worden voor een passend niveau van cyberbeveiligingsbescherming voor het AI-model en de fysieke infrastructuur van het model[7].

Wanneer de organisatie alleen gebruiker is van de modellen en het niet wordt gebruik in een hoog risico AI-systeem (een GPAI-model is dus niet direct een AI-systeem) zullen er geen verdere verplichtingen zijn onder de AI Verordening. Echter is het waarschijnlijker dat het model wordt aangepast en systeemrisico's heeft vanwege de tekst-naar-tekst modaliteit[8].

Afbeelding 1:

AI-modellen kunnen onderdeel zijn van een AI-systeem. Binnen AI-modellen is er een categorie General Purpose AI-modellen (GPAI) die mogelijk systeemrisico's met zich mee kunnen brengen. Generatieve AI, zoals ChatGPT, is een bijzondere vorm van GPAI.



1, 2, 3, 4 In de AI Verordening worden vier risicocategorieën aangehouden voor AI-systemen:

1. Verboden AI-systemen mogen niet gebruikt of in de markt gezet worden, wanneer dit toch het geval is kunnen er boetes van 35 miljoen euro, of 7% van de totale omzet, opgelegd worden;
2. Hoog risico AI-systemen mogen gebruikt worden, echter is er een hele lijst aan verplichtingen waaraan voldaan moet worden voor aanbieders en gebruikers van deze systemen;
3. Beperkt risico met transparantie vereisten, dit zijn o.a. chatbots en deepfakes;
4. Geen of laag risico AI-systemen zijn systemen die geen invloed hebben op de inhoud, en daarmee op het resultaat, van de besluitvorming. Hier gelden beperkte verplichtingen voor;
5. GPAI-modellen kunnen onderdeel zijn van een AI-systeem. Wanneer er GPAI-modellen aangeboden worden (in AI-systemen) zijn er extra verplichtingen;
6. GPAI-modellen kunnen ook systeemrisico's hebben, wanneer er sprake is van systeemrisico's gelden er bovenop extra verplichtingen.

Non-compliance met de AI-verordening kan leiden tot boetes tot 35 miljoen euro of 7% van de totale jaaromzet (wanneer er verboden AI-systemen worden gebruikt) tot 7,5 miljoen euro of 1,5% van de totale omzet (voor onjuiste informatieverstrekking)[9].

Het voorkomen van bias en desinformatie

Om modelbias te verkleinen kan een model doorgetraind worden met politiedata. Aangezien doortrainen vrij kostbaar is en dit continue gedaan zou moeten worden om het model up-to-date te houden is een Retrieval-Augumented Generation (RAG) systeem een duurzamere oplossing. Met een RAG bereik je het beste van twee werelden: vloeiende gegenereerde tekst door de LLM, gebaseerd op data uit je eigen gegevens waar je zelf controle op houdt[10]. Voor een RAG wordt een kennisbank ingericht waarin het systeem kan zoeken naar antwoorden. Deze kennisbank kan voortdurend bijgewerkt worden, waardoor het systeem altijd up-to-date blijft met de meest recente wetgeving, werkinstructies of nieuwsontwikkelingen die relevant zijn voor het politieonderzoek. Bovendien kan de LLM ook altijd de bronnen vermelden waarop het antwoord gebaseerd is. Dit is voor specifiek politiewerk, wat bijvoorbeeld gebaseerd moet zijn op bewijs van feitelijke gebeurtenissen; uitermate belangrijk.

Daarnaast kan het aannemen van een strategie waarbij kleinere, meer gespecialiseerde modellen worden gebruikt, de risico's van LLM's helpen beperken en kunnen deze modellen buiten de GPAI-categorie vallen[11].

Ook het implementeren van robuuste cyberbeveiligingsmaatregelen, zoals encryptie, toegangscontroles en veilige gegevensopslag, helpt om lekken van modellen en gegevens te voorkomen, waardoor gevoelige informatie wordt beschermd tegen ongeoorloofde toegang.

---

1. Europol (2023). ChatGPT - The impact of Large Language Models on Law Enforcement, a Tech Watch Flash Report van the Europol Innovation Lab. Publications Office of the European Union, Luxembourg.
2. Andringa, R. (2023, November 19). Tekorten bij politie houden nog Jaren Langer aan Dan Gedacht. NOS.nl - Nieuws, Sport en Evenementen. https://nos.nl/artikel/2498459-tekorten-bij-politie-houden-nog-jaren-langer-aan-dan-gedacht
3. In Mistral AI heeft Microsoft onlangs wel een minderheidsbelang genomen en stelt haar Azure AI platform beschikbaar.
4. Het gebruik van een LLM API heeft het afgelopen jaar tot een lek van zeer gevoelige data geleid bij Samsung. Ray, S. (2024, February 20). Samsung bans chatgpt among employees after sensitive code leak. Forbes. https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/?sh=6b2250b76078
5. De wet op de artificiële intelligentie (P9_TA(2024)0138), 13 maart, 2024, aangepaste versie van het Europees Parlement
6. De wet op de artificiële intelligentie (P9_TA(2024)0138), 13 maart, 2024, art. 53
7. De wet op de artificiële intelligentie (P9_TA(2024)0138), 13 maart, 2024, art. 55
8. De wet op de artificiële intelligentie (P9_TA(2024)0138), 13 maart, 2024, Annex XIII
9. Echter bepaalt elke lidstaat de regels betreffende de vraag in hoeverre administratieve geldboeten kunnen worden opgelegd aan de gevestigde overheidsinstanties of -organen
10. Merritt, R. (2023, November 15). What is retrieval-augmented generation aka rag?. NVIDIA. https://blogs.nvidia.com/blog/what-is-retrieval-augmented-generation/
11. Een AI-model voor algemene doeleinden wordt geacht capaciteiten met een grote impact te hebben wanneer de cumulatieve hoeveelheid berekeningen die wordt gebruikt om het model te trainen, gemeten in FLOP's, groter is dan 10^25 (AI Act, Marart. 51, lid 2). Deze drempelwaarde legt momenteel meest geavanceerde GPAI-modellen vast, namelijk OpenAI's GPT-4. Artificial Intelligence – Questions and Answers*. European Commission - European Commission. (2023, December 12). https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683

Opbouwen van kennis

De Nederlandse politie streeft ernaar om de werking van LLM's goed te begrijpen en zo waar mogelijk toe te passen. Tijdens experimenten wordt er kennis verzameld hoe een LLM tot bepaalde resultaten komt en wat de (on)mogelijkheden zijn. Het gebruik vraagt om de nodige zorgvuldigheid, en het gegeven dat een LLM iets zou kunnen, betekent nog niet direct dat dit dan ook gebruikt zou moeten worden. In een gecontroleerde proeftuin wordt kennis opgebouwd over de werking en de impact van deze technologie op het politiewerk. Hierbij wordt ook gekeken naar de impact op de samenleving en hoe andere publieke en private partijen ermee omgaan.

Hoewel LLM's een enorm potentieel hebben voor het veiligheidsdomein, brengen ze ook risico's met zich mee die aangepakt moeten worden door een combinatie van regelgevend toezicht, technologische keuzes en ethische overwegingen. Daarnaast is het zeer belangrijk om voldoende kennis op te bouwen over de werking van LLM's en keuzes te maken waarvoor deze wel en niet zijn in te zetten in politiewerk. Door scherp te zijn op genoemde risico's bij de inzet van generatieve taalmodellen (en politiemensen hier ook in op te leiden) kunnen dergelijke modellen een waar geschenk zijn voor de politie. Duizenden binnenkomende meldingen kunnen door LLM's in een mum van tijd worden gecategoriseerd, samengevat en aan elkaar worden gelinkt wat politiemensen uren aan repetitief werk zou kosten. Met de huidige personeelstekorten en toenemende meldingen op gebied van cybercriminaliteit kan dit de politie enorm helpen om de werkdruk te verlagen en capaciteit vrij te spelen. Minder repetitief werk betekent meer tijd voor effectief politiewerk en minder kansen voor criminaliteit. Dat is AI voor een veiliger Nederland.

Over de auteurs

Shelly van Erp | Data Science & AI Consultant bij Capgemini Insights & Data

Shelly is gespecialiseerd in het toepassen van generative AI en natural language processing binnen de publieke sector

shelly.van.erp@capgemini.com
https://www.linedin.com/in/shellyvanerp/

Marije Merckens | Managing Consultant AI Strategy bij Capgemini Invent

Als Managing Consultant in AI Strategy is Marije gespecialiseerd in het leiden en opzetten van organisatiebrede initiatieven voor verantwoorde ontwikkeling en gebruik van algoritmes en AI.

marije.merckens@capgemini.com
https://www.linkedin.com/in/marije-merckens/

Oscar Wijsman | Sr. Business Expert Intelligence, Digitalisering

Oscar Wijsman werkt als sr. Business Expert Intelligence & Digitalisering binnen de Nederlandse politie en is de internationale AI & Data Science Lead.

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

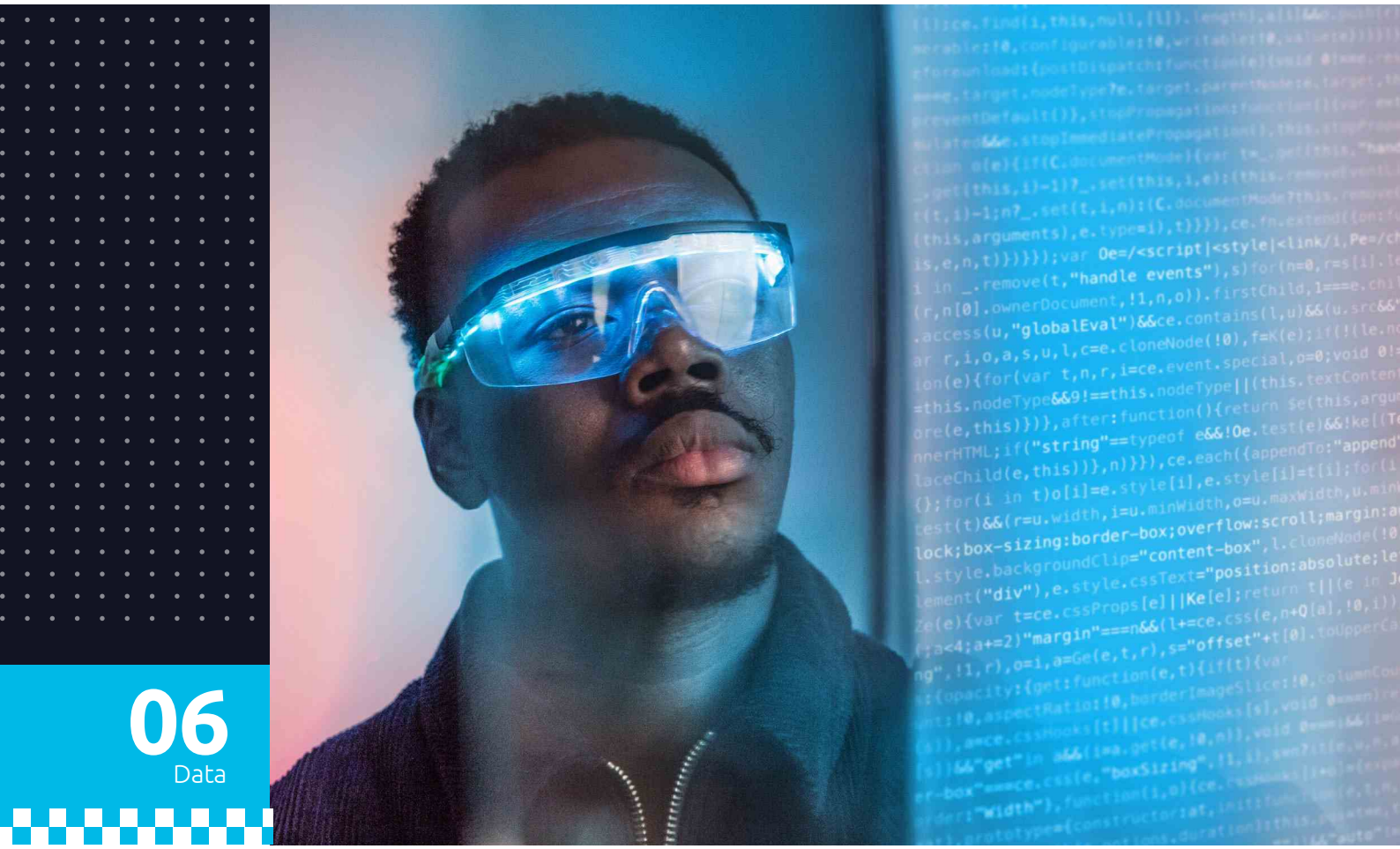
Veiligheid vergroten: cruciale rol data governance in waardecreatie AI

Wat zijn factoren voor een succesvolle data governance implementatie?

AI heeft gigantische potentie maar brengt ook risico's met zich mee. Data governance is cruciaal om de waarde ervan te maximaliseren en risico's te beperken.

Highlights:

- Waardecreatie door AI is afhankelijk van data.
- Data governance is een cruciale randvoorwaarde voor het krijgen van grip op data.
- Binnen de veiligheidssector krijgt data governance steeds meer aandacht.
- Met een succesvolle data governance implementatie kan de waarde van AI worden gemaximaliseerd en risico's worden beperkt.



06
Data

Waarde en risico's van AI

Steeds meer mensen en organisaties maken gebruik van Artificiële Intelligentie (AI). Zo ook in de veiligheidssector. Denk bijvoorbeeld aan de Robot en Autonome Systemen-eenheid van de Koninklijke Landmacht[1], die onbemande voertuigen gebruikt voor het transport van zware materialen. Of aan toepassingen die de Politie gebruikt om vluchtroutes te voorspellen en zo op een slimme manier criminelen te vangen of om relevante informatie voor opsporingsonderzoeken te vinden. AI kan hier helpen bij het herkennen van patronen in grote hoeveelheden data[2]. Verder neemt generatieve AI momenteel een enorme vlucht en experimenteren organisaties met dergelijke toepassingen. Zulke (generatieve) AI-toepassingen hebben de potentie veel waarde te leveren en de maatschappij veiliger te maken. Tegelijkertijd brengen ze ook risico's met zich mee, zoals bij het toeslagenschandaal gebeurde, waarbij burgers onterecht verdacht werden van fraude met toeslagen. Met name in de veiligheidssector kan een foutief besluit, gebaseerd op een AI-toepassing, enorme impact hebben en zelfs een kwestie van leven en dood zijn. Daarmee wordt verantwoording afleggen over het gebruik van AI dus ook steeds belangrijker. Zo werd in 2023 tijdens de REAIM-summit (Responsible AI in the Military Domain) ingestemd met een gezamenlijke "call to action" over de verantwoorde ontwikkeling, toepassing en het gebruik van AI in het militaire domein[3].

Succes afhankelijk van data governance

De maximalisatie van de waarde en minimalisatie van de risico's van AI is afhankelijk van data, die als input dient voor de AI-modellen. Om ervoor te zorgen dat data geschikt is als input en (o.a.) beschikbaar, betrouwbaar, volledig en begrijpelijk is, moet een organisatie een aantal zaken op orde hebben. Voor de hand liggende voorbeelden zijn de databases waarin data toegankelijk is opgeslagen en waar adequaat opgeleide mensen deze data kunnen verwerken. Een minder voor de hand liggende en soms onbegrepen maar cruciale randvoorwaarde die binnen de veiligheidssector steeds meer aandacht krijgt is data governance, wat we definiëren als de formalisering van rollen en verantwoordelijkheden over data. Dit artikel schetst een aantal factoren voor een succesvolle implementatie van data governance als randvoorwaarde om de waarde die door AI gecreëerd wordt te maximaliseren, bijbehorende risico's in te perken en verantwoording af te kunnen leggen over het gebruik ervan.

Wat is data governance?

Data governance wordt hierboven gedefinieerd als de formalisering van rollen en verantwoordelijkheden over data om er zo voor te zorgen dat de data in de organisatie de aandacht krijgt die het verdient. Data eigenaren en data stewards zijn de rollen in de organisatie die (eind)verantwoordelijk zijn voor een set aan data, bijvoorbeeld personeelsdata, materiële data of data uit een wapensysteem.

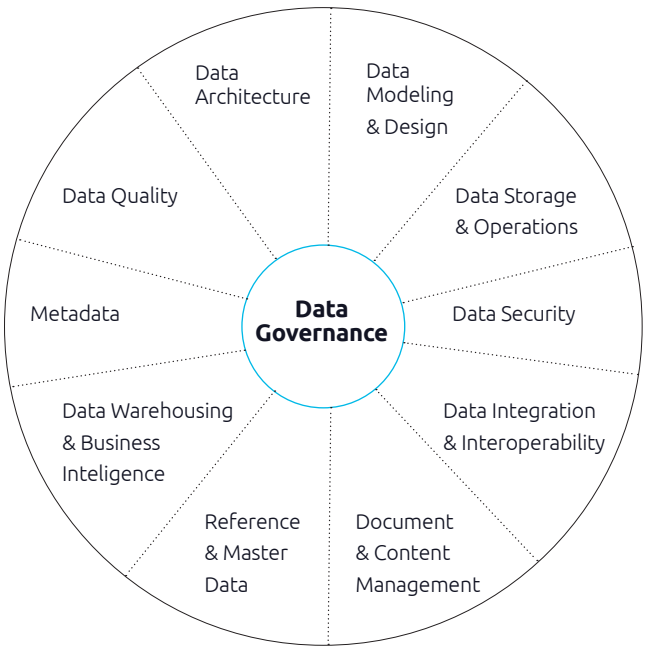
Data governance en datamanagement

Een veelgebruikt framework voor de implementatie van data governance is DAMA's datamanagementwiel (zie afbeelding 1)[4]. In dit wiel wordt data governance gezien als besturende as met rollen en verantwoordelijkheden. De tien spaken van het wiel representeren de datamanagementaspecten. Waar data governance gaat over verantwoordelijkheden, gaat datamanagement over het daadwerkelijk verwerken (verzamelen, organiseren, rubriceren, opslaan) van data. Herkenbare voorbeelden van datamanagementaspecten zijn datakwaliteit, metadata en data security. Door data eigenaren en data stewards aandacht te laten besteden aan de datamanagementaspecten wordt de bruikbaarheid van data en de grip erop stapsgewijs verhoogd.

Toenemende aandacht voor data governance

Steeds meer organisaties in de veiligheidssector besteden in hun datastrategie aandacht aan data governance. Zo is één van de vier doelstellingen van de Defensiestrategie data science & AI 2023-2027 organisatiebrede data governance[5], noemt de Politie in haar Datastrategie Politie 2022-2025 data stewardship als een randvoorwaarde om een datagedreven organisatie te worden[6] en wordt data governance als belangrijke uitdaging gezien in de Interbestuurlijke Datastrategie Nederland[7]. Daarbij geldt vanaf eind september 2023 in de EU de Data Governance Act[8], die Europese richtlijnen geeft op het gebied van data governance.

Afbeelding 1: DAMA's datamanagementwiel



Data governance maximaliseert de waarde van AI

De aandacht voor data governance is terecht omdat helder belegde verantwoordelijkheden duidelijkheid scheppen voor de organisatie wie ervan is en een eerste belangrijke stap vormen richting beschikbare, betrouwbare, volledige en begrijpbare data. Het beleggen van verantwoordelijkheid over data bij rollen als data eigenaar en data steward kan namelijk zorgen voor efficiënte en verantwoorde datadeling, inzicht hierin (data lineage) en duidelijkheid over de betekenis van data (metadata). Verder is het een opmaat voor de verbetering van datakwaliteit en een gecontroleerde toegangscontrole tot data. Het op deze manier grip krijgen op data zorgt ervoor dat een AI-model gevoed kan worden met data die de waarheid zo goed mogelijk weergeeft en waarvan men ook begrijpt wat het betekent. Andersom geredeneerd, gebeurt dit niet, dan vormt mogelijk foutieve data de input van een AI-model, wat kan leiden tot ongewenste situaties. Voorbeelden hiervan zijn het door de Politie ingrijpen in een conflict op basis van een foutief escalatiesignaal of het bij de Luchtmacht inplannen van een vlieger die onvoldoende getraind is in een bepaalde vaardigheid die benodigd is voor een missie. Ondanks dat de AI-modellen die reageren op het escalatiesignaal en de trainingsgereedheid op zichzelf uitstekend werken, wordt er géén waarde gecreëerd. Integendeel, de burger en de vlieger lopen juist enorm risico. Verder gaat grip op data ervoor zorgen dat de verantwoording over het gebruik van AI mogelijk wordt. Rede genoeg om data governance op waarde te schatten en te implementeren en zo een cruciale stap te zetten naar waardemaximalisatie en risicominimalisatie van AI.

Succesfactoren van een data governance implementatie

1. **Start met de belangrijkste domeinen**
   Data governance dient een organisatiebreed programma te zijn. Dat betekent echter niet dat overal tegelijkertijd gestart hoeft te worden. Kies een domein wat strategische aandacht heeft en start hier met het beleggen van verantwoordelijkheden bij data eigenaren en data stewards. Is dit gelukt, pak dan door met de rest van de organisatie. Deze agile aanpak zorgt voor lerend vermogen. Daarbij kunnen succesverhalen gebruikt worden om anderen te enthousiasmeren en draagvlak te creëren.

2. **Gebruik datamanagement use cases om waarde te creëren**
   Zoals beschreven, gaat datamanagement over de daadwerkelijke verwerking van data. Een onderdeel van datamanagement waar veel mensen direct beeld bij hebben, is datakwaliteit. Het in samenwerking met data eigenaren en data stewards bepalen van normen, meten van datakwaliteit en het vervolgens verbeteren van de datakwaliteit kan een eerste use case zijn om de waarde van data governance te bewijzen. In de eerdergenoemde voorbeelden heeft een hogere datakwaliteit direct positieve invloed op burger, agent en militair. Het vermarkten van dergelijke successen zal zorgen voor realisatie dat data governance belangrijk is en bij zal dragen aan het maximaliseren van de waarde die de organisatie haalt uit haar AI-toepassingen.

3. **Maak het tastbaar en herkenbaar**
   Data governance moet duidelijkheid scheppen over dataverantwoordelijkheid binnen de organisatie als eerste cruciale stap richting beschikbare, betrouwbare, volledige en begrijpbare data. Data governance en de introductie van nieuwe rollen en verantwoordelijkheden kan als vaag gepercipieerd worden en de toegevoegde waarde is daardoor mogelijk niet voor iedereen direct duidelijk. Gebruik daarom herkenbare voorbeelden van uitdagingen die je probeert op te lossen, maak een data governance organogram met namen en foto's en communiceer periodiek over de voortgang van het programma.

4. **Werk aan databewustzijn**
   Bijna iedereen in bijna elke organisatie werkt met data. Dat kan bijvoorbeeld in de vorm van het invoeren van data (een agent die een rapport opstelt na een aanhouding) of als gebruiker van informatie (een commandant die handelt op basis van een dashboard met informatie). Bewustwording dat iedereen een rol heeft in de keten van dataverwerking tot aan waardecreatie middels AI is belangrijk; onzorgvuldigheid in het begin van de keten kan immers invloed hebben op (geautomatiseerde) besluiten die genomen worden aan het einde van de keten. Vergroot het databewustzijn van de gehele organisatie door het aanbieden van opleidingsmogelijkheden en gebruik voorbeelden die de ontvanger herkent. Kies daarvoor een aanpak die van domein tot domein kan verschillen om de ontvanger zo veel mogelijk aan te spreken.

5. **Weeg een centrale en een decentrale aanpak tegen elkaar af**
   Het binnen verschillende domeinen benoemen van data eigenaren en data stewards is een voorbeeld van een decentrale data governance aanpak. Dit heeft als voordeel dat de mensen die daadwerkelijk met de data werken en belang hebben bij waardemaximalisatie door AI verantwoordelijk zijn voor de data. Een uitdaging hierbij is dat kennis en ervaring over de invulling van data governance rollen versplintert. Zorg daarom (zeker in de opstartfase) voor een centraal team die de data governance-rollen ondersteunt in hun werkzaamheden.

6. **Kies voor top-down én bottom-up**
   Een combinatie van een top-down en bottom-up aanpak kan helpen om data governance consistent en organisatiebreed in te richten én de uitdagingen van de werkvloer op te lossen. Zorg voor draagvlak op het hoogste niveau om zo de rest van de organisatie mee te krijgen in de organisatiebrede richtlijnen. Zorg tegelijkertijd voor connectie met de werkvloer om de specifieke uitdagingen per domein op te lossen. Gebruik continu de lessons learned om de top-down aanpak te verfijnen.

1. https://magazines.defensie.nl/defensiekrant/2023/06/02_artificial-intelligence_06
2. https://www.digitaleoverheid.nl/achtergrondartikelen/artifical-intelligence-maakt-politiewerk-makkelijker-en-moeilijker/
3. https://www.defensie.nl/actueel/nieuws/2023/02/16/call-to-action-verantwoord-gebruik-ai-in-het-militaire-domein
4. https://www.dama.org/cpages/body-of-knowledge
5. https://open.overheid.nl/documenten/d49f42ca-181b-4e2f-9986-b412de40f2f5/file
6. https://www.politie.nl/binaries/content/assets/politie/wet-open-overheid/00-landelijk/it-systeem-politie/09---2022-10-19-datastrategie-politie-v1.0_geredigeerd.pdf
7. https://open.overheid.nl/documenten/ronl-bf2acf54-ad5f-4f32-afe2-0904a1d8e700/pdf
8. https://www.rijksoverheid.nl/actueel/nieuws/2023/09/28/data-governance-act-van-kracht-om-data-betrouwbaar-en-makkelijk-te-delen

Conclusie

AI heeft de potentie veel waarde voor de veiligheidssector te genereren. Helaas zijn er ook legio voorbeelden waarin dergelijke toepassingen juist tot schade leiden. Om de waarde te maximaliseren, risico's in te perken en verantwoording over het gebruik ervan af te kunnen leggen, is het van belang dat organisaties grip hebben op data die als input dient voor AI-modellen. Dat wil zeggen dat data o.a. beschikbaar, betrouwbaar, volledig en begrijpbaar moet zijn. Naast allerlei technische zaken vormt data governance een belangrijke randvoorwaarde in de realisatie hiervan. Data governance krijgt steeds meer aandacht binnen de veiligheidssector maar tegelijkertijd weten veel organisaties nog niet exact hoe hier invulling aan te geven. De zes gepresenteerde succesfactoren vormen een handvat om data governance in te richten en een belangrijke stap te zetten naar waardemaximalisatie door middel van AI om zo de maatschappij veiliger te maken.

Over de auteur

Jeroen Jeschke | Managing Consultant
Insights & Data

Jeroen is werkzaam bij Insights & Data. Hij is een expert op het gebied van datagedreven werken en werkt momenteel aan een data governance implementatie binnen de Koninklijke Luchtmacht.

jeroen.jeschke@capgemini.com
https://www.linkedin.com/in/jeroenjeschke/

HR-data binnen de Koninklijke Landmacht: geen besluiten meer op basis van ‘onderbuikgevoel’

Hoe ziet de doorontwikkeling van het gebruik van Human Resource data binnen de Koninklijke Landmacht eruit?

Highlights:

- Het gebruik van HR-data draagt zorg voor een completer beeld van de situatie.
- HR-adviseur is van meerwaarde voor interpretatie en communicatie van inzichten.
- Aandacht voor meerwaarde en de gebruiker tijdens implementatie.
- Investeren in data mindset en vaardigheden zijn cruciaal om datavolwassen te worden.

07
Data

Zonder data analytics kan de HR van de Koninklijke Landmacht geen goede richting geven aan het vormgeven van een schaalbare krijgsmacht. Juist in deze turbulente tijden bewijst HR Analytics zijn waarde bij de Koninklijke Landmacht. Om waarde vermeerderend te zijn moet HR analytics verder door ontwikkelen, maar hoe?

In de wereld om ons heen zien we onzekere ontwikkelingen in verschillende factoren zoals de internationale veiligheidssituatie, economie en andersoortige vormen van dreiging. Maar ook de meer voorspelbare ontwikkelingen in demografie, technologie en de arbeidsmarkt hebben gevolgen voor het functioneren van de maatschappij en de defensieorganisatie in het bijzonder. Om de toenemende onvoorspelbaarheid tegen te gaan neemt de behoefte aan een flexibel samengestelde, snel op- en afschaalbare en inzetbare krijgsmacht toe. De Defensievisie 2035 (oktober 2020) beschrijft de visie om daar mee om te kunnen gaan. Defensie moet nu en in de toekomst kunnen beschikken over voldoende, geschikt én inzetbaar personeel in snel inzetbare, schaalbare en op informatie gestuurde eenheden. De uitdaging op HR-gebied voor Defensie ligt in het kunnen bijblijven in de ontwikkelingen op de arbeidsmarkt (schaarste, loonontwikkeling) en het implementeren van nieuwe ontwikkelingen (HR Analytics, Strategisch Talentmanagement) binnen de organisatie. Defensie komt vanuit een tijd van bezuinigingen (weinig geld voor innovatie) en krimp (onvoldoende personeel). Dit heeft zijn effect gehad op de mindset binnen de organisatie. Door de ophoging van het defensiebudget, als gevolg van de verschillende ontwikkelingen in de wereld, heeft de groei-mindset meer ruimte gekregen. Door het vormgeven aan flexibele aanstellings- en contractvormen, Strategisch Talentmanagement (STM), beloningsbeleid, Strategische Personeelsplanning (SPP) en een HR-organisatie die dit ondersteunt met IT-middelen wil Defensie inhoudelijk vormgeven aan de Defensievisie 2035. Om hier invulling aan te geven zijn defensiebreed werkgroepen begonnen met het uitwerken van deze plannen. Om zicht te krijgen op wat het personeel doet binnen en buiten de organisatie en hierop te kunnen te anticiperen is er behoefte aan HR-data. De doorontwikkeling van HR Analytics (HRA) is essentieel om inzichten te verkrijgen om op basis van data de besluiten te kunnen nemen.

Besluiten op basis van ‘onderbuikgevoel’

Acht jaar voor het uitkomen van de Defensievisie 2035 deed het Commando Landstrijdkrachten (CLAS) in 2012 de eerste ervaringen op met HR Analytics. Daarvoor konden HR-adviseurs inzichten voor lokale eenheden uit centrale rapportages halen. Zij moesten dan zelf analyses maken en daar inzichten uit afleiden. De rapportages waren op basis van dagwaarden en vaste tabellen. Deze wijze van data verwerken, toepasbaar maken en presenteren was lastig, arbeidsintensief en droeg onvoldoende bij om tot juiste inzichten te komen. Dit had als gevolg dat commandanten regelmatig besluiten namen op basis van ‘onderbuikgevoel’ en niet op basis van ‘cijfers’. Door de toen opgelegde bezuinigingen begon het CLAS met het verwerken van HR-data om inzichten te creëren om te bezien wat de bezuinigingen voor impact hadden op het personeelsbestand. Een HR-team maakte deze inzichten op centraal stafniveau. Ook waren deze inzichten waardevol om categorieën personeel te identificeren en om personeel op een juiste manier te begeleiden richting interne doorstroom of uitstroom.

Groei in volwassenheid op het gebied van HR Data

Doordat in het nieuwe HR-beleid HR Analytics op de kaart stond, kreeg het CLAS de kans om met moderne tooling meer adequatere HR-inzichten te creëren en intern te delen. Voor de uitvoering zocht het CLAS de samenwerking met het Commando Luchtstrijdkrachten (CLSK) omdat zij al eerder kennis en ervaring opgedaan hadden met het toepassen van HR Analytics. Als pilot konden beiden HR Analytics door ontwikkelen; dit met steun van de defensiestaf en het Joint IV Command (JIVC). Het CLAS schafte servers aan, huurde specialisten in en kopieerde en paste datamodellen van het CLSK aan. Vervolgens bouwde het CLAS dashboards ter ondersteuning van haar eigen bedrijfsvoering en paste de eigen bedrijfsvoering aan om de nieuwe tooling en werkwijze op een verantwoorde wijze te ontsluiten naar de eindgebruikers. Dit alles stelde het CLAS in staat om met dashboarding inzichten te geven op basis van data aan commandanten, HR-adviseurs en

kenniswerkers. Trendlijnen, getallen en inzichten op het gebied van instroom en uitstroom, en ziekteverzuim zijn op lokaal niveau bij eenheden beschikbaar. Dit stelt een commandant en adviseur op decentraal niveau in staat om in gesprek te gaan over het personeelsplan voor de eenheid. Dit leidt tot besluiten op basis van 'cijfers' in plaats van 'onderbuikgevoel'.

Door trendlijnen, getallen en inzichten aan te bieden via dashboarding is team HR Analytics onder andere in staat te beschrijven wat o.a. de instroom, uitstroom en ziekteverzuim doet voor eenheden in een bepaalde periode. Beschrijvende analyse is het eerste volwassenheidsniveau binnen HR Analytics. Het is vanuit beschrijvende analyse een eerste stap naar het tweede volwassenheidsniveau: diagnostische analyse (waarom is het gebeurd). Vanuit een dashboard iets signaleren vraagt van HR-adviseurs om zich de vraag te stellen: wat zie ik en wat betekent dit voor de organisatie en haar medewerkers? Het proces van het doorlopen van de 8 stappen van HR Analytics[1] met een commandant leidt ertoe dat van een signalering, een businessvraag komt en op basis van data een advies vanuit de HR Adviseur: van signalering (dashboard of onderbuik) tot advies, interventie of zelfs besluit. Het gebruik van HR-data draagt zorg voor een completer beeld van de situatie en voegt daardoor waarde toe. Daar is de HR-adviseur van meerwaarde voor de interpretatie en communicatie van deze inzichten.

Op de korte termijn gaat CLAS door met het ontwikkelen van nieuwe dashboards. Specifiek dashboards op het gebied van personele gereedheid en exploitatie van personeelsbudgetten. Het dashboard personele gereedheid biedt het inzicht aan commandanten wat de personele gereedheidsgraad is van hun personeel. Om gereed te zijn voor operationele taken dienen militairen te voldoen aan een aantal zaken waaronder het afleggen van een conditieproef, bij zijn met vaccinaties en tandartsbezoek en het afleggen van militaire basisvaardigheidstesten. Het dashboard biedt ook een mogelijkheid om de 'currency' te bezien van de eenheid in de toekomst. Hierdoor kan een commandant op tijd anticiperen op een verlaging van de personele gereedheidsgraad. Met het toekennen van decentrale budgetten aan commandanten en hier op personeelsgebied op te kunnen plannen zijn een commandant en HR in staat om vooruit te kunnen kijken richting (operationele) opdrachten en met wat voor workforce dit kan worden uitgevoerd. Vacatures die niet door vast militair personeel kunnen worden bemenst kunnen dan middels dit budget alternatief worden ingevuld, bijvoorbeeld door het inzetten van een reservist of het inhuren van extern personeel. Het dashboard biedt inzicht in de financiële ruimte en gevolgen van keuzes. Daarnaast steunt het CLAS een programma vanuit de defensiestaf waarin de kennis en ontwikkeling van HR Analytics uitrolt over de andere defensieonderdelen.

Stappen voor de toekomst van HR Analytics binnen het CLAS is in twee delen uiteen te zetten. Het eerste deel is het zetten van de stap van beschrijvende en diagnostische analyse naar voorspellende analyses. Dit zal het CLAS in staat stellen om flexibeler in te kunnen spelen op de toekomst. Voorspellende datamodellen kunnen het CLAS ondersteunen met het nemen van besluiten op het gebied van personeel en de organisatie. Het andere deel ligt op het gebied van AI. Doordat data niet enkel uit cijfers bestaan, maar ook uit andere gegevens zoals beleidsmatige rapportages en open bronnen, zijn modellen die AI zouden kunnen toepassen van grote waarde in het analyseren van deze data. AI kan de HR-adviseurs in staat stellen om op basis van de uitkomsten betere voorspellingen te doen op het gebied van de personele behoefte van het CLAS en de bewegingen van de arbeidsmarkt.

Om gereed te zijn voor toekomstige ontwikkelingen is het van belang dat een organisatie inzicht heeft in het hier en nu én een vooruitkijk kan maken. HR-data en HR Analytics zijn hierbij van essentieel belang, waarbij de verschuiving van besluiten op basis van 'onderbuik-gevoel' naar data ten goede komt voor de besluitvorming. Hierover zijn de stappen die CLAS heeft ondernomen beschreven om gereed te zijn voor toekomstige ontwikkelingen; iets waar (non-profit) organisaties ook hun voordeel mee kunnen doen, of ook al aan het (door) ontwikkelen zijn.

Lessons learned

Over de ontwikkeling die CLAS op het gebied van HR Analytics heeft doorgemaakt zijn verschillende lessen te leren en te delen.

Leiderschap

HR Analytics binnen CLAS is gegroeid doordat directeur HR de meerwaarde zag van HR Analytics en de bijdrage die het zou kunnen leveren. De directeur vertegenwoordigde het CLAS-belang bij de verschillende stakeholders buiten CLAS en zorgde er voor dat er groen licht kwam voor het door ontwikkelen van HR Analytics en daarbij ook voor de benodigde financiering van essentiële randvoorwaarden (personeel en hard- en software). Gedragenheid vanuit de top voor HR Analytics is voor het CLAS essentieel geweest voor het ingezette traject.

Privacywetgeving

Omdat HR Analytics met persoonsgegevens werkt is het van belang om te voldoen aan de bescherming van deze persoonsgegevens. Dit accreditatietraject is voor CLAS ondersteunt door een specialist die het team begeleidt en helpt bij het opstellen van de Advanced Risktool en de Data Protection Impact Assessment. Door specialisten hiervoor te gebruiken heeft CLAS zich ervan verzekerd dat het accreditatieproces werd versneld en de nauwkeurigheid van dit proces én de tooling geborgd zijn.

Eindgebruiker

Het team HR Analytics CLAS ontwikkelt dashboards en zit diep in de (technische) materie. Tijdens de implementatie merkte het team op dat de eindgebruiker het dashboard niet altijd gebruikt. Door in gesprek te gaan met (een vertegenwoordiging van) de eindgebruiker haalde het team feedback op wat voor sommige eindgebruikers het gebruik van dashboards in de weg staat: performance van het dashboard (te traag), onbekendheid met wat het dashboard kan en vertrouwen op oude rapporten (implementatiestrategie,

1. Al, T. & Doze, I. (2015) HR Analytics. Waarde creëren met datagedreven HR-beleid

verbeteren handboeken), niet competent voelen in het gebruik (training sluit nog onvoldoende aan) en het dashboard biedt niet wat de eindgebruiker nodig heeft (ophalen van de door ontwikkelwens). Bij alle personeelsdiensten is er een ambassadeur die de eindgebruiker vertegenwoordigd. Dit zorgt voor een feedbackloop om producten en dienstverlening goed aan te kunnen sluiten. Hieruit kan worden opgemaakt dat het DevOps ontwikkelen van dergelijke dashboards of applicaties de uiteindelijke werking ten goede komt.

Datamindset

Het werken met data en de integratie in bedrijfsvoering is een belangrijk aandachtspunt voor de implementatie van HR Analytics. Dit begint met de erkenning van de toegevoegde waarde van het werken met data. Het is belangrijk om dit op een betrouwbare manier te doen en te herkennen wanneer data moet worden ingezet bij besluitvorming of advisering. Het beschikbaar stellen van data via dashboards helpt om het gebruik van data toegankelijker te maken en bevordert een groeiende datagerichte mindset. Dit betekent concreet voor ons dat we verder investeren in de eindgebruikers zoals: hoe zij dashboards kunnen interpreteren, hoe vervolgonderzoek uitgevoerd wordt en hoe effecten gemeten worden, want het investeren in de verandering van de datamindset is essentieel voor het succes van de implementatie van HR Analytics.

Conclusie

Om op basis van data weloverwogen besluiten te kunnen nemen, is er een voortdurende behoefte aan (voorspellende) HR-data en aan HR Analytics. Om dit te realiseren, heeft het CLAS, naast commitment en de technische ontwikkelingen voor de verwerking en ontsluiting van data, ook inspanningen op het gebied van verandermanagement nodig gehad om HR Analytics succesvol te maken.

Over de auteurs

Johan de Jong | Senior Business Analist DS

Johan is werkzaam bij Capgemini Domain, Digital Society. Johan is gespecialiseerd in data analyse binnen de Krijgsmacht en richt zich momenteel op de ontwikkeling van een adaptieve applicatie met betrekking tot de data ontsluiting binnen het inlichtingen domein van de Koninklijke Marechaussee

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

Steve Kloosterman | Hoofd HR Analytics

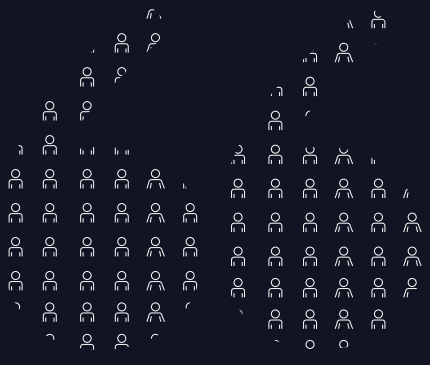
Steve is werkzaam als Hoofd HR Analytics bij de directie HR van de Koninklijke Landmacht. Steve is gespecialiseerd in HR binnen de Koninklijke Landmacht en richt zich op het uitvoering geven aan en het doorontwikkelen van HR Analytics binnen de Koninklijke Landmacht.

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

Natanya Hartgers | Staf Officier Bestandsanalyse

Natanya is werkzaam als Stafofficier Bestandsanalyse binnen het HRA team van de Landmacht. Natanya heeft als hoofdfocusgebied HRA data, Dashboards- en bestandsanalyse binnen de Landmacht en richt haar focus op verschillende aandachtsgebieden die een relatie hebben met de bestandopbouw, binnen het HR domein.

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



Interview:

“Een adaptieve beheerorganisatie is ons antwoord op toekomstige uitdagingen”

Om burgers in nood efficiënt en snel te helpen én hulpdiensten goed te faciliteren in noodsituaties, moeten meldkamers altijd beschikbaar zijn. Nu en ook met oog op de toekomst. Dat betekent een nieuwe inrichting met een flinke digitaliseringsslag. Tegelijkertijd moet de Landelijke Meldkamer Samenwerking (LMS) zich voorbereiden op vergrijzing en de uitdagingen die Society 5.0 met zich meebrengt. “Onze opdracht is complex maar ontzettend mooi.”

De burger centraal stellen om zo snel mogelijk te kunnen functioneren bij noodsituaties; daarom werken politie, brandweer, ambulancezorg en de Koninklijke Marechaussee multidisciplinair samen in een netwerk van meldkamers. De meldkamers zijn operationeel en technisch met elkaar verbonden en werken zoveel mogelijk volgens gestandaardiseerde protocollen. LMS beheert dit netwerk en is een zelfstandig onderdeel binnen de politieorganisatie met een eigen sturing, budget en medewerkers. LMS heeft als taak het beheer van de multidisciplinaire meldkamers. Daarbij ligt er de opdracht om te komen tot een netwerk van tien meldkamers dat aangesloten is op één IV/ICT-infrastructuur. Zo kunnen de verschillende meldkamers elkaars taken overnemen wanneer nodig. LMS is verantwoordelijk voor het leveren van de meldkamervoorzieningen.

Geïntegreerd meldkamersysteem

In 2010 waren er nog meer dan 25 meldkamers, nu zijn dat er twaalf. “En dat moeten er uiteindelijk tien worden in 2025 met één gestandaardiseerde dienstverlening”, legt Melvin Doorn uit. Hij is hoofd functionele meldkamervoorzieningen LMS. “In 2020 hebben we alle bestaande systemen overgenomen van de meldkamers. Dat betekende ook een hoop legacy: we zijn meer dan vierhonderd applicaties, systemen en technieken gaan beheren en hebben onderdelen daarvan gepland geïntegreerd naar centrale platformen.”

Doel van de centralisering is enerzijds het verbeteren van het beheer en de security en anderzijds om te zorgen dat de meldkamercentralisten op elke meldkamerlocatie hun werk uit kunnen voeren en elkaars taak over kunnen nemen: “Voorheen moest iedere meldkamer de techniek en infrastructuur zelf regelen. Hierdoor werkte bijna iedere locatie met verschillende systemen. Dus als een meldkamer in fysieke zin moest uitwijken naar een andere locatie, bijvoorbeeld bij brand of bij storing, moest men met heel andere systemen werken”, zegt Doorn. “LMS heeft deze voor een groot deel geoptimaliseerd en gestandaardiseerd ondergebracht in nieuwe voorzieningen.”

Wanneer een burger belt, komt diens melding terecht op de incidentafdeling van de 112-meldkamer in Driebergen. Daar wordt de situatie beoordeeld en doorgezet naar de meldkamer van het betreffende gebied. Daar wordt de melding genoteerd in het geïntegreerd meldkamer systeem. Doorn: “Bijvoorbeeld: ‘Ongeluk op de A2, beknelling, brand.’ Het systeem heeft de intelligentie om een inzet van hulpdiensten voor te stellen. Bijvoorbeeld: er moet een ambulancevoertuig en een politieauto naar toe. Via razendsnelle verbindingen worden de acties gerealiseerd. De communicatie daarover vindt veelal plaats over C2000. Bijna 600 masten in Nederland realiseren deze communicatie. Hier gaan bijna 4 miljoen gesprekken per jaar overheen.”

Melvin Doorn
Hoofd functionele meldkamer voorzieningen LMS

Invloed van AI

De meldkamer ontwikkelde zich van draaitelefoons en analoge techniek naar het moderne intelligence-center dat het nu is. Naast de continue doorontwikkeling heeft LMS ook te maken met andere veranderingen, waaronder de ontwikkeling van Artificial Intelligence. Dat kan substantiële ondersteuning bieden voor de meldkamers, meent Doorn. Een mooi voorbeeld is het aanpakken van misbruik van het 112-noodnummer. “In 2023 was 42.6% van het binnenkomende telefoonverkeer in Driebergen misbruik of oneigenlijk gebruik van het 112-nummer. Denk aan broekzakbellers of kinderen die voor de grap 112 bellen. 42.6% is gigantisch als je dit afzet tegen het totaal aantal oproepen. Daarom onderzoeken we nu of AI hier iets in kan betekenen. Kan AI bijvoorbeeld aan de voorkant bepalen of het een serieuze melding is of niet? Ook eenvoudigere toepassingen als speech to text of vertaaltoepassingen zouden een uitkomst kunnen bieden. Dan kunnen anderstaligen, bijvoorbeeld toeristen of mensen die de Nederlandse taal niet goed machtig zijn, een melding in hun eigen taal doen. Die melding wordt dan direct vertaald naar het Nederlands zodat de centralist het kan begrijpen.”

Nieuwe technieken leveren kansen en dilemma’s

Gebruik van AI brengt echter ook ethische dilemma’s met zich mee. “Het systeem moet altijd werken: dag en nacht, 24/7. Dus als we besluiten AI in te zetten, moeten we 100% zeker zijn dat het altijd werkt. Neem de broekzakbellers: dat kan een foutieve melding zijn. Maar het kan ook een serieuze melding zijn van iemand die zich om wat voor reden dan ook niet verstaanbaar kan maken. We kunnen niet het risico lopen dat noodmeldingen door AI verkeerd worden beoordeeld.”

Doorn: “We onderzoeken nu ook de toepassing ‘livestream’. Dat is een functionaliteit waarbij de centralist een link naar de telefoon van de melder stuurt en zo live kan meekijken bij het incident.” De technologie is er en de toepassing bevindt zich in de pilotfase. Maar niet alle functionaliteiten zijn al waar ze moeten zijn, zegt Doorn. “Zo zagen we onlangs een grote stijging van 112-meldingen. Wat bleek? Samsung had een functionaliteit gekregen die bij een val automatisch 112 belde. Dan moet je dus in gesprek met Samsung om die nieuwe functionaliteit in Nederland weer uit te zetten vanwege de piekbelasting op ons systeem en de centralisten. Je maakt dan wel van tevoren een afweging: hoe zwaar weegt het voordeel voor de burger of voor de hulpverleners? In dit geval was de belasting op centralisten simpelweg te hoog, terwijl de burger bijna nooit in gevaar was.”

Overwegingen voor toekomstbestendige systemen

Het toekomstbestendig maken van de LMS-systemen brengt verschillende uitdagingen met zich mee. Doorn: “De techniek is vaak relatief eenvoudig. Maar het hele proces daarachter is vaak ingewikkelder. Wat ga je bijvoorbeeld wel en niet opslaan? En welk termijn zit daaraan gekoppeld? Dat verschilt conform wetgeving namelijk per discipline. Bij een ongeluk waarbij beide disciplines ter plaatse zijn, heb je dus al een probleem.” Bij de ‘livestream’-technologie moeten centralisten in het geval van een livestream eerst geselecteerd en getraind worden om met emotionele gevolgen van heftig beeld om te gaan. “Iemand die enkel bureauwerk gewend is, kan behoorlijk schrikken van de beelden van een dodelijk ongeval of ernstige verminkingen.” Daarnaast ziet Doorn de hoeveelheden data fors groeien. “Waar gaan we dat allemaal opslaan? Veel data zijn bovendien niet van ons. Het gaat dan om beeld- en geluidsfragmenten van burgers tijdens een melding of incident. De verwerking van dat soort gegevens brengt de nodige vraagstukken met zich mee. Want als je data verwerkt, moet je ook voldoen aan richtlijnen uit bijvoorbeeld de AVG. Over dit soort consequenties moet je dus aan de voorkant al over nadenken als je je systemen toekomstbestendig wilt maken.”

Toekomst van werk: flexibiliteit

Een uitdaging van een heel andere orde is de behoefte van de meldkamercentralisten om plaats- en tijdonafhankelijk te werken, meent Doorn. “Als je met je laptop een 112-melding thuis kan afhandelen als je bijvoorbeeld een dag thuis wil werken of verkouden bent, dan zou dat mooi zijn. Een grote uidaging op de meldkamers is het werven van nieuw personeel. Zoals bijna overal in de arbeidsmarkt kampen de hulpverleningsdiensten ook met een tekort aan mensen. En ook centralisten willen flexibeler kunnen werken. In andere landen zoals Oosterijk doen ze dit al.”

Maar de veiligheidsregels die gelden voor politie, brandweer, en ambulance, beperken soms die flexibiliteit. “C2000 mag momenteel alleen gebruikt worden op een meldkamerlocatie, in een beveiligde omgeving”, legt Doorn uit. “Daar zitten allerlei normeringen met basisbeveiligingsniveaus aan gekoppeld. Dit zorgt ervoor dat de communicatie veilig is en blijft. Maar het gaat ook om zorgvuldig inzicht willen hebben in de performance van de techniek en waar een gesprek zich in de keten bevindt. Je wilt namelijk niet hebben dat iemand die in nood is op de verkeerde plek terecht komt of helemaal geen verbinding krijgt. De technieken in het systeem zorgen dat alle informatie direct inzichtelijk is en blijft. Buiten het systeem om bellen is dus niet handig en niet te monitoren. Dan missen we cruciale informatie, zaken om rekening mee te houden als we de pilot doen met het plaats- en tijdonafhankelijk kunnen werken.”

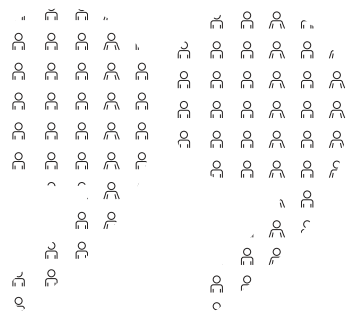
Van een belletje aannemen naar de regie pakken

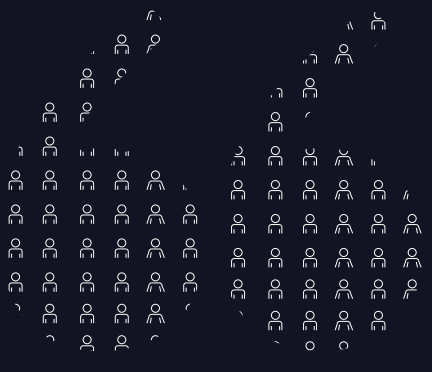
Society 5.0 en specifiek de burger centraal is van groot belang voor de meldkamer van de toekomst. Zo zal de ontwikkeling van slimme devices zoals smartwatches, automatische systemen in auto’s en het gebruik van videosystemen de komende jaren het werk van de meldkamer beïnvloeden. Auto’s kunnen nu bijvoorbeeld zelf al melden als er een ongeluk plaatsvindt op de snelweg en dat specifieke voertuig betrokken is bij het ongeluk. Nieuwe toepassingen zullen daar verder op inspelen. “Dan ontvang je veel meer informatie dan alleen uit een belletje”, aldus Doorn. “Op basis van informatie uit auto’s komt daar straks extra informatie bij over of het een ongeluk betreft. Smartwatches en camera’s sturen straks aanvullende informatie. Zo kunnen we mensen na een melding direct monitoren op fysieke gezondheid en komt al deze data geautomatiseerd op de meldkamer terecht. Ook de rol van de centralist verandert door dit soort technologieën: van iemand die de telefoon opneemt en uitvraag doet, naar een regisseur die omni-channel informatie analyseert en opdrachten geeft. Vanuit de techniek kunnen we de gekste dingen bedenken. Maar de centralisten moeten ook digitaal vaardig genoeg zijn én onze wetgeving moet voldoende afgestemd zijn op dit soort ontwikkelingen zodat we deze technologische mogelijkheden ook kunnen benutten.”

De komende jaren

Wat betreft de ambities heeft LMS een duidelijk doel voor ogen, zegt Doorn. “Over vijf jaar willen we een regieorganisatie zijn met als uitgangspunt een adaptieve beheerorganisatie. Onze kernsystemen moeten 24/7 dienstverlening kunnen leveren en always on zijn. Ik zie dat we over vijf jaar een digitale transformatie hebben doorlopen en naast een solide basis ook bruikbare, wendbare en op de gebruikersbehoefte afgestemde toepassingen leveren. En ik verwacht en hoop op nog meer snelheid en nieuwe ontwikkelingen.”

Doorn vervolgt: “We willen de komende jaren flexibeler kunnen inspelen op de vraag vanuit de verschillende disciplines. Die kennen allemaal een eigen snelheid, hebben een andere ontwikkelingsbehoefte en een eigen dynamiek. Dat vereist organisationele adaptiviteit van de LMS maar de beheerfunctie is even belangrijk. Een groot deel van van onze mensen zijn beheerders en een beheerder wil vaak geen geen enorme verandering maar vooral stabiel beheer. Dat willen wij waarborgen. Het gaat dus om adaptiviteit én stabiliteit in beheer. Dat vraagt van ons dat we beide aspecten meenemen en borgen in onze strategie voor de komende jaren, een soort ambidexteriteit. We werken enerzijds aan een stabiel platform, en anderzijds aan een model waar we de nieuwe technologieën snel en flexibel kunnen inzetten ten gunste van onze collega’s in de hulpverlening en met doel het zo snel en efficient mogelijk kunnen helpen van de burger. Die balans vinden en behouden, is een mooie uitdaging om de komende jaren aan te werken.”





Interview:

“Door nauwkeurige data kunnen we als organisatie kalm blijven in chaos”

Onder druk van toenemende maatschappelijke complexiteit wordt de asielketen in Nederland geconfronteerd met verschillende uitdagingen. De toenemende instroom van asielzoekers, de druk op de woningmarkt en een veranderend politiek klimaat brengen nieuwe vraagstukken met zich mee voor organisaties zoals het Centraal Orgaan opvang asielzoekers (COA). De rol van technologie wordt in deze context steeds belangrijker om de efficiëntie van besluitvorming te vergroten.

Rogér Pellemans

Directeur Opvang & Begeleiding COA (Centraal Orgaan opvang en Asiel)

De asielketen heeft te maken met hoge instroom: in 2024 is er een stijging van ongeveer 40% ten opzichte van 2023 rond dezelfde periode. Rogér Pellemans is als directeur van het COA verantwoordelijk voor de opvang en begeleiding van asielzoekers in Nederland: “Wie in Nederland asiel aanvraagt, heeft recht op opvang. Het COA biedt die opvang.”

Maatschappelijke veranderingen, gekenmerkt door een gevoel van onveiligheid en een verminderd vertrouwen in de overheid, hebben invloed op hoe er vanuit de maatschappij wordt gekeken naar het asielvraagstuk. “Sociale media spelen hierbij een cruciale rol”, legt Pellemans uit. “Framing, blaming en shaming op sociale media hebben een enorme invloed op het realiteitsgehalte van dingen die gebeuren. Ik weiger om daarin mee te gaan en richt me liever op de honderdduizenden mensen in Nederland die elke dag met mij gedreven bezig zijn met dezelfde issues.”

Groeipijnen

De grootste uitdaging is de alsmaar toenemende instroom van asielzoekers. Dit veroorzaakt een capaciteitsprobleem in de asielketen, voornamelijk op het gebied van huisvesting. Maar door de druk op de capaciteit moeten er soms noodmaatregelen worden getroffen, zoals crisisopvang. Pellemans: “Gemeentes hebben moeite met het bieden van adequate opvangmogelijkheden. Dat is niemands schuld, het is gewoon heel erg ingewikkeld om huisvesting te vinden en te bieden. Bovendien is de Immigratie- en Naturalisatiedienst, de IND, niet in staat sneller te procederen. Daardoor zijn wij als COA een soort longstay voor statushouders geworden. Dat vraagt iets van je organisatie, van je structuur en van hoe je met mensen omgaat. Een longstaysituatie doet ook iets met het veiligheidsgevoel van zowel de bewoners als de medewerkers.”

“Daarbij groeien we als organisatie ook hard. In de afgelopen vier jaar zijn er meer dan vierduizend mensen bij gekomen. Dat maakt ons een van de grootste scale-ups van Nederland, met bijbehorende groeipijnen. En anders dan een bedrijf als Zalando of Bol.com kunnen wij niet zeggen: we handelen vandaag tienduizend pakketten en het overige doen we morgen. Als mensen voor de poort staan, dan hebben wij de wettelijke taak om ze direct te voorzien van een veilige slaapplek.”

Digitale transformatie

Accurate cijfers zijn hoognodig om niet alleen de nood van opvang te duiden, maar ook een realistische kijk te geven op de situatie, benadrukt Pellemans: “Iedereen kent de situatie in Ter Apel. Daarmee wordt vaak gedaan alsof dat het COA is. Maar we hebben 311 locaties. Op maximaal tien locaties komen er af en toe incidenten voor. Dat komt vaak voort uit pubers die

vanwege gebrek aan een stabiele locatie dagelijks versleept worden van de ene naar de andere plek. Die gaan zich verzetten. Ik zal niet zeggen dat het gedrag gelegitimeerd is, maar ik begrijp wel waar het vandaan komt. Op de andere 95% van onze locaties is het nagegenoeg altijd rustig. Dankzij dit soort nauwkeurige data kunnen wij als organisatie ook rustig blijven wanneer het algemeen sentiment chaotisch en vijandig wordt. We mogen ons niet verliezen in de hectiek van de dag."

Het COA staat momenteel aan de vooravond van een digitale transformatie. Het fundament voor cloud en cybermogelijkheden is inmiddels gelegd. Technologische toepassingen zouden een helpende hand kunnen bieden bij het ondersteunen van asielzoekers. Pellemans: "Asielzoekers die wij opvangen zijn vaak al digitaal vaardig. De meeste vragen die wij krijgen gaan over de Nederlandse regelingen en manier van doen. Het is dus helemaal geen gek idee om ze via een chatbot toegang tot informatie te geven. Ook kijken we naar de mogelijkheden van digitale processen. Denk aan een soort aanmeldproces waarbij je bij aankomst in Europa geregistreerd wordt en er meteen zicht is op waar er in Europa plaats is. Dus dat je vanaf Lesbos meteen kunt zien of er in Nederland plek is. Dat zou ook voor versnelling van de asielprocedure kunnen zorgen. We zouden ook veel meer kunnen met AI om voorspelalgoritmes te vertalen naar scenario's en die scenario's verder uit te werken zodat we beter voorbereid zijn op een daling of stijging van onze instroom."

Technologisch kijkje in de toekomst

In het toepassen van AI kan nog een behoorlijke slag gemaakt worden door het COA, vindt Pellemans. "Bol.com kan bijvoorbeeld met gebruik van AI seizoenspatronen duiden en daarop seizoensgerichte producten aanbieden. Dat zou voor ons ook kunnen, want ook wij hebben seizoensgebonden patronen. Dat geldt ook voor geopolitieke ontwikkelingen. Er zit een duidelijke relatie tussen brandhaarden die ontstaan en een daaropvolgende stroom van vluchtelingen die onze kant opkomt. Hoe eerder we deze conflicten lokaliseren, hoe eerder we daarop voorbereid kunnen zijn."

Een essentiële stap is de zelfredzaamheid van bewoners vergroten. Pellemans: "We hospitaliseren behoorlijk: vanaf het moment dat mensen binnenkomen, pakken we zoveel mogelijk verantwoordelijkheden over en zetten we een schild van mensen om ze heen. Het verder digitaal vaardig maken van bewoners kan hierbij helpen. Via een app bijvoorbeeld zouden ze zelf meer informatie kunnen vinden over hoe bepaalde processen werken in Nederland. De IND en het COA werken al hard aan een innovatieprogramma om dergelijke zaken mogelijk te maken. Technologie kan deuren openen, de zelfredzaamheid vergroten en verantwoordelijkheid bij de bewoners leggen. Idealiter zetten we het ook in bij het bieden van duidelijkheid over de toekomst en transparantie over het proces. We zouden nu bijvoorbeeld al ervaringsverhalen kunnen aanbieden. Als bewoners deze regelmatig lezen, via zo'n app, dan kan dat al meer duidelijkheid bieden."

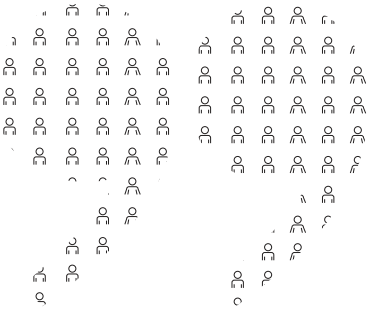
Optimaliseren van de supply chain

Hoe kan technologie helpen bij het beter inzichtelijk maken van rode cijfers? Pellemans: "We hebben nu meer instroom van mensen dan er kamers zijn. Het zou mooi zijn als we digitaal kenbaar kunnen maken dat er maar een paar plaatsen beschikbaar zijn, of dat mensen zich kunnen aanmelden voor bepaalde locaties in het land. Net als Zalando zouden we een supply chain kunnen inrichten met een 'distributiecentrum' van waaruit we mensen gaan herbergen. Ik denk dat er genoeg partijen zijn die ons zouden kunnen helpen met het versimpelen van onze logistieke supply chain. Dat betekent ook een heroriëntatie van het gehele logistieke systeem. Technologie kan ons hierbij helpen."

Ook binnenin het COA zullen aanpassingen gemaakt moeten worden om klaar te zijn voor de massale intrede van digitalisering. "Het gaat niet alleen om de techniek maar ook om sociale innovatie. We moeten de juiste medewerkers aan boord hebben en zorgen dat ze digitaal fit worden. Techniek kan ook helpen om onze mensen daar in te zetten waar ze het hardste nodig zijn. We doen bijvoorbeeld pilots met Trigion Security met mobiele camera's om de veiligheid te helpen waarborgen. Niet dat we nu een personeelsgebrek hebben: we groeien juist hard, ook qua personeel. Dat is een enorm compliment voor het COA als organisatie. Maar de voorspelling is dat we over twee jaar 135.000 asielzoekers gaan opvangen. Dat is meer dan een verdubbeling ten opzichte van nu. Die groei gaan we niet bijbenen met de huidige manier van werken. We moeten ons dus echt klaarmaken voor de toekomt."

Toekomstbestendig werken

Wat zijn de grootste wensen voor de komende jaren? "Ten eerste hoop ik dat we in 2025 een digitaal loket hebben waarbij gemeentes voorafgaand aan de opening van een nieuw AZC informatie beschikbaar kunnen stellen voor zowel omwonenden als asielzoekers", spreekt Pellemans uit. "Ten tweede hoop ik dat we qua dataontwikkeling zover zijn dat we een strategisch dashboard hebben dat met één druk op de knop de realtime situatie weergeeft: op welke locaties alle statushouders zijn en wat dat qua belasting betekent voor de komende tijd. Als we allemaal naar dezelfde werkelijkheid kijken en ons geen zorgen hoeven te maken over de betrouwbaarheid van cijfers dan kunnen we echt vanuit de data-analyse gaan werken. Om dit te realiseren moeten we het complexe systeemlandschap simplificeren. Daar ligt voor ons een mooie uitdaging."



Burger centraal

Attentie! Attentie! Digitale assistentie!

Hoe kan technologie de fysieke en digitale veiligheid verbeteren?

Een veiliger gevoel ‘s nachts op de fiets en thuis op de bank, wanneer je online bent. Het kan met technologie die nu al bestaat.

08
Burger centraal

Highlights:

- Wat als 112 altijd met ons meeluistert en ons proactief helpt in nood?
- Criminaliteit daalt bij meer blauw op straat, ook met meer blauw online?
- Politiedata aanvullen met eigen data en gebruikers proactief waarschuwen.
- Veilig zijn wil je altijd en overal, fysiek en online.

Jarenlang waren de kinderen veilig thuis. Nu is kindlief voor het eerst op stap in de grote stad en zelfs na herhaaldelijk aanbieden mag je ze niet ophalen. Ze gaan liever midden in de nacht op de fiets naar huis. Als ouder is het dan lastig om de slaap te kunnen vatten.

Ook wanneer je kinderen naast je op de bank zitten, zit je vast met de vraag wat ze nou allemaal uitspoken op hun telefoon. Wie komen ze daar online tegen en hoe zorg je als ouder dat ze veilig met hun gegevens omgaan? Moet je constant meekijken, of kan je ondertussen rustig naar de televisie kijken? Kunnen we technologie inzetten om in deze situaties veiligheid te bieden?

Zoals Janny Knol (Korpschef van de politie) in een interview zei: *"De politie is altijd aanwezig en staat altijd aan"*.[1] Niet alleen fysiek, maar ook digitaal is veiligheid een steeds belangrijker goed. Maar hoe doe je dat in een wereld die steeds meer digitaal plaatsvindt en waar de technologische ontwikkelingen steeds sneller gaan? Iedereen kent Cloud, virtuele assistenten en Generatieve AI, maar hoe helpt dit de omgeving veilig te maken? In dit artikel geven we antwoord op de volgende vraag:

Hoe kan technologie (real-time) de fysieke en digitale veiligheid verbeteren?

We delen een aantal oplossingsrichtingen op basis van onze visie waarmee technologie, die nu al beschikbaar is, ingezet kan worden om een veilig gevoel te creëren en proactief veiligheid aan te bieden voor de burgers in Nederland. Met als randvoorwaarde dat de data en informatie omtrent de burger veilig (of anoniem) zijn.

112 luistert met je mee

Laten we techniek inzetten in die situaties waarin we ons onveilig voelen, voor onszelf of voor een ander. Zoals in het voorbeeld dat iemand alleen naar huis fietst. 112 kan nu gebeld worden in noodsituaties, maar wat als 112 eigenlijk altijd (indien zo ingesteld) met ons meeluistert en ons proactief gaat helpen bij nood?

Op dit moment kan technologie in ons huis of op onze telefoons al meeluisteren om hulp te bieden. Zo kan je middels een spraakcommando muziek aanzetten, de verkeersinformatie opvragen of de oven voorverwarmen. Wat als we 112 toevoegen aan dat rijtje? Door gebruik van die bestaande technologie kan een app op iemands telefoon ingericht worden zodat in geval van nood een signaal gaat naar het alarmnummer, BOA's en/of de dichtstbijzijnde (wijk)agent.

Net als Alexa en Siri kun je van tevoren instellen of de app altijd mee mag luisteren, of dat het meeluisteren bijvoorbeeld pas geactiveerd wordt zodra de gebruiker een vooraf ingesteld woord gebruikt. Als burger ben je dan zelf in controle over wanneer data verzameld mag worden. Nog een stap verder zou automatische activatie zijn gebaseerd op locatie en tijdstip, in combinatie met een trendanalyse waar vaak problemen zijn ontstaan. Zo kan er op basis van bestaande klachten of aangiftes een analyse gedaan worden die proactief wordt ingezet om gebruikers van de app te "beveiligen" of om snel hulp in te schakelen zodra er wel iets aan de hand is.

Veiligheid in een digitale wereld

Fysieke veiligheid is één ding, maar tegenwoordig is veiligheid in een digitale omgeving minstens net zo belangrijk. Een groot deel van ieders dagelijkse activiteiten vindt inmiddels online plaats. De impact van digitale criminaliteit op de samenleving wordt hiermee ook steeds groter.

Technologiebedrijven zetten zich al jaren in om het gebruik van software of een apparaat veilig te maken. Dit zie je terug in functionaliteiten als:

- Virusscanners voor je laptop, desktop of smartphone;
- De spamfolder waarin e-mails verdwijnen die potentieel gevaarlijk zijn;
- Phishing- en malwaredetectie in je browser;
- Het kinderprofiel of kinderslot op een device waarbij je als ouder regie houdt over wat je kind kan doen;
- Suggesties van de locatie van een onbekende beller die gegeven wordt door je smartphone en mogelijk binnenkort het opzoeken van een beller met één knop[2];
- Een functie waarbij je in de app van de bank kunt zien of je door hen gebeld wordt of door een oplichter[3].

Dit bestaat al, maar kan de politie hier niet een meer proactieve rol in pakken? Criminaliteit daalt met meer blauw op straat, geldt dit ook met meer blauw online? En kan ze dit doen én de veiligheid van de persoonsgegevens van de betrokken personen garanderen?

De digitale Agent

Bzzzt, nieuw bericht. Het bericht is van een onbekend nummer. Deze persoon zegt jouw kind te zijn. In het bericht staat dat hij/zij hun telefoon is vergeten en vraagt via dit bericht of jij een kopje koffie kan betalen via een tikkie.

Bzzzt, nieuwe melding. Dit keer van Wout; "Let op, dit telefoonnummer is bekend bij de politie. Dit nummer wordt gebruikt door criminelen die proberen te frauderen."

Wout is momenteel de Chatbot op politie.nl. Wout geeft geautomatiseerd antwoord én kan je doorverbinden naar een politiemedewerker. Maar wat als Wout nog veel meer kan? Wat als Wout jou behoedt voor digitale criminelen?

De politie weet door aangiftes en meldingen welke rekeningnummers, e-mailadressen, telefoonnummers en websites mogelijk malafide zijn. Dit kan iedereen nu al checken op politie.nl. Door de chatoplossing van de politie door te ontwikkelen als widget kan Wout actief meekijken op de website waar de burger op aan het browsen is. De burger kiest zelf om deze in te schakelen bij twijfel, of altijd aan te laten staan. Komt Wout dan een bekend rekeningnummer, e-mailadres of telefoonnummer tegen, dan kan de widget een melding geven. Ditzelfde kan wanneer men op een mogelijk malafide webshop komt. Wout kan een website bestempelen als risicovol of onbetrouwbaar. De politie hoeft data alleen maar te scannen en matchen op data die zij hebben en niet op te slaan wat de burger doet.

Dit soort plug-in technologie zou ook gebruikt kunnen worden op grote (sociale media) platformen, of is dit niet de taak van de politie?

Dienst van de politie of verantwoordelijkheid van technologiebedrijven?

Ontwikkelingen zullen snel blijven gaan, waarschijnlijk nog sneller dan het nu gaat. Voor de politie is het niet realistisch om voor elk (nieuw) platform of elke applicatie eigen software te publiceren die gebruikers behoedt voor digitale criminaliteit. De politie kan wel haar informatie beschikbaar stellen, op zo'n manier dat technologiebedrijven dit gemakkelijk op kunnen vragen. Zij

kunnen de politie data combineren met data en feedback die zij zelf verzamelen met betrekking tot verdachte gebruikers en berichten en daarmee gebruikers proactief waarschuwen. Zodat zij op elk (nieuw) platform of in elke gebruikte applicatie, met de kennis die de politie heeft verzameld, jou kunnen behoeden voor digitale criminaliteit.

Tijdens het schrijven van dit artikel werd bekend dat de Europese Commissie werkt aan een wetsvoorstel om berichtendiensten zoals WhatsApp, Signal en Telegram te verplichten om detectiesoftware te installeren om de verspreiding van kinderporno tegen te gaan. Hier is veel kritiek op vanuit de wetenschap met oog op privacy en uitvoerbaarheid[4].

Digitale veiligheid binnen kaders

Innovatie is niet per definitie een nieuwe technologie. Innovatie kan ook een verbetering zijn op basis van bestaande applicaties, technologieën of methodieken. Hetgeen wat er al is zo goed mogelijk benutten, kan evengoed baanbrekend zijn en grote impact hebben op of voor gebruikers.

Het is belangrijk om vanuit het veiligheidsdomein te kijken naar die impact, maar ook zeker binnen de gestelde veiligheidskaders te kijken naar de mogelijkheden. Ontwikkelingen als generatieve AI hebben hun weerslag op de veiligheid van de burger. Draai het om en het kan ingezet worden in gerichte mogelijkheden die de burger een veiliger gevoel geven en veiligheid bieden in een digitale omgeving.

Veilig zijn wil je altijd en overal, fysiek en online. Maar het liefst kies je zelf wanneer je dit nodig hebt. Je wilt niet dagelijks herinnerd worden aan de airbag in je auto, maar het is heel fijn als die beschikbaar is wanneer nodig. De technologie van nu kan jouw airbag zijn. Fysiek, wanneer je kind 's nachts naar huis fietst, of online wanneer kindlief naast je op de bank op Instagram of TikTok zit.

Over de auteurs

Quido de Zwart | Managing Consultant – Portfolio lead Augmented Service

Quido zet de mens centraal. Dit doet hij bijna 10 jaar vanuit verschillende rollen. Op dit moment als consultant bij opdrachtgevers binnen het publieke domein en als Customer Experience Service lead en deputy clustermanager binnen Capgemini.

quido.de.zwart@capgemini.com
https://www.linkedin.com/in/quido-de-zwart/

Mirjam Smid | Senior Consultant

Mirjam is een ervaren consultant die al geruime tijd organisaties helpt om mensgerichte dienstverlening goed in te richten en te borgen. Bij Capgemini heeft zij een focusgroep die zich richt op het centraal stellen van de burger binnen de dienstverlening van de overheid.

mirjam.smid@capgemini.com
www.linkedin.com/in/mirjamsmid/

1. https://www.politie.nl/nieuws/2024/februari/29/00-nieuwe-korpschef-janny-knol-zorgen-dat-de-politie-midden-in-de-samenleving-blijft-staan.html
2. https://tweakers.net/nieuws/220578/google-test-pixel-functie-voor-het-opzoeken-van-onbekende-telefoonnummers.html
3. https://www.ing.nl/de-ing/veilig-bankieren/wat-kan-je-zelf-doen/check-het-gesprek
4. Kinderporno opsporen met detectiesoftware op mobiel: experts tegen EU-wetsvoorstel (nos.nl)

09
Burger centraal

Veiligheid op maat: het transformerende effect van klantreizen

Hoe kunnen klantreizen ingezet worden om de burger centraal te stellen en daarmee de veiligheid te vergroten?

De mens centraal stellen vereist naast inzicht in de behoeften van mensen, ook het blootleggen en overwinnen van uitdagingen die de weg naar een effectieve uitvoering bemoeilijken.

Highlights:

- Het centraal stellen van een burger draait om behoeften, rechten en waardigheid van de mens.
- Een burgerreis maakt inzichtelijk hoe de burger de dienstverlening beleefd.
- Met burgerreizen kunnen organisaties oplossingen bieden die aansluiten bij de realiteit.

Een aanpak voor een rechtvaardige en veilige samenleving

De burger centraal stellen is een actueel thema. Zo riep informateur Kim Putters eind 2023 de politiek al op om de belangen van de burger voorop te stellen: "Los de echte problemen van mensen op […] Zodat ze er ook echt weer vertrouwen in kunnen hebben dat de overheid er ook voor hen is."[1] Dit om te komen tot een verbetering in de (gezamenlijke) dienstverlening vanuit de uitvoeringsorganisaties en waar nodig het vertrouwen in de overheid terug te winnen[2]. In 2021 werd er ook door Politie en Dienst Justitiële Inrichtingen (DJI) binnen het veiligheidsdomein een beroep gedaan op de (toenmalige) minister-president om de burger centraal te stellen.

Achter het streven van 'de mens centraal stellen' schuilen talrijke uitdagingen die het succes ervan kunnen belemmeren. Zo staat het Ministerie van Justitie en Veiligheid voor aanzienlijke uitdagingen, zoals bijvoorbeeld het voorkomen van recidive en revictimisatie[3] die inzet vereisen voor een rechtvaardige en veilige samenleving. Ook het aanpakken van ondermijning, geopolitieke spanningen, terrorisme, bedreigingen tegen de democratie, technologische vooruitgang en klimaatverandering vergt voortdurende aandacht[3].

Bij het centraal stellen van de burger draait het om behoeften, rechten en waardigheid van de mens[4]. En worden besluiten genomen, beleid gemaakt en acties ondernomen[5]. Wanneer we het hebben over de burger centraal stellen komt bij bovenstaande definitie de nuance van burgerlijke vrijheid, participatie, rechten en verantwoordelijkheden binnen de staatsstructuur[6].

Het realiseren van een echt burgergerichte aanpak vereist niet alleen inzicht in de behoeften van burgers, maar dus ook het blootleggen en overwinnen van uitdagingen die de weg naar een effectieve uitvoering bemoeilijken. Het aanpakken van deze uitdagingen vergt een doordachte en gestructureerde werkwijze. Een veelbelovende optie om deze uitdagingen aan te pakken is om gebruik te maken van de methodiek 'burgerreizen'.

Publieke organisaties in staat stellen om een stap vooruit te zetten naar een veilig Nederland dat de burger daadwerkelijk centraal stelt

Een burgerreis (ook wel bekend als klantreis) is een visuele procesbeschrijving van alle interacties die een specifieke burger heeft met een bepaalde dienst, vanaf het allereerste contactmoment tot het doel van de burger bereikt is. Een burgerreis wordt altijd opgesteld vanuit het oogpunt van een specifieke persona zoals bijvoorbeeld een asielzoeker in het aanvraagproces van een verblijfsvergunning en een gedupeerde in het aangifteproces na diefstal. Een burgerreis maakt inzichtelijk welke processtappen een burger doorloopt en hoe deze de dienstverlening beleefd, waardoor inzichtelijk wordt waar de knelpunten zich in de dienstverlening bevinden. Burgerreizen worden als methode vaak gebruikt door Capgemini om publieke organisaties zich meer in te laten leven in de behoeftes van burgers en daarmee de dienstverlening te kunnen verbeteren. Het stelt publieke organisaties in staat om een stap vooruit te zetten naar een veilig Nederland en tevens de burger daadwerkelijk centraal stelt. Relevante voorbeelden waarbij het in kaart brengen van burgerreizen van toegevoegde waarde bleek, zijn de burgerreizen voor LGBTI-asielzoekers binnen het asielproces[7], te bewaken advocaten binnen het Marengo proces[8] en kinderen betrokken bij geweldincidenten binnen het jeugdzorgstelsel[9]. In afbeelding 1 is een burgerreis gevisualiseerd.

Voor de totstandkoming van een specifieke burgerreis is het van cruciaal

Afbeelding 1: Klantreis

Voorbeeld klantreis van een LHBTI+ asielzoeker

belang dat burgers echt betrokken worden, en dus centraal worden gesteld. Het onderzoek start met het identificeren van een persona, ofwel de gebruiker van de dienst. Een persona is altijd een fictief persoon die een specifieke doelgroep representeert. Aan de hand van interviews met de doelgroep wordt er een diepgaand inzicht verkregen in de ervaringen, voorkeuren en uitdagingen van de burgers. Deze inzichten stellen publieke organisaties in staat om op maat gemaakte, (technologisch) ondersteunde oplossingen te ontwikkelen die direct inspelen op de specifieke behoeften en pijnpunten van de burger.

Het gebruik van burgerreizen biedt publieke instanties niet alleen inzicht in de behoeften en ervaringen van burgers, maar brengt ook andere voordelen met zich mee. Burgerreizen kunnen daarnaast ook benut worden als strategisch instrument. Het analyseren en verbeteren van de burgerreis stelt publieke instanties in staat om inefficiënties en pijnpunten in processen te identificeren en aan te pakken. Dit kan leiden tot een verbeterde operationele efficiëntie en een betere allocatie van middelen. Daarnaast kunnen publieke instanties geïnformeerde beslissingen nemen over beleid, dienstverlening en investeringen die daadwerkelijk aansluiten bij de behoeften van de samenleving.

De kracht van burgerreizen zit in het potentieel tot transformatie: door samen te werken met burgers gedurende de hele reis, hebben publieke instanties de mogelijkheid om niet alleen te voldoen aan de behoeften van de samenleving, maar deze ook te transformeren door middel van continue verbetering.

De behoeften en verwachtingen van burgers in het publieke domein zijn echter voortdurend in beweging. Burgerreizen moeten om deze reden regelmatig worden geëvalueerd en aangepast om deze veranderingen bij te houden. Dit vereist een cultuur van voortdurende verbetering en flexibiliteit om snel te reageren op feedback. Door voortdurende optimalisatie blijven publieke organisaties voldoen aan de steeds veranderende behoeften van de samenleving en tegelijkertijd de burgertevredenheid verder te blijven verhogen. Dit aanpassingsvermogen is cruciaal om effectief te blijven opereren en het vertrouwen van de burgers te behouden in onze dynamische en complexe maatschappij.

Het voorkomen van georganiseerde criminaliteit met burgerreizen

Zoals al eerder gesteld is het centraal stellen van de mens en burger niet alleen een uitdaging, maar ook een kans om een meer inclusieve en veerkrachtige samenleving te creëren en tevens de veiligheid van burgers te vergroten.

Eén van de meest bekende en meest schrijnende zaken van de afgelopen jaren is het Marengo proces, met in de hoofdrol Ridouan Taghi. Meneer Taghi is ooit ook jong geweest[10]. Hij sloot zich in begin jaren '90 aan bij de jeugdbende Bad Boys, oftewel de start van zijn criminele carrière. Op dit moment zijn verschillende gemeenten hard aan het werk om te voorkomen dat er nieuwe 'Taghi's' ontstaan binnen de Nederlandse samenleving. Gemeentes zetten hierbij in op het gebruik van burgerreizen. Allereerst zijn de verschillende doelgroepen (jonge aanwas, doorgroeiers, harde kern) binnen de samenleving geïdentificeerd. Per doelgroep wordt vervolgens de levensloop van de kinderen binnen de doelgroep uitgestippeld om te komen tot passende interventies. Vandaag de dag noemen we waar Taghi zich in de jaren 90 bevond 'jonge aanwas'. Vanuit het Ministerie van Justitie en Veiligheid is er een programma opgezet dat toegewijd is aan het voorkomen dat jongeren, zoals de toen jonge Taghi, in de georganiseerde criminaliteit belanden of daarin verder afglijden. In dit programma worden de jongeren centraal gezet. Het programma heet Preventie met gezag[11].

Conclusie

In een tijd van voortdurende veranderingen is het van cruciaal belang om veiligheid te benaderen vanuit het perspectief van de burger. Door het gebruiken van de burgerreis methodiek kunnen publieke instanties de uitdagingen rondom het centraal stellen van de burger overwinnen en tegelijkertijd de veiligheid en het veiligheidsgevoel van burgers vergroten. Burgerreizen bieden een gestructureerde benadering om het pad te visualiseren dat burgers doorlopen, waardoor publieke instanties een diepgaand inzicht krijgen in de huidige processen, de klant behoeften, zorgen en ervaringen. Door deze benadering kunnen organisaties proactief reageren op de behoeften van burgers en oplossingen bieden die daadwerkelijk aansluiten bij hun dagelijkse realiteit.

Als leiders, beleidsmakers en uitvoerders moeten we deze benadering omarmen en actief investeren in de implementatie van burgerreizen binnen publieke instanties en vooral het veiligheidsdomein. Laten we een meer mensgerichte en veerkrachtige samenleving creëren, waarbij de behoeften en belangen van de burger centraal staan.

Over de auteurs

Chèr van Slobbe | Senior Consultant

Chèr is een ervaren consultant die werkzaam is binnen het publieke domein en de focus legt op het centraal stellen van de burger om dienstverleningen te verbeteren. Zij heeft ruime ervaring in het toepassen van design thinking methodieken, waaronder klantreizen.

cher.van.slobbe@capgemini.com
https://www.linkedin.com/in/cher-van-slobbe/

Teddy van Eijk | Senior Consultant

Teddy helpt publieke organisaties om strategie en innovatiemanagement met een mensgerichte inslag te bewerkstelligen. Zij doet dit graag in samenwerking met de klant en de burger.

teddy.van.eijk@capgemini.com
https://www.linkedin.com/in/teddy-van-eijk/

Inge Koning | Senior Consultant

Inge is gespecialiseerd in strategie en innovatiemanagement en legt voornamelijk de focus op het aanpakken van grote vraagstukken binnen publieke organisaties, met een sterke nadruk op het centraal stellen van de burger.

inge.koning@capgemini.com
https://www.linkedin.com/in/koninginge/

1. NOS. (2022, 14 januari). Informateur Kim Putters riep politiek steeds op het belang van de burger voorop te stellen. https://nos.nl/collectie/13962/artikel/2508868-informateur-kim-putters-riep-politiek-steeds-op-het-belang-van-de-burger-voorop-te-stellen Politie Nederland. (2021). Strategische agenda politie 2021-2025 [Brochure]. https://www.politie.nl/informatie/strategische-agenda-politie-2021-2025.html
2. Belastingdienst. (2021, 20 mei). Uitvoeringsorganisaties roepen politiek op: zet burger centraal. https://over-ons.belastingdienst.nl/uitvoeringsorganisaties-roepen-politiek-op-zet-burger-centraal/
3. https://jenvbredewerkagenda.nl/news/view/34e5779c-161d-4b79-a3d6-47137d395011/de-mens-is-de-maat-niet-het-percentage-of-de-doorlooptijd
4. Valk Leadership. (z.d.). Managers weten niet meer hoe de mens centraal te zetten. https://www.valkleadership.nl/managers-weten-niet-meer-hoe-de-mens-centraal-te-zetten/
5. Programma Mens Centraal. (z.d.). Over ons. https://www.programmamenscentraal.nl/over-ons
6. Zelfbouw in Nederland. (2018). De burger centraal. https://www.zelfbouwinnederland.nl/informatie/algemeen/de-burger-centraal
7. https://eenvandaag.avrotros.nl/item/je-krijgt-blikken-je-wordt-gepest-lhbti-asielzoekers-vertellen-hoe-onveilig-ze-zich-voelen-in-nederlandse-azcs/
8. https://www.rijksoverheid.nl/actueel/nieuws/2023/03/31/naar-een-nieuw-stelsel-het-stelsel-beveiligen-van-personen#:~:text=Na%20de%20moorden%20op%20de,beveiligingssituaties%20van%20deze%20drie%20personen.
9. https://jenvbredewerkagenda.nl/news/view/34e5779c-161d-4b79-a3d6-47137d395011/de-mens-is-de-maat-niet-het-percentage-of-de-doorlooptijd
10. https://www.dutchmultimedia.nl/ridouan-taghi-een-korte-biografie-van-de-grootste-kleine/
11. https://gemeenteraad.rotterdam.nl/Reports/Document/09a5b6ee-1ba2-4a07-b117-b857ed590890?documentId=b70f83f8-1e34-46d9-895b-23bfd81218d

Interview:

“We leven in een tijd waarin we lastige puzzels moeten leggen”

De toekomst van onze samenleving is de toekomst van de arbeidsmarkt. Society 5.0 verandert ook de bestaande arbeidsstructuren ingrijpend. In een wereld van mondiale spanningen moet het personeelsbestand van Defensie flexibel en schaalbaar zijn. “In vredestijd moet je je arbeidsmarktstrategie ontwikkelen”.

Paul van der Touw
Brigadegeneraal
Souschef Personele Gereedheid / Defensiestaf

Paul van der Touw is brigadegeneraal en souschef Personele Gereedheid bij de Defensiestaf. “Onze rol als werkgever verandert sterk. Willen we een duurzaam personeelsbestand opbouwen, dan moeten we structureel inzetten op persoonlijke ontwikkeling, inspelen op levensfasen en duurzame inzetbaarheid. Je ziet dat werknemers zich toenemend als consument op de arbeidsmarkt gedragen. Dat geldt vooral voor jongeren die weten dat ze nog lang gaan werken. Ze zijn kritisch: wie krijgt de eer om mijn werkgever te zijn? De vraag is dus: hoe worden wij die werkgever? Bovendien zien veel jongeren werk inmiddels als ‘extra’. Een relevant deel richt hun leven zo in dat ze minder geld nodig hebben en minder tijd aan werk hoeven te besteden. Als werkgever moet je dit soort keuzes overzien en faciliteren via de arbeidsvoorwaarden, wil je interessant zijn én blijven.”

Hevige concurrentiestrijd

De concurrentiestrijd om personeel binnen het veiligheidsdomein is intens. In 2023 wist het ministerie 3.600 nieuwe militairen aan te stellen tegenover een uitstroom van 3.200. Van der Touw: “Voor jongeren zijn we niet altijd een competitieve werkgever. Vooral werknemers tot 35 jaar stromen uit. Veel jongeren zijn niet uit op een levenslang dienstverband. Daarom bieden we diverse loopbaanvormen aan.” De gemiddelde instroomleeftijd van militairen staat inmiddels op 21 jaar; een toenemende groep niet-schoolverlaters solliciteert. “Dat ondersteunt onze diversiteit qua opleidingsachtergrond en leeftijd. Belangrijk, want we zijn ‘een samenleving binnen de samenleving’. Bijna iedere beroep kun je bij ons uitoefenen. We moeten onze organisatie namelijk kunnen oppakken en elders in de wereld neerzetten. Dat maakt onze behoefte aan functiediversiteit groot. Die diversiteit geldt overigens voor ons gehele functiebestand. Er werken ruim 21.000 burgers bij Defensie. Voor hen zijn onze arbeidsvoorwaarden vaak concurrerend.”

Vergroten van diversiteit

Waar een flexibel personeelssysteem voor bijna alle functies de norm was, wordt nu ook een vast contract aangeboden aan korporaals en manschappen. Van der Touw: “Daarmee komen we tegemoet aan veranderende wensen. Het is nog vroeg om te beoordelen hoe groot het effect op behoud is, maar de eerste signalen zijn positief. We zien de noodzaak de rechtspositie van militairen en in algemene zin de arbeidsvoorwaarden van defensiepersoneel te moderniseren. Die zijn nog vaak gebaseerd op klassieke denkbeelden, waardoor recruiters en managers ervaren dat ze te weinig speelruimte hebben in het gesprek met een kandidaat. We willen bijvoorbeeld financieel aantrekkelijker zijn voor schaarse categorieën personeel. Maar gesprekken met kandidaten lopen ook vast op niet-financiële aspecten, zoals bijvoorbeeld de garantie om niet buiten een bepaalde regio te worden geplaatst of structureel in deeltijd te kunnen werken. Op die en andere vlakken hebben we huiswerk. Daarnaast is het nuttig de ontwikkelingen in andere EU-landen en NAVO-lidstaten te volgen, die op het punt staan hun krijgsmacht te openen voor burgers uit andere EU-landen.

Van der Touw: “Op de korte termijn is het belangrijk dat we ons pakket aanstellings- en contractvormen uitbreiden. Dat geeft meer speelruimte in het gesprek met een kandidaat. Daarvoor hebben we intern nog zaken te doen omdat de organisatie

zich moet inrichten op een grotere rechtspositionele diversiteit. Daar zitten lastige kanten aan maar er is vanwege de arbeidsmarkt niet aan te ontkomen. Cruciaal is dat de krijgsmacht in staat blijft haar taken uit te voeren en personeel dus gegarandeerd beschikbaar is. Maar dat betekent niet dat al ons personeel 52 weken per jaar op de werkvloer aanwezig hoeft te zijn. We richten ons op het tot stand brengen van een schaalbare krijgsmacht van in 2030 ruim 52.000 militaire arbeidsplaatsen. Maar een relevant deel van ons personeel mag, al dan niet in deeltijd, een tweede werkgever hebben. Belangrijk is dat alle spelers in dat duaal werkgeverschap goede afspraken maken. Als het meest ernstige scenario ooit werkelijkheid wordt is het niet logisch te veronderstellen dat arbeidsrelaties een belemmering vormen. Dan weten we allemaal wat ons te doen staat."

Schaalbaarheid als sleutel

Strategische speerpunten voor het personeelsbeleid bij Defensie richten zich vooral op schaalbaarheid. Van der Touw: "Met een bondgenootschappelijke verdediging, een krappe arbeidsmarkt en een gelimiteerde defensiebegroting is het onhaalbaar om 365 dagen per jaar een krijgsmacht op oorlogssterkte op de been te houden. Dat is ook niet nodig. Mocht het zover komen hebben we echt wel een paar weken tijd om de krijgsmacht te bemensen uit het getrainde schaalbare bestand. Schaalbaarheid gaat verder dan medewerkers in deeltijd of als reservist aanstellen. Een schaalbare krijgsmacht neemt ook civiele organisaties op in voornamelijk, maar niet uitsluitend, logistieke ketens die in situaties waar dat verantwoord is militaire taken verrichten. Een vrachtauto hoeft niet groen te zijn om voorraden te vervoeren. Als we dat per sé willen wordt de krijgsmacht heel duur. Er zijn nu ruim honderd civiele organisaties die zich in ecosystemen aan Defensie hebben verbonden. We hebben het klassieke denken over sourcing achter ons gelaten en willen in een volgende stap civiele organisaties integreren in militaire structuren."

Strategisch personeelsmanagement cruciaal

Een schaalbare krijgsmacht vraagt grote veranderingen. Alles en iedereen moet meebewegen met andere werkwijzen, bijvoorbeeld met betrekking tot de manier waarop we de krijgsmacht gereed stellen en financieren. Een voorbeeld is de snel toenemende interesse in het Dienjaar Defensie[1]. Van der Touw: "De krijgsmacht kan vandaag nog niet 4.000 Dienjaar militairen per jaar absorberen. We moeten onze organisatie inrichten op dat grote aantal militairen dat een relatief korte opleiding krijgt en misschien maar een jaar in actieve dienst blijft. Aansluitend worden ze opgenomen in het beroepsbestand of worden reservist. We kennen dit model uit de tijd voor het opschorten van de opkomstplicht in 1997, maar voor de krijgsmacht van vandaag is het een grote personeelslogistieke verandering. Voorop staat dat de krijgsmacht getraind en inzetbaar moet zijn en blijven. Dit soort grote veranderingen in de personeelslogistiek betekent iets voor de manier waarop we de krijgsmacht gereed stellen."

Invloed van digitalisering en techniek

Ook de toepassing van nieuwe technologieën brengt volgens Van der Touw uitdagingen: "Overal waar je technologische innovaties succesvol integreert in militaire concepten ontstaat een groeimarkt en een tekort aan mensen. Zo hebben we veel ICT-ers en cybertechnici nodig want we verdedigen Nederland ook in het informatiedomein. In dat domein wordt gevochten, 365 dagen per jaar." Ook technologieën als open source intelligence zijn belangrijk voor de krijgsmacht. Via metadata en geolocatie is veel strategische informatie beschikbaar. Bewegingen van gevechtseenheden kun je bijvoorbeeld waarnemen als militairen hun smartphones op zak mogen houden. Van der Touw: "Er zijn systemen die beelden razendsnel analyseren en er vervolgens een heel precieze locatie aan koppelen. Die informatie is snel te uploaden in drones of te gebruiken om binnen enkele minuten een wapensysteem te richten. De effecten van technologie in ons vak zijn onvoorstelbaar groot, maar bij het gebruik ervan blijven de mens en de menselijke afweging centraal staan." Naast specifiek militaire toepassingen van technologie maken krijgsmachten ook gebruik van systemen die primair civiele toepassingen kennen, zoals ERP applicaties of blockchain. Van der Touw: "De krijgsmacht leunt op logistieke ketens die we efficiënt inrichten. Daarmee houden we grip op voorraden en zorgen we voor de juiste middelen op de juiste plek. Het effectief kunnen besturen van logistieke ketens is bepalend voor de uitkomst van een conflict."

Nationaal samenwerken in oorlogstijd

In geval van een NAVO-oorlogssituatie zal het leeuwendeel van de krijgsmacht niet aan de Nederlandse, maar aan de Europese grenzen vechten. Van der Touw: "Oorlog betekent dus ook iets voor veel andere crisispartijen in Nederland, zoals politie, koninklijke marechaussee en douane. Zo'n extreme situatie vereist intensieve samenwerking die we in vredestijd tot stand moeten brengen. Daarom komt een nationaal plan tot stand met taakafbakeningen, raakvlakken en keuzes. Hoe opereren we gezamenlijk in een oorlogssituatie? Wat is bijvoorbeeld de impact op Nederland als 400.000 Amerikaanse militairen met materieel via Rotterdam en Vlissingen door Nederland verplaatsen? Helaas leven we in een tijd waarin we deze puzzels met elkaar moeten leggen. Maar als je deze puzzels legt ligt het voor de hand dat je ook samen nadenkt over een arbeidsmarktstrategie voor beroepen in het veiligheidsdomein. We begrijpen allemaal dat dit belangrijk is. We doen het voor Nederland."

1. Het Dienjaar Defensie is een intensief jaar (GapYear) waarin mensen voltijd werken als militair bij één van de krijgsmachtdelen: de Landmacht, Marine, Luchtmacht of Marechaussee. In tegenstelling tot de dienstplicht, is deelname aan het Dienjaar Defensie gebaseerd op vrijwilligheid, professionaliteit en intrinsieke motivatie.

Toekomst van werk

10
Toekomst van werk

De nieuwe dimensie van forensisch onderzoek: Virtual Reality als brug tussen plaats delict en rechtszaal

Hoe verandert Virtual Reality de toekomst van de forensische opsporing?

Ontdek hoe Virtual Reality de Nederlandse forensische opsporing revolutioneert, van plaats delictanalyses tot rechtszaal toepassingen.

Highlights:

- Virtual Reality herdefinieert forensisch onderzoek.
- De Nederlandse politie is wereldleider in de implementatie van Virtual Reality in de forensische opsporing.
- Er zijn uitdagingen in realisme, acceptatie en technologie Virtual Reality.
- Doorontwikkeling in technologie Virtual Reality en opslag data is cruciaal.
- Virtual Reality is de sleutel in toekomstige misdaadbestrijding.

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 wordt volledig afgesloten van de fysieke werkelijkheid, waardoor de driedimensionale, virtuele werkelijkheid als de fysieke werkelijkheid wordt ervaren.

De afdeling Forensische Opsporing van de Nederlandse Nationale Politie heeft door de jaren heen significante veranderingen ondergaan, vooral met de introductie van technologische innovaties. Een van de meest opmerkelijke ontwikkelingen in dit veld is de toepassing van Virtual Reality (VR) in de opsporing. De landelijke eenheid van de Nationale Politie verricht baanbrekend werk in het digitaliseren van plaatsen delict (PD's) en heeft met de VR-technologie een nieuw hoogtepunt bereikt. Zo kunnen onder andere rechercheurs, forensisch deskundigen, officieren van justitie en ook rechters de PD virtueel (blijven) betreden, onderzoeken en ervaren, wat voor meer inzicht en onderzoeksmogelijkheden zorgt. Dit biedt meer duidelijkheid in strafzaken en zorgt daardoor voor een beter strafproces. VR levert ook uitdagingen op zoals de opslag van data en het omgaan met de beperkingen zoals het realiteitsgevoel van een virtuele omgeving. Dit artikel gaat in op de nieuwe kansen, toekomstige perspectieven en uitdagingen van VR in de strafrechtketen.

Implementatie en toepassingen

De opsporing zet al jaren technologische ontwikkelingen in om de PD zo goed mogelijk vast te leggen. Zo werd met de komst van de videocamera de PD en de omliggende omgeving gefilmd zodat niet alleen de plaats, waar het misdrijf zich had voltrokken, vastgelegd werd, maar ook de sfeer in de buurt op dat moment. De Forensische Opsporing brengt PD's in kaart door middel van foto's, lasers en metingen met gebruiksvriendelijke software. In slechts 3 minuten levert dit een dusdanig nauwkeurige weergave op dat zelfs individuele blaadjes in een bos geteld kunnen worden. Deze methode is al met succes toegepast in grote zaken zoals de Puttense moordzaak, de zaak Nicky Verstappen en de zaak van Marianne Vaatstra, waarbij oude beelden werden gebruikt voor reconstructies. Daarnaast wordt deze tool ook ingezet bij briefings en trainingen, operationele voorbereidingen, zoals bij heimelijke operaties en bij het opstellen van evacuatieplannen voor grote evenementen.

De toepassing van VR-technologie in de rechtszaal vormt een innovatieve doorbraak in het forensisch onderzoek en de rechtspraak. Deze technologie stelt rechters en advocaten in staat PD's en andere relevante scenario's op een ongeëvenaarde manier te ervaren en te begrijpen. VR biedt namelijk een nieuwe dimensie in het beoordelen van bewijs doordat de ruimtelijke en visuele aspecten van een getuigenis beter onderzocht kunnen worden. In verschillende zaken speelde VR daardoor een cruciale rol in het verhelderen van gebeurtenissen. Een voorbeeld daarvan is de Puttense moordzaak. In die zaak was de verklaring van een ooggetuige van cruciaal belang. VR maakte een simulatie van de PD mogelijk, zodat de exacte zichtlijnen en perspectieven van deze getuige gereconstrueerd konden worden. Door visueel te demonstreren wat vanuit het perspectief van de getuige zichtbaar was, kon de geloofwaardigheid van de getuigenis bepaald worden. De rechter kon op die manier een grondiger en beter geïnformeerde beoordeling maken van de getuigenis.

Een andere zaak waar VR bepalend was, was een zaak met een overleden baby. De verdachte in die zaak beweerde dat het kind was gevallen. VR bood de mogelijkheid om het scenario van de val te reconstrueren in de omgeving waar het incident plaatsvond. De reconstructie toonde aan dat de ruimte te beperkt was voor het scenario zoals beschreven door de verdachte, waardoor de bewering onwaarschijnlijk werd. Dit soort visuele en ruimtelijke analyse biedt een krachtig hulpmiddel voor de opsporing en de rechtspraak, omdat het helpt om de feiten van een zaak te verhelderen op een manier die met traditionele methoden niet mogelijk zou zijn.

Verder helpt VR bij het visualiseren van complexe ruimtelijke scenario's zoals de trajecten van projectielen in schietincidenten. Door de banen van kogels in een driedimensionale ruimte te simuleren, helpt VR bij het bepalen van schietposities en schietrichtingen. Deze technologie maakt het daardoor mogelijk om verschillende scenario's te modelleren en te analyseren, wat kan leiden tot een beter begrip van wat er werkelijk is gebeurd en welke scenario's er uitgesloten kunnen worden.

Vraagstukken en aandachtspunten

Ondanks de onmiskenbare voordelen die VR-technologie biedt in de (forensische) opsporing, worden professionals geconfronteerd met diverse uitdagingen die niet mogen worden onderschat. De weerstand tegen de implementatie

van VR-technologie is een van deze uitdagingen. Dit kan voortkomen uit gebrek aan vertrouwen in nieuwe technologieën, onzekerheid over de effectiviteit ervan of simpelweg gebrek aan kennis over het gebruik van deze systemen. Het overwinnen van deze weerstand vereist uitgebreide training en demonstratie van de concrete voordelen die VR biedt.

Een ander vraagstuk is het ontbreken van een realistisch gevoel in virtuele omgevingen. Hoewel VR indrukwekkende visuele reconstructies kan bieden, mist het vaak de tactiele en sensorische aspecten van een echte omgeving, zoals het gekraak van glas onder je voeten. Dit kan invloed hebben op de interpretatie en het begrip van een PD tijdens onderzoek of in de rechtbank. Een virtuele reconstructie wekt de suggestie van een exacte kopie. Het is daarom essentieel dat geen belangrijke details worden gemist in de beeldvorming, omdat dit mogelijk tot tunnelvisie leidt. Denk bijvoorbeeld aan het vastleggen van verborgen ruimtes, die moeilijk waarneembaar zijn wanneer materie niet gevoeld kan worden. Het ontwikkelen van geavanceerdere VR-systemen die een rijkere en meer natuurgetrouwe ervaring bieden, kan dus van cruciaal belang zijn. Ook de toepasbaarheid van VR bij bepaalde PD's vormt een uitdaging. Zo is VR minder effectief bij misdrijven in open velden of andere minder afgebakende ruimtes in het bieden van nuttige inzichten. Dit benadrukt de noodzaak voor flexibele en adaptieve VR-systemen die inzetbaar zijn bij een breed scala aan scenario's.

Bovendien brengt de distributie en infrastructuur van VR-platforms aanzienlijke technische en logistieke uitdagingen met zich mee. Zo vereisen VR-systemen een hoge bandbreedte om soepel te functioneren, wat vraagt om geavanceerde en vaak kostbare netwerkupgrades. Dit is een belangrijk aandachtspunt, vooral voor rechtshandhavingsorganisaties die werken met beperkte budgetten en middelen. De veiligheid van gevoelige data is een andere topprioriteit. Met de toenemende digitalisering van bewijsmateriaal neemt het risico op datalekken en cyberaanvallen toe. Het waarborgen van de integriteit en vertrouwelijkheid van digitale bewijsstukken en persoonsgegevens is van het grootste belang. Dit vereist geavanceerde beveiligingsmaatregelen en continue updates om de systemen te beschermen tegen nieuwe bedreigingen. Het veilig distribueren van de software en het waarborgen van data-integriteit, vooral wanneer informatie op laptops en mobiele apparaten wordt bekeken, is een complexe taak. Dit vereist niet alleen robuuste beveiligingsprotocollen, maar ook een cultuur van beveiligingsbewustzijn onder de gebruikers. Training en bewustwording zijn essentieel om te waarborgen dat de gebruikers verantwoordelijk omgaan met de toegang tot gevoelige informatie.

Kortom, hoewel VR een veelbelovende toekomst biedt in de forensische opsporing, moeten de uitdagingen op het gebied van acceptatie, realisme, toepasbaarheid, technische infrastructuur, en data-veiligheid serieus worden genomen en worden aangepakt om het volledige potentieel van deze technologie te realiseren.

Toekomstperspectieven

De toekomst van VR in de forensische opsporing ziet er zoals gezegd veelbelovend uit. VR geeft onder andere de mogelijkheid voor gedetailleerde trainingssimulaties ten behoeve van forensisch onderzoek. Zowel forensische als tactische rechercheurs kunnen getraind worden in het herkennen van subtiele aanwijzingen en patronen in een virtuele omgeving, wat hun vaardigheden in de echte wereld zou kunnen versterken. Deze simulaties kunnen ook worden aangepast aan specifieke scenario's, waardoor een meer gerichte en effectieve opleiding mogelijk wordt. Bovendien biedt het de mogelijkheid om naast rechercheurs ook andere specialisten te trainen, zoals bijvoorbeeld zaaksanalisten in het opstellen van mogelijke scenario's.

De Nederlandse aanpak onderscheidt zich van andere landen door de brede implementatie over alle verschillende eenheden binnen de politie en de integratie in rechtszaken. Nederland positioneert zich daardoor als wereldleider in de implementatie van 3D-visualisatie in forensisch onderzoek. Dit biedt kansen voor internationale kennisdeling en samenwerking in de toepassing van VR-technologie, zoals al gebeurt met landen als Zweden, Canada, België en Frankrijk. Bovendien opent VR de deur naar real-time samenwerking met internationale teams, waardoor grensoverschrijdende misdaadbestrijding effectiever kan worden.

Als een van de meest fascinerende mogelijke ontwikkelingen voor de toekomst zien de schrijvers het virtueel sporenonderzoek. Dit houdt in dat rechercheurs, forensisch deskundigen en ook bijvoorbeeld officieren van justitie virtueel door een PD kunnen navigeren, sporen kunnen analyseren en interactie kunnen hebben met de omgeving op een manier die voorheen onmogelijk was. Het biedt de mogelijkheid om een PD meerdere keren te bezoeken zonder de fysieke locatie te verstoren of aan tijdslimieten gebonden te zijn. Dit kan waardevol zijn in complexe of gevaarlijke situaties, waar de toegang tot de locatie beperkt is. Bovendien kan het van grote meerwaarde zijn om op een later moment nogmaals de PD te kunnen onderzoeken, bijvoorbeeld bij nieuwe inzichten, in het geval van cold cases of bij langlopende zaken waar nieuwe rechercheurs of specialisten aansluiten. Daarnaast krijgen officieren van justitie ook de mogelijkheid om de PD in detail te bekijken, wat hen als leiders van de opsporingsonderzoeken meer inzicht geeft. Door het integreren van virtueel sporenonderzoek kunnen onderzoekers en rechercheurs niet alleen efficiënter werken, maar ook dieper en gedetailleerder onderzoek doen dan voorheen. Het stelt hen in staat om complexe misdrijven te reconstrueren en te analyseren op manieren die de grenzen van traditioneel onderzoek overschrijden.

VR in de rechtszaal opent nieuwe mogelijkheden voor het beoordelen van bewijs en het begrijpen van complexe scenario's. Het biedt een unieke kans om zaken vanuit een ander perspectief te bekijken. Bovendien kan het rechters ondersteuning bieden bij het beoordelen van alternatieve scenario's wanneer verdachten, die zich eerder beriepen op hun zwijgrecht, met alternatieve scenario's komen tijdens een zitting. Zo kan VR, zoals dit al bij de Puttense moordzaak en de zaak met de overleden baby het geval was, leiden tot meer nauwkeurige en rechtvaardige uitspraken. De toekomst van VR belooft daardoor een diepere en meer gedetailleerde exploratie van de waarheid in forensische en juridische contexten.

Met deze vooruitgang evolueert de forensische opsporing naar een meer geïntegreerde en technologie-gedreven discipline. Deze ontwikkeling verbetert niet alleen de nauwkeurigheid van forensische analyses, maar opent ook nieuwe wegen voor de opleiding en professionalisering van toekomstige forensische experts. Zo ontstaan nieuwe mogelijkheden voor de samenwerking tussen de forensische en tactische rechercheurs, de analisten en mogelijk ook onderzoekers van het Nederlands Forensisch Instituut en andere specialisten. Een groot aantal van hen heeft op dit moment niet de mogelijkheid om de fysieke PD te onderzoeken. Zij vormen nu een tweedehands beeld van de PD op basis van foto's en omschrijvingen in het dossier. Door verschillende specialisten een virtueel PD te tonen, krijgen zij een realistischer beeld en de mogelijkheid om in een vroeg stadium met elkaar te sparren over mogelijke scenario's. Meerdere invalshoeken kunnen eerder overwogen worden, wat een positieve invloed heeft op keuzes in het veiligstellen van sporen, het prioriteren van scenario's en het uitsluiten van alternatieve scenario's.

Conclusie

Nederland behoort tot de wereldtop in 3D-visualisatie en de implementatie van VR in forensische opsporing. De integratie van deze technologie biedt aanzienlijke voordelen, van verbeterde briefings tot gedetailleerde reconstructies in de rechtszaal. Hoewel er uitdagingen zijn, zoals de acceptatie van VR-technologie, infrastructuurbehoeften en databeveiliging, is de potentie onmiskenbaar.
De voortdurende ontwikkeling en wereldwijde interesse in deze technologie benadrukken de rol van VR als een onmisbaar instrument in de toekomst van werk voor de forensische opsporing. Het blijft een spannende tijd voor de forensische wetenschap, met Nederland voorop in deze revolutionaire verandering.

Over de auteurs

Athena van den Busken | Senior Consultant

Athena van den Busken LL.M. MA is recherchekundige en is werkzaam bij Capgemini in het openbare orde- en veiligheidsdomein. Athena specialiseert zich in vraagstukken omtrent verandering, met een focus op de inzet van nieuwe technologieën binnen operationele omgevingen.

athena.vanden.busken@capgemini.com
https://www.linkedin.com/in/athena-van-den-busken/

Anne-Sophie Fritschij | Market Lead Justitie & Veiligheid, Managing Consultant

Anne-Sophie Fritschij LL.M. is als Market Lead Justitie & Veiligheid en Managing Consultant werkzaam bij Capgemini. Zij is gespecialiseerd in het verbeteren van de informatievoorziening binnen de criminaliteitsbestrijding, Virtual Reality in het veiligheidsdomein en wetsimplementatie in de strafrechtketen.

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

Vien Germawi | Senior Consultant

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.

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

Generatieve AI en het vertrouwen in de rechtsstaat

Waar let je op als je in het veiligheidsdomein met kunstmatige intelligentie aan de slag gaat?

Ontdek hoe kunstmatige intelligentie, zoals belichaamd door Gemini en ChatGPT, de wereld transformeert, met specifieke focus op het publieke veiligheidsdomein. Zoals ontwikkelingen van generatieve AI voor getuigenverklaringen.

Highlights:

- Kunstmatige intelligentie biedt het perspectief om veiligheidsvraagstukken te beantwoorden.
- Samenwerking tussen startups en overheid vraagt om wederzijds begrip en inlevingsvermogen.
- De mens centraal stellen is cruciaal in ieder AI project.
- Opschaling van innovaties is kansrijk als eindgebruikers vroegtijdig betrokken zijn.
- Binnen AIWitness wordt op het gebied van getuigenverklaringen verantwoord geëxperimenteerd met (generatieve) AI.

11
Data

Dat kunstmatige intelligentie kansen biedt, is voor de meeste mensen sinds de komst van Gemini en ChatGPT wel duidelijk. AI heeft de potentie om de wereld zoals we die nu kennen en de dingen die we nu doen tot in de kern te veranderen. Dat is een spannend proces waarbij succes en falen elkaar zullen afwisselen. Van belang is dat we experimenteren en dat we dat op een verantwoorde en transparante manier doen. Juist in de veiligheidsketen. AI kan bij uitstek op dit domein een grote maatschappelijke impact hebben. Capgemini neemt, in samenwerking met de Rijksuniversiteit Groningen en Scotty Technologies bijvoorbeeld het voortouw om generatieve AI in te zetten in het kwalitatief beter en sneller verkrijgen van getuigenverklaringen.

Generatieve AI verandert het veiligheidsdomein

Als gevolg van onder andere vergrijzing zien we in het veiligheidsdomein flinke personeelstekorten. In het jaarverslag 2022 constateert ook de politie dat sprake is van een stevig personeelstekort. De komende jaren zullen duizenden nieuwe agenten nodig zijn. Ook de rechterlijke macht en het Openbaar Ministerie kampen met structurele tekorten. Dat heeft consequenties. Zo besloot het OM in Oost-Nederland 1.500 zaken niet voor de politierechter te brengen. Marthyne Kunst, hoofdofficier van Justitie van het parket Oost-Nederland, gaf bij EenVandaag aan te hopen op meer technologische ontwikkelingen die helpen om opsporing sneller te laten verlopen.[1]

Vanuit zakelijk perspectief is het te begrijpen dat gekeken wordt welke zaken wel capaciteit krijgen en welke misdrijven niet. Maar vanuit het perspectief van het slachtoffer blijft dat wrang. Vooral als er genoeg bewijs is om een tot een veroordeling te komen. Het geeft mensen het gevoel dat misdaad loont en dat de rechtsstaat er niet voor hen is. In die zin is het rapport ‘van persoonlijke krenking tot vertrouwensbreuk’ uit 2021 nog steeds zeer relevant.[2] Daarin werd onder andere geconstateerd dat 25% van de Nederlanders geen vertrouwen meer heeft in de instituties van de rechtsstaat. Het gevoel dat anderen worden bevoordeeld en er sprake is van incompetentie draagt hierin bij. Er is noodzaak om te zoeken naar nieuwe manieren die bijdragen aan een rechtvaardige en veilige samenleving.

De hoop van hoofdofficier Kunst in technologische ontwikkelingen is niet ongegrond. Als we kijken naar de markt van generatieve AI dan ontwikkelt die zich snel. In Europa verwacht men een groei van 12,2 miljard in 2023 naar een marktomvang van 56,8 miljard in 2030.[3] Nieuwe toepassingen van generatieve kunstmatige intelligentie worden volop verkend. Binnen het AIWitness-project werken men aan een geaccepteerde oplossing om bruikbare getuigenverklaringen te verkrijgen via generatieve AI. En er zijn meer toepassingen denkbaar in het brede veiligheidsdomein. Zoals het sneller verwerken van asielaanvragen. Rechters kunnen ondersteund worden in het doorspitten van relevante jurisprudentie. En een officier van justitie kan bijvoorbeeld veel sneller dossiers tot zich nemen en vergelijken met andere casussen.

Die nieuwe toepassingen zullen hun weg moeten vinden naar het veiligheidsdomein. Dat is makkelijker gezegd dan gedaan. De snelle wereld van startups en scale-ups, die deze nieuwe toepassingen ontwikkelen, verschilt wezenlijk van complexe overheidsorganisaties die nu eenmaal te maken hebben met langdurige, zorgvuldige processen. Het verbinden van deze twee werelden is één van de centrale opgaven voor de komende jaren om met elkaar maatschappelijke vraagstukken in het veiligheidsdomein te beantwoorden en concreet te werken aan het herstel van vertrouwen in de rechtsstaat.

Vier tips voor veiligheidsorganisaties die met generatieve AI aan de slag gaan

De komende jaren zal het aantal startups op het gebied van generatieve kunstmatige intelligentie flink toenemen. Ook in het veiligheidsdomein worden initiatieven gestart om deze nieuwe technologie te verkennen. Capgemini onderzoekt hoe nieuwe, disruptieve technologieën, zoals generatieve AI, impact hebben op overheidsorganisaties. Op basis van onze ervaringen vier tips voor elke organisatie die aan de slag gaat met generatieve AI.

De eerste tip is het meest fundamenteel, namelijk om in elk generatieve AI-project expliciet de mens centraal te stellen. Of het nu gaat over slachtoffers, daders of professionals, elk initiatief zou moeten gaan over de vraag hoe we het leven van mensen beter maken of niet. Dat geldt in het bijzonder voor het veiligheidsdomein waar het per definitie gaat over kwetsbare mensen. Binnen Capgemini waarborgen we dit principe door een Code of Ethics for AI[4]. Elk project of initiatief waarin onze organisatie meewerkt voldoet hieraan.

De tweede tip gaat ook over mensen, en in het bijzonder medewerkers. Het is van belang om nu al na te denken over de betekenis van generatieve AI voor eigen medewerkers. Binnen bijvoorbeeld AIWitness zien we bijvoorbeeld dat generatieve AI de rol van de menselijke verbalisant over kan nemen. Dat heeft impact op de mensen die nu (regelmatig) verbaliseren, maar ook op de werving van nieuwe medewerkers. In beide gevallen vraagt dit om daar nu al over na te denken. Voor de huidige medewerker die tijd krijgt om andere taken op te pakken en daarvoor wellicht scholing voor nodig heeft. Voor de toekomstige medewerker omdat heel andere vaardigheden gevraagd worden. Bijvoorbeeld het ‘prompten’ (besturen) van generatieve AI tools.

Innovatie zou niet iets moeten zijn van een enkele afdeling of enthousiasteling, maar is de bron waardoor publieke organisaties maatschappelijk relevant blijven. Een derde tip is daarom om meer mensen binnen de organisatie kennis op te laten doen van de (on)mogelijkheden van nieuwe technologie en de betekenis ervan in hun werk. Dat betekent niet dat zij ineens in staat moeten zijn

om bijvoorbeeld zelf te prompten of te programmeren. Zij kunnen wel uitgedaagd worden om nieuwe mogelijkheden te zien om bestaande vraagstukken op te lossen. Het is die creativiteit in de uitvoeringspraktijk die uiteindelijk concreet bijdraagt in het herstel van vertrouwen in de rechtsstaat.

Regelmatig wordt er geëxperimenteerd zonder nauwe betrokkenheid van de 'business', de dagelijkse praktijk. Dat is een belangrijke factor waarom mooie ideeën uiteindelijk toch niet worden opgeschaald. De vierde tip is daarom om zo vroegtijdig mogelijk de eindgebruiker erbij te betrekken. Daar hoort ook bij dat goede ideeën eerst gevalideerd worden. Is de startup waarmee je wil samenwerken stabiel? Is de oplossing wel echt zo baanbrekend of toepasbaar? Is er nagedacht over opschaling als de pilot succesvol is? Welke andere risico's zijn er? Het zijn onder andere deze vraagstukken waar we samen met de overheid naar oplossingen opzoek moeten gaan. Op zoek naar een veiligere Society 5.0.

AI Witness is een voorbeeld van samenwerking tussen verschillende bedrijven en instanties om te komen tot technologische innovatie.

AIWitness: een livinglab

De toepassing van generatieve AI in het veiligheidsdomein is nieuw, spannend en veelbelovend. De mogelijkheden en beperkingen ontdekken we met elkaar. In dat proces is het van belang om stap voor stap op een verantwoorde en transparante manier toe te werken naar een geaccepteerde oplossing voor een specifieke opgave. Capgemini, Rijksuniversiteit Groningen en Scotty Technologies doen dat op het gebied van getuigenverklaringen binnen het voorgenomen livinglab AIWitness.

Technologisch gezien is het ontwikkelen van een geautomatiseerde verbalisant-bot mogelijk. Doorontwikkelde conversational AI gaat daarbij niet alleen het gesprek aan met getuigen, maar biedt hen de mogelijkheid om, in welke landstaal dan ook, te verklaren zonder dat een kostbare tolk ingezet hoeft te

worden. Koppelingen met locatie- en camerafuncties zijn te realiseren en bieden de getuige de mogelijkheid om naast tekstuele verklaringen, aanvullende data toe te voegen aan zijn of haar verklaring. Te denken valt ook aan een zelfgekozen verbalisant-avatar, zodat de getuige zelf een personage kan kiezen waarbij hij of zij zich het meest comfortabel voelt.

Bij een ontwikkeling als deze zijn vele relevante vragen te stellen. Bijvoorbeeld wat een dergelijke oplossing betekent voor betrokkenen. Binnen het livinglab is daar veel aandacht voor. We onderzoeken bijvoorbeeld of mensen daadwerkelijk bereid zijn technologie te gebruiken om verklaringen af te leggen. En of zij zich beter of juist minder gehoord of gezien voelen. Maar ook onderzoeken van juridische (on)mogelijkheden en praktische uitvoeringsproblemen. Dat gebeurt in verschillende 360 graden experimenten waarin we steeds de mens centraal stellen. De mens als getuige, de mens als professional in de keten en de mens als dader. Want uiteindelijk gaat het erom dat technologie werkt voor mensen.

Vandaag aan de slag met de oplossingen van morgen

De komende periode gaat het project AIwitness ervaringen opdoen in verschillende experimenten. Alleen wanneer de gewenste AI-toepassing technologisch, juridisch en ethisch de toets kan doorstaan, wordt de stap naar een pilot op straat gezet. Bij succes is het doel natuurlijk om de oplossing op te schalen.

De eerste zaak waarin een strafrechter uitspraak zal doen aan de hand van een door AI tot stand gekomen getuigenverklaring zal daarom nog even op zich laten wachten. Tegelijkertijd is dat scenario niet enkel toekomstmuziek. Voor professionals betekent dat: bereid u voor op een verdere uitbreiding van AI in uw vakgebied. De vier tips in dit artikel gaan daar ongetwijfeld bij helpen.

Als we dat met elkaar goed doen, ben ik ervan overtuigd dat we samen een positieve bijdrage leveren in het vertrouwen wat burgers mogen hebben in de rechtsstaat en het veiliger maken van onze samenleving.

1. https://eenvandaag.avrotros.nl/item/openbaar-ministerie-kan-door-personeelstekort-sommige-strafbare-feiten-niet-meer-vervolgen-we-moeten-scherper-kiezen/
2. https://repository.wodc.nl/bitstream/handle/20.500.12832/3014/3027-van-persoonlijke-krenking-tot-vertrouwensbreuk-volledig%20rapport.pdf?sequence=1&isAllowed=y
3. https://www.statista.com/forecasts/1449848/generative-ai-market-size-europe#:~:text=The%20European%20market%20for%20generative,of%20the%20decade%20in%202030.
4. https://www.capgemini.com/about-us/who-we-are/our-values/our-ethical-culture/ethical-ai/

Over de auteur

Frederik Peters | Principal Consultant Capgemini

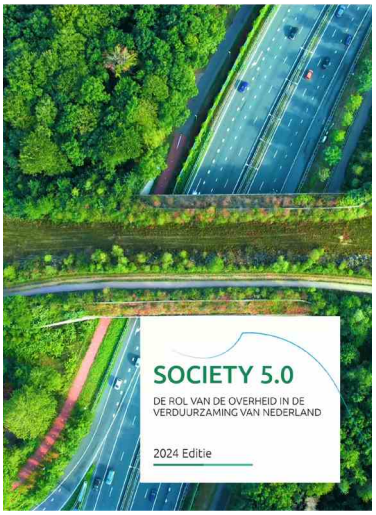
Frederik Peters is Principal Consultant en expert GovTech. Peters heeft jarenlange ervaring in het werken met startups, scale-ups en publieke organisaties. Binnen Capgemini houdt hij zich vooral bezig met de relatie tussen overheid en disruptieve technologie.

frederik.peters@capgemini.com

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

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

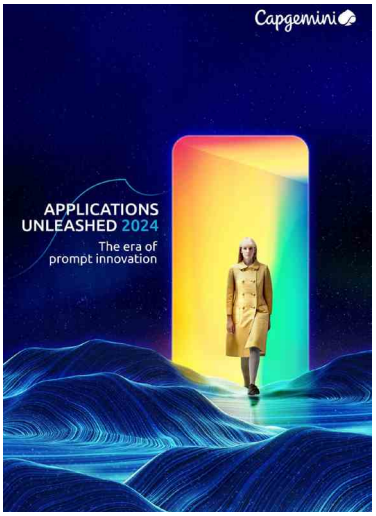


Society 5.0

Wat is de rol van de overheid in de verduurzaming van Nederland

De vierde editie van het society 5.0 rapport biedt een nieuw narratief en praktische handvatten om Society 5.0 toe te passen op duurzaamheidsdoelen. Ontdek hoe de overheid de transitie kan versnellen door inzichten in de rol van de overheid in sociale, bedrijfsvoering- en ruimtelijke transitie te krijgen, strategieën om gedragsverandering te bewerkstelligen en duurzame praktijken te bevorderen, en een kader voor publiek-private samenwerking en het toepassen van digitale technologieën op maatschappelijke uitdagingen in te zien.

https://www.capgemini.com/nl-nl/wat-is-de-rol-van-de-overheid-in-de-verduurzaming-van-nederland/



Applications Unleashed

The Era of Prompt Innovation

De voortdurend evoluerende technologieën van het afgelopen jaar hebben onze wereld hervormd, waardoor directe bevrediging als vanzelfsprekend is geworden. Maar nu de grenzen van innovatie hun hoogtepunt hebben bereikt, rijst de vraag: Wat staat ons te wachten? Hoe ziet de toekomst van het techlandschap eruit? En hoe zal het onze ondernemingen beïnvloeden? De stabiliteit van onze banen? Hoe zal dit weerspiegelen in onze leefomgeving, en een stempel drukken op ons alledaagse bestaan? Deze vragen worden behandeld in Applications Unleashed 2024, waar concrete voorbeelden uit het dagelijkse leven en praktisch toepasbare inzichten een geëffend pad banen naar de baanbrekende ideeën van de toekomst.

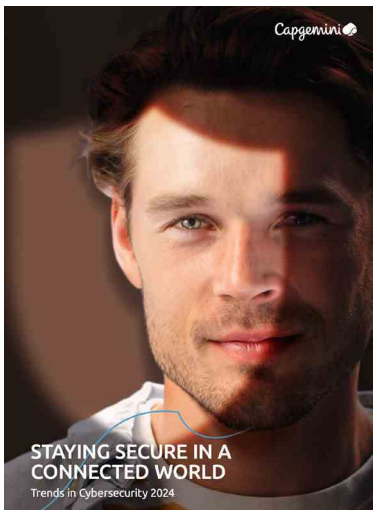
https://www.capgemini.com/nl-nl/applications-unleashed-2024/

The Eco-digital Era

De tweeledige overgang naar een duurzame en digitale economie

In dit rapport van Capgemini Research Institute, The Eco-Digital Era: The dual transition to a sustainable and digital economy, dat is ontwikkeld in samenwerking met het Digital Value Lab van het Digital Data Design Institute aan Harvard, gaan we dieper in op de digitale economie en hoe deze, naast de zakelijke voordelen, het potentieel heeft om aanzienlijke ecologische en sociale waarde te bieden.

https://www.capgemini.com/insights/research-library/the-new-digital-economy-research/



Trends in Cybersecurity

Veilig blijven in een verbonden wereld - Capgemini Nederland

Trends in Cybersecurity 2023, het rapport dat speciaal is samengesteld voor senior cybersecurity professionals. In een wereld die steeds verder met elkaar verbonden is, staat veiligheid centraal. Deze nieuwste editie biedt waardevolle inzichten om jouw organisatie te beschermen tegen moderne bedreigingen.. Dit rapport biedt een uitgebreide behandeling van deze thema's en meer, waarbij we verder ingaan op de trends en uitdagingen die de kern vormen van een robuuste beveiligingsinfrastructuur.

https://www.capgemini.com/nl-nl/trends-in-cybersecurity-veilig-blijven-in-een-verbonden-wereld/

Colofon

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

- Natasja Pieterman
- Erik Staffeleu
- Martijn van de Ridder
- Marcel Kordes
- Aydan Gunduz
- Thomas de Klerk
- Ernes Mahmutovic
- Bas Koper
- Ismay van de Water

Advies, ontwerp en productie:

Marketing & Communicatie, Capgemini Nederland B.V.

- Johanna Achterberg
- Arindam Dey
- Puja Sengupta

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 360,000 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 50 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

2D-017.24