WAT ZIEN DE BESTUURDERS UIT HET VEILIGHEIDSDOMEIN?

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

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

Innovatie in het veiligheidsdomein: ‘A person says no’

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

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

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

De burger centraal in een informatie gestuurde wereld

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

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

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

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

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

Digitale veiligheid staat prominent op de bestuurders agenda

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

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

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

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

De zoektocht naar talent

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

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

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

Conclusie

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

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

Over de auteurs

Marcel Kordes
Director public sector

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

Erik Staffeleu
Senior Director public sector

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

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