Capgemini

Trends in Veiligheid 2021-2022

Adaptieve organisaties houden Nederland veilig

Inhoudsopgave

Trends in Veiligheid 2021: adaptieve organisaties houden Nederland veilig

Op het moment van schrijven van dit trendrapport is de strijd tegen COVID-19 nog in volle gang. Woorden schieten tekort om te beschrijven hoe blij we zijn met de inzet van eenieder in deze strijd, waaronder niet in de laatste plaats de medewerkers in het veiligheidsdomein. Want juist ook de organisaties in het veiligheidsdomein hebben moeten reageren op de nieuwe werkelijkheid, zowel wat die betekent voor de samenleving als ook wat die betekent voor de eigen organisatie en manieren van werken.

Een van de interessante aspecten in deze omwenteling is de rol van technologie. Technologie heeft nu, nog meer dan eerder, mensen samengebracht, is faciliterend geweest in samenwerking en in het delen van creativiteit en informatie. Het heeft er zelfs voor gezorgd dat ontwikkelingen die al een tijdje langzaam gingen, opeens een versnelling kregen door de urgentie die gevoeld werd. Niet het vermijden van risico's, maar de focus op het benutten van kansen staat daarbij centraal. Ook binnen het veiligheidsdomein was dit waarneembaar, zoals Ric de Rooij, plaatsvervangend secretaris-generaal bij het Ministerie van Justitie en Veiligheid, ons vertelde in een recent gesprek:

"Corona heeft ons bijvoorbeeld geholpen in het versterkte besef dat we meer moeten investeren in de informatiebeveiliging. Niet om de boel meer dicht te zetten, maar juist om stapsgewijs bewust risico's nemen. Veiligheid als driver om risico's te nemen. Niets doen is ook geen optie. Het urgentiebesef heeft ons bijvoorbeeld geholpen om versneld een Cloudstrategie en Cloudafwegingskader te maken. Dat gaat de organisaties in het domein helpen in de doorontwikkeling."

In dit trendrapport zien we talloze voorbeelden van het grote vermogen van het veiligheidsdomein om adaptief te zijn, als respons op de crisis maar ook als reactie op de steeds sneller digitaliserende samenleving.

Ric de Rooij: "Je ziet hierin een aantal praktische ontwikkelingen die nu versneld zijn gerealiseerd, zoals het meer gebruikmaken van telehoren. Maar breder zijn we veel meer bezig met het gebruik van data en hoe je slim en veilig organiseert dat data op het juiste moment op de juiste plek beschikbaar is. Zo moet een officier van Justitie overtuigd kunnen zijn dat hij/zij kan vertrouwen op de informatie van de politie zonder dat deze tussentijds gecorrumpeerd is. De strafrechtketen is belangrijk als het gaat om dergelijke waarborgen."

In enkele artikelen komt dit aspect van informatiegestuurd werken en de deling van data of informatie terug. Slimme technieken kunnen helpen in het delen van informatie zonder dat onderliggende data gedeeld hoeft te worden.

We herkennen duidelijk in het domein dat meer en beter gewerkt wordt aan informatiegestuurd werken. Zo wordt verkend hoe met behulp van Artificial Intelligence (AI) de prioritering van strafzaken kan worden ondersteund. En wordt gewerkt aan een verbeterde intake van cyberzaken en gedigitaliseerde criminaliteit om intelligence te genereren die gebruikt kan worden bij het bestrijden van dit fenomeen met vernieuwende interventies. De toename van gedigitaliseerde criminaliteit en cybercriminaliteit heeft ervoor gezorgd dat het inmiddels de hoeveelheid woninginbraken voorbij is. Het is VVC (Veel Voorkomende Criminaliteit) in het jargon. Daar waar traditioneel de strafrechtketen toegerust is op het aanpakken van één of enkele daders die één of enkele slachtoffers maken, zal men nu moeten omgaan met een enkele dader die honderden slachtoffers kan maken, verspreid over het land, in een middag tijd. Het gebruik van techniek en meer in het bijzonder data zal hierin een oplossing moeten verzorgen. Hoe dit kan worden gedaan wordt ook in een artikel in dit rapport mooi beschreven.

Informatiegestuurd werken en het gebruik van data, helemaal bij de overheid en in het bijzonder het veiligheidsdomein, staat meer dan ooit in de belangstelling. Transparantie, veiligheid en ethiek zijn enorm van belang. Ook hier geldt dat er naast risico's, vooral kansen te benutten zijn. Zo zien we dat innovatieve ontwikkelingen ook organisaties kansen biedt om nieuwe maatschappelijke waarde te creëren. Kijk bijvoorbeeld naar het CJIB, dat de meesten van ons zullen kennen van het verwerken en innen van verkeersboetes. Door middel van slimme data-analyses in het Datalab JenV willen zij burgers met schulden kunnen signaleren om hen in een vroeg stadium te kunnen (laten) helpen in plaats van het stug verder opstapelen van de schulden. Op deze manier wil het CJIB voorkomen dat mensen verder in de problemen komen.

Een ander voorbeeld is op het vlak van identiteitsfraude, een criminaliteitsvorm die de afgelopen 6 jaar met meer dan 500% toegenomen is. Door de digitale versnelling in de periode van COVID-19 is dit alleen maar verder toegenomen. Om één van de grootste oorzaken van dit groeiende probleem het hoofd te bieden, ondersteunen data en AI de mens bij het sneller en beter detecteren van de echtheid van identiteitsdocumenten. In dit rapport leest u daar meer over.

De recente coronacrisis heeft ook nog eens versneld duidelijk gemaakt dat de organisaties in het veiligheidsdomein zich niet enkel te richten hebben op een veranderende samenleving, maar ook de eigen organisatie zich snel heeft aan te passen. De pandemie heeft voor een verschuiving gezorgd in hoe en waar we werken. Werken op afstand is hiervan het meest voor de hand liggende aspect, maar het is slechts het topje van een ijsberg. Het heeft fundamentele gevolgen voor het behouden van talent in de organisaties, de processen, onroerend goed, duurzaamheid en technologie. De organisaties in het domein moeten een nieuw sociaal contract smeden met werknemers en de samenleving, waarin de autonomie en flexibiliteit die werknemers nu tijdens de pandemie opdoen, de verwachtingen permanent herdefiniëren. Door deze ontwikkeling te omarmen, kan het domein straks profiteren van een (nog) meer betrokken en loyale groep medewerkers, lagere bedrijfskosten en een kleinere ecologische voetafdruk.

Echter, ook al voor COVID-19 was er een stroomversnelling waarneembaar in het toepassen van AI en robotisering en de ingrijpende gevolgen die dit heeft voor het personeel en de aard van het werk. Om het rendement op investeringen in AI en automatisering te maximaliseren, moeten de managers en bestuurders in het domein de implicaties ervan begrijpen voor de rollen, vaardigheden en talent die ze nodig hebben om in de toekomst te gedijen, en een cultuur creëren van continu leren en aanpassen. Wetende dat vrijwel iedere organisatie begint te beseffen dat men versneld nieuwe vaardigheden in huis moet halen, volstaat de 'fire-and-hire' methode niet meer. De vijver waaruit gevist wordt voor nieuwe talenten is klein en er zijn straks te veel vissers. Nu kijken hoe je daarop kunt anticiperen, bijvoorbeeld door kritisch te kijken naar de omscholing van een deel van je personeel, of de inzet van techniek is noodzakelijk. Wij noemen dit 'Reinventing work' en in dit trendrapport wordt bijvoorbeeld inzicht gegeven in hoe Defensie middels strategische personeelsplanning anticipeert op deze ontwikkeling.

Ook Ric de Rooij benadrukt deze noodzaak: "Wij hebben het besef dat we ook meer moeten investeren in wat we noemen ambtelijk vakmanschap op digitalisering. We hoeven niet alles zelf in huis hebben maar we moeten wel voldoende kunnen inschatten wat de kansen en bedreigingen zijn van digitalisering, zoals bijvoorbeeld op het vlak informatiebeveiliging. We hoeven niet alle state-of-the-art kennis te hebben, daarvoor kunnen we jullie inhuren, maar we moeten wel in staat zijn om te zien waar we waarde toe kunnen voegen en de impact op veiligheid kunnen vergroten."

In dit trendrapport vindt u vele artikelen die gaan over hoe data en informatie het domein helpen om effectiever en doelmatiger te zijn, hoe cyber(security) enorm toeneemt en hoe er in de eigen organisatieontwikkeling en innovatie processen wordt geanticipeerd op de toekomst. Het was ons wederom een waar genoegen om dit rapport samen te stellen en we wensen u veel leesplezier.

Erik Staffeleu
Senior Director Publieke Sector, Capgemini Invent

erik.staffeleu@capgemini.com

Martijn van de Ridder
Hoofd Insights & Data Publieke Sector, Capgemini

martijn.vande.ridder@capgemini.com

Wijkagent – Assistentie gevraagd!

Hoe kunnen wijkagenten geholpen worden om niet te verdrinken in de toenemende hoeveelheid beschikbare informatie?

Highlights

- **Te veel informatie en infobesitas bedreigen de effectiviteit van wijkagent.**
- **Een Intelligente Virtuele Assistent (IVA) kan informatie filteren op relevantie.**
- **De IVA kan gedrag en stress monitoren, om informatie effectief te doseren.**
- **Aandachtspunten zijn 'filterbubbels' en de uitlegbaarheid van keuzes.**
- **Met hulp van de IVA houdt de wijkagent regie op het eigen werk.**

Het werk van de wijkagent verandert door een stroom aan informatie uit sociale media, sensoren en statistieken. Een eigen Intelligente Virtuele Assistent (IVA) gaat hierbij helpen.

In het gebiedsgebonden politiewerk (GGP) zijn wijkagenten de schakel tussen bewoners, bedrijven en instanties in de buurt. Wijkagenten zijn cruciaal bij de integrale aanpak van veiligheid in de wijken. In de regel is één wijkagent verantwoordelijk voor 5000 burgers. Vanuit het principe van 'kennen en gekend worden' proberen wijkagenten het vertrouwen in de politie te verhogen en de afstand tot burgers te verkleinen. Nauw contact met burgers en organisaties is in deze digitale tijd belangrijker dan ooit. De eerste aanwezigen bij gebeurtenissen in de wijk zijn burgers die smartphones, sociale media en lokale buurt-apps gebruiken om hoge kwaliteit video's, foto's en ook realtime informatie te delen. Daarnaast komt er ook steeds meer informatie digitaal binnen vanuit lokale instanties, overheden, publieke en private sensoren. En uiteraard krijgt de wijkagent ook informatie van collega's doorgespeeld. Daaruit moet de wijkagent filteren wat relevant is en waarop geacteerd moet worden. Er zijn grote verschillen te onderkennen in informatiebehoeften bij wijkagenten in grote steden en op het platteland. In steden wordt vaak gewerkt met GGP-teams waarin wijkagenten ook nog individuele expertise hebben met specialistische informatiebehoefte als gevolg. In de huidige situatie vindt filtering van informatie plaats via intakekanalen zoals servicecentra, webcare en operationele coördinatoren. Zij zijn niet in staat om het gewenste maatwerk te leveren voor individuele wijkagenten. Om niet het risico te lopen dat relevante informatie wordt gemist, wordt meer informatie gedeeld aan de wijkagent dan hij of zij daadwerkelijk aankan. Daardoor sneeuwt de wijkagent onder in deze groeiende hoeveelheid informatie.

AI als oplossing voor informatie-overload

Zou Artificial Intelligence (AI) kunnen helpen om uit deze grote hoeveelheid informatie te halen die voor een specifieke wijk of expertise van een wijkagent relevant is? We spraken over de mogelijkheden van Intelligente Virtuele Assistenten met prof. dr. Tibor Bosse, hoogleraar Sociale AI aan de Radboud Universiteit Nijmegen, en dr. mr. Charlotte Gerritsen, universitair docent Sociale AI en Criminologie aan de VU Amsterdam.

Bij het bespreken van het informatieprobleem van de wijkagent, typeerden prof. dr. Bosse en dr. mr. Gerritsen het probleem als infobesitas[1]. Zij gaven aan dat infobesitas ervoor zorgt dat het overzicht kwijtraakt door een continue stroom van informatie. Hierbij wordt vooral die informatie gelezen die aansluit bij de eigen voorkeuren en vooroordelen. Over de gevaren van infobesitas bij de politie werd al eerder gewaarschuwd in 2016

in een Belgisch onderzoek naar de aanslagen in Zaventem en Maalbeek[2]. Hierin kwam naar voren dat infobesitas en gefragmenteerde informatiebronnen één van de grootste problemen zijn voor de hedendaagse politie. De politie kent van oudsher een informatiebeleid van 'need to know', wat heeft geleid tot de fragmentatie van informatie door de politie heen. Op basis van het onderzoek besloot de politie in België daarom de aanpak meer te verschuiven van 'need to know' naar 'need to share'. Ook in Nederland is deze verschuiving merkbaar. En met een need to share-aanpak zal het probleem van infobesitas alleen maar groter worden.

Zou AI kunnen helpen met het tackelen van het probleem van infobesitas?

In de wereld van AI worden steeds vaker Intelligente Virtuele Assistenten (IVA) ingezet om mensen te helpen in het werk en te behoeden tegen problemen als infobesitas. IVA-en kunnen bijvoorbeeld getraind worden om informatiestromen effectief te filteren voor de gebruiker en om zelfs proactief verschillende gefragmenteerde informatiebronnen te doorzoeken. Om te komen tot een goede eindselectie van informatie kan een IVA gebruikmaken van een aanbevelingsalgoritme ('recommender engine'). Deze aanbevelingsalgoritmes kennen we uit ons privéleven van bijvoorbeeld YouTube en Netflix, die ons adviezen geven over interessante producten of films. Deze algoritmes maken in eerste instantie gebruik van historische kennis, en passen het advies daarna aan op het kijk-en luistergedrag van de specifieke gebruiker. In het geval van de wijkagent, zou het aanbevelingsalgoritme getraind worden op historische informatie van de politie intakekanalen en de collega wijkagenten in verschillende geografische gebieden. Bij het eerste gebruik zal de virtuele assistent voor elke wijkagent vergelijkbare soort informatie naar voren brengen uit de wijk, maar na verloop van tijd zal het aanbevelingsalgoritme steeds meer leren van het persoonlijke kijkgedrag. Ook kan de agent specifieke feedback geven over hoe relevant het gepresenteerde resultaat is, waardoor de IVA steeds beter leert welke informatie meer of minder relevant is voor de specifieke wijkagent. Daarnaast zou de virtuele assistent gebruik kunnen maken van bijvoorbeeld huidgeleiding in een slim horloge of de telefooncamera om stressvolle situaties te detecteren. Daarmee zou in acute situaties de informatie verder beperkt kunnen worden tot alleen de nú relevante informatie. Zo zal de Intelligente Virtuele Assistant de wijkagent in verschillende situaties kunnen ondersteunen en beschermen tegen het groeiende gevaar van infobesitas.

Explainable AI

Ook vroegen wij aan prof. dr. Bosse en dr. mr. Gerritsen of er risico's verbonden zijn aan het gebruik van deze IVA-en? Er blijken enkele belangrijke risico's hierin te typeren. Zo is er bijvoorbeeld het risico op het ontstaan van een filterbubbel of 'fabeltjesfuik', zoals Arjen Lubach dat heeft genoemd in zijn programma[3]. Doordat een systeem alleen nog informatie toont, die interessant wordt gevonden, komt de gebruiker terecht in een soort digitale informatiebubbel. Hierdoor ontstaat ook het beeld dat andere informatie dus ook irrelevant is. Een onderzoek uit 2015 door Facebook[4] toonde aan dat mensen op sociale media zich 15% meer beperken tot eigen interesses dan ze via TV of kranten zouden doen. Een manier om dit tegen te gaan is door juist extra te attenderen op ander soort informatie in de buurt. Ook deze aanpak wordt veel gebruikt voor webwinkel bezoekers. Websites als bol.com gebruiken deze aanpak om je te verleiden om naar andere producten te kijken dan waar je naar zocht. Hier zal de Intelligente Virtuele Assistent op ingericht moeten worden om een filterbubbel tegen te gaan.

Een ander risico waar we met prof. dr. Bosse en dr. mr. Gerritsen over spraken was de verklaarbaarheid van de keuzes van de assistent. Dit concept wordt 'explainable AI' genoemd, waarbij een mens in staat moet zijn om het pad te herleiden dat een AI-systeem heeft gebruikt om tot een beslissing te komen. Neurale netwerken zijn een bekend voorbeeld van zo'n AI-systeem waarbij het keuzepad niet terug te lezen is door een mens; het is een 'black box'. Voor een wijkagent zal dit onwenselijk zijn, omdat je altijd moet weten waarop informatiekeuzes zijn gebaseerd. Daarom zal de intelligente virtuele assistent gebruik moeten maken van explainable AI. In het geval van de geselecteerde informatie door de wijkagent kan dat bijvoorbeeld zijn dat het onderwerp door hem of haar zelf in het verleden als interessant was gemarkeerd.

Na een discussie over de voor- en nadelen, concludeerden wij samen met prof. dr. Bosse en dr. mr. Gerritsen dat IVA-en veel mogelijkheden voor de wijkagent kunnen bieden. Wel is het hierbij van belang om rekening te houden met alle valkuilen van AI. Als dat goed gebeurt, zal de wijkagent met een Intelligente Virtuele Assistent op zak meer regie kunnen houden op het eigen werk én de verdere digitalisering van de maatschappij het hoofd kunnen bieden. De wijkagent zal minder tijd besteden aan lezen van irrelevante informatie, en meer tijd overhouden om als 'koene boevenvanger' de wijk en Nederland veiliger te maken.

Aan het einde van ons gesprek vertelde prof. dr. Bosse nog kort over zijn werk met Europese ruimtevaartorganisatie ESA[5]. ESA werkt namelijk ook aan ontwikkeling van e-Partners voor astronauten, die tijdens een Mars-missie zullen helpen bij complexe situaties, en zelfs emotionele steun kunnen bieden. Als dit soort futuristische technologie óók aan de IVA van de wijkagent zou kunnen worden toegevoegd, dan is bescherming tegen infobesitas wellicht nog maar het tipje van de sluier voor de wijkagent van de toekomst.

[1]Infobesitas and psychologische factoren: https://www.researchgate.net/publication/336612222_DECISION_MAKING_IN_THE_ERA_OF_INFOBESITY_A_STUDY_ON_INTERACTION_OF_GENDER_AND_PSYCHOLOGICAL_TENDENCIES

[2]Belgisch Onderzoek uit 2016 naar aanslagen Zaventem en Maalbeek: https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/pdf/94442.pdf

[3]Uitzending 'De Fabeltjesfuik' van Arjan Lubach: https://youtu.be/FLoR2Spftwg

[4]Exposure to ideologically diverse news and opinion on Facebook – E. Bakshy, S. Messing, L.A. Adamic: https://science.sciencemag.org/content/348/6239/1130

[5]Supporting Human-Robot Teams in Space Missions using ePartners and Formal Abstraction Hierarchies – T. Bosse, J. van Diggelen, M.A. Neerincx, and N.J.J.M. Smets, 2015

Auteurs

Arul Elangovan
Enterprise Architect

arul.elangovan@capgemini.com

Arul Elangovan MBA Msc focust vooral op dienstverlening naar burgers en partners in het publieke veiligheidsdomein en verzorgt daarin ook trainingen.

Frank Inklaar
Business Analist

frank.inklaar@capgemini.com
twitter.com/frin63

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

Veiligheid is mensenwerk: hoe Defensie in de ‘strijd om talent’ haar strijdplan bepaalt

Hoe zet Defensie ‘Intelligent HR’ in om deze talentenstrijd te winnen?

Highlights

- **Veiligheid is mensenwerk: technologie valt of staat met het juiste talent.**
- **De snelle ontwikkelingen en de 'strijd om talent' maken dit tot een forse uitdaging.**
- **Een sterk strijdplan is noodzakelijk om over het juiste talent te beschikken.**
- **Een gedeelde visie en krachtige samenwerking tussen operatie en HR is cruciaal.**
- **Een adaptieve krijgsmacht vraagt om 'Intelligent HR', afgestemd op de visie van Defensie.**

Het veiligheidsdomein is aan disruptieve verandering onderhevig. We liggen dagelijks onder vuur in het cyber- en informatiedomein. Het is voor Defensie – én ons Koninkrijk – cruciaal om over het juiste talent te beschikken. Gezien de 'strijd om talent' in het IT-domein, is dit geen sinecure.

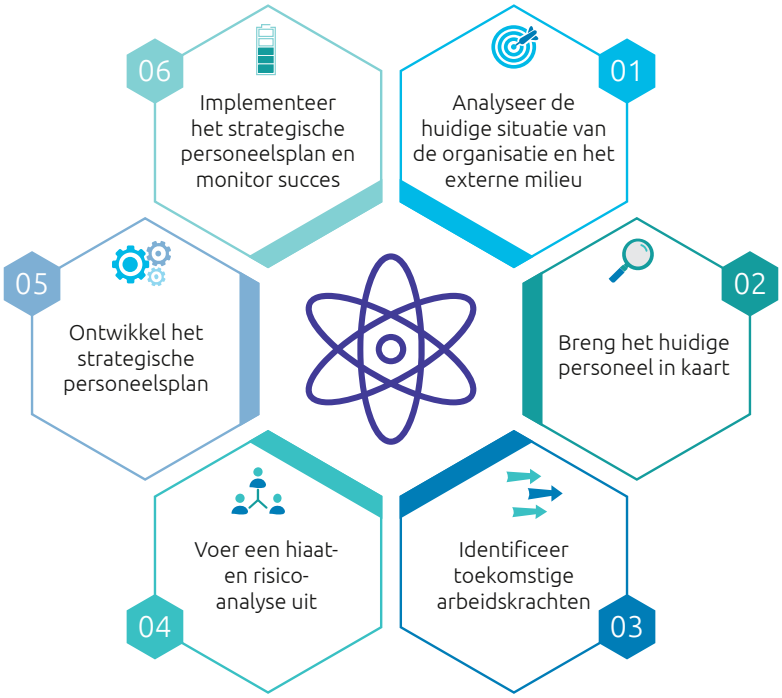
De Defensievisie 2035 liegt er niet om:

"Er is wat aan de hand: ons Koninkrijk wordt dagelijks aangevallen in het cyber- en informatiedomein. Defensie moet daarom een antwoord hebben op de vele dreigingen die, nu en in de toekomst, op ons afkomen."

De dreiging waartegen Defensie ons land beschermt, verplaatst zich steeds meer naar een combinatie van fysiek en cyber en neemt nieuwe vormen aan. Deze dreiging komt van statelijke actoren die zich in hoog tempo ontwikkelen in het cyberdomein. Denk bijvoorbeeld aan het fenomeen van 'fake news': dit wordt ingezet om mensen te beïnvloeden, verkiezingen te manipuleren en kan maatschappijen destabiliseren. Fake news wordt mogelijk gemaakt door een breed scala aan nieuwe technologieën: denk aan artificial intelligence, machine learning, deep fake en big data. Krachtige middelen, die afhankelijk van de toepassing tot veel goeds of kwaads kunnen leiden. 'Klassieke wapensystemen' transformeren steeds meer naar IT-systemen met grote hoeveelheden sensoren. Het adequaat verwerken, analyseren en toepassen van deze data wordt doorslaggevend op het strijdtoneel. Daarmee neemt ook het belang toe van 'Cyber Defense'. Dit gaat inmiddels al veel verder dan je antivirusprogramma regelmatig updaten. Defensie bereidt zich voor op nieuwe wapens die worden gebruikt in het digitale domein.

CIO Defensie, Jeroen van der Vlugt geeft aan: "Om ons land adequaat te kunnen beschermen moeten onze mensen er kunnen staan – toegerust, geoefend en getraind. En juist díe mensen, die beschikken over het juiste talent (kennis en kunde) om met deze nieuwe digitale technologieën te werken, zijn schaars. Bovendien is de concurrentie tussen organisaties groot: Defensie bevindt zich in een zogenaamde 'strijd om talent' en ook in deze strijd moet Defensie haar strijdplan bepalen." Nog steeds zeer relevant is het oude adagium van Capgemini-oprichter Serge Kampf: "technologie is niets zonder de mens" en dit geldt net zo goed voor het veiligheidsdomein.

In dit artikel lichten we toe hoe Defensie haar strijdplan heeft bepaald en wat andere (veiligheids)organisaties hiervan kunnen leren. Volgens Van der Vlugt is Defensie "voor een hoop jonge mensen een prachtige organisatie met unieke carrièremogelijkheden op het gebied van data en cyber. Daarnaast is het een organisatie met veel maatschappelijke impact, waarbij het om meer draait dan het optimaliseren van een conversie-algoritme van een webwinkel. Ons werk doet er echt toe voor vrede en veiligheid."



Het juiste strijdplan bepalen is een holistische exercitie

Het opstellen van een strategisch personeelsplan (= een 'strijdplan') is geen sinecure. Het vraagt coöperatie tussen de operatie en de HR-functie, tussen specialisten en generalisten en tussen teamleiders en de top van de organisatie. Het juiste strijdplan bevat immers een gedegen visie op een onvoorspelbare toekomst en daar zijn vele vormen van kennis en expertise voor vereist:

- Welke technologische ontwikkelingen gaan ons raken en wanneer?
- Welke functies zullen er in de toekomst nog zijn en welke nieuwe komen erbij?
- Hoeveel nieuwe technologische ontwikkelingen kunnen we als organisatie absorberen en hoe moeten wij ons daarvoor organiseren?
- Werkt de hiërarchische command-and-control lijn nog wel, of moeten we ons richten op flexibelere vormen van samenwerking zoals Agile of DevOps?

Al deze vragen vormen de kern van wat we strategische personeelsplanning (SPP) noemen: op een strategische, langetermijnmanier naar de organisatie en het medewerkersbestand kijken om te bepalen hoe deze zich dient te ontwikkelen én wat hiervoor van de organisatie gevraagd wordt. Bij het opstellen van het SPP staat de Defensievisie 2035 centraal en vormt de Defensie IT-strategie het startpunt. "Om haar uiteindelijke doel te behalen, namelijk het zijn van een adaptieve krijgsmacht, zet Defensie in op de vijf pijlers van haar IT-Strategie. De IT binnen Defensie moet robuust, wendbaar, digitaal weerbaar, datagedreven en interoperabel zijn. Maar zoals gezegd, alleen het juiste talent is cruciaal. Het startschot voor het opstellen van het strijdplan is hiermee gegeven", aldus Jeroen van der Vlugt.

Capgemini en het CIO Office stelden gezamenlijk een strategisch personeelsplan op voor de IT-/IV-/IM-functiegroep, waarbij naast Landmacht, Luchtmacht, Marine en Marechaussee ook de Bestuursstaf, het Defensie Ondersteuningscommando en de Defensie Materieelorganisatie betrokken zijn. De fases voor het maken van een SPP zijn gezamenlijk doorlopen (aan de hand van het e-CF[1]) om uiteindelijk het strijdplan op te kunnen stellen. De uitdaging voor Defensie bleek na afloop van dit traject fors: Defensie moet flink veel mannen en vrouwen gaan aantrekken, om- of bijscholen om aan de behoefte aan technologie-talent te voldoen. Dit inzicht was zonder het gezamenlijk en stapsgewijs werken aan een analyse van het medewerkersbestand niet mogelijk geweest en geeft richting en urgentie. "Wij zien met name een duidelijke behoefte op het gebied van data science en cyber", zegt Jeroen van der Vlugt.

Wat is e-CF?

Het e-CF is een Europese standaard voor ICT-professionals. Het vakgebied ICT wordt daarbij zeer breed geïnterpreteerd. Het bestaat uit (inmiddels) 40 competentiebeschrijvingen die het vakgebied goed afdekken en gebruikt kunnen worden als 'gezamenlijke taal', om de kwaliteiten van IT'ers inzichtelijk te maken, om te bepalen wat er in de toekomst aan kwaliteiten nodig zal zijn en om te bepalen hoe medewerkers zich kunnen (door-)ontwikkelen. Het kwaliteitsraamwerk IV (Informatie Voorziening) van de Nederlandse overheid is gebaseerd op het e-CF.

Deze uitdaging vraagt om een nieuwe vorm van HR-management: 'Intelligent HR'[2]

Het is algemeen bekend dat getalenteerd personeel met kennis van de laatste (informatie)technologie voor de Defensieorganisatie, maar ook voor andere grote organisaties, een moeilijk te vullen categorie is. Gecombineerd met het gegeven dat de uitdaging van Defensie al fors zou zijn als er géén 'strijd om talent' in Nederland gaande was, mag het duidelijk zijn dat géén van de traditionele HR-instrumenten in isolement krachtig genoeg is om deze uitdaging te realiseren.

- **Werving & Selectie:** De aantrekkelijkheid van de organisatie bepaalt het succes van deze opgave, maar hoe succesvol ook: externe recruitment is slechts één pijler.
- **Leren & Ontwikkelen:** Opleiding en ontwikkeling van eigen medewerkers is een tweede pijler die vooral op middellange-termijn een bijdrage kan leveren.
- **Samenwerken met partners in een ecosysteem:** Defensie zoekt nadrukkelijk de samenwerking op met partners, om zo (op korte termijn) van de kennis en kunde van haar partners te kunnen profiteren. Een voorbeeld is het reservistenprogramma waar ook Capgemini aan meewerkt. Uit een studie van Defensie blijkt dat in de publieke context meer dan tien initiatieven zijn opgestart om in samenwerking met ecosystemen dit probleem op te lossen.

Intelligent HR is noodzakelijk voor een duurzaam medewerkersbestand

De 'strijd om talent' vraagt om een nieuwe vorm van HR-organisatie, die wij 'Intelligent HR' noemen. In Intelligent HR worden traditionele HR-instrumenten aangevuld met 1) gepersonaliseerde en gedigitaliseerde tools en processen, 2) wordt er gestuurd op continu leren, 3) is er sprake van een cultuur van transparantie en feedback en 4) draait het om toegevoegde waarde en de 'reden' van het werk dat we doen.

De eerder genoemde HR-instrumenten hebben hun waarde, maar om op de lange termijn en op een strategische manier aan het juiste medewerkersbestand te bouwen heeft Defensie meer nodig: Intelligent HR.

Een belangrijke randvoorwaarde voor een duurzaam medewerkersbestand zijn de condities waaronder de schaarse getalenteerde werknemers hun rol uitvoeren. Dat vraagt onder andere dat men bij indiensttreding goed kan acclimatiseren. De persoonlijke en 'digital touch' kan hierin op kostenefficiënte wijze het verschil maken, door middel van een goede 'employee experience' precies datgene aan de medewerker te bieden wat deze op het specifieke moment nodig heeft.

Belangrijker nog is het behouden van medewerkers door aantrekkelijk te blijven als organisatie, onder andere door het bieden van 'state of the art' kennis- en ontwikkelmogelijkheden. Defensie moet een personeelsbestand ontwikkelen dat adaptief is en zich kan aanpassen en leren door middel van een cultuur van continu leren om de snelle en voortdurend veranderende omgeving het hoofd te bieden.

Medewerkers hebben hogere verwachtingen en meer informatie en onderhandelingspositie dankzij social media en bedrijfsbeoordelingssites. Dit vereist dat organisaties hun aantrekkelijkheid als werkgever heroverwegen en versterken, met name rond een cultuur van continue feedback en transparantie.

En tot slot, wil men ook weten wáár men het voor doet: medewerkers willen deel uitmaken van organisaties met een sociaal geweten. HR moet leren hoe hierin te faciliteren, zich aan te passen aan veranderingen en te innoveren om toegevoegde waarde te blijven realiseren.

De visie en IT-strategie waar Defensie voor staat zal niet gerealiseerd worden met een traditioneel HR-instrument of binnen de silo van de IT-functie. Het aantrekken van getalenteerd personeel met kennis van de laatste (informatie)technologie is voor Defensie, maar ook voor andere grote organisaties, een moeilijke opgave. De 'strijd om talent' in Nederland is alleen maar te winnen met Intelligent HR. Het draait bij uitstek om het samenspel in de gehele organisatie: men zal de HR-organisatie moeten transformeren naar een moderne HR-organisatie die de medewerker ondersteunt in haar ontwikkeling.

Het toepassen van technologie hierbij is cruciaal, want de medewerker van morgen is per definitie een digital-savvy medewerker. Om medewerkers te behouden blijft het aanpoten: “Met het schrijven en onderhouden van een strategisch personeelsplan is de eerste stap gezet. De SPP-activiteiten moeten tot een vast onderdeel van de HR-functie gemaakt worden om continu zicht te hebben op de (impact van de) ontwikkelingen. Om de directe ambities waar te maken gaat Defensie aan de slag met een Leergang Data en het benutten van het eigen potentieel, door mensen op te leiden in 1 of 2 specifieke competenties. Op deze manier”, zegt Van der Vlugt, “brengen we technologie steeds meer als vaste waarde in, in onze functieprofielen en opleidingen.”

Grote organisaties realiseren zicht steeds meer dat de medewerker van de toekomst een ‘digital savvy’ medewerker is. De strijd om deze medewerker vraagt om het juiste strijdplan.

[1]https://www.ecompetences.eu/

[2]https://www.capgemini.com/2020/10/intelligent-hr/

Auteurs

Jeroen van der Vlugt
CIO, ministerie van Defensie

Jeroen is verantwoordelijk voor alle IT, Data en Cyber binnen het Ministerie van Defensie. Door de impact van digitalisering in de krijgsmacht wordt de slagkracht van de krijgsmacht vergroot.

Roeland de Koning
Director Public Security

roeland.de.koning@capgemini.com

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

Marjolein Wenderich
Head of People & Organization

marjolein.wenderich@capgemini.com

Marjolein is verantwoordelijk voor People & Organization van Capgemini Invent. De belangrijkste thema’s zijn onder andere Strategische Personeelsplanning, Changemanagement, (HR-) Transformaties en Reinventing Work.

Lucas Ruijs
Managing Consultant

lucas.ruijs@capgemini.com

Lucas is expert op het gebied van datagedreven HR, waaronder strategische personeelsplanning en people analytics. Hij helpt publieke en private organisaties met het opzetten, uitbouwen en optimaliseren van datagedreven HR.

De politie krijgt een nieuw wapen!

Hoe helpt de werkplek van 2025 de agent om zijn of haar taken effectief uit te voeren?

Highlights

- **Informatie is pas waardevol in de juiste context, op de juiste plek en op de juiste tijd.**
- **Een werkplek kan vele verschijningsvormen hebben, ook een AR-bril of smartwatch kan een werkplek genoemd worden.**
- **De werkplek voorziet in de 'instant gratification' van de gebruiker: nú de juiste info.**
- **De mobiele werkplek vraagt een krachtige basisinfrastructuur voor de juiste en veilige informatievoorziening.**
- **De werkplek van 2025 voldoet aan de verwachtingen van de nieuwe generatie agenten.**

In 2025 heeft elke agent een nieuw wapen in de strijd tegen de misdaad; zijn mobiele werkplek! Hiermee wordt altijd en overal veilig samenwerken de norm.

Dit wapen is niet gevaarlijk, het is namelijk een digitale mobiele werkplek waarmee de agent altijd en overal contact heeft met zijn collega's, de burger en de informatiesystemen die nodig zijn om zijn taken dírect te kunnen uitvoeren.

Het 'informatiepistool'! In 2011 al genoemd door de toenmalige CIO van de Politie[1].

Deze mobiele werkplek komt voor in verschillende vormen. Dat kan variëren van de nu al gebruikte smartphone, tablet of laptop, tot nieuwe verschijningen zoals een lichtgewicht AR-bril.

Augmented Reality (AR) betekent 'toevoegen' aan de realiteit. Met een AR-bril kan men de 'echte wereld' zien, aangevuld met digitale inhoud die aan de binnenkant van de glazen weergegeven kan worden.

Deze AR-bril projecteert pictogrammen en korte teksten met contextafhankelijke, relevante informatie. Nu al kan de politie met de smartphone kentekens en ID-bewijzen scannen, vingerafdrukken controleren en bonnen uitschrijven. Daarnaast kan een agent een veelheid aan informatiebronnen raadplegen waarmee de informatiepositie verbeterd kan worden en op basis van de beschikbare informatie kan acteren[2].

Vanaf 2025 moet het mogelijk zijn om informatiebronnen naadloos en automatisch te koppelen, zowel intern binnen de politie als extern, in de context van de locatie en de rol van de agent. Dat kan enerzijds gebeuren op initiatief van de agent, maar anderzijds ook proactief op basis van de op dat moment relevante context. Hierbij is niet alleen samenwerking met collega's op straat relevant, maar met name ook de samenwerking met collega's die zich gespecialiseerd hebben in een bepaald onderwerp. Dit maakt het mogelijk om, sneller en effectiever dan nu het geval is, relevante informatie te delen, te analyseren en daarop meteen te acteren.

De politie heeft in 2025 ruime ervaring met videovergaderen. Het is dan volkomen normaal geworden om elkaar via de smartphone even kort te videobellen om te overleggen en een probleem op te lossen. E-mail en aparte formulieren worden tegen die tijd als oud en onhandig ervaren, omdat met één geïntegreerde applicatie al die handelingen met één druk op de knop of met één stemcommando gedaan kunnen worden.

Wat is nodig voor deze nieuwe werkplek?

De nieuwe werkplek vraagt om een stabiele en veilige basis die aan de nieuwe functionele vraag kan voldoen. Dit wil zeggen dat de agent in 2025 bijna geen tijd meer kwijt is aan handelingen die te maken hebben met structuur en proces, maar alleen met het verkrijgen, verzamelen en het verwerken van de informatie om te kunnen handelen. Met de juiste expertise kan deze basisstructuur opgebouwd zijn in 2025. De werkplek is daarmee apparaat-en (interne) organisatie-agnostisch geworden, oftewel de werkplek is functioneel toegespitst naar de rol die een medewerker vervult en die past bij de persoonlijke ervaring van de medewerker met digitale omgevingen. Zo zal de werkplek voor een rechercheur anders ingericht zijn en uit andere hardware bestaan dan die van een wijkagent.

Het beheer van de werkplekken moet functioneel gestuurd zijn. De vraag wat een agent moet kunnen doen staat daarin centraal. Hoe en waarmee een agent moet kunnen werken, zijn dan de vervolgvragen. De basisstructuur zal ook zorgen voor de juiste samenstelling van expertise. Dit kan in de vorm van contacten voor directe kennisoverdracht van de ene naar de andere agent zijn, maar het kan ook meer in de vorm van contextgestuurde informatie. Dit wil zeggen dat de werkplek voldoet aan de positie van de agent in het proces, de locatie, het gedrag van de agent en de beschikbare informatie.

Persona's

Door het analyseren van beschikbare openbare bronnen is een grove indeling in vier persona's te maken, inclusief een inschatting van de percentages per persona:

Persona	Voorbeeld-functie	Percentage
Niet-mobiele kenniswerker	Data-Analist	15-25%
Mobiele kenniswerker	Forensische opsporing, rechercheurs	<10%
Mobiele taakwerker	GGP (onder andere wijkagent)	40-60%
Niet-mobiele taakwerker	Administratief medewerker	20-30%

Dit overzicht toont dat de agent vooral een mobiele taakwerker is en dat komt overeen met de huidige manier van werken. Dat zal in de nabije toekomst opschuiven in de richting van mobiele kenniswerker. De politie vergrijst in hoog tempo en moet maatregelen nemen om in de toekomst haar taken te kunnen blijven uitvoeren. Enerzijds zal het werk met minder mensen op een slimmere manier gedaan moeten worden[3] en anderzijds zal de politie aantrekkelijk moeten blijven voor jonge mensen.

Een logische stap is om deze generatie-Z (ook wel i-generatie genoemd) te faciliteren met een werkomgeving die voldoet aan het persoonlijke gedrag van deze nieuwe groep (die nu nog op de middelbare school zit). Dit betekent een veel grotere rol voor social media, gamification en het gebruik van een smartphone alsof het een nieuw aangegroeide ledemaat is. De ontwikkelingen op het gebied van netwerken zoals 5G, helpen om deze werkplek altijd en overal te kunnen inzetten.

Om de hierboven beschreven werkplek te realiseren moet de politie focus aanbrengen in haar informatievoorziening, te beginnen bij de informatielaag.

Architectuurkader

Het architectuurkader van de politie heeft historisch gezien een breed perspectief zoals architectuur voor business, informatie, applicaties en technologie. De meeste ontwikkelingen van de werkplek in 2025 zijn verplaatst naar de informatielaag. Informatie is immers de 'munitie' voor het wapen. Zonder munitie heb je niets aan het wapen en zo is het ook met de werkplek. De beschikbare informatie in de juiste context op meest geëigende manier gepresenteerd, maakt de werkplek een krachtig wapen. Op de werkplek zijn dus applicaties nodig om de informatie op een goede manier te presenteren, te verrijken, te verwerken, vast te leggen en te delen met collega's, (keten)partners en burgers.

Samenwerking is noodzakelijk

Een samenwerkingsomgeving zoals Microsoft Teams maakt het mogelijk om een veelheid aan apps en informatiebronnen samen te brengen tot het noodzakelijke aantal en op een eenvoudige manier aan de eindgebruiker te presenteren.

MS Teams is onderdeel van Microsoft 365 en biedt een breed scala aan digitale tools en services die het mogelijk maken om op een veilige manier overal en altijd met elkaar samen te werken. Het biedt onder andere opslag in de cloud voor documenten en mogelijkheden om samen aan documenten te werken in Office applicaties zoals Word en Excel. Met behulp van Microsoft Teams kunnen teams samenwerken en met elkaar communiceren in een afgeschermde en veilige omgeving en daar ook gebruik maken van de chat en videofunctionaliteit. Al deze toepassingen zijn beschikbaar op een veelheid aan apparaten.

Is het veilig?

Microsoft 365 heeft een uitgebreide gereedschapskist met beveiligingsproducten waarmee informatie versleuteld kan worden en waarmee labels voor rubricering aan een document gekoppeld kunnen worden. Dit kan ook automatisch op basis van door de organisatie vastgestelde regels. Daarnaast zijn er producten waarmee toegang gegeven kan worden op basis van verschillende criteria en waarmee apparaten beveiligd kunnen worden zodat gevoelige informatie niet in verkeerde handen kan vallen en zelfs op afstand verwijderd kan worden.

Een werkdag van de wijkagent in 2025

In 2025 zal de dag van een agent nog steeds met een briefing beginnen bij aanvang van een dienst. COVID-19 heeft ons geleerd dat het niet nodig is om met de hele ploeg fysiek bij elkaar te komen om de laatste informatie te krijgen voordat de agent de straat opgaat. Dit zal in 2025 ook nog het geval zijn. De agent kan inloggen op zijn werkplek, ongeacht waar hij zich op dat moment bevindt. Doordat de briefing standaard wordt opgenomen en meteen beschikbaar is via zijn werkplek, kan de agent ook op een later tijdstip kijken als dat nodig is. Op basis van steekwoorden of gesproken opdrachten kan de agent naar de voor hem relevante delen in de opname springen en doorklikken op de onderliggende informatiebronnen. Hij kan items markeren en alerts instellen die een signaal geven als hij bijvoorbeeld in de buurt van een locatie is die in de briefing genoemd is. De agent stapt op zijn e-bike en start de dienst met in zijn zak zijn nieuwe 'wapen'.

Tijdens zijn dienst worden kentekens automatisch[4] gescand met hulp van de kleine camera met ANPR-scanner in zijn AR-bril en licht er een symbooltje op in zijn ooghoek als daar aanleiding toe is.

Op zijn mobiel kan de agent zien welke collega's met bepaalde expertise in de buurt zijn en hen direct vragen om assistentie als dat nodig is. Bij een meer complexe casus is de agent in staat om op basis van de context meteen de juiste expertise aan te haken in de vorm van een collega die (virtueel vanaf een bureau) kan helpen of in de vorm van een kennisbank met daarin de relevante actuele informatie. Bij een staandehouding na een overtreding kan de agent met een paar keer klikken op zijn smartphone de juiste informatie opzoeken en invoeren. Dit bespaart tijd en maakt het proces eenvoudiger en betrouwbaarder omdat het dossier bijna volledig automatisch wordt gemaakt. Op een rustig moment kan de agent naadloos zijn rooster bijwerken, alvast wat overuren of vakantiedagen opnemen of simpelweg het intranet bekijken. Allemaal vanaf dezelfde werkplek, altijd en overal.

De agent in 2025 is een combinatie van een kennis- en taakwerker zowel mobiel als op het bureau. De traditionele scheiding tussen deze twee gebieden vervaagt. De agent anno 2025 moet digitaal vaardig en ook actiegericht en stressbestendig. De agent van 2025 moet in staat zijn te schakelen tussen uitvoering en analyse en tussen handelen en denken. Gelukkig wordt hij of zij daarbij ondersteund door zijn nieuwe wapen.

[1]Politie VtsPN "het tablet is ons nieuwe informatie pistool 2013 https://www.youtube.com/watch?v=8kP10QjmOss

[2]Zie bijvoorbeeld ook dit artikel uit Trends in Veiligheid 2019: Effectief informatiegestuurd werken (IGW) in een wereld met 5G-sensing - Trends in Veiligheid

[3]Zie ook dit artikel uit Trends in Veiligheid 2020: Meer misdaden oplossen met minder politiemensen - Trends in Veiligheid

[4]Tot zover dit in 2025 volgens wet- en regelgeving toegestaan is.

Auteurs

Jeroen Oosterwal
Enterprise Architect Director

jeroen.oosterwal@capgemini.com

Jeroen heeft meer dan 30 jaar ervaring als adviseur en architect in het veiligheidsdomein. Hij heeft een achtergrond in kantoorautomatisering, cloud en security. Hij is werkzaam bij de marktgroep Openbare Orde en Veiligheid binnen Capgemini Nederland.

Sjoukje Zaal
CTO Microsoft Capgemini

sjoukje.zaal@capgemini.com
https://twitter.com/SjoukjeZaal

Sjoukje Zaal is werkzaam binnen Capgemini als CTO Microsoft en heeft meer dan 20 jaar ervaring in verschillende rollen binnen het Microsoft-domein. Daarnaast is zij Microsoft RD & Azure MVP en deelt zij haar kennis binnen de Microsoft community.

Jan Zonnenberg
Transformation Director

jan.zonnenberg@capgemini.com

Jan Zonnenberg heeft meer dan 25 jaar ervaring in het veranderen en toepassen van werkwijzen en – middelen ten behoeve van effectief samenwerken. Hij is werkzaam bij de marktgroep Openbare Orde en Veiligheid binnen Capgemini Nederland.

Innoveren met impact: succesvol opschalen van innovaties

Wat zijn de valkuilen voor het opschalen van innovatie en wat kan de overheid eraan doen om dit te overwinnen?

Highlights

- De taak die de innovatie vervult voor de gebruiker moet centraal staan in het innovatietraject.
- Samenwerking over departementen heen is vaak nodig voor het succesvol implementeren van innovatie.
- Het opschalen van innovatie is van groot belang voor het continue aanpassingsvermogen van organisaties en overheden.
- Daarom moet opschalen als apart aandachtspunt worden behandeld in het innovatietraject.

Innovaties zijn pas waardevol als ze opgeschaald zijn. Echter, het opschalen van innovaties blijkt voor organisaties en overheden een grote uitdaging te zijn. Een juiste aanpak faciliteert het opschalen van innovatie en het maximaal benutten van de innovatiepotentie.

Er worden miljoenen geïnvesteerd door organisaties en overheden in innovatie om in te spelen op de veranderende behoeften van burgers en de nieuwe mogelijkheden van technologie. De COVID-19-pandemie heeft daarbij een aantal ontwikkelingen nog eens versneld. Bovendien laat de pandemie zien dat technologie het mogelijk maakt om werk en wonen op een andere manier in te richten, wat weer een stroom aan innovaties en veranderingen met zich mee zal brengen.

Hoewel ideeën steeds sneller kunnen worden omgezet in innovaties, blijkt het voor veel organisaties moeilijk om die innovaties in de organisatie te implementeren en op te schalen, waardoor het potentieel niet volledig wordt gerealiseerd[1]. De implementatie van innovaties vraagt steeds vaker om samenwerking over organisatieonderdelen of zelfs organisaties heen. Iets waar veel organisaties problemen mee hebben. Succesvol opschalen vraagt om de vaardigheid op een resource-efficiënte manier een innovatie snel op grote schaal uit te rollen zonder dat de kwaliteitsdoelen in het geding komen[2]. Daarbij geldt dat de technologie vaak wel op kan schalen, maar dat de organisatieveranderingen die nodig zijn om de innovatie te ondersteunen, zoals het afbouwen van de oude competenties en het opbouwen van nieuwe competenties, vaak een barrière vormen. Er zijn grote verschillen tussen organisaties in de mate van succes van opschalen. Er zijn organisaties waarbij 1 op de 10 innovaties succesvol opgeschaald wordt en er zijn organisaties die meer dan 85% succes hebben met het opschalen van innovaties[3]. Wat zijn de grote uitdagingen bij opschaling en wat is de succesformule?

Van product-focus naar taak-focus

Als een innovatief idee of product wordt uitgewerkt en uitgerold is de focus vaak op het verbeteren van het product of idee. Echter, innovaties creëren geen waarde door de innovatie zelf, maar door de taak die de innovatie voor de gebruiker vervult. Dit is wat Harvard-professor Clayton Christensen in zijn boek The Innovators Solution (2003) noemt de "job-to-be-done"-lens. Door het perspectief te verplaatsen van product naar functionaliteit kunnen organisaties aan het begin van het innovatietraject al stilstaan bij welke oplossing de innovatie biedt voor de gebruiker. Dit leidt ertoe dat innovators een initiële innovatie op de markt brengen die beter aansluit bij waar gebruikers waarde aan hechten om zodoende hun behoeften te vervullen.

Een taakgerichte lens in innovatie is niet nieuw. Echter, in de enorme vaart waarin verandering vandaag de dag plaats vindt, is deze lens vertroebeld. Dat dit niet nieuw is, bewijst de bekende quote van Henry Ford; "If I had asked people what they wanted they would have said: faster horses". In plaats daarvan dacht Ford na over wáárom mensen dit wilden. De taak die de consument vervuld wilde zien, was het sneller kunnen verplaatsen van A naar B. Het ging dus niet over het 'product' (het paard), maar over 'de taak' die het product vervulde (snel verplaatsen van A naar B). Door deze verandering van perspectief was Henry Ford in staat de innovatie optimaal af te stemmen op de behoefte van de klant en werd het Ford Model T als een van de eerste auto's in massaproductie genomen.

Het voorbeeld laat zien dat het belang van innovatie zit in de focus op de klantbehoeften. Een succesvolle innovatie speelt in op de klantbehoefte door op een verbeterde of nieuwe manier beter de klantbehoefte te vervullen. Bijvoorbeeld door een nieuwe technologie in te zetten die ervoor niet beschikbaar was, zoals in het geval van Ford. Daarbij geldt dat de bestaande organisaties tot dat moment vormgegeven zijn op basis van de oude technologie, en dat door de nieuwe technologie wellicht nieuwe organisaties nodig zijn. Om bij het voorbeeld van Ford te blijven: de introductie van de automobiel zal de vraag naar hoefsmeden verminderd hebben, maar de vraag naar tankstations vergroot. Eenzelfde effect is zichtbaar in het veiligheidsdomein. Als we veel veiligheidscamera's ophangen, kunnen we een betere veiligheid op straat creëren met minder blauw op straat. Dat betekent voor de organisatie dan wel dat er minder agenten nodig zijn, maar meer IT-experts om ervoor te zorgen dat de beelden op de juiste wijze geïnterpreteerd worden en dat aan alle privacy-voorwaarden voldaan wordt.

Dit maakt ook gelijk duidelijk waarom het invoeren en opschalen van innovaties vaak moeilijk is. Stelt u zich het volgende voor. Er wordt een pilot uitgevoerd waarin de software heeft laten zien dat het mogelijk is om met 5 camera's op het Leidseplein 24/7 toezicht te houden en dat er automatisch gesignaleerd wordt als er iets aan de hand is. Dat betekent dat de technologie feilloos werkt. Dan betekent implementatie en opschaling van deze innovatie dat de politie haar bezetting zal moeten wijzigen door agenten om te scholen naar data-analisten. Als op voorhand al duidelijk is dat dit niet gaat gebeuren, hoeft men eigenlijk ook de pilot met de technologie niet te doen. Organisaties die goed zijn in implementatie en opschaling vertalen daarom al vanaf het begin de implicaties van de innovatie door naar de effecten op de gehele organisatie en begrijpen dat als de benodigde organisatieveranderingen niet gerealiseerd kunnen worden, de innovatie ook niet succesvol kan worden.

Cross-departementaal organiseren van innovatie

Veel teams zien het opschalen van innovatie als losstaande stap in het innovatietraject. Na het bedenken en uitwerken van innovatie wordt pas nagedacht over het opschalen ervan. Echter, het is van belang om eerder in het proces over het opschalen van de innovatie na te denken vanwege de grote uitdagingen die het vaak met zich meebrengt.

Een belangrijk probleem bij het opschalen is de samenwerking tussen verschillende departementen. Traditionele organisaties en overheidsorganen zijn vaak departementaal georganiseerd en voor het succesvol opschalen van innovatie zijn vaak meerdere departementen nodig. Een complicatie die we vaak zien is dat innovaties die over verschillende afdelingen gaan, de kosten op de ene plek vallen terwijl de baten voor een andere afdeling zijn. Dit zorgt voor scheve verhoudingen en bemoeilijkt de samenwerking omdat afdelingen verschillende belangen hebben bij dezelfde innovatie. Dit zorgt ervoor dat verschillende afdelingen niet schouder aan schouder naar hetzelfde doel toewerken en elkaar versterken, maar dat er verschillende richtingen gekozen en inspanningen vertoond worden waardoor de innovatie niet het gewenste effect bereikt. Een voorbeeld is het opschalen van Smart Traffic oplossingen: voor het ministerie van Infrastructuur en Waterstaat een manier om mobiliteit te verduurzamen, maar voor het ministerie van Justitie en Veiligheid brengt het grote veiligheids- en cybersecurity-vraagstukken met zich mee. Namelijk, zorgen de systemen wel voor meer verkeersveiligheid? Zijn privacy en bescherming van persoonsgegevens wel voldoende gewaarborgd? Om ervoor te zorgen dat beide belangen worden meegewogen in de ontwerp-en uitvoeringsfase is het van belang de innovatie cross-departementaal te organiseren. Dit zorgt ervoor dat de innovatie aansluit bij de belangen van verschillende departementen en deze elkaar versterken in de opschalingsfase.

Om innovatie succesvol op te schalen is het dus belangrijk dat partijen hun krachten bundelen en gezamenlijk werken aan het opschalen van innovatie. Essentieel hiervoor is het ontwikkelen van een sterke visie en het formuleren van een gemeenschappelijke innovatiestrategie met gezamenlijke doelen. Dit zorgt ervoor dat de expertise van verschillende afdelingen een versterkend effect op elkaar heeft waardoor het opschalen van innovatie kan worden versneld.

De Japanse Society 5.0-visie is hier een succesvol voorbeeld van. Door het integreren van innovaties in elke sector en sociaal domein streeft men ernaar sociale problemen aan te pakken en evenwicht te brengen in de maatschappij[4]. De visie is krachtig en wordt nagestreefd. Zo is het in 2017 verwerkt in het Charter of Corporate Behavior[5] en worden bedrijven opgeroepen proactief bij te dragen aan de Sustainable Development Goals door de realisatie van Society 5.0[6]. Deze eenduidige strategie zorgt voor een gezamenlijk belang van publieke en private partijen waardoor elkaars inspanningen versterkt worden.

Naast een sterke gemeenschappelijke innovatievisie heeft het rapport genaamd 'Scaling Innovation' van het Capgemini Research Institute laten zien dat het van belang is opschalen als een aparte discipline te behandelen in het innovatieproces met daaraan concreet gekoppelde opschalingsdoelstellingen. Vaak wordt over het opschalen van innovatie pas nagedacht na een proof of concept. Voor het opschalen van innovatie zijn echter andere uitdagingen aan de orde, zoals het creëren van netwerkeffecten, dan voor het uitwerken van ideeën. Een team met leden van de betrokken afdelingen aanwijzen als verantwoordelijke voor het opschalen van nieuwe ideeën zorgt ervoor dat al in de beginfase van innovatie rekening wordt gehouden met de voorwaarden voor het succesvol bereiken van schaal. Door de vertegenwoordiging uit de betrokken afdelingen worden hier de belangen van individuele afdelingen vroeg in het proces meegenomen waardoor succesvolle ideeën eenvoudiger en sneller kunnen worden opgeschaald.

Conclusie

Het opschalen van innovatie is belangrijk voor organisaties en overheidsorganen om zich niet alleen snel aan te kunnen passen, maar ook voor het zijn van de architect van de toekomst. Echter, het opschalen van innovatie is een grote uitdaging waardoor de potentie van innovatieve ideeën vaak onbenut blijft. Om ideeën succesvol op te schalen is het van belang de focus van innovatie te verleggen van productgericht naar taakgericht om zodoende de innovatie aan te laten sluiten op de onderliggende behoefte van de gebruiker. Een gestructureerde samenwerking over departementen heen met daarin gezamenlijke doelen en een aparte discipline voor het schalen van innovatie zijn daarnaast van belang om het schalen van innovaties al in een vroeg stadium te behandelen.

Een taakgerichte focus en cross-departementale samenwerking met een duidelijke innovatievisie helpen Nederland om innovatieve ideeën op te schalen tot impactvolle innovaties en hiermee richting te geven aan de toekomst.

[1]Capgemini Research Institute, 2020. What's the Big Idea? Why most innovations fail to scale and what to do about it

[2]Dudnik, N. 2020. Social Entrepreneurs' Tricky Issues of Sustainability and Scale. *Harvard Business Review.*

[3]https://strategyn.com/our-results/

[4]Capgemini Invent, 2020. Rapport Smart Cities in de G40: Overzicht versnellers en knelpunten en advies

[5]Keidanren Japan Business Federation, 2017. Charter of Corporate Behavior

[6]Capgemini Invent, 2021, Society 5.0: Naar een Superslimme Samenleving?

[7]Capgemini Research Institute, 2020, What's the Big Idea: Why most innovations fail to scale and what to do about it

Auteurs

Guus Kok
Consultant Innovation & Strategy

guus.kok@capgemini.com

Guus is werkzaam voor Capgemini Invent op het gebied innovatiemanagement en het ontwikkelen en opschalen van nieuwe businessmodellen

Han Gerrits
Vice President, Head of Innovation & Strategy

https://twitter.com/hangerrits

Han werkte ten tijde van schrijven voor de innovatie-en strategie-consultancy van Capgemini Invent en is hoogleraar aan de Vrije Universiteit Amsterdam. Zijn interesse is het verbeteren van organisaties met nieuwe technologie.

Cybercriminaliteit dwingt de politieorganisatie tot verandering

Hoe dient de politie zich te organiseren om adequaat cybercriminaliteit aan te pakken?

Highlights

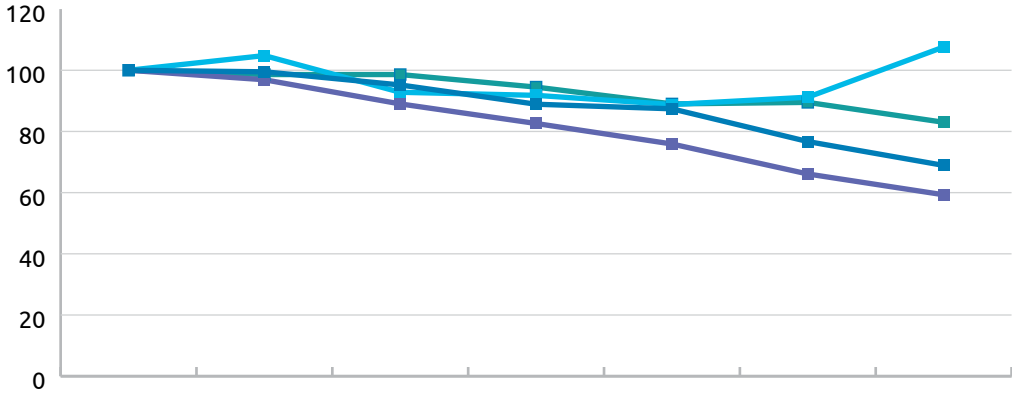
- **Cybercriminaliteit is dynamisch, grenzeloos en uiterst effectief.**
- **Sinds de COVID-19-pandemie is cybercriminaliteit flink toegenomen.**
- **Samen proactief handelen via preventie en disruptie is noodzakelijk.**
- **Data-gedreven werken en digitale kennis en kunde eisen meer aandacht.**
- **De politie moet van cybercrime de topprioriteit maken.**

Cybercrime maakt een opmars en is dermate uniek dat het de politie voor een grote veranderopgave stelt om deze vorm van criminaliteit effectief te bestrijden.

Cybercriminaliteit is een relatief nieuwe vorm van criminaliteit die uit de schaduw komt van de digitalisering van onze samenleving. Cybercrime (of cybercriminaliteit) wordt gedefinieerd als een misdaad die gepleegd is met ICT, gericht op ICT[1]. Bekende voorbeelden zijn hackingactiviteiten, DDoS-aanvallen (zogenaamde gedistribueerde netwerkaanvallen) en het gebruiken van ransom- en malware. Daarnaast ziet men ook steeds meer gedigitaliseerde criminaliteit voorbijkomen. Dit zijn klassieke delicten die online gepleegd worden, denk aan internetoplichting, online afpersing of phishing activiteiten.

Vanaf 2013 is een duidelijke groei te zien in het aantal geregistreerde incidenten van cybercrime, in tegenstelling tot andere vormen criminaliteit. Daarnaast zijn er meerdere indicatoren die aangeven dat het aantal incidenten sterk is toegenomen tijdens de COVID-19-crisis. Zo gaven de cijfers van mei 2020 aan dat er een toename van 383% was ten opzichte van mei 2019 in het aantal cybercrime-incidenten[2]. Daarmee had Nederland de primeur te pakken dat er meer cybercrime-delicten geregistreerd waren dan woninginbraken[3].

Figuur 1: Slachtoffers cybercrime in Nederland in vergelijking met andere criminaliteit.



Slachtoffers Cybercrime	2012	2013	2014	2015	2016	2017	2019*
Slachtoffers traditionele criminaliteit1) (2012 = 100)2	100	99.5	95.2	88.9	87.4	76.7	68.9
Geregistreerde misdrijven (politie) (2012 = 100)	100	96.9	89	82.6	75.9	66.1	59.3
Slachtoffers cybercrime) (2012 = 100)	100	104.8	92.8	91.8	88.8	91.2	107.6
Meldingsbereidheid slachtoffers traditionele criminaliteit) (2012 = 100)	100	98.6	98.6	94.5	89	89.5	83

* In 2018 heeft er geen meting plaatsgevonden en de cijfers van 2019 zijn nog voorlopig

Bron: CBS: Minder traditionele criminaliteit, meer cybercriminaliteit: https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime

Het uitdagende karakter van cybercriminaliteit

Dat cybercriminaliteit een bijzondere vorm van criminaliteit is, heeft niet alleen te maken met het feit dat het een technologisch en digitale component heeft. Het heeft ook te maken met de unieke kenmerken van dit type criminaliteit. Cybercriminaliteit is:

1. **Dynamisch.** In een rap tempo volgen de verschillende technologische ontwikkelingen en trends elkaar op. De modus operandi van cybercriminelen verandert voortdurend.
2. **Effectief.** Daders kunnen met één druk op de knop heel veel slachtoffers maken.
3. **Onopgemerkt.** Impact is soms niet direct zichtbaar waardoor slachtoffers niet door hebben dat ze gehackt zijn.
4. **Grenzeloos.** Een dader kan een computerinbraak uitvoeren vanaf elke plek in de wereld door toegang proberen te krijgen via verschillende methodes. Zo zie je steeds vaker dat er gerichte DDoS-aanvallen of hacks plaatsvinden bij Nederlandse bedrijven door daders die ergens anders in de wereld 'lijken' te zitten.
5. **Niet gebonden aan een duidelijk daderprofiel.** De huidige ervaring leert dat er geen sprake is van een homogene groep daders[4]. Onderzoek toont aan dat er relatief veel variatie in zit in de factoren en drijfveren voor cyberdaders om over te gaan op deze vorm van criminaliteit ten opzichte van andere vormen van criminaliteit.

De organisatorische impact van cybercrime op de politie

Het feit dat cybercriminaliteit deze unieke kenmerken heeft maakt dat het van de politie een andere aanpak eist. Cybercriminaliteit forceert de volgende bewegingen:

1. **Van opsporen en vervolgen naar preventie en disruptie**

   Hoe pak je criminaliteit aan die digitaal, snel, behendig, dynamisch en uiterst effectief is? De focus bij het bestrijden van cybercriminaliteit moet komen te liggen op het uitvoeren van preventie en disruptie (verstoren) van criminele activiteiten.

   De beweging naar meer preventie en disruptie dwingt de politie om van een reactieve organisatie naar een proactieve organisatie te gaan. Om een effectieve organisatie te zijn die aan gedegen preventie en disruptie doet, moet men in zoverre weten wat er speelt in de digitale wereld dat het de aangiftes voor kan zijn. Dit betekent dat cybercrimeteams dienen te investeren in een krachtig in- en extern netwerk, nauw moeten gaan samenwerken binnen de politie en met het OM alsook private (internationale) partijen. Gebaseerd op wederzijds vertrouwen en een collectief belang. Daarbij moeten de cybercrime-teams de juiste voelsprieten ontwikkelen om te weten wat er speelt in de digitale samenleving en hoe daar potentieel misbruik van gemaakt kan worden. Dit betekent dus niet alleen het investeren in een goede informatiepositie, maar ook een goed inlevend vermogen om te kunnen voorspellen wat de volgende stap is van een cybercrimineel. Met die inzichten kan er snel gehandeld worden om interventies op het vlak van preventie en disruptie in te zetten.

2. **The science is in the data: meer informatie-gestuurd en data-gedreven werken**

   De politie heeft echter niet genoeg aan een krachtig netwerk van belanghebbenden, ze moeten ook actief aan de slag met de (big) data die ze tot hun beschikking hebben. Het opbouwen van een betere intelligence positie en het datagestuurd werken is een kernvoorwaarde om de beweging naar preventie en disruptie te kunnen faciliteren.

   In 2025 zal er in de wereld 175 zetabytes (1 zetabyte staat gelijk aan 10.000 terabytes) aan data te vinden zijn[5]. De crux voor elke organisatie zit hem in het verzamelen van gegevens, het betekenis geven aan deze informatie, de informatie te combineren, in context te plaatsen en aan eerdere ervaringen te koppelen[6]. Op deze manier bouw je aan waardevolle informatieproducten voor de organisatie. Dit betekent een grote verandering in de opsporing. Waar vroeger werd geleund op de expertise van de tactische opsporing en later ook de forensische tak, zal data en informatie nu de hoofdtak worden waar keuzes in de operatie en opsporing gemaakt zullen worden. Opsporing en intelligence zullen steeds meer met elkaar samen moeten gaan werken.

   Omgaan met deze trend en het ontwikkelen van deze capaciteit vergt grootschalige veranderingen in de organisatie[7]. Naast de vraagstukken rondom privacy, ethiek en juridische elementen die beantwoordt moeten worden, moet de politie ook beschikken over de vaardigheid om goede datakwaliteit te waarborgen en om vaker nieuwe databronnen te delen of raadplegen. Alleen dan kan de stap gemaakt worden van inzicht naar vooruitzicht en ontstaan de juiste voorwaarden om aan gedegen preventie en disruptie te doen.

3. **Verandering in de gevraagde kennis en kunde van de medewerkers door de gehele organisatie.**

   Digitalisering heeft impact op alle aspecten binnen de politie. Van het bewaken van de veiligheid, het in verbinding zijn met de wijk en maatschappij en het bestrijden van misdaad tot het handhaven van de orde. Digitale kennis, vaardigheden en een algemeen begrip van digitalisering is nodig voor iedereen in de organisatie. Iedere politiemedewerker zou in de basis digitaal bewust en in zekere mate digitaal vaardig moeten zijn[8].

   Voor de politie betekent dit bijvoorbeeld dat elke medewerker snapt hoe de verschillende systemen en applicaties (van Outlook tot BOSZ) werken, iemand die een aangifte opneemt begrijpt wat een DDOS-aanval in de basis inhoudt en dat het ophalen van het IP-adres en het IMEI-nummer van belang is voor het toekomstig onderzoek en dat de wijkagent snapt dat er voor jongeren ook een digitale wijk of wereld is via de games die ze spelen of de apps waar zij op zitten.

   In het geval van cybercrime gaat dit nog een stapje verder, hier is namelijk specifieke kennis en kunde nodig om de verschillende fenomenen, nieuwe aanpakken en methodes te begrijpen die komen kijken bij deze vorm van criminaliteit. Zo moet er een goed begrip zijn van de verschillende vormen van cybercriminaliteit en de impact hiervan. Je moet bij een phishingzaak namelijk op andere dingen letten dan bij een fysieke fraudezaak en een goede inschatting kunnen maken van de ernst van de situatie en de opsporingsindicaties. Daarnaast zijn er ook gehele nieuwe procedures zoals het verstoren van cybercriminelen online, die een nieuwe set aan specialistische kennis en kunde vragen.

Zes kernvoorwaarden voor de politie om succesvol cybercrime te bestrijden

Door de explosieve toename (mede door COVD-19) van cybercriminaliteit en gedigitaliseerde criminaliteit dreigt de politie achter te gaan lopen ten opzichte van de cybercriminelen.

Er is een grote verander- en transformatie-opgave ontstaan om in te spelen op al deze ontwikkelingen. De snelheid van de ontwikkelingen staan consensusvorming, polderen en het afwegen van prioriteiten niet toe. Als de politie niet nu sneller in beweging komt en van cybercrime de topprioriteit maakt, zal het te laat zijn om haar legitimiteit te bestendigen en veiligheid te bieden in het digitale domein van onze samenleving.

Om toekomstbestendig te zijn moet de politie inspelen op de trends en meebewegen met de digitale ontwikkelingen. Hiervoor stellen we 6 kernvoorwaarden voor succes:

1. Het is essentieel dat het opsporen, vervolgen, voorkomen en verstoren van cybercriminaliteit een volwaardige plek krijgt binnen de politieorganisatie. Niet als een bijzondere tak die ‘anders’ is dan de andere activiteiten binnen de politie. Cybercriminaliteit is de snelst groeiende criminaliteit en zou als ‘core business’ moeten worden gezien, zowel binnen als buiten de politie.

2. Investeer grootschalig in het verzamelen, analyseren en gebruik van kwalitatieve (big) data en intelligence over de gehele organisatie om door middel van preventie en disruptie een duurzame impact te maken op cybercriminaliteit.

3. Ontwikkel de algemene digitale vaardigheden en het digitale bewustzijn van alle medewerkers. Basisteams moeten kundig genoeg zijn om gedigitaliseerde criminaliteit op te kunnen pakken. Daarnaast moet er in de huidige cybercrime-teams geïnvesteerd worden in het specialiseren en ontwikkelen van de huidige medewerkers en het aantrekken van nieuw IT-talent.

4. Bouw aan duurzame relaties, partnerschappen en een werkend netwerk om de politieorganisatie te voeden en ervoor te zorgen dat preventie aansluit en landt.

5. Werk op een integrale wijze, zowel binnen als buiten de eenheid. Verschillende teams in verschillende eenheden moeten elkaar kunnen vinden en van elkaar leren. Cybercriminelen houden zich niet aan regiogrenzen, voor effectieve opsporing, vervolging, preventie en disruptie activiteiten moeten deze grenzen binnen de politie ook gaan vervagen.

6. Draag het geloof breed uit in de cultuur van de politie dat andersoortige interventies en duurzame publiek-private samenwerkingen de norm zullen zijn in plaats van 'het vangen van de boef'. Het is essentieel dat de medewerkers in gaan zien dat deze interventies noodzakelijk zijn om impact te kunnen maken op deze ingewikkelde en gehaaide vorm van criminaliteit.

[1]Cybercrime | politie.nl (2021). Geraadpleegd van: https://www.politie.nl/themas/cybercrime.html

[2]Schurer, E. (2020, 9 december). Explosieve stijging cybercrime in eerste helft 2020. Geraadpleegd van: https://www.vpngids.nl/veilig-internet/cybercrime/cybercrime-statistieken-nederland/

[3]Schurer, E. (2020, 9 december). Explosieve stijging cybercrime in eerste helft 2020. Geraadpleegd van: https://www.vpngids.nl/veilig-internet/cybercrime/cybercrime-statistieken-nederland/

[4]Van der Wagen, van 't Zand-Kurtovic, Matthijsse, Fischer. (2019). Cyberdaders, uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin. WODC, Ministerie van Justitie en Veiligheid, December 2019

[5]Datacenterworks. (2019, 19 september). Hoe managen we de almaar groeiende hoeveelheid data? Geraadpleegd van: https://datacenterworks.nl/artikelen/hoe-managen-we-de-almaar-groeiende-hoeveelheid-data

[6]Den Hengst, ten Brink & Ter Mors. (2017). Informatiegestuurd politiewerk in de praktijk. Politieacademie, 2019.

[7]Den Hengst, ten Brink & Ter Mors. (2017). Informatiegestuurd politiewerk in de praktijk. Politieacademie, 2019.

[8]Politie Onderwijsraad. (2020). Let's get digital! Een solide basis voor een digitaalvaardige politie. Politie Onderwijsraad, December 2020.

Auteurs

Harm van der Wal
Consultant

harm.vander.wal@capgemini.com

Harm is werkzaam bij Capgemini Invent. Hij begeleidt en ondersteunt organisaties om de volgende stap te maken, vanuit inzicht en structuur. Dit doet hij met name in het veiligheidsdomein.

Tessa Rammers
Managing Consultant

tessa.rammers@capgemini.com

Tessa is werkzaam bij Capgemini Invent. Zij is gespecialiseerd in het opzetten en managen van (complexe) verandertrajecten in het publieke domein. Ze focust hierbij op het adviseren in en begeleiden van leiderschap, gedragsverandering en teamontwikkeling.

Ketensamen-werking zonder gegevens te hoeven delen

Hoe wordt het mogelijk om binnen het publieke veiligheidsdomein informatie uit te wisselen zonder dat er gevoelige gegevens gedeeld en/of gerepliceerd hoeven te worden?

Highlights

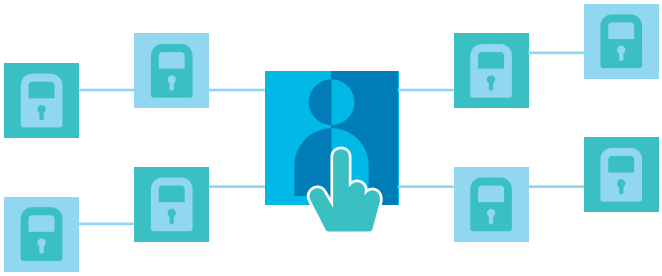
- Privacy en rubricering zorgen voor veel uitdagingen.
- Gegevensdeling kan plaatsvinden zonder beschermde informatie te verstrekken.
- Er zijn geen veiligheidsverplichtingen of -risico's voor data die er niet is.
- Zero-Knowledge Proof cryptografie is een gamechanger voor het veiligheidsdomein.
- Informatie gestuurd werken moet efficiëntie en veiligheid verhogen.

Binnen het openbare orde- en veiligheidsdomein is gegevensdeling belangrijk, maar ook gevaarlijk en lastig. Nieuwe technologie kan het verschil gaan maken.

Oude problematiek, nieuwe oplossingen

Sinds de invoering in 2018 komt iedere organisatie in Nederland in aanraking met de AVG. Al deze organisaties moeten hun systemen daarop inrichten. In het veiligheidsdomein is er nog een belangrijke schat aan kennis die in het belang van de hele samenleving bescherming verdient: gerubriceerde informatie.

Het is soms lastig of zelfs onmogelijk om binnen het publieke veiligheidsdomein informatie uit te wisselen. Deze informatie komt uit verschillende bronnen van verschillende organisaties en/of ketenpartners. Het overtreden van de privacyregels of niet kunnen communiceren door ongelijke rubriceringsniveaus zijn problemen. Een gevolg daarvan is dat het verstrekken van te veel aan informatie de organisatie of een onderzoek kan schaden, terwijl het verstrekken van te weinig informatie een remmende zo niet destructieve werking heeft.



Keteninteracties zonder gegevens te onthullen

De huidige werkelijkheid dwingt organisaties om verder vooruit te kijken. Want als data voor eeuwig is, dan geldt dat ook voor gegevens die lekken of gestolen worden. Als data eenmaal uit de fles is, krijg je het niet meer terug in de fles. Zeker in het veiligheidsdomein kan de schade tot en met het strategische niveau in de organisatie, maar ook aan individuen, substantieel zijn. Een ander aspect bij gegevensuitwisseling is het belang van de garantie van integriteit, de veiligheid en bovenal de betrouwbaarheid. Traditionele integratietechnologieën zoals een Enterprise Service Bus (ESB) of een Service Oriented Architecture (SOA) spelen hier een cruciale rol. De gebruikte technologie kan om aan de moderne maatstaven te voldoen niet de gewenste integratie-oplossing bieden zonder het zeer complex en tijdrovend te maken. Huidige architecturen zijn met name gebaseerd op intensief maatwerk waarbij de veiligheid geborgd wordt door autorisaties voor de gebruikers en beveiligingseisen voor de gegevensdragers.

Het introduceren van een nieuwe innovatieve technologie zoals het gebruik van cryptografie, kan daarbij een oplossing bieden. Een speciaal type cryptografie dat door de opkomst van blockchaintechnologie nu volwassen aan het worden is, is Zero-Knowledge Proof cryptografie. Deze vorm van cryptografie wordt voornamelijk ingezet als manier om privacy te waarborgen, terwijl de correctheid van de transactie nog altijd geverifieerd kan worden. Zo zouden bijvoorbeeld kernregisterbevragingen in ketens op basis van cryptografische bewijzen met elkaar kunnen (gaan) interacteren.

Deze technologie heeft inmiddels zijn intrede gedaan binnen de financiële wereld[1] en zou ook een rol kunnen spelen binnen het veiligheidsdomein.

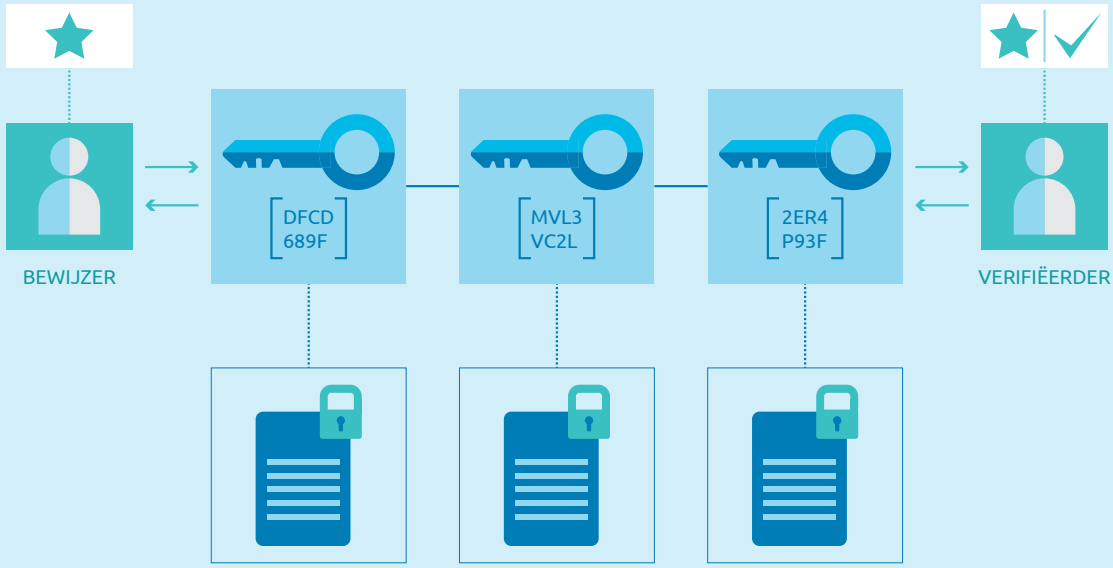
Wat is Zero-Knowledge Proof cryptografie?

Bij cryptografie is een Zero-knowledge Proof of Zero-Knowledge Proof Protocol een methode waarmee een partij aan een andere partij kan bewijzen dat ze een waarde x kennen, zonder enige informatie over te brengen, afgezien van het feit dat ze de waarde x kennen. Partijen kunnen op deze manier via een aantal interacties vaststellen of een bepaald gegeven bekend is, zonder enige informatie over dit gegeven prijs te geven.

Onderliggend aan deze cryptografie zijn een aantal wiskundige principes waarmee het triviaal is om een bewijs te genereren en te verifiëren over het kennen van waarde x, maar waarbij het onmogelijk is om te herleiden wat waarde x is.

Formeel dient een Zero-Knowledge Proof de volgende 3 eigenschappen te hebben:

1. Compleetheid: als de bewering waar is, zal een eerlijke verifiëerder (i.e. het protocol op juiste wijze volgend) overtuigd zijn van dit feit door een eerlijke bewijzer.
2. Robuustheid: Als de bewering onwaar/onjuist is, kan een valsspelende bewijzer de eerlijke verifiëerder niet overtuigen dat het waar is.
3. Zero-Knowledge/nulkennis: Als de bewering waar is, zal een verifiëerder niets anders te weten komen behalve het feit dat de bewering waar is.



BEWIJZEN EN GEHEIME DATA

Een gecompliceerd probleem eenvoudig oplossen

Een technologie waarvan de basis zo simpel is, zou bij kunnen dragen aan een systeem wat zeer ingewikkeld is. In de huidige situatie kennen we vele vormen van rubricering, van nationaal tot NAVO en EU gerubriceerd, met ieder weer eigen gradaties. Toegang tot gegevens gaat op basis van het verstrekken van autorisaties. Dit is een tijdrovend proces waarbij de procedure voor veiligheid moet zorgen. Overdracht van gegevens met rubricering van het ene naar het andere systeem gaat in veel gevallen moeizaam (handmatig) of helemaal niet. Daarnaast geldt voor gerubriceerde informatie die niet in systemen zitten, maar in documenten staan, dat het gevaar altijd op de loer ligt dat de verwerking onveilig gaat (via open mail, telefoon of papier).

Zero-Knowledge Proof cryptografie wordt gezien als één van de belangrijkste ontwikkelingen op het gebied van privacy-enhancing computation[2]. Oplossingen op basis van Zero-Knowledge Proof cryptografie kunnen het oerwoud aan autorisaties overbodig maken en tegelijkertijd de veiligheid verhogen. Vaak is het doel van de overdracht van privacygevoelige of gerubriceerde informatie namelijk helemaal niet om het volledige pakket informatie over te dragen, maar is het slechts nodig om aan te geven of iets klopt of niet klopt. Dat bewijs kan Zero-Knowledge Proof cryptografie leveren.

Waar staat de technologie nu

Capgemini heeft binnen het Applied Innovation Exchange (AIE) een oplossing ontwikkeld waarbij bewijsbare interacties tussen partijen op basis van gegevens worden uitgevoerd, zonder dat er nog gevoelige gegevens gedeeld en/of gerepliceerd worden. Hierbij is het aanmeldproces voor een huurwoning, waar normaliter persoonsgegevens en financiële gegevens gedeeld worden, teruggebracht naar een minimale set van (cryptografische) interacties tussen de betrokken partijen. Er zijn een aantal specifieke API's ontwikkeld die cryptografische bewijzen genereren en verifiëren. Omlijst met een aantal aanvullende technieken, zoals het digitaal ondertekenen van bewijzen en een rule-management systeem om misbruik en overbevraging te voorkomen, biedt de oplossing veilige en betrouwbare gegevensinteractie met slechts een aantal simpele 'API-interacties' tussen bronsystemen. Dit proof-of-concept toont aan dat het met inzet van deze technologie mogelijk is om een sterke reductie van fraudeoppervlakken, privacyrisico's en beveiligingsrisico's in keteninteracties te bewerkstelligen. In de AIE wordt nu gewerkt aan use-cases in het veiligheidsdomein.

Binnen het veiligheidsdomein biedt Zero-Knowledge Proof cryptografie verschillende mogelijkheden om organisaties te ondersteunen in beveiligingsbehoeften en te ontlasten van het beheer van gevoelige gegevens.

Een concreet voorbeeld is bijvoorbeeld het MIT (Multi-disciplinair Interventie Team), een recent opgestart samenwerkingsverband tussen Politie, Koninklijke Marechaussee, Openbaar Ministerie, FIOD, belastingdienst en de douane, waarbij de betrokken organisaties een gezamenlijke informatiepositie opbouwen ten behoeve van effectiever interveniëren op veiligheidsthema's. Het inzetten van Zero-Knowledge proof cryptografie kan de informatiepositie van het MIT verrijken, doordat gegevens geïntegreerd kunnen worden die anders niet gebruikt kunnen en/of mogen worden. Dit zou een directe impact kunnen hebben op de effectiviteit en slagvaardigheid van dit samenwerkingsverband.

Een ander voorbeeld zijn samenwerkingsovereenkomsten rondom terrorismebestrijding, zoals het CTI (Contra-Terrorisme Informatie). Hierbij zijn onder andere Defensie, de belastingdienst, de AIVD, de KMar, de FIOD en ISZW betrokken. Bij dit type informatieuitwisseling zijn de gegevens dermate geheim, dat samenwerking ernstig bemoeilijkt wordt. Als een van de betrokken partijen namelijk gegevens over iemand wil opzoeken, moet voorkomen worden dat andere partijen weten dat er mogelijk een onderzoek naar deze persoon loopt en eigen stappen gaan ondernemen (waardoor het initiële onderzoek gehinderd zou kunnen worden). In dit geval lekt er al informatie op het moment dat er gegevens over iemand worden opgevraagd. Het toont namelijk dat er interesse is naar deze persoon in de context van terrorismebestrijding. Deze bevragingen kunnen 'ingepakt' en gemaskeerd worden met Zero-Knowledge Proof cryptografie. Het komt ook voor dat een van de partijen bepaalde gegevens heeft, maar niet bevoegd is om te handelen. Zero-Knowledge Proof cryptografie kan ook hier een rol spelen in het faciliteren van een veilige notificatie naar een andere instantie, zonder gegevens te onthullen over een persoon of mogelijk onderzoek.

In bredere context kan gedacht worden aan reeds bestaande noodzakelijke keteninteracties die er in het veiligheidsdomein plaatsvinden, waarbij het ongewenst vrijkomen van informatie potentiëel grote gevolgen heeft in het kader van informatiebeveiling of privacywaarborging. Denk bijvoorbeeld aan het communiceren van medische gegevens van militairen van/naar conflictgebieden, waarbij zowel de persoonsgegevens als de medische conditie van een militair niet onthuld mogen worden. Anderzijds kunnen er op basis van Zero-Knowledge Proof cryptografie keteninteracties ontworpen worden die op dit moment in het geheel niet mogelijk of toegestaan zijn. Hier ligt voor het veiligheidsdomein een wereld om te ontdekken.

Conclusie

Systemen die communiceren op basis van Zero-Knowledge Proof cryptografie kunnen bij de uitwisseling van gegevens zorgen voor een grote mate van veiligheid en daarmee rust in organisaties en rust in de samenleving brengen. Wat niet bekend is kan ook niet zomaar op straat of in de verkeerde handen terechtkomen. Systemen die met elkaar verbonden zijn op basis van Zero-Knowledge Proof cryptografie kunnen de uitdaging van ongelijke rubriceringsniveaus oplossen. Dat kan zonder een rechtstreekse verbinding te maken. Daarbij kan het inrichten van processen in de dagelijkse bedrijfsvoering helpen om het oerwoud van autorisaties kleiner te maken en de druk op de veiligheidsdiensten verlichten terwijl de algehele veiligheid stijgt.

[1]ING launches Zero-Knowledge Range Proof solution, a major addition to blockchain technology

[2]Gartner: Top Strategic Technology Trends 2021

Auteurs

Joop Koster
Chief Architect

joop.koster@capgemini.com, https://twitter.com/joopko

Joop is gespecialiseerd in het realiseren van bedrijfssystemen in verschillende industrieën, met een specialisatie in basisvoorziening-oplossingen in de openbare orde- en veiligheidsdomein. Zijn thoughtleadership is ontstaan uit vele interacties met politie- en inlichtingenorganisaties wereldwijd.

Daan Verwaaij
Business Analist

daan.verwaaij@capgemini.com

Daan is gespecialiseerd in het herkennen, vertalen en beantwoorden van de uitdagingen die het openbare orde- en veiligheidsdomein elke dag tegenkomt op het gebied van IT, maar ook daarbuiten.

Michael Kolenbrander
Domein Architect

michael.kolenbrander@capgemini.com

Michael is gespecialiseerd in het realiseren van systemen voor informatievoorziening in het openbare orde- en veiligheidsdomein, in het bijzonder in de context van informatie als Intelligence. Hij is bedenker en co-auteur van het Whiteflag Protocol en expert op gebied van opkomende technologieën zoals blockchaintechnologie.

Onze nationale, digitale veiligheid: van compliance naar risicobeheersing

Hoe kan de WBNI de digitale veiligheid van onze voornaamste infrastructuur versterken?

Highlights

- De WBNI is de Nederlandse vertaalslag van de Europese Netwerk- en Informatiebeveiligingsrichtlijn.
- Aanbieders van essentiële diensten moeten cyberbeveiliging in hun risicocultuur integreren.
- De wet is een unieke kans om op bestuursniveau aandacht te krijgen voor cybersecurity.
- De implementatie zal worden gecontroleerd door de publieke autoriteiten.
- Publiek-private samenwerking is essentieel voor een duurzame naleving.

Anders dan een cyclische compliance-benadering van cyberveiligheid, triggert de WBNI een nieuwe visie door een risicobeheercultuur op alle lagen te bevorderen.

Het is al vaak besproken dat onze samenleving steeds afhankelijker wordt van digitale systemen en infrastructuur. Toenemende digitale dreigingen en belangen worden door het NCSC jaarlijks beschreven in het Cybersecuritybeeld Nederland. De WRR concludeerde al in 2019 dat toenemende risico's de overheid ertoe dwingen om een grotere rol te spelen in de digitale veiligheid van onze kritieke infrastructuur. Met de invoering van de WBNI is deze rol voor het eerst vastgelegd in wet- en regelgeving.

Met de focus op het creëren van een 'risico-managementcultuur', vereist de WBNI dat organisaties in de vitale infrastructuur een minimum niveau van digitale beveiliging borgen. De continuïteit van bijvoorbeeld onze havenbedrijven is immers niet alleen in het belang van deze (commerciële) organisaties, maar in het belang van ons allemaal. Wat zou er in de samenleving gebeuren als er enkele weken slechts beperkte import van voedsel, brandstof of grondstoffen mogelijk zou zijn?

Daarbij krijgt de private sector de verantwoordelijkheid om hun kernprocessen te beveiligen als die van belang zijn voor nationale stabiliteit, weerbaarheid en economie.

Het succes van de WBNI wordt echter mede bepaald door de opstelling van private organisaties én de overheid. Het risico bestaat dat private organisaties de WBNI beschouwen als een compliance oefening in plaats van een actiegerichte oproep om de security-volwassenheid te vergroten. De vraag is dan ook, hoe we ervoor kunnen zorgen dat de WBNI de drijvende kracht wordt om de security-volwassenheid te versnellen binnen de nationale kritieke infrastructuur?

Cybersecurity als onderdeel van de risicocultuur van de organisatie

De EU heeft in 2016 de Network and Information Systems (NIS) Directive aangenomen om de kritieke infrastructuur te beschermen en de samenwerking rondom incident meldingen te versnellen. De NIS Directive is in Nederland in 2018 omgedoopt tot de Wet beveiliging netwerk- en informatiesystemen (WBNI). Met de invoering van de WBNI ontstaat er voor het eerst een wettelijke verplichting voor een aantal belangrijke organisaties/bedrijven die cruciale diensten leveren voor het functioneren van onze maatschappij om 'passende technische en organisatorische' maatregelen te nemen om de digitale veiligheid te borgen. Bijvoorbeeld door gebruik van encryptie, awareness campagnes en security- monitoring.

Het principe is natuurlijk niet nieuw. Veel bedrijven baseren hun informatiebeveiligingsbeleid al jaren op (internationale) standaarden, zoals ISO 27001 of NIST. Dergelijke standaarden stellen eigenlijk allemaal dat het bedrijf maatregelen moet implementeren om de geïdentificeerde risico's te beheersen

tot een acceptabel niveau. Tot zo ver lijkt de WBNI dus logisch aan te sluiten op de bekende werkwijze van de meeste organisaties. Dat was overigens ook de bedoeling van de wetgever. Een en ander zou de indruk kunnen wekken dat organisaties weinig hoeven te doen om voorbereid te zijn op de WBNI. Dat zou echter een misrekening zijn die niet alleen kan leiden tot onderschatting van de compliance-vereisten, maar belangrijker nog tot ondermijning van de effectiviteit van de WBNI om de Nederlandse samenleving te beschermen. De risicoanalyses moeten namelijk vooral ook rekening houden met impact op de samenleving en niet alleen met de impact op het bedrijf. Het is de vraag of de vitale bedrijven hier voldoende aandacht aan geven.

De vergelijking naar een enigszins gerelateerde wetgeving is interessant. Daar waar de maatschappelijke aandacht voor de WBNI vooralsnog vrij beperkt blijft, leidde de Algemene Verordening Gegevensbescherming (AVG) tot veel beroering. Dat is opmerkelijk, ook de WBNI kent de bevoegde autoriteit immers de mogelijkheid toe om een stevige bestuurlijke boete van maximaal 5 miljoen euro op te leggen. Dat is weliswaar minder dan de maximale boete onder de AVG, maar desondanks nog altijd een stevig bedrag. Het ontbreken van publieke aandacht kan ook juist een positieve bijdrage leveren aan de implementatie van de WBNI. Een paniekerige respons leidt al snel tot windowdressing en compliance-denken en vaak te weinig tot inhoudelijke actie om de digitale veiligheid te versterken.

Tegelijkertijd moeten vitale organisaties en digitale dienstverleners zich niet in slaap laten sussen. De publieke aandacht, meldplicht van incidenten, toezichthoudende rol van de overheid en juridische context gaan zorgen voor een nieuwe dynamiek in de organisatie. Door de WBNI als wetgevend kader zullen bestuurders zich moeten realiseren dat cyberveiligheid direct raakt aan de bedrijfsvoering, het vertrouwen van klanten en de stabiliteit van de samenleving. De WBNI zou door bedrijven in onze vitale infrastructuur dus niet alleen moeten worden benaderd als een gangbare 'checkbox-compliance' maar als een unieke kans om hun algehele benadering van cyberveiligheid opnieuw vorm te geven. Dit is ook in lijn met de ENISA-richtlijnen die de volledige cybersecurity-lifecycle bestrijken – van governance en bedrijfscontinuïteit tot detectie en respons. Gelukkig zien wij dat bedrijven zich steeds meer realiseren dat zij in de weerbaarheid van hun cyberveiligheid blijvend moeten versterken.

Het is daarbij interessant dat de WBNI belicht dat cybersecurity niet beschouwd moet worden als een IT-kwestie, maar als een integraal onderdeel van de kritieke operatie en strategische besluitvorming. Op dit moment wordt cyberveiligheid nog te vaak gezien als een verantwoordelijkheid van de IT-afdeling. De invoering van de WBNI maakt het glashelder dat dit onderwerp aandacht verdient op het hoogste bestuurlijke niveau. Wat ons betreft met één kapitein, bij voorkeur de CISO, die stuurt op de digitale veiligheid en belangrijke zaken adresseert in direct overleg met het bestuur, de juridische en compliance-afdelingen én de business. Het is cruciaal dat belangrijke stakeholders binnen organisaties snel gezamenlijk bepalen hoe ze dit zo goed mogelijk organiseren.

Samenwerking met partijen in een veranderend speelveld

In de afgelopen jaren is cyberveiligheid een steeds belangrijker onderwerp geworden op de agenda van overheden en publieke organisaties. De NIS-richtlijn eist van lidstaten dat zij naar behoren zijn uitgerust met een nationale cyberstrategie, een Computer Security Incident Response Team (CSIRT) en dat zij toezien op naleving van veiligheidseisen door aanbieders van essentiële diensten. De komende periode zal de toezichthoudende rol van de overheid steeds beter merkbaar worden bij commerciële bedrijven in de vitale sectoren. Gezamenlijk hebben zij de belangrijke opdracht om een werkwijze die daadwerkelijk onze nationale digitale veiligheid vergroot. Het is daarbij belangrijk dat de cultuur van risicobeheersing in deze samenwerking niet opeens omslaat in een compliance-gerichte aanpak. Het succes van de WBNI hangt in onze ogen af van succesvolle publiek-private samenwerking en de inzet van decentrale CERTS (bijvoorbeeld).

Samenwerking rondom incidenten

Tot nu toe worden significante cybersecurity-incidenten veelal intern door de geraakte organisatie afgehandeld. Met de invoering van de WBNI moeten organisaties in vitale sectoren ernstige incidenten melden bij het NCSC, waarna deze de impact van het incident kan analyseren en mogelijke mitigerende maatregelen in kaart brengen. Op basis van de informatie kan verdere impact van het incident op andere organisaties mogelijk worden voorkomen of beperkt. Dat versterkt niet alleen de nationale digitale veiligheid, maar ook de digitale veiligheid binnen de EU. Cyberaanvallen op organisaties kunnen een domino-effect hebben op andere sectoren en schade berokkenen over grenzen heen.

De verantwoordelijkheid om het incident te melden en het NCSC van de juiste informatie te voorzien ligt uiteindelijk bij de bedrijven die onderdeel uitmaken van de vitale sectoren. Echter, hoe vollediger, tijdiger en concreter de informatie is, hoe waardevoller voor de analyse en opvolging. Eerder is in Trends in Veiligheid al betoogd dat het delen van cyber-informatie een kwestie van vertrouwen is[1]. Informatie over cyberrsecurity-incidenten is vaak gevoelig, omdat het wat zegt over de (technische) security-maatregelen, de aard van data en systemen én de impact van het incident op de bedrijfsvoering. De natuurlijke neiging van private organisaties om bedrijfsgevoelige informatie zoveel mogelijk te beschermen staat daarmee op gespannen voet met het beoogde doel van de WBNI. Overheid en bedrijfsleven moeten daarom tijd en moeite investeren om, buiten de wettelijke vereisten om, te zorgen dat zij elkaar vertrouwen en leren begrijpen om belangrijke cyberinformatie met elkaar te delen.

Samenwerking met de toezichthouder

Een goede vertrouwensrelatie tussen de publieke en private sector is niet alleen essentieel zijn voor het melden van incidenten, maar ook voor het inrichten van een effectieve toezichthoudende rol van de overheid. Voor deze taak zijn een aantal toezichthoudende diensten aangewezen per sector (onder andere het Agentschap Telecom en De Nederlandsche Bank). Het is interessant om te volgen hoe deze toezichthoudende rol wordt ingevuld. Bemoedigend is dat bijvoorbeeld het Agentschap Telecom in 2019 al aangaf het stimuleren van de zorgplicht als een belangrijke taak te beschouwen[2]. Zoals eerder in dit artikel is betoogd, zou het de nationale digitale veiligheid sterk verstevigen als de bedrijven hun verplichting niet als 'compliance checklist' beschouwen, maar serieus werk maken van hun digitale veiligheid. De andere kant van de medaille is dat zij dan ook mogen verwachten van de toezichthouder dat deze oog heeft voor en ondersteuning biedt bij de risico-afwegingen. Daarom moet de autoriteit voldoende inspanning leveren om de soms complexe technische en bedrijfsmatige context mee te nemen in de oordeelsvorming. Nationale experts zullen de zakelijke-, en beveiligingsuitdagingen van bedrijven moeten begrijpen om een succesvolle audit uit te kunnen voeren.

De voorbeeldfunctie van de overheid

In de nieuwe situatie wordt het voor de overheid ook nog belangrijker om het goede voorbeeld te geven in de beveiliging van eigen diensten en infrastructuur om een geloofwaardige wetgever te zijn. Zowel de overheid als essentiële organisaties moeten zich realiseren dat het overtreden van de WBNI feitelijk betekent dat de nationale stabiliteit op het spel wordt gezet. Of dat dat in elk geval zo kan worden beschouwd in de maatschappij.

Samenvattend heeft de WBNI de potentie om een drijvende kracht te zijn om de security-volwassenheid van organisaties te versnellen en te borgen in de cultuur. Dit zorgt voor een nieuwe balans binnen bedrijven die er uiteindelijk toe moet leiden dat onze vitale infrastructuur beter wordt beveiligd.

In de weg daar naartoe, ontstaan nieuwe (invullingen aan) verantwoordelijkheden:

1. De rijksoverheid als toezichthouder op de digitale weerbaarheid en;
2. de vitale organisaties krijgen de wettelijke verantwoordelijkheid om de digitale veiligheid van hun diensten te borgen en incidenten te melden.

Om de WBNI succesvol te maken, ligt publiek-private samenwerking aan de basis. De volgende doelstellingen moeten gezamenlijk worden nagestreefd:

- De risico-management cultuur kan alleen duurzaam ontstaan als er een stevige governance structuur op het gebied van cybersecurity wordt ingericht.
- De organisaties moeten zorgen voor inzicht en transparantie rondom hun essentiële assets, zodat zij deze kunnen beschermen en snel en effectief kunnen reageren op incidenten.
- De overheid zal tijd en moeite moeten investeren om als toezichthouder een faciliterende rol te kunnen spelen.
- Informatiedeling rondom cyber-incidenten vereist een vertrouwensrelatie tussen overheid en private organisaties.

[1]Capgemini, Nederland digitaal veilig: internationale samenwerking als voorbeeld. https://www.trendsinveiligheid.nl/rapport/2018-vertrouwen-en-wantrouwen-in-de-digitale-samenleving/nederland-digitaal-veilig-internationale-samenwerking-als-voorbeeld/

[2]https://magazines.agentschaptelecom.nl/staatvandeether/2019/01/eidas-etd-wbni

Auteurs

Ana-Isabel Llacayo, CISM
Consultant Cybersecurity

ana.isabel.llacayo@capgemini.com

Ana-Isabel is gespecialiseerd in cyberveiligheid en EU-aangelegenheden. Ze werkt op het raakvlak van strategie en het technische domein. De afgelopen jaren heeft ze ruime ervaring opgedaan in het adviseren van publieke en private organisaties om zodoende hun cyberveiligheid te versterken.

Jasper van Buren
Managing Consultant Cybersecurity & Privacy

Jasper werkte ten tijde van het schrijven van het artikel bij Capgemini en hield zich bezig met adviesvraagstukken op het gebied van security-strategie, digitaal vertrouwen en de borging daarvan binnen organisaties en de samenleving.

Willen, moeten, kunnen: de weg naar informatiegestuurd werken

Hoe versterk je veranderbereidheid bij het streven naar IGW?

Highlights

- De focus op veranderbereidheid is een kansrijke strategie om de kloof tussen IGW-ambitie en IGW-realiteit te dichten.
- Behandel het streven naar IGW vooral als verandervraagstuk en niet zozeer als technologiekwestie.
- De beproefde DINAMO-methode geeft handvaten voor het meten en verbeteren van veranderbereidheid.
- Deze methode hanteert de drie motivatoren willen, moeten en kunnen om concrete uitdagingen en interventies te duiden.
- Ervaren noodzaak, betrokkenheid en vaardigheden van medewerkers maken het verschil om mens en technologie met elkaar te verbinden.

Ambities van publieke veiligheidsorganisaties voor informatiegestuurd werken (IGW) lopen achter op de realiteit. Een focus op veranderbereidheid is een kansrijke strategie om dit gat te dichten.

Ambitie en realiteit

IGW is al jaren een prioriteit in het publieke veiligheidsdomein. Politie, inspecties, defensie, gemeenten en uitvoeringsinstanties hebben allen stevige ambities op IGW-gebied. Dat is niet gek, want IGW biedt vele kansen voor de veiligheidssector. Zo kunnen handhavings- en preventietaken effectiever worden uitgevoerd en schaarse menselijke capaciteit slimmer worden ingezet.

Een zo sterk mogelijke informatiepositie is sinds mensenheugenis een prioriteit in het veiligheidsdomein. We hebben steeds meer en sterkere connecties met elkaar via apparaten, wat steeds meer digitale sporen oplevert. Door deze hyperconnectiviteit, samen met de opkomst van big data en kunstmatige intelligentie zijn er in rap tempo tal van nieuwe mogelijkheden ontstaan voor de identificatie van overtredingen, misstanden en verdachte situaties. Zo worden slimme camerasystemen ingezet om het werk van de marechaussee op Schiphol effectiever te maken en uiteindelijk zowel de veiligheid als het reizigersgemak te verbeteren. Kunstmatige intelligentie wordt ingezet om fraude op te sporen in enorme transactievolumes. De politie zet algoritmen in om aan de hand van 'crime heat maps' te voorspellen waar de volgende woninginbraak gaat plaatsvinden.

Het moge duidelijk zijn dat informatiegestuurde besluiten doorgaans betere besluiten zijn, wanneer deze informatie op betrouwbare en ethische wijze tot stand komt en wordt gebruikt. Het blijft echter een uitdaging om de juiste informatie op het juiste moment op de juiste plek te krijgen om besluitvorming optimaal te ondersteunen. Hoewel er steeds meer succesvolle experimenten zijn te vinden met IGW-toepassingen, belandt meer dan de helft in de 'valley of death' – de kloof tussen prototype en operationele implementatie. Wat is hiervan de oorzaak?

IGW: een veranderuitdaging

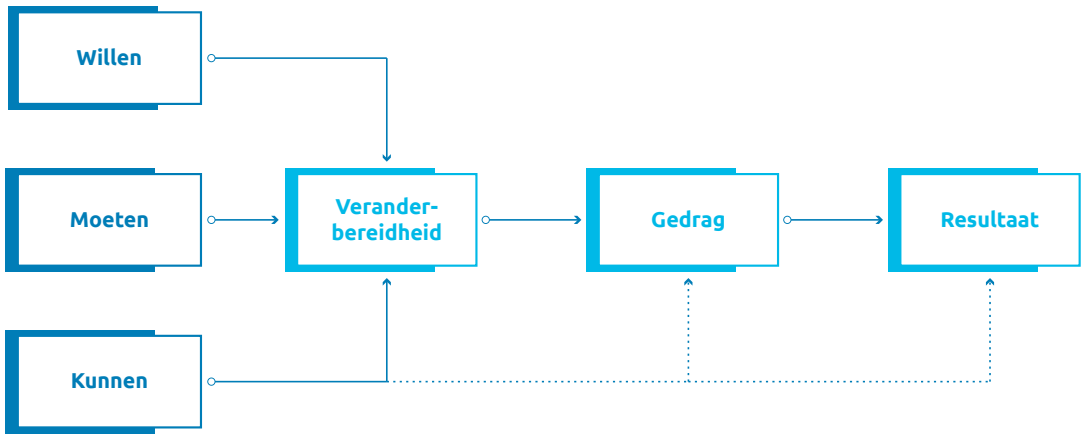
Defensie geeft aan dat deze 'valley of death' komt door (gepercipieerde) belemmeringen, een andere mindset of een gebrek aan capaciteit of middelen[1]. Uit recent onderzoek[2] blijkt dat 91% van de topmanagers uitdagingen op het vlak van mens en proces aanwijzen als grootste barrière om een informatiegestuurde organisatie te worden. Daarnaast blijkt dat twee op de drie datateams te maken heeft met weerstand tegen de adoptie van datagestuurde methoden, met als grootste oorzaken dat medewerkers onvoldoende op de hoogte zijn van de datastrategie en de positieve impact van data[3].

IGW vraagt om een cultuurverandering in het publieke veiligheidsdomein. IGW betekent geïnformeerd en proactief kunnen handelen in plaats van puur incidentgericht en reactief[4]. Dit is een attitudeverandering van 'wat denken we?' naar 'wat weten we?' Een open blik is hierbij essentieel. Daarnaast betekent IGW een procesgerichte aanpak: sturing, informatie verzamelen, analyseren en delen, en actie[5]. Dit cyclische proces loopt door alle organisatieniveaus heen en raakt daarmee alle medewerkers. Die medewerkers zijn naast gebruikers zelf ook bronnen van informatie. Net als een sensor nemen zij van alles waar, maar kunnen zij daar ook betekenis aan toekennen. Echter blijkt het goed vastleggen en delen van deze informatie in de praktijk een heikel punt.

We constateren dat in de praktijk technologische mogelijkheden vaak vooruitlopen op de veranderbereidheid van medewerkers. Betrokkenheid en vaardigheden van mensen om daadwerkelijk verandering te realiseren maken het verschil, maar dit is een onderbelicht aspect.

Aan de hand van de beproefde DINAMO-methode[6] beschrijven we hoe een publieke veiligheidsorganisatie bij het streven naar IGW-veranderbereidheid kan vaststellen en kan vergroten met interventies. Het basismodel (Figuur 1) achter deze methode steunt op de drie motivatoren **willen, moeten en kunnen**, die tot concrete gedragsverandering en daaruit volgende resultaten zijn te herleiden.

Figuur 1: Basismodel achter de DINAMO-methode.[7]



Willen veranderen

De motivator **willen** gaat over de houding van een persoon ten aanzien van de verandering. Dit wordt voornamelijk bepaald door drie factoren: de verwachte gevolgen van de verandering voor het werk, emoties die de verandering oproepen en de betrokkenheid bij het veranderproces.

De verwachte gevolgen van de verandering voor het werk zijn in onze ervaring doorgaans positief, tenzij medewerkers zich zorgen maken dat IGW hen meer werk gaat kosten dan het oplevert. Het is dan ook van groot belang dat het ondersteunen van medewerkers in hun dagelijkse werkzaamheden centraal staat en te voorkomen dat er vanuit een ivoren toren een te complex systeem wordt ontwikkeld[8]. Daarbij moet het voor medewerkers helder zijn dat een ICT-oplossing (middel) voor -IGW (doel) op zichzelf geen wondermiddel is. De rol van de mens blijft cruciaal voor het verzamelen van informatie, duiding en besluitvorming. Door dit te benadrukken blijft de meerwaarde van de bijdrage van medewerkers aan de organisatie duidelijk. Het gaat hierbij dus om het succesvol verbinden van mens en technologie[9].

De emoties die de verandering oproepen kunnen in het geval van IGW bijvoorbeeld gaan over nieuwe technologie. Zo blijkt uit onderzoek dat senior politieagenten in het Verenigd Koninkrijk bezorgd zijn dat kunstmatige intelligentie bestaande vooroordelen versterkt[10]. Dergelijke emoties zijn deels gevormd door eerdere ervaringen met (soortgelijke) veranderingen en worden verder ook gevormd bij de eerste communicatie over de actuele verandering. Hier wordt de basis gelegd voor het succes van de implementatie. Daarom is het tijdig actief betrekken van stakeholders van belang, zodat ze zich gehoord voelen.

Dit versterkt **de betrokkenheid bij het veranderproces** en maakt het mogelijk zicht te krijgen op de emoties ten aanzien van de verandering en deze vroegtijdig positief te beïnvloeden. Wees hierbij wel realistisch over de te verwachte tijdlijn en resultaten. Er worden maar al te graag mooie toekomstbeelden geschetst om medewerkers enthousiast te maken. In het begin werkt dit goed; het enthousiasme slaat echter om in scepsis zodra de verwachtingen niet worden waargemaakt.

Moeten veranderen

De motivator **moeten** omvat de houding van anderen in de omgeving van een persoon tegenover de verandering. Deze motivator bestaat uit twee factoren: ervaren externe noodzaak om te veranderen en ervaren interne druk om te veranderen.

De externe noodzaak om te veranderen heeft door veranderde maatschappelijke omstandigheden de status bereikt van meest zwaarwegende factor voor veranderbereidheid[11]. De coronacrisis is een extreem voorbeeld van een externe noodzaak die digitalisering in korte tijd enorm heeft versneld. Tegelijkertijd benutten criminelen de mogelijkheden van (kwetsbaarheden in) state-of-the-art technologie. De maatschappij verwacht dat veiligheidsorganisaties dat ook doen. Voorwaarde is uiteraard dat de noodzaak wel ervaren moet worden door medewerkers, wil dit een positieve invloed hebben op veranderbereidheid.

Ervaren interne druk om te veranderen wordt vooral beïnvloedt door rolmodellen in de organisatie, met name leidinggevenden[12]. Zij hebben daarom een cruciale rol om continu het belang van IGW over te brengen[13] en met gedrag te tonen dat zij achter de IGW-verandering staan. Organisaties slagen niet met IGW omdat ze simpelweg meer of betere data en tools bezitten. Het verschil wordt gemaakt doordat het leiderschap heldere doelen stelt, definieert hoe succes eruitziet, de juiste vragen stelt en zo nodig interventies pleegt. Een uitdaging hierbij is dat zij de juiste randvoorwaarden creëren voor creativiteit en innovatie op de werkvloer én om IGW mogelijk te maken in het operationele proces.

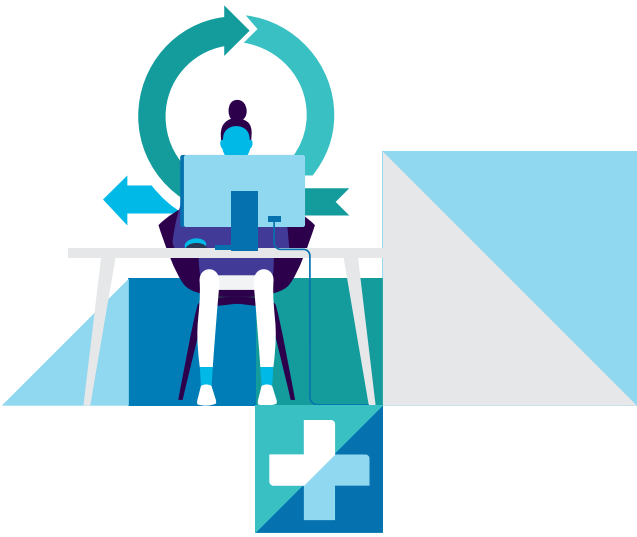
Kunnen veranderen

Kunnen is de meest zwaarwegende motivator en verwijst naar de mate waarin de benodigde middelen, kennis en ervaring beschikbaar zijn evenals de aansturing van de verandering. De belangrijkste factoren hierbinnen zijn de timing van de verandering en de kennis en ervaring van de betrokkenen.

De timing van de verandering is al snel een knelpunt als er geen noodzaak wordt ervaren. In dat geval wordt vooral in beperkingen gedacht. Kan de medewerker de verandering bijhouden? Is deze eraan toe om te veranderen? Kan de medewerker aan de gevraagde eisen voldoen? En komen de veranderingen volgens de medewerkers op een goed moment? Als het antwoord overwegend nee is, dan moet er eerst een crisis of gerichte interventie plaatsvinden om de urgentie te vergroten. Bijvoorbeeld het blootleggen van de gevolgen van niet veranderen door een belangrijke leider en het aantrekken van mensen met een IGW-competentieprofiel. Meeliften op een andere verandering die wel momentum heeft is ook een optie. Zo kan IGW meeliften op veranderprogramma's op gebied van digitalisering, data & analytics, kunstmatige intelligentie of sensing. Verder is het verstandig om klein te beginnen. Dan kan vroegtijdig worden vastgesteld of medewerkers klaar zijn voor de verandering en worden bijgestuurd voordat grotere investeringen worden gedaan. Bovendien kan een experiment de angst wegnemen om iets nieuws te doen en te denken dat je niet de juiste kennis hebt.

Met **de kennis en ervaring van betrokkenen** valt of staat een verandertraject. Kunnen medewerkers op basis van hun vakinhoudelijke kennis bijdragen aan het succes van de toekomstige verandering? Zijn zij zelf actief betrokken geweest bij voorgaande veranderingen? Het antwoord op deze vragen geeft waardevolle inzichten voor een IGW-verandertraject. Zo noemt de politie het absorptievermogen van de organisatie en de medewerkers die daarin werken als een risico bij het realiseren van haar ambities voor het verbeteren van het intelligencewerk[14]. Bij onvoldoende kennis en ervaring kunnen verwachtingen en strategie worden bijgesteld. Denk aan het omscholen van personeel of het rekruteren van medewerkers met het gewenste profiel.

IGW biedt vele kansen en staat dan ook hoog op de agenda in het veiligheidsdomein. Er wordt volop geëxperimenteerd met IGW-toepassingen op basis van state-of-the-art technologieën. Echter verloopt de vertaling hiervan naar organisatiebrede verandering vaak stroperig en niet zelden strandt deze in de "valley of death". Om IGW-ambities waar te maken is meer aandacht nodig voor veranderbereidheid: in hoeverre zijn de ingrediënten willen, moeten en kunnen aanwezig? De sleutel tot succes: behandel het streven naar IGW vooral als verandervraagstuk en niet zozeer als technologiekwestie. Wij pleiten ervoor om voorafgaand aan elk IGW-verandertraject de veranderbereidheid vast te stellen, de veranderstrategie hierop aan te sluiten en gerichte interventies te plegen waarbij de medewerker centraal staat.



[1]https://www.rijksoverheid.nl/documenten/rapporten/2018/11/19/samen-sneller-innoveren---innovatiestrategie-defensie

[2]https://www.businesswire.com/news/home/20200106005280/en/NewVantage-Partners-Releases-2020-Big-Data-and-AI-Executive-Survey

[3]https://www.exasol.com/exasol-cloud-report_adopting-data-driven-methods/

[4]https://magazines.defensie.nl/kmarmagazine/2021/01/05_kmar_future_proof-igo_01-2021

[5]https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/72506.pdf

[6]https://www.managementboek.nl/code/inkijkexemplaar/9797090077326/gratis-whitepaper-van-weerstand-naar-veranderbereidheid-erwin-metselaar.pdf

[7]Metselaar E., Cozijnsen A., Delft P. van (2016). Van weerstand naar veranderbereidheid. Bricklayer Productions.

[8]Hengst M. den, Brink T. ten, Mors J. ter (2017). Informatiegestuurd politiewerk in de praktijk. Vakmedianet.

[9]https://www.defensie.nl/downloads/publicaties/2020/11/25/strategische-kennis--en-innovatieagenda-2021-2025

[10]https://artificialintelligence-news.com/2019/09/17/uk-police-concerned-ai-bias-automation/

[11]https://www.managementboek.nl/code/inkijkexemplaar/9797090077326/gratis-whitepaper-van-weerstand-naar-veranderbereidheid-erwin-metselaar.pdf

[12]Boonstra, J. (1994). Herontwerp, reengineering en ontwikkeling. Gedrag en Organisatie, 6, 331-351.

[13]https://magazines.defensie.nl/kmarmagazine/2021/01/05_kmar_future_proof-igo_01-2021

[14]https://www.rijksoverheid.nl/documenten/begrotingen/2020/09/15/begroting-nationale-politie-2021

Auteurs

Luuk Tubbing
Senior Consultant

luuk.tubbing@capgemini.com

Luuk is Senior Consultant bij Capgemini Insights & Data. Hij is actief op het gebied van Intelligence en Informatiegestuurd Werken, met name in het domein openbare orde- en veiligheid.

Siebe Vaartjes
Senior Consultant

siebe.vaartjes@capgemini.com

Siebe is Senior Consultant bij Capgemini Business Technology Solutions. Hij is actief in het openbare orde- en veiligheidsdomein op het gebied van Intelligence en Informatiegestuurd Werken.

Hoe semantiek kan bijdragen aan een veiliger Nederland

Is ‘kennisbewust opereren’ de volgende stap na datagedreven werken en informatie-gestuurd optreden?

Highlights

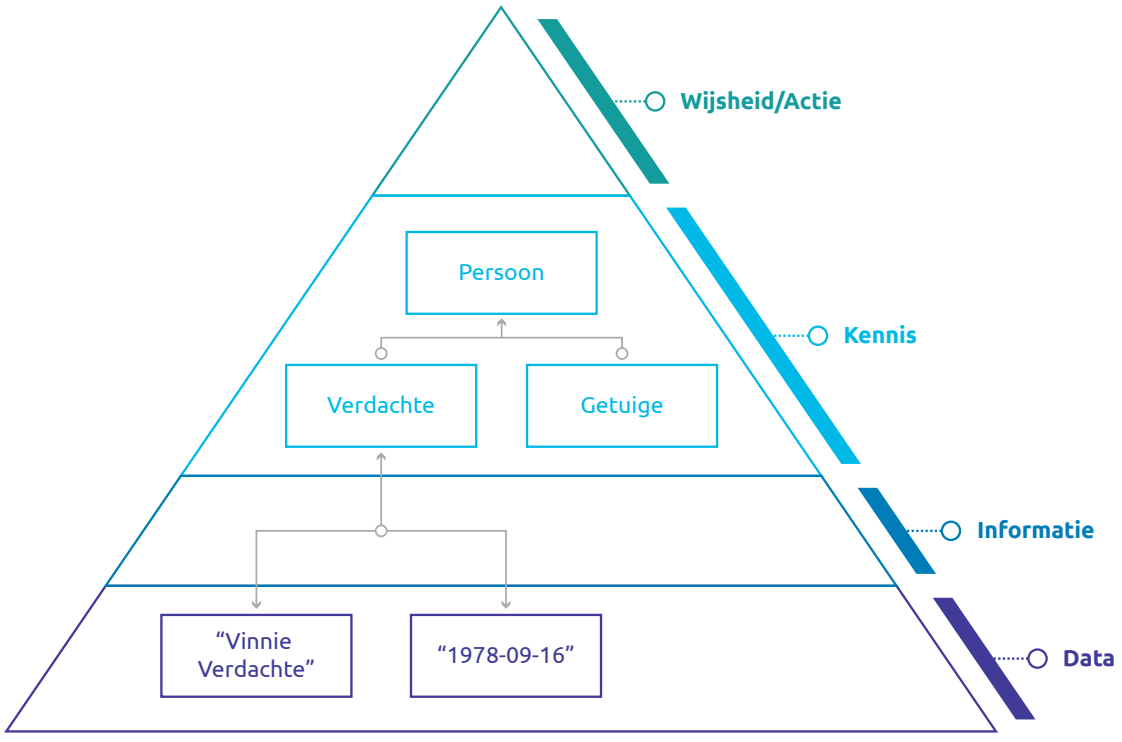
- Het gebruik van gemodelleerde kennis in RDF kan leiden tot betere acties en conclusies.
- Het 'graafmodel' van RDF sluit aan op het menselijk denken.
- RDF helpt bij het trainen en uitlegbaar houden van kunstmatige intelligentie.
- RDF kan de kans op fouten in ketens verkleinen en efficiëntie verhogen.
- RDF sluit aan bij een opkomende modellering-standaard voor publieke organisaties.

In dit artikel schetsen we hoe veiligheidsprofessionals in staat worden gesteld om effectiever met informatie om te gaan, door het gebruik van semantische modellen op basis van RDF.

Het modelleren van kennis in RDF

Semantiek is de leer van de betekenis en houdt zich bezig met het zinvol gebruik van symbolen en taal om informatie over te brengen. In de communicatie tussen mensen is het belangrijk dat iedereen hetzelfde bedoelt met hetzelfde woord. Eveneens, als er tussen digitale systemen gegevens moeten worden uitgewisseld is een gedeelde betekenis ook essentieel. In het kader van systeemontwikkeling kan semantisch modelleren worden begrepen als het vastleggen van een werkgebied in een model waarbij elk objecttype een definitie heeft en de mogelijke relaties tussen objecttypen betekenisvol zijn gemodelleerd. Informatiearchitecten en datamodelleurs doen dit effectief al jaren, waarbij het resultaat meestal eindigt als naslagwerk. Echter, RDF (Resource Description Framework) maakt het mogelijk om modellen in dezelfde vorm op te slaan als de gegevens die door het werkende systeem stromen, waardoor data en de betekenis ervan (semantiek) beide bruikbaar zijn voor analyses en zoekvragen aan het systeem. Het potentieel van de modellen wordt zodoende optimaal benut; het systeem kan dan niet alleen zoekvragen en berekeningen uitvoeren op geregistreerde gegevens maar ook op relevante en gerelateerde begrippen. Dit wordt kennisrepresentatie genoemd.

Figuur 1: De piramide van data, informatie, kennis en wijsheid/actie.



Een simpel voorbeeld van kennisrepresentatie is het volgende: voor mensen is het helder dat zowel verdachten als getuigen van een incident personen zijn (in een bepaalde rol), maar een systeem heeft deze kennis in principe niet. Wanneer 'verdachte' en 'getuige' dus als specifiekere klassen van 'persoon' worden gemodelleerd, dan zijn alle personen aan de hand van de generieke klasse 'persoon' snel op te vragen, terwijl ze misschien niet als zodanig waren geregistreerd. De pyramide uit figuur 1 illustreert conceptueel hoe een systeem dat gebruik maakt van kennisrepresentatie, een gebruiker kan ondersteunen: data zijn ruwe, geregistreerde symbolen, informatie is data in samenhang die voor iemand van nut is en kennis is informatie over informatie. Over de modelleringswijze van dit simpele voorbeeld valt te twisten en het voorbeeld resulteert niet direct in iets dat niet ook anders opgelost had kunnen worden. Echter, het dient om aan te geven dat wanneer bepaalde domeinkennis zinvol is gemodelleerd, dit zou kunnen leiden tot snellere inzichten of gerichtere acties. Zoals de piramide conceptueel laat zien zou deze winst dus mede tot stand komen door het toepassen van gemodelleerde kennis in RDF.

Overeenkomst met het menselijk denken

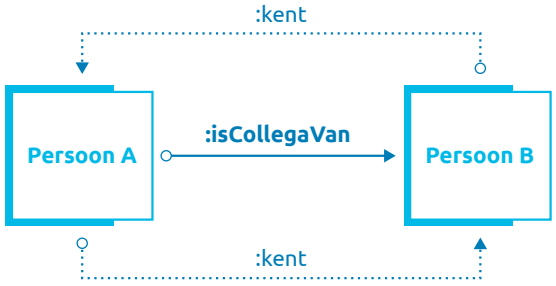
Het toepassen van RDF onderscheidt zich verder van traditionele systemen in het feit dat gegevens niet worden opgeslagen als tabellen, maar als een 'graaf'. Dit is een wiskundig concept dat zich laat visualiseren als een netwerk van bolletjes (of nodes) die zijn verbonden met lijnen die relaties voorstellen. In RDF is behalve aan de nodes, ook aan de relaties daartussen betekenis te geven. Een relatie kan worden hergebruikt en vormt zodoende een belangrijke bouwsteen in een systeem of applicatie dat met betekenisvolle relaties werkt. In het veiligheidsdomein is dit belangrijk, omdat zaken als dreiging vaak gepaard gaan met personen en objecten die op een bepaalde manier met elkaar zijn verbonden. Bovendien sluit deze manier van data verzamelen, verwerken en visualiseren beter aan op het menselijk denken, dan het werken met tabellen. Het voorbeeld van relaties tussen een groep mensen is veel makkelijker te visualiseren in bollen en lijnen (vergelijkbaar met het tekenen op een whiteboard of het maken van een mindmap) dan in één of meerdere tabellen. In grote datasets met complexe gegevens zijn in dit paradigma sneller inzichten te verkrijgen zoals welke nodes een hoge mate van verbondenheid hebben in het netwerk (en dus belangrijk zijn) of dat sommige nodes ongeveer dezelfde relaties of eigenschappen hebben (en daarmee in letterlijke zin een gemeenschap vormen). Dit soort inzichten zijn typerend voor wat ook wel graph-based intelligence wordt genoemd. Wanneer ook semantische modellen in RDF worden toegepast, zoals hieronder wordt geschetst, spreekt men van semantic knowledge graphs.

Toepassingen in de praktijk van het veiligheidsdomein

Een hogere mate van aansluiting bij menselijk denken is volgens ons al van aanzienlijke waarde, omdat dit tijd kan schelen in bepaalde (denk)processen, maar RDF maakt nog meer zaken mogelijk. Kunstmatige intelligentie (AI) kan semantische modellen in digitale vorm namelijk goed gebruiken om slimmer en efficiënter te worden. Sinds Garri Kasparov door een schaakcomputer werd verslagen is al veel geëxperimenteerd met het automatisch classificeren van data zodat een systeem kan leren van automatisch ontdekte patronen. Echter, dit leidt veelal tot oplossingen waarbij professionals niet meer eenvoudig kunnen uitleggen hoe er tot een bepaalde conclusie of actie wordt gekomen. Wanneer een algoritme de menselijke denkcapaciteit overstijgt, is het dus nuttig – bijvoorbeeld wanneer in de rechtszaal helder bewijs moet kunnen worden overlegd – om elementen uit een door mensen bedacht semantisch model te kunnen aanwijzen waar het algoritme rekening mee heeft gehouden. Voor processen waar dit van belang is kan een semantisch model dus essentieel zijn om AI-toepassingen uitlegbaar te houden.

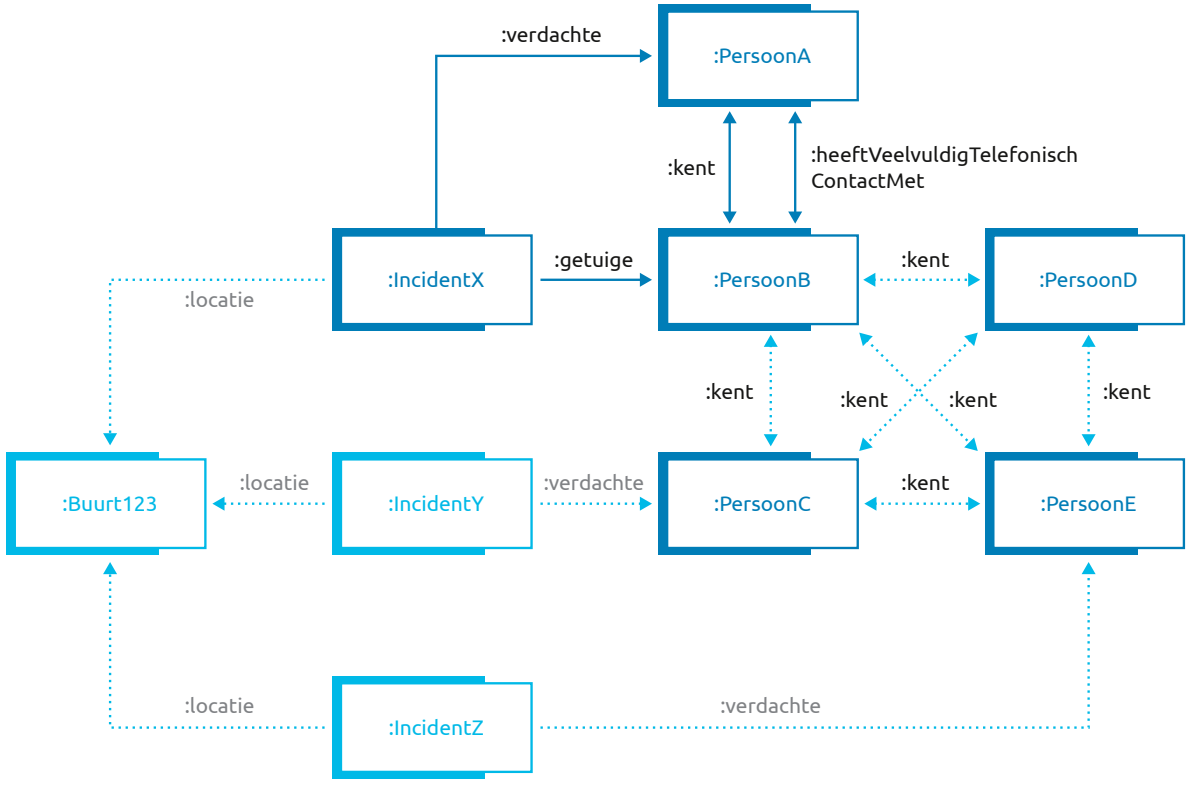
Daarnaast kunnen semantische modellen een basis zijn voor het vormgeven van gebruikersinteractie met een modern systeem. In een semantisch model in RDF kan bijvoorbeeld worden uitgedrukt hoe de ene relatie zich verhoudt tot een andere. Zo is het bijvoorbeeld mogelijk om te modelleren dat zowel het bevriend zijn met iemand als het zijn van een directe collega, specifiekere vormen zijn van iemand kennen. Ook kan worden uitgedrukt dat iemand kennen een symmetrische relatie is en dat dezelfde relatie dus ook van toepassing is in de tegengestelde richting. Als dus is geregistreerd dat persoon A een collega is van persoon B, zou er achteraf ook vanuit persoon B bekeken kunnen worden wie deze persoon allemaal kent en zal in ieder geval ook persoon A naar boven komen (zie figuur 2). Op basis van dit soort modellen, ook wel ontologieën genoemd, zouden gebruikersschermen kunnen worden ontworpen waarbij het visueel leggen van relaties centraal staat. Het semantische model faciliteert dan vanwege de gemodelleerde kennis niet alleen de gegevensanalyse achteraf, maar ook direct een meer intuïtieve manier van werken voor de gebruiker.

Figuur 2: Kennen als afgeleide relatie.



Zoals eerder aangestipt: het inzicht dat iemand een significant aantal andere mensen kent in een netwerk zou bijvoorbeeld kunnen betekenen dat iemand belangrijk is en dat verder onderzoek nuttig kan zijn. Stel dat er een aanleiding is om de afhandeling van een incident als vreemd te bestempelen en dat dit tot nader onderzoek leidt. Belgegevens van de verdachte, persoon A, worden opgevraagd en laten zien dat de verdachte veelvuldig telefonisch contact heeft gehad met persoon B, de getuige van het incident die zich vrijwillig heeft gemeld (zie Figuur 3). Omdat dit vreemd lijkt, wordt persoon B onder de loep genomen en blijkt het dat deze persoon meer mensen kent die betrokken waren bij verschillende incidenten (Incident X, Y en Z) in de buurt. Persoon A blijkt na onderzoek als enige deze andere personen niet te kennen. Persoon B, hoewel zelf nooit verdachte van een incident en dus niet eerder bekend in het systeem, heeft mogelijk een reden om als getuige op te treden tegen persoon A en wordt op basis hiervan extra aan de tand gevoeld. Uiteraard gaat het hier om een sterk gesimplificeerd voorbeeld, maar laat het zien dat als de incidenten X, Y en Z apart werden bekeken, een stevigere aanpak ten aanzien van persoon B mogelijk achterwege was gebleven.

Figuur 3: Visualisatie van het voorbeeld.



Semantische data-interoperabiliteit in ketens

Naast het feit dat RDF het toepassen van betekenisvolle relaties mogelijk maakt, heeft RDF ook de potentie om organisatie-overstijgend gebruikt en ontwikkeld te worden. Waarin RDF duidelijk verschilt van traditionele systemen is het gebruik van HTTP-URI's als identificatiekenmerk van gegevens in een systeem. Traditionele systemen en databases die niet op basis van RDF werken, gebruiken meestal een voor mensen betekenisloos identificatiekenmerk dat prima werkt binnen het gesloten systeem, maar daarbuiten – zelfs binnen dezelfde organisatie – zegt dit identificatiekenmerk niets. Een HTTP-URI (wat neerkomt op een URL, bijv: 'http://data.mijnorganisatie.nl/id/123456') heeft in de context van het internet een functie en zou dus kunnen worden gebruikt om de betekenis van data en modellen van anderen op te kunnen halen of simpelweg kunnen dienen als referentie. Zo is het bijvoorbeeld mogelijk om uit te drukken dat een gegeven of begrip van organisatie of afdeling A hetzelfde of ongeveer hetzelfde is als die van organisatie of afdeling B. Wanneer dit openlijk wordt gedaan, ontstaat een netwerk van gegevens en modellen waarbij semantiek altijd opzoekbaar is voor zowel mens als machine. Dit wordt ook wel aangeduid als 'Linked Data' en is sinds 2005 de droom van de uitvinder van RDF alsook van het wereldwijde web daarvoor, Tim Berners-Lee. Het publiceren van begrippenkaders in RDF zou verwarring over gegevens in een keten kunnen voorkomen en daarmee de kans op fouten in de keten kunnen verkleinen. Waar dit is toegestaan zouden in data-analyses zelfs gegevens van andere organisaties kunnen worden meegenomen, zonder deze te hoeven kopiëren en kan het beheer ervan worden gelaten bij de bron. Uiteraard moet goed nagedacht worden over zaken als privacy en security, al zouden dergelijke overwegingen eerder in beeld moeten zijn dan de keuze voor RDF.

De vraag rijst al gauw: als RDF al het bovenstaande mogelijk maakt, waarom is dan nog geen sprake van grootschalige adoptie? Uitdagingen die een grote rol spelen zijn het bestaande IT-landschap dat niet zomaar met RDF gemengd kan worden en dat nieuwe mogelijkheden zich het makkelijkst laten integreren met technologieën waar men al veel ervaring mee heeft. Gartner plaatste RDF in 2020 (onder de noemer Ontologies and Graphs) in de Trough of Disillusionment van hun hype-cyclus, en schetst daarmee de situatie dat steeds meer organisaties met realiteitszin de stap aandurven. In dit kader is het Metamodel Informatiemodellering (MIM) van onder andere Geonovum een belangrijke ontwikkeling om te noemen. Dit model beoogt standaardisering van informatiemodellen in het Nederlandse publieke domein en reikt RDF aan als een manier om met het metamodel te modelleren. Het is de verwachting dat Forum Standaardisatie in 2021 de toetsingsprocedure van MIM hervat voor op de pas-toe-of-leg-uit-lijst, waardoor het MIM voor publieke organisaties een verplicht of aanbevolen karakter krijgt. Het veiligheidsdomein zou er volgens ons goed aan doen om zich voor te sorteren op deze ontwikkeling en deze standaard te volgen. Zeker wanneer dit ook wordt opgepakt door ketenpartijen en wanneer in het veiligheidsdomein steeds meer semantisch wordt gemodelleerd in RDF, zal de veiligheidsprofessional ons inziens ook steeds meer kennisbewust kunnen opereren.

Auteurs

Amir Westhoff
Senior Consultant

amir.westhoff@capgemini.com
https://twitter.com/AmirWesthoff

Amir is gespecialiseerd in Linked Data/RDF/semantisch modelleren.

Laura van Dijk
Senior Consultant

laura.van.dijk@capgemini.com

Laura is gespecialiseerd in business- en informatieanalyse binnen het openbare orde- en veiligheidsdomein.

Robocop: de vlucht van een drone als handhaver

Hoe de technologische en strategische ontwikkeling van drones in juiste banen leiden?

Highlights

- **Snelle ontwikkeling van drones stimuleert autonoom gebruik.**
- **Ontwikkeling van sensoren leidt tot meer toepassingen.**
- **Alternatief voor vergrijzing en daarmee minder personeel.**
- **Hogere kwaliteit besluiten door meer informatiebronnen.**
- **Overkoepelend Drone Expertise Centrum nodig.**

Het aantal menselijke ogen en oren op straat neemt, als gevolg van de vergrijzing, af. Drones en sensoren helpen het tekort aan te vullen, zorgen voor een goed overzicht en helpen bij het nemen van beslissingen.

Het is erg onrustig is in een woonwijk, de meldkamer ontvangt een melding. Auto's worden in brand gestoken en er zijn veel mensen op de been. Er wordt dringend om hulp gevraagd. Door de beperkt beschikbare menscapaciteit besluit men een drone op verkenning te sturen. De drone krijgt de gps-coördinaten van de betreffende wijk en vliegt er zelfstandig naar toe. In de wijk aangekomen schakelt de drone zijn camera in en vliegt in een gestructureerd patroon over de wijk om de situatie zo goed mogelijk in kaart te brengen. De opname wordt live naar een politiespecialist gestuurd die de situatie inschat en vaststelt welk type medewerkers worden opgeroepen om naar de wijk te worden gestuurd. De politie coördineert hierbij ook de brandweer en andere hulpdiensten. Als de hulpdiensten ter plaatse zijn aangekomen, blijft de drone vanuit de lucht de wijk in de gaten houden om te voorkomen dat hulp onverwacht verstoord wordt. Nadat de rust is teruggekeerd vliegt de drone terug naar de thuisbasis.

Huidige status

Het gereedkomen van wetgeving rondom Unmanned Aerial Vehicles (AUV), in de volksmond drones genoemd, is een teken dat de ontwikkeling en toepassingen voor drones serieuze vormen aan neemt. Nederland start in 2022 proeven[1] met luchttaxi's en drones in drie steden: Enschede, Amsterdam en Rotterdam. De ANWB voert testvluchten uit met drones van AVY voor het vervoeren van organen. De brandweer voert proeven uit in het gebruik van drones bij bluswerkzaamheden op grotere hoogte. Defensie werkt al 20 jaar met drones waaronder de bekende Reaper en Raven. Daarnaast heeft Defensie ook mini-drones[2] van het type Black Hornet in gebruik. De Nederlandse politie onderzoekt sinds 2017 het gebruik van drones in verschillende proeftuinen. Denk bijvoorbeeld aan crowd control (zoals recent de coronademonstraties) en het in kaart brengen van een ongeval-locatie. De drone zelf is slechts een vervoermiddel, de sensor bepaalt de toepassing. Dit zijn slechts enkele voorbeelden, de toepassingen zijn (al) legio.

De nabije toekomst: besturing vanuit centrale locaties

Een politie droneteam bestaat nu nog uit drie personen (vlieger, operator en waarnemer), een behoorlijke aanslag op het aantal beschikbare politiemensen. Door de snelle technologische ontwikkelingen kunnen drones zelfstandig vliegen, bijvoorbeeld op basis van gps-coördinatoren naar een plaats van bestemming. Met behulp van sensoren en Artificial Intelligence (AI) bepaalt de drone zijn positie en corrigeert de operator de drone op afstand als dat nodig is. Met dezelfde sensoren en intelligentie detecteert de drone of er andere objecten in de buurt zijn en ontwijkt deze. Ter plekke bepaalt de drone, op basis van vooraf ingegeven parameters, de te vliegen route en voert taken als observatie of volgen uit. Juist door de autonomie van de drone, de ingebouwde intelligentie en de sensoren kan de drone door één persoon worden bediend.

Iedere politie-eenheid heeft een zogeheten Dienst Regionaal Operationeel Centrum (DROC)[3]. Deze dienst heeft het totaaloverzicht van alle lopende politieacties en voert bij incidenten de regie over de noodhulp, handhaving en opsporing. De dienst behandelt de aanname van (112-) meldingen en verrijkt deze met realtime intelligence. Zij vormt de lifeline-functie voor collega's, alarmeert eenheden bij mono- en multidisciplinaire opschaling en ondersteunt de crisisbeheersing. Bij elk van de DROC's kan een commandoruimte worden ingericht van waaruit de drones en de inzet worden aangestuurd. Het is denkbaar dat twee of drie vliegers/operators op afstand meerdere drones tegelijkertijd aansturen. Een lokale commandant kan dan op basis van de binnenkomende beelden en andere sensorinformatie de eenheden op de grond aansturen.

Op sensorgebied staan de ontwikkelingen ook niet stil. Naast de bekende cameratypen worden sensoren ontwikkeld die gevaarlijke stoffen meten, geheime draadloze communicatienetwerken opsporen of geografische metingen uitvoeren. LIDAR (Laser imaging Detecting And Ranging) is onder andere een techniek waarbij bijvoorbeeld het (micro) reliëf in het landschap in kaart wordt gebracht. Deze techniek komt uit de archeologie om oudheden in onbereikbare gebieden te vinden. Dit kan ook gebruikt worden om veldonderzoek te doen naar bijvoorbeeld lichamen.

Het Drone Expertise Centrum

Naast het operationele gebruik van drones pleiten wij voor het oprichten van een Drone Expertise Centrum (DEC). Het DEC dient na te denken over de benodigde organisatie, processen en besluitvorming en borgt deze in de staande lijnorganisatie. Aansluiting bij, of integreren met, andere sensing-ontwikkelingen als cameratoezicht en bodycams is noodzakelijk. Hierbij kunnen alle beschikbare beeld- en geluidopnamen onderzocht worden op basis van menselijke intelligentie (Human Intelligence – HUMINT) en/of Artificial Intelligence (AI). Ook dient er aandacht zijn voor interregionale of landelijke samenwerking, opsporing stopt niet bij regio- en landsgrenzen. Naast de politie zetten ook andere hulporganisaties drones in. Intensieve samenwerking tussen de verschillende hulporganisaties en gezamenlijk gebruik van verschillende sensoren helpt de inzet van schaarse mensen en middelen en bespaart kosten. Het DEC kan hier een strategische en tactische rol in nemen.

Privacy

Naast technologische ontwikkelingen en de groeiende mogelijkheden van drones vinden wij het van groot belang dat de veiligheid en ethiek rondom drones hoog in het vaandel moet staan. Een rapport van het Rathenau Instituut geeft in het rapport Burgers en Sensoren[4] aan dat de acceptatie van sensorinzet afhankelijk is van de mate van veiligheid: hoe onveiliger burgers een situatie inschatten, des te meer ze het geoorloofd vinden om sensoren toe te passen om de veiligheid en leefbaarheid te vergroten. Hieraan gekoppeld vinden burgers dat privacy-by-design moet worden toegepast bij de inzet van sensoren. Dit is onder andere afhankelijk van de veiligheid in de betreffende situatie. Wij vinden dat privacy en daaraan verbonden ethiek in de uitwerking van het gebruik van drones meegenomen moeten worden.

Samenvatting en conclusie

De technologische ontwikkeling en het gebruik van drones, in het veiligheidsdomein, neemt een grote vlucht. Naast de al gebruikte sensoren als camera's en bodycams krijgt de politie een extra grote hoeveelheid aan data die gecombineerd met andere informatiebronnen een betere informatiepositie geeft. Verwerking van al die informatie kan niet meer alleen door mensen worden gedaan en moet worden ondersteund door intelligente systemen. Het uitbreiden van het gebruik van drones is voor de politie een goede aanvulling om het tekort aan ogen en oren op straat deels op te vangen. Het integreren van en uitbreiden met drones heeft alleen zin als de organisatie daaromheen wordt aangepast. Een in te richten Drone Expertise Centrum (DEC) helpt de organisatie om proces- & organisatieverandering te initiëren en overzicht te hebben en houden op het gebruik van drones en zorgt voor een succesvolle inzet in de komende jaren.

[1]https://www.computable.nl/artikel/opmerkelijk/smart-logistics/7126416/5933077/nederland-proeftuin-voor-luchttaxis-en-drones.html

[2]https://www.defensie.nl/actueel/nieuws/2018/05/02/verkenners-landmacht-en-mariniers-krijgen-mini-drones

[3]De Dienst Regionaal Operationeel Centrum vormt de schakel tussen de organisatie en de taken die de politie 'op straat' verricht. De dienst bestaat uit de meldkamer en het regionale informatieknooppunt voor actuele informatie.

[4]Snijders, D., M. Biesiot, G. Munnichs, R. van Est, met medewerking van S. van Ool en R. Akse (2019). Burgers en sensoren – Acht spelregels voor de inzet van sensoren voor veiligheid en leefbaarheid. Den Haag: Rathenau Instituut

Auteurs

Frans van Vliet
Transformatiemanager

frans.van.vliet@capgemini.com

Frans heeft, als business consultant en project-/programmamanager, meer dan 30 jaar ervaring in IT en organisatieveranderingen. Hij heeft ruime ervaring in de sectoren telecommunicatie, energie en overheid. Hij is werkzaam in het publieke veiligheidsdomein voor Capgemini.

Jeroen Oosterwal
Enterprise Architect Director

jeroen.oosterwal@capgemini.com
https://twitter.com/jeroenoosterwal

Jeroen Oosterwal heeft meer dan 30 jaar ervaring als adviseur en architect in het veiligheidsdomein. Hij heeft een achtergrond in kantoorautomatisering, cloud en security. Hij is werkzaam in het publieke veiligheidsdomein voor Capgemini.

Verbeterde identificatie door AI-gedreven documentcontrole

Hoe werken AI en privacy-gevoelige gegevens samen?

Highlights

- Controlerende instanties moeten met de complexiteit van identiteitsdocumenten omgaan.
- Gebrek aan data eist een opsplitsing in generieke AI-componenten.
- Hoe een hybride vorm van mens, data en AI voor een toekomstbestendige applicatie zorgt.

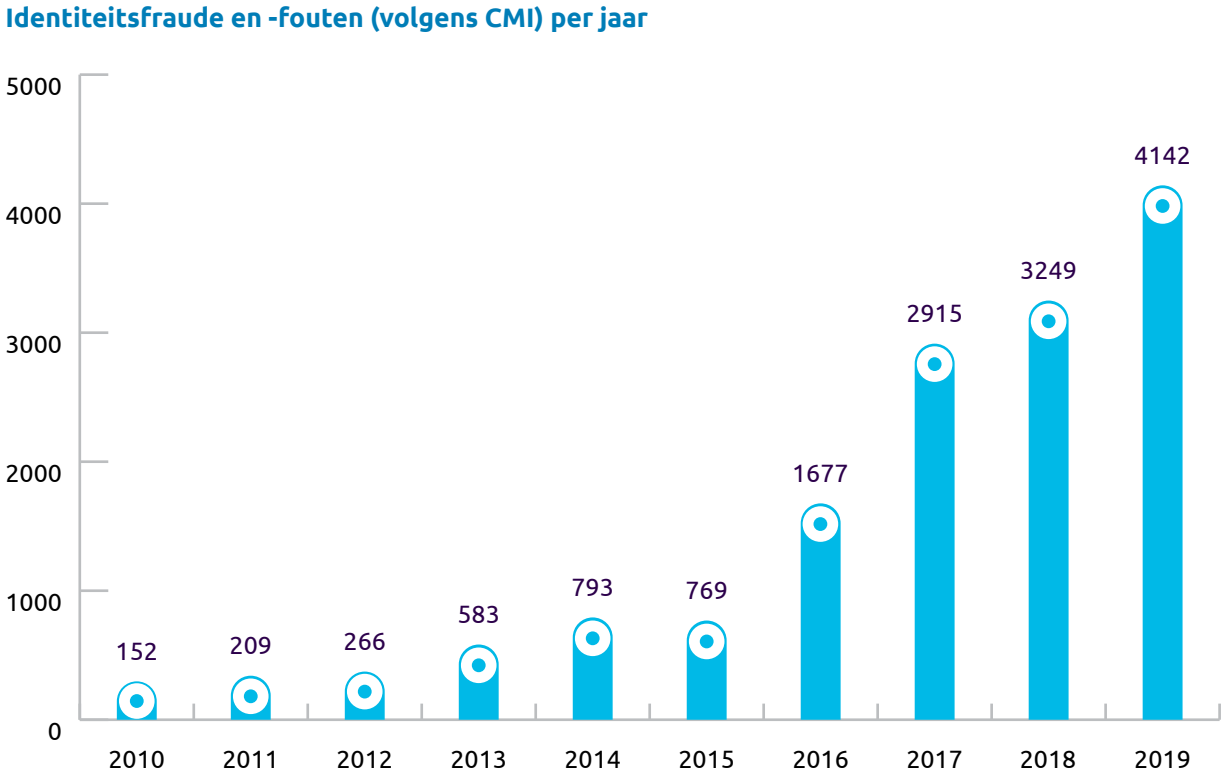
Met een AI-gedreven oplossing het toenemend probleem van identiteitsfraude onder de knie krijgen.

De strijd tussen orde en criminaliteit is een voortdurend fenomeen in de maatschappij waarbij innovatie een cruciale rol speelt voor beide kanten. Uit onderzoek van Europol[1] in 2020 blijkt dat criminelen al langer gebruik maken van AI om aan geld of andere voordelen te komen.

Identiteitsdocumenten zijn de belangrijkste documenten die mensen bezitten en iedereen boven de veertien jaar is verplicht om over tenminste één identiteitsdocument te beschikken. Deze documenten bevatten de basisinformatie over het individu en zijn van belang tijdens officiële acties of evenementen zoals reizen, een bankrekening openen, een verzekering afsluiten, een politiecontrole etc.

Het is daarom bijzonder verontrustend dat de ontwikkeling en beschikbaarheid van geavanceerde beeldbewerking-technologieën en printtechnieken voor een toename aan identiteitsfraude zorgt. In de afgelopen zes jaar is deze criminaliteitsvorm binnen Nederland met meer dan 500% toegenomen.

Figuur 1: Aantal meldingen van identiteitsfraude bij het Centraal Meldpunt[2].



Dit betekent niet dat identiteitsdocumenten niet veilig genoeg zijn. Landen introduceren regelmatig nieuwe en ingewikkeldere echtheidskenmerken op de identiteitsdocumenten, juist om het fraudeurs zo moeilijk mogelijk te maken.

Echter, het probleem ligt aan de kant van de controlerende instanties. Overheidsinstanties zoals de politie of de Koninklijke marechaussee, maar ook instituten zoals banken of verzekeraars, moeten steeds ingewikkeldere en specifiekere controles uitvoeren om de echtheid van een identiteitsdocument te valideren. Hierbij is het belangrijk dat de middelen die men kan gebruiken meegaan met de tijd en dat deze controles dus goed ondersteund kunnen worden.

Uitdagingen op het gebied van documenten controle

Op het gebied van documentcontrole kunnen drie grote uitdagingen worden geïdentificeerd, waarmee tijdens het ontwikkelen van een applicatie rekening moet worden gehouden.

Complexiteit van identiteitsdocumenten

Een van de grootste uitdagingen bij de controle van identiteitsdocumenten is de document-complexiteit. Er zijn rond de tweehonderd landen op de wereld waarvan eenieder eigen identiteitsdocumenten heeft. Per land kom je vaak meer dan tien verschillende geldige typen en modellen tegen[3]. Voorbeelden daarvan zijn gewone en dienstpaspoorten, ID-kaarten en verblijfsvergunningen. Elk document heeft tussen de vijftig en honderd echtheidskenmerken. Deze kunnen worden gecategoriseerd in gestandaardiseerde afspraken[4] in de structuur van een document en land- en of model-specifieke echtheidskenmerken op het document. Bijvoorbeeld het standaard controlegetal in een MRZ (Machine-Readable-Zone, onderaan op het paspoort) of een land-specifiek hologram[5].

De complexiteit van documenten is dusdanig dat forensische documentexperts nodig zijn met gespecialiseerde apparatuur om alles te kunnen onderzoeken. Deze kennis en middelen zijn bij veel mensen en bedrijven niet of onvoldoende beschikbaar. Bovendien zijn er ook echtheidskenmerken die niet bij iedereen bekend (mogen) zijn. Tenslotte zijn er ook processen te bedenken waar het aan voldoende tijd ontbreekt om diepgaande controles uit te voeren.

De complexiteit van vorm en structuur van identiteits-documenten is duidelijk een uitdaging voor geautomatiseerde processen. Naast de vorm levert ook de inhoud van de documenten problemen op.

Privacygevoelige gegevens

Een tweede uitdaging bij het ontwikkelen van een applicatie ter validatie van identiteitsdocumenten is het gebrek aan data. Identiteitsdocumenten bevatten persoonlijke en gevoelige gegevens over de houder, waardoor de scans niet opgeslagen en bewaard mogen worden voor de ontwikkeling van een AI-model. Echter, voor een volledige AI-oplossing zijn grote hoeveelheden documenten nodig. Hierbij zou het niet voldoende zijn om alleen authentieke documenten in de dataset te hebben, maar is het juist belangrijk om ook tientallen voorbeelden van (realistisch) vervalste echtheidskenmerken voor elk document te gebruiken. Dit is praktisch niet haalbaar, omdat voor elk echtheidskenmerk niet zo veel vervalsingen bekend of te vinden zijn.

Overigens worden documenten ook door landen uitgegeven die zich niet goed aan de normen houden of waar productiefouten zijn ontstaan. Dit betekent dat ook daarvan voorbeelden aan het AI-model moeten worden gevoerd, zodat deze leert dat afwijkingen kunnen bestaan en deze geen vervalsingen zijn.

De gevoeligheid van de gegevens en menselijke fouten in het productieproces zorgen ervoor dat een volledige AI-oplossing niet van toepassing kan zijn op de controle van identiteits-documenten. Dat komt niet alleen door de documenten zelf v, ook de bron van de data zorgt voor beperkingen in de applicatie.

Technische limieten van de scanapparatuur

Als derde uitdaging zijn er technische limieten van de huidige scanners en controleprocessen. Ondanks dat er regelmatig nieuwe scanners op de markt komen[6] met hogere resoluties en extra functionaliteiten, waardoor heel kleine tekst (zogenaamde microprints) kan worden herkend, zullen altijd echtheidskenmerken bestaan, die niet via scans kunnen worden gecontroleerd. Landen ontwikkelen bewust echtheidskenmerken die alleen op het fysieke identiteitsdocument en met behulp van specialistische forensische apparatuur kunnen worden gecontroleerd. Gangbare documentscanners kunnen dus bepaalde echtheidskenmerken niet zien. Daarnaast hebben sommige controle-instanties, zoals bijvoorbeeld de politie, niet altijd de mogelijkheid om deze geavanceerde scanners te gebruiken, omdat deze scanners op straat niet mee kunnen worden genomen.

Dit heeft als gevolg, dat de applicatie, die wordt gebruikt voor een automatische controle beperkt is door de technische limieten en de beschikbaarheid van de scanners.

Hybride AI-oplossingen als toekomstbestendige applicatie

Hoe kan het best gebruik gemaakt worden van bestaande technologieën om deze uitdagingen aan te gaan?

De toegevoegde waarde van documentsjablonen

In eerste instantie is het belangrijk om op een slimme manier de informatie over de verschillende echtheidskenmerken en documenten te verzamelen en op te slaan. Er zijn meerdere verzamelingen van deze informatie, zoals PRADO[7] en Edison[8], publiek beschikbaar. Met deze informatie kunnen voor elk type en model van een identiteitsdocument aparte

documentsjablonen worden aangemaakt, die als basis voor de applicatie dienen. Hierbij is het aan te raden om rekening te houden met herhalende elementen of structuur eigenschappen, zoals bijvoorbeeld de ICAO standaarden om de benodigde opslag in de database en de hoeveelheid werk van de invoerende mensen te minimaliseren.

Op die manier kan een database worden gecreëerd, die sjablonen voor ieder bekend identiteitsdocument bevat met de bijhorende echtheidskenmerken, variaties en controles. Deze documentsjablonen maken de complexiteit van de identiteitsdocumenten beheersbaar en stellen de applicatie in staat naast de standaard ICAO controles ook land- en model-specifieke controles toe te passen.

De uitdaging met betrekking tot de vorm van de documenten kan aldus worden verholpen door het gebruik van documentsjablonen, maar hoe staat de uitdaging rondom de gevoeligheid van de gegevens?

Toegepaste generieke AI

Het gebrek aan data voor een volledige AI-oplossing betekent niet dat de kracht van AI niet alsnog kan worden gebruikt voor de validatie van identiteitsdocumenten. Het is mogelijk om het validatieproces op te knippen in zodanig generieke stappen, waarvoor gespecialiseerde AI-componenten kunnen worden ontwikkeld. Deze AI-componenten zouden dan met minder data of niet privacygevoelige data uit kunnen komen.

Figuur 2: Validatieproces opgeknipt in generieke stappen met gespecialiseerde AI-componenten.

Zo kan voor het herkennen van het juiste documentsjabloon (classificatie van het documenten) een Deep Learning model worden gebruikt, welke nieuwe gescande documenten kan vergelijken met een database bestaande uit maar één voorbeeld (specimen-)document per documentsjabloon. Deze stap is belangrijk om de land- en model-specifieke informatie voor een gescand document uit de database op te halen.

Daarnaast kan voor het uitsnijden van het document uit de scan object herkenning worden gebruikt. De AI hiervoor kan worden getraind op alle soorten documenten en scans, waardoor de gevoelige data kan worden omzeild. Gezichtsherkenning, zoals degene op mobiele telefoons, maakt het mogelijk om de foto van het document te vergelijken met een live-opname van de houder. De tekst van het document kan worden uitgelezen door de nieuwste OCR (Optical Character Recognition) technieken, om deze in een latere processtap verder te verifiëren.

Voor al deze gespecialiseerde AI-componenten zijn geen gevoelige identiteitsdocumenten en gegevens nodig. In plaats van een volledige AI-oplossing kan het dataprobleem dus worden verholpen door slim gebruik te maken van meerdere en specifiekere AI-componenten. Bovendien is er controle over welke stappen op welke manier worden uitgevoerd en kan een 'black box' fenomeen worden voorkomen. Deze aanpak levert betrouwbaardere en beheerbaardere resultaten op en maakt tegelijkertijd gebruik van de nieuwste vooruitgang op het gebied van AI.

Omgang met technische limieten

Het probleem van de technische limieten van de scanners en het scanproces kan niet door een applicatie worden opgelost. Om een volledige documentinspectie toe te passen is en blijft het noodzakelijk het fysieke identiteitsdocument handmatig te controleren. Hierbij is een door technologie ondersteunde handmatige controle aan te raden, om het eerder geconstateerde probleem van de complexiteit te verhelpen en menselijke fouten te minimaliseren.

In eerste instantie kan de classificatie uit de applicatie worden (her-)gebruikt om het juiste documentsjabloon voor de handmatige inspectie te tonen. Dit bespaart tijd. Daarnaast kan het overzicht van het documentsjabloon zo worden ingericht, dat de controleur stap voor stap door de handmatige inspectie, die bij dit specifiek document hoort, wordt geleid. Hierdoor wordt ervoor gezorgd dat alle te controleren echtheidskenmerken op de juiste manier worden gecontroleerd. Daarnaast biedt een overzicht nog de mogelijkheid om aanvullende informatie aan de controleur te tonen. Zo kan bijvoorbeeld een alert voor bekende vervalsingen voor het getoonde document verschijnen, zodat hier extra aandacht aan wordt besteed.

Deze aanpak kan ook bij de politie worden gebruikt om het gebrek aan documentenscanners op straat te verhelpen. Via hun mobiele telefoon zouden zij naast de automatische controle via de camera ook toegang kunnen krijgen tot de handmatige inspectie, om grondigere controles uit te kunnen voeren.

De toevoeging van een stapsgewijze handmatige inspectie omzeilt de technische limieten van scanners door de overige echtheidskenmerken door een mens handmatig te laten controleren.

Samen tegen identiteitsfraude

Identiteitsfraude is een steeds groter wordend risico voor de veiligheid van ons land en systemen. Landen zullen steeds meer en complexere echtheidskenmerken in hun identiteitsdocumenten gaan verwerken om het fraudeurs zo moeilijk mogelijk te maken. Hierdoor hebben overheidsinstanties en andere instituten slimme, schaalbare en toekomstbestendige tools nodig om deze kenmerken te kunnen blijven controleren.

De gevoeligheid van de persoonsgegevens houdt de implementatie van volledige AI-oplossingen, zoals we deze op andere gebieden zien, tegen. Daardoor moeten controle-instanties overstappen naar gespecialiseerde AI-componenten om met de technologische vooruitgang mee te gaan en de kracht van AI in de toekomst alsnog te gebruiken.

[1]Europol onderzoek: https://www.europol.europa.eu/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

[2]Monitor Identiteit 2019 - Bezit, gebruik en misbruik van identiteitsmiddelen, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/02/29/monitor-identiteit-2019/Monitor+Identiteit+2019.pdf

[3]PRADO archief: https://www.consilium.europa.eu/prado/en/search-by-document-country.html

[4]ICAO richtlijnen: https://www.icao.int/publications/pages/publication.aspx?docnum=9303

[5]PRADO glossary: https://www.consilium.europa.eu/prado/en/prado-glossary/prado-glossary.pdf

[6]Nieuwe scanner “Osmond”: https://adaptiverecognition.com/osmond/specifications/

[7]PRADO: https://www.consilium.europa.eu/prado/en/prado-start-page.html

[8]Edison: http://www.edisontd.net/

Auteur

Kilian Toelge
Data Scientist & Software Architect

kilian.toelge@capgemini.com

Kilian is gespecialiseerd in het maken van toegesneden AI-oplossingen. De afgelopen jaren is hij bezig met het ontwerpen en ontwikkelen van een applicatie ter validatie en controle van identiteitsdocumenten doormiddel van AI in de publieke sector.

Sturen op intelligence in samenwerkingsverbanden

Op welke wijze kan een samenwerkingsverband sturen op het intelligence-proces om daadwerkelijk impact op de ondermijnende criminaliteit te maken?

Highlights

- **Ontwikkel een gezamenlijke taal, scope en stel een te bewerken effect op het domein vast en blijf deze continu ontwikkelen.**
- **Richt het intelligence-proces vanaf de start samen met de sturing dynamisch en kortcyclisch in.**
- **Prioriteer vanuit een strategisch, objectief beeld van het domein.**
- **Richt een lerende organisatie in door de effecten van de interventies te evalueren.**
- **Zet in de bouwfase de gelijkwaardige netwerksamenwerking in de aanpak centraal.**

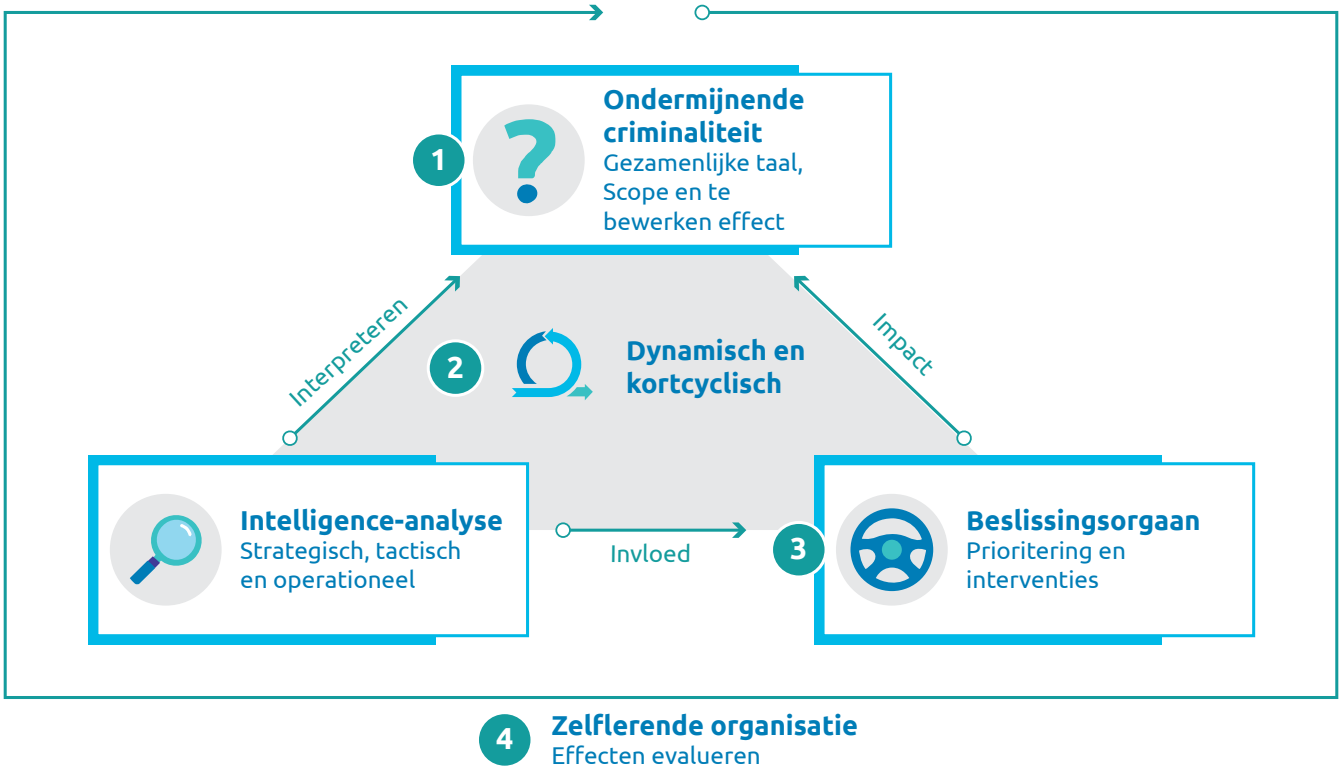
Intelligence wordt vaak gezien als een technisch of privacyvraagstuk, maar gerichte intelligence staat en valt bij een sturingsstrategie opgebouwd vanuit de samenwerking.

De moord op de advocaat Derk Wiersum in 2019 heeft de Nederlandse rechtstaat opgeschud en men realiseert zich hierdoor dat justitie meer grip op ondermijnende criminaliteit moet krijgen. Daarom is begin 2020 het zogenoemde Multidisciplinair Interventie Team (hierna: MIT) gelanceerd, een samenwerkingsverband van zes overheidsorganisaties (Politie, Openbaar Ministerie, KMar, douane, belastingdienst en FIOD). Het MIT moet de data en expertise uit deze organisaties gaan gebruiken om onder andere nationale en internationale barrières op te werpen voor crimineel handelen en voor het verkrijgen van crimineel geld. De hoeksteen van de werkwijze is het creëren van intelligence op ondermijnende criminaliteit.

Dergelijke initiatieven worden gelanceerd op de premisse: 'Data is de nieuwe olie van deze tijd, die wij moeten ontginnen'. Echter, bij het daadwerkelijk ontginnen van deze zogenaamde 'olie' komt veel meer kijken, voordat het daadwerkelijk in de samenwerking gebruikt kan worden. Data heeft namelijk op zichzelf geen waarde, net zoals olie uit de grond, moet deze eerst worden verwerkt. Het gaat dan over intelligence. Voordat we hierop ingaan is het belangrijk om een begrip te hebben van de definitie van 'intelligence'. Hierin staat namelijk de beslissing om impact te maken op een domein centraal, weliswaar op basis van de betekenisvolle data en kennis over het (criminele) domein. Het is dus een samenspel van data, kennis over het criminele domein en de beslissing of impact die men daarop wil maken.

De reflex van intelligence samenwerkingsverbanden is om veel focus op de techniek en juridische uitdagingen te leggen: 'als we maar alle data bij elkaar (mogen) zetten, dan hebben we meer inzicht en krijgen we meer grip op het domein'. Toch is dit slechts een deel van het verhaal en miskent dit de noodzakelijke aandacht voor een deugdelijke sturingsstrategie op het intelligence-proces en daarmee de samenwerking tussen de verschillende partijen. De huidige praktijk drijft namelijk veelal op incidenten. Het is daarom de vraag of er niet met de kraan open wordt gedweild. Is het oppakken van een kopstuk van een criminele organisatie de meest strategische keuze, staan er dan niet al drie nieuwe klaar om het over te nemen? Daarom is een duidelijke sturings- en samenwerkingsstrategie nodig om de intelligence gerichter in te zetten en daardoor strategisch, adaptief en informatiegestuurd impact te kunnen maken op ondermijnende criminaliteit.[1] Hieronder worden vier bouwstenen uiteengezet die nodig zijn voor een sturings- en samenwerkingsstrategie, die opgebouwd zijn op basis van ervaringen van Capgemini Invent.

Figuur 1: Gebaseerd op het model van Ratcliff (the structure of strategic thinking, Sidney: Federation Press, 2009).



Bouwsteen 1 - Ontwikkel een gezamenlijke taal, scope en stel een te bewerken effect op het domein vast en blijf deze continu ontwikkelen

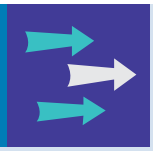
Het MIT is opgericht om criminele netwerken en bedrijfsprocessen duurzaam te verstoren. De zes betrokken organisaties hebben diverse perspectieven op het domein, dat is juist de kracht van de bundeling. Echter, – 'elk voordeel heb zijn nadeel' – onderken dat deze organisaties ook verschillende ideeën of invullingen bij het samenwerkingsverband hebben en het samenbrengen daarvan een cruciale stap is. Dat is niet alleen voor de vraag naar de scope van het samenwerkingsverband, maar zeker ook voor de invulling van specifieke definities, zoals tactisch/operationeel[2] of de term ondermijning en wat dat voor het samenwerkingsverband betekent. Dat geldt ook voor termen die op het eerste gezicht bijvoorbeeld vanuit juridisch perspectief heel duidelijk zijn, zoals bij witwassen. Naast de gemeenschappelijke taal en scope voor de samenwerking is het definiëren van het te bewerken effecten op het domein een belangrijke stap in de sturingsproces en samenwerking; bijvoorbeeld het verminderen van het zwart geld in Nederland. Dit vormt de basis van het sturingsmechanisme en de onderlinge samenwerking. Welke samenwerkingsorganisatie draagt wat en op welke wijze bij aan deze effecten? Het sturingsmechanisme moet bewust en continu worden ontwikkeld op basis van het lerende vermogen van de organisatie (zie bouwsteen 4).

Bouwsteen 2 - Richt het intelligence proces vanaf de start samen met de sturing dynamisch en kortcyclisch in

In het huidige intelligence landschap worden intelligence producten verwerkt tot een advies en worden deze voorgelegd aan een stuurgroep die vervolgens een besluit neemt over het advies. Hierdoor stuurt – ondanks de naam van de groep – de stuurgroep niet op de intelligence, maar op de adviezen van de analist(en). De sturing op het intelligenceproces moet worden gezien als een trechter, waarin vanaf een breed inzicht op het domein naar concrete operationele interventies continu tussentijdse besluiten worden genomen. Tussen deze diverse stappen zitten legio beslissingen, bijvoorbeeld inzicht krijgen in het bedrijfsproces van een criminele organisatie, simpel gezegd productie, opslag, distributie en witwassen.

Het kortcyclisch en dynamisch sturen vanaf de start van het intelligenceproces, namelijk verzamelen van de noodzakelijke data, zorgt voor een betere inzet van capaciteit en keuzes van de uit te voeren interventies. Daarnaast worden inzichten gedemocratiseerd en kunnen partijen continu keuzes maken en eventueel bijsturen in het intelligenceproces, duiding geven aan het domein en prioritering aanbrengen. Intelligence is hierdoor – anders dan in het huidige proces – geen lineair proces van verzamelen, verwerken in een datawarehouse, analyseren en het nemen van interventies, maar een dynamisch en kortcyclisch proces waarin de samenwerkingspartners in gezamenlijkheid vanuit hun expertise sturing aan geven.

Bouwsteen 3 - Prioriteer vanuit een strategisch objectief beeld van het domein



Strategische intelligence[3] geeft de organisatie richting en kan de organisatie helpen bij het maken van (prioriterings)beslissingen van de beperkte capaciteit in toezicht, opsporing en analyse. Bij het opstellen van de strategische intelligence is het zaak om dit beeld zo objectief mogelijk op te stellen. In samenhang met de kortcyclische en dynamische werkwijze is het verstandig om een strategisch beeld op te bouwen vanuit één databron dat vanuit een specifiek systeem, fenomeen of thema steeds wordt verrijkt met een nieuwe databron, zodat inzichten worden verrijkt en nieuwe analysevragen ontstaan.[4] Na een prioritering op het strategische beeld (markt, culturele aspecten, geografische verdeling en onderlinge verhoudingen) kunnen tactische (onder andere fenomenen of criminele samenwerkingsverbanden) en operationele intelligence (onder andere subjecten, objecten en systemen) worden verzameld. Het aanbrengen van deze gelaagdheid in de intelligence is noodzakelijk om onderbouwd prioriteiten aan te brengen en gericht te sturen op capaciteit.

Het criminele domein is niet statisch, daarom moet het beeld periodiek worden bijgesteld in het proces door bijvoorbeeld kennis met betrekking tot de 'modus operandi' van criminelen ('hoe ze werken') te verwerken of een effect van een specifieke interventie.

Bouwsteen 4 - Richt een lerende organisatie in door de effecten van de interventies te evalueren

Interventies worden met een bepaald beoogd effect op het domein genomen, zo moet het MIT naast strafrechtelijke interventies een breder handelingsperspectief hebben om de ondermijnende criminaliteit aan te pakken, door nationale en internationale barrières op te werpen. Een voorbeeld daarvan is het maken van afspraken met private partijen om witwassen te beperken. Om te bepalen of een interventie effect heeft gehad is een evaluatiemodel nodig om enerzijds (maatschappelijke) verantwoording af te leggen en anderzijds een lerende organisatie neer te zetten. Het resultaat van de kortcyclische evaluatie- en effectmetingen kunnen invloed hebben op de analyses voor de intelligence, bijsturing op de genomen of nieuwe interventies en begrip van de werking van het domein.

Een evaluatie- en effectmeting is niet een sluitstuk van het proces, maar vormt onderdeel van de beslissing voorafgaand aan de interventie. Hierdoor kunnen interventie nader worden onderbouwd en nadien ook worden verantwoord. Daarvoor is het belangrijk om in het samenwerkingsverband de volgende vragen te bespreken voorafgaand aan de beslissing over de interventies:

1. Welk beoogd effect wordt met de interventie bereikt en welke (mogelijke) neveneffecten en exogene factoren[5] kent de interventie?
2. Op welke wijze kunnen deze worden gemeten (kwalitatief of kwantitatief)?
3. Binnen welke termijn worden de (eerste) effecten verwacht?

Het MIT heeft de kans om ondermijnende criminaliteit duurzaam te bestrijden en de ingrediënten voor dat succes liggen op tafel, namelijk bestuurlijke en politieke commitment, middelen en veel ervaring in het bestaande landschap. Daarin moet worden onderkend dat het bouwen van en samenwerken in een nieuwe organisatie met zes partners een complexe opgave is en dat het veel tijd kost. De partners zijn namelijk in de basis gelijkwaardig aan elkaar en werken gezamenlijk aan een complex maatschappelijk probleem, zonder dat één partner doorzettingsmacht heeft. Dat zorgt voor een additionele dimensie op de sturingsstrategie. Daarom vraagt de implementatie van de vier besproken bouwstenen een gestructureerde aanpak waarin het vraagstuk allereerst wordt gekaderd, de inzet wordt ingericht, de uitvoering wordt gemobiliseerd en vervolgens geborgd en het netwerk en organisatie verder worden gebracht. De methode van Empowering Ecosystems van Capgemini Invent geeft daar een gerichte invulling aan en kan het MIT helpen bij de invulling van het sturingsmechanisme op de intelligence en de implementatie daarvan in het complexe samenwerkingsverband.[6]

[1]Ratcliff, the structure of strategic thinking, Sidney: Federation Press, 2009 en NJSP Investigations Branch. 2006. "Practical Guide to Intelligence-Led Policing"

[2]De invulling van tactiek en operationeel verschillen bijvoorbeeld tussen de politie en militaire organisaties.

[3]Johnson, L. (2007). Introduction. p. 1-16 in: L.K. Johnson (Ed.). Handbook of intelligence studies. London; New York: Routledge: 'Strategische intelligence': kennis en voorkennis van de wereld om ons heen, gericht op besluitvorming en actie.

[4]NJSP Investigations Branch. 2006. "Practical Guide to Intelligence-Led Policing"

[5]Zoals het dalen van de criminaliteit door corona.

[6]https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2019/07/06-027.19a-Factsheet-Empowering-Ecosystems-Dutch_web.pdf\

Auteur

Marcus van der Velpen
Managing Consultant

marcus.vander.velpen@capgemini.com

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 en centrale rol vervult.

Wendbaar en ‘in control’ blijven in de risicosamenleving: de toepassing van Artificial Intelligence (AI) in een risicomanagementsysteem

Op welke wijze kunnen een ISMS en AI bijdragen aan cyber-risicomanagement van een organisatie?

Highlights

- Risicomanagement is essentieel voor organisaties om in control te zijn over de belangrijkste strategische, preventieve, cyber en externe risico's.
- Cyber-risico's nemen per jaar exponentieel toe en vormen een separate risicocategorie die een andere wijze van management nodig heeft.
- Een ISMS helpt een organisatie om zich te weren tegen cyber-risico's zonder de businessdoelen uit het oog te verliezen.
- Organisaties zijn op zoek naar mogelijkheden om risicomanagement te automatiseren en kunnen daarbij ook AI inzetten.
- Organisaties zullen in toenemende mate een ISMS moeten gaan integreren met hun business om in control te blijven over risico's.

Risicobeheersing is relevanter dan ooit. Nog nooit in de geschiedenis is men zo bewust geweest van alle risico's waar we aan blootgesteld worden.

De opkomst van de risicosamenleving en haar digitale veiligheid

Wanneer men tegenwoordig denkt aan het concept 'veiligheid', dan is dit onlosmakelijk verbonden met het concept 'risico'. Veiligheid staat namelijk gelijk aan de perceptie of men gevaar loopt. Het was de socioloog Ulrich Beck (1992) die als eerste deze link legde tussen veiligheid en de perceptie van risico's. Hij stelde zelfs dat onze huidige samenleving getypeerd kan worden als een 'risicosamenleving'. Hij wijst op twee belangrijke trends die onze risicosamenleving kenmerken.

Ten eerste stelt hij dat modernisering onze samenleving een hoop voorspoed en welvaart heeft gebracht. Echter, deze voorspoed heeft tevens tot gevolg dat wij worden blootgesteld aan vele nieuwe risico's. Zo heeft de digitalisering van de samenleving veel nieuwe kansen geboden op vooruitgang, maar creëert deze tegelijkertijd ook nieuwe cyber-risico's. Veiligheidsregio's weten dat veel risico's in de omgeving zijn 'verborgen', doordat de omvang, aard en ernst van cyber-risico's niet goed in beeld zijn (IFV, 2019). Boutellier (2005) stelt dat politieke sturing daardoor minder is gaan draaien om ideologische tegenstellingen, maar meer om vormen van expertkennis. De dreiging en de beheersing van cyber-risico's is een steeds belangrijker thema in de politiek geworden.

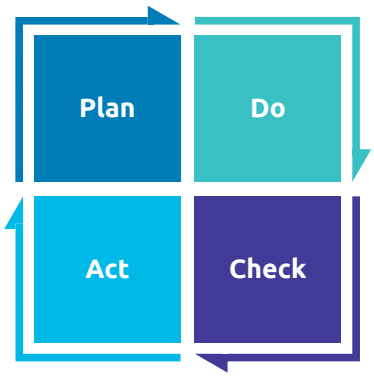
Ten tweede stelt Beck (1999) dat de burger zich door de modernisering tegelijkertijd steeds bewuster is geworden van deze risico's en dreigingen. Dit komt onder meer door technologische ontwikkelingen die ons beter in staat stellen om cyber-risico's te duiden en te voorspellen. Mensen willen zich zoveel mogelijk weren tegen deze waargenomen dreigingen en passen zich aan om deze cyber-risico's af te zwakken of te verdelen. Voorbeelden hiervan zijn de klimaatmodellen van de IPCC en de pogingen om klimaatverandering tegen te gaan met duurzaamheidstrategieën. Verder kan de opkomst van technologieën zoals Artificial Intelligence (AI) ondersteuning bieden bij het herkennen van cyberdreigingen (Gartner, 2020b). Burgers zijn zich nog nooit zo bewust geweest van het bestaan van risico's en lijken niet meer bereid deze te dragen (van der Woude, M. & van Sliedregt, E, 2007).

De digitalisering van de samenleving heeft significante effecten op de huidige risicosamenleving. Aan de ene kant plukken organisaties de vruchten van de mogelijkheden die digitalisering met zich meebrengt. Aan de andere kant worstelen ze ook met nieuwe en onvoorziene risico's die hierdoor zijn ontstaan. Het is dus niet verwonderlijk dat de Nationaal Coördinator Terrorismebestrijding en Veiligheid (2020) digitale veiligheid zelfs een randvoorwaarde noemt voor het functioneren van de nieuwe digitale maatschappij.

Een ISMS geeft op efficiënte wijze sturing aan risicomanagement van een organisatie

Op organisatieniveau moeten spelers in de publieke sector methoden ontwikkelen en toepassen om zich te kunnen blijven wapenen tegen gebeurtenissen in de risicosamenleving, door middel van risicomanagement. Dit moet met rust, beleid en overzicht gebeuren. Het is daarbij essentieel dat cyber-risicomanagement in lijn is met de organisatiestrategie en dat het de organisatiedoelen ondersteunt. Om cyber-risicomanagement zo effectief mogelijk te laten verlopen kan een Information Security Management System (ISMS) worden opgezet. Dit is een procesgerichte benadering voor informatiebeveiliging, waarin het risicobeheersproces centraal staat. Het doel van het ISMS is om continu te blijven beoordelen of beveiligingsmaatregelen passend en effectief zijn en of deze bijgesteld moeten worden (IBD, 2019). Dit maakt het ISMS een onmisbaar gereedschap voor een organisatie haar risicomanagement.

Figuur 1: De vier fasen van de ISMS-cyclus worden doorgaans als Plan-Do-Check-Act omschreven.



Om een ISMS op te zetten voeren organisaties een risicoanalyse uit binnen het gekozen kader. Het staat organisaties vrij om daarvoor een eigen methode te definiëren. Voor een goede uitvoering is het voornamelijk essentieel dat dezelfde methodiek consistent wordt toegepast. Een belangrijk denkmodel is bijvoorbeeld dat van Kaplan & Mikes (2012), waarin risico's worden ingedeeld in strategische, preventieve en externe risico's met cyber als een additionele categorie. Risico's worden zo geclassificeerd en binnen de context van de organisatie gewogen. Dit helpt om te bepalen op welke manier ze beheerst moeten worden. Daarnaast zijn de ISO27005, NIST 800-30, COSO ERM 2017 en ISO31000 veelgebruikte raamwerken om de waarschijnlijkheid en impact van risico's in beeld te krijgen en te mitigeren. Het geheel van alle activiteiten die ondernomen gaan worden om de risico's te beheersen legt men vast in het informatiebeveiligingsplan. Dit wordt periodiek getoetst om te kijken of er correcties uitgevoerd moeten worden. Zo ontstaat er een leercyclus die ervoor zorgt dat een organisatie alert blijft om effectief te kunnen reageren op veranderingen in het risicolandschap.

Om het belang ervan te kunnen aantonen dat organisaties snel moeten kunnen sturen op veranderingen in het risicolandschap, hoeft men niet verder te kijken dan de actualiteit. COVID-19 heeft in een zeer korte tijd significante verstoringen veroorzaakt in onze samenleving. Gartner (2020a) wijst daarom op de nieuwe risico's die worden veroorzaakt door deze pandemie. Ons werkende leven is door COVID-19 in rap tempo verder gedigitaliseerd. Deze ontwikkeling heeft het risicolandschap van overheden sterk beïnvloed. Zo is er bijvoorbeeld een sterke toename waar te nemen in transformaties van lokaal naar cloudopslaggebruik of in het gebruik van andere diensten van derde partijen. Daarnaast vallen veel werknemers door thuiswerken niet meer onder de gebruikelijke controlemaatregelen, waardoor kwetsbaarheden ontstaan en risico's toenemen. Ten slotte is er geen zekerheid over de mate waarop deze situatie het 'nieuwe normaal' betreft. Er bestaat een kans dat organisaties over een jaar weer terug moeten veranderen als het coronavirus onder controle is.

Gezien het aantal cyber-risico's en de complexiteit daarvan lijkt het lastig om weerbaar te blijven in het dynamische risicolandschap. De opkomst van nieuwe technologieën, zoals AI, zou onze weerbaarheid kunnen versterken.

Wat is Artificial Intelligence?

Artificial Intelligence is een technologie die zich richt op het repliceren van menselijk gedrag door middel van slimme algoritmes. Belangrijkste randvoorwaarden voor het functioneren van een AI zijn de kwaliteit en kwantiteit van beschikbare data. Deze datasets worden vervolgens gebruikt voor het trainen van het AI-algoritme en het slimmer maken ervan. Onvoldoende data of data van onvoldoende kwaliteit kan als gevolg hebben dat de AI een bias of inaccurate output creëert. Wanneer we AI willen inzetten om organisaties weerbaarder te maken, bijvoorbeeld door middel van het integreren van AI binnen het ISMS, is het van belang om bias zo veel mogelijk te reduceren. Naast de vele organisaties die geavanceerde technologieën zoals AI inzetten, ziet ook de Europese Commissie hier de toegevoegde waarde van in. Zij investeert maar liefst 2.5 biljoen euro in het ontwikkelen van AI-capaciteiten in Europa als onderdeel van het Digital Europe Programme (ENISA, 2020).

Hoe kan Artificial Intelligence worden ingezet om een ISMS te verbeteren?

AI wordt in het cybersecuritydomein al industrie-breed ingezet voor het herkennen van en waarschuwen voor malwareaanvallen of phishing. Daarnaast kan AI helpen bij het identificeren van abnormaal gedrag en het bijhouden en voorspellen van cyber-risico's in een veranderlijk dreigingslandschap. Dit kan worden gerealiseerd door middel van 'predictive analytics' en het is mogelijk om deze methode

te combineren met een GRC-tooling. Zo zien we dat AI in toenemende mate wordt ingezet bij digitale transformaties om het risicomanagement van bedrijfsprocessen slimmer en sneller te maken.

Cybersecurityrisico's nemen bijna dagelijks toe en aanvallers zetten in toenemende mate geavanceerde technologieën als AI in, om in te breken bij systemen en hierdoor waardevolle data buit te maken. Om deze vormen van aanvallen bij te houden zullen verdedigers ook gebruik moeten gaan maken van AI. Dit benadrukt de urgentie voor organisaties om dergelijke technologieën in te zetten om informatiesystemen goed te beveiligen. Er zijn hierbij tal van mogelijkheden. Dit kan bijvoorbeeld door de inzet van 'AI-agents' tijdens het pentesten. Daarnaast kan AI een bijdrage leveren aan een Intrusion Detection System bij het vroegtijdig signaleren of voorspellen van cyberaanvallen. Daarnaast kunnen 'supervised learning models' gebruikt worden bij analyseren van netwerkverkeer, het monitoren van firewalls of het classificeren van data. Zo levert AI al een bijdrage aan veel bestaande verdedigingsmechanismen van een organisatie, zodat de organisatie opgewassen is tegen de toenemende dreigingen.

Ook binnen het ISMS kan AI veel toevoegen. Bijvoorbeeld bij het automatiseren van standaardactiviteiten en het voorspellen van risico's. Dit helpt bij het borgen van informatiebeveiliging, wat cruciaal is binnen het veiligheidsdomein. AI zou het risico-analyseproces in sommige gevallen automatisch kunnen laten verlopen. Verder zou de toepassing van AI het ISMS naar een meer monitorende functie binnen de organisatie kunnen sturen. Daarnaast kan AI een rol spelen bij het voorspellen van incidenten. Op basis van kansberekeningen kan AI abnormale activiteiten verbinden aan risico's en het dreigingsniveau inschatten. Dit 'smart cyber risk management' helpt bij het prioriteren van mitigatie-acties om risicomanagement efficiënter en effectiever te laten verlopen. Hierbij is het wel van belang dat de besluitvorming van de AI over deze risicoprofielen transparant en verklaarbaar blijft. Voornamelijk als de AI-output zal worden gebruikt voor Risk en Compliance-activiteiten, zoals audits. Er zal altijd een menselijk oog op moeten worden geworpen om mogelijke technische fouten in het algoritme te ontdekken.

Slot

Nog nooit in de geschiedenis is men zich zo bewust geweest van risico's als nu. Er ontstaan dagelijks nieuwe risico's waar de samenleving aan blootgesteld wordt. Daarnaast moeten ook organisaties in het publieke domein manieren vinden om zich te blijven beschermen tegen het snel veranderende risicolandschap. Een efficiënte manier om dit te bereiken is de toepassing van een ISMS. Het ISMS introduceert een cyclisch informatiebeveiligingsproces waarmee een organisatie haar informatiebeveiliging periodiek herziet en aanpast. Het risico-analyseproces staat hierin centraal en het is aan elke organisatie zelf om een methodiek uit te kiezen die hierin uitgevoerd wordt. Door het periodiek uitvoeren van risico-analyse kan een organisatie haar controlemaatregelen herzien en monitoren of deze nog wel effectief zijn. De effectiviteit van een ISMS kan vergroot worden door toepassing van automatisering met AI. Het gebruik van AI binnen cybersecurity en risicomanagement neemt tegenwoordig sterk toe. De technologie kan ook veel toevoegen aan een ISMS. Dit komt doordat AI versterking kan bieden aan veel functies van het ISMS, door middel van predictive analytics of smart cyber risk management. Met name de combinatie van een ISMS met de aanvulling van AI zorgt ervoor dat organisaties in het veiligheidsdomein hun digitale weerbaarheid ook op lange termijn zullen blijven borgen.

Aanbevelingen

- Organisaties in het veiligheidsdomein moeten meegaan met de technologische ontwikkelingen om weerbaar te blijven tegen zowel interne als externe risico's. De kritische infrastructuur van Nederland moet voldoende beschermd blijven en dit kan bereikt worden door middel van innovatie.
- Organisaties kunnen een ISMS toepassen om de effectiviteit van haar risicomanagement te borgen, zonder hierbij de organisatiedoelen uit het oog te verliezen. Voor een optimale werking van een ISMS wordt deze ondersteund door een GRC-tool.
- Artificial Intelligence kan sommige functies van het ISMS automatiseren. Hiermee zou het ISMS een meer monitorende functie kunnen aannemen binnen de organisatie en de werkdruk voor de CISO verlichten.

Literatuur

- Beck, U. (1992). Risk Society (1ste editie). SAGE Publications.
- Beck, U. (1999). World Risk Society. Wiley.
- Boutellier, H. (2005). De veiligheidsutopie. Boom Lemma.
- ENISA. (2020). Artificial Intelligence Cybersecurity Challenges. https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

- Gartner. (2020a). 2021 Planning Guide for Security and Risk Management. https://www.gartner.com/en/doc/729015-2021-planning-guide-for-security-and-risk-management
- Gartner. (2020b). Tool: Use Cases to Seize AI Investment Opportunities. https://www.gartner.com/en/doc/732817-tool-use-cases-to-seize-ai-investment-opportunities
- IBD. (2019). Handreiking Information Security Management System (ISMS). https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/04/201902-Handreiking-Information-Security-Management-System-ISMS-v2.0.pdf
- Instituut Fysieke Veiligheid. (2019). Whitepaper digitale ontwrichting en cyber. https://www.ifv.nl/kennisplein/Documents/20190912-IFV-Whitepaper-digitale-ontwrichting-en-cyber.pdf
- Kaplan, R. S., & Mikes, A. (2012, juni). Managing Risks: A New Framework. Harvard Business Review. https://hbr.org/2012/06/managing-risks-a-new-framework
- Ministerie van Justitie en Veiligheid. (2020, 29 juni). Cybersecuritybeeld Nederland. Nationaal Coördinator Terrorismebestrijding en Veiligheid. https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland
- van der Woude, M., & van Sliedregt, E. (2007). De risicosamenleving: overheid vs. strafrechtswetenschap? Aanwijzingen voor het debat rondom veiligheid en risico's. Proces, 216–226. https://core.ac.uk/download/pdf/15601463.pdf

Auteurs

Marieke van de Putte
Lead Incubator Cyber Risk, Compliance and Enterprise Resilience

marieke.vande.putte@capgemini.com

Marieke is gespecialiseerd in het ontwikkelen van praktische aanpak van Risicomanagement & Compliance door automatiseren van controls - risico-analyse & controls en het inzetten van Risk & Compliance kennis bij de Digitale Transformatieprojecten van onze klanten.

Rutger Clijnk
Cybersecurity Consultant

rutger.clijnk@capgemini.com

Rutger is beleidssocioloog en criminoloog met een specialisatie in organisatievraagstukken omtrent de strategie en governance van cybersecurity. Tevens adviseert hij organisaties over de toepassing van een ISMS om hun risicomanagement te optimaliseren.

Mehrnaz Pour Morshed
Cybersecurity Consultant

mehrnaz.pour.morshed@capgemini.com

Mehrnaz is werkzaam als cybersecurity consultant bij Capgemini. Ze heeft een Msc. In Artifical Intelligence en kijkt graag naar het effect van menselijk gedrag op het gebruik van technologie in risicovolle situaties. Verder focust ze zich op Intelligent Cybersecurity Risk en Resilience bij diverse klanten.

Innovatie en ethiek in de forensische zorg: de juiste balans

Hoe borg je ethische aspecten bij het realiseren van nieuwe technologie met maatschappelijke waarde?

Highlights

- **Politieke gevoeligheid leidt tot terughoudendheid met technologische innovatie.**
- **Maatschappelijk vertrouwen in technologische innovatie is cruciaal.**
- **Redeneren vanuit ethische waarden leidt tot goed onderbouwde oplossingen.**
- **Een vooraf vastgesteld ethisch kader wordt getoetst in een pilot.**
- **De eisen voor ethische toepassing worden bij de pilotfase vastgelegd.**

Het vooraf definiëren van ethische waarden stelt organisaties in staat om de forensische zorg op een maatschappelijk verantwoorde wijze te innoveren.

De overheid streeft naar een geleidelijke en verantwoorde terugkeer van daders in de samenleving door de kwaliteit en effectiviteit van forensische zorg continu te optimaliseren. De forensische zorgketen zet daarvoor steeds vaker innovatieve technologieën in om de publieke veiligheid te vergroten. Kunstmatige intelligentie bijvoorbeeld, heeft de potentie om professionals te ondersteunen bij het maken van beter gefundeerde beslissingen ten behoeve van verlof, het door- en uitstromen in zorg of het herkennen van gevaarlijk afwijkend gedrag zoals suïcide en zelfmutilatie in isolatie.[1] Ook maken forensische zorgaanbieders al gebruik van virtual reality bij agressiepreventie om ervaringsgericht te behandelen in een realistische context, waarmee de grens tussen een gesloten setting en de buitenwereld vervaagt.[2] Het hoofddoel van forensische zorg is altijd het bijdragen aan terugdringen van delictgedrag met een passende behandeling en waar nodig beveiliging.

De razendsnelle ontwikkelingen in de techsector bieden nieuwe kansen om een (bestaand) probleem op te lossen, waarbij het cruciaal is om stil te staan bij de morele overwegingen binnen de forensische zorgketen. Het snijvlak waarop de forensische zorg zich beweegt en de impact die het heeft op de veiligheid van de samenleving maakt dat innovatie niet alleen draait om wát en hóe een probleem opgelost kan worden, maar vooral om wáárom iets opgelost dient te worden.[3] Een diepgaand begrip van de situatie geeft zorgaanbieders daarbij een mogelijkheid om in hun beleidsontwikkeling rekening te houden met wat er in de samenleving speelt.

Om tot een weloverwogen en onderbouwd besluit te komen over de inzet van technologische innovaties, dient een organisatie een gestructureerd proces te doorlopen om te voorkomen dat het in een onnavolgbare retoriek vervalt. Het vooraf definiëren van ethische waarden helpt inzichtelijk te maken welke opvattingen, belangen en achterliggende waarden een mogelijke oplossing bij verschillende betrokkenen oproept. Dit artikel beschrijft hoe het redeneren vanuit ethische waarden kan leiden tot een goed onderbouwde afweging voor de start van een pilot. Hierbij wordt gebruik gemaakt van een batenlogica, waarmee oplossingen en beleidskeuzes worden gekoppeld aan de doelstellingen van een organisatie. Zo wordt in één oogopslag duidelijk op welke vlakken waarde wordt gecreëerd.

Stap 1: van ethische bezwaren naar ethiek als waarde

Bij het overwegen van innovatieve oplossingen voor een geïdentificeerde kans of risico, heeft de overheid ook de rol om te bepalen of de oplossing de publieke waarden versterkt en beschermt. In een werkveld dat maatschappelijk erg gevoelig ligt, vraagt dat om een breed begrip van individuele opvattingen, (tegenstrijdige) belangen en emoties bij een mogelijke oplossing. Door ethiek als reflectieproces op te zetten aan het begin van het traject, stelt een organisatie zichzelf in staat om zulke waarden principieel en continu te blijven beoordelen en bijsturen om de forensische zorg op een maatschappelijk verantwoorde wijze te innoveren.

Uit ervaring blijkt dat het in kaart brengen van de diversiteit in (individuele) waarden en principes van betrokken partijen helpt bij het bepalen hoe innovaties kunnen bijdragen aan het vormgeven van de oplossing. Door gezamenlijk met een onafhankelijke gespreksleider te verkennen welke eerste reacties een initiatief oproept, wordt een afweging tussen belangen en alternatieven gemaakt. Grofweg kan daarin een positie worden aangenomen als voorstander, tegenstander of neutraal/twijfelachtig over de oplossing. Om dit inzichtelijk te maken hanteren we het verminderen van incidenten tijdens het verlof van cliënten met behulp van technologische innovaties als fictieve casus. Voorbeelden van eerste reacties die deze casus oproepen zijn:

- Wanneer technologie kan worden ingezet om nauwkeurigere voorspellingen te maken van de zorgbehoefte van onze cliënten moet dit niet worden tegengehouden.
- Bij nieuwe incidenten tijdens verlof is het lastig te bepalen wie de verantwoordelijkheid voor deze besluitvorming draagt: de technologie of een medewerker.
- Bij gevoelige casuïstiek is het wenselijk dat de inschatting van het recidiverisico altijd een menselijk besluit blijft.

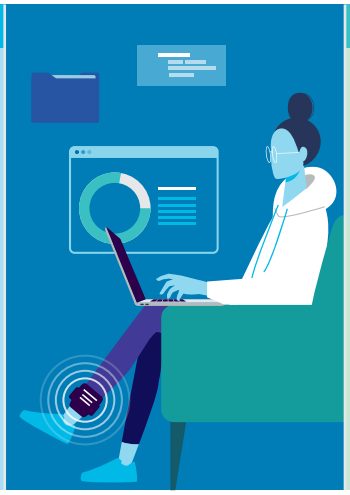
Op basis van deze gesprekken en reacties wordt bepaald welke feiten of informatie ontbreekt, zoals vragen over eigenaarschap ('Wie mag zo'n algoritme bouwen?'); vragen over relevantie van de oplossing ('Hoe vaak ontstaat een incident tijdens verlof,

en wat kan de meerwaarde van technologie dan precies hierin zijn?'); of vragen over de scope ('Over welke cliënten spreken we bij het maken van zo'n inschatting van recidiverisico?').

Na het vaststellen van deze kaders wordt een inschatting gemaakt hoe de waarden met elkaar conflicteren, en of dit kan leiden tot een ethisch maatschappelijk vraagstuk. Zo kan iemand die het inzetten van kunstmatige intelligentie in de zorg onmenselijk vindt zich bijvoorbeeld zorgen maken over de waarde van relationele zorgverlening. De belangrijkste waarden en principes worden in dat geval op groepsniveau met behulp van één concrete hoofdvraag in kaart gebracht om tot een gezamenlijk beeld te komen (zie Figuur 1).

Een afweging tussen objectiviteit, veiligheid en de persoonlijke benadering in de forensische zorg kan bijvoorbeeld leiden tot een uitgangspunt dat zo'n advies te allen tijde dienend moet zijn aan het oordeel van de behandelaren. Dit kan bijvoorbeeld door een voorselectie te maken van patiënten die een groter maatschappelijk risico tijdens het verlof lopen op basis van de beschikbare documentatie. Zodra de ethische kaders zijn gedefinieerd kan er een volgende stap worden gezet: de vormgeving van de implementatie van de oplossing.

Figuur 1: Een voorbeeld van argumenten die door deelnemende partijen voor de inzet van technologie bij risicotaxatie gegeven kunnen worden, inclusief achterliggende waarde.

Voor		Tegen	Neutraal / Twijfel
Veiligheid voor samenleving, medewerkers en cliënt Als technologie de kans op incidenten (en daarmee risico voor de samenleving) verlaagt, moet deze innovatie nooit worden tegengehouden **Eerlijkheid** Technologie baseert keuzes enkel op feiten, nooit op intuïtie		**Ontbreken van relationele zorgverlening** Relatiegerichte zorg draait om context en begrip voor de situatie wat mogelijk een bijdrage levert aan de behandeling. Bij technologie ontbreekt dat 'onderbuikgevoel' **Vergelding** Als het mis gaat, kan de technologie daar niet op worden aangesproken	**Besluitvorming** De autonomie van zulke besluitvorming roept vragen op

Stap 2: inventariseren van mogelijke ethische oplossingen

In deze fase stellen de deelnemende partijen in een workshop samen de batenlogica[4] op. Vanuit de doelstelling om het aantal incidenten tijdens verlof te verminderen zal worden geredeneerd naar mogelijke oplossingen. Dit gebeurt door steeds de vraag te stellen 'Hoe doe je dat?'. Dit voorkomt niet alleen tunnelvisie bij deelnemende partijen door de mogelijkheid te geven om alle mogelijke oplossingen te overwegen, maar kan met de ethische kaders uit stap 1 ook inzicht geven in waarom sommige oplossingen moreel problematisch worden gevonden.

Figuur 2: Eén stroom van de batenlogica die leidt tot de oplossing om een algoritme te ontwikkelen.

Oplossingen	Waardedrijvers			Doel
Algoritme automatisch analyseren van risicogedrag	↑ Analyseren van beschikbare data over recidive	↑ Inzicht in voorspellende factoren voor risicogedrag	↑ Juist inschatten kans op incident	Voorkomen van recidive tijdens verlof

In deze casus hebben wij één stroom van de batenlogica uitgewerkt die leidt tot de oplossing om een algoritme te ontwikkelen (Figuur 2). Bij elke stap van rechts naar links worden de morele waarden meegewogen in het definiëren van mogelijke waardedrijvers. Zo kan het beantwoorden van de vraag 'Hoe doe je dat?' na 'Verbeteren van de inschatting kans op een incident' op verschillende manieren worden bereikt. Een mogelijk alternatief pad kan zich bijvoorbeeld richten op het verzamelen van meer data als blijkt dat betrouwbare informatie op dit moment ontbreekt. Deze vraag wordt net zolang gesteld totdat er een concrete oplossing is geformuleerd. Zo valt meer inzicht in voorspellende factoren voor risicogedrag te verkrijgen door de beschikbare data over recidive (zoals dossiers en klinische relevante informatie ingevuld door behandelaars) te analyseren.

Mogelijk willen betrokken partijen geen besluit nemen over de beste technologische oplossing als aan de toepassingsmogelijkheden wordt getwijfeld. In de batenlogica worden de morele vragen uit stap 1 verwerkt in de route richting mogelijke oplossingen.

Stap 3: vormgeven van de pilot

De laatste stap is het kiezen van de beste oplossing: wat gaan we implementeren? De beste oplossing is niet alleen aantrekkelijk vanwege de haalbaarheid en impact op het bereiken van het doel, maar is ook te realiseren binnen de in stap 1 gedefinieerde ethische kaders. Deze oplossing wordt vormgegeven samen met de deelnemers in de vorm van een pilot die ook voldoet aan het vastgestelde ethische kader. In de voorbereiding van een pilot wordt vastgelegd aan welke eisen bij de implementatie van de oplossing moet worden voldaan. Een voorbeeld is het vastleggen van de minimaal vereiste datavelden om voor een specifieke patiënt het risico op een incident in te schatten.

Deze testfase is ook de perfecte kans om enkele voorwaarden die in stap 1 zijn opgesteld te toetsen. Hoe nauwkeurig werkt het algoritme als het wordt toegepast op historische data waarbij de uitkomst al bekend is? Dit geeft meer vertrouwen in de toepassingsmogelijkheden voor de behandelaren. Daarnaast kan het uitgangspunt zijn dat een mens het laatste oordeel heeft voordat verlof wordt toegekend. Door alle stappen gezamenlijk te doorlopen en vast te leggen ontstaat een transparante beschrijving van het besluitvormingsproces. Dit document is daarmee direct een onderbouwing naar de buitenwereld hoe de oplossing tot stand is gekomen en binnen welk ethisch kader dit is gedaan.

De forensische zorg ligt constant onder een maatschappelijk vergrootglas vanwege de angst voor incidenten. Dit leidt tot druk om de kwaliteit en effectiviteit te blijven optimaliseren met het doel Nederland veiliger te maken zonder dat burgers zich daar minder veilig door gaan voelen.

Organisaties zijn voorzichtig in het nemen van stappen richting technologische innovaties, omdat zij de maatschappelijke impact onvoldoende overzien. Het vooraf definiëren van ethische waarden en het doel van het innovatietraject helpen zowel de maatschappelijke waarde als mogelijke impact inzichtelijk te maken, waarbij de afwegingen en conclusie worden vastgelegd. Het meenemen van ethiek als criterium voor deze afweging helpt om een weloverwogen en onderbouwd besluit te nemen over de beste richting.

[1]Haarms, R. & Peterse. J. (2019). Smart Detect: vroegtijdig detecteren van risicovol gedrag (zie bron).

[2]Kip, H. et al. (2019). Technologie in de forensische zorg – Crossing borders (zie bron).

[3]Simon Sinek (2010). Start with Why: How Great Leaders Inspire Everyone to Take Action.

[4]De batenlogica is een methode om een logische relatie te leggen tussen het doel van het innovatietraject en mogelijke oplossingen door van het doel (rechts) via waardedrijvers (midden) naar mogelijke oplossingen (links) te redeneren.

Auteurs

Eva Lo-van Steenbergen
Senior Manager, Capgemini Invent

eva.lo@capgemini.com

Met ruim zes jaar ervaring in de publieke sector en (forensische) zorg is Eva gespecialiseerd op het gebied van waardemanagement. Zij adviseert klanten hoe ze waarde voor hun organisatie kunnen identificeren en bewaken.

Esmée Stouten
Senior Consultant, Capgemini

esmee.stouten@capgemini.com

Esmée heeft een achtergrond in kunstmatige intelligentie en ethiek, waar thema's als verantwoordelijkheid, governance, privacy en transparantie de revue passeren. Zij heeft ervaring met diverse trajecten in de forensische zorg.

Digitale veiligheid en kwantuminternet; gaat dat samen?

Welke vragen moet het veiligheidsdomein zich stellen in voorbereiding op het kwantuminternet?

Highlights

- **Encryptie verandert met de komst van kwantumtechnologie.**
- **Overheden moeten nu beslissingen nemen om straks veilig te zijn.**
- **Kwantummechanica maakt nieuwe onbreekbare beveiliging mogelijk.**
- **Kwantumtechnologie mag niet in de verkeerde handen vallen.**
- **Een breed gedragen kader beperkt de kans op fataliteit in de toekomst.**

De keuzes die we nu maken over het 'kwantuminternet', zullen onze toekomstige veiligheid bepalen. Met de komst van computers die hedendaagse encryptie zonder moeite kraken, moeten we nu al nadenken over de wetten en regels in de wereld van morgen.

Overheden opgelet: de tweede kwantumrevolutie is zich aan het ontvouwen. Waar de eerste kwantumrevolutie de basis legde voor de moderne wetenschap, zien we binnenkort dat de wetenschap zich zal vertalen naar praktische toepassingen om 's werelds meest complexe problemen op te kunnen lossen. Deze problemen vergen nu nog letterlijk miljoenen jaren rekentijd op 's werelds sterkste (klassieke) supercomputers. U begrijpt: in verschillende industrieën zal kwantumtechnologie een disruptief effect hebben.

Net als gewone computers, zullen ook kwantumcomputers met elkaar verbonden worden. De mondiale aaneensluiting van klassieke computers is het internet dat wij kennen, en is niet meer weg te denken uit huidige maatschappij. Met het internet ontstond ook de zorg rondom (online) veiligheid. Van internetbankieren, tot het opslaan van persoonsgegevens; cybersecurity zit verweven in het internet. Een vergelijkbare situatie zullen we gaan zien bij het kwantuminternet.

Veiligheid van het kwantuminternet

De zorg rondom veiligheid van het kwantuminternet schuilt in twee aspecten. Enerzijds brengt het kwantuminternet de mogelijkheid, en de noodzaak, voor veranderende digitale beveiliging. Hoewel nieuwe soorten beveiliging uiteindelijk kunnen leiden tot een verbeterde digitale veiligheid is het risico dat overheden, bedrijven, en personen niet op tijd aangepast zijn om veiligheid te garanderen. We lopen dan het risico dat kritieke systemen gemakkelijk te breken zijn. Anderzijds geven kwantumcomputers ongekende rekenkracht welke - wanneer deze in handen van kwaadwillenden komt - desastreuze gevolgen kan hebben. Vijandige naties of internetterroristen zouden met deze rekenkracht staatsgeheimen kunnen achterhalen, intellectueel eigendom kunnen stelen, of financiële markten kunnen ontwrichten. Het is daarom van cruciaal belang om te voorkomen dat kwaadwillenden toegang krijgen tot de benodigde delen van het kwantuminternet.

Overheden zullen zich moeten voorbereiden op de komst van het kwantuminternet. Wanneer niet tijdig gebruik wordt gemaakt van de vernieuwde beveiliging lopen overheden het gevaar dat gevoelige en kritieke informatie wordt gestolen. De beveiliging van kritieke informatie, die ook op lange termijn vertrouwelijk moet blijven, zal het snelst aangepast moeten worden; er is hierbij geen tijd meer te verliezen. Daarnaast zullen overheden moeten reguleren wie gebruik kan maken van de ongekende mogelijkheden van het kwantuminternet. Wanneer kwantumcomputers in de handen vallen van kwaadwillenden,

kunnen deze veel schade aanrichten. Daarnaast maakt onbreekbare encryptie, en 'blind quantum computing', het steeds ingewikkelder om inzicht te hebben in de bedoelingen van gebruikers van het kwantuminternet. Er zal daarom een goed overdacht protocol ontwikkeld moeten worden, waarmee toegang van de juiste personen tot het kwantuminternet gewaarborgd kan worden, en waarmee kwaadwillenden toegang ontzegd kan worden. Het is van belang om als overheid hierin voorop te lopen. Keuzes over standaarden, protocollen en regulering zullen doorslaggevend zijn om verstandig gebruik van het kwantuminternet te garanderen. De keuzes die we nu maken, zullen dus bepalend zijn voor onze digitale veiligheid later.

Digitale veiligheid ten tijde van kwantumtechnologie

In een eerder verschenen artikel[1] kwam de term post-quantum cryptography (PQC) al aan bod. PQC is cryptografie waarvan gedacht wordt dat zelfs kwantumcomputers het niet kunnen breken. Zeker weten doen we dat echter nooit. In het verleden is vaker gebleken dat versleuteling waarvan we dachten dat het veilig was, toch gekraakt kon worden. Zo werd in de jaren 90 verondersteld dat essentiële sleutels in internetverkeer, zoals symmetrische sleutels RC2, RC4, DES of 3DES en hashing functies zoals MD2, MD5 of SHA1 veilig waren. Later bleek door nieuw wiskundig inzicht, en snellere computers, dat deze standaarden toch succesvol gebroken konden worden door slimmere algoritmes op gewone computers. Nu blijkt dat asymmetrische sleutels, zoals ECC en RSA, en in mindere mate symmetrische sleutels, zoals AES, gebroken kunnen worden met behulp van kwantumcomputers. Hoewel we dus verwachten dat PQC niet gebroken kan worden, door zowel klassieke of kwantumcomputers, weten we dit dus niet zeker. Nieuw wiskundig inzicht zou er toe kunnen leiden dat ook PQC weer vervangen zou moeten worden.

Voor de meest gevoelige data is het daarom van belang om nog een stapje verder te gaan. Gelukkig biedt het kwantuminternet hierbij uitkomst. Door gebruik te maken van de verstrengeling van kwantummechanische deeltjes, kan versleuteling worden ontworpen die bewijsbaar onbreekbaar is. Zelfs als nieuw wiskundig inzicht zich zou voordoen, zal deze versleuteling dus niet worden gebroken. De technologie die hierachter zit, genaamd 'quantum key distributie' (QKD) is op dit moment in volle ontwikkeling. Er zijn echter nog vele doorbraken nodig voordat een Europees netwerk met versleuteling gebaseerd op QKD beschikbaar is. Ook dan zal de implementatie van QKD echter extreem duur en complex zijn, en daarom niet voor elke gebruik geschikt zijn. Wanneer data echter voor lange tijd beschermd moet blijven kan het een uitkomst bieden.

Zelfs wanneer deze vorm van onbreekbare versleuteling beschikbaar komt, zullen we te maken hebben met een variëteit aan verschillende versleuteltechnieken. QKD dient namelijk alleen voor sleuteluitwisseling. Voor overige cryptografische primitieven (zoals digitale handtekeningen of berichtversleuteling) zijn we nog steeds afhankelijk van andere versleuteling (zowel PQC of oudere traditionele of hedendaagse versleuteling). Voor deze verschillende toepassingen zullen verschillende vormen van PQC gebruikt moeten worden; er zal niet een 'one size fits all' oplossing zijn. Het gebruik van PQC zal per situatie afgewogen moeten worden, waarbij verschillende eigenschappen zoals sleutellengtes en ver/ontsleuteling prestaties in acht genomen moeten worden, maar ook het algoritme en de implementatie ervan.

Al met al zal onze digitale veiligheid ten tijde van kwantumtechnologie flink veranderen. In toenemende mate zal onze veiligheid afhangen van complexe systemen. Daar komt bij dat door de tsunami van roulerende data, migratie naar veiligere systemen steeds complexer wordt. Op dit moment is het besef voor de noodzaak nog te laag. Hoewel grote bedrijven de noodzaak beginnen in te zien, zal het een grote uitdaging worden om in de brede reikwijdte waarin versleuteling wordt gebruikt standaarden te vernieuwen. Daarnaast zullen kleinere overheden of bedrijven met minder grote budgetten moeite hebben om het grote aantal complexe systemen te bevatten. Hiermee zal de migratie vertraagd worden. Het gevaar dat er dan in sluipt, is dat er gaten zullen vallen in de bescherming van onze digitale veiligheid. De oplossing hierin ligt in betere ketensamenwerking binnen de overheid.

Verantwoordelijke gebruik van het kwantuminternet

De vraag hier blijft hoe voorkomen kan worden dat kwaadwillenden kwantumtechnologie kunnen misbruiken. Wanneer criminelen, terroristen, of vijandige overheden toegang krijgen tot essentiële infrastructuur (zoals energiecentrales of militaire systemen) zijn de gevolgen hiervan niet te overzien. Naast de disruptieve werking van het Shor's algoritme om traditionele encryptie te kraken, zijn andere kwantumalgoritmes bijzonder efficiënt in het berekenen van chemische eigenschappen van moleculen en stoffen. Hierdoor kunnen nieuwe materialen en medicijnen worden uitgevonden, die ingezet kunnen worden voor positieve ontwikkelingen. Maar ook hier schuilt een keerzijde. Wat als een eigenmachtige overheid kwantumcomputers gebruikt om chemische wapens te ontwikkelen? Of een nieuw virus?

Daarin schuilt een extra gevaar. Door de veranderende versleuteling op het kwantuminternet wordt het steeds ingewikkelder om de juiste bedoelingen van gebruikers te controleren. Door gebruik te maken van PQC of QKD kunnen berichten die over het kwantuminternet verstuurd worden niet meer achterhaald worden, zelfs niet door inlichtingendiensten. Daarnaast zou het kwantuminternet mogelijkheden kunnen bieden om naast internetverkeer ook berekeningen volledig anoniem uit te voeren. Dit zogenaamde 'blind quantum computing' zorgt ervoor dat zelfs de eigenaar van de kwantumcomputer niet in staat is om te achterhalen welke berekeningen gebruikers op de computers uitvoeren. Hoewel dit mooie toepassingen kan bieden op het gebied van privacy, is het risico dat het zicht volledig verloren raakt op de bedoelingen van gebruikers.

In Europa wordt innovatie op het gebied van kwantumtechnologie vooral door publieke fondsen gefinancierd. Voordelen ervan zullen dus ook bij de gehele bevolking terecht moeten komen. Het is goed denkbaar dat als het kwantuminternet functioneel is, er winnaars en verliezers zullen zijn. Wereldwijd zouden we er daarom als mensheid goed aan doen om dit kwantuminternet open te stellen en voor kritieke informatie elkaar het recht te gunnen om geheim te kunnen communiceren. Geheimen zouden niet enkel voor de slimste landen en partijen weggelegd moeten zijn. Ook moet bijgehouden worden waar het kwantuminternet voor wordt ingezet, want ook zonder het onkraakbaar kunnen versturen van gegevens moeten zowel de verzender als de ontvanger geen kwaad mogen verspreiden.

Met de naderende mogelijkheden van het kwantuminternet is daarom een breed gedragen kader nodig dat stuurt richting verantwoordelijk gebruik. We zullen ons vragen moeten stellen als: hoe zorgen we voor een eerlijke toegang, controle, en garantstelling? En hoe weren we ons tegen kwaadwillenden?

Technologisch soevereiniteit

Inmiddels beginnen overheden wereldwijd het belang, en gevaar, van het kwantuminternet in te zien. In de Verenigde Staten bijvoorbeeld, is het 'National quantum initiative' goed voor een subsidie van ruim meer dan een miljard dollar (AIP, 2018[2]). Baas boven baas: het programma van de Verenigde Staten is nog maar een schijntje bij dat van China. In 2020 kondigde de Chinese overheid een subsidieprogramma[3] van tien miljard aan. Het ambitieuze wetenschapsprogramma van China is daarmee inmiddels niet meer te ontkennen als een van de wereldleiders op het gebied van kwantumtechnologie. Ook de Europese Unie heeft de afgelopen jaren flink geïnvesteerd in verschillende kwantumtechnologieën. Het Europese Quantum Flagship programma is goed voor een budget van ruim een miljard tot 2028. Daarnaast verkrijgt kwantumtechnologie ook een rol in andere subsidieprogramma's, zoals Horizon Europe[4] (voorgesteld budget van 100 miljard euro), en hebben lidstaten afzonderlijk ambitieuze programma's.

Naast overheidsprojecten steken ook bedrijven veel geld in onderzoek. Hoewel de gerelateerde winst nog nagenoeg nul is, anticiperen deze bedrijven op de paradigmaverschuiving die kwantumtechnologie kan brengen. Ook Europese bedrijven zitten niet stil. Door de noodzakelijkheid van een ruimtevaartelement in kwantumcommunicatie en -security, zijn multinationals zoals Airbus en Thales te vinden in de voorlinie van kwantuminnovatie. Desondanks wordt de markt gedomineerd door Amerikaanse BigTech. Financiering komt niet alleen uit de diepe zakken van de BigTech zelf, ook durfkapitaal (venture capital) vloeit rijkelijk in de Verenigde Staten.

Om Europese waarden te beschermen, aanspraak te maken op economische kansen, en onze technologische soevereiniteit te beschermen, moeten we daarom snel onze achterstand wegwerken. Europa heeft eerder de race voor kunstmatige intelligentie verloren: hebben we nog een kans op het gebied van kwantumtechnologie?

Keuzes maken in de voorste linie

Het kwantuminternettijdperk is nabij, en de tijd is daar om nu al gewogen keuzes te maken in de openheid en soevereiniteit ervan. Adresseer het onderwerp dus nu al bij het maken van veiligheidsbeleid.

De overheid zal een voorbeeldfunctie moeten tonen in een wereld van veranderde digitale veiligheid. Miljarden euro's aan subsidietrajecten zullen nodig zijn in de uitrol van QKD-netwerken en bedrijven zullen op de gevaren en baten van het kwantuminternet moeten worden gewezen. Tegelijkertijd zullen we staatsgevoelige gegevens op de juiste manier moeten beschermen.

Tot slot zullen we keuzes moeten maken om eerlijk en verantwoordelijk toegang tot het kwantuminternet te borgen. Om het belang van burgers te beschermen moeten we daarbij voorkomen dat toegang alleen voor de rijkste of slimste is, en dat kwaadwillenden het kwantuminternet gebruiken om maatschappelijk systemen te ontwrichten.

Kiezen we voor een structuur die gedomineerd is door (Amerikaanse en Chinese) BigTech, of streven we naar een vorm wat lijkt op ons huidige internet? Leren we van de historische ontwikkeling van het internet of vormen we proactief al universele wet- en regelgeving, protocollen en standaarden?

In de voorlinie van innovatie te staan in plaats van het passief volgen is van groot belang voor de veiligheid en soevereiniteit van Nederland en Europa. Laat het adagium 'alleen ga je snel, samen kom je verder', ook gelden voor onze Europese toekomst in de wereld van kwantuminnovatie.

Begrippenkader

Quantum Internet	De visie van een kwantuminternet is om kwantumprocessoren te verbinden doormiddel van kwantumcommunicatie. Het kwantuminternet zal, in synergie met het klassieke internet, nieuwe internettechnologie mogelijk maken, welke klassieke onmogelijk is. Voorbeelden hiervan zijn onbreekbare cryptografie, clusters van parallelle kwantumcomputers, en kwantumsensornetwerken.
Quantum key distribution	Quantum Key Distribution (QKD) is een techniek die gebruik maakt van de verstrengeling van kwantumdeeltjes waardoor er onkraakbaar sleutels gedeeld kunnen worden.
Post-quantum Crypto	Post-Quantum Cryptography (PQC) is klassieke encryptie, waarvan verondersteld wordt dat het veilig is tegen toekomstige kwantum aanvallen.
Quantum computing	Kwantumcomputers zijn machines die slim gebruik maken van kwantummechanische fenomenen waardoor sommige rekenkundige taken extreem versneld kunnen worden.
Blind quantum computing	'Blind' betekent dat leverancier van de kwantumcomputer geen (volledige) informatie heeft over de taken die worden uitgevoerd. Dit betekent dat gebruiker volledige privacy heeft.

[1]https://www.trendsinveiligheid.nl/rapport/2020-samen-veilig/quantumcomputers-een-forse-inbreuk-op-vertrouwelijkheid/

[2]https://www.aip.org/fyi/federal-science-bill-tracker/115th/national-quantum-initiative-act

[3]https://www.forbes.com/sites/moorinsights/2019/10/10/quantum-usa-vs-quantum-china-the-worlds-most-important-technology-race/

[4]https://ec.europa.eu/info/horizon-europe_en

Auteurs

Julian van Velzen
Expert quantum technology

julian.van.velzen@capgemini.com

Julian van Velzen is werkzaam bij Capgemini Insights & Data als Consultant. Julian heeft een achtergrond in de computationele natuurkunde. Hij richt zich nu op kwantumcomputing en cloud services.

Luc Baardman
Senior Consultant Publieke Sector

luc.baardman@capgemini.com,
https://twitter.com/lucbaardman

Luc is werkzaam bij Capgemini Invent. Tijdens 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.

Organisatie-innovatie: Criminaliteitsbestrijding op z'n Cruijffiaans

Hoe moet de veiligheidsketen zich organiseren om te winnen in de dagelijkse praktijk?

Highlights

- **Organisatie-innovatie is het implementeren van andere manieren van denken en organiseren. Dit is voorwaardelijk om Nederland veiliger te maken.**
- **Het inzetten van de 'wisdom of the crowd' is hier een voorbeeld van.**
- **De tegenstander heeft ook beschikking over nieuwe technologieën dus daarmee alleen kun je de wedstrijd niet winnen.**
- **De veiligheidsketen – veiligheidsnetwerk is wellicht ook een goede term - moet versnellen om de wedstrijden te (blijven) winnen.**

Johan Cruijff zei ooit: "Voetbal is een simpel spelletje: je maakt gewoon één doelpunt meer dan je tegenstander en dan heb je in principe gewonnen". Dat geldt ook in de strijd tegen misdaad.

"De strafrechtketen piept en kraakt", zegt Gerrit van der Burg, voorzitter van het college van procureurs-generaal van het Openbaar Ministerie. Naast hem knikt Hanneke Ekelmans. Zij is lid van de korpsleiding van de politie. Henk Naves, voorzitter van de Raad voor de rechtspraak, deelt die zorg. Ook personeel is een gedeelde prioriteit. Naves, Ekelmans en Van der Burg maken zich alle drie zorgen over de enorme werkdruk die rechters, officieren van justitie en agenten ervaren. De politie worstelt met het vullen van de roosters; daar zijn de personeelstekorten het grootst. Er zijn volgens de korpsleiding duizend extra mensen nodig en op de lange termijn zelfs 3500, met name agenten in de wijk[1].

Voor de uitdaging die hier geschetst wordt, kan digitalisering worden ingezet. Echter, dat kan niet zonder organisatie-innovatie. Digitalisering komt als middel alleen tot zijn recht als het voldoende snel ingezet kan worden. Wat is dan snel genoeg? Net een stap sneller dan de tegenstander. Wat is organisatie-innovatie? Het is lastig hiervan een eenduidige definitie te geven. Bij organisatie-innovatie binnen de eigen organisatie gaat het bijvoorbeeld om procesverbetering, vernieuwing van de organisatiestructuur en het verleggen van verantwoordelijkheden naar een ander niveau in de organisatie. Organisatie-innovatie helpt uiteindelijk om de tegenstander een stapje voor te zijn. Om dat te bereiken is het niet alleen zinvol om naar de eigen organisatie te kijken, maar ook te onderzoeken of er nieuwe organisatievormen zijn, gericht op het samenwerken daarbuiten. Hierbij nemen we in ogenschouw dat 'de snelheid van een proces wordt bepaald door de langzaamste speler (schakel)'. Het team wint, niet het individu. Als we in de veiligheidsketen werken moeten we dus niet alleen individuele schakels verbeteren maar ook de keten als geheel. Tegelijkertijd is het zinvol om 'out-of-the-box' te denken en te kijken of we 'nieuwe schakels (spelers) kunnen toevoegen' die de snelheid van de keten als geheel kunnen verhogen.

De verwachting van de maatschappij is dat alles snel en direct moet. Vandaag besteld, morgen in huis is een belofte die je als bedrijf moet waarmaken om succesvol te zijn. Deze verwachting zou je in de veiligheidsketen kunnen vertalen naar 'vandaag crimineel, morgen opgepakt'. Natuurlijk simplistisch gesteld en het is de vraag of dit binnen de juridische kaders überhaupt mogelijk is. Aan de andere kant een wenkend perspectief dat - samen met de zich snel ontwikkelende criminaliteit met telkens vernieuwde vormen en veranderende (Europese) wet- en regelgeving - vraagt om een adaptief systeem. Een systeem waarin de veiligheidsketen in staat is om proactief in te spelen op de veranderingen in de wereld/samenleving en op die manier in staat is haar tegenstanders een stap voor te blijven.

Een paar concrete, recente opgaven die vragen om dat adaptieve systeem:

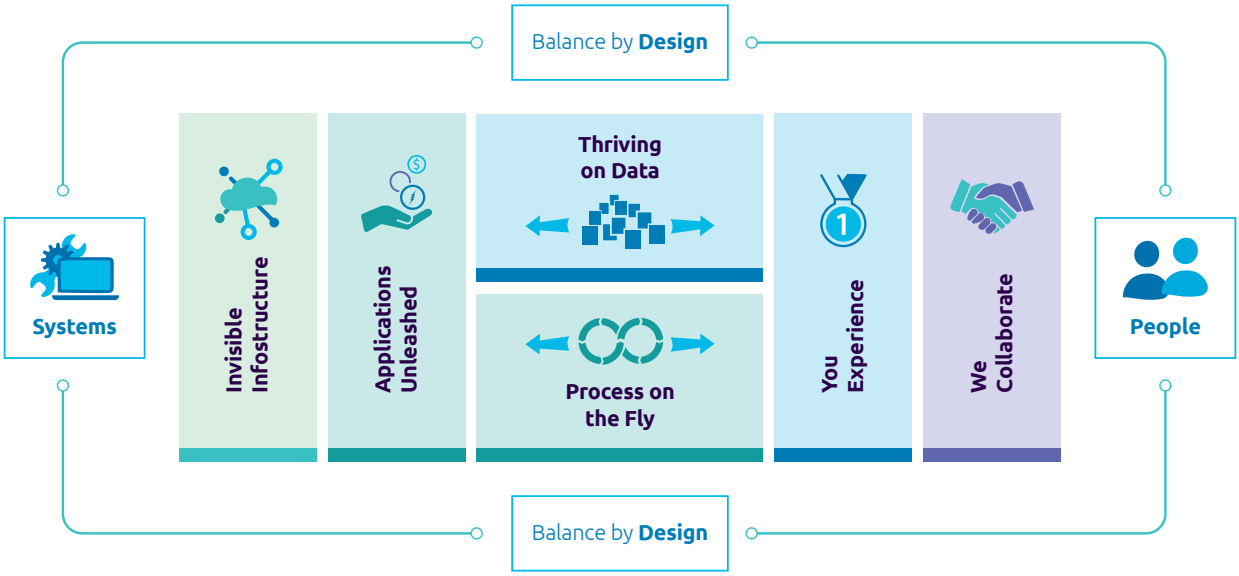
- De verschuiving van traditionele naar online criminaliteit. Hoe blijf je in staat om de tegenstander voor te zijn op nog onbekend terrein met een onbekende toekomst?
- Mobilisatie van onvrede via sociale media. Recente voorbeelden zijn #BLM, de COVID-onrust en de bestorming van het Capitool. Hoe houd je Nederland veilig binnen de kaders van wet- en regelgeving?

En zo zullen nieuwe opgaven volgen. Technologie, data en kennis zijn onmisbaar, en alleen mogelijk in combinatie met wendbaarheid en actie. Organisatie-innovatie is randvoorwaardelijk voor succes. In dit artikel blijven we gebruikmaken van de metafoor van een wedstrijd en de daarbij behorende termen als team, speler, tactiek, en spelsysteem.

Spel

Hoe dan tot die organisatie-innovatie te komen? Wij gebruiken Capgemini's Technovision 2021. Dit raamwerk bestaat uit de belangrijkste technologietrends die als inspiratie dienen voor innovatie. Daarnaast doen wij als bescheiden scouts de suggestie voor een talentvolle nieuwe speler: SafetyCat. Aan de hand van deze suggestie, beschrijven we hoe je kunt komen tot organisatie-innovatie die tot de winst leidt. We richten ons op de trends 'We Collaborate', 'Thriving on Data', 'Process on the Fly' en 'You Experience'.

Figuur 1: Technovision raamwerk 2021.[2]



We collaborate - Ultieme (team) samenwerking

Nederland veilig houden is een teamprestatie. Binnen de veiligheidsketen wordt al jaar en dag samengewerkt tussen de verschillende organisaties. Wij zien kans en meerwaarde om het team aan te vullen met de kracht van de maatschappij zelf, zoals samenwerkingsverband Bellingcat. Bellingcat is een burgerjournalistiek-netwerk dat is opgericht door de Britse blogger Eliot Higgins. Het maakt onder andere gebruik van onlinebronnen, zoals sociale media. Het onderzoekt internationale conflicten en werd bekend door berichtgeving over de Syrische Burgeroorlog, de oorlog in Oost-Oekraïne en de vliegramp met MH17. De veiligheidsketen zou kunnen onderzoeken hoe ze dit door middel van het inzetten van een nieuw concept als SafetyCat kunnen faciliteren, binnen de bestaande wetgeving uiteraard[3].

Thriving on Data – Bouwen op data

Tijdens rellen voor de lockdown in Nederland werd de politie al enigszins geholpen door burgers die informatie deelden over de relschoppers. Daardoor konden verdachten opgespoord worden. Dit willen we door SafetyCat structureel verweven met de werkwijze in de veiligheidsketen. Mensen organiseren zich, activeren elkaar en krijgen andere mensen op de been. Social media zijn het platform waar dit gebeurt. Dit is niet altijd (geoorloofd) zichtbaar voor de handhavers. Politie en justitie willen uiteraard wel op de hoogte blijven, maar mogen niet alles. Burgers zijn bereid dit ter beschikking te stellen aan de veiligheidsketen (mits hun eigen privacy wordt gewaarborgd) maar SafetyCat zou meer kunnen doen: burgers gaan zelf de informatie die ze hebben combineren, analyseren en maken de resultaten vrijelijk beschikbaar voor de maatschappij, en dus ook voor de veiligheidsketen. Zo kan de veiligheidsketen worden ontlast aangezien een deel van het analysewerk door vrijwilligers gebeurt. Dit moet uiteraard plaatsvinden binnen de juridische kaders, maar vraagt wellicht ook om aanpassing van de juridische kaders.

Process on the Fly – Agile als katalysator

Een winnende speltactiek binnen de veiligheidsketen is essentieel. Daarbij is goed samenspel op basis van het spelsysteem randvoorwaardelijk. Maar als de omstandigheden op het veld wijzigen, moet de tactiek in het veld snel aangepast kunnen worden. Een van de succesfactoren ligt in het (snel) uitwisselen van relevante informatie. Willen we de wedstrijd winnen dan moeten we met deze extra informatie ook nog scoren. Kortom, de informatie moet snel kunnen worden verwerkt, geanalyseerd en tot actie leiden en we moeten nieuwe technologie snel kunnen inzetten. De huidige manieren van werken voldoen niet meer en zijn te traag.

Tegenwoordig is transformeren naar agile werken – wat eveneens een vorm van organisatie-innovatie is - een tactiek die veel organisaties inzetten om te winnen. Er zijn allerlei frameworks die helpen om nieuwe producten of diensten sneller bij de eindgebruiker te krijgen met als doel de concurrentie voor te blijven. Deze frameworks geven een heldere structuur en control hoe op snelle wijze nieuwe producten of diensten in te zetten met optimaal gebruik van budget. Ook voor SafetyCat zullen we dit inzetten (lees: SafetyCat moet worden ingebed in de keten én de veiligheidsketen zelf zal verder moeten transformeren naar agile werken).

In grove lijnen komt het erop neer dat nieuwe producten of diensten kortcyclisch worden ontwikkeld, getoetst en aangepast. De reden dat transformeren naar agile werken vaak toch lastig is, is omdat het een verandering van mindset vraagt: 'hoger' in de organisatie moet men in staat zijn om verantwoordelijkheden deels te delegeren, op de werkvloer moet men in staat zijn om deze gedelegeerde verantwoordelijkheid ook te dragen en tot betere resultaten laten leiden. Het uiteindelijk resultaat is dat de veiligheidsketen als geheel sneller en beter nieuwe producten of diensten 'naar buiten krijgt' en als zodanig de boef voor blijft. Iedere organisatie is een schakel in een keten van verschillende schakels en dus alle schakels moeten verbeteren. En de 'aansluitpunten' tussen de schakels zuilen ook moeten worden verbeterd. Zo kunnen we de keten als geheel optimaliseren en daarmee de wedstrijden (blijven) winnen, waarmee we Nederland veiliger maken. Onze oproep is dan ook aan de schakels om te transformeren naar agile werken én de samenwerking in de veiligheidsketen op te zoeken om de keten als geheel te verbeteren.

You Experience – Beleving van waarde

Deze trend is van belang voor de mensen in de veiligheidsketen die gebruik maken van de nieuw ontwikkelde tools om de wedstrijd te winnen. Voor SafetyCat geldt dat het voor de deelnemers (burgers, vrijwilligers) aantrekkelijk moet worden gemaakt om hun informatie en analyse te delen maar ook dat de resultaten van hun werk (een gewonnen wedstrijd) 'gevierd' worden. Dat kan al heel eenvoudig beginnen: zoals bij Opsporing Verzocht wordt aangegeven hoeveel tips er zijn binnengekomen en wat er met die tips is gedaan en wat ze hebben opgeleverd. Dit is het schouderklopje van je teamgenoten als je gescoord hebt.

Wij willen met dit artikel een aanzet geven tot organisatie-innovatie in de brede zin binnen de veiligheidsketen, waarbij het volledige maatschappelijke potentieel benut wordt om Nederland veilig te houden. We vertrouwen hier op 'the wisdom of the crowd' (veiligheidsketen en burgers) om dit aan te vullen, verbeteren en implementeren.

De bal ligt klaar. Wie wil meehelpen het uiteindelijk winnende doelpunt te scoren om zo Nederland veiliger te maken?

[1]'Politie, OM en rechtspraak willen 850 miljoen voor sterke rechtsstaat.'Dagblad Trouw 30 januari 2021

[2]Technovision 2021 https://www.capgemini.com/technovision-2021-technology-trends-in-business/

[3]Burgerparticipatie in online opsporing - Kunnen burgers helpen in opsporingszaken met het verzamelen van online informatie (OSINT)? Auteur Frank Inklaar Trends in Veiligheid 2020

Auteurs

Addo de Visser
Agile Transformation Consultant

addo.de.visser@capgemini.com

Addo heeft de afgelopen 25 jaar veel organisaties begeleid in hun Business/ICT professionalisering. Vanaf 2014 is hij fulltime bezig met Agile Transformaties. Tevens trainer Agile & workshop facilitator. Auteur boek 'Agile – the times they are a-changin'.

Stijn de Keijzer
Agile coach / scrummaster

stijn.de.keijzer@capgemini.com

Stijn heeft meer dan 15 jaar ervaring als adviseur en agile coach in de publieke sector. Hij is werkzaam in het publieke veiligheidsdomein voor Capgemini.

Veiligheid ten tijde van een pandemie

Het afgelopen jaar heeft in het teken gestaan van de pandemie en de maatregelen die de overheid heeft genomen om de verspreiding van het virus tegen te gaan. Dit heeft een grote maatschappelijke impact gehad.

In de vorige editie van Trends in Veiligheid is onderzocht hoe het veiligheidsgevoel zich in de afgelopen tien jaar heeft ontwikkeld. In dit decenium is de burger zich over het algemeen iets onveiliger gaan voelen. Echter, het online veiligheidsgevoel is juist in deze periode gestegen. Burgers zijn zich meer bewust geworden van de risico's en gevaren die de digitale wereld met zich meebrengt. Tegelijkertijd is men zich ook bewuster van waar de burger op moet letten en welke maatregelen genomen moeten worden om digitaal veilig te zijn. Het onderstreept de groei in volwassenheid, van een analoge maatschappij naar een digitale of hybride maatschappij. Deze ontwikkelingen zetten zich onverminderd voort. Waarbij een constante ontwikkeling verwacht kan worden. Als gesproken kan worden over een verandering van tijdperk, dan lijkt dit nieuwe tijdperk zich aan te dienen als de superslimme samenleving, oftewel Society 5.0[1]. Daarnaast is deze samenleving een plek waar technologieën kunnen worden toegepast om maatschappelijke vraagstukken aan te pakken.

Deze digitale ontwikkeling van de maatschappij maakt in 2020 vanwege de coronapandemie en de betreffende maatregelen een majeure stap. Basisscholen stappen over van fysiek naar digitaal onderwijs. Winkelen kan alleen nog maar digitaal en online vergaderen is de standaard geworden. Deze versnelde digitalisering verandert de maatschappij zodanig, dat dit mogelijk ook een impact op het veiligheidsgevoel kan hebben. Vandaar dat de volgende vraag in dit artikel centraal staat: Welke effecten heeft de coronapandemie en met name de genomen maatregelen op de perceptie van veiligheid van burgers?

Individueel veiligheidsgevoel en slachtofferschap

Over het algemeen lijkt men zich het afgelopen jaar veiliger te zijn gaan voelen. Vorig jaar gaf namelijk 45% van de respondenten aan zich soms tot vaak onveilig te voelen en voelde 54% zich juist zelden tot nooit onveilig. Dit jaar zijn deze percentages respectievelijk 39% en 61%. De afname in het gevoel van onveiligheid zou mogelijk verklaard kunnen worden door het feit dat het openbare leven nagenoeg tot stilstand is gekomen. Als vervolgens verder wordt ingezoomd op de cijfers, is een interessante trend te ontdekken. Thuis en op straat zijn meer respondenten zich veiliger gaan voelen ten opzichte van vorig jaar, terwijl dit online juist is afgenomen. Als gevraagd wordt naar ervaring met digitale criminaliteit, valt op te maken dat bepaalde delicten ten opzichte van vorig jaar hoger scoren. Het gaat dan om phishing en hacking. Dat lijkt overeen te komen met de door het Centrum voor Criminaliteitspreventie en Veiligheid[2] beschreven probleem dat criminelen de coronacrisis lijken te misbruiken door online meer delicten te plegen. De toename in digitale criminaliteit lijkt dus ook het online veiligheidsgevoel van burgers aan te tasten.

De verschuiving van gevoelens van onveiligheid van fysiek naar digitaal kan dus verklaard worden op meerdere manieren. Allereerst is zoals eerder genoemd het openbare leven nagenoeg stil komen te liggen. Daardoor begeven mensen zich minder in fysieke ruimten en meer online. Een voorbeeld daarvan is de sluiting van winkels en de daaruit volgende toename van digitale bestellingen in webshops[3]. Daarnaast blijkt uit dit onderzoek dat het grootste deel van de bevolking het afgelopen jaar ervaring heeft gehad met een vorm van internetcriminaliteit, zoals spam en phishing. Echter, het merendeel van de respondenten lijkt zich tijdig te kunnen verweren waardoor het daadwerkelijk slachtofferschap een stuk lager ligt. Ondanks dat niet iedereen slachtoffer wordt van een poging tot internetcriminaliteit, zijn deze pogingen wel zichtbaar. Dit kan dus ook impact hebben op het digitale veiligheidsgevoel.

De zichtbaarheid en herkenbaarheid van bepaalde internetcriminaliteitsvormen neemt wel af. Momenteel geeft 68% van de respondenten aan dat ze een phishing e-mail kunnen herkennen, terwijl 67% vindt dat het de afgelopen jaren steeds moeilijker is geworden om ze te herkennen. Daarnaast geeft 55% aan dat ze over vijf jaar phishing e-mails waarschijnlijk niet meer kunnen herkennen. Dit betekent dat naast de kwantitatieve toename van digitale criminaliteit ook de kwaliteit toeneemt. Daardoor zou slachtofferschap mogelijk kunnen gaan toenemen.

Nationale veiligheid

Naast individuele veiligheidsgevoelens is het ook interessant om te bestuderen hoe men aankijkt tegen nationale veiligheid. Uit het onderzoek komt namelijk naar voren dat slechts 23% van de respondenten een fysieke aanval op Nederland waarschijnlijk acht, terwijl 58% van de respondenten een digitale aanval voorstelbaar vindt. Vorig jaar gaf 49% van de respondenten aan een digitale aanval waarschijnlijker te vinden dan een fysieke aanval. Doordat de vraagstelling dit jaar anders is dan vorig jaar, zijn de cijfers niet direct te vergelijken. Echter, de trend dat men denkt dat de kans op een digitale aanval groter is dan een fysieke aanval lijkt te worden voortgezet. Een opvallende uitkomst daarbij is dat 74% van de respondenten denkt dat een digitale aanval het hele land kan platleggen, terwijl 37% zich er echt zorgen over maakt.

Naast de waarschijnlijkheid van een digitale aanval is het ook van belang om in te gaan op hoe Nederland hiermee om dient te gaan. Slechts 26% van de respondenten denkt namelijk dat Nederland zich goed kan verdedigen. Respondenten willen vooral dat de overheid transparant is over dit soort aanvallen. 66% vindt dat Nederland kenbaar moet maken wanneer het een digitale aanval heeft voorkomen. Daarnaast geeft 25% aan dat Nederland ook zelf actief aanvallen moet gaan uitvoeren en als dat dan gebeurt, vindt 50% dat dit ook openbaar gemaakt moet worden.

Digitale criminaliteit bestrijden

Ten tijde van de huidige pandemie lijkt dus digitale criminaliteit toe te nemen en voelt men zich online steeds onveiliger, zowel op individueel niveau als op nationaal niveau. Daarom is het ook relevant om in te gaan hoe de burger denkt dat Nederland digitale criminaliteit moet bestrijden. Men vindt vooral dat de burger zelf een verantwoordelijkheid heeft om zich te beschermen tegen digitale criminaliteit, namelijk 69% geeft dit aan. Opvallend is dat weinig respondenten (25%) vinden dat de overheid en politie verantwoordelijk zijn hiervoor, terwijl men wel vindt dat de overheid moet investeren in digitale criminaliteitsbestrijding. 61% vindt namelijk dat er meer geïnvesteerd moet worden in technische middelen bij de politie en 58% vindt dat de kennis van digitale criminaliteit beter kan. Wat betreft de voorgestelde kennisverwerving vindt 69% van de respondenten dat bij lastig speurwerk ook burgers ingezet kunnen worden om de politie te ondersteunen.

Als verder ingezoomd wordt op de rol van de overheid in de bestrijding van digitale criminaliteit, blijkt dat 58% van de respondenten vindt dat de overheid meer bevoegdheden moet creëren om de aanpak te verbeteren. Daarnaast zijn beschermende wetgeving en harder straffen ook veel genoemde antwoorden. Een minder populaire actie is meer internationaal samenwerken. 28% vindt dat Nederland meer moet samenwerken met de EU of de NAVO. Dat lijkt overeen te komen met de eerdergenoemde relatief lage cijfers over de stelling of men zich zorgen maakt over een digitale aanval.

Conclusie

Na een jaar corona en lockdowns is het leven in Nederland flink veranderd. Het leven van veel mensen heeft zich verplaatst van de openbare ruimte naar de digitale wereld. Daarmee lijkt de trend van de verschuiving van fysieke criminaliteit naar digitale criminaliteit het afgelopen jaar versterkt te zijn. Meer mensen geven aan te maken te hebben gehad met digitale criminaliteit en meer mensen zijn zich online ook onveiliger gaan voelen. Het gaat dan voornamelijk om individuele veiligheid. Wat betreft nationale veiligheid vindt men dat een digitale aanval verstrekkende gevolgen kan hebben, maar maakt men zich hier over het algemeen geen grote zorgen over. Interessant is dat wordt aangegeven dat de overheid meer moet investeren in technische middelen en kennis om digitale criminaliteit te bestrijden.

De versnelde toename van digitale criminaliteit als gevolg van de pandemie dwingt om meer aandacht te hebben voor de bestrijding daarvan. Het advies van de burger aan de overheid is daarbij om meer kundige mensen in te zetten en technisch met creatieve oplossingen te komen, waarbij de samenwerking met de burger niet geschuwd moet worden. Alleen samen krijgen we digitale criminaliteit onder controle.

[1]Society 5.0 https://www.capgemini.com/nl-nl/bronnen/society-5-0-naar-een-superslimme-samenleving/

[2]https://hetccv.nl/onderwerpen/corona-en-veiligheid/internetcriminaliteit/

[3]https://www.emerce.nl/nieuws/corona-verantwoordelijk-extreme-groei-online-aankopen

NB: het onderzoek is uitgevoerd door Ipsos in opdracht van Capgemini Nederland B.V. Het onderzoek is gedaan in januari 2021. De steekproef populatie is 'de Nederlander' en N>999. Uitwerkingen van alle vragen zijn verderop te vinden in dit rapport.

Auteurs

Thomas de Klerk
Marketing Manager

thomas.de.klerk@capgemini.com

Thomas is marketing manager en richt zich onder andere op de publieke sector. Zijn focus ligt op delen van delen van kennis, visie en het versterken van publiek private samenwerking.

Zeger de Bruijne
Criminoloog & OOV informatie-analist

zeger.bruijne@capgemini.com

Zeger is werkzaam bij Capgemini Business Technology Service in het domein van openbare orde en veiligheid. Zeger is gespecialiseerd in het analyseren van processen en ontwikkelingen binnen criminaliteitsbestrijding.

Marcel Kordes
Manager sector Openbare Orde & Veiligheid BTS

marcel.kordes@capgemini.com

Marcel is verantwoordelijk voor de afdeling Business Technology Service in het domein van openbare orde en veiligheid. Marcel is senior business analist en heeft 15 jaar werkervaring in het openbaar orde- en veiligheidsdomein.

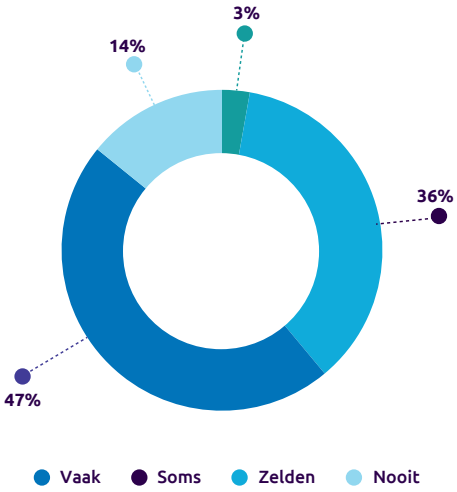
Onderzoek Trends in Veiligheid 2021

1 Digitale versus fysieke dreiging

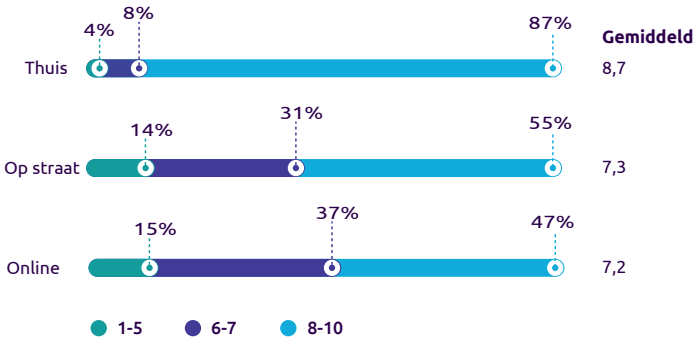
Waar maakt men zich de meeste zorgen over?

Online voelt men zich minder veilig dan fysiek

Onveilig voelen



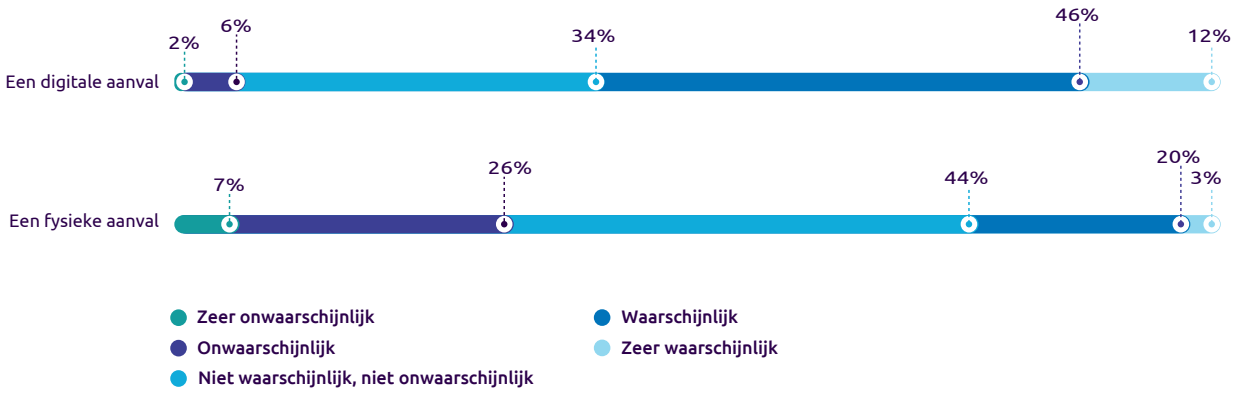
Gevoel van veiligheid



- 39% voelt zich soms of vaak onveilig. Dat is vergelijkbaar met 2019 (3% vaak, 42% soms onveilig). Vrouwen (49%) en jongeren van 18 t/m 29 jaar (53%) geven relatief vaak aan dat zij zich soms of vaak onveilig voelen.
- Het gevoel van veiligheid is het grootst in huis, gevolgd door op straat. Online veiligheid beoordeelt men relatief vaak met een 6 of 7 en minder vaak met een 8 of hoger. Mannen en 65-plussers geven voor alle drie de locaties relatief hoge cijfers voor hun gevoel van veiligheid.

Men acht het waarschijnlijker dat Nederland digitaal wordt aangevallen dan fysiek

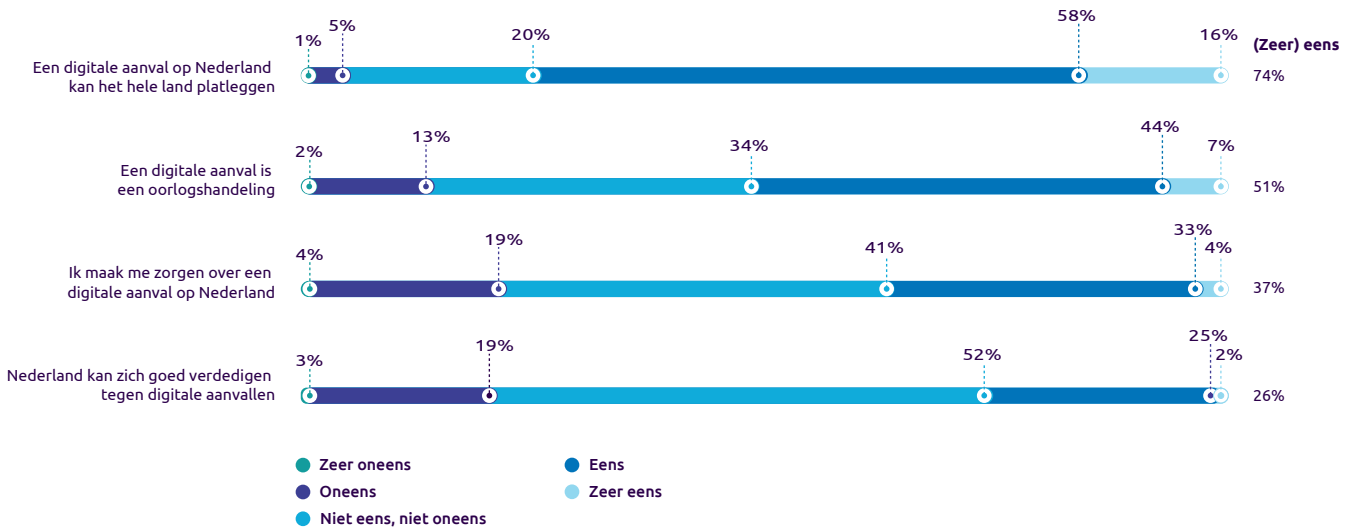
Waarschijnlijkheid gebeurtenissen



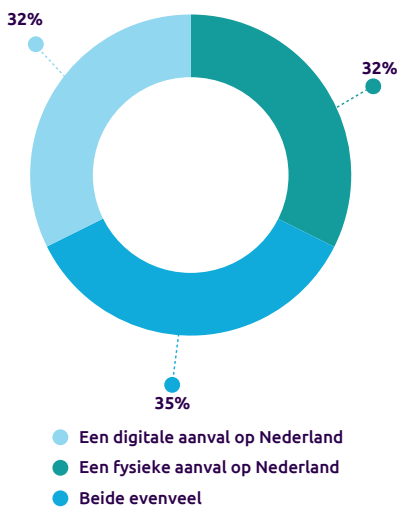
- 58% acht een digitale aanval in Nederland (zeer) waarschijnlijk. Hoe hoger opgeleid, des te vaker men deze mening is toegedaan.
- Een fysieke aanval acht men een stuk minder waarschijnlijk (23%). Het zijn relatief vaak middelhoog opgeleiden die dit (zeer) waarschijnlijk vinden. Verder vinden vrouwen dit waarschijnlijker dan mannen, terwijl 65-plussers relatief weinig aangeven dat zij dit waarschijnlijk vinden.

Driekwart meent dat een digitale aanval het hele land kan platleggen, toch maakt lang niet iedereen zich hier zorgen over

Digitale aanval



Boezemt meeste angst in



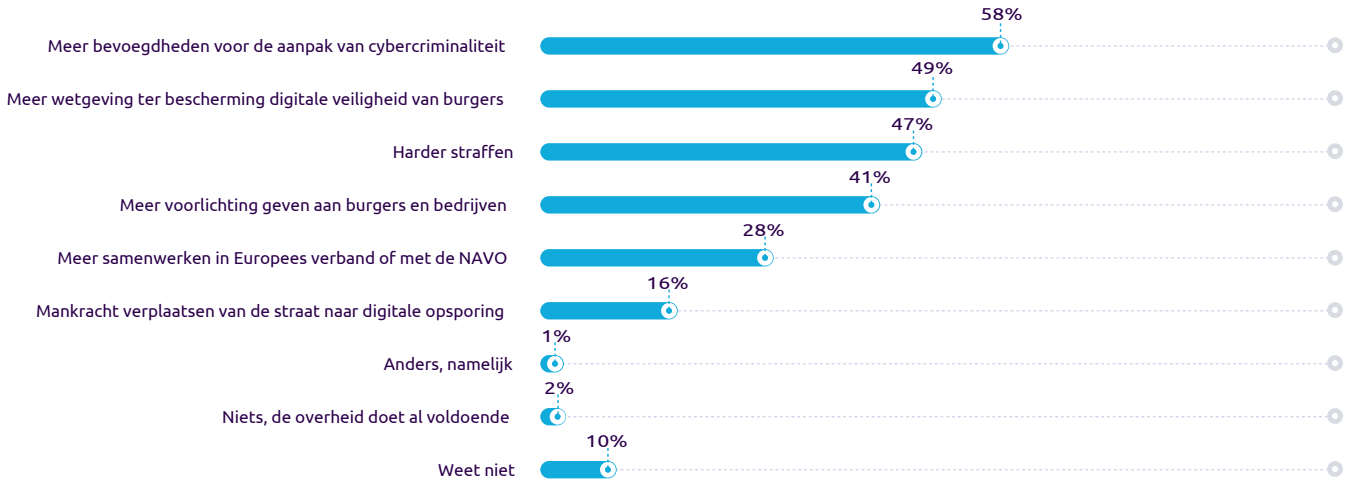
- Degenen die een digitale aanval in Nederland (zeer) waarschijnlijk vinden, maken zich daar ook relatief vaak zorgen over (51%) en zijn relatief vaak van mening dat een digitale aanval het hele land kan platleggen (82%).
- Een digitale en fysieke aanval boezemen Nederlanders vergelijkbare angst in. Mannen en 65-plussers zijn angstiger over een digitale aanval dan over een fysieke aanval, vrouwen en jongeren van 18 t/m 29 jaar, zijn angstiger over een fysieke aanval dan over een digitale aanval.
- Degenen die aangeven dat een digitale aanval hen meer angst inboezemt dan een fysieke aanval, geven ook relatief vaak aan dat zij zich zorgen maken over een digitale aanval (50%). Zij zien dit relatief vaak als een oorlogshandeling (63%). Verder zijn zij relatief vaak van mening dat een digitale aanval op Nederland het hele land kan platleggen (81%) en vrezen zij dat Nederland zich niet goed kan verdedigen tegen digitale aanvallen (27% '(zeer) oneens').

2 Hoe dient Nederland zich te beschermen?

- **Wat verwacht men van de overheid?**
- **Welke middelen mogen worden ingezet?**
- **Welke investeringen zijn er nodig?**

Van de overheid verwacht men met name een faciliterende rol in de strijd tegen cybercriminaliteit

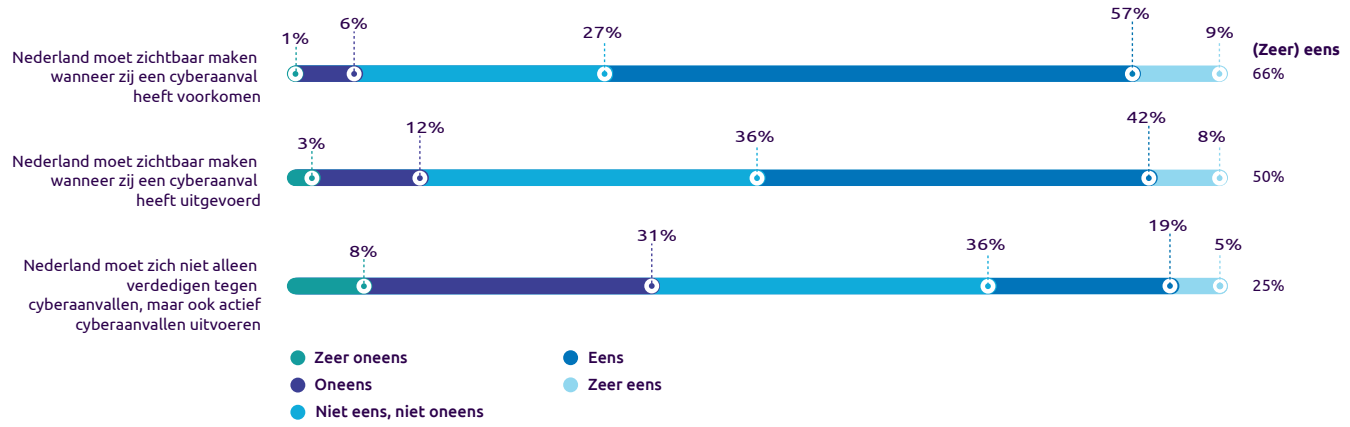
Rol overheid in vergroten digitale veiligheid



- De meerderheid ziet een rol weggelegd voor de overheid in het vergroten van de digitale veiligheid. Dit is met name een faciliterende rol: verruimen van bevoegdheden en extra wetgeving doorvoeren. Maar ook harder straffen en meer voorlichting geven, wordt door veel mensen toegejuicht. Dit waren ook een jaar geleden de vier belangrijkste acties die men van de overheid wilde zien.

Men wenst transparantie over voorkómen en uitgevoerde cyberaanvallen

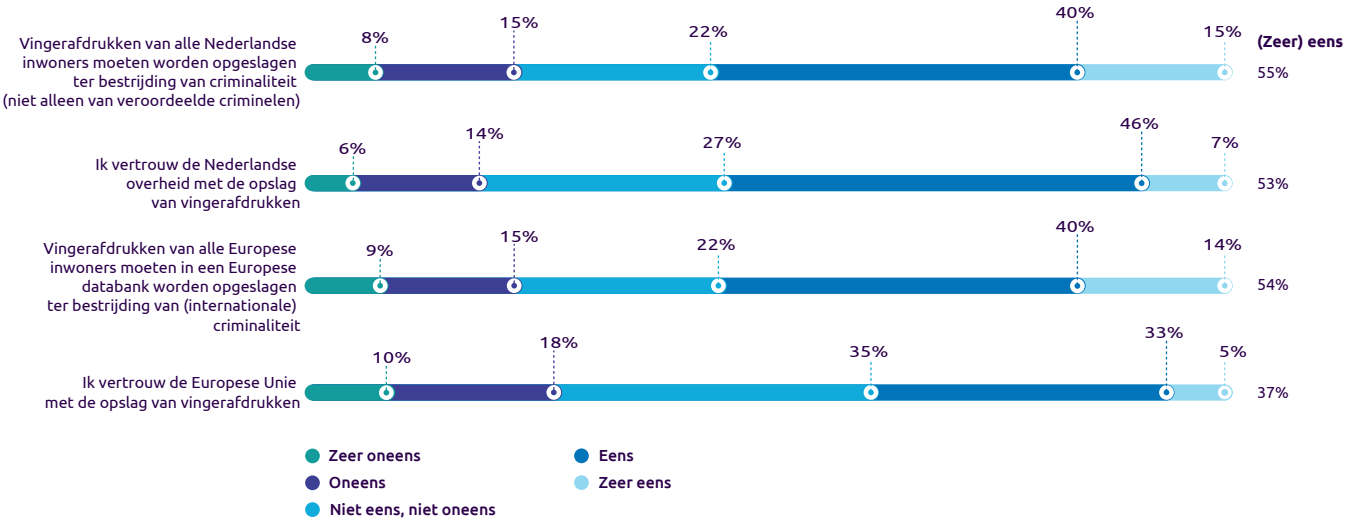
Verdediging tegen cyberaanvallen



- Tweederde wil graag op de hoogte gehouden worden wanneer Nederland een cyberaanval heeft voorkomen en de helft wil het weten wanneer Nederland zelf zo'n aanval heeft uitgevoerd.
- Het zelf uitvoeren van cyberaanvallen door Nederland stuit op weerstand: 39% is hier tegen (relatief vaak mannen en laagopgeleiden), 25% is hier voor (relatief vaak jongeren van 18-29 jaar en hoger opgeleiden).
- Degenen die vinden dat Nederland zelf actief cyberaanvallen moet uitvoeren, geven relatief vaak aan dat Nederland dit ook zichtbaar moet maken (77% vs. 45% van de tegenstanders).

Iets meer dan de helft is voorstander van de opslag van vingerafdrukken van burgers ter bestrijding van criminaliteit

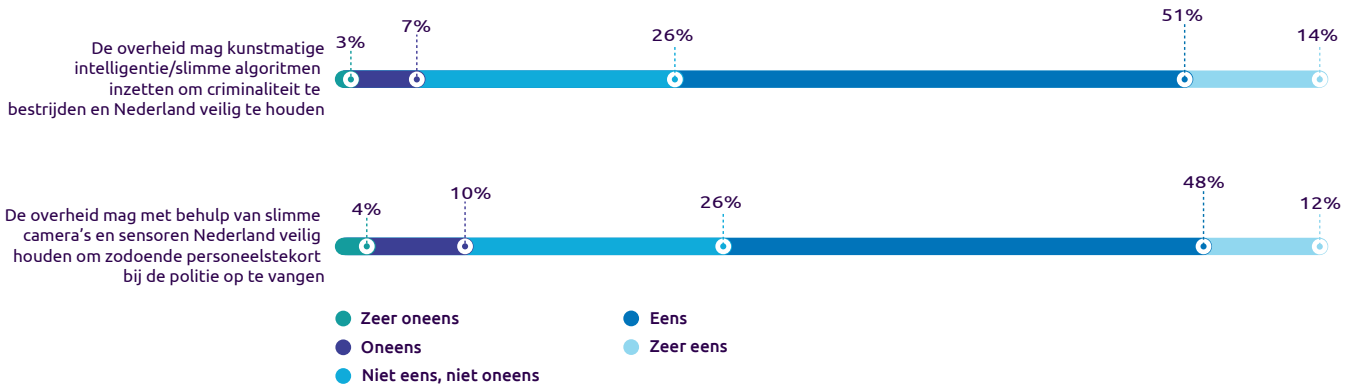
Gebruik vingerafdrukken



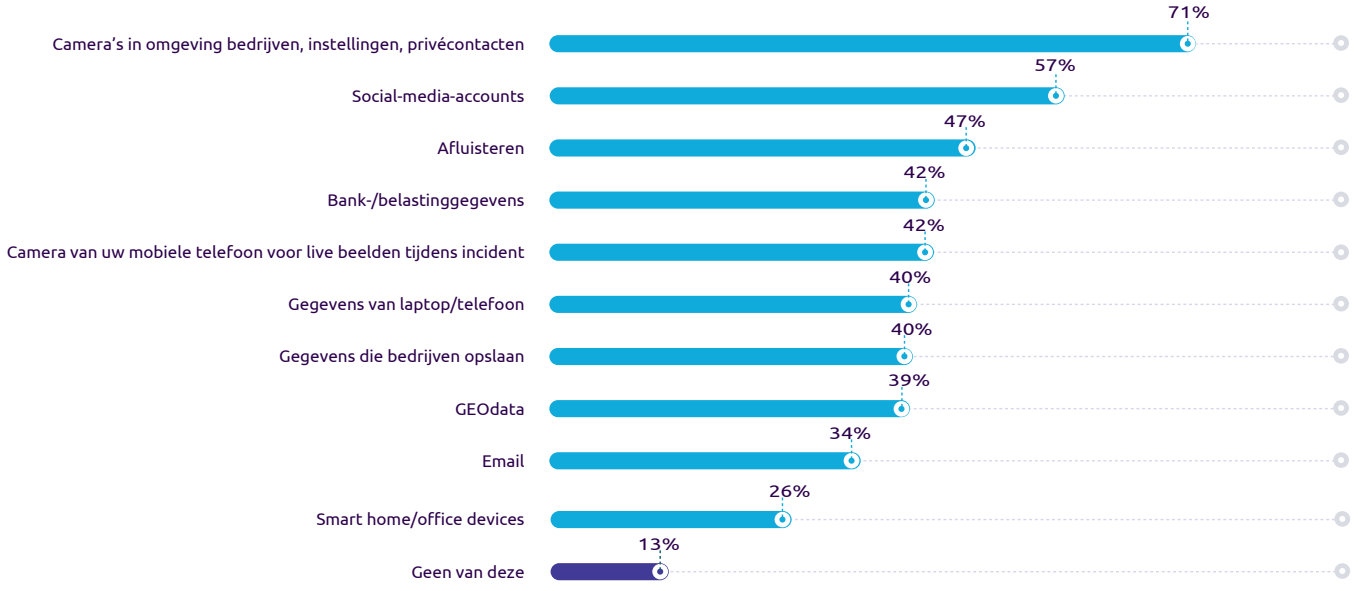
- 55% vindt dat vingerafdrukken van alle Nederlandse inwoners moeten worden opgeslagen ter bestrijding van criminaliteit. 54% vindt dat om diezelfde reden vingerafdrukken van alle Europese inwoners in een Europese databank moeten worden opgeslagen.
- Of men achter de opslag van vingerafdrukken staat, is deels een kwestie van vertrouwen: degenen die vertrouwen hebben in de Nederlandse overheid en de Europese Unie, staan relatief vaak positief tegenover de opslag van vingerafdrukken door deze partijen (resp. 76% en 79%).
- Men heeft voor de opslag van vingerafdrukken meer vertrouwen in de Nederlandse overheid dan in de Europese Unie (53% vs. 37%). Het vertrouwen in de Nederlandse overheid is flink toegenomen in het afgelopen jaar: van 39% eind 2019 naar 53% nu. Het vertrouwen in de Europese Unie is niet eerder uitgevraagd.

Er is draagvlak voor het gebruik van technologie door de overheid/politie voor de bestrijding van criminaliteit

Gebruik technologie door de overheid



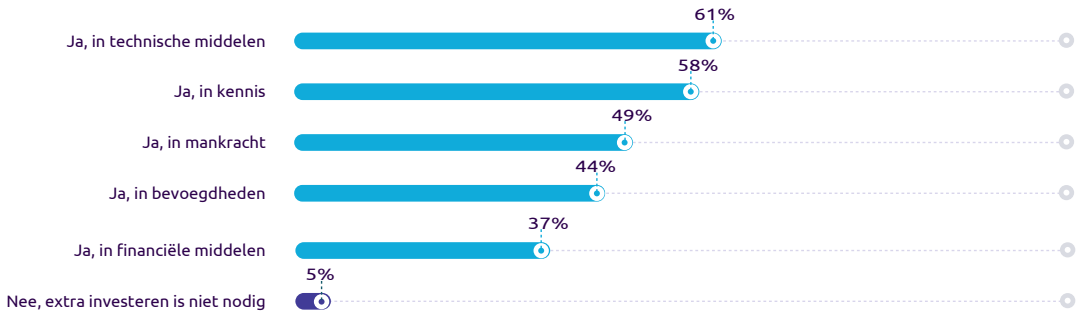
Mag door politie/meldkamer/overheid worden ingezien/gebruikt voor bestrijden van criminaliteit



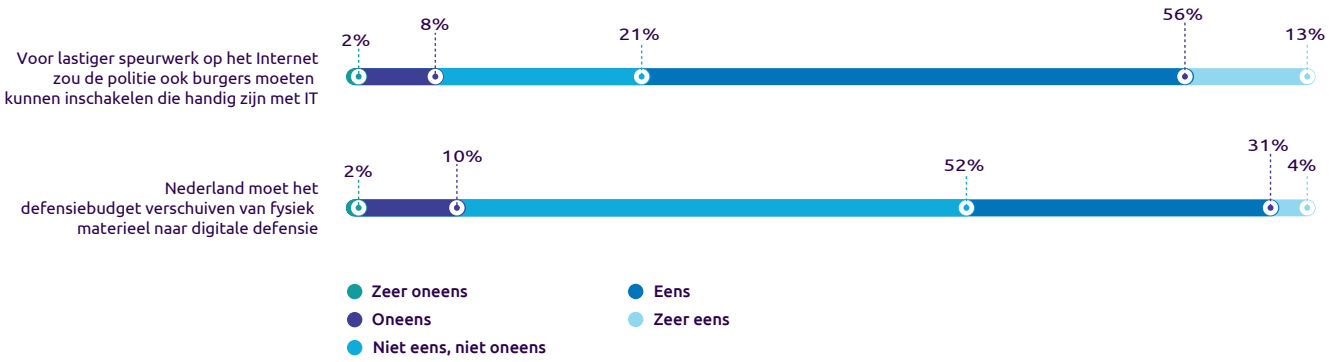
- De meerderheid heeft er geen bezwaar tegen dat de overheid of politie gebruikmaakt van technologie bij de bestrijding van criminaliteit. Dit kan in allerlei vormen: kunstmatige intelligentie/slimme algoritmen (65%), slimme camera's en sensoren als oplossing voor het personeelstekort bij de politie (60%), camera's in de nabije omgeving van bedrijven, instellingen of privécontacten (71%), social-media-accounts (57%), etc. Voor het gebruik van sommige databronnen is het draagvlak beperkt, zoals voor het gebruik van data van smart home/office devices en e-mail.

Steun voor extra investering in veiligheid door politie en overheid, met name in technische middelen en kennis. Op dit laatste vlak kan ook de inzet van IT-handige burgers helpen

Mening over extra investering door politie/overheid om Nederland veilig te houden



Herkomst investeringen



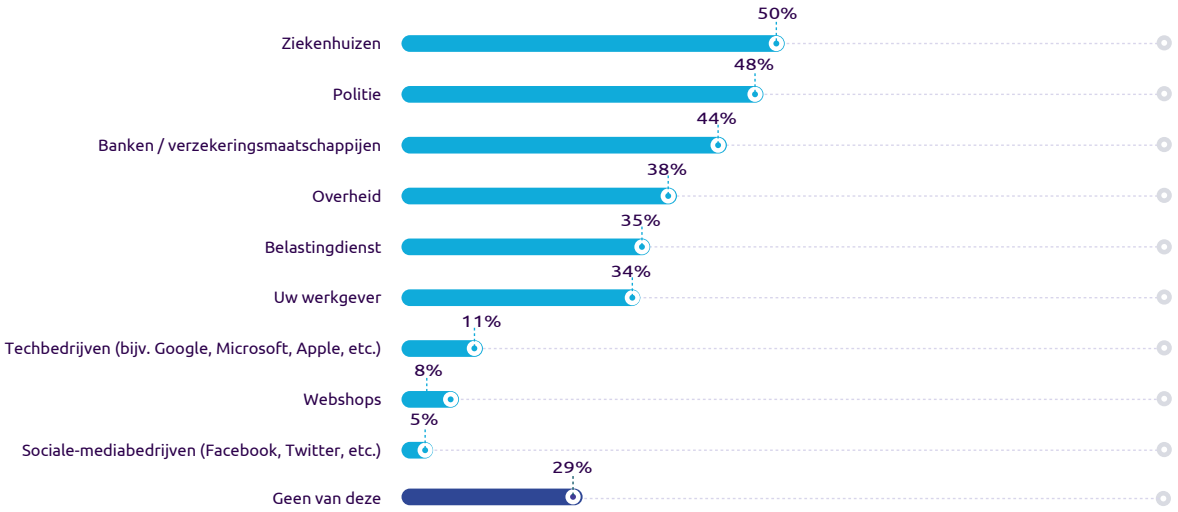
- Nagenoeg iedereen staat achter extra investeringen door politie of overheid om Nederland veilig te houden (95%). Hierbij denkt men met name aan technische middelen en kennis, en pas in derde instantie aan extra mankracht.
- Van degenen die vinden dat de politie/overheid extra moet investeren in kennis, vindt 72% het een goed idee dat de politie burgers die handig zijn met IT inschakelt voor lastiger speurwerk op het internet. 10% keurt dit idee af. Hiermee scoren zij niet anders dan degenen die een extra investering in kennis niet nodig vinden.
- 37% vindt dat er extra financiële middelen nodig zijn om Nederland veilig te houden. Hierbij kan ook worden gedacht aan het anders inzetten van defensiebudget. 43% van degenen die extra financiële middelen nodig vinden, vindt dat Nederland het defensiebudget moet verschuiven van fysiek materieel naar digitale defensie. Deze oplossing spreekt met name degenen aan die zich zorgen maken over een digitale aanval op Nederland (48%) en degenen die banger zijn voor een digitale aanval dan voor een fysieke aanval (47%).

3 Vertrouwen in instanties

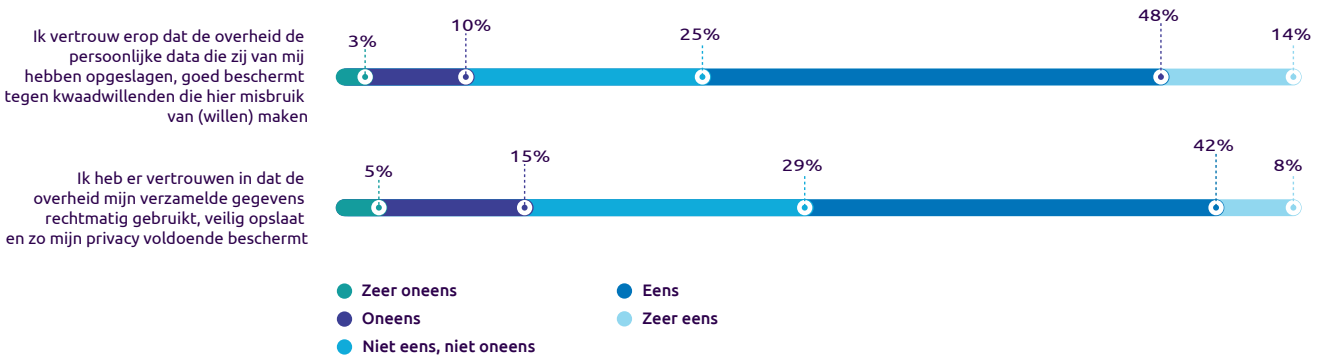
In hoeverre vertrouwt men instanties persoonlijke data toe?

Niet iedereen heeft er vertrouwen in dat de overheid veilig omgaat met persoonlijke gegevens van burgers

Vertrouwen in veilig omgaan met uw gegevens



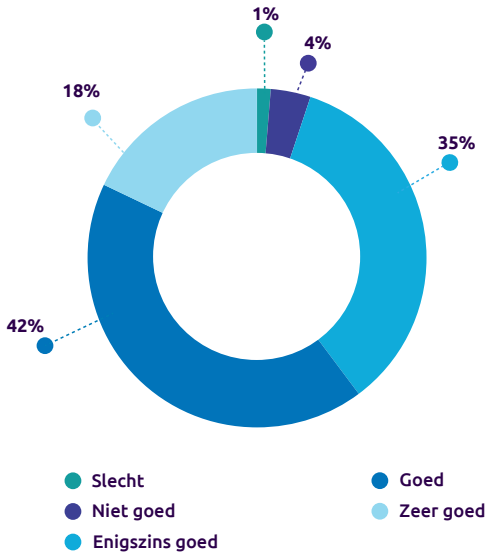
Vertrouwen in overheid



- 38% heeft er vertrouwen in dat de overheid veilig omgaat met hun gegevens. De overheid scoort daarmee slechter dan ziekenhuizen, politie en banken/verzekeringsmaatschappijen. Het vertrouwen in de overheid is relatief hoog onder jongeren van 18-29 jaar (48%) en hoogopgeleiden (42%).
- Wanneer er in iets meer detail wordt gekeken naar de overheid, blijkt het vertrouwen in de overheid toch iets groter: 62% vertrouwt erop dat de overheid de persoonlijke data die zij hebben opgeslagen van burgers goed beschermen tegen kwaadwillen die hier misbruik van willen maken en 51% heeft er vertrouwen in dat de overheid die gegevens rechtmatig gebruikt, veilig opslaat en zo de privacy van de burger voldoende beschermt.

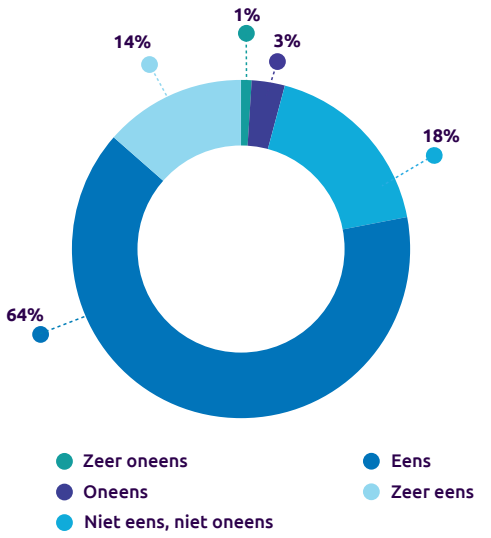
Niet iedereen heeft er vertrouwen in dat de overheid veilig omgaat met persoonlijke gegevens van burgers

Uitwisselen persoonsgegevens door inlichtingendiensten ter bestrijding van terrorisme of fraude



- 60% staat er positief tegenover dat verschillende inlichtingendiensten gegevens over personen uitwisselen voor het bestrijden van criminaliteit. Mannen en hoogopgeleiden staan hier relatief vaak positief tegenover (resp. 69% en 66%).
- 78% verwacht dat de politie inzage heeft in de eventuele historie bij de politie (zoals eerdere meldingen en aangiften) van iemand die contact met hen zoekt. Dit is wat vaker het geval onder degenen die vertrouwen hebben dat de politie veilig met hun gegevens omgaat dan onder degenen die dat vertrouwen niet hebben (86% vs.71%).

Wanneer ik contact zoek met de politie, verwacht ik dat de politie inzage heeft in mijn eventuele historie bij de politie (zoals eerdere meldingen en aangiften)

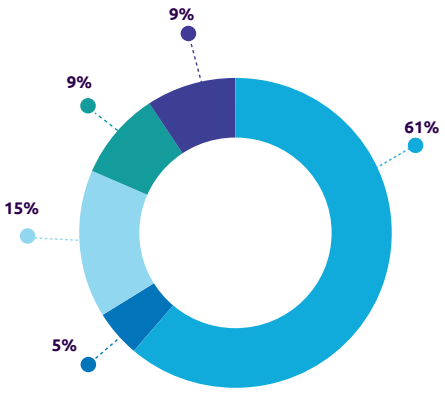


4 Hoe veilig waant men zichzelf?

- Welke ervaring heeft men met internetcriminaliteit?
- Hoe groot acht men het risico om slachtoffer te worden?
- Wat doet men om zichzelf te beschermen?

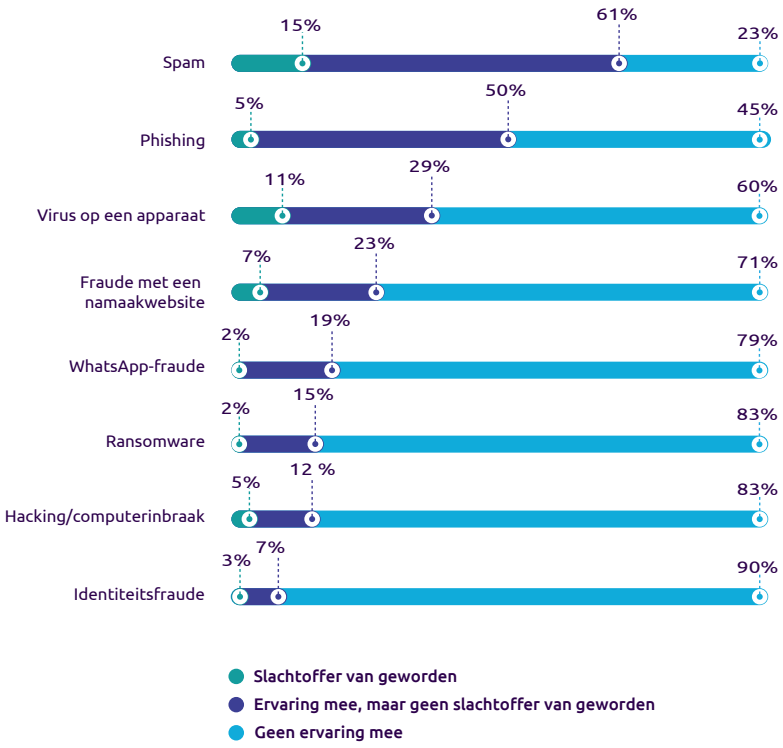
Meerderheid is weleens in aanraking gekomen met internetcriminaliteit, ruim een kwart is slachtoffer geworden

Ervaring met internetoplichting



- Nee, dat heb ik nooit meegemaakt
- Ik heb een poging tot oplichting meegemaakt en heb daarvan melding van gemaakt bij de politie
- Ik heb een poging tot oplichting meegemaakt, maar heb daarvan geen melding gemaakt bij de politie
- Ik ben opgelicht en heb daarvan melding gemaakt bij de politie
- Ik ben opgelicht, maar heb daarvan geen melding gemaakt bij de politie

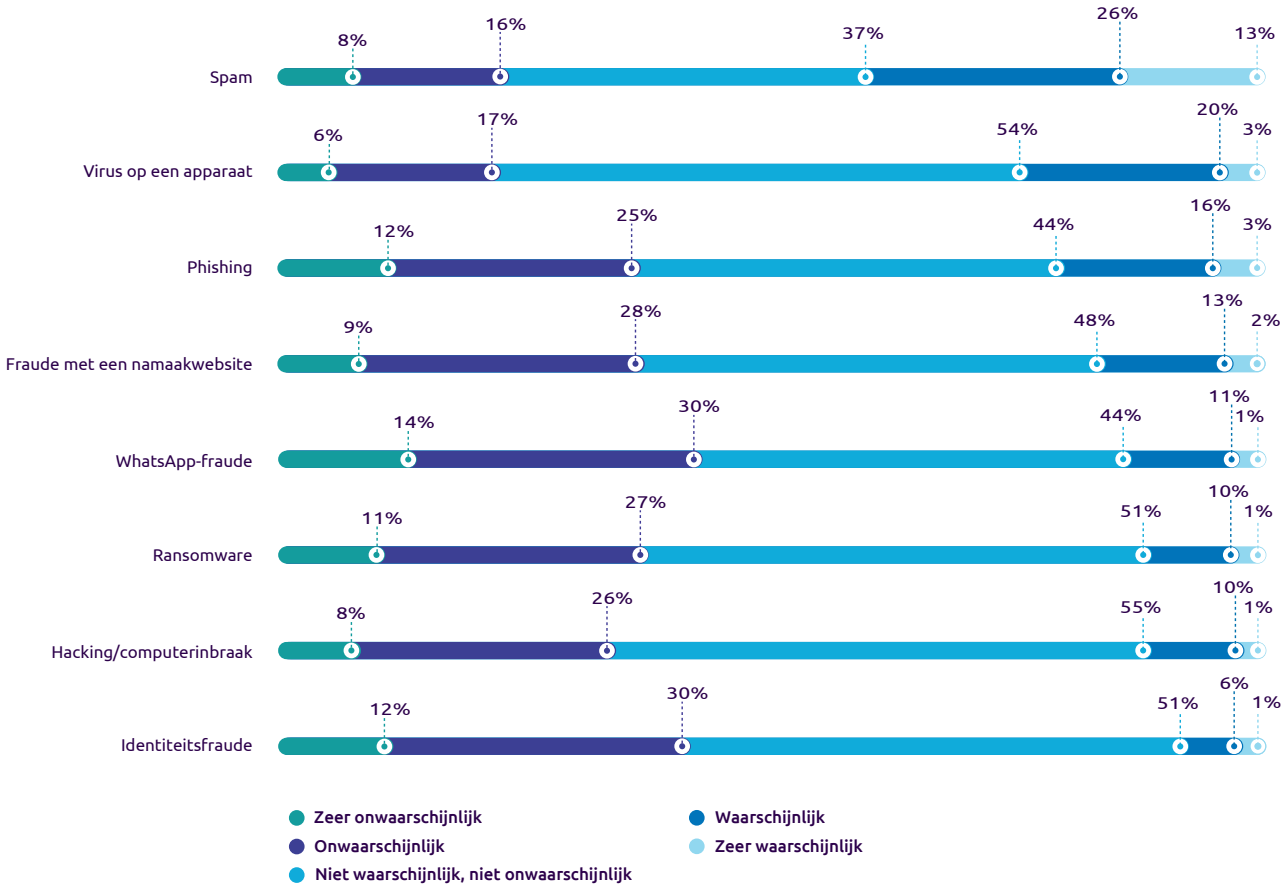
Ervaring met internetoplichting



- 39% heeft ervaring met internetoplichting: in 52% van die gevallen bleef het bij een poging tot, bij 48% was er daadwerkelijk sprake van oplichting.
- Wanneer er sprake is van oplichting, wordt daarvan vaker melding gemaakt bij de politie dan wanneer het slechts een poging betreft (50% vs. 24%).
- 86% heeft met minimaal één van de voorgelegde vormen van internetcriminaliteit ervaring (en is daar al dan niet slachtoffer geworden), 28% is van minimaal één van de vormen slachtoffer geworden. Spam en phishing zijn de vormen van internetcriminaliteit waar men het meest mee in aanraking is gekomen. De meeste slachtoffers zijn gevallen door spam, virussen en fraude met een namaakwebsite.

Eerdere ervaring met internetcriminaliteit zorgt voor een grotere bewustwording van de risico's om slachtoffer te worden

Inschatting slachtoffer te worden van internetcriminaliteit in de komende twee jaar

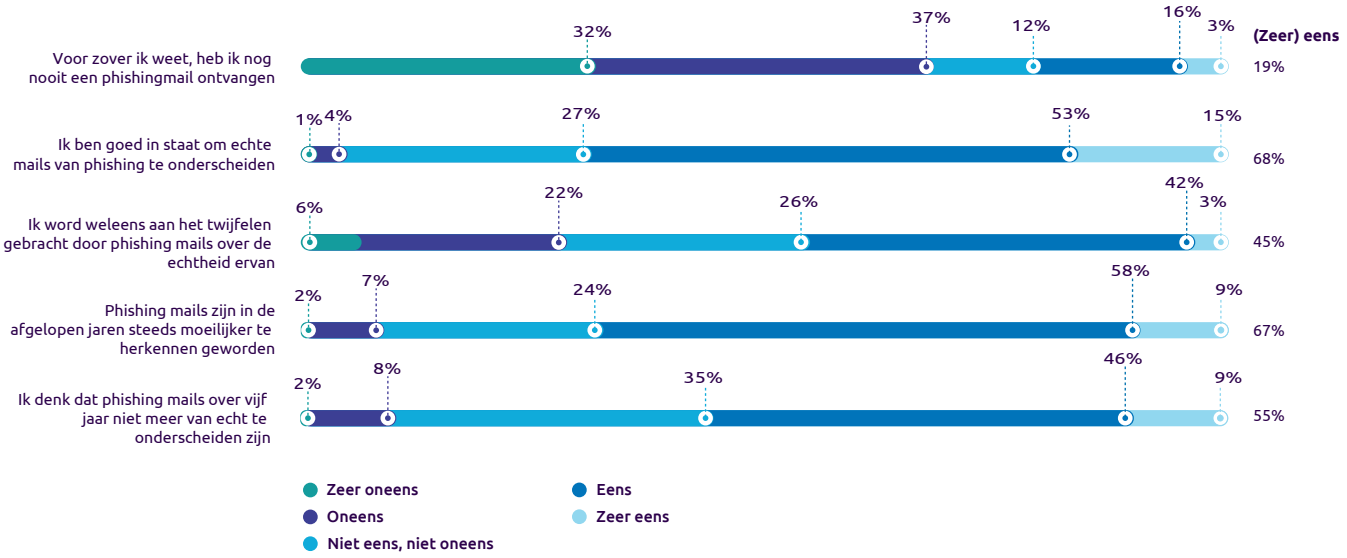


% (zeer) waarschijnlijk dat zij hier in de komende twee jaar slachtoffer van worden	Geen ervaring mee	Ervaring mee, geen slachtoffer	Slachtoffer van geworden
Spam	20%	38%	75%
Virus op een apparaat	12%	36%	51%
Phishing	12%	24%	37%
Fraude met een namaakwebsite	9%	27%	42%
WhatsApp-fraude	10%	20%	24%
Ransomware	7%	27%	30%
Hacking/computerinbraak	8%	19%	28%
Identiteitsfraude	6%	19%	10%

- De volgorde van de diverse vormen van internetcriminaliteit is qua risico-inschatting nagenoeg hetzelfde als qua ervaring ermee. Alleen phishing en virus op een apparaat hebben van plek gewisseld.
- Over het algemeen geldt dat degenen die in aanraking zijn gekomen met of zelfs slachtoffer zijn geworden van een bepaalde vorm van internetcriminaliteit, het relatief vaak waarschijnlijk achten dat zij hier in de komende twee jaar slachtoffer van worden. Zijn zij zich beter bewust geworden van hun kwetsbaarheid of weten zij van zichzelf dat zij minder goed in staat zijn om zichzelf te beschermen?

Men vindt het steeds lastiger om phishing mails te herkennen, met name slachtoffers geven aan dat zij daar moeite mee hebben

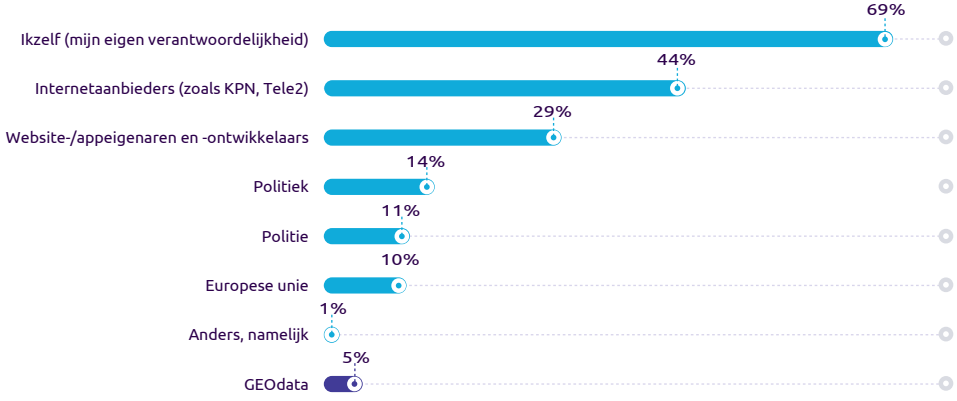
Phishing



- Eerder zagen we dat 55% ervaring heeft met phishing, 5% is er zelfs slachtoffer van geworden. En 19% acht het (zeer) waarschijnlijk dat zij hier in de komende twee jaar slachtoffer van worden.
- 67% geeft aan dat phishing mails in de afgelopen jaren steeds moeilijker te herkennen zijn geworden. Van hen meent 68% dat phishing mails over vijf jaar niet meer van echt te onderscheiden zijn.
- Slachtoffers van phishing achten zichzelf minder goed in staat om echte mails van phishing te onderscheiden (39%, versus 78% van degenen die ermee in aanraking zijn gekomen maar geen slachtoffer zijn geworden, en 62% van degenen zonder ervaring). Degenen die met phishing in aanraking zijn gekomen zonder er slachtoffer van te worden, geven relatief vaak aan dat zij weleens aan het twijfelen worden gebracht (50%, vs. 45% van de slachtoffers en 38% van degenen zonder ervaring met phishing).

Nederlanders zien hun digitale veiligheid vooral als hun eigen verantwoordelijkheid

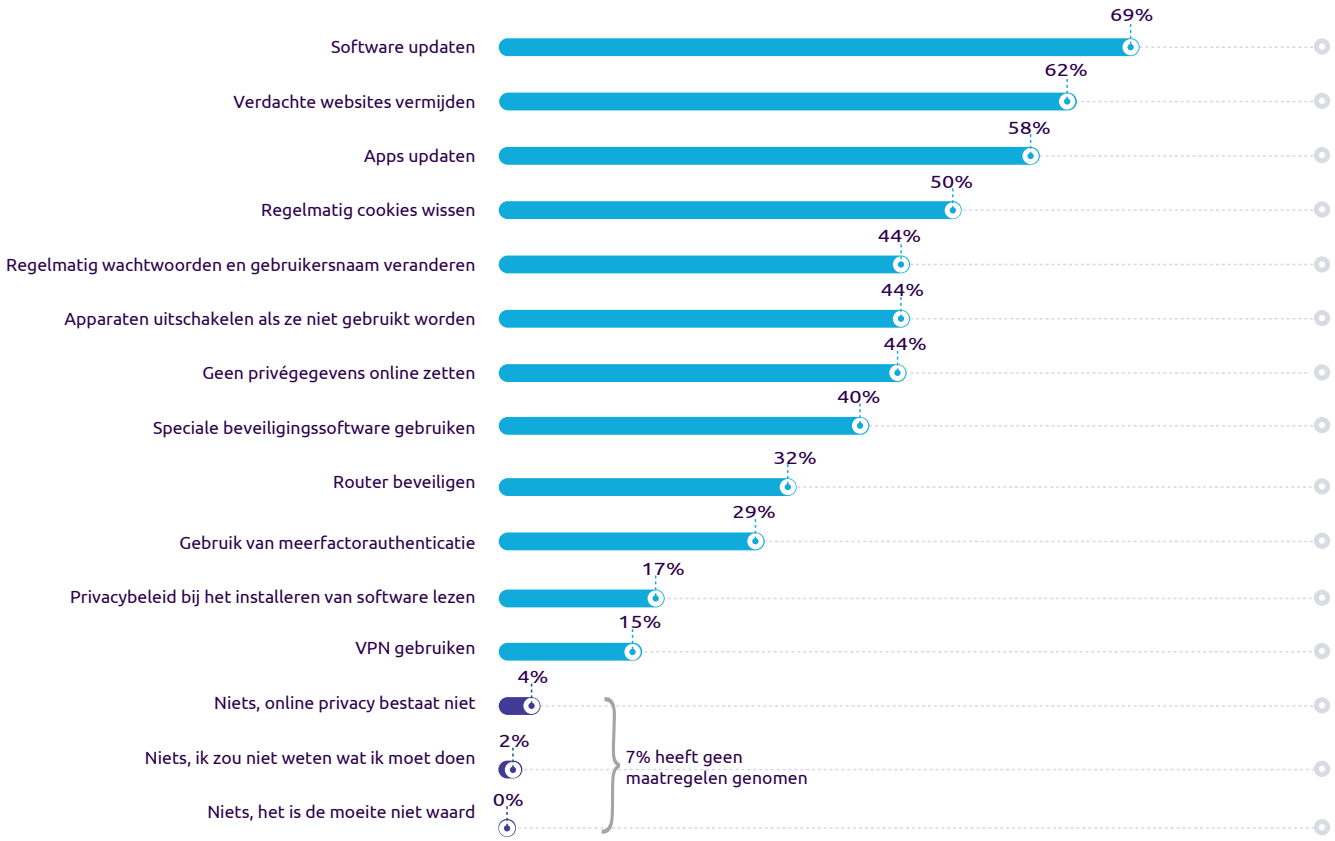
Verantwoordelijk voor uw digitale veiligheid



- Men houdt men name zichzelf verantwoordelijk voor zijn of haar digitale veiligheid, nog meer dan eind 2019/begin 2020 (62%). Ook legt men de verantwoordelijkheid nu wat vaker bij website-/appeigenaren en -ontwikkelaars (29% vs. 24%) en bij de politie (11% vs. 4%) en juist wat minder bij de politiek (14% vs. 21%).

Meest genomen maatregelen ter bescherming van privacy: software en apps updaten en verdachte websites vermijden

Genomen maatregelen om online privacy te beschermen



- Diverse maatregelen worden door hoger opgeleiden en door mannen vaker genomen dan door laag opgeleiden. Laag opgeleiden en vrouwen geven relatief vaak aan dat zij niet zouden weten wat zij moeten doen (beide 5%).

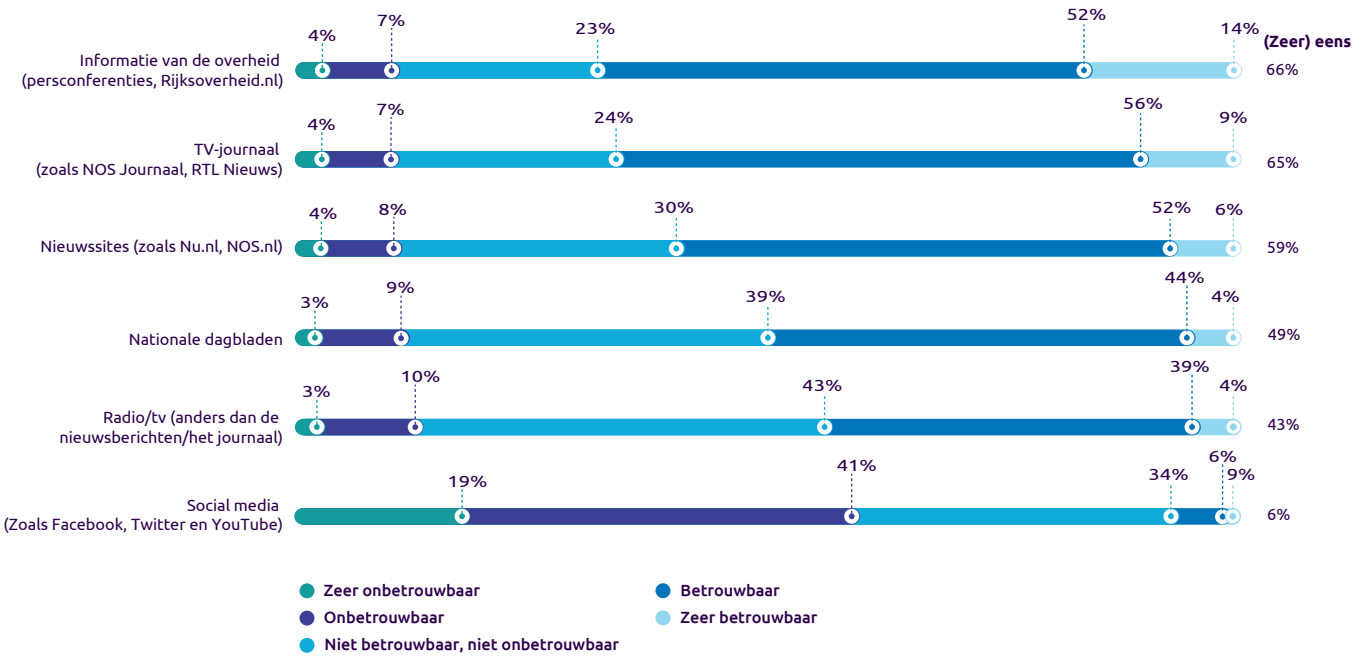
5 Actuele thema's

- Corona
- Tweede Kamerverkiezingen
- Nepnieuws

5a Corona

Alle informatiebronnen hebben te maken met veel twijfel over de betrouwbaarheid van de berichtgeving over het coronavirus

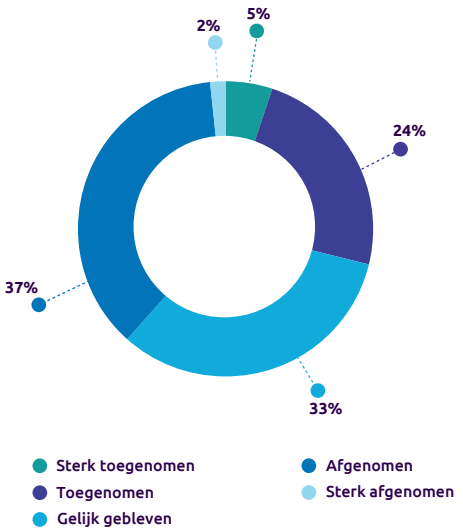
Betrouwbaarheid berichtgeving omtrent coronavirus via diverse bronnen



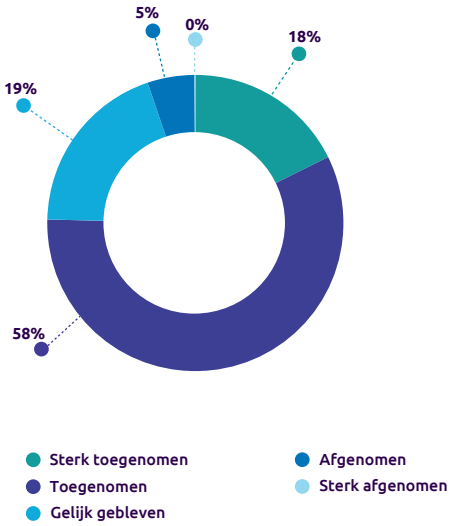
- Berichtgeving over het coronavirus vanuit de overheid en TV-journaals wordt als het meest betrouwbaar gepercipieerd. Toch geeft ook bij deze bronnen nog een kwart aan dat zij de informatie 'niet betrouwbaar, niet onbetrouwbaar' vinden en 11% dat zij de informatie (zeer) onbetrouwbaar vinden.
- Er wordt veel gesproken dat jongeren onvoldoende bereikt zouden worden door de communicatie vanuit de overheid over corona. Toch duidt de jongste groep (18-29 jaar) de informatie van de overheid het vaakst aan als betrouwbaar (74%).
- Voor alle bronnen, met uitzondering van social media, geldt dat het vertrouwen onder hoogopgeleiden groter is dan onder lager opgeleiden. Bij social media is juist het omgekeerde het geval, daar zijn hoogopgeleiden relatief vaak sceptisch over.

Men meent dat tijdens corona veel criminaliteit zich heeft verplaatst van offline naar online

Offline criminaliteit sinds corona



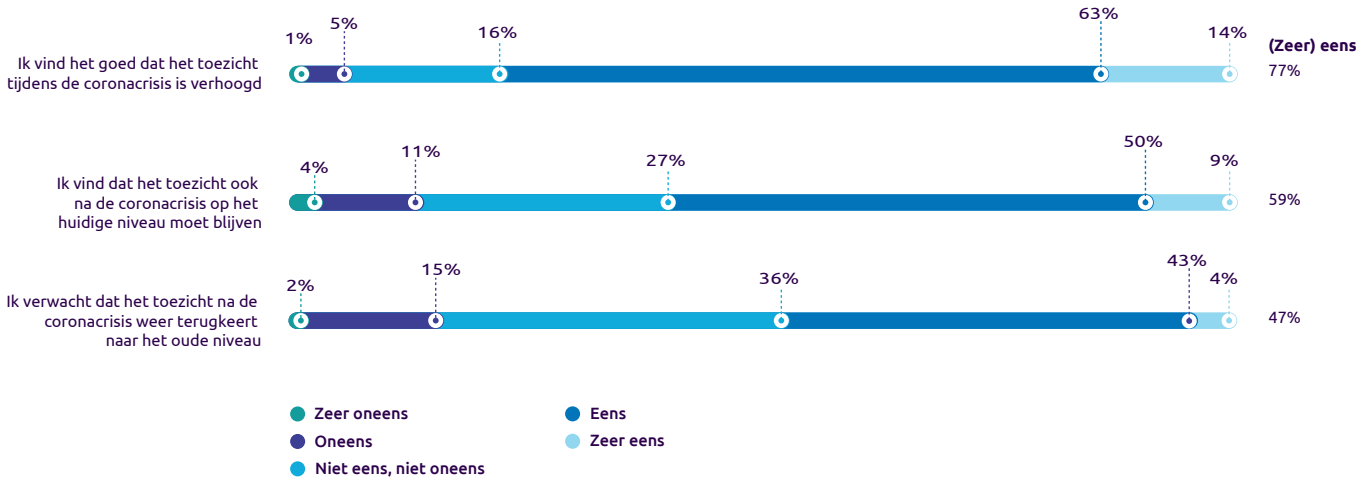
Online criminaliteit sinds corona



- 29% meent dat de **offline** criminaliteit sinds corona is toegenomen, 38% dat die is afgenomen. In plaats daarvan is meer **online** criminaliteit gekomen: 75% meent dat dat sinds corona is toegenomen, slechts 5% dat het is afgenomen.

Zes op de tien hoopt dat het verhoogd toezicht ook na de coronacrisis blijft, maar velen verwachten anders

Verhoogd toezicht door corona

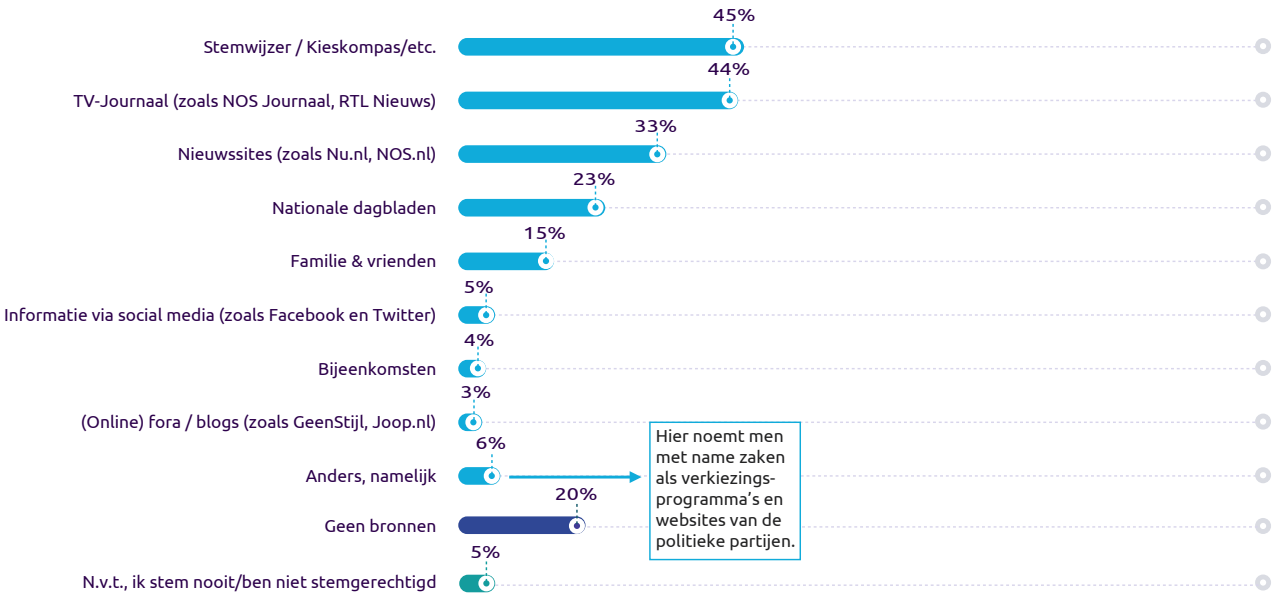


- De meerderheid vindt het goed dat er tijdens de coronacrisis sprake is van verhoogd toezicht. Met name de ouderen zijn hier blij mee (50-64 jaar: 80%, 65-plussers: 92%), terwijl jongeren hier relatief vaak negatief tegenover staan (18-39 jaar: 12%).
- Van degenen die achter het huidige verhoogd toezicht staan, vindt 69% dat het verhoogd toezicht gehandhaafd moet blijven na de coronacrisis. Echter, 51% van hen verwacht dat het weer zal terugkeren naar het oude niveau.
- Van degenen die vinden dat het toezicht ook na de coronacrisis op het huidige niveau moet blijven, verwacht 42% dat het weer terugkeert naar het oude niveau.

5b Tweede Kamerverkiezingen

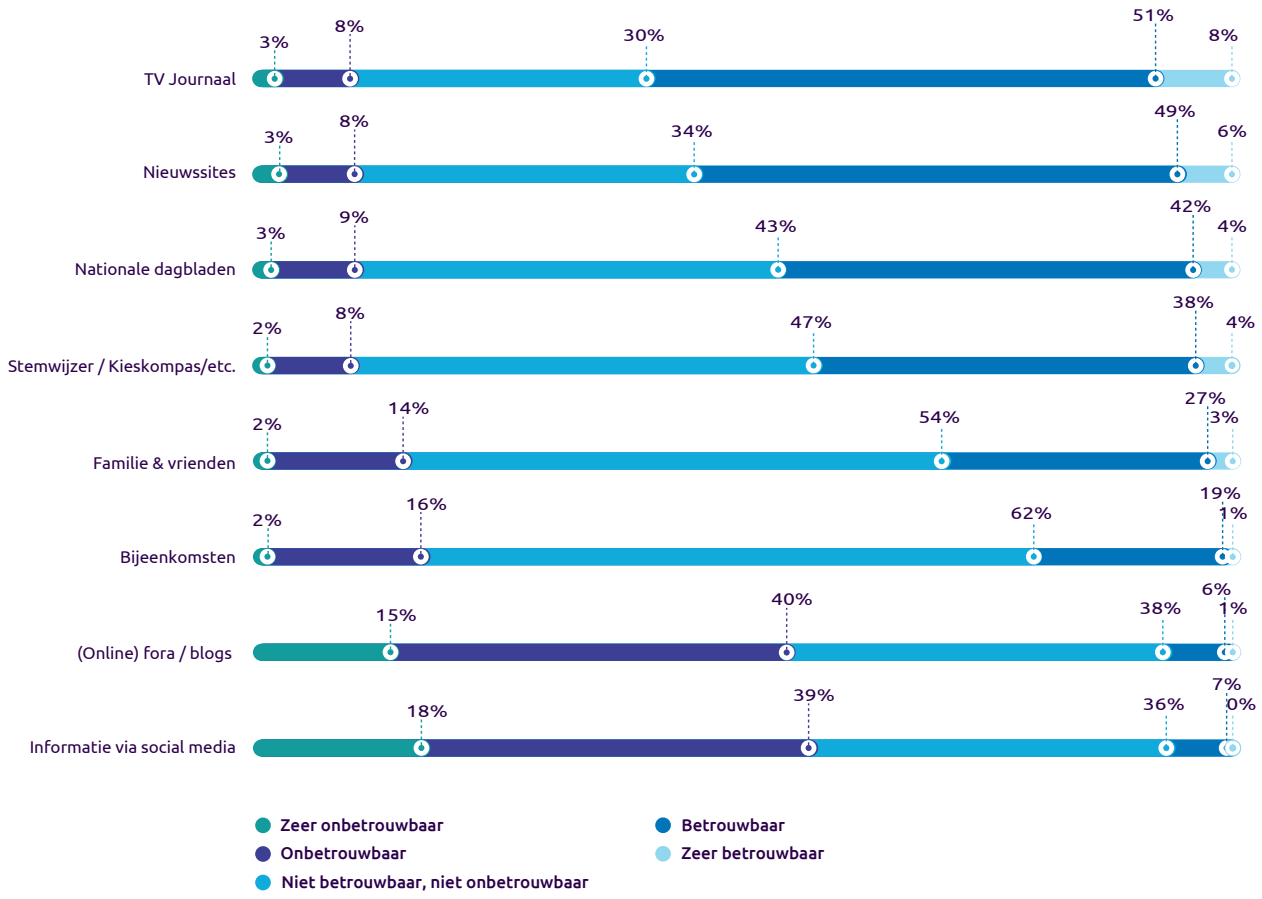
Stemwijzer/Kieskompas zeer populair, ondanks twijfels over de betrouwbaarheid

Informatiebronnen die men gebruikt bij het maken van een keuze bij de Tweede Kamerverkiezingen



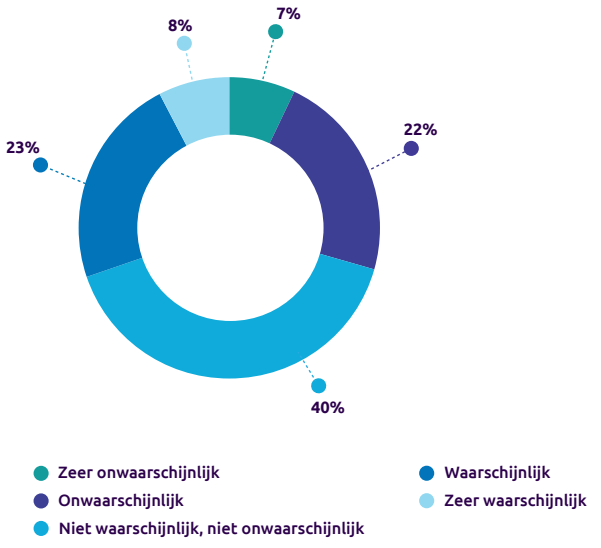
- Bij het maken van een keuze voor de aanstaande Tweede Kamerverkiezingen denkt men met name gebruik te maken van Stemwijzer/Kieskompas het TV-journaal.
- Hoewel de gebruiksintentie van Stemwijzer/Kieskompas groot is, zijn velen niet overtuigd over de betrouwbaarheid ervan. 31% van degenen die deze bron wil gebruiken, vindt deze 'niet betrouwbaar, niet onbetrouwbaar' en 4% vindt het zelfs (zeer) onbetrouwbaar.
- Het TV-journaal en nieuwssites, na Stemwijzer/Kieskompas de meest gebruikte informatiebronnen, scoren beter op betrouwbaarheid.

Betrouwbaarheid informatie omtrent Tweede Kamerverkiezingen via diverse bronnen



Meerderheid houdt rekening met pogingen tot beïnvloeding Tweede Kamerverkiezingen door andere landen

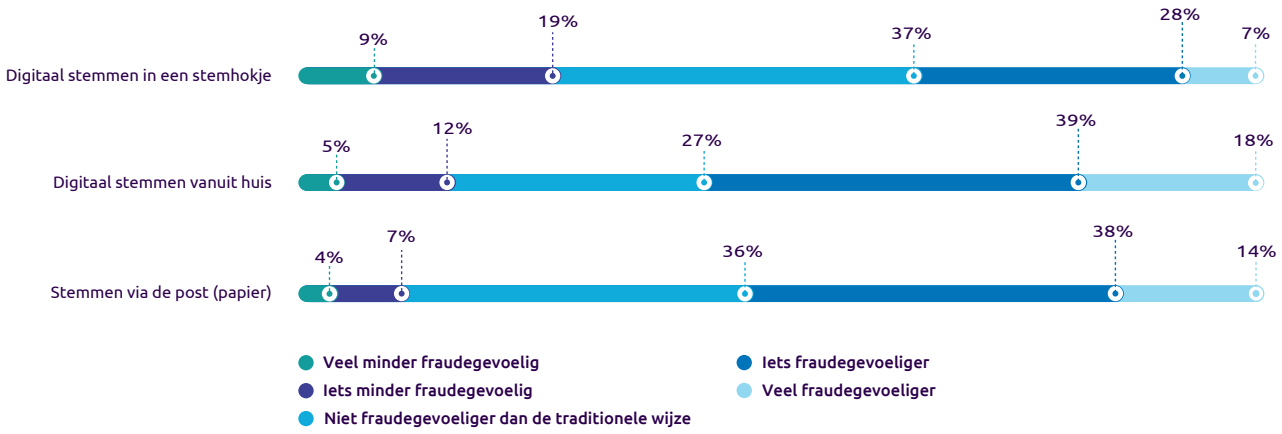
Invloed vanuit andere landen op de Nederlandse Tweede Kamerverkiezingen



- 30% acht het (zeer) waarschijnlijk dat andere landen invloed proberen uit te oefenen op de Nederlandse Tweede Kamerverkiezingen en nog eens 40% spreekt dat niet tegen (‘niet waarschijnlijk, niet onwaarschijnlijk’).

Voor en tegenstanders voor digitaal stemmen. Stemmen op afstand gezien als meer fraudegevoelig dan in een stemhokje

Fraudegevoeligheid alternatieve stemwijzen t.o.v. de traditionele wijze

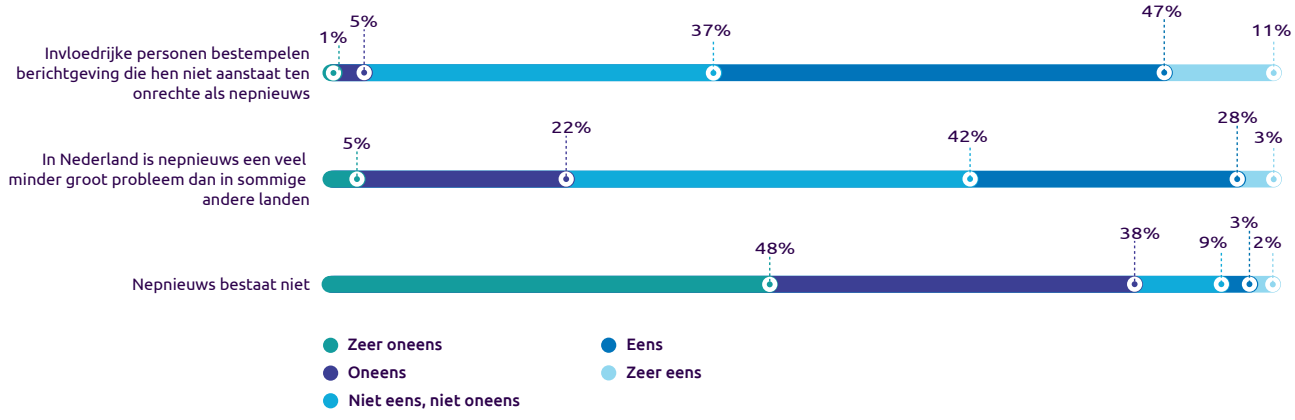


- Traditioneel gebeurt stemmen in Nederland nog steeds met potlood en papier, in een stemhokje. Vanwege de coronapandemie mogen 70-plussers bij de Tweede Kamerverkiezingen op 17 maart hun stem uitbrengen via de post. 53% vindt dit echter fraudegevoeliger. Onder 70-plussers zelf is dat 43%.
- Er gaan ook al jaren geluiden op om digitaal stemmen mogelijk te maken. In dat geval gaat de voorkeur uit naar digitaal stemmen in een stemhokje. Dat wordt als minder fraudegevoelig gezien dan digitaal stemmen vanuit huis. 27% vindt digitaal stemmen vanuit een stemhokje zelfs minder fraudegevoelig dan de traditionele manier van stemmen.
- Hoger opgeleiden geven van alle drie de alternatieven relatief vaak aan dat zij deze fraudegevoeliger vinden dan de traditionele wijze van stemmen.

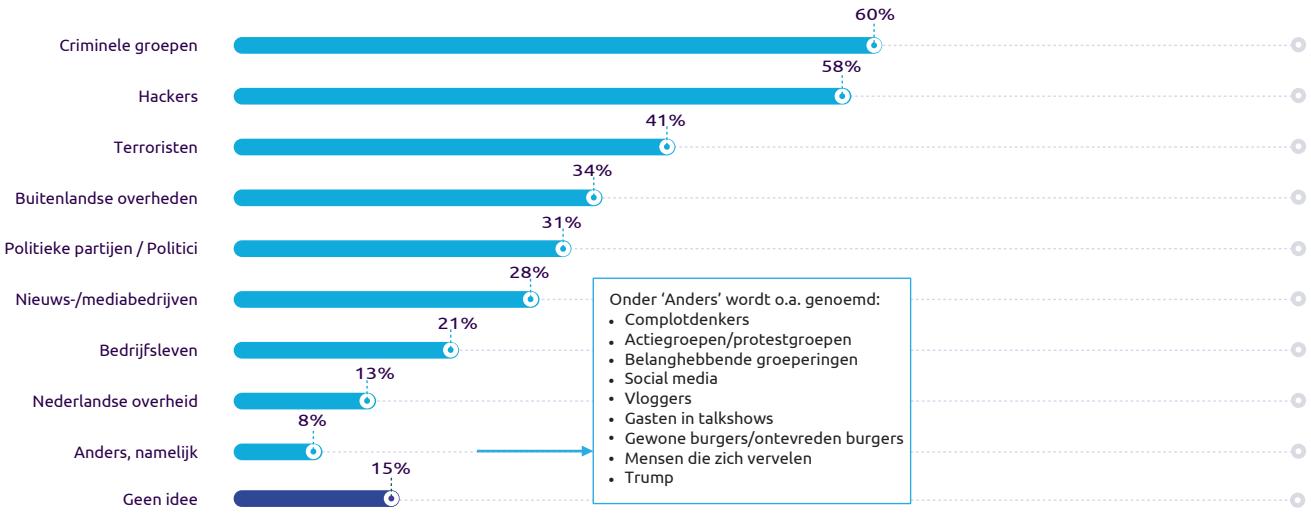
5c Nepnieuws

De meerderheid onderschrijft het bestaan van nepnieuws en schrijft dat met name toe aan criminele groepen en hackers

Vóórkomen van nepnieuws



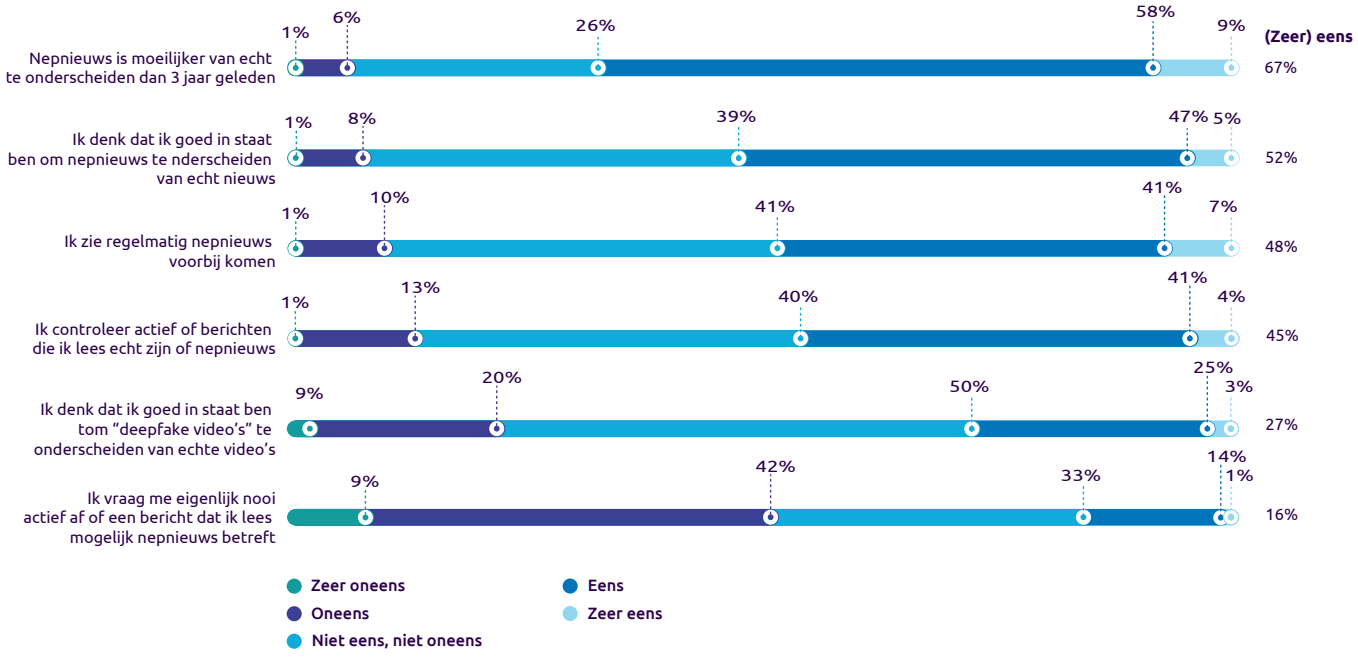
Herkomst van nepnieuws



- De meerderheid onderschrijft het bestaan van nepnieuws, slechts een kleine groep (5%) ontkent dit. Wel is een wat grotere groep van mening dat nepnieuws in ons land een minder groot probleem is dan in sommige andere landen (31%).
- Het feit dat er nepnieuws bestaat, wordt volgens 58% ook weleens misbruikt: zij zijn van mening dat invloedrijke personen berichtgeving die hen niet aanstaat weleens onterecht aanduiden als nepnieuws.
- Voor de oorsprong van nepnieuws wijst men met name naar criminele groepen en hackers.

De helft twijfelt of zij nepnieuws nog kunnen herkennen, het is steeds lastiger om het onderscheid te maken tussen echt en nep

Herkennen van nepnieuws



Meer lezen? Zie ook het **internationale onderzoek naar** nepnieuws dat Ipsos in 2020 heeft uitgevoerd.

- 67% meent dat nepnieuws lastiger te herkennen is dan drie jaar geleden. Van hen acht 53% zichzelf goed in staat om nepnieuws van echt te onderscheiden en meent 52% regelmatig nepnieuws voorbij te zien komen.
- Men heeft meer moeite om deepfake video's te herkennen dan nepnieuws in het algemeen.
- 45% beweert actief te controleren of berichten die zij lezen echt zijn of nepnieuws. Zij achten zich relatief goed in staat om nepnieuws (65%) en deepfake video's (38%) te herkennen, al geeft 74% van hen wel aan dat nepnieuws nu moeilijker te herkennen is dan drie jaar geleden. Of deze groep daadwerkelijk zo actief is in het controleren op nepnieuws als zij zeggen, valt te betwijfelen: 14% van hen geeft aan dat zij zich eigenlijk nooit afvragen of een bericht dat zij lezen mogelijk nepnieuws betreft.

Voor de identificatie van nepnieuws kijkt men voornamelijk naar de bron/afzender, naar andere bronnen en stijl/taalgebruik

Afzender controleren

- Adres controleren.
- Afzender.
- Afzenderslotje.
- Afzender checken door met je muis op de afzender te gaan staan.
- Domeinnaam controleren.
- Het emailadres checken.

Bronnen controleren

- Bekijken van welke bron(nen) de informatie komt.
- Bron achterhalen.
- Bron checken.
- Bronnen opzoeken en controleren op echtheid.

Andere bronnen raadplegen

- Door bij twijfelen eerst te Googelen.
- Aan de hand van andere sites met hetzelfde nieuws.
- Of berichten ook elders staan gepubliceerd.
- Als ik iets lees, ook checken bij NOS.
- Andere bronnen raadplegen.
- Betrouwbare bronnen zoeken.
- Bij enige vorm van twijfel over een bericht ga ik op zoek naar andere bronnen die het bericht kunnen bevestigen al dan niet ontkrachten.
- Checken op de site van Radar.
- Controleren met andere, vertrouwde bonnen.

Stijl/taalgebruik

- Door de tekstopbouw.
- Hoe het geschreven is.
- Staan o.a. schrijffouten in.
- Door goed te lezen en de inhoudelijke tekst nauwkeurig te bekijken en de logica.
- Nepnieuws heeft vaak al een oordeel in artikelen.
- Wanneer er maar 1 kant van een verhaal wordt belicht en de mening van de andere kant totaal wordt genegeerd.
- Tekstopmaak.
- Ook te onderscheiden indien het technisch gezien niet heel goed gemaakt is.

Geloofwaardigheid

- Als er onwaarschijnlijke dingen in staan.
- Als iets te mooi is om waar te zijn, is dat vaak ook zo.
- Nepnieuws is vaak te ongeloofwaardig, overdreven, onlogisch.
- Nepnieuws klinkt meestal raar en moeilijk te geloven.

Opletten/gezond verstand gebruiken

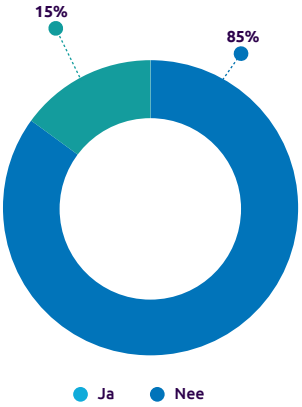
- Door gewoon na te denken.
- Door goed te kijken / Door goed te lezen.
- Door logisch na te denken en feiten op een rij te zetten.
- Door mijn gezonde verstand te gebruiken.
- Door op de hoogte te zijn dat er ook nepnieuws is.
- Onderbuikgevoel en logisch redeneren.

- 45% geeft aan actief te controleren of de berichten die zij lezen, echt zijn of nepnieuws. En 52% meent goed in staat te zijn om nepnieuws te onderscheiden van echt nieuws.
- In de toelichting op beide aspecten (hoe zij dat controleren en hoe zij dat onderscheid maken) komen dezelfde werkwijzen naar voren. Meest genoemd zijn:
  - Controleren van de afzender (o.a. emailadres en of er een slotje in de URL-balk van de browser staat)
  - Controleren van bronnen
  - Andere bronnen raadplegen (waaronder andere nieuwssites, Google, etc.)
- Daarnaast wordt er gelet op de stijl en het taalgebruik en op de geloofwaardigheid van het bericht.
- Tot slot geven veel mensen aan dat zij het onderscheid maken op gevoel, dat zij gewoon opletten en hun gezond verstand gebruiken.

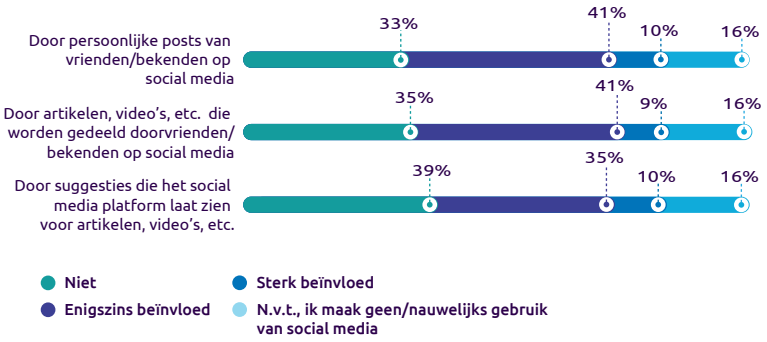
Meerderheid is bekend met het bestaan van de socialemediafuik. Deze kennis zorgt dat zij zich minder beïnvloedbaar voelen

Op de hoogte van de socialemediafuik?

"Gebruikers van sociale media (zoals Facebook, YouTube) krijgen vooral berichten te zien die aansluiten bij hun profiel. Dat profiel wordt bepaald en voortdurend bijgewerkt op basis van hun zoekgeschiedenis."



Gepercipieerde beïnvloeding door sociale media



- In oktober 2020 introduceerde Arjen Lubach in zijn programma Zondag met Lubach het woord fabeltjesfuik ter aanduiding van wat je de 'socialemediafuik van complotdenkers' zou kunnen noemen. Hierdoor is veel aandacht geweest voor de socialmediafuik. 85% zegt op de hoogte te zijn van het bestaan van zo'n socialemediafuik. 50-plussers en laagopgeleiden zijn hier wat minder mee bekend (resp. 21% en 32% niet).
- Degenen die niet op de hoogte zijn van het bestaan van de sociale mediafuik, geven relatief vaak aan dat zij geen/nauwelijks gebruikmaken van social media (32%).
- Gebruikers van sociale media die bekend zijn met de socialemediafuik denken minder vaak dat hun mening wordt beïnvloed door suggesties die het platform laat zien, dan gebruikers die niet bekend zijn met de fuik (53% vs. 64%).

Onderzoeksopzet | Hoe we dit onderzocht hebben

Met wie we hebben gesproken

- Doelgroep: Nederlanders van 18 jaar of ouder.
- Steekproef: n=1000.
- De data zijn achteraf gewogen zodat deze representatief zijn op geslacht, leeftijd, regio en opleiding.

Hoe hebben we met ze gesproken

- Online kwantitatief onderzoek op het Ipsos Online Interview Panel.
- Dataverzameling vond plaats van 1 t/m 5 februari 2021.

Capgemini – 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: Naar een Superslimme Samenleving?

De afgelopen decennia stonden in het teken van ongekende verandering. Digitalisering heeft onze manier van werken, produceren, consumeren, reizen, ontspannen en wonen ingrijpend veranderd. Daarbij lijkt de coronacrisis deze verandering nog te versnellen. Als we leven in een verandering van tijdperk dan lijkt dit nieuwe tijdperk zich aan te dienen als de superslimme samenleving, oftewel Society 5.0. Een samenleving waarin de grens tussen mensen en computer steeds vager wordt en de fysieke en digitale wereld meer dan ooit met elkaar verknoopt raken.

Oplossingen ontwikkelen zich steeds meer in ecosystemen. Dat geldt ook voor de overheid die naast haar traditionele rollen nu ook steeds vaker de innovatie rol krijgt

Het rapport geeft inzicht achter de drijvende technologieën achter Society 5.0. En de toepassingen van technologieën in onze samenleving zoals nieuwe manieren van werken, sociale inclusie, toegankelijkheid van overheidsdiensten, duurzaamheid, security & privacy én hoe dat bij elkaar komt in Smart Cities.

Waarom duurzaamheid collectieve actie, doortastend leiderschap en slimmere technologie vergt

Conversations for Tomorrow is gelanceerd door het Capgemini Research Institute en is een nieuwe Engelstalige publicatie waarin wordt gesproken met internationale bestuurders en deskundigen over strategieën voor de toekomst van het bedrijfsleven en de samenleving. Het thema voor de eerste editie is duurzaamheid, en is getiteld "Why sustainability means collective action, bolder leadership, and smarter technologies". In deze eerste editie wordt samen met bestuurders en deskundigen dieper ingegaan op het thema duurzaamheid en wat dit betekent voor het bedrijfsleven en de samenleving. Het biedt diepgravende inzichten om wereldwijde strategische programma's te voeden die gericht zijn op het creëren van een duurzamere toekomst. Met onder andere een bijdrage van Frans Timmermans, executive vice-president van de Europese Commissie voor de European Green.

Spelen met technologie voor een Superslimme Samenleving

De Superslimme Samenleving – ook aangeduid als Society 5.0 – komt eraan. Dat gebeurt op de vleugels van innovatieve technologieën die tot voor kort exclusief tot het domein van hightech leken te behoren. Nu zulke technologieën gemeengoed worden, komen de voordelen van een Superslimme Samenleving onder handbereik. Daarvoor moeten nog wel muren worden geslecht. Technologie moet speelser worden, makkelijker toegankelijk voor een meer diverse groep van betrokkenen. Technovision is een raamwerk dat speciaal daarvoor ontworpen is.

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

Overige Capgemini blogs via:

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

Global: www.capgemini.com/blog

Colofon

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

Lisa Marie Brouwer
Zeger de Bruijne
Pablo Derksen
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, Anindya Chakrabarti & Runa Roychowdhury.

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

Dit rapport is gedrukt op BalanceSilk, papier gemaakt van 60% gerecycleerde en 40% primaire FSC-gecertificeerde vezels.

Over Capgemini

Capgemini is een wereldwijde, maatschappelijk verantwoorde en multiculturele marktleider met 270.000 mensen in bijna 50 landen. Als strategisch partner ondersteunt Capgemini organisaties bij hun transformatie door gebruik te maken van de kracht van technologie. Hierbij laat de Group zich leiden door zijn bestaansreden: menselijke energie vrijmaken door middel van technologie voor een inclusieve en duurzame toekomst. Met meer dan 50 jaar ervaring en expertise in uiteenlopende sectoren, vertrouwen klanten de aanpak van hun zakelijke behoeften toe aan Capgemini: van strategie en ontwerp tot operationeel beheer. Dit gebeurt door gebruik te maken van innovaties in cloud, data, kunstmatige intelligentie, connectiviteit, software, digital engineering en platforms. De Group behaalde in 2020 een omzet van 16 miljard euro.

Get the Future You Want

www.capgemini.nl

www.trendsinveiligheid.nl

For more details contact:

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

INV 1A-027.21