TRENDS IN VEILIGHEID 2022-2023

Het veiligheidsdomein als baken in dynamische tijden

Dit rapport is opgedragen aan onze dierbare collega en zeer betrokken lid van de stuurgroep Trends in Veiligheid

Zeger de Bruijne†

Pablo Derksen, Martijn van de Ridder, Erik Staffeleu, Thomas de Klerk, Judith Groenewoud, Jule Hintzbergen en Marcel Kordes

TRENDS IN VEILIGHEID 2022-2023

Het veiligheidsdomein als baken in dynamische tijden

INHOUDSOPGAVE

WAT ZIEN DE BESTUURDERS UIT HET VEILIGHEIDSDOMEIN?

In Europa en Nederland is het afgelopen jaar veel gebeurd binnen het veiligheidsdomein. Wat is de invloed van de toeslagenaffaire, het log4j incident en de krapte op de arbeidsmarkt op het veiligheidsdomein? Wij gingen in gesprek met 15 bestuurders van de grote organisaties in het veiligheidsdomein. Bestuurders uit het veiligheidsdomein stellen dat het veranderingsvermogen van de veiligheidsorganisaties van cruciaal belang is gebleken in de afgelopen twee jaar. Er moet een nieuwe balans gezocht worden tussen de oude en nieuwe manier van werken terwijl de veiligheid geborgd blijft. Dit brengt allerlei uitdagingen met zich mee, terwijl Europa alweer wordt geconfronteerd met de volgende crisis. De vraag rijst waar het veiligheidsdomein staat halverwege dit decennium.

Gezamenlijk concluderen wij en de bestuurders dat de digitalisering van onze samenleving inmiddels tot onze haarvaten is doorgedrongen. Digitalisering is niet langer enkel ondersteunend, we zijn er compleet afhankelijk van geworden. Neem onze persoonlijke levens: een drankje op het terras bestel je tegenwoordig via een QR-code of app. Winkelen, colleges volgen en vergaderen vinden deels online of hybride plaats. Naast dat deze ontwikkelingen onze samenleving sterk Deels online en hybride is hetzelfde lijkt me? veranderd heeft, is de impact ook voelbaar binnen het veiligheidsdomein. Hier heeft het werk zich verplaatst van een grotendeels fysieke naar een nieuwe hybride manier van werken.

Innovatie in het veiligheidsdomein: ‘A person says no’

Net als in de afgelopen jaren blijkt innovatie een belangrijk thema te zijn binnen organisaties in het veiligheidsdomein. Tot op heden hebben technologische mogelijkheden een belangrijke rol gespeeld binnen de vernieuwing in het veiligheidsdomein. Naast dat dit vaak mooie en goede innovaties oplevert, kan het tegelijkertijd soms ook verkeerd uitpakken. Bestuurders wijzen op het belang van het centraal stellen van de burger binnen innovatie en vernieuwing.

Een belangrijk en schrijnend voorbeeld van hoe dit verkeerd kan uitpakken, is de toeslagenaffaire. In deze affaire, werden duizenden ouders, als gevolg van het toepassen van een discriminerend risicomodel op basis van AI door de fiscus, onterecht als fraudeur bestempeld. Dit met alle negatieve gevolgen van dien. Een voorbeeld als dit benadrukt het belang van de menselijke component in innovatie. Zoals beschreven in hoofdstuk 9 van dit TiV-rapport, bestaat ‘unbiased’ Artifical Intelligence anno 2022 nog niet[1].

De geïnterviewde bestuurders uit het veiligheidsdomein benadrukken het belang van de menselijke rol in het uitvoeren van de processen. Processen, nu vaak nog gedigitaliseerd, worden door de komst van nieuwe technieken geautomatiseerd. Hierbij moet automatisering onlosmakelijk verbonden zijn met menselijk handelen. Het is niet langer de “computer says no”, maar “a person says no”. Deze verantwoordelijkheid zal altijd zo blijven. Deze ontwikkeling doet een beroep op een solide ethische afweging bij innovatie(s). Bij het ontwerpen van processen en het toevoegen van nieuwe innovaties dient dit vooraf te worden meegenomen en afgewogen te worden.

De burger centraal in een informatie gestuurde wereld

Een succesvolle doorontwikkelde innovatie binnen het veiligheidsdomein is het gebruik van sensoren en data in de opsporing. Een belangrijk voorbeeld hierbij is de snelle opsporing van de verdachten van de moordaanslag

op Peter R. de Vries op 6 juli 2021. Dankzij beveiligingscamera's van particulieren en bedrijven, automatische kentekenplaatherkenning (ANPR) en aanvullende getuigenverklaringen kon de politie de vluchtauto van de verdachten van de moordaanslag een uur later aanhouden op de A4 bij Leidschendam. Dit is een belangrijk voorbeeld van hoe informatie gestuurd werken kan bijdragen aan een snelle opsporing. Een opsporingsonderzoek gericht op het pakken van de verdachten had heel veel capaciteit gekost. Capaciteit die nu ingezet kan worden in de onderbouwing van de zaak of in andere opsporingsonderzoeken.

De bestuurders (h)erkennen de cruciale rol van datamanagement voor het goed functioneren van hun organisaties. Bij het verzamelen, verwerken en inzetten van data komt een heel ecosysteem kijken. Dit vereist dat de eigen en ketenprocessen helder worden beschreven en dat er exact duidelijk is op welke manier data verzameld wordt. Volgens bestuurders spelen ethiek, privacy en security hierbij een enorm belangrijke rol. Zij zijn zich hierbij terdege bewust van de andere kant van de medaille van dataverzameling en verwerking: de mogelijke perceptie van Nederlanders dat zij in een surveillancestaat wonen.

De verwachting van bestuurders is dat mensen, voertuigen en wapens alleen maar slimmer zullen worden in de toekomst. Deze worden meer en meer uitgerust met sensoren om data te verzamelen en zijn daarmee een voedingsbodem voor informatie gestuurd werken. Zoals ook de ontwikkelingen rondom nieuwe technologieën als de cloud en AI die informatie gestuurd werken een push gaan geven. Ook hier geldt wederom dat de burger centraal moet blijven staan en dat er oog moet blijven voor de ethische aspecten.

In dat kader wordt door de bestuurders gewezen op een groeiende behoefte om op slimme wijze data tussen organisatie te vergelijken zonder daadwerkelijk de informatie uit te wisselen. Uit de ervaringen van de bestuurders blijkt dat dit in de praktijk nog niet altijd even makkelijk is door wetgeving zoals de AVG. De wil om meer en beter samen te werken is er meer dan ooit. Zowel tussen overheidsorganisaties als met private partijen. Een knelpunt hierin is het verschil in volwassenheid van de IT organisaties. dit is een legacy uitdaging die de digitale samenwerking nog bemoeilijkt.

Digitale veiligheid staat prominent op de bestuurders agenda

Niet alleen verandert de huidige wereld voor de inwoners van Nederland en de organisaties in het veiligheidsdomein, ook de criminaliteit en dreiging van buitenaf verschuiven van de fysieke naar de digitale wereld. Sinds 2012 neemt de traditionele criminaliteit al af en zit de online criminaliteit in de lift[2]. Covid 19 heeft dit versterkt, onder andere door de grote toename van virtuele activiteiten, onzekerheid met betrekking tot informatie en wantrouwen in instituties en de overheid[3]. Dit doet een beroep op de digitale weerbaarheid van de Nederlander.

Geconstateerd wordt dat de digitale veiligheid achterblijft ten opzichte van de digitalisering en dus extra aandacht behoeft. Bestuurders geven aan dat via de CISO's van de verschillende organisaties security continu prominent op de agenda van de bestuurders wordt gezet. Lees hiervoor ook het interview met Hans De Vries (hoofdstuk 1). Het Log4J incident eind november 2021, waarin kwetsbaarheid in deze zeer veel gebruikte software tot cyberaanvallen leidde, toont deze noodzaak nogmaals aan. Alle prioriteit ging uit naar het mitigeren van de risico's die deze software met zich meebracht.

De bestuurders pakken de uitdagingen op het gebied van digitale veiligheid op diverse manieren aan. Er worden budgetten vrijgemaakt om software en infrastructuur veilig te maken en houden. Security wordt 'by design' meegenomen in de ontwikkeling van nieuwe systemen. Dit geldt ook voor privacy en ethiek. Daarnaast worden ook specifieke teams opgericht als 'flying squads' om in te vliegen wanneer nodig. Het tegenovergestelde is ook waar, bestuurders geven aan dat er weinig tot geen ruchtbaarheid gegeven wordt aan jubilea van diensten die stabiel en veilig zijn om niet de aandacht te trekken van kwaadwillenden. Er gaat dus ook veel goed.

Door het gedistribueerd werken ontstaan er nieuwe vraagstukken rondom veiligheid. Hoe weet je dat medewerkers thuis veilig kunnen werken? Dat privacygevoelige informatie vernietigd wordt en welke verantwoordelijkheid bestaan hierin? Dit zijn vragen waar nog niet direct een antwoord op is maar die wel op de radar staan van de bestuurders.

De zoektocht naar talent

Corona heeft de samenwerking tussen medewerkers en organisatie blijvend veranderd. Veel organisaties gingen in de lockdowns van een kantoorcultuur naar een virtuele en later hybride werkcultuur. Volgens de bestuurders is deze nieuwe manier van werken een blijvertje, niet in de laatste plaats om het duurzaamheidaspect ervan. Wel vereist dit de nodige inspanningen voor het voortzetten van de werkzaamheden. Een bijkomende, overstijgende uitdaging voor organisaties is het aantrekken en behouden van de juiste mensen en expertise om het werk in het veiligheidsdomein goed te kunnen blijven uitvoeren. In een krappe arbeidsmarkt, waarin de vraag naar nieuw talent vele malen groter is dan het aanbod hiervan, vissen organisaties binnen het veiligheidsdomein vaak in dezelfde vijver of 'concurreren' zij met private organisaties. Met zijn allen blijven vissen in een kleiner wordende vijver lijkt geen houdbare strategie.

Veel geïnterviewde bestuurders zijn het erover eens dat de groei en innovatie van organisaties valt of staat met voldoende werknemers die beschikken over de juiste vaardigheden. Als het niet langer lukt om gekwalificeerd personeel van buiten aan te trekken, dient hierop geanticipeerd te worden en moet in de eigen organisatie gekeken worden of het mogelijk is om personeel bij- of om te scholen. Een strategische personeelsplanning (SPP) kan hierin uitkomst bieden.

Tegelijkertijd wijzen de bestuurders erop dat ook innovatie een rol speelt bij het aantrekken en behouden van medewerkers. Er wordt tijd en geld gereserveerd voor innovaties, dit gebeurt al in het ontwikkelproces, gebaseerd op best practices vanuit bijvoorbeeld het SAFe framework. De verwachting is dat er kruisbestuiving zal plaatsvinden binnen de organisatie. Nieuwe ideeën worden opgedaan en er wordt geëxperimenteerd met nieuwe technologieën. Zonder direct de verwachting te hebben dat alles geïmplementeerd wordt in de werkprocessen. Geld wordt gereserveerd om de meest kansrijke ideeën op te pakken en verder uit te werken. De medewerker staat hierbij centraal en niet de productie, een delicate balans.

Conclusie

Iedere bestuurder vanuit de verschillende geïnterviewde organisaties van het veiligheidsdomein bevestigt de grote lijnen: digitalisering is versneld en verschoven van ondersteunend naar uitvoerend en daarmee van essentieel belang geworden voor de organisatie. Innovatie is belangrijk om te blijven vernieuwen en moet ingebed worden in het ontwikkelproces. Ook blijkt het een manier om medewerkers te behouden. Aan de andere kant moet er oog zijn voor de burger en is ethiek, net zoals security en privacy, van essentieel belang en is het absoluut noodzakelijk om dit 'by design' te doen. Door de verschuiving van een fysieke naar een hybride samenleving is er ook een verschuiving in criminaliteit en dreigingen die vragen om nieuwe antwoorden.

In het komende decennium gaat de digitalisering verder toenemen en worden stappen gezet in de verdere professionalisering binnen het veiligheidsdomein. Dit zal een transformatie in werking zetten van alle organisaties, zowel in de uitvoering van de primaire processen als in de ondersteuning van alle organisaties. Ieder levend systeem, zoals onze samenleving ook is, heeft een zekere mate van dynamiek nodig om zich aan te kunnen passen aan veranderingen, maar ook stabiliserende elementen om te voorkomen dat de samenhang verloren gaat. Een steeds verder professionaliserend veiligheidsdomein is zo'n waardevol stabiliserend element. Een baken in dynamische tijden.

Over de auteurs

Marcel Kordes
Director public sector

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

Erik Staffeleu
Senior Director public sector

Erik Staffeleu is Senior Director in de publieke sector en onder andere verantwoordelijk voor de adviesgroep Veiligheid en Rechtsketens. Erik is veranderkundige en een ervaren adviseur binnen het veiligheidsdomein. Zijn opdrachten liggen veelal op het vlak van strategievorming en organisatieontwikkeling.

[1]AI zonder bias is een leugen
[2]https://www.cbs.nl/nl-nl/nieuws/2022/09/minder-traditionele-criminaliteit-meer-online-criminaliteit
[3]https://vng.nl/rubrieken/onderwerpen/maatschappelijke-onrust-en-desinformatie

01

TRENDS IN DIGITALE VEILIGHEID: IN GESPREK MET HANS DE VRIES, DIRECTEUR NCSC

Wat zijn de belangrijkste trends en ontwikkelingen om onze samenleving digitaal veilig te houden?

Trends in veiligheid kan tegenwoordig niet meer zonder de specifieke blik op trends in digitale veiligheid. In 2021 nam Hans de Vries, Directeur van het Nationaal Cybersecurity Centrum deel in de paneldiscussie tijdens de webcast Trends in Veiligheid 2021[1]. In een levendige discussie gaf hij aan dat er in het rapport meer aandacht mocht zijn voor de trends in digitale veiligheid.

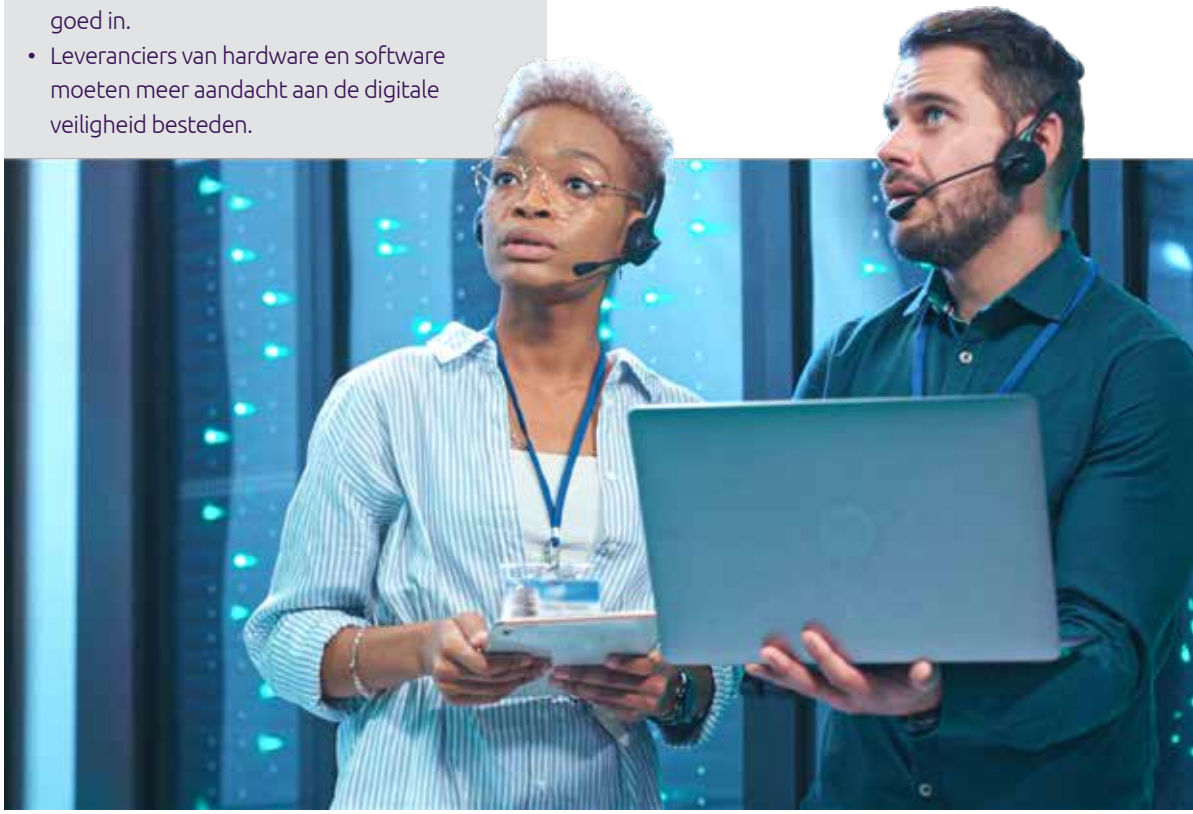
Highlights

- We werken steeds meer digitaal en gedistribueerd en de digitale veiligheid blijft achter.
- Om veiliger te worden is een stelsel met duidelijke rolverdeling tussen publiek, privaat en overheid cruciaal, het mandaat voor het NCSC moet breder.
- Voor het ontvangen van relevante informatie vanuit de overheid moet het niet uitmaken of je 'vitaal' bent of niet.
- Onze rol als digitaal knooppunt in Europa is niet alleen technisch we hebben de taak om partijen met elkaar te verbinden, daar zijn we goed in.
- Leveranciers van hardware en software moeten meer aandacht aan de digitale veiligheid besteden.

Die handschoen pakken wij natuurlijk graag op in het rapport van 2022. In gesprek met Hans bespreken wij de laatste trends die hij ziet om de Nederlandse samenleving digitaal veilig te maken. Nu de meeste coronamaatregelen zijn vervallen en aan de oostgrens van Europa veel aan de hand, is dit onderwerp urgenter dan ooit tevoren.

Digitalisering en veiligheid

Afgelopen twee jaar is onze samenleving sneller gedigitaliseerd dan de vijf jaar hiervoor. In het huidige regeerakkoord is een volledige paragraaf gewijd aan 'digitalisering'. Erkend wordt dat "de huidige digitale revolutie geweldige kansen biedt voor onze samenleving en economie", maar tegelijkertijd zorgt "voor een digitale kloof en groeiende ongelijkheid in onze samenleving". Welke digitale trend was afgelopen jaar dominant voor de digitale veiligheid in Nederland? Hans: "Wat mij betreft is de dominante trend in 2021 dat door de coronacrisis gedistribueerd werken in hoog tempo is doorontwikkeld en dat digitale veiligheid hierbij achterblijft en aandacht behoeft."



Afgelopen twee jaar is onze samenleving sneller gedigitaliseerd dan de vijf jaar hiervoor. In het huidige regeerakkoord is een volledige paragraaf gewijd aan 'digitalisering'. Erkend wordt dat "de huidige digitale revolutie geweldige kansen biedt voor onze samenleving en economie"

Waaruit blijkt dat de digitale veiligheid achterblijft bij de snelheid van digitalisering? "Dit komt onder andere tot uitdrukking in de vragen die wij van CISO's krijgen. Zij vragen hulp om cybersecurity op de agenda van de bestuurder te zetten. Het wordt beter maar we moeten blijven benadrukken dat digitale veiligheid 'chefsache' is. **Cyber is veel meer dan techniek alleen.** Er wordt nog te weinig aan risicomanagement gedaan door organisaties. Te vaak zien we dat organisaties niet nadenken over de keten waarin ze zich bevinden of het wordt pas gedaan als het te laat is. Ook zijn er voldoende voorbeelden dat het updaten van software met de laatste versie ('patch gedrag') niet past bij de afhankelijkheid en kwetsbaarheid van digitale systemen."

Van welk cybersecurity incident heb je afgelopen jaar het meest 'wakker gelegen'? Hans: "Dat is de problematiek rondom kwetsbaarheden zoals in Log4j, een door IT-ontwikkelaars veelgebruikt softwareproduct. Dit product wordt gebruikt voor het vastleggen van input van buitenaf in software op een server. Bijvoorbeeld een inlogpoging. Maar dit soort software zit in vele honderden, zo niet duizenden softwareproducten en applicaties. De vergelijking met suiker wordt vaak gemaakt: bijna in ieder levensmiddel zit wel suiker, ook waar je het misschien niet verwacht. Daarom is het moeilijk om zicht te hebben op de omvang van misbruik en kan impact reusachtig zijn."

Hoe ontwikkelt de digitale veiligheid zich in Nederland?

Hans: "Zoals gezegd, als gevolg van COVID-19 is de digitalisering van de maatschappij versneld. Dat betekent dat nog meer dan voor de pandemie een zwaar beroep wordt gedaan op de digitale ruimte. Digitalisering biedt onze maatschappij volop kansen en oplossingen, maar zorgt ook voor een groter aanvalsoppervlak waarin criminelen en statelijke actoren snel kunnen inspelen op het uitbuiten van nieuwe kwetsbaarheden."
Wat betekent dit voor de digitale risico's? "De digitale risico's zijn onverminderd groot: denk daarbij aan spionage en sabotage door andere landen maar ook ransomware aanvallen door criminelen. Dit kan maatschappelijk ontwrichtende gevolgen hebben. De digitale dreiging blijft zich ontwikkelen, de impact van cyberaanvallen neemt toe en de weerbaarheid is nog onvoldoende."

Hoe gaat het bedrijfsleven en onze vitale infrastructuur hiermee om?

"Er zijn er grote verschillen in weerbaarheid tussen bedrijven die kunnen investeren in kennis en kunde op het gebied van cybersecurity en (veelal kleine) bedrijven die niet de middelen hebben om de weerbaarheid naar een hoger plan te tillen. In het bedrijfsleven is cybersecurity nog steeds onvoldoende onderdeel van volwassen risicomanagement en daardoor blijven investeringen uit die dat risico reflecteren. Toch is er goed nieuws: tijdens Log4j zag je dat organisaties, ook buiten de ICT-afdeling, meteen op scherp stonden en hebben gehandeld. Een inhaalslag is nodig om Nederland weerbaarder te maken. Het is tijd om naast de fysieke infrastructuur (weg, spoor, water en lucht) ook de digitale infrastructuur waar Nederland van afhankelijk is op orde te brengen."

Vanuit de overheid zetten we nu volop in op een ‘landelijke dekkend stelsel’ om potentiële slachtoffers van cyberaanvallen tijdig te informeren, maar tegelijkertijd merken we dat we daar nog niet zijn en het landschap nog te versplinterd is. Goede nationale coördinatie is echt nodig in cybersecurity en daarbij moet het NCSC de spilfunctie in het midden vervullen.

Structurele samenwerking

In het huidige regeerakkoord wordt gepleit om het bedrijfsleven beter te beschermen en beter informatie te delen, door middel van een structureel samenwerkingsverband en een meerjarige cybersecurity-aanpak.
Hoe ziet deze meerjarige cybersecurity aanpak er idealiter voor jou uit?
“We moeten als Nederland voldoende slagkracht organiseren om de toenemende dreiging het hoofd te kunnen bieden. Dat betekent: de vrijblijvendheid is voorbij en geen versplintering in de aanpak, maar juist samenhang. Belangrijk daarbij is samenwerking tussen publiek en privaat binnen overheid, een stelsel met duidelijke rolverdeling en groter mandaat voor NCSC (dus niet alleen meer overheidsorganisaties en Vitale infrastructuur, maar een bredere doelgroep).”

Ook volgens de Cyber Security Raad (CSR) moet Nederland de krachten bundelen om te komen tot een integrale aanpak van onze cyberweerbaarheid en werken aan één cyberweerbaarheidsstrategie met een meerjarenprogramma en dekkende financiering. Zij pleiten voor een bijbehorende investering van € 833 miljoen. Besteedt Nederland voldoende aan digitale veiligheid? Is er een verbetering zichtbaar in de budgetten voor het veiliger maken van onze huidige digitale wereld?
Hans: “Het wordt beter, maar we hebben nog wel echt een weg te gaan. Het is fijn dat er meer middelen beschikbaar komen naar aanleiding van het coalitieakkoord. Dat is enorm nodig. Het is misschien niet de € 833 miljoen waar de CSR om vroeg maar met het geld dat er wel extra komt voor cybersecurity kunnen we ook al belangrijke dingen gaan doen, ook bij het NCSC. Ten behoeve van ons allemaal.“

Stap voor stap beter in digitale veiligheid

In het OVV Rapport ‘Kwetsbaar door software’ stelt haar voorzitter Jeroen Dijselbloem: “Aanpak digitale veiligheid moet anders”: De Nederlandse aanpak van digitale veiligheid moet snel en fundamenteel veranderen om te voorkomen dat de maatschappij ontwricht raakt door cyberaanvallen. Uit de casus ten aanzien van de kwetsbaarheden in software van Citrix concludeert de OVV dat Nederlandse overheidsorganisaties en bedrijven zeer kwetsbaar zijn voor cyberaanvallen en dat er geen nationale structuur is waarbinnen alle potentiële slachtoffers van cyberaanvallen tijdig worden gewaarschuwd.” Wat kan er aan de waarschuwing verbeteren en hoe kan publiek-private samenwerking hieraan bijdragen?
Hans: “Waar ik heel blij mee ben, is de al bestaande samenwerking tussen publiek, privaat, wetenschap en non-profit. Denk aan bijvoorbeeld onze samenwerking met Cyberveilig Nederland of DIVD, partijen die hun eigen verantwoordelijkheid willen nemen als het gaat over onze digitale veiligheid. Zij weten ons te vinden en te informeren en vice versa. Ik ben trots op deze publiek-private samenwerking in Nederland. Dit is iets wat je in andere landen echt met veel meer moeite van de grond ziet komen. Maar ook in Nederland kan het intenser.“

Welke andere acties worden genomen?

“Vanuit de overheid zetten we nu volop in op een ‘landelijke dekkend stelsel’ om potentiële slachtoffers van cyberaanvallen tijdig te informeren, maar tegelijkertijd merken we dat we daar nog niet zijn en het landschap nog te versplinterd is. Goede nationale coördinatie is echt nodig in cybersecurity en daarbij moet het NCSC de spilfunctie in het midden vervullen. Het NCSC zou daarbij meer mandaat moeten hebben om organisaties te waarschuwen als dat nodig is. Een eerste stap is daarvoor het wetsvoorstel dat binnenkort in het parlement behandeld wordt waarmee de mogelijkheden voor het NCSC om informatie te delen worden vergroot. Als het voorstel uiteindelijk wetgeving wordt, zal het NCSC meer dreigingsinformatie kunnen delen met organisaties die niet onder de ‘vitale infrastructuur’ worden geschaard. Daarnaast is ook een wetsvoorstel ingediend dat het Digital Trust Center voorziet van een wettelijke grondslag om dreigingsinformatie, inclusief persoonsgegevens, te gaan delen met het niet-vitale bedrijfsleven. Voor het ontvangen van informatie vanuit de overheid die voor jouw organisatie van belang is, moet het mijns inziens niet uitmaken of je ‘vitaal’ bent of niet.“

Op welke wijze gaat de overheid organiseren dat overheden, bedrijfsleven, ‘vitaal’ en ‘niet-vitaal’ digitale veiligheid beter op orde hebben?

“Er zijn natuurlijk al allerlei normen zoals BIO, NEN 7510, et cetera en bestaande wetten zoals WBNI en de AVG. Een grote verandering is wel aanstaande met de vernieuwde Europese NIS2-richtlijn. De huidige wetgeving is voornamelijk georiënteerd op vitale, of essentiële, sectoren en organisaties, maar daar gaat dus verandering in komen. Als de verbreding van de NIS2 doorgaat en organisaties van zowel de categorie ‘essential’ als ‘important’ moeten voldoen dan is deze scope veelvoudig van wat het nu is. Al deze partijen gaan te maken krijgen met een verzwaard toezicht op het naleven van cybersecurity eisen en standaarden. Ik zeg wel vaker dat we de vrijblijvendheid voorbij moeten en deze Europese wetgeving biedt daar een goede basis voor. We moeten ook meer de durf hebben om te zeggen: hier moet je je echt aan houden. We moeten de druk op opvoeren om de weerbaarheid bij zowel publiek als privaat naar een nieuw niveau te tillen.”

Nederland is een Europees digitaal knooppunt

Nederland is ambitieus. Alle delen van het land moeten robuust, veilig en supersnel internet krijgen om het digitale knooppunt van Europa te worden. Onze regering wil het voortouw nemen en zet op Europees verband in op ‘versterking van de samenwerking tussen lidstaten op het gebied van digitalisering, onder meer op mensgerichte inzet van kunstmatige intelligentie, digitale ethiek, ontwikkeling van digitale identiteit en cybersecurity en ‘open source’.’ Wat moet er nog gebeuren om een veilig digitaal knooppunt van Europa te worden?

Hans: "Met AMS-IX heeft Nederland letterlijk een belangrijk internetknooppunt van Europa binnen haar grenzen. Hier moeten we er dus zorg voor dragen dat er niet alleen sprake is van snel, maar ook vooral van veilig internet. Ik zou onze NCSC-rol als digitaal knooppunt wel veel breder willen trekken. Dit gaat onder andere om de taak die we hebben om partijen met elkaar te verbinden, iets waar we in Nederland goed in zijn en dus ook in Europa het voortouw in kunnen nemen. Er ligt een evidente meerwaarde in Europese samenwerking, we zijn immers

met elkaar verbonden. Tegelijkertijd is betere en strakke coördinatie op Europees niveau in tijden van crisis nodig en ook dat is iets waar wij aan kunnen bijdragen. We laten vaak genoeg zien dat we als Nederlanders weten hoe we samenwerkingsverbanden kunnen optuigen, ook als er zowel publieke en private partijen betrokken zijn. Daarnaast hebben we ook genoeg kennis en expertise in huis die we kunnen inbrengen en ontsluiten, denk bijvoorbeeld aan onze ervaring met ISACs of ons Coordinated Vulnerability Disclosure beleid. Overigens gaat dit allemaal verder dan alleen Europa, het is ook van belang om de mondiale samenwerking op te zoeken en bijvoorbeeld bij te dragen aan capaciteitsopbouw in minder ontwikkelde landen. Ook op dit niveau geldt dat we zo sterk zijn als de zwakste schakel. Ten slotte mag de Nederlandse slagkracht om te kunnen acteren tegen statelijke actoren en criminelen best versterkt worden. Dit is niet voor het NCSC weggelegd, maar de digitale slagkracht om onze nationale belangen te verdedigen mag een belangrijk onderdeel worden van een nieuwe cybersecurity aanpak."

Welke trends in digitale veiligheid mag vooral niet onbenoemd blijven om een goed voorbereid te zijn op de steeds verdergaande digitalisering.

"De belangrijkste overkoepelende trend is dat we door de coronacrisis versneld afhankelijk zijn geworden van de digitale levensader. Het is belangrijk hierbij voldoende aandacht aan de digitale veiligheid te besteden. Ik hoop dus in de eerste plaats dat bij iedereen en misschien wel vooral bij leveranciers (van hardware en software) het besef doordringt dat het gebruik van digitale functies van al onze apparaten onlosmakelijk verbonden is met het zorgdragen voor de veiligheid daarvan. Het is zo een integraal onderdeel van ons 'zijn' geworden dat je daar op die manier naar moet kijken, handelen en durven te acteren. Dit vereist een fundamentele andere kijk. Het gebruik van een 'Software Bill of Material' (beschrijving welke software er in een product zit) is hierin een goede ontwikkeling."

"Andere trends om in de gaten te houden zijn de mogelijke effecten van grondstoffen schaarste en van klimaat/ duurzaamheid maatregelen op de beschikbaarheid en inzet van ict-middelen. De recente ontwikkelingen in Oekraïne laten ook weer zien dat het risico op de inzet van digitale middelen in conflicten met bovenregionale uitstraling reëel is."

Over de auteurs

Roeland de Koning

Director Public Security

Roeland is gespecialiseerd in nationale en internationale ISACs samenwerkingsvraagstukken tussen organisaties die werken aan digitale veiligheid en cybersecurity.

roeland.de.koning@capgemini.com

Fokko Dijksterhuis

Managing Consultant Cybersecurity

Fokko is gespecialiseerd in (internationale) samenwerking en cyber crisismanagement in het digitale veiligheidsdomein. Fokko houdt zich daarnaast bezig met beleidsmatige, organisatorische en gedragsmatige vraagstukken binnen cybersecurity.

fokko.dijksterhuis@capgemini.com

[1]https://www.trendsinveiligheid.nl/live-webcast/

02

DE LANGE LAT TEGEN RANSOMWARE

Hoe de politie een effectieve vuist maakt tegen de exponentiële groei van ransomware

Ransomware-aanvallen vormen een groeiende bedreiging voor de samenleving. De politie weet met een gestructureerde aanpak een vuist te maken tegen deze plaag

Highlights

- Ransomware is een dreiging tegen onze nationale veiligheid geworden.
- De criminelen opereren in een geprofessionaliseerd ecosysteem.
- De politie pakt met datakennis onderliggende criminele patronen aan.
- Naast boeven vangen wordt ingezet op slim voorkomen en verstoren.
- Het kan iedereen overkomen, bedrijven kunnen zich wel beter wapenen.

De vlag kan uit in Driebergen. Tien jaar geleden werd daar begonnen met een gerichte intensivering van de cybercrime-aanpak, die landelijk en internationaal navolging heeft gekregen. Hoewel ransomware inmiddels als een gevaarlijk groeiende wolk boven de samenleving hangt, wordt het politiekorps steeds effectiever bij het bestrijden ervan. In dit artikel leggen we uit wat ransomware is en hoe de politie met datagedreven werken, slimme samenwerkingen en alternatieve interventies werkt aan het indammen van dit gevaar voor onze nationale veiligheid[1].

Wat is ransomware en hoe groot is het probleem?

Ransomware (letterlijk: gijzelprogrammatuur) is een criminaliteitsvorm waarbij misdadigers op afstand systemen onklaar maken en gegevens versleutelen om losgeld (ransom) te eisen van het slachtoffer. Hierbij worden ook aangesloten back-ups beschadigd. Om de data terug te krijgen, moet het slachtoffer betalen. Steeds vaker dreigen de criminelen daarnaast om gevonden vertrouwelijke informatie te publiceren. Soms worden ook klanten, partners of andere partijen afgeperst. Nadat het slachtoffer heeft betaald (vaak via cryptogeld zoals bitcoins) zou de bedrijfsvoering hersteld moeten zijn, beweren de criminelen. In praktijk gebeurt dat lang niet altijd of blijven er achterdeurtjes achter waarna – een poos later – een nieuwe afpersing volgt.

Hoe werkt een ransomware-aanval?

Een ransomware-aanval is onderdeel van een breder proces in een groot crimineel ecosysteem[2]. Er zijn cybercriminelen die zich richten op het aanvallen van veel individuen en kleine bedrijven in één golf, terwijl professionele groepen soms maanden investeren in het binnendringen en onderzoeken van de financiële bewegingsruimte van één groot bedrijf, uiteindelijk leidend tot een op maat vastgestelde losgeldeis, die dan in de tonnen of zelfs miljoenen kan lopen. Vanwege het financiële gewin is er sprake van een

volwassen, transnationale schaduweconomie waar kopers en verkopers handelen, investeren en diensten aan elkaar verlenen. Elke aanval kent verschillende fases met eigen stappen en technieken[3]. Zo heb je een Initial Access Broker die toegang verkoopt tot gekraakte netwerken, waarbij vaak via phishing de allereerste toegang is geforceerd. Er is een Affiliate die de daadwerkelijke aanval uitvoert en gegevens doorsluist. Dan is er de Operator die de software beheert en de gegevens versleutelt. Ook is er een team voor 'klantcontact' om de transactie te laten slagen. Ten slotte moet het afgeperste geld worden witgewassen voor je het kunt uitgeven; ook daar is dienstverlening voor.

Afbeelding 1: verschillende stappen in Ransomware

Hoe groot is het probleem in onze samenleving?

Ransomware is 'big bad business'. Het wordt inmiddels gezien als de meest voorkomende en lucratieve vorm van cybercrime, met doorlopende aanvalsgolven vanuit georganiseerde criminele netwerken[4]. Alleen al het verhandelen van toegang tot gehackte computersystemen die vervolgens aangevallen kunnen worden is een industrie op zichzelf geworden. Vanwege het gemak van cryptovaluta en het solide verdienmodel wordt digitale afpersing steeds populairder. Wereldwijd was er sprake van een explosieve groei van 715% van het aantal meldingen van ransomware-gevallen tussen 2019 en 2020[5].

Aan de andere kant staan de slachtoffers. Schattingen van de totale schade van ransomware, in de zin van betaald losgeld, verlies aan bedrijfscontinuïteit, gevolgschade en herstelkosten, lopen wereldwijd in de miljarden euro's per jaar en dit bedrag groeit exponentieel[6]. Naast de reputatieschade en de financiële kosten kunnen door keteneffecten veel bedrijven niet meer werken na een aanval elders. Dit heeft impact op de rest van de samenleving. Een voorbeeld uit 2021 is de aanval op een logistiek bedrijf, die leidde tot lege schappen in de supermarkt (de 'kaas-hack')[7]. In dezelfde tijd zorgde de aanval op de Colonial Pipeline voor een stijging in de brandstofprijs in de Verenigde Staten[8]. Ransomware vormt aldus een risico voor de publieke sector, voor vitale processen en voor de daar gehuisveste gevoelige informatie.

In 2021 verdachten van de ransomware-aanval op de Universiteit Maastricht opgepakt in Oekraïne en haalden Driebergse politiehackers het grootste ransomware-verspreidende netwerk ter wereld, Emotet, op afstand neer.

De vuist van de politie tegen ransomware

Sinds 2012 investeert de politie gericht in de aanpak van cybercrime. Dit stelt het korps in staat om, net als de criminelen, gestructureerd maatwerk te ontwikkelen voor diverse typen cyberdelicten. De Nederlandse politie behaalt regelmatig internationale successen. Zo werden in 2021 verdachten van de ransomware-aanval op de Universiteit Maastricht opgepakt in Oekraïne[9] en haalden Driebergse politiehackers het grootste ransomware-verspreidende netwerk ter wereld, Emotet, op afstand neer[10].

De transitie vanuit aangifte-gedreven opsporing richting een meer fenomeengerichte aanpak vormt het fundament voor deze succesvolle aanpak. Dit betekent dat de politie niet naar één dadergroep kijkt, maar naar de gehele criminele keten (de zogenoemde killchain) en alle onderdelen wil begrijpen om ze te kunnen aanpakken. Door patronen te onderzoeken en aanwijzingen uit individuele zaken te combineren, kan focus worden aangebracht om in te grijpen op de meest bepalende elementen.

In de Emotet-casus leidde deze analyse naar een criminele server die in Nederland stond. Op basis van haar bevoegdheden wist de politie onopvallend tientallen terabytes aan gegevensverkeer van deze machine af te vangen. Zo kregen de digitaal specialisten zicht op het netwerk en de zwakke plekken.

Anders en samen ingrijpen

Andersoortige criminaliteit vraagt om meer dan alleen boeven vangen. De politie richt zich op andere manieren van misdaadbestrijding als aanvulling op het opsporen van cybercriminelen. Naast vervolging kan de samenleving immers ook worden geholpen met het voorkomen of verstoren van het strafbare feit. De politie probeert hierbij zicht te krijgen op daders, slachtoffers en criminele gelegenheidsstructuren (zoals Emotet). Het doorgronden van het criminele proces zorgt ervoor dat de politie kan afwegen wat de meest effectieve interventie is op dat moment. Samen sta je sterk. Het oorspronkelijk Nederlandse verstorings-initiatief NoMoreRansom.org is, vijf jaar later, beschikbaar in tientallen talen. Op de site kunnen slachtoffers van ransomware kosteloos terecht voor mogelijke oplossingen vanuit de hele wereld. Miljoenen mensen met versleutelde machines hebben hier gratis tegengif gevonden tegen één van 150 ransomware families. Sinds 2016 is zo bijna een miljard euro uit handen van criminelen gehouden[11]. Ook kan via deze site (afhankelijk van het land) aangifte worden gedaan, leidend tot een betere informatiepositie van de politie wereldwijd.

Doorgronden met data

De digitalisering van de samenleving zorgt ervoor dat ook de politie meer uit data kan halen voor haar onderzoeken. Concreet betekent dit dat ze vaker onderzoek doet om, naast het aanpakken van het delict zelf, een onderdeel van de ransomware-killchain beter te begrijpen. Zo zijn er eind 2021, vanuit een nieuwe Ransomware Taskforce, landelijk opererende werkgroepen geformeerd die per stap in de killchain gericht inzichten verzamelen. De bundeling van deze delictkennis zorgt, in samenwerking met de juiste partners, voor nieuwe kansen in de effectieve bestrijding van deze criminaliteitsvorm.

De grootte van de bijbehorende datasets leidt wel tot aanvullende uitdagingen. Zo verkent de politie momenteel welke rol ze zou moeten hebben in het bereiken van mogelijk miljoenen mensen, volgens de goede richtlijnen, met de waarschuwing dat die slachtoffer zijn van een digitale inbraak. Een kleine insluiping kan later de opmaat vormen voor een ransomware- of andere aanval. Naast de mogelijke schaalbaarheid van een dergelijke politiecompetentie ligt hier ook een belangrijke privacy-afweging. Wat voor impact heeft het op het gevoel van vrijheid en veiligheid als burgers en bedrijven regelmatig hack-waarschuwingen krijgen van de politie?

Wat is er nodig om verdere bestrijding te verbeteren?

De politie is steeds beter in staat om een antwoord te geven op ransomware, via een gestructureerde aanpak met aantoonbare successen. Toch gaat de enorme uitdaging voor de samenleving niet weg. Behalve ransomware wint ook andere digitale criminaliteit terrein van de traditionele vormen; cybercriminaliteit als geheel blijft een professioneel, uitdijend en snel veranderend speelveld[12].

Allereerst ligt er een uitdaging voor de strafrechtketen om nieuwe interventies naast het klassieke opsporen van een verdachte te omarmen. Dit is uitdagend voor bestuur en gezag, voor de maatschappij en voor een deel van de politieprofessionals. Verouderde prikkels belonen succes in kleine zaken soms beter dan een structurele verbetering als gevolg van doorgronding en aanpak van de criminaliteitsvorm. De inzet kan nog meer worden gericht op samenhang en samenwerking, impact en kwalitatieve resultaten. Dit levert idealiter een nieuwe manier van verantwoorden en sturen op.

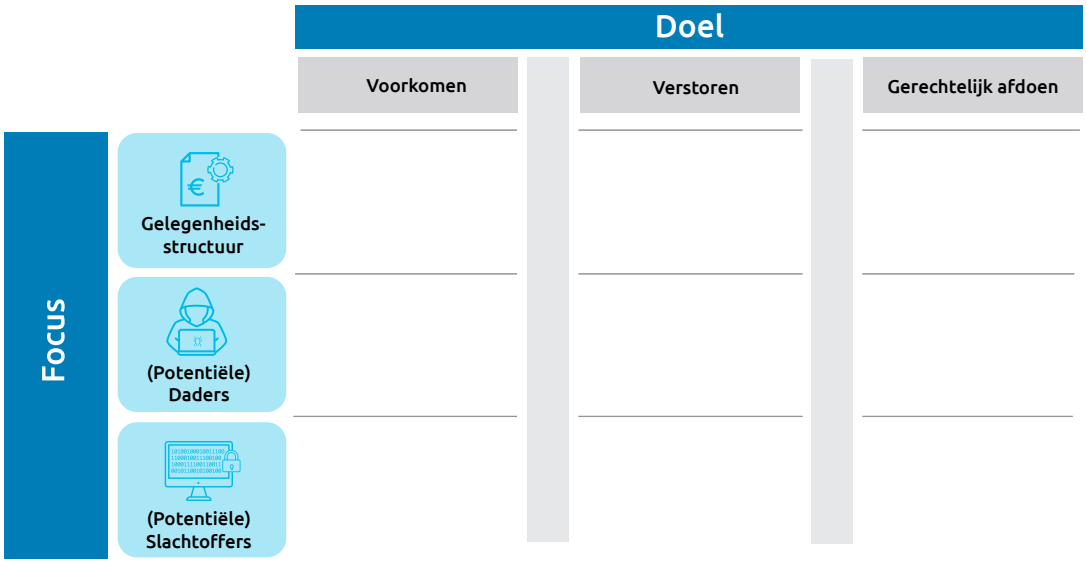
Bovendien zullen alle publieke en private partijen in dit veld naar een duurzamer, zaaksoverstijgende relatie moeten gaan. De politie kan daartoe meer structureel kijken hoe zij met anderen kan samenwerken bij het bewaken en beschermen van de samenleving tegen cybercriminelen, voor zover capaciteit en wettelijke kaders dit toestaan. Op hun beurt moeten andere partijen beseffen dat zij zelf waardevolle data hebben die de politie kan helpen, bijvoorbeeld als men direct of indirect slachtoffer is geworden. De uitdagingen komen onder meer bij elkaar in het vraagstuk van de noodzaak en wenselijkheid van het waarschuwen van (potentiële) slachtoffers. Dit is ook een vraag voor de samenleving.

Als de politie met haar partners een gedeeld antwoord weet te geven op dergelijke vragen, kan ze een nog grotere vuist maken tegen ransomware. En dan kan uiteindelijk in heel Nederland de vlag uit.

2021, vanuit een nieuwe Ransomware Taskforce, landelijk opererende werkgroepen geformeerd die per stap in de killchain gericht inzichten verzamelen. De bundeling van deze delictkennis zorgt, in samenwerking met de juiste partners, voor nieuwe kansen in de effectieve bestrijding van deze criminaliteitsvorm.

[1]Cyber Security Beeld Nederland: toegenomen dreiging Ransomware | politie.nl (2021). Geraadpleegd van: https://www.politie.nl/nieuws/2021/juni/28/00-cyber-security-beeld-nederland-toegenomen-dreiging-ransomware.html
[2]Cyberveilig Nederland. (2021). Whitepaper Ransomware. Cyberveilig Nederland, Augustus 2021.
[3] Cyberveilig Nederland. (2021). Whitepaper Ransomware. Cyberveilig Nederland, Augustus 2021.
[4]Cyberveilig Nederland. (2021). Whitepaper Ransomware. Cyberveilig Nederland, Augustus 2021.
[5]Bitdefender. (2020). Mid-Year Threat Landscape Report 2020, Bitdefender, https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf
[6]Osborne, C. (2021). The cost of ransomware attacks worldwide will go beyond $265 billion in the next decade. Geraadpleegd van: https://www.zdnet.com/article/the-cost-of-ransomware-around-the-globe-to-go-beyond-265-billion-in-the-next-decade/

Afbeelding 2: interventiematrix



Over de auteurs

Roeland van Zeijst

Senior Landelijk Projectmanager Cybercrime bij de Nationale Politie

Roeland van Zeijst is gespecialiseerd op de onderwerpen cybercrime, cybersecurity en cyberprivacy binnen het veiligheidsdomein. Hij is gepassioneerd om te beschermen wat ons dierbaar is door innovatie.

Harm van der Wal

Senior Consultant bij Capgemini Invent

Harm van der Wal is werkzaam bij Capgemini Invent als management consultant. Hij is gespecialiseerd in het opzetten en managen van transformaties in het publieke veiligheidsdomein.

harm.vander.wal@capgemini.com

[7]NOS. (2021). 'Kaas-hack' opgelost, ging om gijzelsofware. Geraadpleegd van: https://nos.nl/artikel/2376425-kaas-hack-opgelost-ging-om-gijzelsoftware
[8]NOS. (2021). Stilleggen oliepijplijn VS veroorzaakt door gijzelsoftware van Darkside. Geraadpleegd van: https://nos.nl/artikel/2380207-stilleggen-oliepijplijn-vs-veroorzaakt-door-gijzelsoftware-van-darkside
[9]Algemeen Dagblad. (2021). Verdachten achter ransomware-aanval op Universiteit Maastricht in Oekraïne gearresteerd. Geraadpleegd van: https://www.ad.nl/limburg/verdachten-achter-ransomware-aanval-op-universiteit-maastricht-in-oekraine-gearresteerd~ab3a69b1/
[10] Internationale politieoperatie Ladybird: wereldwijd botnet Emotet ontmanteld | politie.nl. (2021). Geraadpleegd van: https://www.politie.nl/nieuws/2021/januari/27/11-internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld.html
[11]Bracken, B. (2021). No More Ransom Saves Victims Nearly €1 billion over 5 years. Threatpost, 2021. Geraadpleegd van: https://threatpost.com/no-more-ransom-saves-victims-e1-5-years/168192
[12]Politie ziet verdubbeling van digitale criminaliteit | Security management. (2021). Geraadpleegd van: https://www.securitymanagement.nl/politie-ziet-verdubbeling-van-digitale-criminaliteit/

03

GROTE UITDAGINGEN IN EUROPA MET GRENZEN EN VEILIGHEID

Kunnen inzichten uit de agile-aanpak helpen om grote internationale programma's beter onder controle te houden?

Highlights

- Europa heeft op de lange termijn te maken met een toenemende druk van migratie en terrorismedreiging.
- Binnen Europa (en met namen het Schengengebied) is meer zicht nodig op wie zich binnen de grenzen bevindt. Ook voor niet-visumplichtige reizigers.
- Complex samenspel tussen lidstaten, wetgeving en praktijk.
- Dit vereist een enorme IT-inspanning over vele autoriteiten van alle EU-landen heen.
- De werkwijze wordt vooraf bedacht en in wetgeving verankerd. Dus absoluut niet agile. Dit levert risico's op voor het succes.

De Europese grenzen staan onder druk. Met de komst van het Akkoord van Schengen (1985) zijn veel Europese binnengrenzen verdwenen en is het toezicht op de buitengrenzen steeds belangrijker geworden. Door de groei van de Europese Unie is die buitengrens ook langer en diverser geworden. Echter, is er nauwelijks sprake van uitwisseling van informatie over dat grensproces tussen de verschillende lidstaten. Kortom, de Europese informatievoorziening rond het grensproces heeft een grote slag te maken.

Dat gebeurt nu ook in het programma 'Grenzen en Veiligheid'. Met 26 deelnemende lidstaten en nog meer betrokken instanties is de omvang van zo'n programma enorm, zo ook de risico's. Welke inzichten heeft de ontwikkeling van informatiesystemen in het verleden opgeleverd die deze risico's kunnen verkleinen?

De rol van grenzen

In de geschiedenis van de mensheid hebben grenzen altijd een belangrijke rol gespeeld in de veiligheid. Maar die grenzen zijn steeds verder weg komen te liggen. Van kasteelmuur naar stadvesting, van staatsgrenzen naar uiteindelijk de buitengrens van heel Europa. Daarbij is die grens ook steeds langer maar ook diverser geworden. We passeren de grens niet alleen meer over land maar ook per rivier, in zeehavens en op luchthavens. Tussen die grote aantallen personen die zo soepel mogelijk de grens willen passeren, zit een klein deel dat een veiligheidsrisico vormt. Dit zijn personen van buiten de EU ('derdelanders' in jargon) die langer dan toegestaan binnen de EU verblijven, migranten die op oneigenlijke gronden proberen asiel te krijgen en ook mensen die met criminele of zelfs met terroristische bedoelingen proberen de EU in te komen. De Europese instroom van asielzoekers varieert sterk onder invloed van onder meer de strijd in Syrië en de COVID-19 uitbraak, maar neemt op de lange termijn gezien geleidelijk toe[1]. Die toenemende vluchtelingenstroom zorgt steeds meer voor politieke onrust binnen de lidstaten. Die onrust mondt weer uit in problemen tussen EU-landen over de verdeling van asielzoekers. Net over de grens zien machthebbers dit als een kans om via 'hybride oorlogvoering' druk op de EU te zetten om meer onderhandelingsruimte te krijgen. Denk aan de vluchtelingendeal met Turkije.

In de geschiedenis van de mensheid hebben grenzen altijd een belangrijke rol gespeeld in de veiligheid. Maar die grenzen zijn steeds verder weg komen te liggen. Van kasteelmuur naar stadvesting, van staatsgrenzen naar uiteindelijk de buitengrens van heel Europa.

Aan de andere kant kan en wil Europa het reizen makkelijker maken voor de reguliere reizigers. Via grote luchthavens zoals Schiphol landen dagelijks duizenden passagiers vanuit de hele wereld voor werk, studie of toerisme. Hierbij is een snelle en soepele doorstroming van belang, zonder (grote) rijen voor de paspoortcontrole en (risico op) het missen van aansluitingen. Tenslotte wil de EU nadrukkelijk een humaan asielbeleid blijven voeren, privacy zoveel mogelijk waarborgen en aan de grens en binnen de EU niet discrimineren op onder meer afkomst, geaardheid, leeftijd en zaken als laaggeletterdheid of lichamelijke beperkingen[2]. Kortom het grenstoezicht staat voor een enorme uitdaging.

Grenzen en IT

Kan IT een (deel)oplossing van deze uitdaging zijn? Op dit moment bestaan er al EU-systemen die helpen om als één Europa op te treden en te voorkomen dat er misbruik wordt gemaakt van de open grenzen binnen Europa. Zo zorgt het Schengen Informatie Systeem (SIS-II[3]) ervoor dat personen en objecten (zoals gestolen auto's) die door de autoriteiten van de ene lidstaat worden gezocht ook bij de andere lidstaten op de radar staan. Ook is er het systeem EURODAC (European Asylum Dactyloscopy Database) een centrale database waarin biometrische kenmerken worden geregistreerd van asielzoekers en aangetroffen derdelanders die illegaal in de EU verbleven. Maar toch draagt dit nog onvoldoende bij aan een goede informatiepositie. Personen die op grond van hun criminele verleden niet meer welkom zijn, of die de maximale verblijfsduur in de EU overschrijden, worden nu pas ontdekt als ze al in het vliegtuig zitten of zelfs pas bij de paspoortcontrole. Dit is zowel voor de betrokkene als voor de luchtvaartmaatschappij (verplichte retourvlucht) zeer onwenselijk. Daarbij is bij terroristische aanslagen de beschikbare informatie in de EU-systemen te versnipperd en ontoereikend gebleken

om snel te kunnen reageren[4]. Zo kunnen vragen als 'wanneer en waar (en met wie?) is iemand de EU binnengekomen?' niet worden beantwoord en is het vaak onduidelijk welke registraties over dezelfde persoon gaan. Hierdoor gaat kostbare tijd verloren om daders of medeplichtigen in beeld te krijgen. Tevens is er maar weinig zicht op de details van de migratiestromen. Vliegen mensen wel naar hetzelfde land als waar ze een visum hebben aangevraagd? Hoe vaak komt het voor dat reizigers langer dan 90 dagen in de EU blijven (overstayers) en wat voor personen zijn dat dan? Dit zijn vragen die met de huidige registraties niet of lastig te beantwoorden zijn.

Met dit op het netvlies heeft de EU een ambitieus programma 'Grenzen en Veiligheid' opgesteld, met op hoofdlijnen de volgende inhoud:

- SIS-II wordt aangepast om ook personen met een inreisverbod of een terugkeerbesluit te registreren.
- Het visumsysteem EU-VIS wordt aangepast om naast de visa voor kort verblijf ook visa voor langere duur en verblijfsvergunningen te registreren.

Ook wordt bij een visumaanvraag meer in andere registraties gecontroleerd:

- Een nieuw Entry en Exit System (EES) vervangt de in- en uitreisstempels in het paspoort. Hiermee kan snel geautomatiseerd worden uitgerekend welke resterende verblijfsduur iemand nog heeft (bij inreis in de EU) of dat iemand zijn termijn heeft overschreden (bij uitreis).
- ETIAS (European Travel Information and Authorization System) vormt de IT-ondersteuning voor een nieuw stelsel waarbij ook visum-vrijgestelde reizigers vooraf toestemming moeten vragen om naar de EU te reizen (conform het ESTA-systeem in de Verenigde Staten). Hiermee wordt het mogelijk om al voor het boeken van de reis te beoordelen of een persoon welkom is in de EU.
- ECRIS-TCN (European Criminal Record Information System – Third Country Nationals) gaat het strafblad van niet-EU burgers bijhouden van misdaden waarvoor ze binnen de EU veroordeeld zijn.

- Voor reizigers van buiten de EU kunnen aan de grens en op luchthavens zelfbedieningskiosken worden ingericht waarmee aan de hand van het paspoort de aanwezigheid van een visum of ETIAS-autorisatie kan worden gecontroleerd. Hierbij wordt de identiteit gecontroleerd met gezichtsherkenning en/of vingerafdrukken. Tenslotte is er een systeem van Interoperabiliteit (IO) voorzien tussen deze systemen, waarbij het creëren of muteren van persoonsgegevens (biografisch, biometrisch, of reisdocumenten) in de verschillende EU-systemen aan elkaar worden gelinkt, zodat eventuele afwijkingen van worden gesignaleerd en onderzocht kunnen worden. Dit omvat ook statistische rapportages voor beleidsdoeleinden.

De aanpak

De omvang van het totale programma Grenzen en Veiligheid is enorm: 5 nieuwe of aangepaste systemen met zowel een centrale (EU) component als aanpassingen in 26 Schengen lidstaten. Daarbij geldt dat voor elke lidstaat er meerdere instanties betrokken zijn (voor Nederland: de Koninklijke Marechaussee, de IND, Buitenlandse Zaken, de Nationale Politie, Schiphol, het Openbaar Ministerie en de Justitiële Informatiedienst) waarbij per organisatie soms ook meer dan één systeem aangepast moet worden. Ook zijn er uitbreidingen en aanpassingen nodig aan hardware (infrastructuur aan de grens op Schiphol en voor de zeehavens) en werkprocessen. Een dergelijke omvangrijke aanpassing van informatiesystemen brengt risico's met zich mee. Dat zijn enerzijds risico's van uitloop van planning en daarmee ook overschrijding van de budgetten maar anderzijds ook dat het gerealiseerde systeem uiteindelijk niet oplevert wat er beoogd was. De Europese commissie hanteert hierbij de gebruikelijke aanpak: na een grondige inventarisatie worden de eisen en specificaties juridisch vormgegeven in verordeningen die op een vastgestelde datum de kracht van een wet krijgen. Hierdoor zijn de lidstaten wettelijk verplicht om zelf de nodige inspanningen te verrichtten om tijdig

aan te kunnen sluiten met hun eigen informatiesystemen. Hoewel dit natuurlijk een prima manier is om er zeker van te zijn dat alle lidstaten tijdig aan de slag gaan, kleven er wel nadelen aan deze aanpak.

Nadelen

De hierboven beschreven werkwijze is wat in de systeemontwikkeling bekend staat als de 'waterval'methode: er wordt een grondig uitgewerkt ontwerp gemaakt wat door een realisatieteam exact zo gebouwd moet gaan worden. Zo extreem is het in het geval van het programma Grenzen en Veiligheid overigens ook weer niet: met name over detailuitwerkingen wordt regelmatig afgestemd met experts en IT-architecten uit de lidstaten. Desondanks neemt dat de volgende twee nadelen niet weg:

1. Lidstaten zullen geneigd zijn om zich vooral te richten op het voldoen aan de wet (implementeren van de verordeningen) en minder op de achterliggende bedoelingen.
2. Door de belangrijkste specificaties in wetgeving vast te leggen is het niet of nauwelijks meer mogelijk om tijdens de realisatie opgedane nieuwe inzichten te gebruiken of om te reageren op nieuwe ontwikkelingen.

Met een programma met een looptijd van enkele jaren leidt dit er snel toe dat er uiteindelijk wel het systeem komt dat men 'jaren geleden' op het oog had maar dat het uiteindelijk niet meer optimaal aansluit op de nieuwe situatie.

Minimum Viable Product

In de systeemontwikkeling is om deze redenen de Agile werkwijze de laatste jaren gemeengoed geworden bij vrijwel alle organisaties. Eén van de belangrijkste inzichten hiervan is dat systeemontwikkeling schieten op een bewegend doel is: de realiteit verandert, zeker tegenwoordig, snel. Zeker binnen een meerjarig programma rond een thema dat zo sterk in beweging is moet daar rekening mee gehouden worden. De belangrijkste maatregel om hiermee om te gaan, is dat je begint met een zo simpel mogelijke oplossing te realiseren: het Minimum Viable Product (MVP), de minimale noodzakelijke functionaliteit die nodig is en deze naar productie te brengen[5] . Op het moment dat het MVP in gebruik is, kan je feedback verzamelen vanuit de gebruikers en andere stakeholders. Aan de hand van de feedback kan een MVP vervolgens worden doorontwikkeld in de richting van een optimaal werkend product. Dit heeft een aantal belangrijke voordelen:

- Je hebt sneller een klein en beperkt maar werkend systeem in productie.
- Je kan voortdurend bijstellen in de volgende ontwikkelstap.
- Je kan op elk moment stoppen (of pauzeren) en hebt dan wel een werkend systeem.

En hoe dan wel?

Vanuit deze blik terugkijkend naar de Europese aanpak, valt het op dat de wetgeving van de Europese Commissie (in de vorm van een flink aantal verordeningen) erg gedetailleerd de te bereiken eindsituatie beschrijft. Dikwijls wordt daarbij niet alleen het 'wat' maar ook het 'hoe' in de wet vastgezet, waardoor in de implementatieperiode aanpassingen praktisch niet meer mogelijk zijn. Een mogelijk beter aanpak zou zijn om die wetgeving te beperken tot wat de systemen in essentie moeten gaan doen en binnen welke beperkingen dat moet gebeuren (zoals autorisatie en doelbinding, bewaartermijnen en rechten van de burger). Daarbij kunnen de centrale systemen meer als diensten ('services') worden vormgegeven, waar de nationale systemen gebruik van maken om de in de wet gestelde doelen te kunnen bereiken. Nieuwe inzichten kunnen dan resulteren in een nieuwere versie van zo'n dienst, waarbij de oude dienst ook nog enige tijd beschikbaar blijft totdat elke lidstaat heeft

[1]https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Asylum_statistics
[2]Zie European Union Agency for Fundamental Rights: https://fra.europa.eu/en
[3] https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/schengen-information-system_en
[4] European Council: "The EU's response to terrorism" (https://www.consilium.europa.eu/en/policies/fight-against-terrorism/)
[5]Agile Alliance: MVP (https://www.agilealliance.org/glossary/mvp/)

kunnen overstappen. Ook zou je kunnen denken aan een bibliotheek ('repository') waar de lidstaten herbruikbare producten kunnen uitwisselen. Hierdoor zou men meer kunnen leren van elkaars goede ideeën en bovendien zou het een positieve invloed kunnen hebben op de ontwikkelkosten en de onderlinge standaardisatie.

Het programma Grenzen en Veiligheid staat dus voor een enorme uitdaging om meerdere EU-systemen te realiseren en aan te passen. Deze EU-systemen moeten daarnaast ook nog interoperabel worden. De maatstaf van succes van het project is de tijdige en correcte oplevering van de producten die nodig zin voor implementatie van de wetgeving.

Het zou dus een goede zaak zijn als het Agile denken juist bij deze grote programma's een plek kan krijgen. Met name door eerst te richten op een Europa-breed Minimal Viable Product (zowel in wetgeving als systeemontwikkeling) zou het risico op uitloop en met name op het realiseren van een niet goed functionerend systeem sterk verkleind kunnen worden.

Conclusie

Het programma Grenzen en Veiligheid staat dus voor een enorme uitdaging om meerdere EU-systemen te realiseren en aan te passen. Deze EU-systemen moeten daarnaast ook nog interoperabel worden. De maatstaf van succes van het project is de tijdige en correcte oplevering van de producten die nodig zin voor implementatie van de wetgeving.

Het zou dus een goede zaak zijn als het Agile denken juist bij deze grote programma's een plek kan krijgen. Met name door eerst te richten op een Europa-breed Minimal Viable Product (zowel in wetgeving als systeemontwikkeling) zou het risico op uitloop en met name op het realiseren van een niet goed functionerend systeem sterk verkleind kunnen worden.

Over de auteurs

Frank Inklaar
Business Analist
Frank Inklaar MSc is Senior Consultant bij Capgemini Digital Society. Hij richt zich op het toepassen van advanced analytics en Artificial Intelligence in het domein openbare orde en veiligheid.

frank.inklaar@capgemini.com

Pascal Speek
Business Analist
Pascal is Senior Consultant bij Capgemini Digital Society

pascal.speek@capgemini.com

Paul Lengkeek
Transformatie manager
Paul Lengkeek is Managing Consultant bij Capgemini Digital Society

paul.lengkeek@capgemini.com

04

QUANTUM MACHINE LEARNING: BELOFTE OF BEDREIGING?

Zal QML de IT-security hoofdzakelijk nieuwe middelen voor beveiliging geven, of nieuwe uitdagingen?

Door slim samenvoegen van Quantum Computing en Machine Learning kan in de nabije toekomst al worden geëxperimenteerd met optimalisatie van huidige beveiliging en ontgrendelingstechnieken.

Highlights

- Machine-Learning wordt nu al gebruikt in veel IT-security use-cases.
- Quantum-Computing kan met behulp van Shor's algoritme klassieke encryptie breken.
- QML biedt mogelijkheden door het slim samenvoegen van de beide technologieën.

Intro: Quantum Machine, wat?

Waar Machine Learning (ML) sinds een aantal jaar in rap tempo onmisbaar is geworden in veel moderne IT-security, komt anno 2022 steeds meer aandacht voor de volgende generatie computers en haar implicaties. Dit artikel neemt je mee in de wereld van Quantum Technologie (QT), en verklaart hoe de twee werelden van ML en QT elkaar vinden in een (nu nog) niche van de cybersecurity sector: Quantum Machine Learning (QML). Je leest wat QML in potentie kan betekenen voor nu nog typische ML-taken als classificatie en regressie. Voordat we daar aan toe komen, leggen we eerst kort de geschiedenis van ML en de basisprincipes van QT uit.

Machine learning in security: Een korte historie

Het is februari 1987. Binnen DARPA publiceert informaticus Dorothy Elizabeth Denning een paper over computerinbraakdetectiesystemen, gestoeld op principes die we vandaag de dag nog gebruiken in machine-learning[1]. Haar detectiesysteem berust op het ontdekken van een anomalie: een ongebruikelijk event. Informatie die in een systeem ingevoerd wordt die anders is dan dat het systeem herkent, wordt gescand en bestempeld met de tag 'mogelijk gevaarlijk'.

De cybersecurity industrie kan niet zonder Artificiële Intelligentie (AI), zo beaamt 69% van de ondervraagde bedrijven in een eerder verschenen studie uitgevoerd door Capgemini.

Het systeem is ook wel unsupervised: de computer wordt niet door mensen bijgestuurd. Machine Learning is geboren.

Tientallen jaren later, met het opkomen van het fenomeen big data, koppelen de eerste wetenschappers deze unsupervised modellen met supervised modellen. Deze supervised modellen kunnen informatie uit andere bronnen halen (bijvoorbeeld een blacklist aan verdachte webpagina's) en zo een model verrijken (bijvoorbeeld een spamfilter). Als een binnenkomend bericht anders is dan alle andere berichten die tot dan toe zijn binnengekomen én er staat een verdachte weblink in die elders geclassificeerd is als spam, dan pas classificeert een computer het bericht als spam. Hoewel dit handig is bij het opdoen van nieuwe kennis, sijpelen positieve en vals-negatieve berichten soms nog door. Hierdoor is de noodzaak tot cybersecurity nog pertinent.

De noodzaak van het gebruik van AI

Vandaag de dag zetten cybersecurity analisten artificiële intelligentie (AI) op veel plekken in. Niet alleen omdat het risico is toegenomen binnen cybersecurity - denk aan recente ransomware-aanvallen en datalekken - maar ook omdat de hoeveelheid informatie die moet worden geanalyseerd is geëxplodeerd. Menselijke capaciteit is simpelweg niet toereikend om handmatig e-mails en bestanden te controleren op gevaar. De organisatie dient te vertrouwen op de regels die de computer zijn meegegeven en de regels die de computer zelf middels AI schrijft.

De cybersecurity industrie kan niet zonder Artificiële Intelligentie (AI), zo beaamt 69% van de ondervraagde bedrijven in een eerder verschenen studie uitgevoerd door Capgemini (2019)[2]. Onder het brede scala van toepassingen binnen AI is Machine Learning (ML) vaak toegepast om sneller gevaren te kunnen detecteren, voorspellen en erop te kunnen handelen. Erkende toepassingen waar hevig gebruikt gemaakt wordt van ML zijn niet alleen te vinden in (reeds genoemde) spam-filters, maar ook in online betalingsportalen en certificaten/ compliance-controlemechanismen. ML wordt niet alleen aan de kant van de verdediging gebruikt: ook kwaadwillenden gebruiken steeds vaker machine learning om complexe data te analyseren en zichzelf zo toegang te verschaffen tot allerlei informatie.

Er is een explosieve toename in vraag aan rekenkracht voor machine learning. Vanaf 2016 verdubbelt elke 3 tot 5 maanden het totaal aantal parameters in machine learning modellen[3]. Deze vuistregel is duidelijk te zien bij modellen voor natural language processing. In 2018 bracht OpenAI GPT-1 uit, destijds van de grootste modellen met 117 miljoen parameters. Vier jaar later in, in 2022 komt GPT-4 uit met 100 biljoen parameters. Voor wie deze getallen duizelen; dit is een vermenigvuldiging van een miljoen keer in slechts vier jaar.

Tegelijkertijd is de rek er bijna uit in de ontwikkeling van klassieke computers. Over de afgelopen decennia zijn computers steeds krachtiger geworden doordat ze meer transistoren bevatten dankzij miniaturisatie[4]. Innovatie verliep zo snel dat het aantal transistors elke twee jaar verdubbelde. Dit fenomeen staat bekend als Moore's law. Moore's law loopt

echter op zijn einde, omdat transistors niet verder verkleind kunnen worden en het proces van miniaturisatie stokt.

Hier komt quantum computing om de hoek kijken. Quantum computers werken op een fundamenteel andere manier en zijn dus niet slechts een snellere klassieke computer. Waarbij klassieke computers gebruik maken van bits, de binaire basis eenheid voor informatie, gebruiken quantum computers quantum bits, ofwel qubits. Qubits kunnen niet alleen in de waardes nul en een aannemen, maar kunnen zogezegd in een superpositie van een en nul zijn. Omdat qubits fundamenteel verschillen bits, is ook de programeertaal, de algoritmes, en de applicaties verschillend voor quantum computers dan voor klassieke computers. In het volgende hoofdstuk gaan we in hoe quantum algoritmes zich kunnen onderscheiden van klassieke algoritmes.

Quantum computer
Een fundamenteel nieuw type computer welke gebruikt maakt van fenomenen uit de quantum mechanica.

Qubit
De fundementele informatie eenheid van quantum computers. Anders dan bij bits, de informatie eenheid bij klassieke computers, kunnen qubits niet alleen de waardes een en nul aannemen, maar een zogenaamde superpositie van deze twee waardes aannemen.

Machine learning
Het gebruik van data en modellen om met computers menselijk leren te imiteren.

Quantum machine learning
Machine learning welke draait op quantum computers

Immense rekenkracht van quantum computers

Je zou quantum algoritmes kunnen opdelen in twee types; algoritmes die complexe vergelijkingen sneller kunnen oplossen, en algoritmes die door het grote geugen van quantum computers tot betere antwoorden kunnen leiden.

De eerste catagorie omvat quantum algoritmes die complexe problemen oplossen door een immense rekenkracht. In sommige gevallen is er een exponentiële versnelling mogelijk. Dit betekent dat als het probleem groot genoeg is, het algoritme miljoenen keren sneller kan zijn. Shor's algoritme is hiervan het beste voorbeeld. Dit beducht algoritme, welke bedacht is door Peter Shor in 1994, is in staat om kritische encryptie, zoals RSA en Diffi-Hellman, te breken door de regelmaat in grote reeksen getallen te vinden. De kracht van de encryptie is gebaseerd op het idee dat computers miljarden jaren nodig hebben om de sleutel te vinden. Dit is niet langer het geval wanneer quantum computers sterk genoeg zijn, waardoor een grote cybersecurity kwetsbaarheid ontstaat. Dit vraagt om een grote en urgente update naar nieuwere encryptiemethodes.

Quantum machine learning op basis van immense rekenkracht

Naast het Shor's algoritme zijn er enkele andere algoritmes bedacht die een flinke versnellingen kunnen bieden. Het HHL algoritme (vernoemd naar de ontwerpers Harrow, Hassidim en Lloyd) is in staat om lineaire systemen van vergelijkingen op te lossen met een exponentiële versnelling. Omdat lineaire algebra de basis vormt van machine learning, zou dit algoritme mogelijk het trainen van deep learning processen kunnen versnellen. Hierdoor zouden kunstmatige intelligentie modellen sneller, en kosten-effectiever op grote datasets getraind kunnen worden. Deze modellen worden dan krachtiger en nauwkeuriger. Het HHL algoritme kan echter maar onder strikte condities toegepast worden en blijkt in de praktijk moeilijk te implementeren. Daarnaast zijn applicaties in deze categorie afhankelijk van quantum geheugen (QRAM) voor

het efficiënt laden van klassieke data naar quantum computers. Omdat QRAM nog niet uitgevonden is, blijven deze algoritmes voorlopig toekomstmuziek.

Quantum machine learning op basis van een enorm geheugen

Naast het versnellen van het machine learning process, zou QML ook een voordeel kunnen bieden ten opzichte van klassieke machine learning door nauwkeurigere resultaten te verkrijgen met minder data. Quantum computers kunnen namelijk gebruik maken van een groter geheugen dan klassieke computers: qubits kunnen niet alleen de waarde een en nul aan kunnen nemen, maar ook alle waarden hier tussen in. Sommige problemen zouden beter gerepresenteerd worden in het geheugen van quantum computers, en daarom efficiënter opgelost kunnen worden.

Het principe hiervan is vergelijkbaar klassieke kernel methods, welke veel gebruikt worden in machine learning. Kernel methods transformeren data naar een hogere dimensie, waardoor makkelijker verbanden gevonden worden. Quantum machine learning werkt op een vergelijkbare manier, door klassieke data in quantum data te vertalen.

Er is in 2021 veel onderzoek gedaan naar deze categorie van quantum algoritmes, en inmiddels zijn er publicaties over quantum support vector machine (qSVM), quantum natural language processing (qNPL), quantum convolutional neural net (qCNN), quantum generative adversarial network (qGAN) en meer

Quantum Natural Language Processing

Een relevant voorbeeld voor cybersecurity is (quantum) Natural Language Processing (NLP). NLP wordt gebruikt voor bijvoorbeeld het doorgronden van documenten of het genereren van phishing scripts. Quantum NLP zou mogelijk beter kunnen presteren dan klassieke algortimes.

De intuïtie hierbij is dat taal interactief is: denk aan het subtiele verschil tussen een bank om op te zitten en daar waar je je geld parkeert of de plaats van woorden in een zin. Voor klassieke computers kost het veel rekenkracht om alle

verschillende opties langs te lopen (wat wordt bedoeld met ‘de bank’ in de zinnen ‘Jip gaat naar de bank’ of ‘jip gaat naar de bank kijken’). Het eerder genoemde GPT-3 model van Facebook, het meest uitgebreide NLP model, kan dit verschil weliswaar ontdekken; het benodigt wel veel rekenkracht. Het GPT-3 model bevat namelijk 180 miljard parameters, en heeft het energieverbruik van een kleine stad nodig om getraind te worden.

De interactiviteit van taal kan efficiënter geprogrammeerd worden in quantum computers. In het grote geheugen van quantum computers kunnen de verschillende betekenissen van woorden en zinnen worden opgeslagen, en door slim gebruik te maken van quantum interference kan de juiste betekenis ontleed worden. Vergelijkbaar met bovenstaande figuur, worden zinnen getransformeerd naar een hogere dimensie, waar de interactie tussen woorden in het geheugen staat, en de quantum computer beter in staat is om verbanden te vinden.

Een bijkomend voordeel is dat qNLP, en veel implementaties van QML in het algemeen, geschikt is voor quantum computers van de nabije toekomst. Deze computers, ook wel NISQ (noisy intermediate scale quantum) computers genoemd, worden gekenmerkd door foutgevoeligheid. Quantum Machine Learning is hier beter bestand tegen fouten dan veel andere algoritmes, doordat ze hybride is. Dit betekent dat klassieke computers een deel van de berekening overnemen, waardoor er minder van de quantum computer wordt gevraagd. Daarnaast zouden fouten bij machine learning niet altijd voor problemen hoeven te zorgen, maar zou het zo kunnen zijn dat fouten zorgen voor betere generalisatie.

Hoewel er dus veel hoop is dat quantum algoritmes een voordeel zou kunnen bieden voor machine learning, is dit nog niet daadwerkelijk aangetoond. Bij machine learning geldt dat de prestaties moeilijk theoretisch aan te tonen zijn. Dit betekent dat we pas weten of QML echt een voordeel biedt als we het zien voor een realistische toepassing. De komende jaren zullen dit moeten gaan aantonen.

Conclusie

Verwachtingen voor QML

Wat betekenen bovenstaande toepassingen voor het veiligheidsdomein? Algemene uitspraken over de toename in veiligheid en kwetsbaarheid van QML zijn momenteel erg moeilijk te maken. QML is tot nu toe uitsluitend van theoretische aard is geweest, omdat er simpelweg geen QML is in de praktijk. Aangenomen mag echter worden dat dezelfde use-cases waar machine-learning hedendaags voor wordt ingezet met grotere precisie dankzij kwantumtechnologie kan worden ingezet, en dat er ook dezelfde bedreigingen uit voortkomen. ML wordt namelijk ook ingezet bij het vervalsen van face-recognition of het namaken van certificaten waarmee een hacker zich kan voordoen alsof hij/zij bevoegd is om ergens een kijkje te mogen nemen.

We hebben hier slechts het tipje van de sluier kunnen oplichten. Waar bedrijven QML willen gaan inzetten voor krachtigere beveiliging en ontsleuteling (voor bijvoorbeeld opsporing), dienen CISO's vandaag al de mogelijkheden gaan verkennen die kwantumtechnologie gaat bieden. Dit om te voorkomen dat er straks bij de komst van wijdverspreide kwantumtechnologie een langzaam antwoord komt vanuit de markt, waardoor er gevoelige informatie op straat kan komen te liggen. Resteert enkel de vraag: is uw organisatie al klaar voor de komst van QML?

Over de auteurs

Julian van Velzen

Head of Quantum Lab Capgemini Group

Julian van Velzen is werkzaam de Capgemini Group als hoofd van het Quantum Lab. Daarnaast is hij onderdeel van de CTO community, en is hij de Nederlandse afgevaardigde van het Europrese quantum consortium (QuIC). Julian heeft een achtergrond in de computationele natuurkunde.

julian.van.velzen@capgemini.com

Luc Baardman

Ecosysteem Facilitator bij Capgemini Invent

Luc is werkzaam bij Capgemini Invent. In zijn projecten zoekt Luc naar de gemene deler in het behalen van winst voor iedere partij in elke samenwerking. Capgemini's methode van Empowering Ecosystems past Luc toe in de publieke thema's als Smart Cities en Cybersecurity. In zowel nationale als Europese speelvelden.

luc.baardman@capgemini.com

[1] https://www.securityinfowatch.com/cybersecurity/article/21114214/a-brief-history-of-machine-learning-in-cybersecurity
[2] https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2019/07/AI-in-Cybersecurity_Infographic-1-2.pdf
[3] https://towardsdatascience.com/parameter-counts-in-machine-learning-a312dc4753d0
[4] Onder miniaturisering wordt in de techniek verstaan een proces waarbij structuren worden verkleind met behoud van hun functionaliteit en eventueel ook hun vorm. Het gaat daarbij om het verkleinen van onderdelen van technische apparaten, en uiteindelijk van die apparaten zelf.

05 ALLEEN DOOR BETERE SAMENWERKING PAKKEN WE (FINANCIËLE) CRIMINALITEIT EFFECTIEF AAN

Welke effecten zijn te verwachten bij betere samenwerking op het identificeren en bestrijden van (financiële) criminaliteit en binnen welke randvoorwaarden zou dit moeten plaatsvinden?

Highlights

- Bestrijden van (financiële) criminaliteit is één van de topprioriteiten voor onze maatschappij.
- Het delen van data en kennis over kolommen heen kan er voor zorgen dat er betere resultaten worden behaald, verdachte transacties worden voorkomen en dat de oorsprong wordt aangepakt door justitie.
- Kijkend naar de toekomst is het een vereiste om kennisdeling en samenwerking te verbeteren, federateive samenwerking speelt hierin een belangrijke rol.
- Het automatiseren van processen en gebruik van AI zorgt voor synergie tussen medewerkers en techniek.

Bestrijden van (financiële) criminaliteit is één van de topprioriteiten voor onze maatschappij. Een belangrijk thema hierin is het vinden en bestrijden van financiële geldstromen die gerelateerd zijn aan criminaliteit en terrorisme. Diverse kolommen houden zich bezig met deze thema's, waarbij de focus veelal binnen de kolom ligt. Samenwerking over de kolommen heen heeft de potentie om in gezamenlijkheid meer resultaat te boeken. Het delen van data en kennis kan er hierbij voor zorgen dat er betere resultaten worden behaald, verdachte transacties worden voorkomen en dat de oorsprong wordt aangepakt door justitie. Hoe zou deze samenwerking eruit moeten zien en welke effecten zijn te verwachten?

Individueel continu op zoek naar uitzonderingen

In Nederland gaat naar schatting jaarlijks voor 16 miljard euro aan zwart geld rond[1]. De Wet voorkoming Witwassen en Financiering Terrorisme (Wwft)[2]

Vanwege geheimhoudingsplicht worden klanten niet geïnformeerd over melding van ongebruikelijke transacties aan de FIU. In 2020 steeg het aantal gemelde verdachte transacties met 58% naar 245.000.

moet zorgen voor meer zicht op (illegale) geldstromen en het risico op terrorismefinanciering en witwassen beperken. De ministeries van Financiën en van Justitie en Veiligheid zijn samen verantwoordelijk voor het beleid en de regels tegen terrorismefinanciering en witwassen.

Per branche kijkt een toezichthouder of alle partijen zich goed aan de Wwft houden, dit zijn bijvoorbeeld: De Nederlandsche Bank (hoofdzakelijk banken en verzekeraars), Bureau Financieel Toezicht (notarissen, accountants, belastingadviseurs) en de Kansspelautoriteit (speelcasino's). Deze toezichthouders kunnen ook boetes uitdelen als dat nodig geacht wordt. Dit heeft de laatste jaren geleid tot meer dan een miljard euro aan boetes voor de grootste banken in Nederland. Boetes die steeds hoger worden, een trend die ook wereldwijd door lijkt te zetten[3].

In de basis moeten alle partijen die onder de Wwft vallen voortdurend een helder en actueel beeld hebben van wie hun klanten zijn, waar het geld van hun klanten vandaan komt en waarvoor klanten het geld gebruiken. Alle financiële transacties moeten tegen het licht worden gehouden (iedere instelling heeft een lijst met relevante risico's die gecontroleerd worden) en ongebruikelijke transacties moeten worden gemeld bij de Financial Intelligence Unit (FIU[4]). Banken hebben veel geïnvesteerd in het identificeren van hun klanten en transactie monitoring. Zo werken er nu ongeveer 12.000 mensen in Nederland om te helpen bij de Poortwachter functie van banken[5]. Dat betekent dat ongeveer 1 op de 6 bankmedewerkers zich (in)direct bezighouden met de Poortwachtersfunctie.

De FIU voert verdere analyses uit met de beschikbaar gestelde informatie. Pas nadat transacties formeel verdacht zijn verklaard door het hoofd van de FIU worden deze ter beschikking gesteld aan handhavings- en opsporingsdiensten. Vanwege geheimhoudingsplicht worden klanten niet geïnformeerd over melding van ongebruikelijke transacties aan de FIU.

In 2020 steeg het aantal gemelde verdachte transacties met 58% naar 245.000[6]. In 2021 worden er 1 miljoen verdachte transacties verwacht[7]. De Politie (en FIU als onderdeel van de Nationale Politie) kampen door de hele keten met een structureel personeelstekort. Zo is er in 2020 capaciteit aan FIU toegevoegd waardoor ze in totaal op 90 mensen uit komen. Dit heeft niet alleen effect op het aantal meldingen dat ze verder kunnen onderzoeken maar ook aan de kwaliteit van de cases die ze aan het OM voorleggen. Zo komt het dat er van de honderdduizenden meldingen die banken aan de FIU leveren maar ongeveer 20.000 aan het OM worden voorgelegd. Uiteindelijk heeft dit geleid tot 240 zaken en 86 veroordelingen[8, 9].

Tussen de verschillende branches vindt weinig tot geen samenwerking plaats. Hierdoor is het vrijwel onmogelijk om een volledig beeld te krijgen van alle relevante eigenschappen van personen en organisaties en de verdachte transacties die tussen hen plaatsvinden. Daarnaast is er sprake van inefficiëntie omdat veel gegevens op meerdere plekken verzameld en bijgehouden worden.

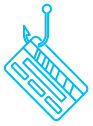
Synergie op deskundigheid en kwaliteit van inzichten

Witwaspraktijken worden steeds geraffineerder en complexer. Ondanks maatregelen en investeringen zal het altijd een wedloop tussen poortwachters en criminelen blijven. Hierbij hebben criminelen het voordeel dat middelen ruim voorhanden zijn en dat ze geen last hebben van bijvoorbeeld regels op het vlak van privacy en ethiek.

Niet alleen de technologische aspecten (bijvoorbeeld steeds meer regels toepassen op steeds meer data) maar ook de toenemende diversiteit en complexiteit van het financiële ecosysteem (steeds meer aanbieders, crypto valuta, etcetera.) maakt het steeds moeilijker om witwassen en financiering van terrorisme op te sporen. Daarnaast is het blijven opbouwen van deskundigheid bij poortwachters een andere factor die steeds verder onder druk komt te staan.

Door beter en meer samen te werken – niet alleen binnen een branche, maar ook tussen de branches en met de toezichthouders - kan er voor alle partijen meer resultaat geboekt worden. Het delen van data en kennis hierover kan ervoor zorgen dat er betere resultaten geboekt worden, verdachte transacties worden voorkomen en dat de oorsprong wordt aangepakt door justitie.

Het thema samenwerking is op zich niet nieuw, zo bestaan er al vele samenwerkingsverbanden en initiatieven tussen banken en overheid. De Serious Crime Task Force (onderdeel van FEC), Fintell Alliance en Transactiemonitoring Nederland zijn allemaal voorbeelden



Witwaspraktijken worden steeds geraffineerder en complexer. Ondanks maatregelen en investeringen zal het altijd een wedloop tussen poortwachters en criminelen blijven.

van samenwerkingsverbanden tussen banken en de overheid. Het Multidisciplinair Interventie Team (MIT) richt zich op samenwerking binnen overheidsinstanties[10]. Met het Financieel Expertise Centrum (FEC) is er zelfs een samenwerkingsverband met als kerntaken: samenwerking, kennisdeling en informatie uitwisselen[11]. Ook is er bij de Nederlandse Organisatie voor Wetenschappelijk Onderzoek 6 miljoen euro beschikbaar gesteld voor onderzoek waarbij de focus op het juist gebruiken van data ligt[12]. De FIU noemt samenwerking 'van groot belang' in hun jaarverslag[13].

Veel samenwerkingsverbanden zijn op dit moment nog vooral projectmatig: er zijn specifieke problemen of vraagstukken en om die aan te pakken is het nodig om de samenwerking op te zoeken.

Federatieve samenwerking

Er zou meer moeten worden geïnvesteerd in het opzetten van een federatieve samenwerking rondom Wwft. Binnen een federatieve samenwerking blijven alle partijen autonoom opereren binnen hun eigen domein maar is er wel structurele samenwerking die domeinen met elkaar verbindt. Samenwerking kan hierbij allereerst gericht zijn op het delen van kennis en kunde om zo gezamenlijk sterker te worden. Als tweede kan samenwerking gericht op het uitwisselen van data, wat veelal aanvullende investeringen in heldere doelstellingen, eenduidige governance, gedragen toezicht en onderling vertrouwen vergt, worden beschouwd als een tweede belangrijk instrument in federatieve samenwerking.

Onderzoek van het Capgemini Research Institute laat zien dat er bij de meeste organisaties de algemene strategie niet goed ondersteund wordt door de data/analytics strategie[14]. Om beide strategieën beter te laten aansluiten, is het van belang te begrijpen welke informatie waar en wanneer nodig is. Hiervoor moeten samenwerkende partijen elkaars processen goed begrijpen voordat ze data gaan uitwisselen. Door transparant te zijn in wat er waarvoor nodig is, kan de juiste informatie worden verzameld. Deze informatie kan vervolgens geleverd worden aan de juiste partij op het juiste moment. Het tijdig verzamelen, leveren en gebruiken van informatie kan goed binnen een federatieve samenwerking worden gerealiseerd. Dit werkt twee kanten op: enerzijds weet de leverancier wat de behoefte van de afnemer is en kan zo een betere kwaliteit data leveren. Anderzijds, kan de afnemer (ketenpartner) data beter interpreteren en binnen de juiste context plaatsen om zo het doel te bereiken. Het werken binnen een vertrouwde omgeving waarin data op een uniforme en veilige manier onderling uitgewisseld kan worden werkt veelal als katalysator voor het opschalen van de toepassing ervan en intensivering van de onderlinge samenwerking.

Federatieve samenwerking binnen geaccepteerde kaders

Het federatief samenwerken in een vertrouwde dataomgeving begint met het afstemmen van datavraag, -aanbod en -gebruik en het minutieus toepassen van relevante wettelijke[15,16] en ethische[17] regelgeving om de kaders waarbinnen geopereerd wordt kristalhelder te definiëren. Altijd kunnen uitleggen wat er gebeurt met data en waarom het gebeurt is van fundamenteel belang om het vertrouwen van belanghebbenden (incl. de maatschappij) te verdienen. Daarnaast is deugdelijk toezicht noodzakelijk om te borgen dat in de federatieve samenwerking te allen

[1] https://www.nvb.nl/themas/veiligheid-fraude/aanpak-witwassen/
[2] https://wetten.overheid.nl/BWBR0024282/2021-07-01
[3] https://www.banken.nl/nieuws/23495/aml-boetes-schieten-wereldwijd-omhoog
[4] https://www.fiu-nederland.nl/en
[5] https://nos.nl/nieuwsuur/artikel/2403990-een-miljoen-ongebruikelijke-transacties-maar-weinig-aanhoudingen
[6] https://www.nvb.nl/themas/veiligheid-fraude/aanpak-witwassen/
[7] https://www.trouw.nl/economie/banken-zitten-in-een-spagaat-tussen-justitie-en-klagende-ondernemers~b5a90fc2/?referrer=https%3A%2F%2Fwww.google.com%2F
[8] https://www.trouw.nl/economie/tienduizenden-witwasmeldingen-amper-strafzaken-soms-lijkt-het-of-het-hele-meldsysteem-voor-niets-is~b03c7f64/

tijde binnen heldere en geaccepteerde kaders gewerkt wordt. De recente Toeslagenaffaire laat zien wat de gevolgen zijn als hier onvoldoende aandacht aan wordt besteed. Door helder te laten zien dat geaccepteerde kaders (en de onafhankelijke controle hierop) in alle vezels van de federatieve samenwerking terugkomen, kan hiermee ook het vertrouwen van de maatschappij worden herwonnen.

Door een federatieve samenwerking wordt er altijd data vanuit diverse bronnen samengebracht – dus meer diversiteit en meer informatierijkdom – en vanuit verschillende oogpunten en afwegingen beoordeeld – dit zal leiden tot betere inzichten, besluiten en resultaten. Een veilige en vertrouwde samenwerking moedigt het stellen van kritische vragen aan en stelt meer eisen aan de manier waarop organisaties met data omgaan. Binnen een federatieve samenwerking worden organisaties al in de ontwerpfases betrokken om deze zo breed draagbaar en toepasselijk te maken. Vanuit verschillende vakgebieden, denk aan: ethisch, juridisch, en veiligheid.

Breed geaccepteerde en gedragen ontwerpprincipes worden extra belangrijk als het gaat om het geautomatiseerd verwerken van grote hoeveelheden data en het toepassen van kunstmatige intelligentie. Een structureel personeelstekort bij de overheid in combinatie met de groeiende hoeveelheid beschikbare data maakt het echter noodzakelijk processen te automatiseren. Net zoals het gebruik van data is het ook bij automatisering noodzakelijk kennis en kunde in het voortraject te delen. Door met ketenpartners samen naar mogelijkheden te kijken en informatie over processen te delen, ontstaat kennis. Deze kennis, over bijvoorbeeld de context en het doel van gebruik, zorgt ervoor dat de juiste taken en stappen geautomatiseerd worden. Het doel van automatisatie is synergie tussen mens en techniek waardoor medewerkers zich op de inhoud kunnen richten. Hetzelfde geldt voor AI: witwassen in steeds complexer, opsporingstechnieken moeten mee evolueren om bij te blijven.

Succesvolle federatieve samenwerking die aantoonbaar en voortdurend binnen de geaccepteerde kaders opereert biedt ook kansen om vertrouwen terug te winnen. Door samen te werken worden verschillende oogpunten betrokken bij het ontwerpen van automatisering en AI-oplossingen. Zo worden deze niet alleen effectiever maar ook beter uitlegbaar. Door transparant te zijn kan dit helpen bij het terugwinnen van vertrouwen van burgers. In de woorden van EU digital chief, Margrethe Verstage: “Bij AI is vertrouwen een vereiste, geen nice-to-have”[18].

Conclusie

Kijkend naar de toekomst is het een vereiste om kennisdeling en samenwerking te verbeteren. Criminelen letten niet op de scheiding tussen afdelingen of gebieden, sterker nog: ze zullen hier actief misbruik van maken als hier zwakheden ontdekt worden. De overheid en banken hebben naast verschillende machtsposities ook verschillende kennis en kunde. Initiatieven zoals de FEC richten zich op samenwerking waarop voortgebouwd kan worden. Hierbij is het belangrijk dat deze doelstellingen en manier van werken tot op bestuursniveaul wordt gesteund. Daarnaast is het belangrijk de dialoog open te houden en kennis te blijven delen.

AI/automatisering is niet optioneel maar noodzaak in de toekomst. Met name onder het structurele personeelstekort. Door samen te werken binnen de keten worden ontwerp principes niet alleen kwalitatief beter maar ook brerder geaccepteerd. Transparantie over waarom en hoe data is gebruikt biedt mogelijkheden om maatschappelijk vertrouwen op dit vlak terug te winnen.

Het automatiseren van processen en gebruik van AI zorgt voor synergie tussen medewerkers en techniek. Zo kan de juiste informatie uit data gehaald worden en kunnen medewerkers zich richten op het bouwen van cases. Of bijvoorbeeld preventie: door AI kwetsbare situaties te leren herkennen kan er eerder voorlichting door de overheid gegeven worden.

Over de auteurs

Christiaan den Hartog

Senior Business Analyst Insights & Data.

Als Business Analist werkt Christiaan tussen in voor overheidsinstanties in het veiligheidsdomein. Hij faciliteert de samenwerking tussen instanties en ondersteunt klanten bij het vinden van oplossingen voor data gedreven vraagstukken

christiaan.den.hartog@capgemini.com

Erwin Vorwerk

Lead Insights & Data voor Financial Services.

Als lead insights & data bij Capgemini richt Erwin zich op de financiële sector in Noord-Europa. Zijn focus ligt op het ondersteunen van klanten om zo veel mogelijk waarde uit data te halen.

erwin.vorwerk@capgemini.com

[9]https://www.groene.nl/artikel/pakkans-0-083-procent
[10] https://magazines.rijksoverheid.nl/jenv/jenvmagazine/2021/16/hoofdartikel
[11]https://www.fec-partners.nl/over-fec/
[12]https://www.nwo.nl/nieuws/integrale-aanpak-onderzoek-naar-ondermijnende-criminaliteit-kic
[13]FIU jaarverslag 2020
[14]https://www.capgemini.com/research/the-data-powered-enterprise/ (rapport, fig 13)
[15]https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving
[16]https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_NL.html
[17]https://www.verzekeraars.nl/media/8082/toolkit-ethisch-kader_def.pdf
[18]https://www.bbc.com/news/technology-56830779

06

DE TOEKOMST VAN AI-GEZICHTSHERKENNING IN HET NEDERLANDSE VEILIGHEIDSDOMEIN

Hoe kunnen organisaties in het Nederlandse veiligheidsdomein AI-gezichtsherkenning, gezien de ingrijpende (wets) ontwikkelingen, optimaal blijven toepassen in de nabije toekomst?

Gezichtsherkenningstechnologie, gedreven door AI, wordt in toenemende mate ingezet binnen het publieke veiligheidsdomein voor bijvoorbeeld (zware) misdrijven en grenscontroles. Dit artikel beschrijft de (juridische) kaders en lopende discussies op Europees niveau om de toekomstige grenzen van de toepassing van AI-gezichtsherkenning te verkennen.

Highlights

- AI-gezichtsherkenning verwerkt gevoelige biometrische gegevens.
- Het Nederlandse veiligheidsdomein experimenteert al met verschillende gezichtsherkenningstechnologieën.
- Er woedt een juridische discussie over de (privacy-)rechten van burgers bij de inzet van AI-gezichtsherkenning.
- De AI-verordening gaat gezichtsherkenningstechnologie aan strengere criteria onderwerpen.
- Gedegen belangenafwegingen en de juiste maatregelen zijn essentieel bij de inzet.

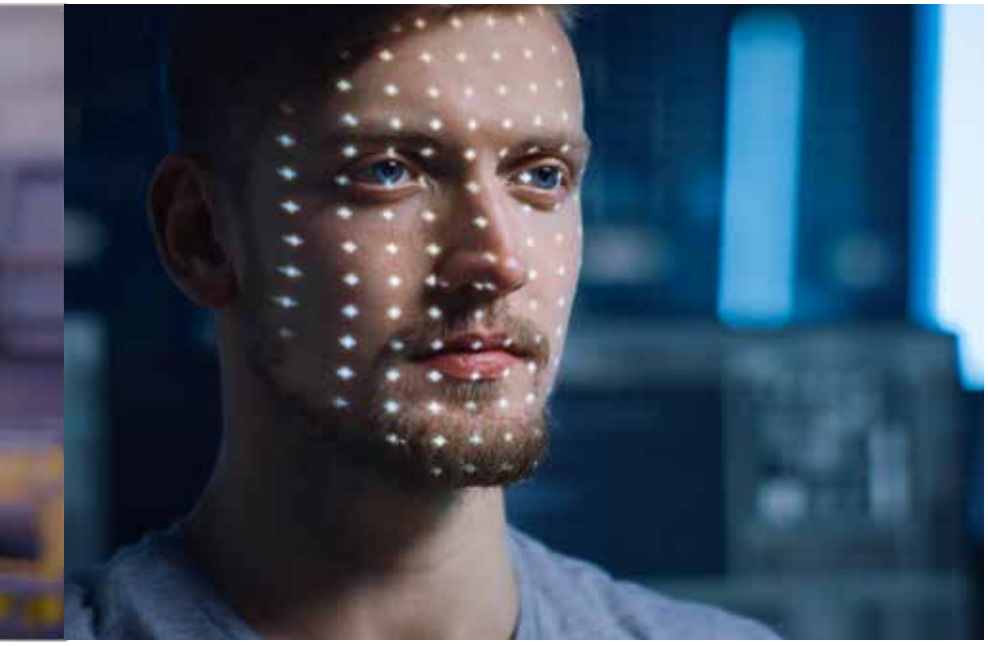
Definitie van (AI-) gezichtsherkenning

Gezichtsherkenningstechnologie bestaat uit een reeks algoritmen die samenwerken om mensen in een video of een statisch beeld te identificeren. Deze technologie bestaat al langere tijd, maar is de laatste jaren veel gangbaarder en innovatiever geworden. Een van die innovaties is de integratie van kunstmatige intelligentie (AI) in gezichtsherkenningssystemen. Intelligente, op AI gebaseerde software kan direct in databases met gezichten zoeken en deze vergelijken met één of meerdere gezichten die in een bepaald beeld worden gedetecteerd[1].

AI houdt zich bezig met de ontwikkeling van slimme machines die taken kunnen uitvoeren waarvoor normaal gesproken enige menselijke intelligentie nodig is.

Foto's van het gezicht kunnen onder bepaalde omstandigheden als 'biometrische gegevens' worden gezien. Dit zijn 'persoonsgegevens die het resultaat zijn van een specifieke technische verwerking van

Een voorbeeld van het gebruik van AI-gezichtsherkenning binnen het Nederlandse veiligheidsdomein is het gebruik van ‘slimme’ camera’s bij voetbalstadions naar aanleiding van de rellen bij een wedstrijd van NEC tegen Vitesse. Het project is opgestart in november 2021.



fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon’[2]. Deze gegevens worden behandeld als bijzondere persoonsgegevens die in hun aard zeer gevoelig zijn en daarom wettelijk extra zijn beschermd.

Gebruik van AI-gezichtsherkenning in Nederland

Er moet daarom in het kader van privacy en gegevensbescherming zeer zorgvuldig worden omgegaan met gezichtsherkenningstechnologie. Dit is met name in het veiligheidsdomein van belang, door de grote schaal van gegevensverzameling en de ingrijpende beslissingen over burgers die op basis van de technologie gemaakt worden. Er is dan ook een maatschappelijke discussie gaande over de inzet van AI-gezichtsherkenning in de publieke ruimte. Privacy vormt hier een belangrijk aspect in. Enerzijds biedt de technologie veel mogelijkheden voor het Nederlandse veiligheidsdomein om efficiënter publieke taken uit te voeren. Anderzijds loert onder andere het gevaar van ‘biometrische surveillance’: het op grote schaal ‘in de gaten houden’ van burgers in de publieke ruimte, en daarmee schending van hun (privacy-)rechten[3]. Aldus is een gedegen aanpak gewenst.

Een voorbeeld van het gebruik van AI-gezichtsherkenning binnen het Nederlandse veiligheidsdomein is het gebruik van ‘slimme’ camera’s bij voetbalstadions naar aanleiding van de rellen bij een wedstrijd van NEC tegen Vitesse. Het project is opgestart in november 2021. Het kabinet wil zo voetbalgeweld en overlast rondom stadions tegengaan. Als iemand een stadionverbod krijgt, moet degene binnen zes weken een recente foto van zichzelf bij het stadion afgeven. De stadions beschikken over gezichtsherkenningscamera’s die gezichten van bezoekers kunnen opsporen[4]. Lang niet alle stadions maken momenteel gebruik van deze slimme camera’s.

Een tweede voorbeeld is het gebruik van gezichtsherkenningssoftware op Schiphol. Luchtvaartmaatschappijen en de overheid begonnen in juli 2021 een proef met registratiekiosken die beschikken over gezichtsherkenning. Personen kunnen zich op hun eigen initiatief registreren. Door registratie bij de speciale kiosk kun je verschillende controlepunten op Schiphol gemakkelijker en contactloos passeren. Ook bespaart de marechaussee zo op controlepersoneel[5].

Tevens werkt de politie in het Innovatie lab (‘Ilab’) aan innovatieve oplossingen voor veranderende veiligheidsuitdagingen in de toekomst. Dit gebeurt door middel van innovatieve technologie, waaronder AI-gezichtsherkenning, en door slimme samenwerkingen[6].

Privacy-uitdagingen op Europees en nationaal niveau

Het Nederlandse veiligheidsdomein heeft bij de toepassing van AI-gezichtsherkenning te maken met diverse wet- en regelgeving, zowel op Europees als nationaal niveau.

Europees niveau

Recentelijk hebben op Europees niveau enkele grote ontwikkelingen plaatsgevonden. Zo heeft het wetsvoorstel van de Europese Commissie (EC) over de inzet van kunstmatige intelligentie de discussie rondom de inzet van AI-gezichtsherkenning in het veiligheidsdomein verder aangewakkerd[7]. Het wetsvoorstel plaatst AI-technologieën in diverse risicocategorieën (zie afbeelding 1).

Technologieën die vallen onder de hoogste categorie bevatten onaanvaardbare risico's voor individuen en worden daardoor verboden, terwijl de laagste categorie met minimale regulering te maken krijgt. AI binnen het publieke veiligheidsdomein, aangeduid als "law enforcement" en "asylum and border management", wordt geplaatst binnen de een-na-hoogste categorie "high risk". De EC stelt een aantal strenge eisen aan de technologie binnen deze categorie voordat het veiligheidsdomein het mag inzetten, waaronder:

- Adequate systematiek voor risico-inschatting;
- Hoge kwaliteit van gebruikte datasets;
- Uitgebreide logging om keuzes en resultaten te traceren;
- Gedetailleerde instructies over de technologie en haar werkwijze;
- Heldere en adequate informatie naar de gebruiker of betrokkene;
- Menselijke tussenkomst en toezicht op het systeem;
- Hoge mate van veiligheid.

Met betrekking tot gezichtsherkenning is het wetsvoorstel ook zeer strikt: 'Real-time' AI-gezichtsherkenning is in het algemeen verboden in de publieke ruimte. Een uitzondering geldt voor opsporingsdiensten, zoals de politie, die 'real-time' AI-gezichtsherkenning mogen toepassen om onder andere criminaliteit te voorkomen en bestrijden.
De uitkomsten van het wetsvoorstel zette de Europese privacy toezichthouders op scherp. Vlak na het wetsvoorstel brachten de European Data Protection Board (EDPB) en de European Data Protection Supervisor (EDPS) een joint opinion uit[8]. Ze pleitten hierin voor een algehele ban op gezichtsherkenning in de openbare ruimte. Hier ligt aan ten grondslag dat de techniek voor grote inbreuk op het privéleven van individuen kan zorgen en de veronderstelling van burgers dat ze zich anoniem in openbare ruimtes kunnen begeven. Een aanpassing van het wetsvoorstel met meer aandacht voor de privacywetgeving is dus gewenst volgens de toezichthouders.

Inmiddels heeft de EC in oktober een resolutie aangenomen waarin ze de inzet van AI-gezichtsherkenning verder aan banden wil leggen[9]. Men stelt voor om de techniek nu enkel in te zetten voor criminaliteitsbestrijding, mits strenge controle plaatsvindt. De EC wil verbieden dat commerciële bedrijven databases voor gezichtsherkenning van Europese burgers aanleggen, zoals ClearviewAI. Bovenstaande ontwikkelingen zullen impact hebben op de definitieve AI-verordening. Dit zal uiteindelijk de inzet van de technologie voor het Nederlandse veiligheidsdomein beïnvloeden.

Figure 1: De risicocategorieën van de AI Verordening

Nationaal niveau

De discussie over de inzet van AI-gezichtsherkenning speelt niet alleen op Europees, maar ook op nationaal niveau. In Nederland heeft de Autoriteit Persoonsgegevens (AP), de nationale toezichthouder voor privacy en gegevensbescherming, een supermarkt op de vingers getikt vanwege hun gebruik van gezichtsherkenning als beveiligingsmiddel. De AP stelde dat een goede balans moest bestaan tussen het doel van de beveiliging en het zwaarwegende belang van een individu om niet gescand te worden door gezichtsherkenningstechnologie. Daarnaast moet de betrokkene altijd uitdrukkelijk toestemming kunnen geven, zoals volgt uit de Algemene verordening gegevensbescherming[10]. De privacy van de betrokkene vormt dus altijd het kernpunt van de balans bij de inzet van gezichtsherkenningstechnologie.

In het Verenigd Koninkrijk heeft het Hof in Cardiff, in de enige Europese zaak tot nu toe, besloten dat het gebruik van publieke gezichtsherkenning door de politie wel voldoet aan de eisen van proportionaliteit en wettelijkheid[11]. Het Hof herkende de inbreuk op privacy, maar vond deze niet zwaarder wegen dan het nut van de gezichtsherkenning.

De verschillen tussen de voorbeelden in Nederland en het Verenigd Koninkrijk tonen aan dat veel beoordelingsruimte bestaat voor rechtbanken en toezichthouders. Het recht op privacy en gegevensbescherming wordt zo constant afgewogen tegen het beoogd gebruik van de gezichtsherkenning en de kaders waarin de technologie wordt ingezet.

Aandachtspunten voor de toekomst van AI-gezichtsherkenning

Op basis van de huidige discussie en (wets-)ontwikkelingen op Europees en nationaal niveau, zoals in dit artikel wordt geschetst, zijn de volgende aspecten van groot belang voor de inzet van AI-gezichtsherkenning in het Nederlandse veiligheidsdomein in de nabije toekomst:

1. Afweging van fundamentele rechten en gezichtsherkenningstechnologie

Uit de voorbeelden op zowel Europees als nationaal niveau blijkt dat bij inzet van AI-gezichtsherkenning een belangrijke (juridische) afweging vereist is. De techniek kan over het algemeen worden ingezet, zeker in het Nederlandse veiligheidsdomein, maar moet wel binnen duidelijke kaders worden ontworpen en ingezet. Er moet continu een balans zijn tussen het nut van de technologie en de impact daarvan op individuen. Twee elementen vormen hierbij de kern: proportionaliteit en subsidiariteit. Proportionaliteit richt zich op de vraag of de gezichtsherkenning ontwikkeld en ingezet wordt op een wijze die in verhouding staat tot het doel. Is het bijvoorbeeld nodig om álle gezichten van álle verdachten te analyseren? Subsidiariteit betreft het zoeken naar alternatieven, zoals de CNIL ook vereiste van de school. Als een minder inbreuk makende technologie voorhanden is, moet daar altijd voor gekozen worden. Het belang van deze balans zal in toenemende mate naar voren komen in de toekomst, met de introductie van de AI-Verordening.

2. De invloed van nieuwe (wets-) ontwikkelingen rondom de inzet van AI-gezichtsherkenning

Wet- en regelgeving biedt ruimte om AI-gezichtsherkenning in bepaalde vormen toe te passen binnen het veiligheidsdomein. Gezien de recente ontwikkelingen zijn enkele aandachtspunten in het bijzonder van belang voor de nabije toekomst:

Europees als nationaal niveau blijkt dat bij inzet van AI-gezichtsherkenning een belangrijke (juridische) afweging vereist is. De techniek kan over het algemeen worden ingezet, zeker in het Nederlandse veiligheidsdomein, maar moet wel binnen duidelijke kaders worden ontworpen en ingezet.

Aangescherpte wettelijke criteria

Het wetsvoorstel van de aankomende AI-verordening laat zien dat Europese Unie haar grip op de regulering van AI-technologie flink verstevigd. Nergens ter wereld bestaat een soortgelijk kader, waardoor Europa als koploper gezien kan worden. Naar verwachting is de verordening in 2024 toepasbaar voor het Nederlandse veiligheidsdomein[12]. Tegen die tijd zullen organisaties bij de inzet van AI-gezichtsherkenning moeten voldoen aan de wettelijke criteria die gelden voor "high risk" categorieën. Voor het veiligheidsdomein is het dus belangrijk om te beoordelen welke impact de AI-verordening zal hebben op de huidige inzet en toekomstige plannen rondom AI-gezichtsherkenning. Op basis daarvan kunnen organisaties al in een vroeg stadium rekening houden met de (nieuwe) wettelijke criteria.

Privacy vormt onmiskenbare pijler

Het belang van privacy bij de inzet van AI-gezichtsherkenning is extra benadrukt door de Europese privacy toezichthouders en zal leiden tot aangescherpte privacy maatregelen in de definitieve AI-verordening. De AVG blijft de belangrijkste leidraad om privacy te borgen voor het Nederlandse veiligheidsdomein. De principes rondom dataminimalisatie, privacy by design, datakwaliteit, transparantie en geautomatiseerde besluitvorming zullen verhoogde aandacht krijgen. Het veiligheidsdomein zal dan ook prioriteit moeten (blijven) geven aan deze principes in hun te voeren beleid.

Discussie is nog niet uitgekristalliseerd

De ontwikkelingen en discussies in aanloop naar de definitieve AI-verordening geven blijk van een dynamisch speelveld voor AI-technologieën. De toekomst zal uitwijzen binnen welke contouren het Nederlandse veiligheidsdomein AI-gezichtsherkenning kan blijven toepassen voor opsporingsdoeleinden. Het is daarom zaak voor organisaties om de (wets-)ontwikkelingen nauwlettend te volgen en een bijdrage te leveren aan de maatschappelijke discussie.

[1]Volgens de Groep gegevensbescherming artikel 29 wordt onder gezichtsherkenning het volgende verstaan: 'Een automatische verwerking van een digitale afbeelding van het gezicht van een persoon ten behoeve van de identificatie, authenticatie of verificatie of categorisering van die persoon.' Groep Gegevensbescherming Artikel 29, Advies 02/2012, p. 2 (link).
[2]Ziehttps://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_regels_voor_gezichtsherkenning_in_supermarkten.pdf
[3]Zie https://edri.org/wp-content/uploads/2021/07/The-Rise-and-Rise-of-Biometric-Mass-Surveillance-in-the-EU_Dutch-Summary.pdf.
[4]Zie https://www.gld.nl/sport/7431451/een-stadionverbod-na-voetbalrellen-dit-zijn-de-straffen-die-je-kan-krijgen en https://www.parool.nl/nederland/hardere-aanpak-tegen-voetbalgeweld-en-overlast-rond-stadions~b747c6a2/?referrer=https%3A%2F%2Fwww.google.com%2F
[5]Zie https://www.schiphol.nl/nl/pagina/proef-met-gezichtsherkenning-bij-vertrek/

Conclusie

AI-gezichtsherkenning biedt veel mogelijkheden voor het Nederlandse veiligheidsdomein. Het is mogelijk om sneller verdachten op te sporen met grote hoeveelheden data die tegenwoordig beschikbaar zijn. Aan de andere kant lopen op dit moment Europese en nationale discussies over de juridische (privacy) kaders waarbinnen dergelijke technologie moet worden geplaatst. Uit deze discussies blijkt dat, ondanks de voordelen van AI-gezichtsherkenning, gedegen belangenafwegingen en maatregelen bij de ontwikkeling van de technologie van groot belang zijn. Met name om de impact op de fundamentele rechten van betrokkenen zo beperkt mogelijk te houden. In dit artikel is met een toekomstvisie gepoogd deze kaders helder uiteen te zetten en de lopende discussies samen te vatten om zo de onvermijdelijke ontwikkeling van AI-gezichtsherkenning te stimuleren.

Over de auteurs

Selma Mujčić

Privacy Consultant

Selma is een gedreven privacy consultant met als focus innovatieve technologieën en strategieën. Ze heeft ervaring binnen zowel de publieke als de commerciële sector.

selma.mujcic@capgemini.com

Mattis van 't Schip

Privacy consultant

Mattis was ten tijde van het schrijven van dit artikel in dienst bij Capgemini als Privacy en Cybersecurity consultant, waarbij hij zich bezighield met privacyvraagstukken in de publieke sector.

Manisha Ramsaran

Privacy consultant

Manisha werkt als privacy consultant bij Capgemini. Ze houdt zich bezig met privacyvraagstukken binnen de private en publieke sector.

manisha.ramsaran@capgemini.com

[6] iLab: https://www.politie.nl/informatie/welkom-bij-ilab.html.
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.
[8] https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.
[9] https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html.
[10] https://autoriteitpersoonsgegevens.nl/nl/nieuws/formele-waarschuwing-ap-aan-supermarkt-om-gezichtsherkenning
[11] https://www.theguardian.com/technology/2019/sep/04/police-use-of-facial-recognition-is-legal-cardiff-high-court-rules
[12] Zie https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

07

EEN DIGITAAL WEERBAAR NEDERLAND IN HET AI-TIJDPERK

Hoe kan Nederland zich wapenen tegen AI-gedreven aanvallen en dreigingen?

De nationale veiligheid staat onder druk door een toename van cyberaanvallen, desinformatie, nepnieuws en autonome wapens. Enerzijds wordt de impact vergroot door AI. Anderzijds biedt AI enorme kansen voor de Nederlandse veiligheidssector om zich tegen deze aanvallen en dreigingen te wapenen.

Highlights

- Nederland heeft steeds meer te maken met AI-gedreven aanvallen en dreigingen zoals cyberaanvallen, desinformatie, nepnieuws en autonome wapens.
- AI-gedreven innovatie biedt ook juist kansen voor de Nederlandse veiligheidssector om tegenwicht te bieden.
- Door onderschatting, gebrek aan samenwerking en spaarzame investeringen is Nederland kwetsbaar voor AI-gedreven aanvallen.
- AI wordt verantwoordelijker, slimmer en beter schaalbaar; betere samenwerking en investeringen zijn nodig om hiervan te profiteren.
- We bieden handreikingen waarmee de veiligheidssector bij kan dragen aan een digitaal weerbaar Nederland.

AI van lab naar samenleving: Een tweesnijdend zwaard

Het afgelopen decennium heeft Artificiële Intelligentie (AI) de weg gevonden van het lab naar de samenleving. Experts voorspellen dan ook een blijvende explosie aan AI-gedreven innovaties. Dit maakt ons leven aangenamer en biedt kansen voor een betere wereld, zoals robots die landmijnen deactiveren[1], AI-aangedreven voertuigen voor de inzet van humanitaire hulp[2], computervisie om de potvispopulatie te identificeren en op te sporen[3] en een intelligent dataplatform voor kleine boeren in Kenia dat helpt bij het oplossen van het wereldvoedseltekort[4].

De integratie van AI in ons dagelijks leven raakt echter belangrijke waarden van onze samenleving zoals veiligheid, autonomie, vrijheid, burgerrechten, de rechtstaat en rechtvaardigheid. De NCTV en het NCSC waarschuwen voor een toenemende digitale dreiging die tot ontwrichting van de maatschappij kan leiden en waartegen de huidige weerbaarheid onvoldoende is[5]. Het (geautomatiseerd) verspreiden van onjuiste of suggestieve informatie draagt bij aan polarisatie en vormt een bedreiging voor onze democratie en openbare orde. De import van digitale dictatuur door de mogelijkheden van AI voor massasurveillance is hierbij een reëel gevaar[6]. Bovendien geeft AI voor militaire toepassingen zero-sum game voordelen aan landen en is er feitelijk een AI-wapenwedloop gaande[7]. Europa loopt gevaar. De westerse

waarden en machtspositie staan onder druk doordat niet-westerse staten verder zijn in het ontwikkelen van AI-oplossingen en niet schromen om deze op (naar westerse maatstaven) onethische wijze in te zetten. De beroemde Amerikaanse diplomaat Henry Kissinger vergelijkt AI zelfs met nucleaire wapens. Beiden zijn een instrument om geopolitieke voordelen te behalen en onderwerp van een wedloop tussen grootmachten, met het potentieel van totale vernietiging[8].

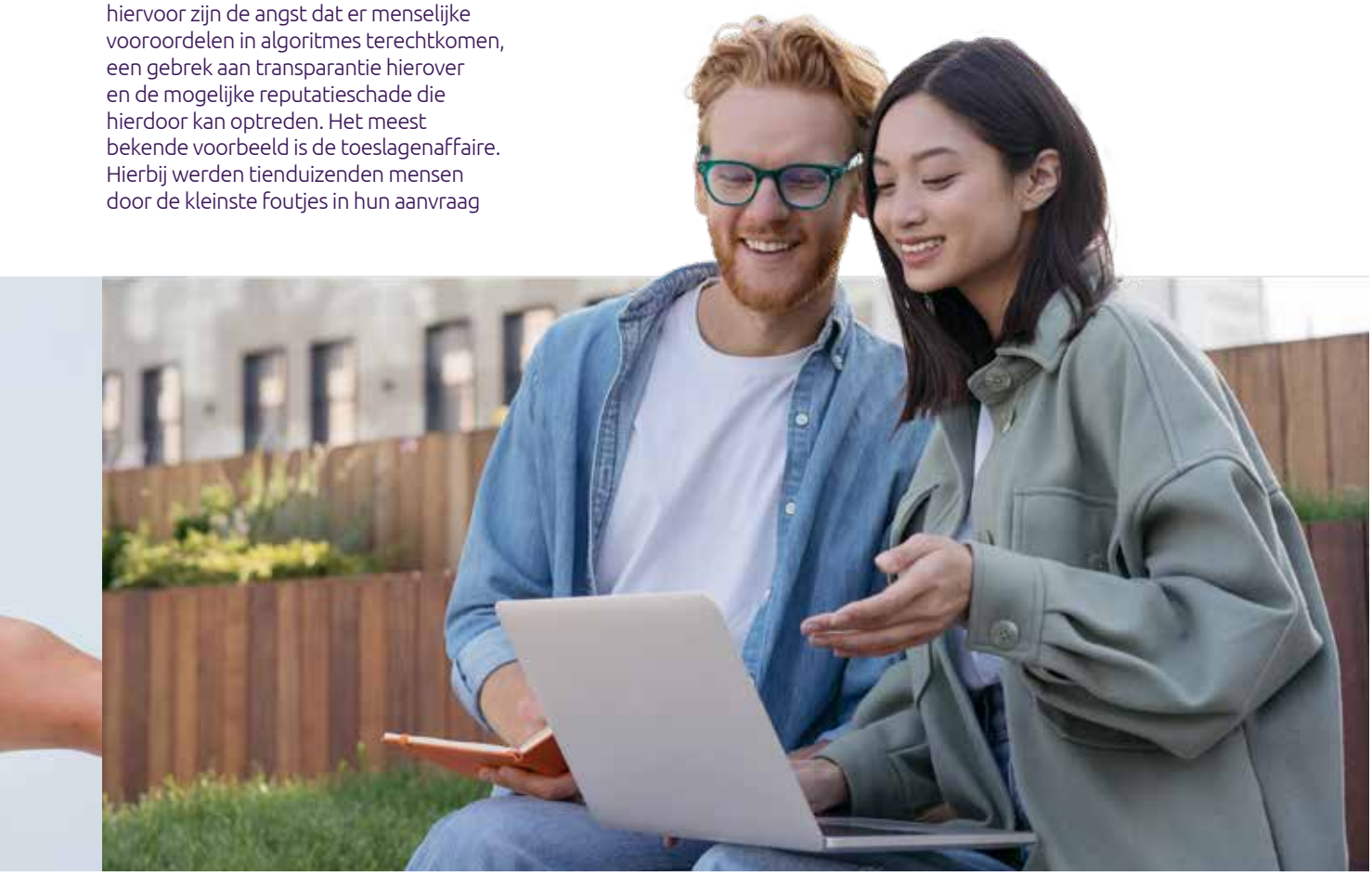
In dit artikel beschrijven we twee zaken: (1) de kansen die AI biedt voor een veiliger Nederland en (2) concrete handreikingen om te profiteren van AI-technologieën om digitaal weerbaar te blijven.

Kansen genoeg: AI wordt verantwoordelijker, slimmer en beter schaalbaar

Gartner verwacht dat AI de komende jaren slimmer, verantwoordelijker en beter schaalbaar wordt[9]. Binnen de overheid zien we echter terughoudendheid in het gebruik van AI-toepassingen. Oorzaken hiervoor zijn de angst dat er menselijke vooroordelen in algoritmes terechtkomen, een gebrek aan transparantie hierover en de mogelijke reputatieschade die hierdoor kan optreden. Het meest bekende voorbeeld is de toeslagenaffaire. Hierbij werden tienduizenden mensen door de kleinste foutjes in hun aanvraag voor kinderopvangtoeslag en door menselijke vooroordelen in het algoritme onterecht als fraudeur bestempeld. Het terugbetalen van de toeslagen bracht vele gezinnen in ernstige financiële problemen met alle gevolgen van dien. Daarnaast zijn er zorgen over toenemende surveillance, zoals camera's met gezichtsherkenningssoftware.

AI de komende jaren slimmer, verantwoordelijker en beter schaalbaar wordt. Binnen de overheid zien we echter terughoudendheid in het gebruik van AI-toepassingen.

Bovengenoemde affaires en zorgen leiden enerzijds tot meer bewustwording over de gevaren van AI en dragen bij aan de trend naar verantwoordelijke en transparante AI. Anderzijds heeft dit geleid tot toenemend technoscepticisme. Met name in de publieke sector staat dit AI-gedreven innovatie in de weg. Daarom is het van belang dat de trend van verantwoordelijke en transparante AI wordt doorgezet. Dit betekent dat AI-toepassingen moeten voldoen aan wetgeving en ethische principes en dat de databeveiliging en privacy op orde is. Ervoor zorgen dat algoritmen voor toetsing en evaluatie publiekelijk



beschikbaar zijn, draagt hieraan bij, zoals bijvoorbeeld het Amsterdam algoritme register. Het voortzetten van deze trend om AI verantwoordelijker te maken, is belangrijk om tegenwicht te bieden aan AI-ontwikkelingen in concurrerende staten, zodat Nederland (als onderdeel van de EU) regie behoudt over de richting waarin AI zich ontwikkelt m.b.t. Europese normen en waarden.

Verantwoordelijke AI biedt draagvlak om meer data te verzamelen voor het trainen van AI-modellen, waardoor deze slimmer worden. Daarbij hebben AI-systemen het vermogen om te blijven leren van ervaringen met data wanneer deze (op grotere schaal) operationeel worden ingezet[10]. Tech auteur en ondernemer Tom Rikert onderscheidt drie niveaus van AI-toepassingen, waarbij de toegenomen waarde exponentieel groeit per stap: AI tools (2-5X), force multipliers (10X) en automatisering (100X)[11]. De Nederlandse veiligheidssector zou moeten streven naar het creëren van force multipliers en waar mogelijk naar ethisch verantwoorde volledige automatisering. Op dit terrein worden er al goede stappen gezet zoals bijvoorbeeld de nieuwe DNA-techniek van het Nederlands Forensisch Instituut, waarbij binnen drie dagen een DNA-spoor geautomatiseerd aan een crimineel kan worden gematcht. Voorheen kostte dit veel mankracht en weken doorlooptijd[12]. Verder kan er worden gedacht aan autonome systemen die bij defensie 'saaie, vieze en gevaarlijke' taken overnemen, zoals bijvoorbeeld zelfrijdende voertuigen die zwaar materiaal kunnen dragen of personeel uit vijandelijk gebied kunnen trekken. Ook kan AI ingezet worden om het situationeel inzicht te vergroten over de gevechtsruimte en om besluitvorming voor gerichte inzet van middelen te ondersteunen (informatie gestuurd optreden). Bovendien is AI cruciaal geworden in het detecteren, voorspellen en adequaat kunnen reageren op cyberaanvallen.

Om echt impact te maken, is het zaak dat AI-innovaties op grotere schaal worden toegepast en dat de weg van proeftuinen naar volledige inzet makkelijker wordt gevonden. Technologie zoals opslag- en rekenkracht is hierbij niet langer de beperkende factor. Cloud-technologie maakt het makkelijker om op te schalen. Daarnaast heeft de coronacrisis een versnelling in de digitalisering teweeggebracht, waarbij een groot deel van de beroepsbevolking IT-vaardigheden heeft opgedaan die waardevol zijn voor AI-innovaties. Dit biedt kansen voor een grotere adoptie van AI-toepassingen.

Figure 1: De risicocategorieën van de AI Verordening[13]

Handreikingen voor een digitaal weerbaar Nederland

Om eerdergenoemde AI-gedreven dreigingen en aanvallen het hoofd te bieden, pleiten we voor een aanpak op verschillende niveaus. Op internationaal niveau zijn, net als tijdens de Koude Oorlog, diplomatie en internationale afspraken en richtlijnen cruciaal om te voorkomen dat de AI-wapenwedloop uit de hand loopt en AI op onethische wijze wordt ingezet.

Op nationaal niveau willen we het belang van samenwerking en kennisdeling benadrukken. Ten eerste is het delen van inlichtingen over cyberdreigingen van groot belang, zowel onderling als tussen inlichtingendiensten en bedrijven. Cyber- en AI-expertise uit de private sector is hierbij onmisbaar.

Ten tweede zal de publieke veiligheidssector meer moeten investeren in AI-innovatie. Niet alleen financieel, maar ook daadkracht en houding. Ook met de huidige middelen en juridische kaders is er meer mogelijk dan er nu gebeurt. Zo worden mogelijkheden voor het proactief opsporen en hacken van cybercriminelen nog onvoldoende benut[14]. Hierin kan AI ingezet worden bij het identificeren van verdacht netwerkverkeer en hackpogingen in gigantische hoeveelheden (log)data.

Wat kunnen organisaties zelf doen om AI-kansen te benutten? Ten eerste is het belangrijk dat er een heldere en gedragen AI-strategie is. In welke vaardigheden is de organisatie uniek of leidend? Zet AI-innovaties daarop in om force multipliers te creëren.

Ten tweede zijn multidisciplinaire en diverse AI-teams een must. Deze dienen niet alleen uit techneuten en data scientists te bestaan. Domeinexperts kunnen de juiste input geven voor het ontwikkelen van algoritmes zodat het AI-systeem kan leren om goede en foute antwoorden te onderscheiden[15]. De beschikbaarheid van privacy- en informatiebeveiligingsexperts vormt vaak een bottleneck, terwijl zij essentieel zijn voor de voortgang en acceptatie van een AI-oplossing. Diversiteit in termen van leeftijd, gender, cultuur en ideeën zorgt voor creativiteit en het minimaliseren van vooroordelen in algoritmen. Verklein daarbij de afstand tussen het AI-team, de gebruikers en de maatschappelijke omgeving waarin AI wordt toegepast. Dit bevordert de relevantie en acceptatie[16].

Ten derde zijn proof of concepts met AI een manier op laagdrempelig te beginnen in een veilige leeromgeving en de toegevoegde waarde aan te tonen voordat de oplossing wordt geïmplementeerd[17]. Het inzetten van AI in de veiligheidssector vraagt meer aandacht

voor nauwkeurigheid en rechtvaardigheid dan bijvoorbeeld een recommendation engine voor films en tv-series. Dit vraagt om extra aandacht voor het testen voordat het systeem operationeel wordt ingezet. De grootste bottleneck zit echter in de implementatie. Dit vraagt van een organisatie dat deze een proces heeft ingericht om innovatieve ideeën naar een werkende oplossing te brengen en na evaluatie desgewenst te implementeren. Hierbij is niet alleen AI-expertise cruciaal, maar ook verandermanagement en een volwassen moderne IT-organisatie die het snel inpassen van nieuwe toepassingen mogelijk maakt. (Zie ook ons artikel in TiV 2021 'Willen, moeten, kunnen: de weg naar informatiegestuurd werken', waarin we ingaan op hoe de veranderbereidheid in de organisatie kan worden versterkt.)

Ten vierde vraagt effectief en ethisch gebruik van AI-systemen om specifieke vaardigheden. Alle werknemers hebben een basisniveau datageletterdheid nodig zodat kansen voor AI worden gezien en benut. Dit betekent zeker niet dat iedereen moet kunnen programmeren, maar wel dat medewerkers kennis hebben over hoe data van waarde kan zijn en dat datakwaliteit cruciaal is om tot betrouwbare inzichten te komen. Daarbij is het kritisch kunnen beoordelen van aanbevelingen door AI-systemen van belang om te zorgen dat de menselijke maat bij het gebruik van algoritmen niet verloren gaat. Zeker in de veiligheidssector kunnen besluiten die grote impact kunnen hebben op de levens van mensen niet zonder meer volledig uit handen worden gegeven. Daarnaast is het van belang dat cyber awareness onder medewerkers wordt vergroot om de organisatie weerbaarder te maken. Zo trainen veel bedrijven tegenwoordig hun personeel op het herkennen van steeds geavanceerdere phishing e-mails. Behalve het trainen en opleiden van het huidige personeelsbestand betekent dit ook het aantrekken van geschikt personeel.

Ten vijfde mag het belang van datamanagement niet worden onderschat. Data is het bloed van een organisatie en dient daarom beschouwd te worden als een vitaal bedrijfsmiddel. Reken maar eens uit wat het kost om verloren data opnieuw op te bouwen of aan te schaffen. Plannen, beleid, programma's en processen om data te beschermen en de waarde ervan te vergroten zijn niet zo sexy als AI, maar minstens zo belangrijk. Bovendien kan AI een rol spelen in het slimmer of sneller uitvoeren van datamanagementactiviteiten, zoals data profiling.

Ten zesde is het belangrijk om te investeren in methoden en technologieën specifiek voor digitale weerbaarheid, zoals AI voor inspectie van software, strenge beveiliging voor certificaten en gedistribueerde beveiligingscontroles. Daarnaast adviseren we red teaming, waarbij wordt gepoogd AI voor de gek te houden en daarmee weerbaarder te maken tegen vijandige aanvallen.

Tenslotte wordt vertrouwen in AI opgebouwd door kleine stukjes verantwoordelijkheid aan het systeem te delegeren. Net zoals je stapsgewijs kinderen steeds meer verantwoordelijkheid geeft bij een taak totdat ze steeds zelfstandiger worden.

Conclusie

De Nederlandse veiligheidssector moet maximaal profiteren van de kansen die AI biedt om de weerbaarheid te versterken tegen AI-gedreven dreigingen. AI wordt slimmer, verantwoordelijker en schaalbaarder. Dit biedt legio kansen om de informatiepositie te verbeteren, processen te automatiseren en zich te wapenen tegen vijandige actoren, die ook flink inzetten op deze technologie.

Over de auteurs

Luuk Tubbing

Senior Consultant

Luuk Tubbing werkt als Senior Consultant voor Capgemini Insights & Data. Hij is gespecialiseerd in intelligence- en datavraagstukken in het domein openbare orde- en veiligheid.

luuk.tubbing@capgemini.com

Siebe Vaartjes

Senior Consultant

Siebe Vaartjes is Senior Consultant bij Capgemini Business Technology Services. Hij is actief in het openbare orde- en veiligheidsdomein op het gebied van Intelligence en Informatie Gestuurd Werken.

siebe.vaartjes@capgemini.com

[1]https://algorithm.data61.csiro.au/designing-robots-to-detect-and-deactivate-landmines/
[2]https://aiforgood.itu.int/event/ai-powered-vehicles-for-humanitarian-help-deployment/
[3]https://www.capgemini.com/nl-nl/nieuws/capgemini-gebruikt-ai-om-potvispopulatie-te-identificeren-en-op-te-sporen/
[4]https://www.capgemini.com/client-story/project-farm-an-intelligent-data-platform-to-resolve-global-food-shortages/
[5]https://www.nctv.nl/actueel/nieuws/2021/06/28/nctv-cyberaanvallen-tasten-zenuwstelsel-maatschappij-aan
[6]https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie
[7]https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie
[8]https://fd.nl/tech-en-innovatie/1425727/in-de-beperking-van-ai-toont-zich-de-meester-ula2cajEVsEZ
[9]https://www.gartner.com/smarterwithgartner/gartner-top-10-data-and-analytics-trends-for-2021
[10]https://www.uu.nl/organisatie/verdieping/het-ontrafelen-van-de-black-box-van-ai
[11]https://insights.nextworldcap.com/ai-hype-has-peaked-so-whats-next-8c72f5e28ea3
[12]https://www.rtlnieuws.nl/nieuws/nederland/artikel/5280674/dna-onderzoek-forensisch-instituut-sneller-uitvinding-politie
[13]https://insights.nextworldcap.com/ai-hype-has-peaked-so-whats-next-8c72f5e28ea3
[14]https://www.volkskrant.nl/nieuws-achtergrond/waarom-hackt-de-politie-ransomwarebendes-niet-helemaal-de-tering~b7671d0a/
[15]https://insights.nextworldcap.com/ai-hype-has-peaked-so-whats-next-8c72f5e28ea3
[16]https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie
[17]https://www.coursera.org/learn/ai-for-everyone

08

ONDERMIJNENDE CRIMINALITEIT VIA WITWASSEN MET CADEAUKAARTEN

De vijfde EU anti-witwasrichtlijn geeft de retailsector een poortwachtersfunctie. Hoe dit te effectueren?

De vijfde EU anti-witwasrichtlijn beperkt het gebruik van de cadeaubon en geeft de retailsector een poortwachtersfunctie. Hoe kan zij deze rol effectueren en wat is daarvoor nodig?

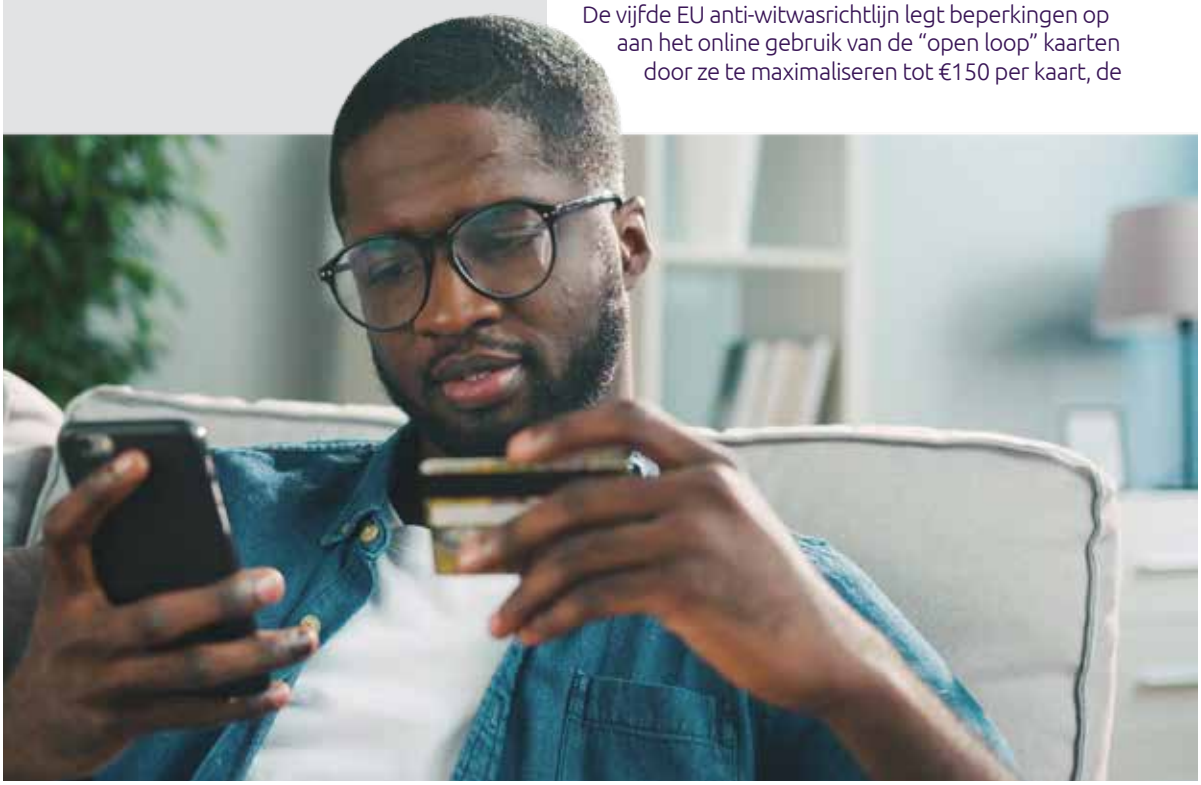
Highlights

- De vijfde EU anti-witwasrichtlijn beperkt onlinegebruik van de cadeaubon.
- Trends in online aankopen, gebruik cadeaukaarten en gevoeligheid voor witwassen.
- Retailsector heeft toenemende rol als poortwachter in anti-witwas strijd.
- Witwasindicatoren in het gebruik van cadeaukaarten.
- Risico-gebaseerd transactiemonitoringsproces in de strijd tegen witwassen.

Sinds 1991 wordt in toenemende mate vanuit de Europese Unie (EU) en de Nederlandse wetgever een strijd gevoerd tegen crimineel en onverklaarbaar vermogen. De eerste focus lag met name op de financiële- en vastgoedsector, maar sinds 2021 zijn de pijlen ook explicieter gericht op de retailsector. De EU had deze sector al in het vizier bij transacties ter waarde van minimaal vijf cijfers en verdachte contante betalingen. Met de vijfde EU anti-witwasrichtlijn[1] wordt de strijd intensiever aangegaan, vooral door het online gebruiken van anonieme bij meerdere retailers te besteden betaal- of cadeaukaarten(open loop) te beperken door middel van verplichte acceptatielimieten. Betaal-cadeaukaarten besteedbaar bij één retailer (closed loop) laat zij voorlopig met rust. Hierdoor biedt deze kaart nog steeds mogelijkheden tot witwassen. Tegelijk geeft het ook kansen om verdachte transacties en witwassers te identificeren. De retailsector heeft een poortwachtersfunctie met bijbehorende verplichtingen, die op de closed-loop cadeaukaarten uitstekend kunnen, eigenlijk moeten, worden toegepast.

Beperkingen open loop versus closed loop

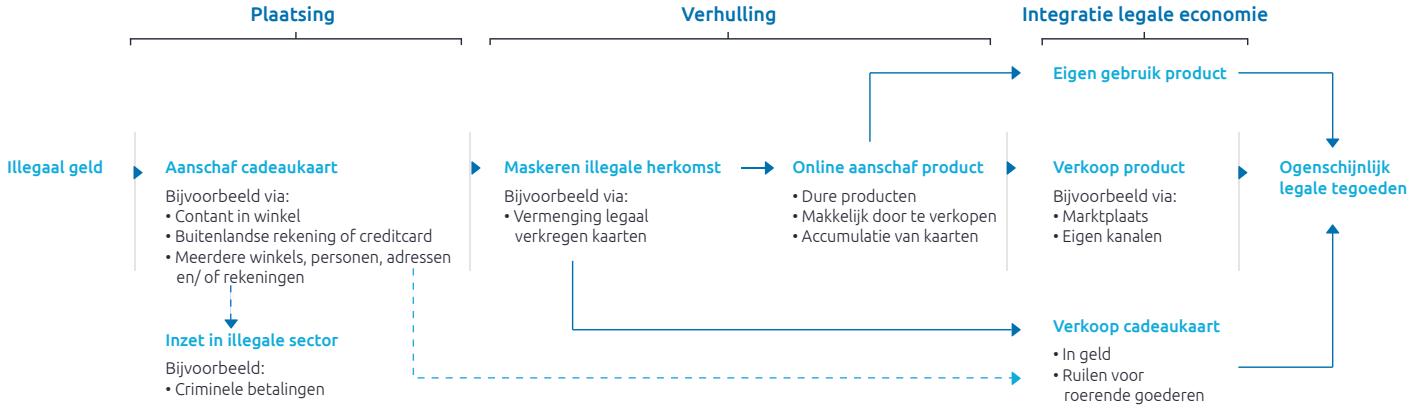
De vijfde EU anti-witwasrichtlijn legt beperkingen op aan het online gebruik van de “open loop” kaarten door ze te maximaliseren tot €150 per kaart, de



verplichtstelling van een clientonderzoek bij online bestedingen van meer dan €50 en het combineren van kaarten te begrenzen tot €50 per aankoop. Clientonderzoek is voor de meeste detailhandelaren niet haalbaar, waardoor zij op veilig spelen door zelf cadeaubonnen te maximaliseren tot €50. Witwassen via online besteding van "open loop" betaalkaarten is onmogelijk gemaakt, doordat de maatregelen de kosten-baten analyse voor de crimineel onvoordelig laat uitpakken.

'Closed loop' betaalkaarten hebben die beperkingen niet. Deze kaarten mogen maximaal €250 bevatten, kennen inherent geen verplichting tot clientonderzoek of verbod van cumulatie. Voor deze cadeaukaarten bestaat nog steeds de onlinemogelijkheid om illegaal geld een ogenschijnlijke legale oorsprong te geven. In een relatief korte periode, vooral bij bestellingen op diverse namen en adressen, kan op deze wijze duizenden tot tienduizenden euro's witgewassen worden. Het proces wordt in het onderstaande schema uiteengezet.

Figure 1: Het witwasproces



Prevalentie versus risico

Over deze transitie van illegale naar legale tegoeden zijn geen officiële cijfers bekend. Wel over de totale online retailmarkt in verhouding met cadeaukaarten in Nederland. In de eerste helft van 2021 vonden er 182,2 miljoen[2] online aankopen plaatst met een waarde van €14,8 miljard. Dit vertegenwoordigt 12,7% van de totale aankopen in deze periode in Nederland. Een groei van 17% ten opzichte van het jaar ervoor. 23% van de aankopen, 42 miljoen artikelen ter waarde van totaal €3,4 miljard (in 6 maanden) werden afgerekend met cadeaukaarten. Dit is maar liefst 64% meer dan een jaar eerder[2]. Over de verdeling van "open en closed" kaarten zijn geen gegevens bekend, maar online winkelen is een sterk groeiende markt. Cadeaukaarten vormen een steeds groter aandeel, net als de aantrekkelijkheid als witwasmiddel.

Het WODC plaatst betaalkaarten niet op de lijst van grootste witwasrisico's in haar "National Risk Assessment Witwassen 2019"[3]. Deze lijst is gebaseerd op inschattingen vanuit een reeks expertmeetings, waarin de retailsector sterk ondervertegenwoordigd is. Daarnaast is de lijst niet gebaseerd op prevalentie maar op geschatte impact, hetgeen een subjectief karakter heeft.

Witwassen is een fenomeen dat anonimiteit opzoekt en cadeaukaarten bieden dit bij uitstek. Ook heeft witwassen met cadeaukaarten geen aparte registratie binnen de opsporing, maar valt het onder andere kapstokken zoals witwassen en

[1]Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=NL
[2]Thuiswinkel.org, Markt Monitor 2021 HY1

Dit wordt onderschreven door de Europese Commissie in een impact assessment uit 20164. Zij geeft hierin aan dat de hoge mate van anonimiteit gecombineerd met de gigantische, en groeiende, omvang van de markt van deze betaalmiddelen tevens een groeiend risico vormen voor witwassen.

fraude. Het wordt dus niet geregistreerd, waardoor het dark number vermoedelijk zeer groot is.

Dit wordt onderschreven door de Europese Commissie in een impact assessment uit 2016[4]. Zij geeft hierin aan dat de hoge mate van anonimiteit gecombineerd met de gigantische, en groeiende, omvang van de markt van deze betaalmiddelen tevens een groeiend risico vormen voor witwassen. Dit assessment is de basis geweest voor de implementatie van de beperkingen in de vijfde witwasrichtlijn.

Retailsector als poortwachter

De vijfde richtlijn kent, via de Wet ter voorkoming van witwassen en financiering van terrorisme (Wwft)[5], een meldingsplicht en clientonderzoeksverplichting toe aan verkopers van goederen indien een betaling of een reeks verband houdende betalingen in contanten plaatsvindt voor een bedrag van €10.000 of meer. “Contanten” en chartaal geld zijn synoniemen van elkaar. Cadeaubonnen worden gezien als chartaal geld en vallen daarmee onder betalingen in contanten. Bijgevolg komen deze twee verplichtingen op deze transacties te rusten. Deze wetgevingen geven retailers daarnaast de derde verplichting om elke verdachte giraal of chartaal verlopen witwastransacties te melden aan het Financial Intelligence Unit (FIU).

Met deze drie verplichtingen heeft de richtlijn en bijgevolg de Wwft van de retailsector poortwachters gemaakt in de strijd tegen crimineel en onverklaarbaar vermogen. Dit zullen de retailers moeten oppakken op straffe van strafrechtelijke vervolging voor een economisch delict. Deze poortwachtersfunctie en haar drie verplichtingen zijn voor de 'open loop' cadeaukaarten grotendeels ontweken door witwassen onmogelijk te maken, door respectievelijk EU wetgeving en marktregulatie. Echter, de functie en de bijkomende verplichtingen bestaan nog voor de 'closed loop' kaarten.

Deze poortwachtersfunctie bestaat op twee momenten; bij de aanschaf van cadeaubonnen en online betaling met dit betaalmiddel. Het eerste moment verloopt door cash aanschaf in een winkel of online bestelling. Bij een contante betaling van de cadeaubon heeft de winkelier de taak te waken voor witwassen. Opleiding en een bewustwordingscampagne zijn hier de sleutel tot detectie. De winkelier zal vermoedelijk minder geneigd zijn te acteren op witwassignalen, immers het raakt zijn omzet. Bij online bestellingen worden vaak buitenlandse bankrekeningen, (prepaid) creditcards en/of bedrijven gebruikt om zo de pakkans te minimaliseren.

[3]Wetenschappelijk Onderzoek- en Documentatiecentrum, H.C.J. van der Veen e.a., National Risk Assessment Witwassen 2019 (Cahier 2020-11), 2020. https://repository.wodc.nl/bitstream/handle/20.500.12832/249/Cahier_2020-11_Volledige_tekst_tcm28-453997.pdf?sequence=2&isAllowed=y

[4]Werkdocument SWD (2016) 223 van de diensten van de Commissie van 5 juli 2016 betreffende de effectenbeoordeling, bijgevoegd bij het voorstel voor de richtlijn van het Europees Parlement en de Raad tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering en tot wijziging van Richtlijn 2009/101/EG https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2016:0223:FIN:EN:PDF

[5]Wet ter voorkoming van witwassen en financieren van terrorisme van 15 juli 2008, BWBR0024282, Stb. 2008, 303 https://wetten.overheid.nl/BWBR0024282/2022-01-28

[6]Aanhangsel Handeling II 2021/12, nr. 927. https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2021Z19707&did=2021D47223

Risico-gebaseerd transactiemonitoringsproces

De kern van dit schrijven is te pleiten voor het gebruik van een risico-gebaseerd transactiemonitoringsproces op deze onlinebestellingen, waarbij transacties via algoritmes gemonitord worden op risicogevoeligheden en detectieregels. Dit is de verantwoordelijkheid van de retailer en de doelbinding wordt ondersteund door het wettelijk kader van de vijfde richtlijn en Wwft. De detectieregels zullen zich concentreren op gebruikelijke indicatoren, zoals risicoland, risicopersonen of aanverwanten, risicosectoren en risicobedragen. Daarnaast zijn verdachte patronen interessant als indicator. Dit zijn vooral niet reguliere bestellingen van cadeaukaarten, zoals een maandelijks terugkerende bestelling van hetzelfde bedrag, betaald met een buitenlandse creditcard op naam van een buitenlandse naamloze vennootschap.

Sterk vergelijkbare algoritmes kunnen tevens gebruikt worden op de monitoring van met cadeaukaarten gedane bestellingen van producten, het tweede moment van de poortwachtersfunctie. De algoritmes dienen wel aangevuld te worden met indicatoren zoals frequentie van bestellingen, zelfde soort producten (bv. dure laptops), zelfde leveringsadres, zelfde familienaam en/of frequentie van bestede cadeaukaartwaarde. Vooral de combinatie van de indicatoren kunnen belangrijke signalen vormen voor verdachte transacties. Indien artificial intelligence toegepast wordt op de indicatorcombinaties en algoritmes, zal dit zelflerend vermogen potentieel een krachtig wapen kunnen worden in de strijd. Uiteraard met ethische en morele bewaking ingebouwd in de business rules en menselijke factor van die algoritmes. Hiervoor zou de retailers zelf verantwoordelijk zijn, met toezicht vanuit de Autoriteit Persoonsgegevens.

Vergelijkbare (transactie) monitoringsprocessen worden reeds gebruikt in de financiële sector en binnen de opsporing, gespecificeerd naar haar specifieke sectorkarakteristieken en “klanten”. De meeste grote online productenaanbieders gebruiken al algoritmes en monitoringsprocessen, echter worden ze momenteel voornamelijk ingezet voor verkoop- en dus winstmaximalisatie en de detectie van frauduleuze betalingen. De kennis van risico-gebaseerde transactiemonitoringsprocessen is dus reeds aanwezig in de sector, maar zullen moeten worden aangepast voor detectie van witwas gerelateerde betalingen. Het is een aanzienlijke opgave met een behoorlijke kostenpost qua tijd en geld. Hierbij wordt wel degelijk beseft dat het risicomonitoringsproces, vanwege het automatisch karakter, vals-positieve witwassignalen zal geven, waardoor een menselijke controle noodzakelijk is.

De financiële sector heeft ook lang geworsteld met de vraag hoe de poortwachtersfunctie effectief en efficiënt in te vullen. Uiteindelijk zal de retailsector deze investeringen wel moeten doen, omdat ze de retailer zullen beschermen tegen strafvervolging op basis van de Wet op Economische Delicten en imagoschade. Het Bureau Toezicht Wwft, onderdeel van de Belastingdienst, heeft hier als toezichthouder uiteraard een rol in te spelen.

Kan de FIU dit aan?

De toestroom van verdachte transactiemeldingen richting de FIU vanuit de retailsector is potentieel gigantisch en het is maar de vraag of zij deze stijging het hoofd kan bieden. Vermoedelijk niet, want ze komen namelijk bovenop de huidige, steeds stijgende, aantallen vanuit andere publieke en private partners. Deze zorgen reeds voor capaciteitsproblemen. De laatste jaren heeft de FIU, volgens voormalig Minister Grapperhaus (Justitie en Veiligheid), geïnvesteerd in uitbreiding en efficiëntie van de analysecapaciteit en zal dit blijven doen[6]. Echter, dit is gebaseerd op de huidige groei en niet op die vanuit de retailsector. De FIU zal dus harder moeten groeien en nog meer efficiëntie moeten brengen in haar analysecapaciteit. De organisatie zal een nog prominentere rol binnen de opsporing, en potentieel beleid, gaan vormen. Daarnaast zal er rijkere data naar de infobox Crimineel en Onverklaarbaar Vermogen (iCOV) vloeien, waardoor haar financiële netwerkbeelden en rapporten uitgebreidere opsporingsinformatie zullen bevatten. De opsporingsonderzoeken gaan hierdoor effectiever worden, net als de veroordelingen.

Over de auteur

Johan Klercq

Senior Consultant Openbare Orde en Veiligheid, Adviseur Anti Money Laundering & Criminoloog

Johan Klercq is werkzaam bij Capgemini BTS. Johan is gespecialiseerd in ondermijning, witwassen en georganiseerde criminaliteit binnen het openbare orde en veiligheidsdomein en richt zich op advies en analyse met betrekking tot opsporing, detectieprocessen en informatiebeveiliging.

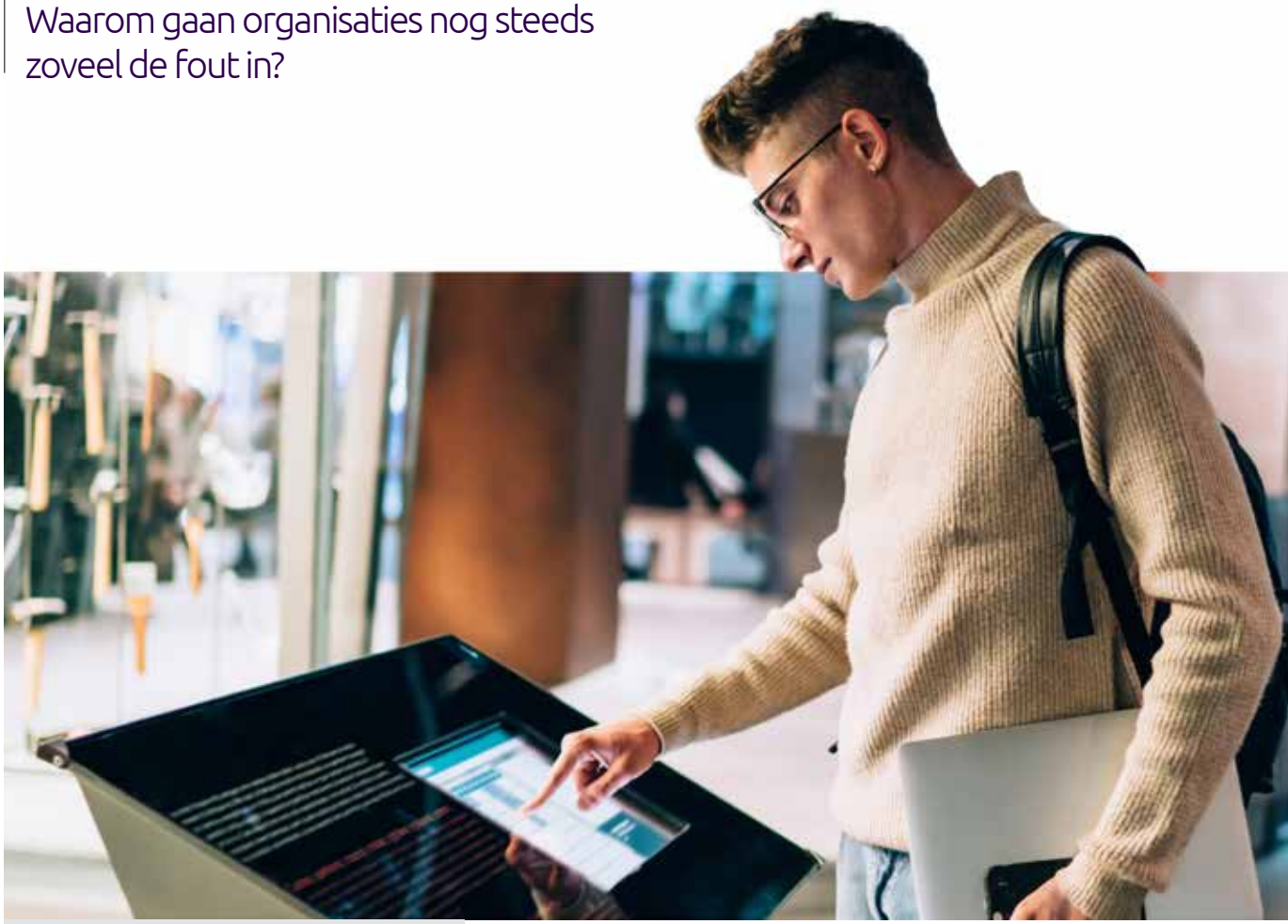
Voor meer informatie kunt u contact met de auteur opnemen via:

johan.klercq@capgemini.com

09

AI ZONDER BIAS IS EEN LEUGEN

Waarom gaan organisaties nog steeds zoveel de fout in?



SyRi, Amazon's recruitment, profileren en de toeslagenaffaire. Voorbeelden van onethisch handelen op basis van algoritmes. Data en AI zijn hier de oplossing voor, niet het probleem.

Highlights

- Organisaties zijn te afhankelijk van hun algoritmes en data.
- AI is altijd biased, net als mensen.
- Modellen zijn juist ontwikkeld om bias te meten, niet te verhelpen.
- Beoordeel de prestaties van AI alleen in vergelijking met een mens.
- Wisselwerking tussen mens en machine is nodig om elkaar te controleren.

Hoe ontstaat bias?

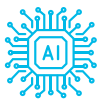
Veel moderne schrijvers besteden aandacht aan de gevaren en gevolgen van bias in AI en data, zoals discriminatie en gebrek aan transparantie in beslissingen. Zo ook in deze editie van Trends in Veiligheid. Echter, hierbij wordt vaak over het hoofd gezien dat de problemen ouder zijn dan deze technologie, en dat AI en data ook een belangrijk deel van de oplossing vormen.

Moderne wetenschap gebruikt steeds meer data en statistiek om bias te detecteren en tegen te gaan. Dit wordt vaak kortzichtig behandeld. Bias is slecht, verwerpelijk en het mag niet. Algoritmes dienen eerlijk, volledig transparant en unbiased te zijn. Er wordt daarom binnen organisaties en wetgeving unbiased AI geëist. Zonder na te denken over hoe dat teweeg moet worden gebracht en nog belangrijker, of het überhaupt mogelijk is.

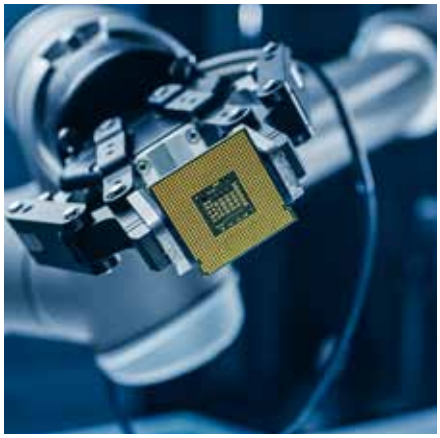
Ethisch verantwoord gebruik van data trekt veel aandacht. Organisaties als WikiLeaks en bewegingen als Black Lives Matter en LGBTQ pleiten voor groter bewustzijn rondom ethiek en gelijkheid. Binnen organisaties heersen veel vraagstukken over gelijkheid – denk

aan recruitment, loonongelijkheid en onbedoeld etnisch profileren bij predictive policing. Juist hier ontstaan steeds meer vragen over AI en algoritmes, over eerlijkheid en bias. Echter, neemt AI deze vraagstukken mee in haar beslissingen? Dat bias een deel is van de mens wordt al snel geaccepteerd. Maar men verwerpt dat bias ook deel is van machines.

Er zijn twee soorten bias te onderscheiden. De eerste is wetenschappelijke bias. Dit is een bias voortkomend uit niet-representatieve data. Data zal in de meeste gevallen nooit helemaal representatief zijn. Dit betekent dat zelfs een 'perfect' model fouten kan maken omdat data nooit perfect is. De tweede soort bias is menselijke bias: onjuiste vooroordelen ten gunste van of ten nadele van iets of iemand. Het gaat in dit artikel om de tweede soort bias en hoe die deel uitmaakt van zowel mens als AI.



AI en algoritmes, over eerlijkheid en bias. Echter, neemt AI deze vraagstukken mee in haar beslissingen? Dat bias een deel is van de mens wordt al snel geaccepteerd. Maar men verwerpt dat bias ook deel is van machines.



Het is belangrijk om te snappen dat een AI-model niet begrijpt wat bias is. Wat een mens wel of niet als bias opvat is afhankelijk van maatschappelijke normen en waarden. Een persoon niet aannemen vanwege een bepaalde werkervaring of huidskleur is voor een computer hetzelfde, terwijl een niet passende opleiding in onze samenleving een goede reden zou kunnen zijn om iemand niet aan te nemen maar een andere huidskleur niet. Machines hebben ook last van tunnelvisie, maar een ander soort dan een agent of belastingadviseur.

Om bias in beslissingen te voorkomen proberen we verschillen in keuzes niet af te laten hangen van bijvoorbeeld etniciteit of gender. Verschillende groepen moeten gelijk behandeld worden, in het streven naar minder ongelijkheden tussen mannen en vrouwen, of mensen van verschillende afkomst. Toch kan er indirecte discriminatie voorkomen, zoals:

- Een systeem dat CV's beoordeelt zal systematisch mensen met "buitenlands-klinkende" namen minder kans geven om aangenomen te worden dan mensen met een "Nederlands-klinkende" naam[1].
- Een systeem dat in juridische zaken voorziet van oordelen zal mannen sneller hogere straffen geven dan vrouwen[2].
- Een systeem dat al jaren loonsverhogingen berekent zal gewend zijn vrouwen minder te betalen dan hun mannelijke collega's[3].
- Een fraudesysteem zal eerder zoeken binnen bevolkingsgroepen waar deze fraude al eerder heeft plaatsgevonden.

De reden is niet dat deze zelflerende AI-systemen inherent discriminerend, racistisch of seksistisch zijn. Machine Learning algoritmes zijn namelijk ontzettend goed in twee dingen: leren van historische data en patronen vinden in data om keuzes op te baseren. Data verkregen uit keuzes die mensen hebben gemaakt zal de biases bevatten van deze mensen. Wanneer een AI wordt getraind op die data, zal de oplossing daarom ook onvermijdelijk bias bevatten. Een AI leert namelijk niet de beste keuzes te maken, een AI leert keuzes maken zoals die al zijn gemaakt. Het legt daarbij dus bias van mensen bloot.

Hier wordt een pijnpunt duidelijk: AI toont bias aan in menselijk handelen, maar dit is lastig om te accepteren. Het vereist namelijk dat we onze fouten, uitgedrukt in data, onder ogen zien, accepteren en er naar handelen. AI wordt waarschijnlijk niet gebruikt met de intentie om iemand nadelig te behandelen, maar zonder een wakend oog en gericht beleid zullen bevooroordeelde besluiten worden genomen die achteraf volledig worden gewijd aan AI. Dit is natuurlijk kortzichtig en gevaarlijk.

Een voorbeeld hiervan zijn de gebeurtenissen rondom PredPol[4]. PredPol is software die in de Verenigde Staten wordt gebruikt om criminaliteit te voorspellen. Het politiedistrict dat PredPol gebruikt, krijgt gebieden te zien waar criminaliteit is voorspeld. De politieagenten gaan deze gebieden dan meer patrouilleren dan andere gebieden. In 2016 meldde een mediabedrijf dat PredPol onterecht vaker verwees naar achterstandswijken. Eind 2021 werd er een rapport gepubliceerd waarin werd aangetoond dat PredPol vooroordelen

Wanneer we eisen van AI dat deze unbiased is dan zijn we hier hard in. Volledig unbiased AI of anders geen AI. Er wordt een mate van onfeilbaarheid geëist die van een mens niet gevraagd zou worden.

op basis van huidskleur in stand hield door het blijven verwijzen naar achterstandswijken. Hierdoor werd de (rijke en blanke) middenklasse gespaard en achterstandswijken gedupeerd.

Nog een voorbeeld is bias in de vorm van onderrepresentatie. Dit komt vaak voor in gezichtsherkenningsalgoritmes. Datasets die gebruikt worden voor gezichtsherkenning bevatten voornamelijk westerse blanke mensen. Andere etniciteiten zijn hierin ondergerepresenteerd. Gezichtsherkenning-algoritmes scoren hierdoor slechter op mensen van kleur. Dit kan zorgen voor error rates die tot 34% hoger zijn voor vrouwen van kleur dan witte mannen[5]. In een studie door het National Institute of Standards and Technology van 189 gezichtsherkenning algoritmes wordt beschreven dat misclassificaties van gekleurde en aziatische gezichten 10 tot 100 keer meer voorkomen dan van blanke gezichten. Als de politie een dergelijk systeem gebruikt, kan door misclassificatie een agent geadviseerd worden de verkeerde persoon te arresteren.

Waarom is de manier waarop we naar bias in AI kijken kortzichtig?

De wens om af te komen van biases is logisch. Het probleem is dat veel organisaties en wetgeving een einddoel eist (unbiased AI) zonder de route er naartoe te bepalen – of zich af te vragen of dit überhaupt mogelijk is. Bias is afhankelijk van geschiedenis en de maatschappelijke norm van wat goed en slecht is. Het is de menselijke ethiek die bepaalt wat bias is – en die ethiek verandert over de tijd. Wanneer we eisen van AI dat deze unbiased is dan zijn we hier hard in. Volledig unbiased AI of anders geen AI. Er wordt een mate van onfeilbaarheid geëist die van een mens niet gevraagd zou worden.

Dit is een onproductieve houding richting AI én mensen. Van mensen wordt er geëist dat ze ethisch handelen, maar er wordt niet verwacht dat ze dit niet altijd zullen doen, want dat is onrealistisch. Eenzelfde houding is nodig richting AI. Onfeilbare systemen bestaan niet.

Het probleem kan opgelost worden door het doel aan te passen. Het huidige doel is om unbiased AI te creëren, maar hoe is dit mogelijk als hetgeen wat als bias wordt gezien verandert met de tijd. Het doel kan dus niet statisch zijn, maar moet juist dynamisch zijn. Het moet meegaan met de tijd. Een beter doel zou zijn om AI te creeëren die minder biased is dan de mens.

AI hoeft namelijk niet de beste te zijn, maar enkel beter dan de mens. De belangrijkste vraag is niet hoe goed of unbiased de machine is, maar hoe goed of unbiased de machine is in vergelijking met een mens? Vaak blijkt dat een mens, gewapend met data van de machine, betere en meer eerlijke conclusies kan trekken dan zonder. Zo kunnen mens en machine elkaar versterken.

Wat doe je dan met de bias?

De mens heeft geen algoritmes nodig om te discrimineren, maar data en algoritmes zijn wel nodig om discriminatie aan te tonen. Moderne psychologie, bedrijfskunde en sociale wetenschappen gebruiken veel empirische data om ongelijkheid en bias te onderzoeken. Sterker nog, de meeste AI-algoritmes van de afgelopen dertig jaar zijn juist ontwikkeld om causale effecten aan te tonen. Om effecten en invloeden te duiden, ongeacht heersende normen of waarden.

Veel dataprojecten leggen juist problemen bloot in recruitment en bias in primaire processen. Een deel van de reden dat zoveel data science projecten 'falen' is niet omdat modellen slecht zijn, maar omdat de uitkomsten niet geaccepteerd worden door de business. Dan blijkt er discriminatie plaats te vinden of vaart management de verkeerde koers. Algoritmes leggen deze bloot. Niet voor niets zijn er zoveel klokkenluiders tegenwoordig.

Om deze problemen voor te zijn moeten bedrijven meer data gedreven gaan werken. Inzetten op kennis en techniek, via algoritmes inzicht verkrijgen om te sturen en bedrijfsvoeren. Niet enkel KPI's opstellen voor bestaande processen. Of een dataclub opzetten zonder deze

De meeste AI-algoritmes van de afgelopen dertig jaar zijn juist ontwikkeld om causale effecten aan te tonen. Om effecten en invloeden te duiden, ongeacht heersende normen of waarden.

zeggenschap te geven om processen te veranderen. Alleen door je medewerkers de kennis en middelen geeft om met data en statistiek om te gaan kan je je organisatie wapenen tegen de risico's van data. Niet alleen onbedoelde discriminatie. Maar ook privacy en bestuur.

Een voorbeeld van hoe dit fout kan gaan, is de toeslagenaffaire. Hier hield de Belastingdienst lijsten met namen van ouders met dubbele nationaliteiten bij, omdat deze meer risico op fraude met zich mee zouden brengen. Een direct voorbeeld van profileren en biased handelen. De Belastingdienst had hier beter gebruik moeten maken van algoritmes om deze bias te detecteren en tegen te gaan, in plaats van blind te varen op een lijst en kritiek te negeren. Het gevolg was overtreding van de grondwet, duizenden mensen die onterecht in schulden zijn beland en hun huizen en gezinnen kwijtraakten. Dit had voorkomen kunnen worden.

Laat medewerkers niet blind vertrouwen op procedures of 'black box'-algoritmes. Maar bewapen ze met de kennis om zelf betrouwbare datamodellen met duidelijke werking en invloeden te produceren. Je kan een algoritme dat je niet volledig begrijpt niet zonder toezicht gebruiken. Op dezelfde manier dat je een menselijk team waarin je de mensen niet kent niet zonder toezicht kan laten functioneren.

Conclusie

Binnen moderne AI heerst een paradox: We zijn bang voor de problemen die de oplossing veroorzaakt, maar we zijn ook bang dat de oplossing nieuwe problemen veroorzaakt. We stellen dat bias in AI ontstaat, omdat het leert van de bias in menselijk handelen om zo keuzes te kunnen maken. De mens heeft die bias namelijk, vaak onbewust, meegenomen in hun beslissingen. De manier waarop we kijken naar bias in AI is kortzichtig omdat er een onfeilbaar systeem wordt geëist. Onfeilbare systemen bestaan niet.

Het doel om unbiased AI te creëren is een onhaalbaar doel. Bias is een dynamisch principe en het doel dient dus even dynamisch te zijn: "Creëer AI die minder biased is dan de mens".

Ook de rechtsstaat is niet onfeilbaar. In plaats van falen enkel te voorkomen - of dit nu mens of AI is - het systeem is robuust juist omdat het om kan gaan met falen, met fouten, met bias.

Data is cruciaal om te zien wat goed én fout gaat. Alleen een data gedreven organisatie kan de voordelen – en niet enkel de nadelen – van data ervaren. Organisaties moeten een wisselwerking creëren tussen mens en machine. Beide dienen elkaar te controleren en terecht te wijzen.

Een volledig unbiased mens bestaat niet en een volledig unbiased algoritme bestaat ook niet.

Beiden zijn nodig om elkaar te versterken.

Over de auteurs

Marijn Markus

AI Lead & Managing Data Scientist

Als Managing Data Scientist richt Marijn zich op het inzetten van data om mensenlevens te verbeteren. Marijn stuurt data teams aan bij verschillende organisaties en maakt onderscheid tussen science en fictie op events.

marijn.markus@capgemini.com

Joris de Jong

Data Engineer & AI Engineer

Joris is een AI engineer en richt zich voornamelijk op het integreren van duurzame oplossingen. Hij focust zich op de continue verbetering van bestaande algoritmes.

joris.de-jong@capgemini.com

René Flohil

AI Engineer & Data Scientist

René is AI Engineer en is opgeleid in de richting van Machine Learning en Neuromorphische Neurale Netwerken. Om de interdisciplinaire kracht van AI te maximaliseren verbindt René graag mensen met verschillende expertises om zo de grenzen van AI op te zoeken.

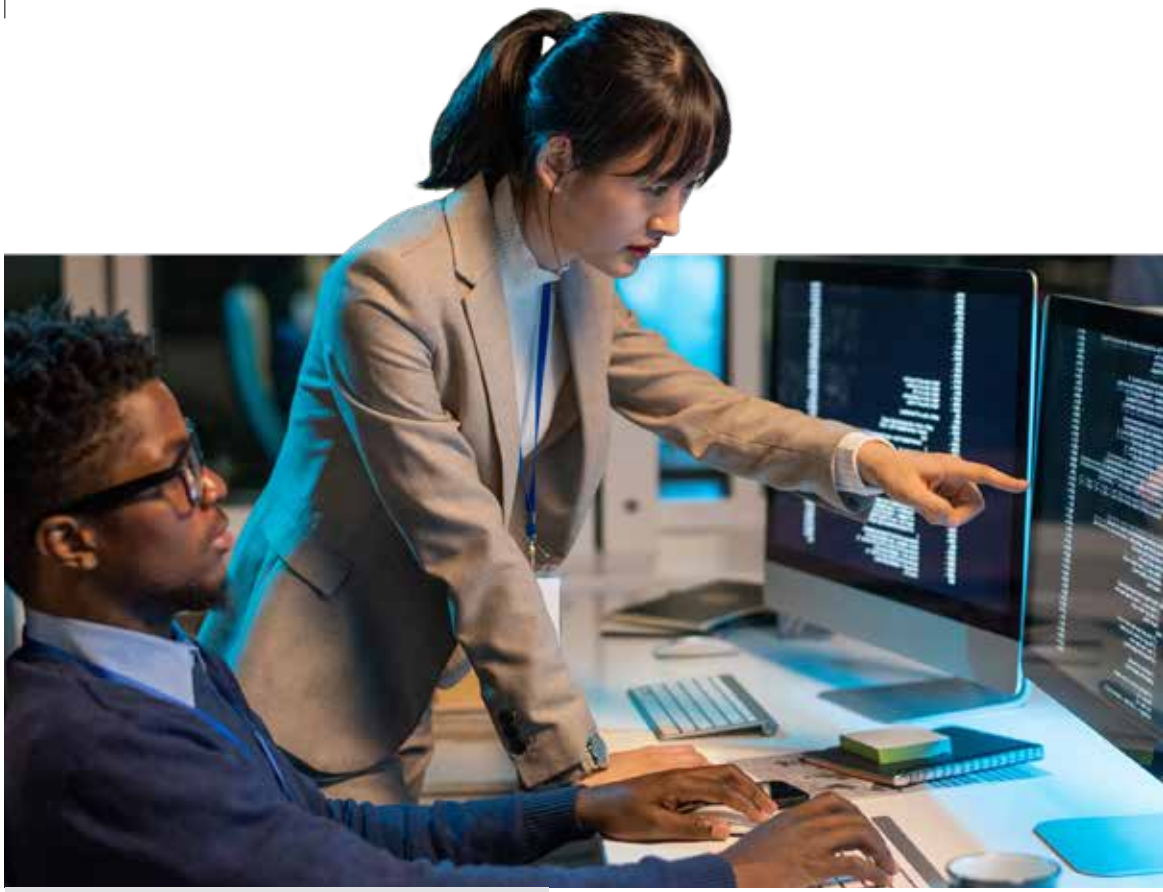
rene.flohil@capgemini.com

[1]https://www.narcis.nl/publication/RecordID/oai:scp.nl:79e0132b-ea63-4a41-8cc1-d8fa0e288bf7
[2]https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2144002
[3]https://www.payscale.com/research-and-insights/gender-pay-gap/
[4]https://www.theverge.com/2021/12/6/22814409/go-read-this-gizmodo-analysis-predpol-software-disproportionate-algorithm)
[5]http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

10

5 ORGANISATORISCHE VOORWAARDEN VAN EEN GOEDE SAMENWERKING

Wat is organisatorisch de basis voor een goede samenwerking binnen het veiligheidsdomein?



Samenwerken is een complexe opgave. Toch groeit de noodzaak om samen te werken, omdat de maatschappelijke uitdagingen niet door één overheid op te lossen zijn. Maar hoe organiseer je een samenwerking?

Highlights

- Werk vanuit een gemeenschappelijk overeengekomen strategie.
- Maak vertrouwen onderdeel van de strategie van de samenwerking.
- Formuleer een gezamenlijk governancemodel en monitoring van de samenwerking.
- Formuleer heldere procesrollen, taken en verantwoordelijkheden op verschillende niveaus.
- Zet technologie en data in om het gezamenlijk resultaat te ondersteunen.

Samenwerken als middel binnen het veiligheidsdomein

Als adviseurs in het veiligheidsdomein beleven wij veel plezier aan het helpen bij het oplossen van taaie vraagstukken. En het veiligheidsdomein kent vele uitdagende trends waarop het moet inspelen en kent ook vele patronen in de eigen organisaties die niet helpen om heel adaptief te zijn. Een gevleugelde uitspraak in deze context is ‘dat de cultuur niet helpt’ en dat ‘samenwerken een probleem is’. Over deze onderwerpen zijn boeken vol geschreven en in dit artikel brengen wij al die kennis terug tot vijf organisatorische voorwaarden die ingeregeld kunnen worden om samenwerking te verbeteren.

Het aanpakken van maatschappelijke problemen vraagt steeds vaker om een multidisciplinaire aanpak, zo ook binnen het veiligheidsdomein. Deze vraagstukken vragen om meerdere perspectieven en een bredere aanpak dan één organisatie kan bieden. Denk hierbij aan straf

Als adviseurs in het veiligheidsdomein beleven wij veel plezier aan het helpen bij het oplossen van taaie vraagstukken. En het veiligheidsdomein kent vele uitdagende trends waarop het moet inspelen en kent ook vele patronen in de eigen organisaties die niet helpen om heel adaptief te zijn.

met zorg, waarin de veiligheidshuizen zijn versterkt door met gemeenten, hulpverlening, justitie en politie o.a. de aanpak van personen met verward gedrag multidisciplinair te benaderen. Maar ook de aanpak van de ondermijnende criminaliteit vraagt een bredere aanpak en interventiepallet, van preventie waarin de nieuwe aanwas of zogenoemde doorgroei criminele wordt aangepakt tot de repressie van zwaar georganiseerde criminaliteit waarin ook op internationaal vlak wordt samengewerkt.

Het voordeel van samenwerken is evident. Door met meerdere en aanvullende organisaties samen te werken, wordt kennis samengebracht, kan een gecoördineerde aanpak worden afgestemd en het stimuleert bovenal innovaties buiten de bestaande structuren. "Alleen ga je sneller, samen kom je verder." Als gevolg van de noodzaak van samenwerken binnen het veiligheidsdomein schieten dergelijke verbanden als paddenstoelen uit de grond; op lokaal, landelijk en met private partners zoals de samenwerking tussen de publieke en de bancaire sector meldingen van eventueel witwassen aan de FIU te verbeteren of in de Haven Rotterdam werken publieke en private partijen samen om zogenoemde uithalers op het haventerrein nog effectiever tegen te gaan.

Samenwerken met diverse disciplines en verantwoordelijke organisaties is een complexe opgave. Het vraagt om een doorvertaling van de doelstelling van de samenwerking naar een gerichte samenwerkingsstrategie. In de praktijk besteden de samenwerkingspartners weinig tijd aan het ontwerpen van de samenwerking zelf. De inhoud van de samenwerking is wat hen samenbrengt en al snel worden visies en strategieën over de benodigde aanpak uitgewisseld. Gegeven dat veel organisaties in het domein actiegericht zijn, is de kortste route naar actie vaak het gevolg. Het bespreken van de randvoorwaarden voor succesvolle samenwerking wordt beperkt gedaan. Ook wordt onvoldoende stilgestaan bij wat de de samenwerking duurzaam maakt. Een gevolg hiervan kan zijn dat sommige samenwerkingsverbanden zich – op den duur – als een zelfstandige entiteit los van de deelnemende organisaties presenteren en botsende belangen ontstaan. Iedereen werkzaam in het veiligheidsdomein en met zicht op samenwerkingsverbanden kan hier voorbeelden van noemen.

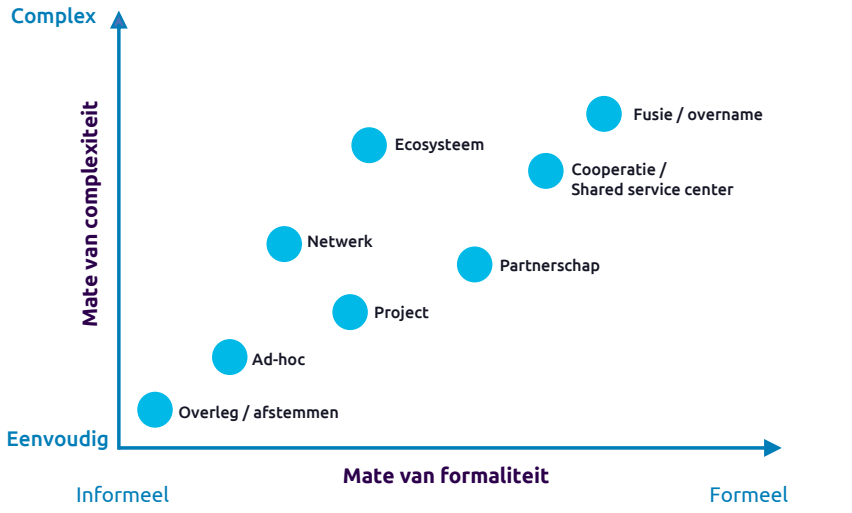
Welke onderdelen zijn essentieel als basis van de samenwerking en hoe pak je dat aan, zeker in een domein waarin duidelijke positionering en sterke hiërarchische verhoudingen niet ongebruikelijk zijn? Allereerst staan we nog kort stil bij wat een samenwerking is en welke samenwerkingsvormen er zoal bestaan. Vervolgens beschrijven we de 5 organisatorische randvoorwaarden van een goede samenwerking.

Wat is een samenwerking?

We hanteren voor dit artikel de volgende definitie:
Een samenwerking is de inbreng van expertise of middelen van 2 of meer mensen of organisaties die door een verbinding aan te gaan een gemeenschappelijke (maatschappelijke) toegevoegde waarde leveren.

Een samenwerking kan zich in de publieke sfeer in diverse vormen voordoen. De te kiezen samenwerkingsvorm is afhankelijk van (1) het aantal betrokken partijen, (2) de duur van de samenwerking en (3) de gemeenschappelijke toegevoegde waarde die de samenwerking moet gaan leveren. Willen partners bijvoorbeeld informatie of een aanpak afstemmen, dan is een overleg of afstemming veelal voldoende. Naarmate het aantal partijen toeneemt, de duur van de samenwerking langer wordt en de te leveren toegevoegde waarde complexer wordt, vraagt het een formelere samenwerkingsvorm. In onderstaande figuur zijn de meest voorkomende samenwerkingsvormen op twee assen geplot, mate van complexiteit van de samenwerking en de mate van formaliteit.

Figuur: De meest voorkomende samenwerkingsvormen



Wat is er nodig voor een samenwerking?

Hierbij wordt uitgegaan dat de doelstelling en noodzaak voor een samenwerking zijn afgewogen en concreet zijn geformuleerd, dit vormt immers de ultieme basis voor de samenwerking, de zogenoemde bedoeling (ofwel: Purpose of 'why')[1] van de samenwerking. Waartoe is de samenwerking op aard?

Werk vanuit een gemeenschappelijk overeengekomen strategie

Het lijkt een open deur maar een gemeenschappelijk overeengekomen strategie wordt soms met een visie verward. Een visie is namelijk een haalbaar lange termijn doel van de samenwerking met een externe blik. De visie kan je vaak starten met "wij willen...". Een strategie is vervolgens een concrete vertaling van deze visie naar een kortere termijn met een uiteenzetting van interne keuzes om deze visie te behalen ("wij kiezen en doen…"). Hierin staan (1) de scope van de samenwerking en de op te leveren resultaten, (2) de in te brengen middelen en expertise en (3) de werkwijze en bijpassende samenwerkingsvorm centraal.

Het ontwikkelen van deze strategie is aan de deelnemende partijen in deze samenwerking en niet een taak van de organisatie die wordt opgezet voor de samenwerking. Immers, de strategie is de opdrachtformulering aan de samenwerking en voorkomt het dat de samenwerking als zelfstandige entiteit los van de deelnemende partijen te werk gaat.

Een concreet voorbeeld is een zorg- en veiligheidshuis dat het als eigenstandige taak beschouwde om een strategie op te stellen met daaruit voorvloeiende prioriteiten. Nadat het veel energie had gestoken in opstellen en vormgeving van de strategie kwam het in conflict met de deelnemende organisaties die de eigen prioriteiten onvoldoende zagen terugkomen.

Een strategie is goed uiteengezet, wanneer deze voor iedereen in de samenwerking de duidelijkheid verschaft op welke wijze deze vertaald kan worden naar specifieke processen, taken en verantwoordelijkheden van professionals en benodigde techniek.

Een voorbeeld hiervan binnen het veiligheidsdomein is het zogenoemde ZSM[2] samenwerkingsverband waarin iedere deelnemende partij bijdraagt aan een snelle, simpele en slimme afdoening van eenvoudige criminaliteit. Door informatie en kennis uit te delen kunnen partijen beter en gecoördineerd interventies plegen op de casuïstiek met oog voor de bredere (maatschappelijke) problematiek.

Maak vertrouwen onderdeel van de strategie van de samenwerking

Het (voort)bouwen van een samenwerking kent in iedere weg diverse hobbels, maar in het geval van wantrouwen wordt de weg een reis zonder navigatie waarbij de ouders voorin met een kaart al rijdend aan het bakkeleien zijn waar en hoe we er moeten komen: "laat mij maar". Het resultaat is dat we te laat aankomen of gaan slingeren, omdat de bestuurder geen focus meer heeft op de weg. In iedere samenwerking is vertrouwen een essentiële basis voor het behalen van de resultaten. Zonder vertrouwen gaat men conflicten uit de weg, brokkelt de betrokkenheid af, wordt verantwoordelijkheid afgehouden en uiteindelijk vertraagt dit de op te leveren resultaten[3].

Voor een samenwerking is het des te belangrijker om vanaf de start vertrouwen in elkaar en de betrokken organisaties uit te laten maken van de algehele strategie en cultuur van de samenwerking. Naast het feit dat organisaties waar het vertrouwen groot is, prettig zijn om in te werken, zijn dergelijke 'high trust' organisatie veel succesvoller[4]. Vertrouwen bouw je echter niet in één middag. De basis ligt verscholen in een aantal duidelijke afspraken en waarden van de samenwerking waarbij specifiek gedrag beloond en bijgestuurd wordt door het leiderschap van iedereen. Naast deze basis vraagt vertrouwen in een samenwerking om:

- Inzicht in elkaars (organisatorische) belangen, de te leveren toegevoegde waarde op de bestaande structuren en de 'win-win' in het resultaat zelf.
- Een gemeenschappelijke en begrijpelijke taal[5]. Deze taal richt zich niet alleen op inhoudelijke terminologie, maar ook woordgebruik dat verbindend is en gelijkwaardigheid stimuleert, zogenaamde samenwerkingstaal, zoals "elkaar begrijpen" ipv "elkaar opvoeden".
- Stimuleer communicatie op diverse niveaus om transparantie te bevorderen, binnen bijvoorbeeld (partner) organisatie, leiderschap en uitvoering.

Een samenwerking met veel vertrouwen is gericht op resultaten, neemt verantwoordelijkheid, kent een sterke betrokkenheid van/bij partnerorganisaties, gaat conflicten niet uit de weg en communiceert transparant over bijvoorbeeld (eventueel niet) behaalde resultaten.

Formuleer een gezamenlijk governancemodel en monitoring van de samenwerking

In een samenwerking dragen de partnerorganisaties gezamenlijk en gelijkwaardig de verantwoordelijkheid voor de resultaten en aansturing. De hiërarchische verhoudingen of de omvang van de inbreng in de samenwerking kunnen daarom niet een reden zijn om als 'baas' over een samenwerking op te treden. Verwar daarom niet de rol en taakstelling vanuit de bestaande structuur met de gezamenlijke verantwoordelijkheid voor de doelstellingen van de samenwerking. De wettelijke gezagsrol kan bijvoorbeeld zeer dominant zijn in de uitvoering van de activiteiten binnen het samenwerkingsverband, maar heeft niet hetzelfde gewicht in de opbouw van een samenwerkingsverband.
Dit doet zich bijvoorbeeld voor rond samenwerkingsverbanden rond opsporingsonderzoeken of handhaving in de openbare ruimte. In het opbouwen en vaststellen van de doelstellingen van de samenwerking en aansturing daarop is het Openbaar Ministerie of een burgemeester een gelijkwaardige gesprekspartner.
Ook zien wij dat de omvang van een specifieke organisatie soms vertaald wordt naar de mate waarin er over het samenwerkingsverband besloten mag worden.

Een vertaling van de te verwachten resultaten en strategie in governance en een sturingsmodel voor de samenwerking is noodzakelijk om de prioriteiten en de verwachtingen scherp neer te zetten. Het sturingsmodel kent een concrete monitoring met KPI's[6] op zowel kwalitatieve als kwantitatieve meetinstrumenten. En er wordt gekeken naar indicatoren die wat zeggen over de aanpak én over de samenwerking werkt. Een dergelijk sturingsmodel en monitoring is geen doel op zich, maar ondersteunt het behalen van de gemeenschappelijke samenwerkingsdoelstellingen en geformuleerde (samenwerkings)strategie. Het biedt daarnaast de mogelijkheid om bij te sturen op alle niveaus en ondersteunt het inhoudelijke gesprek met de partnerorganisaties over de te behalen resultaten.

Een goed governancemodel stelt de partners in staat strategische beslissingen te nemen, zonder de samenwerking te verlammen. Een goede monitoring biedt de mogelijkheid om een gemeenschappelijk inhoudelijk gesprek te voeren over de te behalen resultaten en stelt de governance in staat te sturen op wat er (alsnog) nodig is om dat doel te behalen of bij te stellen.

Een voorbeeld hiervan is de aanpak van personen met verward gedrag door de zorg- en veiligheidshuizen, waar op 3 hoofdlijnen strategisch wordt gestuurd vanuit de samenwerkingspartners, namelijk: (1) risicotaxatie en toezicht, (2) kennisdeling tussen het zorg- en veiligheidsdomein en (3) passende zorg en ondersteuning. De Zorg- en veiligheidshuizen maken dit inzichtelijk door zowel kwantitatieve informatie (van bijvoorbeeld het RIVM), maar ook kwalitatieve gegevens van bijvoorbeeld de gemeente te combineren in een periodieke monitor. Ook betrekt de samenwerking de effectiviteit en het behalen van de minimumnormen van de samenwerking zelf in de monitor.

Formuleer heldere procesrollen, taken en verantwoordelijkheden op verschillende niveaus

Het samenspel van de doelstelling van de samenwerking, de strategie, governance en monitoring van hiervoor, stelt men in staat om heldere procesrollen, taken en verantwoordelijkheden te formuleren. Deze beschrijving dient op diverse niveaus plaats te vinden, namelijk op organisatie, proces en de professional zelf[7]. Een heldere beschrijving van de procesrollen, taken en verantwoordelijkheden ondersteunt de uitvoering in het behalen van de resultaten en zorgt voor een gestroomlijnd proces, waarbij voldoende ruimte bestaat voor de professional om waar nodig af te wijken van (standaard) processen van de samenwerking.

Zet technologie en data in om het gezamenlijk resultaat te ondersteunen
Technologie en data zijn net als de samenwerking zelf vormen waarop het resultaat en het primair proces kunnen ondersteunen, maar veelal noodzakelijk zijn om de samenwerking goed te laten functioneren. Denk bijvoorbeeld aan de toepassing van data science, sensing en vergaande automatiseringen met behulp van bijvoorbeeld artificiële intelligentie (AI). Het is dus geen doel op zich, maar het kan de te behalen werkwijze op een innovatieve wijze, versterken. Het gebruik van data van bijvoorbeeld de partners in een samenwerkingsverband, ligt vaak gevoelig en kennen diverse (juridische) beperkingen. Dit zien wij in bijvoorbeeld in de samenwerkingen van iCOV en de RIEC's. Dit heeft te maken met de verantwoordelijkheid die organisaties dragen in het kader van bijvoorbeeld de algemene verordening gegevensbescherming (AVG) en de wet op de politiegegevens (WPG). Het gebruik van technologie en data moet daarom niet alleen AVG-proof plaatsvinden, zoals privacy-by-design en bijpassende autorisatiestructuren, maar ook zoveel mogelijk in gesprek en transparant met voor de verantwoordelijke partners tot stand komen.

De inzet van technologie en data kan naast de juridische beperkingen juist een uitkomst bieden voor deze problematiek, door bijvoorbeeld het ethische gebruikmaken van deze middelen te versterken, aan privacyregels te voldoen of bedrijfsrisico's te verkleinen. Bijvoorbeeld door gegevens niet met elkaar te delen en centraal op te slaan, maar gebruik te maken van bijvoorbeeld een Zero-Knowledge Proof Protocol[8].

Een voorbeeld hiervan is de CT-infobox, een samenwerking op het gebied van contraterrorisme. Hierbij zijn diverse veiligheids-/inlichtings/- en opsporingsdiensten betrokken die met behulp van cryptografie zeer geheime informatie netcentrisch met elkaar te verbinden, zonder deze met elkaar te delen. Deze technologie en toepassing versterkt de diverse partners in de gebundelde aanpak van terrorisme en geeft het vertrouwen dat vertrouwelijke informatie niet 'zomaar' gedeeld hoeft te worden.

Op naar een duurzame en bewuste samenwerkingsstrategie

Het is een wonderlijke tegenstelling dat binnen het veiligheidsdomein zoveel moet worden samengewerkt en tegelijkertijd zo vaak gemopperd wordt over de mate van samenwerking. Een deel van deze complexiteit komt voort uit de hoeveelheid zelfstandige organisaties die actief zijn. Samenwerkingsverbanden oprichten die vervolgens als zelfstandige entiteiten gaan functioneren vergroot de complexiteit. Dat is het probleem oplossen met de oorzaak. In dit artikel hebben we enkele handvatten toegelicht die helpen om samenwerkingsverbanden effectief te maken. De essentie hiervan is dat een duurzame samenwerking ook een bewuste samenwerkingsstrategie en executie vraagt, bij de start of anders is dit een goed moment voor een tussentijdse toetsing.

Over de auteurs

Marcus Vander Velpen

Managing Consultant
Marcus is gespecialiseerd in sturings- en (complexe) samenwerkingsvraagstukken binnen het domein van justitie en veiligheid. Hierin richt hij zich op vraagstukken waarin het gebruik van data een belangrijke centrale rol vervult.

marcus.vander.velpen@capgemini.com

Erik Staffeleu

Senior Director
Drs. Erik Staffeleu is Senior Director in de publieke sector en onder andere verantwoordelijk voor de adviesgroep Veiligheid en Rechtsketens. Erik is veranderkundige en een ervaren adviseur binnen het veiligheidsdomein. Zijn opdrachten liggen veelal op het vlak van strategievorming en organisatieontwikkeling.

erik.staffeleu@capgemini.com

[1]Simon Sinek
[2]ZSM: zo spoedig, simpel, slim mogelijk
[3]Piramide van Lencioni
[4]Bart Stofberg, Vertrouwen - Waarom alles beter werkt als je mensen vertrouwt, 2020, Uitgever Haystack
[5]Dit betekent niet dat er een nieuwe taal moet ontstaan, maar wel dat begrippen of jargon hetzelfde worden uitgelegd.
[6]KPI's: Keten prestatie indicatoren
79 velden model van Rummler
[8]Ketensamenwerking zonder gegevens te hoeven delen, Daan Verwaaij, Joop Koster, Michael Kolenbrander, TiV 2021/2022

11

HET GEVAAR VAN ARTIFICIAL INTELLIGENCE VOOR DE WAARHEIDSVINDING

Waarom kan artificial intelligence niet zonder human intelligence?

Artificial intelligence is niet weg te denken uit de opsporing in het veiligheidsdomein maar human intelligence is noodzakelijk voor de waarheidsvinding.

Highlights

- Politiewerk kan niet (meer) zonder datavoorzieningen.
- Onjuiste analyse in artificial intelligence kan leiden tot tunnelvisie.
- Het is noodzakelijk om beschikbare data op waarde te schatten.
- De politie heeft in de toekomst meer behoefte aan goede analisten.
- Human intelligence is de randvoorwaarde voor data-gedreven opsporing.

Technische mogelijkheden en nieuwe datatechnologieën hebben een grote impact op de publieke sector en op het veiligheidsdomein. De groeiende populariteit en aandacht voor big data[1] in het politiewerk staan lijnrecht tegenover de wetenschappelijke literatuur die veelal gericht is op de mogelijk negatieve effecten van informatiegestuurd politiewerk (hierna: IGP). Dit is variërend tussen het probleem van function creep (hergebruik van oorspronkelijk met een ander doel vastgelegde data), fishing expeditions en het controleverlies door zogeheten black-box scenario's[2]. Opvallend is dat de meerwaarde van IGP nauwelijks naar voren komt in de literatuur, ondanks dat IGP niet meer weg te denken is uit onze samenleving. Een belangrijk onderdeel van IGP is artificial intelligence.

In deze bijdrage gaat de aandacht uit naar de vraag waarom artificial intelligence niet zonder human intelligence kan. Daarbij wordt gekeken hoe big data effectief kan worden ingezet door de politieorganisatie. De Wetenschappelijke Raad voor het Regeringsbeleid stelt dat data-analyses "vaak sneller en met minder menskracht zijn uit te voeren, waardoor overheidsorganisaties hun schaarse middelen veel efficiënter kunnen inzetten" staat hierbij centraal. Deze stelling staat in deze bijdrage centraal[3]. Wij betogen dat het effectief benutten van big data-toepassingen zonder meer mensenkracht behoeft.

Derde partijen leveren vaak een service waarbij zij ook (persoons)gegevens van de organisatie gebruiken. Organisaties hebben in sommige situaties een gebrek aan inzicht in de werkwijze van deze partijen, en missen procedures om hier wel inzicht in te krijgen.

IGP in de praktijk

Door de toenemende digitalisering van de samenleving is het politiewerk ingrijpend veranderd. Dat informatie daarmee ook in toenemende mate de basis van het politiewerk is, wordt onderschreven door onder meer Maurice den Hertog, Operationeel Specialist bij Politie Oost-Nederland. Er wordt steeds meer van de politie verwacht dat zij ingrijpt voordat een incident plaatsvindt. Hiertoe zijn verschillende strategieën in het leven geroepen en is informatiedeling en IGP centraal gesteld. De politieorganisatie maakt gebruik van informatie uit eigen bronnen, bronnen van andere overheden, bedrijven en brancheorganisaties en openbare bronnen – ofwel Open Source Intelligence (OSINT). De OSINT-specialisten van de politie zoeken gericht naar openbare informatie, waaronder tekst, foto-, video- en audiomateriaal, ten behoeve van het opsporingsonderzoek, risicotaxatie en waarheidsvinding. De politieorganisatie zet relatief eenvoudige big data-toepassingen breed in door grote databestanden aan elkaar te koppelen en informatie snel toegankelijk te maken. Het ligt in de lijn der verwachting dat er in de toekomst gebruik zal worden gemaakt van meer complexe big data-toepassingen, zoals (mogelijk zelflerende) algoritmes en risico-inschattende toepassingen.

De informatieoverdracht

De sterke ontwikkeling van artificial intelligence in de opsporing doet de vraag rijzen waarom er incidenten hebben kunnen plaatsvinden waarbij burgers mogelijk de dupe zijn geweest van fouten in de informatieoverdracht. Zo leidde de moord op Linda van der Giesen in 2015 tot ophef over de aanpak van de politie, omdat Linda herhaaldelijk contact zou hebben gehad met de politie over de dreigende situatie met haar ex-partner. De commissie Eenhoorn onderzocht het incident en bracht het onderzoeksrapport uit waaruit bleek dat de beschikbare gegevens niet optimaal werden ontsloten door ingewikkelde, bureaucratische en gefragmenteerde werkprocessen[4]. In de literatuur wordt in dezelfde lijn het volgende beargumenteerd: wanneer vooral wordt geïnvesteerd in hardware, business intelligence en procedures, maar er op analisten die met die informatie moeten werken wordt bezuinigd, kan dit risico's met zich meebrengen[5]. Denk aan het risico dat er alleen nog op complexe en gefragmenteerde 'systeemkennis' en formele communicatie wordt vertrouwd[6]. Het gebruik van meer complexe big data-toepassingen vereist nauwe samenwerking tussen informatiespecialisten en opsporingsdeskundigen. De informatiespecialisten duiden de beschikbare informatie en opsporingsdeskundigen maken een inschatting van mogelijke risico's en benodigde handelingen. De enorme hoeveelheid informatie die de politieorganisatie – al dan niet na een incident – ontvangt, dient nauwkeurig op waarde te worden beoordeeld door hiertoe specifiek opgeleide analisten.

Het risico van onbeheerde informatie

Ten aanzien van specifieke incidenten is de rol van de analist nog groter omdat er sturingsinformatie uit voort kan komen waar strafvorderlijke keuzes op worden gebaseerd. Dit is niet uitsluitend in het belang van de burger, maar ook voor het proportioneel gebruik van middelen en mensen van de politie. Het ontbreken

van human intelligence kan leiden tot disproportionele strafrechtelijke handelingen tegen onschuldige burgers. Hierdoor gaat niet alleen capaciteit verloren, maar dit kan er ook toe leiden dat politiemensen in onveilige situaties terecht komen doordat cruciale inlichtingen hen niet (tijdig) bereiken. Een voorbeeld van een dergelijke situatie is de onderstaande hypothetische situatie:

De alarmcentrale ontvangt melding van een gewonde vrouw en instrueert ambulance en politie naar de woning te gaan omdat de omstandigheden niet geheel duidelijk zijn. De politie ontvangt de informatie dat het de eengezinswoning van een gehuwd stel met drie kinderen betreft. Bij benadering van de politie komt er informatie van de Realtime Intelligence Center (RTIC) door: 'de man is eerder veroordeeld voor een gewapende overval'. De hulpdiensten moeten de komst van meer eenheden afwachten. Bij aankomst blijkt dat er een keuken-ongeval heeft plaatsgevonden en dat de man noch kinderen in het huis aanwezig waren. De eerder gegeven informatie is afkomstig uit de volgende situatie:

"Jan groeit op in een dorp waar hij op jonge leeftijd wordt verleid tot de verkoop van jointjes op het schoolplein. Hij wordt beroofd van de opbrengst en de opdrachtgever is zacht gezegd 'not amused'. Jan krijgt één week om de opbrengst te compenseren en besluit met een keukenmes op zak de buurtsupermarkt te beroven. Jan belandt voor de rechter en krijgt voor dit eerste vergrijp een taakstraf."

In het voorbeeld worden eenheden ten overvloede ingezet en aangestuurd op basis van verouderde informatie. Zo'n situatie kan zich mogelijk voordoen als er onvoldoende informatieanalisten beschikbaar zijn binnen de politieorganisatie. Hierdoor komt de veiligheid van burgers en van onze politiemensen mogelijk in het geding. Het waarborgen van de veiligheid is dan ook afhankelijk van het onderhoud aan beschikbare informatie. De menselijke waarneming is van grote meerwaarde in het onderhoud aan de informatievoorziening, maar zeker ook in de verbindende functie van de informatieorganisatie[7].

De tunnelvisie die de gegevensmarkt opwerpt

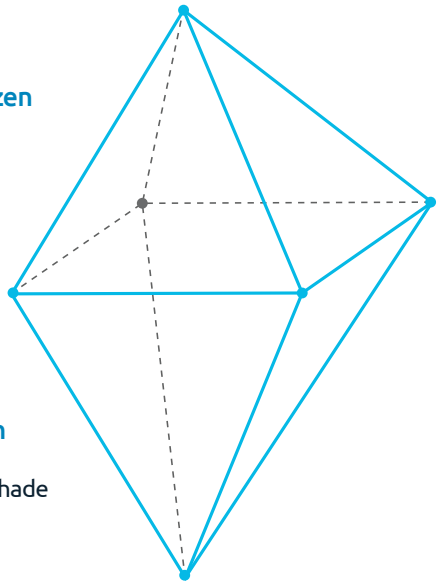
Goed opgeleide analisten zijn zoals gezegd onmisbaar bij het duiden van al verzamelde big data. Zij hebben daarnaast ook een prominente rol bij gegevensverzameling. Eén van de uitdagingen voor de informatievoorziening van de politie is 'de gegevensmarkt'. Het gaat hierbij om fenomenen als 'personal data economy', de verzameling, verwerking en verkoop van persoonsgegevens, en 'pay for privacy', het aanbieden van anonimiteit. De gemiddelde burger heeft onvoldoende financiële middelen voor de forse prijs van anonimiteit[8]. Daarentegen heeft de doorgewinterde crimineel in het hogere circuit – zoals binnen de georganiseerde misdaad – zowel het belang als de financiële middelen om zich buiten het bereik van datasets te plaatsen. Maurice den Hertog stelt dan ook dat het noodzakelijk is dat de data die beschikbaar wordt gesteld op waarde wordt geschat, geduid en van betekenis wordt voorzien. De bekwame analist is hierbij een onmisbare schakel. Het komt bijvoorbeeld voor dat er in een crimineel netwerk een laag is die zich makkelijk laat pakken; hierbij kan worden gedacht aan de katvanger en de jonge crimineel die 'net komt kijken' en makkelijk inwisselbaar is. Vervolgens is er een warrige laag waar het al moeilijk wordt om te duiden wie welke rol vervult in het criminele netwerk. Daarnaast heb je de toplaag met the "Godfather" die ongrijpbaar wordt zonder de juiste informatie.

Het is de human intelligence, de informatiespecialist, die informatie in perspectief kan plaatsen, waarbij aandacht wordt besteed aan de verschillende

---

Henry & Lanier's Crime Prism

Misdaden van de machtelozen
- Direct zeer schadelijk
- Individuele schade
- Maatschappelijke consensus
- Maatschappelijke afkeuring



Sociaal onwenselijk gedrag
- Relatief schadelijk
- Maatschappelijke schade
- Maatschappelijke verdeeldheid
- Maatschappelijke discussie

Misdaden van de machtigen
- Indirect zeer schadelijk
- Ernstige maatschappelijke schade
- Minimale maatschappelijke discussie

Zeer onwaarneembaar

dimensies van strafbare feiten. Het begrip van deze dimensies biedt grond voor een nauwkeurige tegemoetkoming aan de informatiebehoefte. Dit is met name door de wetenschap dat zogeheten 'misdaden van de machtigen' zich aan het zicht onttrekken. Met het oog op de causaliteitstheorieën in het materiële strafrecht wordt opgemerkt dat data-analyse verbanden en patronen weergeeft die lijken samen te hangen. Ter illustratie kan gedacht worden aan het fictieve verband tussen persoon A en persoon B, wie elkaar niet kennen maar slechts dezelfde horecagelegenheid als stamkroeg hanteren. Het vergt human intelligence om deze verbanden op gewogen waarde te schatten en de juiste conclusies aan de bevindingen te verbinden. Het is dan ook van cruciaal belang dat het grotere geheel in beeld wordt gebracht en dat men niet verstrikt raakt in de tunnelvisie die de gegevensmarkt opwerpt.

Tot slot

Uit ons betoog wordt duidelijk dat de informatiespecialist onmiskenbaar cruciaal is voor het effectief benutten van big data-toepassingen en IGP. De informatiespecialist is in staat de uit data-analyse afkomstige informatie te vertalen naar gewogen adviezen en relevante conclusies. Hierbij wordt samenhang van causaliteit onderscheiden, sturingsinformatie losgetrokken en worden cruciale inlichtingen tijdig onder de aandacht van de betrokken collega's gebracht. Het ontbreken van voldoende informatiespecialisten kan de voordelen van technologische ontwikkelingen tenietdoen.

Het advies dat uit ons betoog voortkomt is dan ook om te investeren in software- en hardware, maar het belang van de informatiespecialist voor het effectief benutten van de beschikbare informatie niet uit het oog te verliezen. De menselijke maat in het flexibel tegemoetkomen aan hulpvragen en informatiebehoeften is nu juist de kracht van intelligence binnen de politieorganisatie. Oftewel: human intelligence is de randvoorwaarde voor informatiegestuurd politiewerk.

Met speciale dank aan onze goede vriend en zeer gewaardeerde collega Zeger de Bruijne† voor zijn kritische blik en waardevolle advies aan deze bijdrage.

Over de auteurs

Anne-Sophie Fritschij

Senior Business Analist

Anne-Sophie Fritschij LL.M. is werkzaam bij Capgemini Business Technology Services in het domein Openbare Orde en Veiligheid. Zij is gespecialiseerd in het verbeteren van de informatievoorziening binnen de criminaliteitsbestrijding. Anne-Sophie is strafrechtjurist en senior business analist voor opdrachtgevers binnen het veiligheidsdomein.

anne.sophie.fritschij@capgemini.com

Vien Germawi

Business Analist

Vien Germawi LL.M. is werkzaam bij Capgemini Business Technology Services in het domein Openbare Orde en Veiligheid. Zij is gespecialiseerd in de bestrijding en preventie van fraude en economische delicten. Vien is strafrechtjurist en business analist voor opdrachtgevers binnen het veiligheidsdomein.

vien.germawi@capgemini.com

[1]De term 'big data' wordt geduid aan de hand van drie eigenschappen: volume, snelheid en variatie.
[2] R. Peeters & M. Schuilenburg, 'Machine justice: Governing security through the bureaucracy of algorithms', Information Polity 2018/23, afl. 3, p. 267-280.
[3]Wetenschappelijke Raad voor het Regeringsbeleid, WRR-rapport nr. 95: Big Data in een vrije en veilige samenleving, Amsterdam University Press, Amsterdam 2016.
[4]Kamerstukken II 2015/16, 29628, nr. 644, p. 2.
[5]P. Klerks & K. Vink-Teeven, 'De inzet van data-analysetechnologie ter bevordering van de informatiegestuurde opsporing: de zoektocht naar de optimale balans tussenmens en machine', Cahiers Politiestudies 2020/1, afl. 54, p. 163 – 176.
[6]P. Klerks & K. Vink-Teeven, 'De inzet van data-analysetechnologie ter bevordering van de informatiegestuurde opsporing: de zoektocht naar de optimale balans tussenmens en machine', Cahiers Politiestudies 2020/1, afl. 54, p. 163 – 176.
[7]Denk hierbij aan de wijkagent die Jan sinds jaar en dag kent en hem erop wijst dat hij een verzoek tot verwijdering van verouderde informatie uit 1995 kan indienen.
[8]S. Elvy, 'Paying for Privacy and the Personal Data Economy', Columbia Law Review, 2017/117, no. 6, p. 1369 – 1459.

12

VECHTEN VOOR EEN VEILIGE TOEKOMST, VECHTEN UW LEVERANCIERS MET U MEE?

Hoe mitigeer je het risico dat data in de verkeerde handen valt via de leveranciers waar jij op moet kunnen vertrouwen?

Onze nationale veiligheid speelt zich in toenemende mate af in het digitale domein. Dit brengt voordelen met zich mee, maar ook het risico dat data in verkeerde handen kan belanden. Het lekken, verliezen of misbruik van deze data kan de veiligheid van burgers en de Staat in gevaar brengen. Om deze risico's te beperken nemen organisaties maatregelen. Echter, soms vergeten organisaties dat data zich in toenemende mate kan bevinden bij leveranciers (of derde partijen).

Highlights

- Uw leveranciers kunnen een wezenlijke dreiging vormen.
- Neem controle door het implementeren van een strategie om deze risico's te managen.
- Een open en ondersteunende houding van uw leveranciers is cruciaal.
- Leid uw medewerkers op in het herkennen van risico.

Organisaties zijn afhankelijk van de diensten die deze leveranciers leveren, waarbij ze ook mogelijke (persoons) gegevens van de organisatie delen. Met name voor het veiligheidsdomein, is de kans dat het om gevoelige data gaat vele malen hoger. Afhankelijkheid staat gelijk aan risico, en het is daarom van belang dat u als organisatie niet alleen de data in eigen huis adequaat weet te beschermen, maar dat de leveranciers met u meevechten om uw data te beschermen.

Recente ontwikkelingen zetten leveranciersmanagement op scherp

Sinds de Schrems II uitspraak van het Europese Gerechtshof in 2020 is de uitwisseling van data tussen de Europese Unie en de Verenigde Staten beperkt, waardoor het belangrijker dan ooit is geworden om te weten waar en bij welke leveranciers jouw data zich bevindt[1]. Het Hof kwam tot deze uitspraak doordat het rechtssysteem van de Verenigde Staten toestaat dat inlichtingendiensten de data van bedrijven binnen hun jurisdictie mogen opvragen en gebruiken op een manier die niet in lijn is met de Algemene Verordening Gegevensbescherming. (AVG). Dit geldt niet alleen voor data die leveranciers die zich in de V.S. bevinden, ook andere landen kunnen te risicovol zijn. Sinds deze uitspraak is het meer dan ooit van belang om te weten a) welke externe partijen/leveranciers jouw data

verwerken, b) met wie zij deze data op hun beurt weer delen om de service te kunnen leveren, en c) wat de locatie is waar de data verwerkt wordt.

De rol van leveranciers in een data-gedreven wereld

Derde partijen leveren vaak een service waarbij zij ook (persoons)gegevens van de organisatie gebruiken. Organisaties hebben in sommige situaties een gebrek aan inzicht in de werkwijze van deze partijen, en missen procedures om hier wel inzicht in te krijgen. Met name de overheid, en specifiek het veiligheidsdomein, beschikt veelvuldig over gevoelige data van burgers (denk aan Defensie, de Politie maar ook het RIVM). Het risico voor deze sector kan gemitigeerd worden door middel van een duidelijke risicomanagementstrategie, waarbij een goede samenwerking met leveranciers essentieel is. Het veiligheidsdomein heeft, net zoals andere organisaties, een groeiend aantal leveranciers waar het op steunt. Dit is niet vreemd als je kijkt naar de algemene ontwikkelingen in de (technologische) wereld. Door vooraanstaande onderzoeksbureaus wordt dit geïdentificeerd als “de nieuwe manier waarop organisaties derde partijen gebruiken”[2]. Een vooraanstaand onderzoeksbureau, Gartner, geeft aan steeds vaker organisaties te identificeren die kansen in het gebruik van nieuwe technologieën zien. Deze trend leidt soms tot het verlenen van diensten buiten het core-businessmodel van de organisatie. Zij zijn daardoor in toenemende mate afhankelijk van leveranciers die vernieuwende diensten leveren. Deze veranderingen vragen om een fundamenteel andere benadering van risico-identificatie en controle. Aldus Chris Audet, directeur, Gartner Research & Advisory[3].

Derde partijen leveren vaak een service waarbij zij ook (persoons)gegevens van de organisatie gebruiken. Organisaties hebben in sommige situaties een gebrek aan inzicht in de werkwijze van deze partijen, en missen procedures om hier wel inzicht in te krijgen.

Digitale innovatie in het veiligheidsdomein: Een wereld aan leveranciers

Het is een race tegen de klok: enerzijds willen (veiligheids-)organisaties snelheid houden in de ontwikkelingen en meegaan in de vooruitgang van de technologie. Jaarlijks worden er miljoenen geïnvesteerd door organisaties en overheden om mee te gaan in innovatieve trends en om te voldoen aan de toenemende digitale behoeften van het veiligheidsdomein. Om doorlopend de veiligheid te borgen is het nodig dat het veiligheidsdomein investeert in nieuwe technologieën. Anderzijds brengen deze ontwikkelingen ook risico’s met zich mee.

Het staat buiten kijf dat er energie moet worden gestoken in het onderzoeken welke data uw leveranciers daadwerkelijk verwerken, en welke derden vanuit die leveranciers op hun beurt weer uw data verwerken. Alleen op die manier kan men de risico's collectief in kaart brengen.

Wanneer we denken aan leveranciers (derde partijen), dan wordt dit het best zo breed mogelijk geïnterpreteerd. Derde partijen kunnen leveranciers zijn die digitale diensten verlenen waarbij zij persoonlijke data van werknemers verwerken zoals in HR-systemen of tools. Ook zijn er leveranciers die weliswaar geen persoonlijke data, maar wel metadata of telemetrische data van werknemers verzamelen, bijvoorbeeld bij het gebruik van (communicatie) diensten. In het veiligheidsdomein zijn deze data al snel cruciaal in het beschermen van de activiteiten en/of operaties van de organisatie in kwestie.

Enkel de huidige leveranciers en hun datagebruik in kaart brengen, is niet voldoende. Het vermijden van risico's die leveranciers en derden met zich meebrengen, begint vaak bij de keuze voor bepaalde leveranciers. Het meenemen van het juiste afwegingskader in het aanbestedingsproces zou daarbij een preventieve maatregel zijn waarbij onnodige risico's aan de voorkant al worden geadresseerd. De veiligheidssector loopt gevaar op het oneigenlijk gebruik (misbruik) van haar data waarbij deze gebruikt worden voor cyberintelligence, spionage, of het de mogelijkheid op spionage vergemakkelijkt. Dit vormt uiteindelijk een risico voor de staatsveiligheid. Een afwegingskader is een goede preventieve maatregel, maar de keuze van leveranciers heeft ook te maken met het niveau van bewustzijn/awareness van medewerkers binnen de eigen organisatie.

Awareness is onder andere belangrijk als we denken aan het gebruik van privé-apps door medewerkers, waarbij zij, onbedoeld, gevoelige of organisatie-kritieke data (zoals locatiedata) kunnen delen. Een goed voorbeeld hiervan is het gebruik van Strava door militairen[4]. Ook zijn organisaties steeds vaker bezig met het in gebruik nemen van handige tools die hun in staat stelt om data op een makkelijke manier te analyseren, en eventueel te delen. Hiervoor wordt data geüpload in tools zoals 'Tableau'. Waar de medewerkers ook over na moeten denken is: waar komt de data terecht die ik in deze handige tool stop? Oftewel het menselijke gedrag kan nog steeds bepalend zijn in het beveiligen van data. Medewerkers kunnen onbewust door het gebruik van 'gratis' apps cruciale data verstrekken die impact heeft op de beveiliging in het veiligheidsdomein.

Denk bij het in kaart brengen van leveranciers ook aan missies van Defensie over landsgrenzen waarbij een afhankelijkheid van derde partijen (in dat land) vaak onvermijdelijk is. Een goed voorbeeld hiervan is het gebruik van vehicle tracking. Humanitaire organisaties en NGOs, maar ook organisaties binnen het veiligheidsdomein kunnen hier gebruik van maken. Vaak maakt dit deel uit van een service die geleverd wordt door een leverancier. Deze voorbeelden laten goed zien hoe data bij derden terecht kan komen. Metadata kan echter ook op indirecte manieren bij derden terechtkomen. Denk hierbij aan mobiele telefonie/netwerkproviders die, hoewel zij geen direct identificerende persoonlijke data bijhouden van cliënten/werknemers, wel metadata van deze werknemers verwerken.

Een doeltreffende strategie

Het staat buiten kijf dat er energie moet worden gestoken in het onderzoeken welke data uw leveranciers daadwerkelijk verwerken, en welke derden vanuit die leveranciers op hun beurt weer uw data verwerken. Alleen op die manier kan men de risico's collectief in kaart brengen. Echter, om dit te realiseren, is het zaak dat dat leveranciers niet enkel gecontroleerd en gemanaged worden maar dat zij actief meedenken/meevechten in uw taak om data te beschermen. Samen optrekken maakt immers sterker in de strijd tegen indringers.

De strategie om het risico te managen, is een duidelijk voorbeeld van een goed werkende formule die, met de juiste gealloceerde resources en capaciteit, snel en efficiënt in gebruik genomen kan worden. Het is belangrijk om te melden dat dit geen eenmalige exercitie is. Het gebruik van derde partijen zal blijven groeien en verandert constant. De aangewezen business zal hierin mee moeten blijven bewegen. De strategie ziet er als volgt uit:

01
Inventarisatie
Allereerst dient er in kaart te worden gebracht met welke leveranciers en derden de organisatie samenwerkt. Het is van belang dat er in kaart wordt gebracht van welke aard deze derden zijn (wat voor service leveren zij?). Het is niet altijd duidelijk omschreven maar veel leveranciers gebruiken ook zelf derde partijen wanneer zij een service aanbieden. Zo kan er een specifieke dienst afgenomen worden van een leverancier maar om die dienst te kunnen leveren, schakelen zij op hun beurt weer derden in om een deel van deze service te kunnen leveren. Denk hierbij aan technische middelen om in te loggen zoals e-Herkenning of multi-factor authenticatie mogelijkheden waarbij een derde partij wordt ingeschakeld om een deel van het proces uit te voeren, zoals een SMS-controle of een ander identificatiemiddel of uniek gegeven.

02
Data-mapping
Bij het in kaart brengen van deze leveranciers en derde partijen, dient te worden nagegaan tot welke data deze partijen precies toegang hebben en welke zij daadwerkelijk nodig hebben voor het uitvoeren van de afspraken die in het contract zijn vastgelegd. Er kan dan een mapping-exercise uitgevoerd worden, waarbij naast de verschillende leveranciers ook het type data inzichtelijk wordt gemaakt.

03
Risico-inschatting
Wanneer deze leveranciers en derde partijen in kaart zijn gebracht, dient men een risico-inschatting te maken. Dit kan op verschillende manieren, afhankelijk van de grootte en het karakter van de organisatie. Zo kan het ontzettend verschillen hoeveel risico een organisatie realistisch gezien kan dragen of hoeveel risico de organisatie loopt op het gebied van reputatieschade of financiën. Er bestaan tools waarmee deze risico assessments geautomatiseerd uitgevoerd kunnen worden. Als alternatief kan er ook een gepersonaliseerd risico-raamwerk gecreëerd worden. Het creëren van een gepersonaliseerd raamwerk voor de risico-assessment stap in de strategie is iets eenmaligs waarmee je een base-level creëert op basis van uw inschatting van het risico. Essentieel in deze stap is de medewerking van uw leveranciers. Zij dienen u transparantie te geven in de derden die zij gebruiken om hun service te kunnen leveren, en inzicht geven in wat de risico's zijn aan hun kant.

04
Mitigatie
De voorlaatste stap is om de risico's, die nu inzichtelijk en meetbaar gemaakt zijn =, te mitigeren op een manier waarop het zo min mogelijk negatieve effecten heeft op de operationele werkelijkheid. Dit is uiteraard onderhevig aan de aard van de organisatie, de geïdentificeerde risico's en het daarbij passend gemaakte risicoprofiel in de vorige stap. Behalve transparantie te geven in de derden die zij gebruiken om hun service te kunnen leveren, wat de risico's zijn aan hun kant, dienen leveranciers daarnaast mee te werken aan een oplossing om de (onnodige) risico's te verkleinen.

05
Langetermijndenken
Om te zorgen dat er een continuïteit wordt gecreëerd in het managen van de risico's dienen de voorgaande stappen geworteld te zitten in de cultuur van de medewerkers. Dit begint allereerst bij het creëren van awareness bij de werknemers, daarom staat in deze stap het trainen van de werknemers die verantwoordelijkheden hebben in het proces, centraal. Integratie van de verantwoordelijkheden in het takenpakket en in de langetermijnstrategie en governance van de organisatie zijn essentieel voor de continuïteit van risicomanagement van derde partijen. Deze laatste stap is dan ook onmisbaar in een correcte ingebruikname van deze strategie.

Bereid u voor op de toekomst

In het verleden waren organisaties afhankelijk van een beperkt aantal contractanten en leveranciers waarmee een organisatie verbonden was. Nu zijn er grote én kleine organisaties die zelf ook weer meerdere derde partijen kunnen hanteren. Het is onmogelijk om een goed idee te krijgen van het risico wat een organisatie op dit moment loopt via haar leveranciers, op de wijze waarop risicomanagement in het verleden uitgevoerd werd.

Conclusie

Uiteindelijk is het doel een blijvende cultuurverandering teweeg te brengen. Niet enkel binnen de eigen organisatie, maar ook bij derde partijen en gebruikers. Hierbij is het van belang dat de voorgaande stappen volledig opgenomen zijn in de operationele werkelijkheid van de organisatie. Meer in het algemeen betekent dit dat er een baseline van bewustzijn is binnen de organisatie voor de risico's die leveranciers met zich meebrengen voor de organisatie, haar werknemers en uiteindelijk in veel gevallen ook voor de burger. Het betekent ook dat leveranciers betrokken worden in het nadenken over hoe de risico gemitigeerd kunnen worden, en hoe zij meer bewust kunnen worden over hoe hun werkwijze onbewust een averechts effect kan hebben op een organisatie. Op deze wijze worden zij niet enkel alert, maar kunnen zij ook actief bijdragen aan het veilig houden van Nederland en haar burgers.

Ten slotte is het risicomanagement van derde partijen niet alleen gelimiteerd tot zakelijke leveranciers en (hun) derden. Werknemers moeten zich ervan bewust zijn dat privé-gebruik van services invloed kan hebben op het risicoprofiel van de organisatie. Het hebben van een duidelijke strategie en awareness, waarbij er binnen de organisatie ook openheid is tegenover haar werknemers over de risico's die zich kunnen manifesteren, speelt hier een grote rol.

Over de auteurs

Britt Huveneers

Privacy Consultant

Britt is privacy consultant en heeft ervaring binnen internationale organisaties en de humanitaire sector. Haar expertise ligt bij het legitiem gebruik van data en van nieuwe technologieën, en digital ethics.

britt.huveneers@capgemini.com

Natasja Pieterman

Managing Consultant

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

natasja.pieterman@capgemini.com

Jule Hintzbergen

Principal Cybersecurity Consultant

Jule is 23 jaar werkzaam voor Capgemini op het grensvlak van cybersecurity strategie, fysieke veiligheid, OT en privacy binnen de overheid en het bedrijfsleven.

jule.hintzbergen@capgemini.com

[1]Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020)
[2]Stay Ahead of Growing Third- Party Risk, 20219, Edited by Chris Audet, Director, Gartnerr
[3]Stay Ahead of Growing Third- Party Risk, 20219, Edited by Chris Audet, Director, Gartner
[4]https://www.security.nl/posting/548280/Defensie+wijst+militairen+op+gevaar+van+Strava+en+social+media

13

DE SLIMME DEURBEL : EFFECTIEF TEGEN MISDAAD OF INBREUK OP PRIVACY?

Is het gebruik van beeldmateriaal verkregen door een slimme deurbel effectief in de opsporingsfase en weegt het op tegen de mogelijke inbreuk op privacy?

Highlights

- De slimme deurbel draagt bij aan de trend van dataverzameling.
- Leidt tot inbreuk op privacy van burgers.
- Helpt bij het bestrijden van misdaad.
- Leidt tot een groter veiligheidsgevoel in de wijk.
- De beelden van de slimme deurbel moeten opgeslagen worden in lijn met de AVG.

Toename van de slimme deurbel

In september 2020 was 18% van de Nederlandse huishoudens in het bezit van slimme beveiligingsapparatuur[1]. In 2020 hadden 500.000 huishoudens een slimme deurbel als beveiliging en in oktober 2021 is dit gegroeid naar 640.000[2]. Maar wat is een slimme deurbel precies? Hoewel een slimme deurbel ongeveer hetzelfde werkt als een 'gewone' deurbel, stuurt deze meldingen naar je telefoon, tablet of computer wanneer er iemand voor de deur staat. Op dit moment kun je dan communiceren met de persoon die heeft aangebeld. Daarnaast hebben de meeste slimme deurbellen een ingebouwde camera. Met deze camera kan de omgeving in de gaten worden gehouden en kunnen beelden worden opgeslagen[3].

De toename in de aanschaf van de slimme deurbel heeft, in de meeste gevallen, een simpele verklaring: het voegt een extra laag beveiliging toe voor de bewoner. Sterker nog, deze slimme deurbellen

kunnen bijdragen aan het verminderen van criminaliteit in een woonwijk en het vergroten van het veiligheidsgevoel onder de burgers[4]. In 2018 is er een pilot uitgevoerd waaruit gebleken is dat het plaatsen van een slimme deurbel heeft geleid tot een toename van het veiligheidsgevoel voor de burger: van 5,9% naar 6,5% in verschillende wijken van Almere[5] Volgens de politie helpt het ophangen van een slimme deurbel zowel bij het afschrikken als bij het opsporen van criminelen[6, 7].

'Camera in Beeld'

Sinds 2018 werkt de politie met het initiatief 'Camera in Beeld'. Dit is een politiesysteem dat buitencamera's op een kaart weergeeft. In 2021 heeft de politie een campagne gevoerd om slimme deurbellen aan te melden bij dit initiatief[8]. Op het moment dat er een incident plaatsvindt, kan de politie makkelijk zien wie een slimme deurbel heeft en mogelijk beelden heeft gemaakt van het plaats delict.

Sinds 2018 werkt de politie met het initiatief 'Camera in Beeld'. Dit is een politiesysteem dat buitencamera's op een kaart weergeeft. In 2021 heeft de politie een campagne gevoerd om slimme deurbellen aan te melden bij dit initiatief.

Dilemma:

Dit initiatief brengt een dilemma met zich mee. Hoewel de dataverzameling door de slimme deurbel een belangrijk hulpmiddel geworden is voor de politie in het oplossen van zaken, gaat de dataverzameling door de slimme deurbel gepaard met verscheidene privacyvraagstukken. Hierbij ontstaat er een spanningsveld tussen enerzijds de privacy van burgers en anderzijds het bestrijden van misdaad. De vraag hierbij is: welk belang weegt zwaarder?

Dataverzameling

Zoals benoemd, worden er steeds meer slimme deurbellen aangeschaft. Deze stijging volgt de trend in dataverzameling die we de afgelopen jaren hebben waargenomen: hoe meer data er verzameld kan worden, hoe beter. Dit is echter in strijd met het principe minimale gegevensverwerking[9]. Minimale gegevensverwerking, ook wel dataminimalisatie genoemd, houdt in dat er niet meer gegevens mogen worden verzameld dan strikt nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken.

Hetzelfde geldt voor de beelden die worden verzameld door de slimme deurbel. De toename in het gebruik van een slimme deurbel heeft hierdoor ook een keerzijde, zo meent de Autoriteit Persoonsgegevens (AP). De slimme deurbel beschikt ook over de mogelijkheid om beelden vast te leggen en dus data te verzamelen. De Nederlandse toezichthouder ziet dan ook een toename in het aantal privacyklachten en waarschuwt dat de slimme deurbel niet zomaar opgehangen mag worden. De Belgische toezichthouder heeft in november 2020 de eerste boete uitgedeeld voor het onterecht filmen van de openbare weg en privé-eigendommen door bewakingscamera's van een burger[10].

De toezichthoudende autoriteit stelt dat een bewoner een slimme deurbel mag ophangen zolang deze alleen de eigen bezittingen filmt[11]. Daarnaast stelt zij ook dat ervoor gewaakt moet worden dat de deurbel de openbare weg niet of zo min mogelijk filmt. Het filmen hiervan vergroot de kans dat je ook andere personen of bezittingen filmt, wat leidt tot inbreuk op hun privacy. In de praktijk is het echter zo dat de openbare weg vaker gefilmd wordt door een slimme deurbel dan strikt noodzakelijk is. De AP raadt daarnaast ook ten zeerste aan om duidelijk aan te geven dat er een camera hangt om omwonenden hiervan op de hoogte te stellen.

Opslag van data

Het verzamelen van data gaat gepaard met het goed op moeten slaan van deze data, iets dat de afgelopen jaren al steeds meer centraal stond. Hierdoor ontstaan er privacyvraagstukken, bijvoorbeeld over de opslaglocatie. Een van de meest aangeschafte merken van slimme deurbellen komt van Ring, onderdeel van het Amerikaanse Amazon. Dit betekent dat de beelden worden opgeslagen op servers in de Verenigde Staten[12]. Na de Schrems II-uitspraak[13], waaruit is gebleken dat de VS niet langer voldoet aan het gewenste Europese beveiligingsniveau voor persoonsgegevens, is dit geen gewenste situatie. Zeker gezien het onderzoek dat is uitgevoerd door Electronic Frontier Foundation[14]. Uit dit onderzoek bleek dat de persoonlijke gegevens van consumenten ook werden gedeeld met derde partijen.

Spanningsveld

De politie heeft veel baat bij beelden die onder andere de openbare weg filmen. Zoals eerder benoemd, kunnen deze beelden nuttig zijn voor het opsporen van daders. Particuliere camera's mogen echter alleen opgehangen worden met een specifiek doel. Dit doel zal niet overeenkomen met het doel van de politie. Uitzonderingen zijn hier uiteraard delicten die worden gepleegd bij het desbetreffende huis. Als een burger de slimme deurbel 'zomaar' ophangt en de openbare weg filmt, is de kans dat er een overtreding wordt begaan groter.
Maar hoe denken de AP, de politie en de burger specifiek over het gebruik van de slimme deurbel?

Perspectief AP

De toezichthoudende autoriteit waarschuwt om de camera van de slimme deurbel niet zomaar aan te zetten. Het aanmoedigen vanuit de gemeenten tot continu filmen, zet aan tot onrechtmatig gedrag en een inbreuk op privacy[15]. Daarnaast moet de slimme deurbel zo geplaatst worden dat zo min mogelijk de openbare weg of de bezitting van omwonenden worden gefilmd. Het verkeerd ophangen kan leiden tot een inbreuk op privacy. Uit onderzoek is gebleken dat 87,6 procent van de camera's die geregistreerd staan in de politie-databank 'Camera in Beeld' de openbare weg filmt[16]. De belangrijkste regel volgens de AP is dat de camera alleen de eigen bezittingen mag filmen en dat de privacy van omwonenden gewaarborgd moet worden. Privacy is immers een grondrecht.

Perspectief politie

Hoewel de AP waarschuwt voor mogelijke privacy schendingen door het ophangen van een slimme deurbel, is een woninginbraak daarentegen ook een ernstige privacyschending voor de burger. In dit soort situaties kan de slimme deurbel juist de doorslag geven in een politieonderzoek. Hierdoor kan de vraag ontstaan welke inbreuk op privacy zwaarder weegt.

Natuurlijk moet de politie zich houden aan de Wet Politiegegevens (WPG), welke gaat over het beschermen van persoonsgegevens, en zijn er ook regels en uitzonderingen opgenomen met betrekking tot het gebruik en opslag van deze beelden voor het afhandelen van strafzaken. Echter blijkt in de praktijk dat de politie ook gebruik maakt van beelden die op onrechtmatige wijze gefilmd zijn door de burger[17].

Perspectief burger

Het perspectief van de burger laat een duidelijke tweestrijd zien. Aan de ene kant geeft de slimme deurbel meer mogelijkheden tot beveiliging van de eigen bezittingen, dit verklaart onder andere de toename van het veiligheidsgevoel. Burgers kunnen bijvoorbeeld ten alle tijden zien wie er aanbelt en rechtstreeks met diegene communiceren. Daarnaast kunnen ze met de slimme deurbel de eigen bezittingen blijven monitoren. Bovendien, helpt de slimme deurbel bij het verminderen van criminaliteit in de wijk.

Aan de andere kant kan de slimme deurbel een ernstige inbreuk op privacy leveren, wanneer deze slimme deurbel niet goed is opgehangen (i.e. gericht op de openbare weg of andermans bezittingen). De burgers voelen zich onvrij in hun eigen buurt, omdat ze niet weten wat er gefilmd wordt, wat het doel is van het filmen en waar de beelden worden opgeslagen[18].

Tegenpolen

Met de politie op de linkeras (criminaliteitsbestrijding) en de AP op de rechteras (beschermen van privacy) valt het perspectief van de burger ergens in het midden. Een deel van de burgers vindt hun eigen privacy belangrijker, terwijl een ander deel kiest voor het veiligheidsgevoel en criminaliteitsbestrijding boven privacy.

---

[1]https://fwd.nl/smarthome/smarthome-terugblik-op-2021-en-vooruitblik-op-2022/
[2]Idem.
[3]https://www.gamma.nl/klusadvies/a/wat-is-een-slimme-deurbel
[4]https://www.ad.nl/rotterdam/slimme-deurbellen-moeten-de-stad-veiliger-maken-straat-vol-cameras-kan-criminelen-afschrikken~a^{635355}a/
[5]https://www.thuiscomfort.nl/nieuws/onderzoek-video-deurbel-jaagt-inbrekers-weg-bij-de-buren.html
[6]https://www.pzc.nl/rotterdam/deurbel-met-camera-filmt-iphone-rover-zelfs-ik-herken-hem-op-de-beelden~a8118d7c/?referrer=https%3A%2F%2Fwww.google.com%2F
[7]https://tweakers.net/nieuws/160418/politie-pakt-jongens-op-dankzij-beelden-slimme-deurbel.html
[8]https://www.politie.nl/nieuws/2021/juli/9/04-deurbel-met-camera.html
[9]AVG: Artikel 5 eerste lid sub c
[10]https://www.gegevensbeschermingsautoriteit.be/burger/de-gba-legt-een-boete-op-voor-de-onrechtmatige-verwerking-bewakingscamerabeelden
[11]https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stappenplan_camera_bij_huis.pdf

Conclusie

De slimme deurbel: effectief tegen misdaad of inbreuk op privacy?

Het ophangen van een slimme deurbel blijkt spanningen op te roepen tussen het recht op privacy en het bestrijden van criminaliteit. Uit uitgevoerde pilots is gebleken dat omwonenden slechts een zeer lichte daling van criminaliteit in hun wijk ervaren[19]. Echter, de meerderheid van de deurbellen filmt wel de openbare weg[20]. Deze inbreuk op privacy zien wij als toenemend risico gezien de trend in dataverzameling.

De reeds opgezette publiek-private samenwerking, 'Camera in Beeld', brengt hierdoor mogelijkheden met zich mee om deze inbreuk op privacy te minimaliseren. De politie kan dit initiatief uitbreiden door het stappenplan van de AP toe te voegen aan het aanmeldingsformulier voor 'Camera in Beeld'. Daarnaast dient de politie de burger op de richtlijnen van de AP[21] te wijzen op het moment dat de politie beelden ontvangt die niet in lijn zijn met deze richtlijnen. Op deze manier kan de slimme deurbel gebruikt blijven worden door de politie, terwijl alle mogelijke stappen worden ondernomen om de privacy van omwonenden te beschermen.

Over de auteurs

Samantha Anroedh

Senior Privacy Consultant

Samantha is werkzaam als senior privacy consultant bij Capgemini Nederland, binnen de Cybersecurity Unit. Zij adviseert organisaties om hun weerbaarheid te vergroten op het gebied van cybersecurity en privacy.

Charissa Pinas

Privacy Consultant

Charissa is een expert in privacy. Zij helpt organisaties met strategische of organisatorische vraagstukken op het gebied van privacywetgeving.

Rachelle Miltenburg

Privacy Consultant

Rachelle is een Privacy en Cybersecurity Consultant gespecialiseerd in de AVG en het opstellen van privacy en Cybersecurity beleid.

[12]https://eu.ring.com/pages/privacy-notice
[13]https://autoriteitpersoonsgegevens.nl/nl/nieuws/aanbevelingen-edpb-voor-doorgifte-persoonsgegevens-na-schrems-ii-uitspraak#:~:text=In%20juli%20concludeerde%20de%20hoogste,tekortschiet%2C%20ondanks%20het%20Privacy%20Shield.&text=En%20aan%20andere%20landen%20waarmee,heeft%20over%20bescherming%20van%20persoonsgegevens.
[14]https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers
[15]https://nos.nl/artikel/2351161-privacywaakhond-waarschuwt-zet-camera-slimme-deurbel-niet-zomaar-aan
[16]https://denhaag.partijvoordedieren.nl/vragen/schriftelijke-vragen-privacy-schending-door-slimme-deurbel
[17]https://www.at5.nl/artikelen/205829/de-slimme-deurbel-als-nieuw-opsporingsmiddel-van-de-politie-een-duivels-dilemma
[18]https://autoriteitpersoonsgegevens.nl/nl/over-privacy/privacyverhalen/lilian-68-voelt-zich-onvrij-in-haar-eigen-huis-doordat-ze-niet-weet-wat-de-camera-van-de-buren-filmt
[19]https://denhaag.raadsinformatie.nl/document/9581204/1/RIS307224_Bijlage_2
[20]https://denhaag.partijvoordedieren.nl/vragen/schriftelijke-vragen-privacy-schending-door-slimme-deurbel
[21]https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stappenplan_camera_bij_huis.pdf

14

NOODHULPDIENSTEN HEBBEN MIXED REALITY IN HET VIZIER

Hoe kan mixed reality helpen om noodhulpdiensten beter voorbereid in actie te komen?

Het werk van de noodhulpdiensten bij incidenten vereist snelle informatiedeling en -selectie, betekenisvolle briefing voor aanrijdende diensten en gericht handelen in het moment. In betekenisvolle briefing en gericht handelen zal mixed reality een enorme bijdrage gaan leveren.

Highlights

- Mixed reality (MR) apparatuur wordt steeds lichter, handzamer en sneller.
- Briefing onderweg aan noodhulp-diensten gaat moeilijk met bestaande middelen.
- Mixed Reality zal het "Motorkapover-leg" bij noodhulp écht multidisciplinair maken.
- Bij noodhulp zijn privacy en security risico's bespreekbaar voor burgers en maatschappij.
- De 'technologie imaginaire' van mixed reality gaat meer dan 200 jaar terug.

De werking van mixed reality

Dagelijks wordt alarmnummer 112 ongeveer 4500 keer gebeld voor spoedeisende meldingen. Deze meldingen worden direct doorgestuurd aan politie, brandweer, ambulance, kustwacht en/of traumahelikopters. De ingeschakelde noodhulpdiensten rukken direct uit en zijn binnen 15 minuten ter plaatse. Tijdens het vertrekken en aanrijden worden bijrijders op de hoogte gesteld van de situatie ter plaatse. Echter blijkt deze informatie onvoldoende intuitief en context-afhankelijk gedeeld te worden via conventionele communicatiekanalen. Ter plaatse is herstel van veiligheid eerste prioriteit, waarna in veel gevallen een ad-hoc overleg plaatsvindt met aanwezige diensten: het "motorkapoverleg" genoemd. Vanwege fysieke beperkingen kunnen specialisten op afstand niet deelnemen aan deze overleggen. In dit artikel verkennen we beide problemen meer in detail, en zullen we toelichten hoe mixed reality deze problemen kan tackelen. Mixed Reality (MR) is in staat om context-afhankelijk, intuïtief en op een natuurlijke wijze de noodhulpdiensten bij te staan. Om te begrijpen hoe dit zou kunnen werken, moeten we

Mixed reality (MR) is een technologie die grenzen doet vervagen tussen de fysieke en virtuele wereld. Via een scherm of bril die je opzet worden hierbij digitale objecten geprojecteerd in de fysieke wereld, waar je mee kunt interacteren en die ook kunnen interacteren met de fysieke omgeving die je waarneemt.

eerst begrijpen wat MR is en hoe deze technology zich ontwikkeld heeft de afgelopen jaren.

Mixed reality (MR) is een technologie die grenzen doet vervagen tussen de fysieke en virtuele wereld. Via een scherm of bril die je opzet worden hierbij digitale objecten geprojecteerd in de fysieke wereld, waar je mee kunt interacteren en die ook kunnen interacteren met de fysieke omgeving die je waarneemt. De twee meest bekende voorbeelden van MR zijn de Google Glass uit 2014 en een functie in het spel Pokémon GO van bedrijf Niantic uit 2016. Google Glass was een slimme bril waarmee gebruikers informatie uit Google konden toevoegen aan de echte wereld, die ze zagen. Al snel bleek dat de technologie nog niet rijp was hiervoor, in 2015 stopte Google met productievan de Google Glass. Het andere bekend voorbeeld van MR zit in het spel Pokémon GO dat door 170 miljoen spelers wereldwijd actief gespeeld wordt. In Pokémon GO kunnen spelers Pokémons vangen door rond te wandelen in de buurt. Via een MR modus kunnen spelers extra punten verdienen bij vangen van Pokémons en met hun favoriete Pokémon op de foto gaan.

Naast entertainment, worden MR brillen de afgelopen jaren steeds vaker gebruikt bij bijvoorbeeld defensietrainingen, werken op afstand in de gezondheidzorg en maken van ontwerpen in de industriële toepassingen. Vanwege de vele toepassingen ontwikkelen de meeste grote technologiebedrijven als Microsoft, Apple en Facebook MR producten hiervoor. Meta, de nieuwe naam van Facebook, heeft in 2021 de koers volledig gericht op leven en werken in een MR wereld. Zij noemen deze wereld de “Metaverse”. De enorme technologische vooruitgang, gedreven door eerdergenoemde techreuzen, biedt enorme kansen op de korte en lange termijn voor inzet bij noodhulp. Dit potentieel wordt nog veel te weinig benut. Spoedeisende hulpmeldingen worden in Nederland geregiseerd door de centralisten van de Nationale Meldkamers. De centralisten voeren het gesprek met de melder(s) en coördineren tegelijkertijd de juiste inzet van Politie, Brandweer, Ambulance en Marechaussee. Zij worden daarbij bijgestaan door de medewerkers van het Real-Time Intelligence Center (RTIC), die op basis van beschikbare omgevingsinformatie en real-time informatie een situationeel beeld creeëren ter ondersteuning aan de bijrijders van aanrijdende noodhulpdiensten. Het RTIC gebruikt bij deze informatiedeling beschikbare technologieën in de voertuigen zoals portofoons en tekst- of documentdeling via mobiele devices. Zoals eerder beschreven, blijkt dat deze aangeleverde informatie onderweg veelal niet goed begrepen wordt of onvoldoende situationeel relevant gemaakt wordt. Hierdoor worden noodhulpdiensten gedwongen kostbare seconden ter plaatse te besteden om zich alsnog te oriënteren en zich bewust te maken van de locatie en wat er om hen heen gebeurt. Dit wordt ‘Situational Awareness’genoemd. De gebruikte kennisdelingsinfrastructuur van de noodhulpdiensten schiet hierin klaarblijkelijk nog tekort. MR kan dit gat dichten en helpen bij het creëren van betere Situational Awareness. Hierdoor kan ter plaatse sneller en gerichter gehandeld worden.

Een andere toepassing van MR bij noodhulp is direct na het handelen in het moment. Na het directe herstel van veiligheid, verschuift de focus van de noodhulpdiensten naar het gezamenlijk plannen van de vervolgstappen voor een meer structurele oplossing. Dit gebeurt door middel van het

eerdergenoemde 'motorkapoverleg'. Hierbij worden alle aanwezige disciplines fysiek bij elkaar geroepen om 'over de motorkap' een oplossing te bedenken en de daaruit volgende activiteiten integraal te coördineren. Ook hierbij kan MR van toegevoegde waarde zijn, door specialismes en leidinggevenden op afstand over de schouder te laten meekijken en ze te laten bijdragen aan het vinden van de beste oplossing.

Een verkenning van mixed reality in de context van noodhulp

We spraken over deze mogelijkheden van MR in de context van noodhulp met twee experts op dit gebied, Dhr. Florian Käding en Dr. Imar de Vries. Dhr. Käding is één van de oprichters van Prometech, een bedrijf dat MR-simulaties ontwikkelt voor de ambulance voor moeilijk trainbare situaties, zoals biologische aanvallen met giftige gaswolken. Dr. de Vries is Wetenschapper bij Universiteit Utrecht, en focust zich vanuit een mediastudies perspectief op onder andere de technologische ontwikkeling van mixed reality toepassingen.
In gesprek met Dhr. Käding kwam naar voren dat technologische ontwikkelingen van MR enkele jaren geleden nog vrij onvolwassen waren. MR-brillen vertoonden vaak kwalitatief slecht beeld, waren langzaam in bediening en voelden zwaar aan op het gezicht. De afgelopen jaren zag hij veel nieuwe verbeteringen in de technologie. Kijk bijvoorbeeld naar de succesvolle Hololens van Microsoft, met geavanceerde driedimensionale projecties, waarmee op een natuurlijk manier kan worden geinteracteerd. Het nadeel van de Hololens is volgens Dhr. Käding helaas nog dat deze zwaarder en minder handzaam is dan sommige alternatieven. Wuzix M400 Smart Glass is zo'n lichter alternatief dat is ontwikkeld door de Brits-Nederlandse startup Wuzix. In de Volkskrant stond recentelijk een artikel[1] over deze Wuzix bril in een pilot bij tientallen zorginstellingen. In de pilot konden verzorgers spraakgestuurd experts op afstand laten meekijken. Ook konden verzorgers direct gecoacht worden in hun werk. Deze use case is vergelijkbaar met aanrijdende hulpdiensten aldus Dhr. Käding, waar ook vaak verschillende experts op afstand met elkaar moeten communiceren.

Zijn ervaring met ambulance-diensten was dat autorijden gepaard gaat met (te) veel beweging om een tablet nuttig te kunnen gebruiken. Een MR-bril zou dit probleem kunnen oplossen. Ter plaatse moeten handen vaak vrij gehouden worden vanwege de veiligheidshandschoenen die nodig zijn, waardoor gebruik van touch screens op mobiele telefoons of tablets onwerkbaar zijn. MR-glazen kunnen ook deze beperking overbruggen. Centralisten en RTIC medewerkers kunnen via MR informatie makkelijker delen en projecteren op de omgeving van de aanrijdende diensten. En ter plaatse kunnen de meldkamers meekijken en indien nodig gericht real-time noodhulpdiensten attenderen op bijvoorbeeld aanwezige camera's en de daarbij behorende camerabeelden via zo'n MR-bril.

Eenzelfde toepassing geldt voor het motorkapoverleg, waarbij specialistische publiek- en private diensten face-to-face ingevlogen zouden kunnen worden via MR voor een structurele oplossing. De eerder genoemde pilot met Wuzix MR glazen was succesvol in face-to-face ondersteuning, maar strandde op privacy risico's van de verwerkte data en risico's op hacking van de technologie. Deze risico's omtrent inzet van MR-Glasses, werden ook al eerder in 2016 benoemd in het politie visiedocument 'Visie op Sensing[2]'. Volgens dit visiedocument zou een zwakke schakel in de informatiebeveiliging ertoe kunnen leiden dat hackers kunnen beïnvloeden wat gebruikers zien, horen en voelen. Daarom is het belangrijk bij deze technologie dat de randvoorwaarden van privacy en security in overleg met de wetgevers en maatschappij worden vastgesteld. Hoewel dit een uitdagende opgave lijkt, blijkt uit het visiedocument dat er een maatschappelijke acceptatie lijkt te zijn voor inzet van nieuwe technologieën bij noodhulp en dat de menselijke maat hierbij bepalend is. Deze problemen lijken dus overkomelijk te zijn, zolang de MR-toepassingen primair ingezet worden bij het levensreddende werk van noodhulpdiensten.
In het tweede gesprek met wetenschapper Dr. Imar de Vries kwamen andere aspecten van MR technologie naar voren; met name hoezeer denken en dromen over MR-toepassingen de richting van technologische ontwikkelingen heeft

beïnvloed in de afgelopen decennia. Dr. Imar de Vries lichtte toe hoe belangrijk uitgesproken wensen over toepassing van MR zijn voor ontwikkelaars van deze technologie. Beschrijving van wens-denken over technologie aan de hand van concrete toepassingen noemt hij 'techologyil maginaire'. Dit klinkt wellicht initieel als sprookjesdenken, maar zorgt voor een enorme drive bij jonge technologische bedrijven om van deze 'sprookjes' werkelijkheid te maken. Jaren geleden deed Dr. de Vries een observatie-studie bij Amsterdamse MR startup Layer. Hierbij kwam naar voren dat dit wens-denken vanuit de echte praktijk, in combinatie met inspiratie uit films en boeken, een drijvende kracht vormen voor het opzetten en ontwikkelen van deze technologie. Layer haalde zijn motivatie en inspiratie uit de Japanse tekenfilmserie Dennou Coil en uit de MR contactlensen uit Vernor Vinge's boek 'Rainbow's End'. Deze referenties zullen wellicht niet bij iedereen bekend zijn, maar veelen zullen wel de MR toepassingen uit bekende films als Minority Report uit 2002 of de Star Trek Holodeck kunnen herinneren en hoe wij via TV geïntroduceerd werden tot de enorme potentie van MR in de toekomst. Tot slot gaf Dr. de Vries aan dat uit zijn onderzoek ook blijkt dat esthetische aspecten als herkenbaarheid en de juiste productnaam een rol spelen in het mainstream maken van een technologie. Dr. de Vries sprak als laatste ook nog over de 'technology imaginaire' van de afgelopen 200 jaar rondom immersie en telepresence, waar de hedendaagse MR-technologie een verwezenlijking van is. De ontwikkeling van MR-toepassingen is daarmee onderdeel van een lange geschiedenis en lijkt te voldoen aan een diepe menselijke behoefte die eeuwen terugreikt.

De toegevoegde waarde van mixed reality in noodhulp

Na interessante discussies over de uitdagingen van MR-toepassingen in de noodhulp, blijkt dat de voordelen hoger opwegen dan de privacy en security-risico's. Deze risico's blijken overkomelijk te zijn, mits deze in nauwe samenwerking met burgers en de maatschappij afgekaderd worden. Met name bij het creëren van Situational Awareness en samenbrengen van verschillende disciplines bij het motorkapoverleg zullen MR-toepassingen van grote toegevoegde waarde zijn. Ook is de conclusie dat huidige technologische beperkingen slechts van tijdelijk aard zijn en dat de verdere verbetering van MR-technologie niet geremd zal stoppen. Gedreven door futuristische beelden uit populaire cultuur en creatieve ideeën van medewerkers uit het veld zullen toepassingen van MR binnen de noodhulp niet een kwestie van 'of' zijn, maar van 'wanneer'. En met de enorme hoeveelheid geld die in deze technologie wordt geïnvesteerd door de grote techreuzen, zal MR op korte termijn de noodhulp sneller en effectiever gaan maken voor ons allemaal.

Over de auteur

Arul Elangovan

Enterprise Architect

Arul Elangovan MBA Msc is verantwoordelijk voor Citizen First binnen Capgemini, werkt aan verbetering van de dienstverlening bij de politie en verzorgt customer experience- en architectuurtrainingen en gastcollege's.

arul.elangovan@capgemini.com

[1]https://www.volkskrant.nl/wetenschap/gaat-de-slimme-bril-de-zorg-ontlasten~b565974a/
[2]Visie op Sensing (2016), visiedocument van de Politie

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: de randvoorwaarden voor succes

De beweging naar de superslimme samenleving, oftewel Society 5.0, is volop gaande. Society 5.0 verwijst naar de vierde industriële revolutie (Industry 4.0) waarbij de volgende stap na de digitalisering van de productieprocessen is om alle systemen met elkaar te verbinden en te laten communiceren. De Super Smart Society (Society 5.0) volgt de Informatie Samenleving (Society 4.0) op.

https://www.capgemini.com/nl-nl/bronnen/society-5-0-de-randvoorwaarden-voor-succes/

Trends in Cybersecurity 2022

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

https://www.capgemini.com/nl-nl/bronnen/trends-in-cybersecurity-2022/

De stand van zaken op de Nederlandse cloudmarkt

Dit onderzoek kijkt naar de evolutie van de Nederlandse cloudmarkt.

Het beoordeelt de voortgang van organisaties in hun digitale transformatietrajecten, en waar zij zichzelf zien in termen van cloud- en DevOps-volwassenheid. Het rapport is gebaseerd op enquêtegegevens, onderzoek en analyse uitgevoerd door IDC in opdracht van Capgemini.

https://www.capgemini.com/nl-nl/bronnen/cloudtransformatie-met-capgemini/

BLOGS

Trends in Veiligheid blogs

Onze experts en thoughtleaders zijn dagelijks bezig met organisaties, processen, beleid, sturing en inrichting in het brede veiligheidsdomein.

Frequent publiceren zij een blog op onze Trends in Veiligheid website, om u zo op de hoogte te houden van de nieuwste inzichten in trends en ontwikkelingen binnen het veiligheidsdomein. Ga naar de Trends in Veiligheid blogs via: **www.trendsinveiligheid.nl**

En alle overige Capgemini blogs via:
Blogs

Nederland www.capgemini.com/nl-nl/blogs
Global: www.capgemini.com/blog

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

Zeger de Bruijne †
Pablo Derksen
Judith Groenewoud
Jule Hintzbergen
Thomas de Klerk
Marcel Kordes
Martijn van de Ridder
Erik Staffeleu

Advies, ontwerp en productie: Marketing & Communicatie Capgemini Nederland B.V.
Johanna Achterberg, Ashim karmakar.

Fotografie: Marnix van 't Klooster, Shutterstock

Capgemini Nederland B.V.
Postbus 2575 - 3500 GN Utrecht
Tel. +31 30 689 00 00
E-mail: trendsinveiligheid.nl@capgemini.com
website: www.trendsinveiligheid.nl

Over Capgemini

Capgemini is een wereldwijde, maatschappelijk verantwoorde en multiculturele marktleidermet325.000menseninbijna50landen.Alsstrategischpartnerondersteunt Capgemini organisaties bij hun transformatie door gebruik te maken van de kracht van technologie. Hierbij laat de Group zich leiden door zijn bestaansreden: menselijke energie vrijmaken door middel van technologie voor een inclusieve en duurzame toekomst. Met meer dan 55 jaar ervaring en expertise in uiteenlopende sectoren, vertrouwen klanten de aanpak van hun zakelijke behoeften toe aan Capgemini: van strategie en ontwerp tot operationeel beheer. Dit gebeurt door gebruik te maken van innovaties in cloud, data, kunstmatige intelligentie, connectiviteit, software, digital engineering en platforms. De Group behaalde in 2021 een omzet van € 18 miljard.

GET THE FUTURE YOU WANT | www.capgemini.nl

Capgemini Nederland B.V.
Postbus 2575 - 3500 GN Utrecht
Tel. +31 30 689 00 00
www.capgemini.nl

IN/1A-005.22