Capgemini

Trends in Veiligheid 2020

Samen Veilig

Innovatieve technologie houdt Nederland veilig

Inhoudsopgave

Managementsamenvatting

Auteurs
Marcel Kordes
Erik Staffeleu

Het veiligheidsdomein in tijden van pandemie

De wereld is in de ban van Covid-19. De initiële paniek heeft plaats gemaakt voor handelingsperspectief. Landen hebben verschillende en vergaande maatregelen genomen en de meeste zijn er in geslaagd de eerste fase van de pandemie de kop in te drukken. Inmiddels worden deze maatregelen snel stap voor stap verlicht. Echter, zolang de dreiging van Covid-19 nog bestaat, vraagt dit continu afwegingen maken tussen verschillende belangen. Ook de Nederlandse regering is op zoek naar 'het nieuwe normaal'. Zij neemt hierin met maximaal 50% van de kennis, 100% van de besluiten[1]. Meer en meer wordt in 'het nieuwe normaal' geleund op de digitale wereld. Onder andere voor (politieke) besluitvorming, voor sociaal contact, voor (thuis)werken en samenwerken. Om iedereen gebruik te kunnen laten maken van de digitale wereld heeft de Europese Commissie bij monde van Eurocommissaris Thierry Breton[2] onder andere Netflix verzocht om de datakwaliteit te verlagen. Wat tot ongeveer 25% minder dataconsumptie zal leiden.

Covid-19 zorgt ervoor dat alle organisaties wereldwijd zoeken naar oplossingen die in de Cloud worden aangeboden om daar waar mogelijk verder te werken. Tegelijkertijd neemt het aantal cyber-aanvallen enorm toe[3]. Met de toename in cybercriminaliteit op dit moment nemen de traditionele incidenten af, het lijkt alsof boeven ook in quarantaine zitten[4], niet alleen in Nederland maar ook in de rest van Europa. Het is dus niet vreemd om juist nu extra aandacht te besteden aan cybersecurity awareness én cybersecurity an sich. In dit rapport vindt u daarover een artikel met de centrale vraag of de publieke cloud veilig genoeg is voor het veiligheidsdomein.

In deze 10e editie van ons Trends in Veiligheid-rapport beschrijven we trends op technologisch vlak en verbinden we die vanuit onze kennis en ervaring aan wat er in het veiligheidsdomein speelt. We beschrijven hoe ontwikkelingen van Artificial Intelligence (AI) en Sensing in relatie tot Informatie Gestuurd Werken staan en hoe het veiligheidsdomein balanceert tussen privacy, (cyber)security en opsporing. Het doel van dit rapport is het bieden van een vernieuwende kijk op veiligheidsvraagstukken. Dit wordt gedaan door een brug te slaan tussen actualiteit en onze visie op hoe het toekomstig veiligheidsdomein vormgegeven zou kunnen worden.

10 jaar Trends in Veiligheid

Precies 10 jaar geleden publiceerde Capgemini het eerste Trends in Veiligheid-rapport. Geboren vanuit de intrinsieke motivatie om naast succesvolle opdrachten in het veiligheidsdomein ons 'thoughtleadership' te delen. Een aantal auteurs van het eerste uur publiceert ook in deze editie. Onderwerpen die toen actueel waren, zijn dat nog steeds. Al hebben we als samenleving en veiligheidsdomein stappen gezet in de realisatie van de toenmalige trends. Cybersecurity was destijds al actueel, maar met name voor grote organisaties zoals Defensie. Vandaag de dag is het een integraal onderdeel van onze samenleving. Het raakt ons in ons dagelijks leven. In 2010 schreven we veel over grensmanagement en de functie van Informatie Gestuurd Werken daarbinnen. Ook deze dagen een meer dan actueel thema met het grootschalig sluiten van de grenzen en nieuwe Europese richtlijnen zoals EES[5] en ETIAS[6] die in de voorliggende periode geïmplementeerd moeten worden.

Informatie Gestuurd Werken heeft zich doorontwikkeld, in verschillende snelheden binnen de verschillende organisaties. Inmiddels zijn het niet meer vooral de veiligheidsorganisaties die informatie gebruiken om effectief de interventies te sturen, ook inspecties en gemeentes hebben de mogelijkheden ontdekt. Ook de technologische ondersteuning heeft zich ondertussen doorontwikkeld. De toename van sensoren en de doorontwikkeling van geavanceerde analysetools biedt mogelijkheden die we 10 jaar geleden nog niet kenden. In deze editie gaan diverse artikelen over Informatie Gestuurd Werken en één specifiek over de zeven bouwstenen om Sensing binnen veiligheidsorganisaties succesvol te kunnen implementeren.

> **Onderzoek Trends in Veiligheid:** De Nederlanders zijn verdeeld over de mate waarin de overheid data mag gebruiken voor het bestrijden van criminaliteit.

In het afgelopen decennium heeft het veiligheidsdomein zich ontwikkeld tot een digitale en met de samenleving verbonden netwerkorganisatie. Verschillende events hebben op dit vlak voor een versnelling gezorgd in (technologische) innovatie en ontwikkeling. Zoals de Nuclear Security Summit uit 2014, waar het WiFi-netwerk conform de nieuwste inzichten en state-of-the-art software werd beveiligd[7]. Ook aanslagen in Europa hebben gezorgd voor een versnelling in de ontwikkeling. Zowel op het gebied van wetgeving, als op het gebied van technologische ontwikkelingen.

Op het gebied van wetgeving is er de afgelopen 10 jaar veel veranderd in het veiligheidsdomein, een greep uit deze veranderingen. Zo is in deze periode de Wet op de inlichtingen- en veiligheidsdiensten 2017 (WiV 2017) aangenomen. Daarnaast liep de vorming van de Nationale Politie op basis van de Politiewet 2012 samen met grootschalige ICT-vernieuwing. Zo concludeerde de Algemene Rekenkamer in 2016 dat de politie sinds 2011 vooruitgang boekt op het gebied van ICT[8]. Een andere grote wetswijziging die impact heeft op het veiligheidsdomein is de Algemene verordening gegevensbescherming (AVG). In dit rapport vindt u daarover een artikel waarin privacy gekoppeld wordt aan AI.

De algemene conclusiedie we kunnen trekken, is dat in de afgelopen 10 jaar het veiligheidsdomein nauwer verbonden is geraakt met technologische ontwikkelingen. Dit leidt tot de hamvraag; hoe bereiden we ons voor op de komende 10 jaar? In dit rapport wordt een beeld geschetst van de rol die technologie heeft op de hedendaagse samenleving. We streven hierbij niet naar een volledige beschrijving, maar willen inspireren vanuit verschillende invalshoeken. Met het beschrijven, ter discussie stellen en verbinden van (nieuwe) technologische ontwikkelingen met het veiligheidsdomein geven we vorm aan onze visie om 'samen veilig' te zijn en met innovatieve technologieën Nederland veilig te houden.

> **Onderzoek Trends in Veiligheid:** Het heersende gevoel in de maatschappij dat de overheid harder moet optreden om criminaliteit tegen te gaan én te voorkomen, is gelijk gebleven.

En toch voelen we ons onveiliger. Statistisch gezien is onze samenleving vandaag twintig keer veiliger dan in de middeleeuwen[9]. De trends die beschreven zijn de afgelopen 10 jaar hebben bijgedragen aan een objectief veiligere samenleving. Paradoxaal genoeg blijkt echter, uit het door Ipsos uitgevoerde onderzoek op verzoek van Capgemini, dat Nederlanders zich enigszins onveiliger voelen dan 10 jaar geleden. Iedere editie van Trends in Veiligheid in de afgelopen 10 jaar ging gepaard met een onderzoek naar de veiligheidsbeleving onder burgers. Voor het eerst hebben we een compleet artikel gewijd aan dit onderzoek: 'ons veiligheidsgevoel door de jaren heen'.

Samen met burgers én een innovatieve blik

Vooruitkijkend met een innovatieve blik, zijn er legio mogelijkheden om technologieën op een (andere) manier toe te passen zodat ze een bijdrage kunnen leveren aan onze veiligheid. Denk aan AI, dat een positiever imago verdient vanwege haar grote potentieel. Zo kan de inzet van AI in softwaresystemen onze privacy beter waarborgen of jeugdcriminaliteit in kaart brengen zodat je preventief kunt acteren.

> **Onderzoek Trends in Veiligheid:** Het vertrouwen in de overheid om veilig met jouw gegevens om te gaan blijft nog steeds een punt van kritiek.

Maar ook het succes van Bellingcat bewijst dat burgers via de beschikbaarheid van vele openbare bronnen en tools kunnen bijdragen aan opsporingsonderzoeken. Daarover eveneens een apart artikel in dit rapport. Vanuit het thema digitale veiligheid kun je denken aan een digitale brandoefening om medewerkers en de organisatie te informeren en weerbaar te maken tegen digitale aanvallen. Een andere innovatieve oplossing is het aanstellen van 'gemeentelijke Cybersheriffs' om de digitale weerbaarheid in de publieke sector te versterken.

Kijkend naar de toekomst zullen we een kritische blik moeten werpen op de manier waarop we ons organiseren. Een van de voorspellingen is de toenemende vergrijzing in Nederland de komende jaren, hier zullen capaciteitsuitdagingen uit voortvloeien. De rol van technologie zal een cruciale rol spelen bij het weerbaar houden van Nederland. Voorbeelden zijn de inzet van digitale triage, een informatie gestuurde aanpak om het veiligheidsdomein adaptief in te richten. Ook het versterken van de publiek-private samenwerking kan hieraan bijdragen. Een succesverhaal is bijvoorbeeld het Landelijk Meldpunt Internet Oplichting dan door publiek-private samenwerking online handelsfraude aanpakt.

Daarnaast kan de gehele keten volwassener worden door samenwerkingsverbanden ten aanzien van informatie-uitwisseling te stimuleren. Neem het voorspellen en duiden van criminele activiteiten; waar momenteel veiligheidsbeelden gefragmenteerd zijn door verschillende instanties kan door middel van (gedepersonaliseerde) informatie-uitwisseling een eenduidig veiligheidsbeeld gevormd worden. Tot slot uiteraard de grensoverschrijdende samenwerking op Europees niveau, die op basis van informatie-uitwisseling en cybersecurity een grotere digitale vuist zal maken tegen (statelijke) actoren die kwaadwillend zijn.

Samen innoveren, experimenteren en vernieuwen

Hoe zien de komende 10 jaar er uit en waar staat het veiligheidsdomein in 2030? De vernieuwing en verandering in het veiligheidsdomein kan worden bereikt door meer te investeren in AI-Intelligence, Informatie Gestuurd Werken en cybersecurity. De innovaties op deze drie onderwerpen moeten ongeveer gelijk oplopen; het een kan niet zonder het ander. Samen vormen ze de digitale hoeksteen van een goed opererend veiligheidsdomein.

Kijkend naar dit rapport kunnen we concluderen dat AI een groot potentieel biedt. Waarbij het een open deur is dat het maatschappelijke debat gevoerd moet worden langs de as van veiligheid, echter ook over ethiek en privacy. Want wat nu als geaccepteerd wordt beschouwd hoeft dat over enkele decennia niet te zijn. Hoe had de wereld er vandaag uit gezien als AI had voorkomen dat Rosa Parks in 1955 bleef zitten op de voor blanken gereserveerde zitplaats?[10]

Informatie Gestuurd Werken is gemeengoed geworden op het strategische en tactische niveau binnen het veiligheidsdomein. Op operationeel niveau wordt nog te weinig gebruik gemaakt van de kracht van informatie. Alle kennis, ervaring, informatie en technologie is aanwezig om de operatie op basis van informatie te laten opereren. Nieuwe technologieën zoals sensing en drones bieden nog meer mogelijkheden én genereren tegelijkertijd nog meer data.

De afgelopen maanden hebben aangetoond dat we als maatschappij niet zonder IT kunnen. We zijn nog meer gaan leunen op onze digitale wereld. Het belang van cybersecurity-awareness is persistent en hierop zal continu geïnvesteerd moeten worden. Door de verschuiving van traditionele naar digitale criminaliteit. Deze verschuiving zal ook in de basis van het veiligheidsdomein moeten verschuiven. Van specialist naar generalist. Een derde en laatste onderdeel is het offensief. Het domein moet kunnen handelen ook in de digitale wereld.

Genoeg ontwikkelingen voor het komende decennium. Maar waar staan we in 2030, en hoe kijken we terug op dit decennium? De tijd zal het ons leren. Er zijn voldoende aanknopingspunten om samen en met innovatieve technologie Nederland veilig te houden. Om op basis van slimme(re) technologie en best practices efficiënt op te schalen. En misschien concluderen we dat ons veiligheidsgevoel gestegen is, we een positief effect hebben bereikt op mens en milieu én we meer bereiken met minder. Wij hopen u met alle artikelen te inspireren en nieuwe kansen te creëren. Wij wensen u voor nu vooral veel leesplezier met dit rapport: 'Samen Veilig'.

Over de auteurs

marcel.kordes@capgemini.com

Marcel Kordes is verantwoordelijk voor de afdeling Business Technology Service - Public Security Capgemini

erik.staffeleu@capgemini.com

Erik Staffeleu is Senior Director Publieke Sector, Capgemini Invent

[1]Persconferentie minister president Rutte d.d. 13 maart 2020 https://www.rijksoverheid.nl/documenten/mediateksten/2020/03/13/letterlijke-tekst-persconferentie-na-ministerraad-13-maart-2020

[2]https://www.politico.eu/article/brussels-in-talks-with-netflix-about-reducing-internet-congestion/

[3]https://www.securitymanagement.nl/coronacrisis-leidt-tot-ongekend-hoog-aantal-cyberaanvallen/

[4]https://www.nrc.nl/nieuws/2020/03/23/de-boeven-lijken-ook-in-quarantaine-te-zitten-a3994657

[5]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R2226&from=EN

[6]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2018:236:FULL&from=EN

[7]https://www.thehaguesecuritydelta.com/images/HSD_rapport_LLNSS_NL.pdf

[8]https://www.rekenkamer.nl/publicaties/rapporten/2016/12/13/ict-politie-2016

[9]https://www.rd.nl/meer-rd/onderwijs/prof-beatrice-de-graaf-veiligheid-geen-doel-maar-middel-1.700865

[10]Je hebt wel iets te verbergen – Maurits Martijn + Dimitri Tokmetzis

Ons veiligheidsgevoel door de jaren heen

Hoe ervaart de Nederlander zijn veiligheid, 10 jaar geleden en nu?

Auteurs
Jolien van Aar
Zeger de Bruijne
Rianne Pattipeilohij

Tien jaar geleden voelde 33% van de Nederlanders zich wel eens onveilig. Nu is dat 45%. Wat is er veranderd in de samenleving?

Highlights

- De Nederlander is zich de afgelopen 10 jaar enigszins onveiliger gaan voelen.
- Online voelt men zich juist wel veilig.
- De Nederlander is zich steeds meer bewust van de eigen verantwoordelijkheid in online veiligheid, en neemt deze ook.
- Bijna de helft van de mensen is zelfs bereid om aan privacy in te leveren als het de bestrijding van criminaliteit ten goede komt.
- We maken ons zorgen over de invloed van sociale media op de informatie die we lezen, bijvoorbeeld ten aanzien van de verkiezingen.

Het Trends in Veiligheid onderzoek 2020

Ieder jaar, bij het uitbrengen van Trends in Veiligheid, wordt een onderzoek uitgezet waarin het veiligheidsgevoel van Nederlandse burgers centraal staat. We vragen naar ervaringen en meningen met betrekking tot gebeurtenissen die van invloed kunnen zijn op het veiligheidsgevoel. Verderop in dit rapport vindt u een overzicht van alle onderzoeksresultaten 2020, uitgevoerd door Ipsos met een steekproef van 1200 Nederlanders. In dit artikel blikken we tevens terug op de afgelopen tien jaar. De resultaten van 2020 zijn vergeleken met de resultaten van 2010 tot 2019 en gekoppeld aan maatschappelijke ontwikkelingen. Onderzoeksresultaten van voorgaande jaren zijn in de betreffende uitgaven te vinden.

Elke dag zien we in het nieuws hoe onze veiligheid in het geding komt. Van privacyschending door sociale media bedrijven tot buitenlandse inmenging in onze verkiezingen, tot terroristische aanvallen in de tram. Maar hoeveel invloed heeft dat op ons veiligheidsgevoel? De resultaten van ons jaarlijks onderzoek laten zien dat 45% van de Nederlanders zich wel eens onveilig voelt (zie het hoofdstuk met onderzoeksresultaten achterin dit rapport). Dit is een lichte toename ten opzichte van tien jaar geleden, toen was dit 33%. Hoewel meer mensen aangeven dat zij zich wel eens onveilig voelen, kan men niet goed duiden waardoor men zich precies onveilig voelt. Als we namelijk vragen naar het veiligheidsgevoel thuis, op straat en digitaal, dan geeft men aan zich in alle drie de omgevingen veilig te voelen: 94% voelt zich veilig thuis, 85% voelt zich veilig op straat, en 86% voelt zich veilig online. In deze omgevingen is dat een toename in veiligheidsgevoel ten opzichte van vorige jaren, wat overeenkomt met de cijfers van de veiligheidsmonitor van het CBS[1]. Verassend: de grootste toename is in de online omgeving. Hoe kunnen we de lichte toename van onveiligheid dan verklaren?

Digitaal bewustzijn

Het lijkt erop dat we ons steeds meer bewust zijn van de gevaren online en steeds beter weten wat we ertegen kunnen doen. We proberen online steeds meer onze eigen verantwoordelijkheid te nemen. Tien jaar geleden dacht men namelijk dat internetaanbieders primair verantwoordelijk waren voor het waarborgen van de online veiligheid (60% van de respondenten). Nu, in 2020 denkt men dat het primair de eigen verantwoordelijkheid is (62% van de respondenten). Mogelijk komt dit doordat er steeds meer aandacht wordt besteed aan hacks en datalekken, zoals de Celeb Hack[2], Cambridge Analytica[3] en wachtwoorden die beschikbaar zijn op het darkweb[4]. De meerderheid van de Nederlanders weet nu wat zij kunnen doen om hun eigen veiligheid te vergroten, zoals het vermijden van verdachte websites, regelmatig de software updaten, en, waar nu ook veel campagnes over worden gevoerd, regelmatig wachtwoorden vervangen. Daarnaast is men goed op de hoogte van de nieuwere manieren van beveiligen zoals een meer-factor-authenticatie: 19% maakt hier gebruik van.

Dit digitaal bewustzijn en verantwoordelijkheidsgevoel lijkt zijn vruchten af te werpen. Onder onze respondenten is een dalende trend in het slachtofferschap te zien. Dit staat haaks op het feit dat in de media wordt geroepen dat cybercrime juist toeneemt. Toch laten de cijfers het zien: 10 jaar geleden, in 2010, had 71% van de respondenten in dat jaar een vorm van cybercrime meegemaakt, zoals phishing en oplichting; dit jaar was dat 57% van de respondenten. Misschien komt dat doordat we phishing en nepmails steeds beter kunnen identificeren en er steeds meer melding van maken. Dat laatste wordt mogelijk ook beïnvloed door banken, die slachtoffers erop wijzen om aangifte te doen wanneer zij opgelicht zijn. Maar met de bewustwording van het herkennen van phishing en nepmails lijkt ook de bewustwording te komen van hoe geavanceerd de digitale vorm van oplichting is geworden. Eén op de drie Nederlanders geeft aan dat ze bang zijn over twee jaar geen echte mails van nepmails meer te kunnen onderscheiden. Dit kan mogelijk een aanwijzing zijn voor een groter onveilig gevoel in de toekomst. Mogelijk is het vergrote digitaal bewustzijn één van de factoren waardoor men zich toch wel eens onveilig voelt.

Bestrijden van criminaliteit

De meeste respondenten nemen contact op met de politie bij het waarnemen van een strafbaar feit of een onveilige situatie. Wat opvalt is dat significant meer 65-plussers dit doen, terwijl de groep 40-49 eerder zelf actie onderneemt. De manier waarop mensen contact opnemen is voornamelijk met de telefoon. De meerderheid van de mensen is tevreden over de manier waarop men informatie kan delen met de hulpdiensten.

Er zijn daarnaast ook manieren waarop de overheid criminaliteit kan bestrijden, maar waarbij een inbreuk op de privacy gemaakt wordt. Men is verdeeld over de mate waarin de overheid data mag gebruiken voor het bestrijden van criminaliteit. Welke vorm het meest geaccepteerd is door respondenten, is het bekijken van camerabeelden (60% zegt "ja, dat mag"). Op de tweede plaats staan afluisteren, gegevens van laptops en telefoons gebruiken en informatie van sociale media accounts bekijken (40% zegt "ja, dat mag"). Deze verdeeldheid bestond vijf jaar geleden ook al. Toen vond een deel van de mensen (42%) dat de overheid de privacy van burgers te snel aan de kant zette, en 63% van de burgers vond dat er niet zomaar gebruik gemaakt kan worden van data van burgers.

Bijna alle respondenten (96%) vinden het een goede zaak dat inlichtingendiensten voor het bestrijden van terrorisme en fraude, informatie over personen met elkaar uitwisselen. Dit vond men tien jaar geleden ook al. Zo blijkt dat op het gebied van biometrie de helft van de respondenten aangeeft dat vingerafdrukken van alle mensen opgeslagen mogen worden ter bestrijding van criminaliteit.

Wat gelijk is gebleven is het heersende gevoel in de maatschappij dat de overheid harder moet optreden om criminaliteit tegen te gaan en te voorkomen. De meerderheid (96%) vond tien jaar geleden dat de overheid meer maatregelen moet nemen, zoals harder straffen en meer voorlichting geven aan bedrijven. Een even groot deel van de respondenten is het hier nog steeds mee eens.

Vertrouwen in de waarborging van privacy

De minderheid van de burgers vertrouwt de overheid met betrekking tot het veilig omgaan met je gegevens. Deze minderheid van ongeveer 40% is stabiel over de jaren. Bij de vraag in welke instanties men het meeste vertrouwen heeft, in de omgang met persoonsgegevens, scoren ziekenhuizen en politie het best. Het is een aanzienlijk beter vertrouwen dan het vertrouwen in tech-bedrijven zoals Google, wat al tien jaar niet boven de 10% uit komt. Dat geldt zeker wat betreft de 'internet of things'-apparaten zoals Google Home en Alexa. Daarnaast is er een stabiele groep van ongeveer 5% die alle jaren zegt niet in privacy te geloven, of dat ze niets kunnen doen om hun privacy te beschermen.

Nationaal veiligheidsgevoel

Mogelijk is het veranderende nationale veiligheidsgevoel een verklaring voor het verhoogde percentage dat zich wel eens onveilig voelt. Dit jaar zegt vier op de tien Nederlanders zich weleens zorgen te maken over een digitale aanval van een ander land op Nederland. Dat is méér dan het aantal Nederlanders dat zich zorgen maakt over een fysieke aanval, namelijk minder dan 1 op de tien Nederlanders. Dit was vijf jaar geleden nog wel anders. Toen dacht men nog weinig aan digitale aanvallen. Sinds die tijd zijn er een aantal gebeurtenissen geweest die veel media-aandacht hebben gekregen, zoals de berichten over WikiLeaks de spionage-praktijken van Rusland, China en de Verenigde Staten[5], en de opkomst van DDoS-aanvallen Maar misschien belangrijker nog, sinds 2016 is de meldplicht datalekken ingegaan en sindsdien wordt er ook pas inzicht gegenereerd in digitale aanvallen.

Met die verschuiving is men door de tijd heen ook gaan denken dat er meer gedaan moet worden aan de waarborging van de digitale veiligheid. Waar men zo'n tien jaar geleden nog dacht dat er vooral geïnvesteerd moest worden in kennis, leeft nu het idee dat de politie en de overheid vooral technische en financiële middelen nodig hebben om de nationale digitale veiligheid te waarborgen. In 2013 vond namelijk 94% van de mensen dat er in kennis geïnvesteerd moest worden en 20% in technische dan wel financiële middelen. Nu is dat bijna omgedraaid, nog maar 53% van de mensen vindt dat er geïnvesteerd moet worden in kennis en 79% vindt dat er geïnvesteerd moet worden in technische/financiële middelen.

Mogelijk heeft de Nederlander een beperkt beeld van wat de overheid allemaal doet om de digitale veiligheid te waarborgen. De meerderheid zegt namelijk dat de overheid meer kenbaar mag én moet maken van wat zij bereiken in termen van opsporen, oplossen, en voorkomen. De onwetendheid over wat er aan nationale beïnvloeding is, is een punt dat mogelijk een gevoel van onveiligheid geeft.

Nepnieuws & verkiezingen

De afgelopen tijd gaat het steeds vaker over nepnieuws. Een belangrijk onderwerp voor de Tweede Kamerverkiezingen 2021. Acht op de tien Nederlanders vinden dat nepnieuws een gevaar is voor de maatschappij. Opvallend, want het grootste deel van de bevolking denkt nepnieuws zelf wel te kunnen herkennen. Het lijkt er daarom op dat men vooral bang is dat anderen in nepnieuws trappen. Dat is ook te zien in de cijfers omtrent beïnvloeding van verkiezingen. Méér mensen denken dat zoiets alleen in Amerika gebeurt, en niet in Nederland.

Nepnieuws heeft weinig invloed gehad op het vertrouwen van Nederland in traditionele media. Bijna de helft van de Nederlanders gebruikt dan ook de nieuwssites als informatiebron voor de aankomende verkiezingen. Het heeft wel invloed gehad op het vertrouwen in nieuws via sociale media. De meerderheid van de Nederlanders -voornamelijk jongeren - heeft het idee dat het informatiebeeld via sociale media sterk wordt vernauwd en beïnvloed. Toch zegt nog 13% zijn informatie de aankomende verkiezingen van sociale media te halen.

Conclusie

Hoe komt het dus dat wij, Nederlanders, ons onveiliger zijn gaan voelen in de afgelopen 10 jaar? De Nederlander beweegt mee in het digitale tijdperk. We kunnen niet meer zonder de digitale ontwikkelingen, maar we realiseren ons ook dat iedere ontwikkeling nieuwe veiligheidsvraagstukken met zich meebrengt. We worden bewust van onze eigen verantwoordelijkheid en de potentiële risico's. Dit besef heeft mogelijk een negatieve impact op ons algemene veiligheidsgevoel. Tegelijkertijd weten we ook steeds beter wat we kunnen doen om ons te beschermen tegen digitale gevaren en we nemen die verantwoordelijkheid ook. Samenvattend, we zijn in 10 jaar al ver gekomen; van de eerste smartphone met 3G naar de smartwatches met 5G, en van internetbankieren naar betalen met je telefoon.

[1]Bron: CBS Statline (2020): https://opendata.cbs.nl/statline/#/CBS/nl/dataset/81877NED/table?ts=1582900044533

[2]https://www.ad.nl/show/jennifer-lawrence-boos-om-gelekte-naaktfoto-s-celebrities~ad8c64f7/

[3]https://www.volkskrant.nl/es-b7eb750f

[4]https://www.computable.nl/artikel/nieuws/security/6541231/250449/de-5-spraakmakendste-datalekken-van-2018.html

[5]https://nos.nl/nieuwsuur/artikel/2322865-spionageschandaal-is-wake-upcall-voor-de-nederlandse-politiek.html

Over de auteurs

rianne.pattipeilohij@capgemini.com

Rianne Pattipeilohij is werkzaam bij Capgemini Business Technology Services, Openbare Orde en Veiligheid. Rianne is gespecialiseerd in het vertalen van de businessvragen naar technische oplossing voor data gedreven inzichten.

Jolien van Aar werkte ten tijde van het schrijven van het artikel als onderzoeker/consultant bij Capgemini Invent en richtte zich daarbij op effectmetingen en evaluaties in de publieke sector.

zeger.bruijne@capgemini.com

Zeger de Bruijne is werkzaam bij Capgemini Business Technology Services, Openbare Orde en Veiligheid. Zeger is gespecialiseerd in het analyseren van processen en ontwikkelingen binnen de criminaliteitsbestrijding.

Sensing voor veiligheid – bouwstenen voor succesvol Informatie Gestuurd Optreden

Hoe kan een veiligheidsorganisatie sensing tot een succes te maken in de dagelijkse praktijk?

Auteurs
Luuk Tubbing
Arjan van den Berk
Martijn van de Ridder

Highlights

- Sensing biedt een zesde zintuig voor de veiligheidssector.
- De technologische ontwikkelingen zijn niet tegen te houden.
- Kant-en-klare sensing-oplossingen zijn echter nauwelijks beschikbaar.
- We onderkennen zeven bouwstenen die handvatten bieden voor succesvolle toepassingen in de praktijk.
- Met aandacht voor juridische en ethische kaders draagt sensing bij aan een veiligere toekomst.

De maatschappij verwacht dat innovatieve technologie, onder voorwaarden, wordt ingezet ten gunste van onze veiligheid[1]. Door verbonden sensoren zijn we in staat om steeds meer en op afstand veiligheidssituaties op digitale wijze waar te nemen. Menselijke capaciteit in de veiligheidssector, die steeds schaarser is, kan hiermee aangevuld worden en slimmer ingezet voor interventies[2]. Sensing-technologie als zesde zintuig biedt de veiligheidssector zodoende een kans. Het is echter een enorme uitdaging om sensing succesvol in de praktijk in te zetten.

Wat is sensing?

Onder sensing verstaan we slim digitaal waarnemen met behulp van sensoren, waarbij een waarneming wordt vertaald naar een melding of aanbeveling. Nu bestaan sensoren zoals camera's, weegschalen en thermometers al langer. Met het zogenaamde 'internet of things' zijn deze sensoren met elkaar verbonden via het internet en kan op basis van de sensorwaarnemingen ook (automatisch) een actie in gang worden gezet[3]. Sensing is dan ook een passend middel voor beter Informatie Gestuurd Optreden (IGO)[4].

Met sensing is het mogelijk om continu waar te nemen op locaties waar niet altijd menselijke ogen en oren aanwezig kunnen zijn. Er is alleen een inspecteur of agent ter plaatse nodig als er ook echt wat aan de hand is. Denk aan de inspecteurs van de NVWA die beter en slimmer toezicht op dierenwelzijn en hygiëne kunnen doen. Ook kunnen vitale infrastructuren beter gemonitord worden. In de Verenigde Staten wordt deze technologie ingezet voor een Smart Border aan de kant van Mexico[5]. Dichter bij huis wordt een slimme bagagescanner ingezet die de screeners van de NCTV op Schiphol middels slimme algoritmes ondersteunt bij het bepalen welke bagage wel of niet gevaarlijk is[6]. Of de Designer Outlet Roermond, waar de politie sensing inzet om rondtrekkende zakkenrollers en winkeldieven te vangen en deze criminaliteit uiteindelijk te voorkomen met behulp van data van cameratoezicht, ANPR-camera's en andere zinvolle sensoren[7].

Sensing - een uitdaging in de praktijk

De afgelopen jaren is er met sterk wisselend resultaat in het veiligheidsdomein flink geëxperimenteerd met sensing-oplossingen. Samen met onze klanten in het veiligheidsdomein hebben we bij Capgemini veel geleerd op dit gebied. We hebben ook meerdere artikelen geschreven over het 'waarom' en het 'wat' van sensing[8]. Nu is het tijd om de praktische succesfactoren voor de veiligheidssector te delen. We gaan niet meer in op het 'waarom', maar op het 'hoe'.

Hoe maak je een dergelijke toepassing tot een succes? Het sensing-vakgebied moet nog volwassen worden. Er liggen nauwelijks kant-en-klare oplossingen op de plank. In veel organisaties zijn veel elementen aanwezig om sensing mogelijk te maken, zoals sensoren, de benodigde IT-omgeving en ontwikkelteams. Om echt succesvol te zijn is het echter noodzakelijk een aantal bouwstenen op de juiste wijze in te vullen en bij elkaar te brengen. Op basis van onze ervaringen met sensing beschrijven we zeven bouwstenen voor succesvol IGO.

Bouwsteen 1:
Toetsen in de praktijk

Er zijn nog geen kant-en-klare sensing-oplossingen dus het is van belang om deze te toetsen in de praktijk, waarbij een businessvraag het startpunt is. Gebruik een helder afgebakend bedrijfsproces om het doel te ervaren en te leren van het gebruik. Daarbij is het van belang om vast te stellen wanneer de toets een succes is en dit meetbaar te maken.

Om de organisatie optimaal te laten profiteren is organisatiebrede uitrol een must als de gevalideerde sensing-oplossing levensvatbaar is. Houd bij het ontwerp van oplossingen dan ook rekening met de mogelijkheden en vereisten voor organisatiebrede uitrol.

Cruciaal voor het succes van de toets in de praktijk is de inrichting van een (programma)organisatie die in alle benodigde middelen voorziet en tevens zorgt voor afbakening en focus. Succes zorgt ervoor dat een zuigende werking ontstaat en nieuwe use cases op basis van sensing zich aandienen.

Bouwsteen 2:
Business agility

Agile werken is een must in de jonge, snel veranderende en onvoorspelbare wereld van sensing. Technologische veranderingen gaan erg snel, in alle onderdelen van de keten, van sensor tot en met visualisatie. Criminelen en andere te handhaven groepen veranderen bovendien snel hun gedrag. Oplossingen zijn vaak nieuw voor de organisatie en de gebruikers van de sensing-toepassing. Zij moeten eerst een werkende oplossing ervaren om hun wensen helder(der) te kunnen articuleren. Een technisch sensing-platform bestaat uit veel componenten, van sensor tot en met visualisatie. Bovendien zijn sensoren vaak ontwikkeld voor een ander doeleinde dan het betreffende veiligheidsvraagstuk. Zo kan de positiebepaling van een WiFi-scanner ontwikkeld voor marketingdoeleinden onvoldoende nauwkeurig zijn voor opsporingsdoeleinden. Er zijn dus veel iteraties nodig om te leren en tot een passend product en werkwijze te komen.

Leer zodoende om te gaan met het gebruik van sensordata, initieer verbeterloops en acteer op basis van de geleerde lessen. Het toepassen van sensing zal naar alle waarschijnlijkheid niet direct het gewenste resultaat opleveren. Bereid de business hierop voor door verwachtingen te managen. Een 'zesde zintuig' levert wellicht eerst meer werk op en later minder. Dat extra werk wordt veroorzaakt door het leren werken met een nieuwe toepassing en doordat er meer meldingen binnen komen, waarvan een deel vals-positief zal zijn.

Bouwsteen 3:
Cultuur van Informatie Gestuurd Optreden

Voor het succes van sensing is het essentieel dat de (gebruikers)organisatie durft te vertrouwen op informatie die automatisch wordt gegenereerd door IT-systemen. Door gebruik van slimme algoritmes is het 'black box' gehalte toegenomen. De eindgebruiker weet vaak niet meer hoe gepresenteerde informatie tot stand is gekomen. Doordat de keten van informatieverwerking steeds complexer wordt, is het niet altijd duidelijk wie aanspreekbaar is op de kwaliteit van de resulterende informatie en hierop gebaseerde besluiten. Hierdoor kan het vertrouwen in sensing een heikel punt zijn.

Zeker in het veiligheidsdomein is het toetsen van de juistheid van informatie van een sensing-oplossing van essentieel belang. Neem een systeem dat hits genereert op basis van een daderprofiel. De eerste uitdaging is om tot een valide en gedragen profiel te komen. Zorg ervoor dat de totstandkoming van het daderprofiel transparant is.

De tweede uitdaging is om een feedbackloop te creëren, waarbij registratie van operationele resultaten en het analyseren ervan prioriteit hebben. Registratie heeft echter zelden de hoogste prioriteit, zeker bij actie gedreven teams zoals 'first responders'. Maak registratie eenvoudiger en leuker door een doordacht 'user experience' ontwerp. Daarnaast kunnen doelgerichte rapportages en moderne tools het analysewerk eenvoudiger maken.

Tenslotte kan de dadergroep, ook geholpen door de laatste technologie, snel van gedrag veranderen zodra zij door hebben op basis van welke kenmerken of sensoren zij opgespoord worden. Mobiliseer een groep domeinexperts die kort-cyclisch het daderprofiel bijstellen op basis van nieuwe inzichten.

Bouwsteen 4:
Samenwerking in een ecosysteem

Het ontwikkelen en beheren van een sensing-oplossing in het bedrijfsproces van een veiligheidsorganisatie zoals de politie, betekent samenwerken in een complex ecosysteem. Hierbij kun je denken aan de inzet van verschillende typen sensoren van verschillende (publieke of private) eigenaren en leveranciers, analisten die daderprofielen bedenken, agenten die hits op straat opvolgen en op basis van deze profielen mogelijk aangestuurd zijn vanuit een meldkamer of commandopost. Partners kunnen zowel intern of extern, publiek of privaat zijn. Denk in het voorbeeld van de bagagescanner aan de NCTV, douane, maar dus ook aan Schiphol. Of in het voorbeeld van de outlet in Roermond aan de politie, het OM, rijkswaterstaat en winkeliers of beveiligingsbedrijven. Intern zijn er domeinexperts, juristen, eindgebruikers en managers die een rol hebben bij het vaststellen van nieuwe use cases en nieuwe wensen en eisen.

Ecosysteem-denken is dan ook essentieel voor het succes van sensing-oplossingen. Breng in kaart wie de actoren zijn in dit ecosysteem en welke rol zij hebben. Spreek binnen het team af wie welke contacten onderhoudt. Bouw een vertrouwensrelatie op met partners door hen mee te nemen in het gedachtengoed van jouw systeem en werkwijze. Check of zij en jijzelf geen verkeerde aannames maken. In de wereld van sensoren is dit van wezenlijk belang, omdat standaard oplossingen nog nauwelijks bestaan.

Bouwsteen 5:
Microservice architectuur met open source software

Bij een snel veranderende en onvoorspelbare omgeving past een microservice-architectuur bij de sensing-oplossing. Het belangrijkste idee hierachter is dat applicaties eenvoudiger te bouwen en te onderhouden zijn wanneer ze worden opgesplitst in kleinere stukken die naadloos samenwerken. Deze modules communiceren met elkaar via eenvoudige, universeel toegankelijke applicatie-programmeerinterfaces (API's)[9]. Dit geeft ruimte voor verschillende typen en snel veranderende toepassingen en het opschalen hiervan. Elk type sensor heeft een eigen dataverwerkingsservice. In een microservice-architectuur is data afkomstig van verschillende sensortypen relatief eenvoudig te beheren.

Door hierbij open source software te gebruiken is een organisatie in staat om snel maatwerk te leveren en te profiteren van de nieuwste technologie[10]. Ook is het gemakkelijker om (data van) verschillende soorten sensoren te koppelen. Doordat de code openbaar is, worden kwetsbaarheden snel opgespoord en opgelost door een actieve community van softwareontwikkelaars. Bovendien is het eenvoudiger en goedkoper om van softwarepakket te veranderen (voorkomen van vendor lock-in)[11]. Voorwaarde is dat het ontwikkelteam kennis heeft van dit architectuurdenken, met verandering om kan gaan en bereid is te blijven leren.

Bouwsteen 6:
Voldoen aan wettelijke en ethische eisen

Sensing-toepassingen hebben een grote impact op de openbare ruimte waarin wij allemaal acteren. Tegelijkertijd kan sensing-technologie veel meer dan de wet- en regelgeving toelaat[12]. Met de locatievoorzieningen op onze slimme telefoons is ons leven al een open boek voor allerlei organisaties[13]. Of we hier nu bewust mee instemmen of niet. Het is dan ook van belang om wettelijke, maatschappelijke en ethische kaders te blijven toetsen. Dezelfde technologie wordt namelijk ook ingezet voor totalitaire sturing of het realiseren van een surveillancestaat zoals China[14]. De vraag is dan ook op welke wijze en in hoeverre we sensing in de westerse wereld willen inzetten. Voor meer informatie, lees het artikel over het behouden van de menselijke maat bij het inzetten van technologieën zoals Sensing[15].

De ervaren complexiteit van wettelijke, maatschappelijke en ethische eisen hoeven echter geen onoverkoombare barrière te zijn. Betrek relevante stakeholders zoals burgers of privacy-groeperingen actief door inspraakmomenten en heldere communicatie via de media. Dit bevordert de maatschappelijke acceptatie.

Bouwsteen 7:
IT-competenties voor sensing

Uiteraard zijn voor sensing als basis de gangbare competenties van een data gedreven ontwikkel- en beheerorganisatie nodig. Onderscheidend van andere IT-initiatieven is ten eerste de competentie data-science om in de sensordata patronen in crimineel gedrag te ontdekken. Data-engineering is van belang om de grote hoeveelheid en variatie aan data in goede banen te leiden, zowel voor real-time opvolging als voor analyse achteraf. Ook de combinatie van verscheidene architectuurdisciplines is onmisbaar; van business, systeem, applicatie, informatie, data, technologie, infrastructuur tot security. Onder meer omdat een sensor, en zeker een integrale sensing-oplossing, (nog) niet kant-en-klaar geleverd wordt. Zorg ervoor dat deze expertises in het team zitten en dat nieuwe sensoren met een proefopstelling worden getest om te bepalen of deze in de praktijk kunnen worden ingezet.

Conclusie

Sensing-technologie biedt de samenleving en specifiek de veiligheidssector een zesde zintuig. Deze ontwikkeling is niet tegen te houden. Sterker nog, sensing zal door de introductie van 5G en andere technologische ontwikkelingen een vlucht nemen. De technologie kan echter veel meer dan de wet en onze moraal toestaan. Talloze organisaties zoeken in experimenten de grens op. We kunnen het dus maar beter omarmen en in goede banen leiden. Met de zeven bouwstenen die we hierboven beschrijven, bieden we op basis van onze ervaring handvatten om innovatieve sensing-oplossingen tot een succes te maken in de dagelijkse praktijk. Dit met behoud van wettelijke en ethische kaders. De toekomst zal veiliger en beter zijn.

[1]https://www.rathenau.nl/nl/digitale-samenleving/burgers-en-sensoren

[2]https://www.rtlnieuws.nl/nieuws/nederland/artikel/4808701/personeelstekort-politie-vakantie-gelderland-amsterdam-rotterdam

[3]Definitie: https://internetofthingsagenda.techtarget.com/definition/smart-sensor

[4]Zie ook: https://www.trendsinveiligheid.nl/rapport/2019-slimmer-samenwerken-aan-een-veiliger-nederland/effectief-informatiegestuurd-werken-igw-in-een-wereld-met-5g-sensing/

[5]https://www.vox.com/recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai

[6]https://www.nrc.nl/nieuws/2020/01/02/hoe-controleert-schiphol-je-bagage-a3985503

[7]https://nos.nl/artikel/2250767-politie-wil-zakkenrollers-en-plofkrakers-vangen-met-data.html

[8]https://www.trendsinveiligheid.nl/rapport/rapport-2017/sensing-in-de-verbonden-samenleving/

[9]https://blog.newrelic.com/technology/microservices-what-they-are-why-to-use-them/

[10]https://opensource.com/life/15/12/why-open-source

[11]https://www.pcworld.com/article/209891/10_reasons_open_source_is_good_for_business.html

[12]https://www.nrc.nl/nieuws/2019/11/29/gezichtsherkenning-is-snel-aan-het-ontsporen-a3982169

[13]https://www.theverge.com/2019/12/19/21029992/smartphone-location-tracking-legal-technology-privacy-new-york-times

[14]https://www.theguardian.com/books/2019/jun/30/we-have-been-harmonised-life-china-surveillance-state-kai-strittmatter-review

[15]https://www.trendsinveiligheid.nl/rapport/2018-vertrouwen-en-wantrouwen-in-de-digitale-samenleving/2030-een-truman-show-of-maatschappij-met-menselijke-autonomie/

Over de auteurs

luuk.tubbing@capgemini.com

Luuk Tubbing MSc is senior consultant bij Capgemini Insights & Data. Hij is actief op het gebied van Intelligence en de data-gedreven organisatie, met name in het domein openbare orde en veiligheid.

arjan.vanden.berk@capgemini.com

Arjan van den Berk is principal consultant bij Capgemini Insights & Data. Hij is Agile Coach & Scrum master en heeft een brede ervaring op het gebied van IT-processen en organisatieverandering.

martijn.vande.ridder@capgemini.com

Martijn van de Ridder MSc is principal consultant bij Capgemini Insights & Data en verantwoordelijk voor de publieke sector. Hij is actief op het gebied van intelligence en Informatie Gestuurd Werken.

Het belang van een Europese digitale vuist door civiel-militaire samenwerking

Highlights

- Geopolitieke spanningen uiten zich steeds vaker in het digitale domein.
- Ook Europese landen en bedrijven (inclusief Nederlandse) zijn hierbij steeds vaker doelwit.
- Vanuit de Europese Commissie ligt de focus van cybersecurity-samenwerking op preparatie, responsieve maatregelen en wetgeving gericht op het civiele domein.
- Europa moet daarnaast meer samenwerking faciliteren tussen het civiele, militaire en inlichtingendomein zodat alle cybercapaciteiten optimaal benut worden.
- Het Nederlandse veiligheidsdomein kan dit aanjagen en een voortrekker zijn.

Auteurs
Roeland de Koning
Fokko Dijksterhuis

Waar landen elkaar vroeger nog met artillerie bestookten, gaan naties vandaag de dag de strijd steeds vaker aan met digitale instrumenten. De (pantser)houwitser heeft plaats moeten maken voor wapens zoals 'zero day exploits'; aanvallen waarbij misbruik wordt gemaakt van software-kwetsbaarheid waar anderen niet van op de hoogte zijn. Als we het hebben over de gevaren in het digitale domein dan denken we al snel aan cybercriminaliteit, maar het wordt steeds duidelijker dat de grootste dreiging schuilt in digitale ontwrichting door statelijke actoren. We zien dat landen niet terugschrikken van cyberspionage, aanvallen op (kritieke) infrastructuur of digitale desinformatie/beïnvloedingscampagnes. Nederland kan deze dreiging slechts tot op zekere hoogte zelfstandig het hoofd bieden, maar gezamenlijk met onze Europese buurlanden zijn we van betekenis in de internationale arena. De hamvraag is daarom: wat doen wij als Europa om onszelf te beschermen? Zouden we meer moeten doen? En wat zou de rol van Nederland dan kunnen of zelfs moeten zijn?

Geopolitieke spanningen uiten zich steeds vaker in het digitale domein

Met een gerichte luchtaanval op de internationale luchthaven van Baghdad werd op 3 januari 2020 de Iraanse generaal Qasem Soleimani om het leven gebracht door het Amerikaanse leger. In de dagen na dit incident werd er een drievoudige toename gezien van wereldwijde cyberaanvallen die konden worden getraceerd tot Iraanse IP-adressen, inclusief pogingen om federale, nationale en lokale websites in de Verenigde Staten te hacken[1]. Op 4 januari bleek een website van de Amerikaanse regering inderdaad ook daadwerkelijk gehackt te zijn en zagen bezoekers aan de website een afbeelding van een bebloede president Donald Trump met een begeleidende pro-Iraanse boodschap[2].

Iran wordt niet per se gezien als een grootmacht in cyberspace zoals Rusland of China. Toch heeft ook dit land volgens experts flink geïnvesteerd in cybercapaciteiten en blijken ze niet te twijfelen om deze middelen in te zetten. Dat dit geen recente ontwikkeling is, bleek eerder toen officieel bekend werd gemaakt dat Iran al in 2013 het controlesysteem van een dam in de Amerikaanse staat New York had gehackt[3]. Naar aanleiding van de toenemende spanningen tussen Amerika en Iran kwam het Amerikaanse Homeland Security kort na de aanslag op Soleimani met een waarschuwing voor bedrijven in Amerika, maar ook haar bondgenoten in het buitenland, om voorbereid te zijn op een toename in cyberaanvallen[4]. Deze gebeurtennissen onderschrijven het feit dat geopolitieke spanningen en zelfs oorlogsvoeringen zich steeds meer in het digitale domein uiten en afspelen. De bereidheid van landen zoals China, Rusland, Noord-Korea, Iran, Israël en ook de Verenigde Staten om geopolitieke disputen in het digitale domein uit te vechten is onbetwist.

Europese landen en bedrijven (inclusief Nederlandse) zijn steeds vaker doelwit

Het bovenstaande voorbeeld is geen nieuw fenomeen. Enkele andere noemenswaardige voorbeelden van digitale ontwrichting door natiestaten zijn: de cyberaanval op het elektriciteitsnet van Ukraine in december 2015[5], de wereldwijde reeks aan Wannacry-aanvallen in 2017 waar een verband werd gelegd met Noord Korea[6] en dichter bij huis de Iraanse hack van Diginotar in 2011 en de verijdelde Russische hackaanval op de OPCW in Den Haag in 2018[7]. Meerdere malen is dus gebleken dat ook Europese landen, bedrijven en organisaties steeds vaker doelwit zijn. Recentelijk werd nog bekend gemaakt dat Iraanse overheidshackers achter aanvallen op Nederlandse onderwijsinstellingen zaten[8].

In principe is elke organisatie, maar ook elk land in de eerste plaats zelf verantwoordelijk voor haar digitale verdediging. Binnen Europa betekent dit dan ook dat alle landen zelf een nationale strategie en capaciteiten hebben opgebouwd in het civiele en militaire domein om cyberrisico's het hoofd te bieden. We zien daarin een groot onderling verschil in volwassenheid, zowel wat strategie, wetgeving als capaciteiten betreft. Tegelijkertijd houden cyberdreigingen geen rekening met landsgrenzen. Aanvallen zijn vaak grensoverschrijdend, zelfs als dit soms onbedoeld is. Dit bleek bijvoorbeeld in 2017 toen de Rotterdamse haven grote last ondervond van een grootschalige hack bij het Deense container terminal bedrijf A.P.Møller-Maersk. De honderden miljoenen schade bleken het onbedoelde neveneffect te zijn van een op Oekraïne gerichte cyberaanval. Er werd misbruik gemaakt van een programma waar Maersk toevalligerwijs ook gebruik van maakte. In Europa kunnen landen dan wel hun eigen cybercapaciteiten hebben georganiseerd, cyberaanvallen vragen juist op het Europese continent om intensievere internationale coördinatie. Geen enkel Europees land beschikt bovendien over voldoende cybercapaciteit om op eigen houtje tegenwicht

te kunnen bieden aan grote wereldmachten als China, Amerika of Rusland. Dit buitenlandse 'cyberleger', inclusief 'state sponsored' hackersgroepen en volledige cyberlegers vragen om een intensivering van de Europese cybercapaciteiten. Dit doet de vraag rijzen wat Europese landen (gezamenlijk) doen om zich te wapenen in dit nieuwe tijdperk.

Europa focust zich voornamelijk op preparatie, responsieve maatregelen en wetgeving

Europa staat zeker niet stil, integendeel: lidstaten van de EU zijn hun samenwerking wat cybercapaciteiten betreft de afgelopen jaren aan het intensiveren. Op Europees niveau is er al vele jaren extra aandacht voor digitale veiligheid en het tegengaan van cybercriminaliteit. Europa wil zorgen dat er een veilige interne markt is. Dit geldt zowel op fysiek als op digitaal vlak. In januari 2013 werd het Europees Centrum voor Cybercriminaliteit (EC3) opgericht, gevolgd door de oprichting in 2014 van het EU-agentschap ENISA. In 2019 kreeg dit agentschap vanwege de steeds groter wordende dreiging van 'cyberwarfare' en het belang van internetveiligheid, een permanent mandaat. In haar welbekende rol als wetgever drukt de EU haar stempel zowel binnen als buiten Europa. De AVG (Algemene Verordening Gegevensbescherming) of GDPR (General Data Protection Regulation) is in 2019 in werking getreden om als Europese actor eisen te stellen aan (onder andere) het bewaken van persoonsgegevens. Ook door de zogenaamde NIS-directive (Directive for Network and Information Systems, doorvertaald naar de Wet Beveiliging Netwerk- en Informatiesystemen in Nederland) werden cybersecurity-voorschriften aan Europese bedrijven opgelegd en samenwerking tussen lidstaten bevorderd. In mei 2019 werd de belangrijke stap gezet met een Europees raamwerk dat de EU in staat stelt (financiële) sancties aan personen of entiteiten op te leggen als reactie op cyberaanvallen. Wat cybersecurity-regulatie en-wetgeving betreft, is Europa dus zeker actief. Daarnaast presenteerde de Europese Commissie in september 2018 een voorstel om een Europees kenniscentrum op te richten voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging. Het doel van dit voorstel is om innovatie op het gebied van cyberbeveiliging te stimuleren door de krachten te bundelen. In november 2018 werd het EU Cyber Defense Policy Framework aangepast om dit ook vanuit de EU actief aan te jagen.

In de uitvoering van de NIS-directive is Capgemini al jaren betrokken bij projecten om bijvoorbeeld samenwerking tussen de Computer Emergency Response Teams (CERTs) van lidstaten te faciliteren en te stimuleren[9]. Ook dit jaar leidt Capgemini een consortium in een project om Europese Information Sharing and Analysis Centers (ISACs) op te bouwen[10]. In deze gremia wordt over landsgrenzen heen informatie uitgewisseld binnen een aantal vitale infrastructuren (Operators of Essential Services), zoals financiën, energie of de luchtvaart. Door deze informatie-uitwisseling kunnen incidenten en waarschuwingen snel worden gedeeld over landsgrenzen, zodat ook elders preventieve of responsieve maatregelen kunnen worden getroffen. Een sleutelfactor van dergelijke samenwerkingsverbanden is het feit dat het om publiek-private samenwerking gaat, waarbij de (Europese) overheid onder andere faciliterend optreedt en informatie deelt. De verdere uitvoering en invulling van de initiatieven is volledig in handen van private partijen. Uiteindelijk zijn het vaak de private partijen die het doelwit zijn van cyberaanvallen. Maar wat als deze aanvallen niet afkomstig zijn van 'kleine' cybercriminelen maar van de eerdergenoemde 'state sponsored' hackersgroepen of cyberlegers? Er is dan sprake van een grote mate van asymmetrie en het ligt niet in lijn der verwachting dat civiele organisaties in staat zijn om dergelijke aanvallen het hoofd te bieden. De EU is op meerdere vlakken actief, maar we zullen meer moeten doen.

De sleutel is meer samenwerking tussen het civiele, militaire en inlichtingendomein

Wat kan Europa dan nog meer doen? In 2013 riep Brazilië landen op om een eigen 'intranet' te starten, voornamelijk uit frustratie door internationale cyberspionage van onder meer de Amerikaanse veiligheidsdiensten. In meerdere landen wordt het internet daadwerkelijk actief afgeschermd en gereguleerd, bijvoorbeeld door bepaalde delen van het wereldwijde web te blokkeren. In het geval van China wordt er bijvoorbeeld schertsend gesproken over 'the Great Firewall of China'. Als alle landen hiertoe overgaan, zullen geopolitieke spanningen en verhoudingen zich dus ook letterlijk in internetgrenzen uiten, zodat er een 'splinternet' ontstaat. Enerzijds biedt een dergelijke nationaal 'intranet' afscherming van buitenlandse kwaadaardige bedoelingen. Anderzijds stelt het regeringen ook in staat om veel meer invloed uit te oefenen op hun burgers door de controle op informatiestromen. Naar verwachting zal de EU niet snel overgaan tot dergelijke verdedigingsmaatregelen, gezien het feit dat dit uitnodigt tot internetcensuur wat op gespannen voet staat met de waarde die wij hechten aan burgerlijke vrijheden en rechten. In 2011 werd in de zogenaamde 'Council of the European Union's Law Enforcement Working Party' een voorstel van dergelijke vormen dan ook al snel terzijde gelegd[11].

De EU kan er ook voor kiezen om haar cybercapaciteiten uit te breiden, waarmee zich meer van zich af kunnen bijten. Dat vraagt om meer capaciteiten die liggen in het militaire- en inlichtingendomein. Op dit moment is veel van de Europese samenwerking gericht op reactieve en tot op zekere hoogte preventieve maatregelen. Lidstaten zelf ondernemen wel degelijk stappen om hun militaire cybercapaciteit uit te breiden (in meerdere gevallen bestaat er al meer dan tien jaar een soort cybercommando). Helaas komt de Europese samenwerking slechts mondjesmaat op gang. In 2017 werd op het International Cyber Operations Symposium aangegeven dat het bespreken van offensieve cybercapaciteit bij de NAVO tot voor kort taboe was[12]. Het European Defense Agency begint ook meer in te zetten op Europese defensiesamenwerking in het cyberdomein. Zo werd in 2018 een eerste belangrijke mijlpaal behaald met een grootschalige oefening binnen

het zogenaamde ‘Cyber Range Federation’ project, waarmee cyberdefensie-trainingscapaciteiten van elf landen worden geïntegreerd. Toch lijkt er sindsdien een behoefte te zijn aan meer Europese aansturing en coördinatie. In onze visie is het hierbij essentieel dat er niet alleen sprake is van onderlinge defensiesamenwerking, maar dat er ook een brug wordt geslagen tussen het militaire en civiele domein. We zullen binnen Europa de volgende stap moeten zetten in publiek-private samenwerking en de bestaande capaciteiten in verschillende domeinen zoveel mogelijk moeten verenigen. Alleen op deze manier zal Europa in staat zijn om haar fysieke en digitale markt te beschermen.

Het Nederlandse veiligheidsdomein moet een voortrekker zijn van Europese civiel-militaire samenwerking

Samenwerking tussen defensie en private partijen, maar ook inlichtingendiensten, is cruciaal voor Europa om gezamenlijk sterk te staan. Kruisbestuiving is cruciaal aangezien de traditionele scheiding van domeinen voor het cyberdomein niet opgaat. We kunnen niet meer spreken van militair versus civiel, publiek versus privaat en nationaal versus internationaal; dichotomieën die niet meer opgaan. In onze visie ligt hier bij uitstek een kans en verantwoordelijkheid voor Nederland om op te treden als een voortrekker van deze ontwikkeling. Nederland is van oudsher sterk in civiel-militaire samenwerking en het bouwen van bruggen tussen verschillende werelden. We zullen ontwikkelingen die nationaal al in gang zijn gezet ook internationaal moeten agenderen. In Nederland zitten liaisons van de inlichtingendiensten bijvoorbeeld vaak aan tafel bij sectorale ISACs. Ook Defensie zet de laatste jaren steeds meer in op het betrekken van de private sector bij haar cybercapaciteit, bijvoorbeeld door professionals uit het bedrijfsleven als cyberreservist in te zetten. Dergelijke voorbeelden zijn ook toepasbaar op Europees niveau en zelfs broodnodig. Door onze eigen ervaringen en ‘best practices’ ook in Europees verband te adresseren kunnen wij er zorg voor dragen dat er niet alleen samenwerkingsinitiatieven binnen, maar juist ook over verschillende domeinen heen ontstaan. In de wetenschap dat Nederland alleen niet opgewassen is tegen de uitdagingen die voortkomen uit het internationale cyberdomein zullen wij civiel-militaire samenwerking moeten aanjagen om daarmee een gemeenschappelijke Europese digitale vuist te laten zien.

Over de auteurs

fokko.dijksterhuis@capgemini.com

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

roeland.de.koning@capgemini.com

Roeland de Koning is gespecialiseerd in cybersecurity en crisisbeheersing. Zowel nationaal als internationaal werkt hij aan de realisatie van samenwerkingsvraagstukken op dit gebied, ‘ervaren van het probleem’ en ‘gewoon doen’ zijn daarbij de rode draad.

[1]https://edition.cnn.com/2020/01/08/tech/iran-hackers-soleimani/index.html

[2]https://www.bbc.com/news/technology-51008811

[3]https://edition.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/index.html

[4]https://www.documentcloud.org/documents/6598719-CISA-Insights-Increased-Geopolitical-Tensions.html

[5]https://www.reuters.com/article/us-ukraine-cyber-attacks-idUSKBN19I1IJ

[6]https://www.bbc.com/news/world-us-canada-42407488

[7]https://nos.nl/artikel/2253313-mivd-we-hebben-russische-hack-van-opcw-in-den-haag-voorkomen.html

[8]https://nos.nl/artikel/2322945-iraanse-overheidshackers-vallen-nederlandse-onderwijsinstellingen-aan.html

[9]Zie ook: https://www.trendsinveiligheid.nl/rapport/2018-vertrouwen-en-wantrouwen-in-de-digitale-samenleving/

[10]https://www.capgemini.com/news/capgemini-invent-contract-win/

[11]https://www.bitsoffreedom.nl/2011/05/05/the-virtual-schengen-border-or-great-firewall-of-europe/

[12]https://www.cfr.org/blog/europe-slowly-starts-talk-openly-about-offensive-cyber-operations

Commandovoering in cyberconflicten

Hoe visualiseer je een cyberaanval in een militair commandocentrum

Auteur
Peter Kwant

Highlights

- Een militaire commandant wil in één oogopslag inzicht krijgen in zowel zijn cyber- als zijn reguliere operatiegebied. Een dergelijke integraal beeld bestaat nog niet.
- De technieken en tactieken in het operationele cyberdomein wijzigen voortdurend. Om een duurzaam strategisch voordeel te halen en te houden moet dit beeld dus steeds worden aangepast. Daarvoor heeft de commandant een uitgebreid team van analisten, architecten en ontwikkelaars nodig.
- Actuele inzichten en technologie uit het civiele technologiedomein zijn geprojecteerd op de behoefte van militaire commandanten. Deze resultaten worden nu door NATO verwerkt bij de verdere ontwikkeling van het Recognized Cyber Picture.
- Dit zal er uiteindelijk toe leiden dat toekomstige militaire commandanten gelijktijdig beslissingen kunnen nemen over de inzet van fysieke én digitale wapensystemen in hun operatiegebied.

Binnen de NATO-organisatie ontwikkelen diverse R&D-instellingen technologie en standaarden om als bondgenoten gezamenlijk en effectief op te kunnen treden. NATO maakt ook gebruik van niet-militaire instituten die met hun kennis uit het IT-domein bijdragen aan de innovatie van de bondgenootschappelijke capaciteiten. Recentelijk heeft een team van Capgemini-experts een analyse uitgevoerd naar de wijze waarop cyberinformatie in een militair commandocentrum gepresenteerd en gedeeld kan worden. Dit artikel is een bewerking van het onderzoeksrapport en is tot stand gekomen door de succesvolle samenwerking van de onderzoeksleider van NCIA, Manisha Parmar en de projectleider van Capgemini, Peter Kwant.

Het expertteam van Capgemini bestond verder uit Frits Broekema, Ton Slewe, Jack van 't Wout, Bart van Riel en Manon Kornmann.

De samenwerking tussen NCIA en Capgemini werd mede mogelijk gemaakt door de begeleiding van 'The Hague Security Delta' (HSD) : https://www.thehaguesecuritydelta.com/.

Van oudsher kennen het militaire land-, zee- en luchtdomein hun eigen 'picture'. Op een hoger abstractieniveau worden die pictures geïntegreerd in het Common Operational Picture (COP). Nu het militaire cyberdomein zich razendsnel ontwikkelt, moet ook hiervan een picture samengesteld worden. Hoe deze picture ingevuld moet worden en hoe dit moet worden weergegeven, wordt in dit artikel verder verkend.

Cyberpicture

Deze visualisaties worden 'Common Operational Pictures' genoemd ('COP') en die pictures worden live gedeeld met collega commandanten in het operatiegebied zodat er een gezamenlijk en integraal beeld wordt gevormd. Op basis van dit COP en de gemeenschappelijke doctrines en tactieken kunnen de verschillende commandanten ieder op hun eigen niveau en binnen bevoegdheden operationele besluiten nemen. Een gedegen COP is dus van levensbelang om de operatie goed en effectief uit te voeren.

Naast de pictures van het land-, zee- en luchtdomein heeft de commandant nu ook behoefte aan een cyberpicture. Maar welke informatie stop je hierin? En hoe geef je dat op een militair-operationeel zinvolle wijze weer? Hoe communiceer je dit plaatje met de andere commandanten? En de vervolgvraag: hoe integreer je dit cyberpicture met de pictures van land, zee en lucht?

Het NATO Communications and Information Agency (NCIA) doet al langere tijd onderzoek naar dit complexe vraagstuk. De NCIA heeft in 2019 aan Capgemini gevraagd om met de actuele inzichten vanuit de civiele en militaire wereld een analyse uit te voeren op dit specifieke vraagstuk.

In tijden van verhoogde spanning zijn militaire operators alert op de detectie van signalen die kunnen wijzen op een mogelijke vijandelijke aanval. Militaire doctrines beschrijven de indicatoren voor het activeren van razendsnelle, deels geautomatiseerde, tegenreacties. Daarvoor is het wel nodig dat die indicatoren op een overzichtelijke manier worden gevisualiseerd, zodat de commandant in het commandocentrum in één oogopslag een compleet overzicht wordt geboden en hij ook direct kan beslissen over de tegenactie.

Wicked problem

In een militaire operatie werken veel verschillende partijen samen, elk met eigen economische, politieke en culturele achtergronden. Dat zijn vaak NATO-bondgenoten maar dat kunnen ook ad hoc coalitiepartners van allerlei soort zijn. In deze soms zeer complexe coalities moet technische cyberinformatie kunnen worden uitgewisseld om cyber-gerelateerde aanvallen te detecteren, er op te reageren of juist te voorkomen.

In de door Capgemini uitgevoerde analyse is onderzocht welke informatiestandaarden en applicaties op de markt beschikbaar zijn, om die uitwisseling van informatie mogelijk te maken. Bovendien is onderzocht in welke mate deze voldoen aan de eisen die in het militaire cyberdomein worden gesteld. Hieruit is geconcludeerd dat er een breed aanbod van producten op de markt beschikbaar is, met een grote

variatie aan (on)mogelijkheden voor informatie-uitwisseling. Afhankelijk van de gevraagde interoperabiliteit met reeds in gebruik zijnde tools en informatie-uitwisselingstandaarden en afhankelijk van de gewenste workflow kan een geschikte keuze worden gemaakt. Hierbij is de 'Use Case Analysis methodology' [1,2] uitgewerkt waarmee NATO de productselectie gestructureerd kan uitvoeren en eventuele hiaten met eigen ontwikkeling kan overbruggen.

Information requirements

Naast duidelijkheid over hoe operationele cyberdata gedeeld kan worden, is er ook onderzocht welke cyberdata een commandant nodig heeft om het 'Recognized Cyber Picture' (RCP) zo optimaal mogelijk te vullen. Het RCP vraagt om zinvolle gegevens over de digitale infrastructuur, over de missie van de operatie en gegevens afkomstig van inlichtingen. Alhoewel vele bondgenoten al bezig zijn met de ontwikkeling van dergelijke RCP-visualisaties, is er nog geen breed gedeeld overzicht van de gegevens die nodig zijn om een commandant in het operatiegebied optimaal te ondersteunen.

In de door Capgemini uitgevoerde analyse is een set van initiële information requirements opgesteld die van belang zijn voor de commandant. Uitgangspunt is dat de gepresenteerde informatie aansluit op de beschikbare beslissingsopties voor die commandant. Primair is een commandant vervolgens geïnteresseerd in gegevens die betrekking hebben op de beschikbaarheid van zijn eigen eenheden.

Verder heeft hij behoefte aan inzicht in de operationele situatie in zijn operatiegebied inclusief het cyberdomein. Hierbij gaat het natuurlijk voornamelijk om de capaciteit en de activiteit van de opponenten. Tenslotte heeft hij een visualisatie nodig die hem een zo breed mogelijk overzicht biedt van zijn eigen militair-tactische opties. Oftewel in spreektaal: hij wil weten wat er speelt, waarom dit speelt en een voorspelling over wat er waarschijnlijk gaat gebeuren.

De functionele eisen die voortvloeien uit deze informatiebehoefte is uitgewerkt in concrete informatie-elementen en hun onderlinge samenhang. Op basis van een operationele analyse is vervolgens geëvalueerd welke informatie relevant is voor de missiecommandant.

De belangrijkste conclusie uit deze analyse is dat een cyberpicture meer is dan een vooraf ingericht samenstel van gegevens. Want veel meer dan in het fysieke domein veranderen de technieken en tactieken in het operationele cyberdomein voortdurend. Om een duurzaam strategisch voordeel te halen en te houden moet een picture zich dus steeds aanpassen aan de omstandigheden. En daarvoor heb je een uitgebreid en breed samengesteld team van experts nodig, bestaande uit analisten, architecten en ontwikkelaars. Dit team moet dicht tegen de commandant aan zitten en in staat zijn om razendsnel nieuwe pictures te bouwen van de cybersituatie op dat moment. Maar ook het command-team zelf - de operators die de pictures uitlezen - moeten getraind worden om met deze voortdurende aangepaste pictures om te gaan. Er wordt dus veel gevraagd van de militaire staf en de backoffice. Zij moeten in staat zijn zich snel aan te passen aan de veranderende omstandigheden. Binnen en buiten defensie is er reeds veel ervaring met dergelijke adaptieve methodes. In het operationeel militaire domein worden deze methodes nu echter nog weinig toegepast.

Informatie-uitwisseling in een coalitie vraagt om een 'Combat Cloud'

Militaire operaties vinden vrijwel altijd plaats in coalities. Soms met NATO-partners alleen, maar heel vaak ook met partners daarbuiten, waarbij het per partner kan verschillen welke gegevens wel en niet gedeeld kunnen worden. Ook cybergegevens moeten in dergelijke omgevingen snel en effectief uitgewisseld kunnen worden. De basis voor een dergelijke samenwerking is een minimaal kwaliteitsniveau van de Command & Control (C2) infrastructuur van de partners. Door NATO is een set met minimale kwaliteitseisen gedefinieerd voor de C2-infrastructuur van de partners. Deze eisen maken deel uit van het Federated Mission Network (FMN) programma waaraan inmiddels vele bondgenoten zich hebben gecommitteerd.

Het eerste doel van een militaire operatie is het bereiken van 'superiority' op land, zee en in de lucht. Als die superiority is bereikt kan vervolgens het uiteindelijke doel van de operatie worden gerealiseerd. Voorafgaand aan de superiority in de fysieke domeinen zal eerst 'information superiority' bereikt moeten worden. Met de uitvoering van het FMN-programma wordt invulling gegeven aan deze ambitie.

De gemeenschappelijke C2-omgeving is uiteindelijk nodig voor de ontwikkeling van een concept waarbij de data centraal staat (data-centric). De infrastructuur moet het verwerken en analyseren van grote volumes data mogelijk maken; een 'information highway' dus. Een Virtual Data Warehouse biedt deze beschikbaarheid en toegang. Om een Virtual Data Warehouse ter ondersteuning van de collaborative C2 te creëren is een effectieve en veilige militaire Cloud-oplossing nodig: de 'Combat Cloud'.

De Combat Cloud bestaat uit vier lagen: 1) een laag die de samenwerking en/of samenhang beschrijft tussen sensoren, effectoren en besluitvorming, 2) een functionaliteitslaag, 3) een datalaag en tot slot 4) de infrastructuurlaag.

Bevindingen vertaald naar architectuur: Recognized Cyber Picture architectuur

De resultaten van de voorgaande drie analyses zijn voor verdere analyses en implementatie toegankelijk gemaakt in een set architectuur views die aansluiten op het NATO Architecture Framework. Deze vormen daarmee het proof-of-concept voor de eerste iteraties van het Recognized Cyber Picture. Deze views zijn in een workshop met NATO-architectuur experts getoetst en met de feedback is een basis gecreëerd waar NATO verder invulling aan kan geven.

Tot slot

Het integraal gevisualiseerd overzicht van alle relevante gegevens in een militair operatiegebied, waarbij de beschikbare beslissingsopties gelijktijdig toegankelijk zijn voor alle commandanten in het theater, vormt een randvoorwaarde voor succesvolle militaire operaties. Er is reeds veel ervaring met dergelijke presentaties in het militaire land-, zee- en luchtdomein. In het cyberdomein is die ervaring echter nog zeer beperkt, dit terwijl de cybercomponent in militaire operaties de afgelopen jaren juist enorm is ontwikkeld.

NCIA heeft met Capgemini een analyse uitgevoerd waarin actuele inzichten en technologie uit het civiele cyberdomein worden geprojecteerd op de behoefte van militaire commandanten. Deze resultaten worden nu door NCIA verwerkt in de verdere ontwikkeling van het Recognized Cyber Picture en zullen er uiteindelijk toe leiden dat toekomstige militaire commandanten gelijktijdig beslissingen kunnen nemen over de inzet van fysieke én digitale wapensystemen in hun operatiegebied.

Over de auteurs

Manisha Parmar is Senior Scientist bij de NATO Communications and Information Agency (NCIA) in Den Haag. Ze is gespecialiseerd in cybersecurity en cyberspace operaties. Daarnaast heeft ze een diepgaande interesse in situational awareness, cyber threat intelligence en andere mission assurance gerelateerde onderwerpen. Per 1 september 2020 is Manisha aangesteld bij NATO ACT als Cyberspace Branch Programme Director.

peter.kwant@capgemini.com

Peter Kwant (Executive Master Security & Defence) is Principal Consultant Cybersecurity bij Capgemini en voormalig marineofficier.

[1]https://www.capgemini.com/2019/05/how-to-define-complex-use-cases-and-implement-them-in-your-siem-soc-project/

[2]Use Case Analysis is een methode waarmee de eisen die worden gesteld aan een nieuw te bouwen systeem op een systematische wijze worden geïdentificeerd en vastgelegd. Zie voor een verdere toelichting onder meer: https://en.wikipedia.org/wiki/Use-case_analysis

Stabiliteit en chaos gevraagd: op weg naar een nieuw meldkamersysteem

Hoe komen, en blijven meldkamerorganisatie en meldkamersysteem bij de tijd?

Auteurs
Erik van den Berg
Erik Staffeleu

Highlights

- Blijven voldoen aan technologische trends vraagt ook om het scheppen van enige chaos.
- Experimenteerruimte biedt de kans om 'dingen anders te gaan' doen en blijvend te vernieuwen.
- Experimenteren met couleur locale, met data-analyse, kennistechnologie en met nieuwe functionaliteiten is een doel op zich.
- Het beheer van kritische gegevens los van iedere context versus het gebruik en de analyse ervan binnen ieder voorspelbaar of ondenkbaar scenario is een basisvaardigheid.

Het ontbreekt niet aan visies op de functie van de meldkamer in de toekomst. De Landelijke Meldkamer Samenwerking (LMS) organisatie staat, innovatieprogramma's lopen en de governance is geregeld. Een enorme prestatie. Conform planning komt nu de technische realisatie van de meldkamer van de toekomst dichterbij. Welke eisen stelt de meldkamer van de toekomst? En waarom *lijkt* deze vraag makkelijk te beantwoorden maar blijkt dit geenszins het geval?

De wereld verandert. De digitalisering van de samenleving gaat steeds sneller, enzovoort, enzovoort. U kunt inmiddels ongetwijfeld, net als wij, de start van artikelen over de impact van digitalisering op onze samenleving zelf invullen. Visies op de impact van digitalisering starten vaak met het beschrijven van de digitale revolutie en de enorme beschikbaarheid van informatie, gevolgd door een aantal onderliggende trends, om vervolgens te concluderen dat we nog veel kunnen verwachten van techniek x, y of z. Echter, het ontbreekt in dezelfde artikelen vaak aan handelingsperspectief voor de snelle doorontwikkeling van techniek. Soms door een gebrek aan kennis over informatiebeveiliging, cybersecurity, technische ontwikkelingen als Artificial Intelligence (AI), Internet of Things (IoT)-Smart-[1], 5G[2]-Sensing of Virtualisatie, Digital Twinning[3] maar vaak ook doordat de trends maken dat de technische ontwikkeling lastig te voorspellen is. Het is niet meer een ontwikkeling van A naar B. In plaats van ons te moeten voorbereiden op een toekomst, hebben we ons nu voor te bereiden op meerdere varianten van de toekomst.

Wij zien bovenstaand patroon ook terug in hoe er wordt geschreven over de meldkamer van de toekomst en de rol die techniek heeft in de ondersteuning hiervan. In dit artikel staan we daarom slechts kort stil bij de trends. Dit artikel richt zich meer op de vraag wat continu kunnen inspelen op veranderingen in de techniek vraagt van het nieuwe meldkamersysteem en de bijbehorende meldkamerorganisatie.

Een levend systeem

In onze visie op incidentbestrijding en crisisbeheersing zien wij de meldkamerorganisatie en de ondersteunende meldkamertechnologie als een levend, open en adaptief systeem van samenwerkende burgers, hulpverleners, organisaties en technologie. Een levend systeem zoals bijvoorbeeld ook een koraalrif en een stad levende systemen zijn die zich continu moeten vernieuwen.

De incidentbestrijding en crisisbeheersing is een levend systeem dat moet omgaan met vele trends zoals de toename van sensoren, beschikbaarheid van data, de toename van beeldtechnologie, de steeds grotere betrokkenheid van burgers bij veiligheid en de toename van verwachtingen van burgers over de contactmomenten met hulpverleners. En net als ieder ander levend systeem heeft de meldkamerorganisatie elementen nodig die stabiliteit brengen, en tegelijk elementen die chaos creëren. Elementen die voorspelbaarheid brengen maar ook elementen die vernieuwing brengen.

Zonder stabiliteit en voorspelbaarheid valt het systeem uit elkaar, maar zonder chaos en vernieuwing kan het zich niet aanpassen aan de veranderende omgeving. Elementen die voorspelbaarheid en stabiliteit brengen zijn bijvoorbeeld de verschillende betrokken hulpverleningsorganisaties. Uiteraard zijn de hulporganisaties zelf continu in verandering maar we hebben het nog steeds over dezelfde partners. Ook de ontwikkelde LMS-organisatiestructuur brengt stabiliteit en voorspelbaarheid, een fundament waarop gebouwd kan worden. Tegelijk laten de reeds genoemde trends zien dat er nog genoeg chaos aankomt en dat adaptief verandervermogen nodig is. Duidelijk is dat de toename van sensoren en data zal blijven groeien en daarmee het onnodig reageren op 'false positives' die de inzet van spaarzame responsecapaciteit verder onder druk zet. In welke mate en welke wijze bijvoorbeeld AI kan helpen in de duiding en besluitvorming in de meldkamer is nog onduidelijk maar het biedt de mogelijkheid om 'dingen anders te gaan doen'. Continu vernieuwen van organisatie, werkwijze en technologie is dus een gegeven en experimenteren een doel op zich.

Technologie als permanente vernieuwer

Het ligt voor de hand dat het technisch meldkamersysteem een stabiliserend element gaat zijn in de landelijke meldkamersamenwerking. Het moet ondersteunend zijn aan de vitale processen, het moet het doen als het ertoe doet. Onze visie is echter ook dat er altijd experimenteerruimte moet zijn om met veranderende behoeften en innovatieve technologie om te gaan. Als bijvoorbeeld door realtime AI betrouwbare adviezen ontstaan over het verwachte incidentverloop en daaraan gekoppelde acties en maatregelen, dan ontstaan er ook andere manieren van werken.

Om adaptief te zijn in de kern van het ontwerp van het meldkamersysteem van de nieuwe tijd gelden er een aantal basisvereisten. Een basisvereiste is bijvoorbeeld het meervoudig kunnen gebruiken van centraal beschikbare gegevens van gekende kwaliteit. Dit voor het borgen van de altijd actuele en eenduidige informatiepositie als basis voor een flexibel doch integraal procesverloop ongeacht de context. Voordelen zijn het verder reduceren van de call handling-tijd en de verbeterde besluitvorming tijdens een (dreigend) incident en/of crisis op het gebied van veiligheid. Daardoor worden snellere interventies in het veld haalbaar en verloopt het incident- en crisismanagement beter. De hierop aansluitende visie van Capgemini partner Saab, leverancier van het toekomstgerichte meldkamerproduct SAFE, in deze is:

> At Saab we strongly believe that it is a human right to feel SAFE. For the future, we seek to enable first responders through our world-class technology to also be first preventers by arming all societal stakeholders with the information to make the best decisions possible."

Door de opbouw van de altijd actuele informatiepositie wordt de **Situational Awareness** verbeterd, zowel voor de meldkamerorganisatie als voor de operationele eenheden in het veld. Een **Common Operational Picture** (COP), waarbij verschillende operationele eenheden gelijktijdig en ongeacht hun eigen locatie (of device) eenzelfde beeld krijgen van de situatie, is daarbij noodzakelijk. Naast de pictures van de situatie op land, zee of in de lucht is er bijvoorbeeld ook een 'cyberpicture'[4]. Het beheer van kritische gegevens los van iedere context versus het gebruik en de analyse ervan binnen ieder voorspelbaar of ondenkbaar scenario is een basisvaardigheid van de toekomstige meldkamerorganisatie (zie figuur).

Eenvoudige omni-/multi-kanaalcommunicatie tussen alle actoren op het terrein, via een gedeelde COP laat toe om de meest actuele informatie beschikbaar te hebben en te delen tijdens een incident of een crisis. De meldkamer kan daarin de rol opnemen van opbouwer, beheerder, bewaker en regisseur van de excellente informatiepositie. Die vervolgens in de vorm van op maat gemaakte situatiebeschrijvingen en berichten met het netwerk van betrokken actoren wordt gedeeld.

De meldkamer van de toekomst moet voorzien in alle communicatiemogelijkheden om **multimedia-informatie** (beeld, audio, video, social media feeds, sensoren) snel en veilig te delen en met slimme filtering ter beschikking te stellen van verschillende actoren, afhankelijk van hun positie of hun rol. Vanuit de meldkamer moet het mogelijk zijn om bijvoorbeeld aanvullende informatie over het terrein langs dezelfde kanalen te delen met mobiele gebruikers of input van **mobiele gebruikers** of burgers (112-app, e-call, geotagged foto's etc.) op gestructureerde manier en met gekende kwaliteit aan te bieden aan de meldkamer om ze vervolgens weer te verspreiden.

Bij de verdere groei van het IoT is het ook een vereiste zijn om **sensoren en apparaten** centraal vanuit de meldkamer aan te sturen, bijvoorbeeld het inschakelen van signalisatie, openbare verlichting en camera's.

Om het adaptieve en (zelf-)lerende vermogen van de meldkamer van de toekomst verder te versterken is deze uitgerust met **analytische en kunstmatige intelligentie (AI) functionaliteiten.** Hierdoor is de meldkamerorganisatie in staat om complexe gebeurtenissen via simulaties voor te bereiden, situaties predictief te extrapoleren (bv. verkeerscongestie, inbraakgolven, verspreiding chemische gassen etc.). Data-analyse maakt ook het monitoren van het end-to-end proces mogelijk op basis van meetbare key performance indicators (KPI's), waarmee het noodzakelijke bestuurlijke inzicht ontstaat voor het (bij-)sturen van beleid of van werkwijze.

Iedere veiligheidsregio en meldkamerorganisatie heeft, en is gehecht aan haar, couleur locale. Het **ene geïntegreerde voor meerdere toepassingen en meldkamerlocaties te configureren platform (het meldkamersysteem)** moet voldoende ruimte bieden voor deze couleur locale. Het bestaat daarom uit in één gedeeld platform met zowel een aantal (configureerbare) instanties per meldkamerorganisatie als uit een aantal op centraal, regionaal of lokaal niveau te configureren templates en views.

Voor de eindgebruiker van de meldkamer zelf moet een toekomstige meldkamerapplicatie zich presenteren via één geïntegreerde User Interface (UI) die aan het profiel en/of de concrete operationele omstandigheden aanpasbaar is. Het werken in verschillende views en combinaties van schermen/toepassingen moet volledig verdwijnen om de call-handling en dispatching zo efficiënt mogelijk te laten verlopen en elk incident end-to-end te kunnen opvolgen. Ook de mobiele toepassingen voor actoren op het terrein moeten uitgerust zijn met een **zeer eenvoudige, configureerbare User Interface.**

Basis-meldkamerfunctionaliteiten rondom (112) telefonie, communicatie met en de aansturing van de hulpverleners (politie, brandweer, ambulancezorg) blijven nodig.

Dit stabiel houden van de basis, voldoen aan bovenstaande eisen versus het continu vernieuwen vraagt ook wat van de leverancier van moderne meldkamersystemen. Zie het kader waarin Saab uitlegt hoe zij dit met de SAFE-productlijn mogelijk maakt.

"The changing nature of the threat landscape, combined with rapid digital transformation, requires, but also enables, Public Safety agencies to be pro-active and predictive, rather than reactive. To be able to successfully manage threats of today and the future, a critical element is to operate a control room with an integrated technology platform staffed with well-trained operators. Saab's software integration platform (SAFE), specifically designed for the Emergency Response control room, offers a modern, agile solution that meet tomorrow's challenges. It is robust and battle-hardened through multiple deployments in control rooms at 112 sites, airports, prisons and multi-modal transportation hubs.

SAFE allows for integrating and connecting any existing or future system, sensor or database and in one single pane of glass provide a Common Operating Picture (COP). There is no rip and replace, but use the infrastructure that is already in place, normally beautifully stove piped with many screens, mice, radios and telephones, and simply connect it to SAFE.

Using this platform and configuring workflows of how information is presented, in which order and to which function will streamline processes enabling faster and better decisions. It will lead to standardization of event management that creates centralized repository of event data that is valuable business intelligence. The comprehensive event data can be used to generate many different types of reports and allow measuring towards different measurable key performance indicators (KPI's).

We also currently evaluating an AI tool as a part of the platform that handles many layers of data. This will make it possible to include additional sensor functionality that today not is possible due to information overflow. AI will make it possible to collect information from different components and bring them together in a way that not have been possible before.

Our platform has been build based on research with the aim of providing one unified control room to meet todays and tomorrows needs for the modern control room operators. Hence, we are on top of all trends that we see as important for our customers."

Rickard Häggsjö Director

Sales & Marketing - Public Safety & Security Saab

(Toekomst)Visie op een wendbare architectuur

De architectuur van het meldkamersysteem van de nieuwe tijd moet modulair zijn waardoor het kan worden opgedeeld in services en functionaliteiten en waardoor er ook specifieke functionaliteiten kunnen worden toegevoegd voor de couleur locale of specifieke doeleinden. Het laat daarmee voldoende 'experimenteerruimte' om te kunnen omgaan met de vele trends die op de meldkamer afkomen. Sterker nog, het experimenteren is een doel op zich om een zekere chaos toe te voegen aan het levend systeem van crisisbeheersing en incidentbestrijding zodat vernieuwing proactief kan worden gevonden en het technische meldkamersysteem voldoende innoverend en adaptief kan zijn.

Het meldkamersysteem van de toekomst ontwikkelt altijd door. De meldkamer is dan ook een end-to-end, levend, adaptief, (continu) innoverend netwerk van systemen, software en slimme oplossingen (van vandaag en van de toekomst). Dit stelt eisen aan gegevensbeheer, standaarden, interfaces, uniformiteit en dus aan de onderliggende meldkamersysteem-architectuur. Een goed doordachte modulaire informatie- en systeemarchitectuur kan (adaptief) nieuwe technologieën of informatiebronnen integreren die de snelheid, samenwerking of het inzicht (actuele informatiepositie, COP, situational awareness) verbeteren, zoals:

- Identity en voice recognition die kan ondersteunen bij het vaststellen van de betrouwbaarheid van de bron en/of de melder(s) en het vaststellen van de geolocatie.
- Streaming videobeelden en verkeerscamera's (live en playback modus).
- Camera's en andere sensoren gekoppeld en beschikbaar op de kaart.
- Indoor navigatie in publieke gebouwen, kantoren, winkelcentra etc.
- (Geautomatiseerde) analyses op databronnen inclusief social media feeds.
- Artificial Intelligence om situaties predictief te modelleren en voorspellen. Crowd dynamics, criminaliteitsgolven, verkeerscongestie etc.
- Toegang tot historiek van (gelijkaardige) incidenten voor data-analyse.

Afsluitend

We staan aan de vooravond van de realisatie van een meldkamersysteem dat klaar is en blijft om burgers in nood sneller en efficiënter te helpen. De ambulancezorg, brandweer, marechaussee, gemeenten en politie beter te faciliteren bij hulpverlening, bij communicatie en bij bestrijding van crisis en rampen. De meldkamer van de toekomst raakt aan alles wat met digitalisering in onze maatschappij te maken heeft. Van de toename van sensoren en toename van (beeld)informatie, tot de wijze waarop wij als burgers met alle nieuwe mogelijkheden omgaan en hoe de overheid deze kan inzetten voor meer effectiviteit en efficiency. Dit stelt hoge eisen aan hoe een meldkamersysteem en -organisatie dit kan ondersteunen. Wij pleiten ervoor dat een nieuw meldkamersysteem niet enkel wordt gezien als ondersteunend maar juist ook als aanjager van de continue vernieuwing. Dat het ontwerp van het systeem modulair is en experimenteerruimte laat om niet enkel stabiliteit en voorspelbaarheid te brengen maar ook een zekere mate van chaos en vernieuwing. Dat experimenteren met couleur locale, met data-analyse, met kennistechnologie en met nieuwe functionaliteiten niet alleen reactief gebeurt maar een doel op zich is. Ieder levend systeem heeft een beetje chaos nodig om te kunnen floreren.

Over de auteurs

erik.staffeleu@capgemini.com

Erik Staffeleu is Senior Director Public Security. Hij helpt publieke en private organisaties een stap verder te zetten in hun ontwikkeling. Vanwege persoonlijke affiniteit doet hij dit het liefste met organisaties binnen het veiligheidsdomein.

erik.vanden.berg@capgemini.com

Erik van den Berg is portfoliomanager Business Innovatie en een expert op het gebied van Informatie Gestuurd Werken in veiligheid- en crisismanagement. Hij helpt organisaties in het veiligheidsdomein met innovatie in combinatie met het verkennen van nieuwe business-modellen.

[1]Zie het artikel Sensing voor veiligheid – Bouwstenen voor succesvol Informatie Gestuurd Optreden, in deze editie van Trends in veiligheid, L. Tubbing, A. van den Berg, M. v.d. Ridder

[2]Zie het artikel Effectief Informatie Gestuurd Werken (IGW) in een wereld met 5G-sensing, Trends in Veiligheid, 2019 Capgemini, M. v.d. Ridder, L. Schepers.

[3]Zie het artikel van de virtuele meldkamer in Trends in Veiligheid,2019 Capgemini, J. Kennis, M. Adriaens.

[4]Zie ook het artikel 'Cyber oorlogsvoering is bijna volwassen (P. Kwant)' in dit rapport.

Burgerparticipatie in online opsporing

Kunnen burgers helpen in opsporingszaken met het verzamelen van online informatie (OSINT)?

Auteur
Frank Inklaar

Highlights

- Publieke OSINT-initiatieven als Bellingcat leveren steeds vaker belangrijke bijdragen aan opsporingsonderzoeken.
- Het succes van publieke OSINT-onderzoekers is te danken aan een combinatie van veel beschikbare open informatie en een goed samenwerkend netwerk van verschillende specialisten, ook internationaal.
- Opsporingsinstanties kunnen passief gebruik maken van dergelijke resultaten maar ook actief de samenwerking zoeken in hackatons of door het bewust delen van bepaalde informatie.
- Aandachtspunten in die samenwerking zijn de bescherming van het onderzoek, maar ook de privacywetgeving en de veiligheid van de burgerparticipanten.

In het onderzoek naar het neerhalen van vlucht MH17 werd de wereld tot tweemaal toe verrast door de resultaten van het burgercollectief Bellingcat. Zo slaagden ze er niet alleen in om de complete route van de BUK-lanceerinstallatie vanuit de Russische basis naar de lanceerplek in Oekraïne en weer terug in kaart te brengen, maar ook om op basis van foto- en geluidsmateriaal de complete commandostructuur rond het transport en afvuren van de raket te achterhalen[1].

Uiteindelijk resulteerde dit in een lijst met concrete verdachten en belangrijk bewijsmateriaal. En dit alles grotendeels op basis van informatie die voor iedereen op internet beschikbaar is (maar niet altijd makkelijk te vinden). Het doen van onderzoek op basis van openbare informatie staat bekend onder de afkorting OSINT (Open Source Intelligence). Door de enorme groei van beschikbare open informatie (sociale media maar bijvoorbeeld ook satellietfoto's) nemen de mogelijkheden van OSINT enorm toe, maar daarmee ook de uitdagingen om die optimaal te benutten. Wat is het geheim van de doelmatigheid van collectieven zoals Bellingcat? En hoe kunnen opsporingsinstanties daar ook gebruik van maken?

De opkomst van OSINT voor iedereen

Helemaal nieuw is de opkomst van OSINT niet: er bestaat al een lange traditie van onderzoeksjournalistiek op basis van open bronnen. Vroeger was dit nog voorbehouden aan de enkeling die de tijd en het doorzettingsvermogen had om daadwerkelijk toegang te krijgen tot bepaalde (fysieke) archieven en alles aan elkaar te puzzelen. Met de explosie van op internet beschikbare informatie, de opkomst van online communities en samenwerkingssoftware is het nu voor iedereen mogelijk geworden om vanuit de huiskamer aan dergelijke onderzoeken bij te dragen.

Dit betekent nog niet dat het uitvoeren van een OSINT-onderzoek eenvoudig is. Natuurlijk kan iedereen zoeken met Google en wat rondkijken op Streetview, maar om precies de juiste informatie boven water te krijgen is vrijwel altijd meer nodig dan het standaardgedrag van dergelijke tools. Zo past Google standaard filters toe op grond van de locatie van de gebruiker die in dit verband meestal niet optimaal zijn. Tevens zijn er allerlei opties om de zoekresultaten te sturen die bij het grote publiek niet bekend zijn. Bovendien is Google niet de enige zoekmachine: er zijn andere zoekmachines (onder andere Bing, Yahoo, Baidu, Yandex) die soms handiger en beter zijn in bepaalde aspecten. Neem bijvoorbeeld 'reversed image search' (zoeken op grond van een foto) of voor het vinden van andere foto's van eenzelfde persoon op grond van een beschikbare foto. Daarnaast zijn er ook specialisaties zoals het analyseren van stemmen en geluiden, interpretatie van satellietbeelden, lokaliseren en dateren van foto- en videomateriaal en het opsporen van (al dan niet frauduleuze) bewerkingen in foto-en geluidsmateriaal.

Voor één persoon is het eigenlijk niet mogelijk om in al die gebieden goed thuis te zijn. Door online (en vaak ook internationale) samenwerking wordt het mogelijk die kennis te verbinden en te combineren. Bellingcat is bijvoorbeeld goed in staat gebleken om verschillende specialismen en internationale (taal en cultuur) kennis te bundelen en verbinden. Hierdoor hebben ze naast de MH17-case ook in veel andere zaken een grote bijdrage kunnen leveren. De aanslag met zenuwgas op Skripal in het Verenigd Koninkrijk, het gebruik van gifgas in Syrië, executies door IS en seksueel kindermisbruik in Thailand vormen nog maar een deel van de lijst van zaken waarin Bellingcat belangrijke aanknopingspunten boven water heeft weten te krijgen[2].

Het kennisgebied van OSINT-technieken is breed en complex, maar is wel voor iedereen te vergaren. Binnen de OSINT-gemeenschap worden tips, technieken en tools breed en openlijk gedeeld via websites, blogs en podcasts. Ook op de Bellingcat website is zeer veel informatie over de gebruikte onderzoekstechnieken gepubliceerd. Hiermee komt OSINT binnen het bereik van iedereen die bereid is er voldoende tijd en inspanning in te steken. En daar kunnen ook reguliere opsporingsdiensten hun voordeel mee doen.

De betekenis voor de opsporing

Het gebruik maken van informatie van burgers in opsporingszaken is niet nieuw. Zo wordt in het tv-programma 'Opsporing Verzocht' informatie gedeeld met het publiek in de hoop dat getuigen of personen rond de verdachten met bruikbare tips komen. Ook in de zaak rond de vermissing van Anne Faber werd een aanzienlijke bijdrage geleverd door het netwerk van vrienden en familie van het slachtoffer die actief meewerkten aan het onderzoek. Een belangrijk voorwaarde in die samenwerking is de mate waarin opsporingsinstanties informatie kunnen en willen delen met burgers. Het 'kunnen delen' heeft daarbij

te maken met wettelijke bepalingen met onder andere de privacywetgeving (AVG) en het 'willen delen' heeft te maken met de risico's voor het onderzoek als bepaalde informatie op straat komt te liggen. Maar daarnaast moet er ook de wil zijn om hulp van buiten de eigen organisatie te aanvaarden: men dient dit als een extra kans te leren zien en het niet te ervaren als een bewijs van onvermogen om alles zelf af te kunnen.

In de gevallen waar het niet mogelijk is om informatie te delen betekent dit nog niet dat er niets mogelijk is. Veel traditionele onderzoeksjournalistiek gebeurt al op basis van alleen open bronnen. Dit resulteert uiteindelijk in een eindrapport wat door opsporingsinstanties nog steeds kan worden gebruikt als basis voor een eigen onderzoek. Maar er zijn ook gebieden waar het delen van informatie wel degelijk mogelijk is, bijvoorbeeld 'cold cases', de opsporing van vermiste personen en de opsporing van veroordeelde criminelen die hun straf proberen te ontlopen. In deze gevallen weegt het privacyaspect minder zwaar, maar zal wel altijd kritisch bekeken moeten worden.

Begin 2020 heeft BlueM, een (bottom-up) innovatieonderdeel van de Nederlandse Politie, een hackaton georganiseerd met ruim 90 OSINT-specialisten (deels van de politie zelf en deels van buiten) om in de categorie 'onvindbare veroordeelden' nieuwe aanwijzingen te vinden[3]. Nog tijdens de hackaton leidde dit al tot één nieuwe aanhouding en uiteindelijk tot de opsporing en arrestatie van 5 personen die in totaal zo'n 15 jaar gevangenisstraf moesten uitzitten. In de Verenigde Staten helpt 'Trace Labs' met het opsporen van vermiste personen door het organiseren van 'capture the flag' (CTF) events waarbij deelnemers in een soort wedstrijdsetting proberen nieuwe aanwijzingen boven water te krijgen[4]. Zo is ook in het MH17-onderzoek onderzoek bewust informatie gedeeld: het onderzoek van Bellingcat was nooit zo ver gekomen zonder de vrijgegeven radiogesprekken rond het transport en de lancering van de BUK die door de Oekraïense geheime dienst waren opgepikt. Een ander voorbeeld is Europol die het initiatief 'Trace an Object' heeft gelanceerd[5]. Hierbij worden (fragmenten van) afbeeldingen van voorwerpen, kledingstukken of gebouwen getoond die afkomstig zijn van kinderpornomateriaal in de hoop dat het op grond van dit materiaal mogelijk is om nauwkeuriger te bepalen waar bepaald materiaal geproduceerd is. Ook hier wisten OSINT-onderzoekers belangrijke aanknopingspunten te vinden. Een heel andere toepassing is advies geven over hoe juist niet online traceerbaar te zijn, bijvoorbeeld aan slachtoffers van stalking door een ex-partner[6].

Risico's en aandachtspunten

Er kleven ook nadelen aan publieke opsporing door OSINT-specialisten. Voor zelfstandig door burgers uitgevoerde OSINT-onderzoeken geldt dat de rapporten en gebruikte technieken openbaar zijn en dus dat ook de personen en instanties die onderzocht zijn er wijzer van kunnen worden. Zo is het redelijk waarschijnlijk dat het Russische leger naar aanleiding van het MH17-onderzoek stappen zal ondernemen waardoor foto's van manschappen en materieel tijdens operaties niet meer zo vrijelijk op sociale media gedeeld zullen worden. Ook bij Amerikaanse manschappen is aan het gebruik van bepaalde apps (Strava) tijdens missies beperkingen opgelegd[7].

Waar wel informatie gedeeld wordt, zal steeds gekeken moeten worden naar wat er privacytechnisch mogelijk en wenselijk is. Zo werd voor de BlueM hackaton een beroep gedaan op de eigen privacyfunctionarissen en werd het OM hierin nauw betrokken. Ook kan het nodig zijn om aan burgerparticipanten een geheimhoudingsverklaring te vragen of een mate van screening toe te passen.

Tenslotte kan er een gevaar bestaan voor publieke OSINT-onderzoekers zelf. Recent nog zijn Bellingcat onderzoeker Michael Colborne and Oleksiy Kuzmenko met de dood bedreigd naar aanleiding van een onderzoek naar ultrarechtse groeperingen in Oekraïne[8]. Ook worden Bellingcat-medewerkers lastig gevallen via hackingactiviteiten van aan de Russische staat gelieerde hackerscollectieven. Waar politiemedewerkers vaak enige anonimiteit genieten zijn dergelijke onderzoekers en journalisten met naam en toenaam bekend en zo lastiger te beschermen.

Conclusie

Uit recente ervaringen is gebleken dat burgers met OSINT-kennis en -vaardigheden belangrijke bijdragen kunnen leveren aan zowel nationale als internationale zaken. Doorslaggevend is daarbij de samenwerking in een netwerk van vele specialiteiten en soms ook nationaliteiten, waardoor opsporingsmogelijkheden ontstaan die de eigen organisatie van opsporingsinstanties te boven kunnen gaan. In plaats van passief te wachten op het zelfstandige resultaat van dergelijke collectieven is het ook mogelijk om actief de samenwerking aan te gaan. Bijvoorbeeld via hackatons, CTF-evenementen of door het bewust openbaar maken van bepaald materiaal in een zaak. In de samenwerking moet naast aandacht voor de veiligheid van zaaksinformatie, de privacybepalingen maar zeker ook de veiligheid van de burgerparticipanten in het oog worden gehouden. Mijns inziens zijn binnen die grenzen mooie initiatieven mogelijk die bij kunnen dragen aan het oplossen van opsporingszaken!

[1]Bellingcat MH17 dossier: https://www.bellingcat.com/tag/mh17/

[2]Bellingcat Case Studies: https://www.bellingcat.com/category/resources/case-studies/

[3]BlueM blog: http://blue-m.nl/niet-iedereen-is-blij-met-de-bluem-hackathon-maar-wij-wel/

[4] TraceLabs: https://www.tracelabs.org/

[5]Europol 'Trace an Object': https://www.europol.europa.eu/stopchildabuse

[6]Operation Safe Escape (https://goaskrose.com/)

[7]BBC News: https://www.bbc.com/news/technology-42853072

[8]Council of Europe: https://go.coe.int/tEtbL

Over de auteur

frank.inklaar@capgemini.com

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.

Quantumcomputers: een forse inbreuk op vertrouwelijkheid

Zorg nu voor een gedegen aanpak om quantumcomputer-risico's te mitigeren

Auteurs
Ton Slewe
Koen van der Sanden

Quantumcomputers zijn een nieuw type computers die de wereld gaan veranderen. Hun ongeëvenaarde rekenkracht biedt allerlei nieuwe mogelijkheden.

Highlights

- Quantumcomputers kunnen bepaalde type berekeningen veel sneller uitvoeren dan de computers die we nu kennen.
- Deze rekenkracht kan ingezet worden om bepaalde type versleuteling te kraken.
- Voor gegevens die langdurig beschermd moeten worden, moeten nu al maatregelen genomen worden.
- Voer een impactanalyse uit om te bepalen welke maatregelen uw organisatie moet nemen.
- In dit artikel worden concrete maatregelen voorgesteld waarmee u goed voorbereid kunt zijn voor de opmars van quantumcomputers.

Quantumcomputers brengen vele nieuwe mogelijkheden met zich mee, van het ontwikkelen van nieuwe medicijnen tot het verkorten van reistijden in het openbaar vervoer. Net zoals vele vernieuwingen brengen quantumcomputers echter ook nieuwe risico's met zich mee. Hun gigantische rekenkracht kan ingezet worden voor criminele activiteiten, zoals het kraken van wachtwoorden of versleutelde gegevens.

Versleutelde gegevens vinden we overal. Als we in de winkel betalen met onze bankpas worden de gegevens van onze pas versleuteld naar de bank verstuurd. Om uw auto op afstand te openen wordt gebruikgemaakt van versleuteling zodat anderen niet ongehinderd uw auto kunnen stelen. Daarnaast hebben we een enorme hoeveelheid gegevens veilig opgeslagen op verschillende computers. Ongemerkt speelt versleuteling dus een grote rol in ieders dagelijks leven. Al deze versleutelde data en signalen zijn nu veilig, maar quantumcomputers gaan hier verandering in brengen[1].

Hoewel duidelijk is welke risico's quantumcomputers meebrengen voor versleutelde gegevens, is het vaak onduidelijk hoe organisaties met deze ontwikkeling om moeten gaan. De grote vraag is: wanneer moeten we als organisatie acteren op dit risico? Quantumtechnologie ontwikkelt zich snel. Grote organisaties zoals IBM, Microsoft, Google en Intel, maar ook universiteiten waaronder TU Delft en TU Eindhoven en veiligheidsdiensten investeren allemaal veel geld en menskracht in de ontwikkeling van quantumcomputers. Er wordt grondig onderzoek gedaan naar de mogelijkheden en de risico's die quantumcomputers met zich meebrengen voor versleuteling. Betekent het dat we moeten afwachten totdat al het onderzoek afgerond is voordat we actie kunnen ondernemen? Nee, zeker niet. Begin nu met een impactanalyse als eerste stap om de eigen kroonjuwelen te beschermen!

Welke factoren spelen een rol?

Er zijn vier belangrijke factoren die bepalen wanneer en welke acties ondernomen moeten worden om de impact van quantumcomputers op de beveiliging van 'kroonjuwelen' te verminderen.

1. Tijdstip tot quantumcomputers beschikbaar zijn

Het tijdstip waarop quantumcomputers beschikbaar komen die voldoende rekenkracht hebben om versleuteling te kraken. Dit tijdstip is nog moeilijk te bepalen, maar de ontwikkelingen van quantumcomputers gaan hard. NIST meldde in 2017[2] al dat binnen twee decennia quantumcomputers mogelijk de huidige cryptografische asymmetrische algoritmes kraken.

2. Implementatietijd

De tijd die nodig is om nieuwe cryptografische algoritmen te implementeren. Er vindt nu onderzoek plaats naar nieuwe quantumcomputerbestendige algoritmen. Het duurt nog wel even voordat deze algoritmen gestandaardiseerd en als producten beschikbaar zijn.

3. Beschermingstijd

De minimale periode dat de gegevens van de organisatie beschermd moeten zijn. Voor verschillende typen gegevens zal deze periode verschillend zijn. Medische gegevens moeten bijvoorbeeld veel langer beschermd worden dan de kortetermijnprijsstrategie van een retailbedrijf.

4. Locatie

De locatie waar de informatie zich bevindt en de eigenaar van de informatiesystemen waar de informatie is opgeslagen, denk hierbij aan gegevens binnen het eigen datacenter of in de publieke cloud. Hierbij hoort ook tussen welke fysieke locaties de informatie wordt uitgewisseld.

Welke stappen moeten organisaties ondernemen?

De factoren hierboven geven aan waar organisaties rekening mee moeten houden en geven verschillende sectoren een inzicht in wanneer zij moeten beginnen aan de transitie naar een post-quantum wereld. Uiteindelijk zullen alle organisaties soortgelijke maatregelen moeten treffen om de veiligheid van hun gegevens te waarborgen. Hoe moeten organisaties dit aanpakken? Het pad naar de post-quantum wereld is onder te verdelen in drie fases:

1. Voorbereiding

Op de korte termijn is het van belang dat organisaties zich bewust zijn van de komst van quantumcomputers en de risico's voor de organisatie. Organisaties zullen een impactanalyse moeten uitvoeren om goed voorbereid te zijn voor de opmars van quantumcomputers. Vanwege de vigerende privacywetgeving zijn veel processen en gegevens al in kaart gebracht en dat versnelt de voorbereiding.

Statische data	Data in transit
Op welk device is deze data opgeslagen?	Is de connectie versleuteld?
Heeft dit device een verbinding met de buitenwereld?	Op welke manier wordt de data versleuteld?
Wordt de data versleuteld opgeslagen?	Hoe wordt de cryptografische sleutel uitgewisseld?
Voor hoe lang wordt de data opgeslagen?	Is de connectie openbaar?
Met welk algoritme wordt de data versleuteld?	Via welke 'third party servers' verloopt deze connectie mogelijk?
Kan de data op dit device opnieuw versleuteld worden?	Kan iemand de data nu kopiëren en later ontsleutelen?

De impactanalyse zal alle datastromen binnen de organisatie moeten identificeren. Dit houdt in dat de bron van de data wordt opgezocht en het pad van de data vanaf die bron wordt gevolgd totdat deze wordt verwijderd of voor lange tijd wordt opgeslagen. Met name connecties vanuit de organisatie naar de buitenwereld zijn belangrijk om in kaart te brengen. Hierbij moet ook rekening worden gehouden met digitale handtekeningen en certificaten, aangezien deze een vorm van versleuteling omvatten. Voor het volgen van de data is het nuttig om een onderscheid te maken tussen data die op een device is opgeslagen (statische data) en data die wordt uitgewisseld tussen twee devices (data in transit). Voor deze twee typen data moeten verschillende factoren worden meegenomen in de impactanalyse.

Door voor iedere datastroom te analyseren om welke data het gaat en de bijbehorende vragen te beantwoorden, geeft de impactanalyse een duidelijk beeld van de weg naar een veilige post-quantumwereld. De impactanalyse geeft inzicht in de eerdergenoemde factoren: implementatietijd, beschermingstijd en locaties. Met een goed zicht op deze factoren is uw organisatie in staat om de juiste maatregelen op de juiste momenten te nemen.

2. Maatregelen die nu genomen kunnen worden

Uit de impactanalyse kan volgen dat u met gevoelige data met een zeer lange beschermingstijd werkt. Mocht dit het geval zijn dan kan uw organisatie direct een aantal maatregelen treffen om de veiligheid van de informatie te waarborgen. Vaak zullen dit maatregelen zijn met een korte implementatietijd. Het doel van deze maatregelen is niet om definitief beschermd te zijn, maar om de tijd tot quantumcomputers met voldoende rekenkracht te vergroten.

Het is in elk geval goed om het versleutelingsbeleid te herijken of, als dat er nog niet is, om het op te stellen. Als gegevens met symmetrische versleuteling worden uitgewisseld dan moet geverifieerd worden dat het algoritme en sleutellengte sterk genoeg zijn om bestand te zijn tegen quantumcomputers. Voor het gestandaardiseerde en veel gebruikte algoritme AES wordt een lengte van 256 bits aangeraden. Een dergelijke maatregel is relatief simpel te implementeren en zorgt ervoor dat uw gegevens langere tijd veilig zijn voor quantumcomputers.

Als informatie met een lange beschermingstijd versleuteld via het internet wordt uitgewisseld dan is het gebruikelijk om een geheime sleutel zelf asymmetrisch te versleutelen en te versturen. Quantumcomputers zijn uiterst efficiënt in het kraken van asymmetrische versleuteling en daarmee kunnen zij de sleutel achterhalen en de gegevens ontsleutelen. Door de sleuteluitwisseling op een andere wijze te doen, bijvoorbeeld door deze fysiek te transporteren met een smartcard, worden de gegevens beter beschermd.

Gelukkig zijn er vele kortetermijnmaatregelen die ervoor zorgen dat uw gegevens niet op straat belanden. Deze maatregelen zijn sterk situatie afhankelijk. Om erachter te komen of uw organisatie baat heeft bij dergelijke maatregelen en welke dat dan zijn, is het nodig om de impactanalyse uit te voeren.

3. Post-quantum maatregelen

Als post-quantumcryptografie beschikbaar is, kunnen organisaties overgaan op nieuwe oplossingen om hun data te beschermen. Dit zal in veel gevallen een aanzienlijke implementatietijd met zich meebrengen. Het lijkt nog een aantal jaren te duren voordat deze post-quantum algoritmes daadwerkelijk gestandaardiseerd zijn. NIST hoopt deze algoritmes aan te kondigen in 2024, maar kan dit versnellen als er doorbraken zijn op het gebied van quantumcomputers. Binnen Nederland is de TU Eindhoven betrokken bij de ontwikkeling van post-quantumcryptography[3].

Zodra NIST hun algoritmes aankondigt, kan een bijgewerkte impactanalyse inzicht geven op welke gebieden nog geen maatregelen genomen zijn en waar maatregelen wel gewenst zijn. De kortetermijnmaatregelen kunnen dan vervangen worden door een langetermijnbescherming tegen quantumcomputers. Dit kan in de vorm zijn van nieuwe quantumcomputer-bestendige algoritmes, maar ook de quantum-natuurkundige principes zelf kunnen voor een bescherming zorgen in de vorm van quantum key distrbution (QKD), waarbij speciale hardware wordt gebruikt om sleutels uit te wisselen.

Begrippenkader	
Symmetrische en asymmetrische versleuteling	Cryptografische algoritmen om data mee te versleutelen vallen uiteen in twee categorieën: symmetrische en asymmetrische algoritmen. Bij een symmetrisch algoritme beschikken beide partijen over dezelfde sleutel, die geschikt is om data zowel mee te versleutelen als te ontsleutelen. Bij een asymmetrisch algoritme heeft elke partij een sleutelpaar, dat bestaat uit een 'hangslot' (de publieke sleutel) en een geheime sleutel. Elke derde kan data versleutelen met het hangslot, maar alleen de partij zelf, die de bijbehorende geheime sleutel heeft, kan de data ook weer ontsleutelen. De meeste praktische toepassingen gebruiken zowel symmetrische als asymmetrische algoritmen: dit heet hybride encryptie.
Digitale handtekening	Met een digitale handtekening kan de juistheid van een bericht geverifieerd worden of een bericht onveranderd is en de identiteit van de persoon die het bericht heeft ondertekend.
Versleutelingsbeleid	Beleid waarin wordt vastgelegd welke typen encryptie met welke minimale sleutellengte voor welke periode zijn toegestaan. Naast versleuteling worden ook regels opgesteld voor digitale handtekeningen en hashing.
Post-quantum	Tijdperk nadat grote, stabiele quantumcomputers wijd beschikbaar zijn.

Conclusie

Quantumtechnologie is een disruptieve technologie die vele kansen en vele risico's met zich mee brengt. Hoewel quantumtechnologie nog onmiskenbaar in de kinderschoenen staat en vele toepassingen nog toekomstdromen zijn, is het noodzakelijk om quantumtechnologie mee te nemen voor langetermijnbeslissingen. Met name op het gebied van digitale veiligheid kunnen er al concrete stappen worden gezet om de risico's van quantumtechnologie te beperken. Het is nu tijd om te identificeren welke data opgeslagen is op welke plek, en om de huidige cryptografische algoritmes te herevalueren in combinatie met de beschermingstijd van de data. Het is nu tijd om een korte- en langetermijnstrategie te bepalen voor opkomende quantumtechnologie.

Het is nu tijd om ons klaar te maken voor de toekomst!

[1]Zie ook: 'Kwantum veegt de vloer aan met digitale veiligheid' uit Trends in Veiligheid 2019 (https://www.trendsinveiligheid.nl/rapport/2019-slimmer-samenwerken-aan-een-veiliger-nederland/)

[2]https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[3]https://pqcrypto.eu.org/

Over de auteurs

ton.slewe@capgemini.com

Ton Slewe MBA is principal consultant en adviseur bij Capgemini. Hij richt zich op cybersecurityvraagstukken bij publieke en private organisaties.

Ir. Koen van der Sanden was ten tijde van het schrijven van dit artikel Data Analist bij Capgemini. Hij houdt zich bezig met data-analyses en dataveiligheid. Vanuit zijn natuurkunde-achtergrond heeft hij zich toegespitst op de rol die quantumcomputers gaan spelen op het gebied van cybersecurity.

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.

Is de publieke cloud veilig genoeg voor gebruik in het veiligheidsdomein?

Is de weerstand om publieke clouddiensten in te zetten wel terecht?

Highlights

- Publieke cloud kan veilig gebruikt worden.
- Goedkoper dan een eigen omgeving.
- Neem voldoende maatregelen om gegevens veilig te houden.
- Veiligheid vereist verandering in gedrag.

Auteur
Jeroen Oosterwal

Door de Covid-19 uitbraak is er een enorme versnelling ontstaan in het thuiswerken. Tegelijkertijd zijn clouddiensten als Microsoft Teams in gebruik geëxplodeerd. Ook in het veiligheidsdomein is thuiswerken en video-vergaderen het nieuwe normaal geworden. Het gebruik hiervan brengt nieuwe vragen over de veiligheid met zich mee, zeker in beschermde omgevingen zoals die in het veiligheidsdomein gebruikt worden. Tegelijkertijd is dit de kans om serieus werk te maken van de publieke cloud in het veiligheidsdomein.

Vrijwel elke grote organisatie in Nederland maakt inmiddels gebruik van publieke clouddiensten. Dit varieert van het gebruik van Microsoft Office 365 tot het gebruik van business applicaties als Salesforce. Deze organisaties hebben een bewuste keuze gemaakt om delen van hun infrastructuur en applicaties op een andere manier te gebruiken. Dit biedt deze organisaties legio voordelen, zoals minder kosten en verhoging van de snelheid om te veranderen.

Een sector die weliswaar duidelijk achterloopt is het publieke veiligheidsdomein. Er heerst hier nog steeds angst voor de publieke cloud. Argumenten die je regelmatig hoort zijn; “het is niet veilig en ik heb geen controle over mijn gegevens meer”, “het mag niet van de wet” en vergelijkbare uitspraken. De laatste jaren is er echter een kentering te zien. Ook in het veiligheidsdomein moeten veel organisaties op de kosten letten en een uitgebreide on-premise ICT-omgeving is kostbaar. Bovendien komen er steeds meer diensten op de markt die speciaal ontworpen zijn voor het gebruik in het veiligheidsdomein. Daarnaast lezen we regelmatig berichten over de enorme kosten die de noodzakelijke ICT-vernieuwing met zich meebrengt bij de politie, het OM en de Rechtspraak[1]. Een manier om deze kosten te beperken en tegelijkertijd sneller te vernieuwen is meer gebruik te maken van publieke clouddiensten.

Reactief of proactief

Een kenmerk van het veiligheidsdomein is dat er vooral reactief wordt gewerkt. Als er ergens brand is wordt deze geblust, als er een woninginbraak is wordt er een politieauto op afgestuurd. Veel minder wordt er proactief gewerkt waarbij voorkomen wordt dat er brand ontstaat. Omdat het reactief werken in de haarvaten van deze organisaties zit, is dit ook zichtbaar in de ICT-organisatie. Het blijft moeilijk om vooruit te denken, een strategie te ontwikkelen voor de langere termijn en deze langetermijnstrategie ook te bewaken en uit te voeren. Het vergt lef en doorzettingsvermogen, maar ook cultuurverandering om dit voor elkaar te krijgen. Proactief denken en ernaar handelen zijn belangrijk om de gewenste en noodzakelijke versnelling door te voeren.

Rekkelijken en preciezen

Er is een strijd gaande tussen de preciezen die elke vorm van opslag en gebruik van data buiten de eigen organisatie afwijzen en de rekkelijken die, onder voorwaarden, het gebruik van de publieke cloud omarmen. Wie gaat deze strijd winnen en welke argumenten zijn er voor en tegen het gebruik van de publieke cloud?

Waarom niet?

Laten we eens op een rijtje zetten welke argumenten er tegen het gebruik van publieke clouddiensten zijn. Het eerste en ook belangrijkste argument is privacy. Veel organisaties verwerken privacygevoelige gegevens en zijn er niet van overtuigd dat deze gegevens veilig zijn als ze buiten de deur worden opgeslagen. Men is bang dat een cloud-leverancier deze gegevens kan inzien, of erger nog, deze gegevens kan misbruiken of kan verliezen.

Een tweede argument dat ik hier wil noemen is de wet- en regelgeving. De Wpg, AVG en Archiefwet zijn hierbij leidend. In deze wetten wordt geregeld hoe een organisatie om moet gaan met de informatie die tot haar beschikking staat. Zo moet bijvoorbeeld de verwerkingsverantwoordelijke altijd een risico-analyse doen en adequate maatregelen nemen om de risico’s te mitigeren.

Waarom wel?

Welke argumenten zijn er voor het gebruik van publieke cloudiensten? Een belangrijk argument om meer gebruik te maken van publieke clouddiensten zijn de kosten. Het opslaan en verwerken van data kan door een cloud-leverancier voor een fractie van de kosten gedaan worden door zijn schaalgrootte en

efficiënte inrichting. Het inrichten, onderhouden en beheren van een eigen netwerk, servers, opslag, applicaties en dergelijke is een kostbare aangelegenheid en is nauwelijks een core business te noemen voor de meeste organisaties in dit domein.

Een ander argument om delen van de informatievoorziening uit te besteden naar de publieke cloud is het beheer. Het is voor de veiligheidssector heel lastig om adequaat beheer op de applicaties en data te doen. Het ontbreekt aan voldoende kennis en vacatures zijn moeilijk in te vullen.

Een laatste argument is veiligheid. Publieke cloud-leveranciers hebben hun omgevingen op een zeer hoog beveiligingsniveau ingericht en doen er alles aan om dit ook zo veilig mogelijk te houden. Zij voldoen aan internationale standaarden en tonen dit ook aan door middel van audits op de omgeving. Dit in tegenstelling tot sommige organisaties in het veiligheidsdomein die worstelen met het veilig houden van hun verouderde omgevingen.

Hoe kan het veilig?

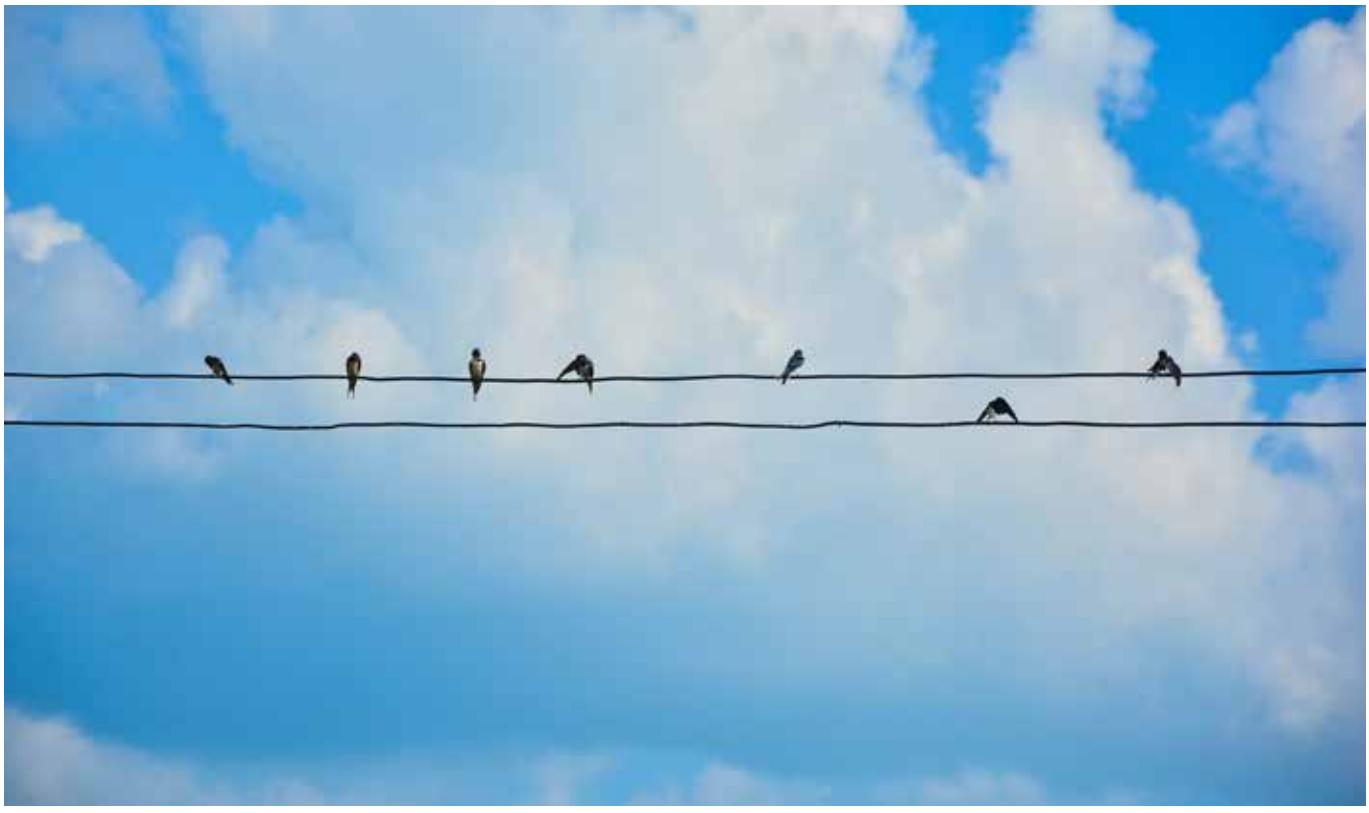
De publieke cloud kan veilig gebruikt worden als er voldaan wordt aan een aantal voorwaarden. Als eerste moet je als organisatie het 'zero trust' model omarmen waarbij je er vanuit gaat dat de infrastructuur gecompromitteerd is. Dit betekent in de praktijk dat 'security by design' meer is dan alleen PowerPointpresentaties, het moet overal in terugkomen. Dit vergt een andere manier van denken en handelen. Ook hier heeft het veiligheidsdomein last van haar verleden. Het is niet meer voldoende om een gewapende bewaker voor de deur te zetten en dan te denken dat je veilig bent. Nee, je zult moeten investeren in een identity & data-driven security-aanpak waarbij je uitgaat van één identiteit en op basis van rollen, attributen en condities die wel of geen toegang biedt tot data en applicaties. Microsegmentering en virtualisatie van de netwerken is hierbij essentieel. Dit om te voorkomen dat aanvallers andere delen van de infrastructuur kunnen bereiken.

Cloudstrategie

Elke organisatie in het veiligheidsdomein moet een cloudstrategie ontwikkelen. Met een goede strategie bereik je meerdere doelen die er gezamenlijk voor zorgen dat je als organisatie beter en sneller kan innoveren tegen lagere kosten.

Elke strategie begint bij het goed begrijpen van de strategische doelstellingen. Hoe sluit de visie op de cloud aan bij de bedrijfsdoelstellingen? Hoe gaat het gebruik van de cloud bijdragen aan het doel van de organisatie? Structureer en prioriteer de te bereiken doelen en breng de risico's en uitdagingen in kaart.

Een volgende stap is het beoordelen van de impact op de organisatie. Dit start met het goed in beeld hebben van het bestaande applicatielandschap, infrastructuur en van de operationele praktijk. Zorg voor een goede business case. Breng in kaart wat de huidige kosten en de baten zijn en maak een inschatting van het toekomstige gebruik waarbij 'pay as you go' modellen een grote rol spelen om de kosten te beperken.



Een heel belangrijke stap is het doen van een 'Cloud Ready Assessment'. Het is essentieel om goed in kaart te brengen op welk niveau van readiness de organisatie staat en wat er moet gebeuren om veilig publieke clouddiensten te gaan gebruiken.

Het gaan gebruiken van de (publieke) cloud is een digitale transformatie. Bij elke transformatie hoort sterk leiderschap en een vooruitziende blik op het vlak van de organisatie en van de technologische ontwikkelingen. Het is hierbij essentieel dat CIO's en ICT-directeuren een team om zich heen hebben of organiseren dat enthousiast is over het vooruitzicht op veranderingen. Het betrekken van strategische partners is hierbij noodzakelijk om de organisatie zo te positioneren dat deze klaar is voor de toekomst.

Cloud security

De traditionele ICT-wereld kende andere beveiligingsrisico's dan nu. In een cloud-omgeving gelden andere eisen en risico's. IT-architecten gebruiken vaak en graag de analogie van een huis. Als het om cloud-beveiliging gaat dan kun je zeggen dat het gaat om de bescherming van alle spullen in het huis en minder van het huis zelf. En als je vervolgens kijkt naar alle spullen in het huis zijn er zaken die beter beschermd moeten worden dan andere. Unieke foto's of kunstwerken wil je beter beveiligen dan de standaard inboedel. Kortom wat zijn de kroonjuwelen en welke risico's loop ik als het fout gaat? Verlies ik data? Kan ik die terughalen? Wat zijn de risico's als de data op straat ligt?

Er is helaas geen 'one size fits all' optie als het gaat om cloud-beveiliging. Datalekken kunnen op vele manieren ontstaan en elk van die manieren moet worden bekeken. 'Voorkomen is beter dan genezen' geldt ook hier. Anticipeer op de mogelijkheden en maak hierop beleid.

Technische maatregelen

Om data in de cloud te beveiligen is het noodzakelijk om op verschillende niveaus maatregelen te nemen. Zorg als eerst voor een goede oplossing tegen het lekken van data (Data Leakage Prevention, DLP). Veel softwaresuites bieden hiervoor oplossingen. Microsoft Office 365 kan bijvoorbeeld standaard al controleren op meer dan 80 veel voorkomende vertrouwelijke gegevens op financieel, medisch en persoonlijk gebied en aan de hand van regels de gegevens automatisch classificeren en voorzien van een label. Op die manier is het mogelijk om gevoelige data standaard te vercijferen of in sommige gevallen zelfs niet toe te staan dat deze data in de cloud wordt opgeslagen.

Je kunt ook nog een stap verder gaan door alle data die je in de cloud opslaat standaard te vercijferen. Dit kan met een eigen sleutel waardoor ook de cloud-leverancier nooit jouw data kan inzien. Onderdeel van het 'zero trust' model is multifactor-authenticatie wat een betrouwbare en laagdrempelige manier is om in te loggen. Hiermee voorkom je datalekken zonder de medewerkers te veel te belasten.

Toekomst

Het gaat razendsnel met de ontwikkelingen in de cloud. Elke dag komen er nieuwe oplossingen en applicaties beschikbaar. De grote cloud-leveranciers bieden complete DevOps-omgevingen aan waarmee ontwikkelaars snel oplossingen kunnen realiseren. De cloud biedt ondersteuning bij het gebruik van IoT, Big Data en AI-toepassingen. Ook het inzetten van virtuele desktops in de cloud is een relatief nieuwe ontwikkeling waarmee je overal je eigen werkplek tot je beschikking hebt.

Conclusie

Het veiligheidsdomein moet zo snel mogelijk naar de publieke cloud. Dit levert niet alleen kosten- en efficiencyvoordelen op, het versnelt de ontwikkeling van nieuwe functionaliteiten en helpt de organisaties in dit domein veiliger en beter hun werk te doen. Net als bij het gebruik van een eigen infrastructuur moet rekening worden gehouden met de gevoeligheid van de data en moeten adequate maatregelen genomen worden op technisch en organisatorisch vlak. Onder het motto 'never waste a good crisis' moet er nu doorgepakt worden om snel, goed en veilig publieke clouddiensten in te richten en te gaan gebruiken.

[1]Onder andere: https://www.computable.nl/artikel/nieuws/overheid/6851804/250449/bit-politie-stop-met-bouw-eigen-it-platform.html

Over de auteur

jeroen.oosterwal@capgemini.com

Ing. Jeroen Oosterwal is Principal Consultant bij Capgemini. Jeroen is werkzaam als Enterprise Architect bij de marktgroep Openbare Orde en Veiligheid.

Van cybersheriff tot regionale kunstmatige intelligentie

Wat betekent decentrale weerbaarheid voor Nederland?

Highlights

- Digitale weerbaarheid en decentralisatie vereist burgerpaticipatie en ondersteuning.
- Er zijn veel innovaties die gebruikt kunnen worden in het belang van digitale weerbaarheid, maar we moeten niet vergeten waarvoor deze veiligheid dient.
- De Digiwacht zijn vrijwilligers die de lokale digitale weerbaarheid waarborgen.
- Een gemeentelijke cybersheriff, door de burgers verkozen om hun digitale weerbaarheid te garanderen.
- Landelijke kunstmatige intelligentie om digitaal Nederland te beschermen, getraind door heel Nederland.

Auteur
Sebastiaan de Vries

Voormalig minister van Economische zaken, Henk G.J. Kamp stelde het al in 2017; digitalisering is een motor voor economische groei[1,3] welke gepaard gaat met kansen en risico's. Door de toenemende digitalisering van Nederland is er een significante toename in digitale dreigingen. Deze digitale dreigingen zijn één van de grootste risico's voor de nationale veiligheid in zowel impact als waarschijnlijkheid[1,2]. Digitale dreigingen, die zowel economische, fysieke en sociaal maatschappelijke gevolgen kunnen hebben, leiden tot maatschappelijke ontwrichting [2,3]. Het volledig benutten van de kansen van digitalisering kan alleen als de digitale weerbaarheid op orde is.

Weerbaarheid tegen digitale dreigingen, zogenoemde digitale weerbaarheid, is een randvoorwaarde en blijft een prioriteit. Zonder digitale weerbaarheid zijn de risico's van digitalisering simpelweg te groot. Hierin speelt decentrale weerbaarheid een belangrijk rol.

Wat is decentrale weerbaarheid?

Wat met decentrale weerbaarheid bedoeld wordt is niet dat elke gemeente, veiligheidsregio, provincie en private organisatie zijn eigen silo gaat vormen. Waar ik voor pleit is de decentralisatie van de autoriteit om invulling te geven aan digitale weerbaarheid. Wanneer de zwakste schakel de keten kan breken, is het dan niet logisch dat elke schakel zichzelf moet versterken?

Dit moet verder gaan dan de gemeente die bijvoorbeeld enkel een nieuwe informatie-beveiligingsfunctionaris aanneemt of de veiligheidsregio's die plannen maken voor cybercrises. De autoriteit moet bij de burger komen. Dezelfde burgers die volop van de kansen genieten, maar ook de risico's lopen en de rekening betalen als het fout gaat. Dezelfde burgers die tijdens de Corona- crisis hebben laten zien prima zelfstandig met oplossingen te kunnen komen wanneer de situatie daar om vraagt.

Welke uitdagingen hebben we vandaag?

De Nederlandse digitale weerbaarheid is, in vergelijking met andere landen, al behoorlijk goed op orde. Zo heeft de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) afgelopen jaar een cyberaanval van de Russische geheime dienst op de Organisatie voor het Verbod op Chemische Wapens (OPCW) in Den Haag verijdeld[4]. Daarnaast zien wij binnen Capgemini onze klanten een steeds hogere prioriteit geven aan digitale weerbaarheid, zowel met als zonder onze hulp.

Helaas zagen we afgelopen jaar ook voorbeelden waar we kwetsbaar zijn als Nederland en waar de digitale weerbaarheid voor verbetering vatbaar is. Zo zagen we het fout gaan met de 112-storing, waardoor het noodnummer tijdelijk onbereikbaar was en drie terugvalsystemen het lieten afweten[5]. We zagen de universiteit van Maastricht getroffen worden door ransomware waar zelfs na het betalen van bijna € 200.000, - losgeld de systemen niet volledig hersteld waren[6]. Om nog maar te zwijgen over onderzoeksgegevens die voor onbevoegden mogelijk toegankelijk waren of verloren zijn gegaan.

Binnen ons Capgemini Security Operations Centers netwerk zagen wij tijdens de Corona-crisis hoe cybercriminelen maar al te graag misbruik maken van de angst rond een crisissituatie. Zo zagen wij phishing-aanvallen stijgen met meer dan 700%. Hier wordt verwacht dat de totale impact nog op zich laat wachten tot iedereen weer op kantoor zit.

Daar bovenop is het aantal bedrijven dat melding heeft gemaakt van cyberincidenten gestegen van 45% naar 61% ten opzichte van 2018[7]. Dit heeft flinke economische schade veroorzaakt. Deze stijging zou veroorzaakt worden door cybercriminelen die gebruikmaken van steeds geavanceerdere technieken[8]. Met deze geavanceerde technieken lijken criminele en statelijke actoren steeds meer succes te hebben. Dus waar moeten we beginnen? De digitale weerbaarheid binnen Nederland kan centraal door de overheid geregeld worden, of decentraal met meer nadruk op de lokale belangen.

Decentralisatie van de digitale weerbaarheid als oplossing

Er zijn veel manieren om de digitale weerbaarheid te verbeteren, maar ik denk dat decentralisatie voor Nederland de volgende stap moet zijn. Gelukkig staat dit al hoog op de Nederlandse cybersecurity-agenda[9].

De reden dat decentralisatie zo van belang is, heeft te maken met de eerdergenoemde geavanceerdere technieken. Veel van deze technieken werken omdat ze zich niet op computers of applicaties richten maar op gebruikers, gebruikers die niet gecentraliseerd in Nederland wonen. Gebruikers met diverse normen en waarden. Zo vinden sommige mensen dat informatie voor iedereen toegankelijk moet zijn terwijl andere vinden dan informatie gereguleerd moet worden.

> Om te voorkomen dat Nederland achterblijft op de groeiende digitale dreiging is het cruciaal dat overheden en private organisaties op decentraal niveau beseffen dat we moeten investeren in cyberveiligheid en zélf de verantwoordelijkheid pakken bij het adequaat beschermen van onze belangen."
>
> **Luuk Stadhouders**
> **waarnemend Chief Information Security Officer (CISO), Gemeente Rotterdam**

Het is de diversiteit in normen en waarden die misbruikt wordt bij deze geavanceerde aanvallen. Dit soort aanvallen hebben al plaatsgevonden in Amerika in de vorm van desinformatiecampagnes. Deze desinformatiecampagnes speelden in op specifieke doelgroepen die geïdentificeerd konden worden door middel van social mediagedrag. Hiermee hebben Russische hackersgroepen invloed uitgeoefend op de Amerikaanse verkiezingen in 2016 door de bevolking te misleiden[10]. Ik ben ervan overtuigd dat de oplossing voor dit soort problemen het makkelijkst te vinden zijn door gebruikers zelf. En dat is de essentie van mijn visie op decentrale weerbaarheid.

Hoe werkt dat, decentrale weerbaarheid?

Om effectieve decentrale weerbaarheid te ontwikkelen hebben we twee dingen nodig; decentralisatie en participatie. Dan volgt verbetering van de digitale weerbaarheid vanzelf. Als ik naar een klant ga, vraag ik ook aan hen welke digitale systemen of informatie van belang zijn. Dit is namelijk niet iets dat een ander voor je kan bepalen, natuurlijk kan ik hierbij helpen maar het blijven jouw normen en waarden die ondersteund worden met digitale middelen.

Dit werkt ook de andere kant op. Als je jouw normen en waarden niet met mij wilt delen, kan ik je niet adequaat helpen. Dit brengt ons bij het belang van burgerparticipatie. Als we van de burger niet weten wat beschermd moet worden, maakt het ook niet uit of de autoriteit gedecentraliseerd is. Deze vorm van burgerparticipatie zal ook helpen in tijden van crisis, zoals we met het coronavirus hebben gezien. Cybercriminelen zullen altijd een crisis proberen te misbruiken voor eigen gewin. Wanneer burgers actief betrokken zijn bij de bescherming zullen zij hier ook minder kwetsbaar voor zijn.

Concrete toepassingen van decentrale weerbaarheid

Decentralisatie van autoriteit in combinatie met burgerparticipatie is geen nieuw idee binnen het veiligheidsdomein. Zo bestaan er historische en futuristische voorbeelden die de meeste mensen wel zullen kennen.

1. Historisch kunnen we terugdenken aan onze 16e-eeuwse burgerwachten (waar onder 'de Nachtwacht'), die als samengestelde groep gewone burgers de openbare orde en veiligheid handhaafde.
2. Iets recenter in de vroege 19e eeuw zagen we in Amerika hoe burgers een lokale sheriff verkozen om hen te beschermen.
3. Wie graag science fictions films kijkt, is natuurlijk bekend met de concepten van kunstmatig intelligente computers die van de mensen moeten leren wat goed en slecht is.

Met deze voorbeelden in gedachten heb ik een drietal voorstellen hoe we in Nederland onze decentrale weerbaarheid kunnen inrichten.

Oplossing 1:
De Digiwacht

Een oplossing geïnspireerd op de Nederlandse geschiedenis, de Digiwacht. Net als met de 16e -eeuwse burgerwachten leggen wij de digitale weerbaarheid van Nederland bij vrijwilligers. Deze vrijwilligers zullen de digitale weerbaarheid van hun stad waarborgen. Naar eigen inzicht, met participatie van hun medeburgers, beveiligen zij het digitale landschap van hun stad.

Deze beveiliging kan de vorm hebben van firewalls, DNS-monitoring, aansluiting op een DDOS-wasstraat of andere oplossingen die de Digiwacht noodzakelijk acht. Zo zou elke Digiwacht zijn eigen Security Operations Center (SOC) bemannen. Dit SOC kan de stad weerbaar maken door in te grijpen op zowel grote- als kleine cyberincidenten.

Wel moet overwogen worden hoe de rest van de stad hier inspraak over krijgt. Niet iedereen zal de vaardigheden of tijd hebben om vrijwilliger te worden bij de Digiwacht. Deze mensen mogen niet de dupe worden van een kleine groep technische elite.

Oplossing 2:
Een gemeentelijke cybersheriff

Om burgerparticipatie te vergemakkelijken is het zinvol aan te sluiten op de al bestaande logische indeling in Nederland. Dit kunnen we realiseren door het Nederlandse digitale landschap te segmenteren op basis van gemeentes.

Hierdoor kunnen de gemeentes samen met burgers en ondernemers hun eigen digitale weerbaarheid organiseren. Om het gebrek aan kennis te overbruggen zal er een specialist aangesteld moeten worden, iemand die kennis heeft van het domein van cybercrime en cybersecurity en ervaring heeft met het implementeren en onderhouden daarvan: de cybersheriff.

Met wat inspiratie uit het wilde westen is mijn voorstel als volgt, tijdens de gemeenteraadsverkiezing wordt ook een cybersheriff verkozen. Dit is een combinatie tussen een Chief Information Security Officer (CISO) en een Chief Digital Officer (CDO) voor de gemeente. Hierdoor heeft de regio in de hand welke belangen de meest maatschappelijke waarde hebben. In combinatie met de groeiende digitale bekwaamheid is de Nederlandse bevolking steeds beter in staat mee te praten over hun digitale weerbaarheid en daarover haar stem te uiten.

Oplossing 3:
Regionale kunstmatige intelligentie

Decentralisatie van de digitale weerbaarheid kan ook door middel van regionale initiatieven in combinatie met burgerparticipatie. Zo ook een oplossing met wat meer futuristische ondertonen, het bouwen van een regionaal overkoepelend digitaal monitorings- en preventiesysteem. Een systeem dat direct digitale aanvallen in Nederland vroegtijdig kan signaleren en erop kan reageren. Een systeem dat beheerd wordt door een kunstmatige intelligentie.

Door een geavanceerde artificiële intelligentie (AI) de leiding te geven over de digitale weerbaarheid kan snel, effectief en geautomatiseerd worden gereageerd op aanvallen van cybercriminelen. De voorwaarde is wel dat we vooraf goed weten wat de normen en waarden zijn, welke systemen en welke informatie beschermd moeten worden. Daarnaast zullen de juiste technologieën geïmplementeerd moeten worden. Zo zal het nodig zijn om de AI te voeden met de juiste informatie. Denk aan zaken zoals netwerkverkeer, gebruikerspatronen, aanvalspatronen en het gedrag van individuele computers.

De burger kan zijn stem laten horen door bij te dragen aan het trainen van de AI. Hierdoor wordt het systeem blootgesteld aan alle normen en waarden in de regio en zal hiernaar handelen. De technische aspecten hiervan zijn veel complexer van aard dan ik hier beschrijf maar zeker niet onmogelijk.

Waar te beginnen?

Verdere digitalisering laat niet op zich wachten: 5G, zelfrijdende auto's en persoonlijke robots zijn er al. Deze innovaties maken ons leven aangenamer, maar we kunnen de gevaren van misbruik door kwaadwillenden niet negeren.

De voorgestelde toepassingen zijn niet makkelijk te verwezenlijken, en bevatten zowel voor- als nadelen. Zo kunnen sommige maatregelingen niet uitsluitend op regionaal niveau genomen worden. Verder is het onvoldoende om alleen de regionale weerbaarheid te versterken, net als dat het voor een organisatie onvoldoende is alleen hun eigen infrastructuur te beschermen. Er zal een manier nodig zijn om incidenten met landelijke impact gezamenlijk af te handelen. Dit wordt bemoeilijkt als elke gemeente, provincie of private organisatie zijn eigen unieke infrastructuur en methodologieën heeft.

Deze uitdagingen maakt het niet minder belangrijk dat we over de voordelen van decentrale weerbaarheid nadenken. Ik ben ervan overtuigd dat decentrale weerbaarheid, in welke vorm dan ook, zal leiden tot een betere digitale weerbaarheid van heel Nederland. We hoeven niet nu te beslissen dat we het morgen allemaal anders doen. Onze veiligheid is al erg sterk en we hebben ruimte om na te denken. Maar als de digitale weerbaarheid niet meegaat met de digitalisering worden we ingehaald door toenemende dreigingen.

Daarom het volgende voorstel: kijk naar je persoonlijke digitale middelen - je smartphone, je applicaties, je laptop en in sommige gevallen zelfs je wasmachine - en sta eens stil bij de vraag of jouw belangen wel beschermd zijn. Wanneer iedereen, particulieren en organisaties, deze vraag met "ja" kan beantwoorden, kunnen we volop gebruik maken van de voordelen die de digitalisering met zich mee brengt.

Over de auteur

sebastiaan.de.vries@capgemini.com

Sebastiaan de Vries is werkzaam bij Capgemini Cybersecurity als Incident Response Expert. Hij werkt vanuit de filosofie dat de technische oplossingen zonder menselijke factor geen oplossingen zijn.

Met dank aan Luuk Stadhouders, waarnemend CISO Gemeente Rotterdam, voor zijn bijdragen het opstellen van dit artikel.

[1]https://zoek.officielebekendmakingen.nl/kst-26643-463.html
[2]nationale veiligheid strategie 2019
[3]https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen
[4]https://www.telegraaf.nl/nieuws/2636194/nederland-betrapt-vier-russische-spionnen
[5]https://www.nu.nl/tech/5989750/wrr-nederland-is-niet-goed-voorbereid-op-grootschalige-cyberaanvallen.html
[6]https://nltimes.nl/2020/01/24/maastricht-univ-paid-eu250k-ransomware-hackers-report
[7]https://beveiligingnieuws.nl/nieuws/cyberincidenten-nederland-kosten-gemiddeld-3-ton
[8]https://cybersecurity-expert.com/wp-content/uploads/2017/05/ISA-lanceert-Cybersecurity-expertprogramma-LR.pdf
[9]https://www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig
[10]https://www.volkskrant.nl/wetenschap/zo-zagen-de-russische-advertenties-op-facebook-tijdens-de-amerikaanse-verkiezingen-eruit~b06c6cdc/

Het Landelijke Meldpunt Internet Oplichting als instrument in de strijd tegen veranderde criminaliteit

Hoe faciliteert het LMIO de aanpak van veel voorkomende cybercriminaliteit?

Auteurs
Erik Hoorweg
Martine Middelveld
Jolien van Aar

Online handelsfraude heeft de traditionele fietsendiefstal van de troon verstoten. Hoe pak je dat aan? Het Landelijk Meldpunt Internet Oplichting (LMIO) geeft antwoorden.

Highlights

- Online handelsfraude is een veel voorkomend probleem en blijft toenemen.
- Zonder centrale analyse staat de politie met lege handen in de aanpak van dit probleem.
- Het Landelijk Meldpunt Internet Oplichting (LMIO) is een publiek-private samenwerking die de online handelsfraude gecentraliseerd aanpakt.
- Het LMIO is de motor/aanjager voor de eenheden in het oppakken van deze zaken.
- Door steeds te experimenteren met nieuwe werkwijzen ontwikkelt het LMIO naar een vernieuwde en verbeterde versie van zichzelf.

Criminaliteit in Nederland is na jarenlange daling vorig jaar voor het eerst gestegen naar 800.000 misdrijven, een stijging van 4 procentpunt[1]. Alles wijst erop dat deze trendbreuk wordt veroorzaakt door een verschuiving naar de digitale criminaliteit. Online handelsfraude heeft de traditionele fietsendiefstal van de troon verstoten. Uit de jaarcijfers van de politie blijkt bijvoorbeeld dat in 2019, 57.915 meldingen zijn gedaan van online handelsfraude[2]. Een toename van ruim 30 procentpunt ten opzichte van 2018 (toen 44.399 meldingen). Het gaat om een schadebedrag van bijna 15 miljoen euro. De veel voorkomende cybercriminaliteit moet worden aangepakt. Zoals Erik Akerboom in 2017 al in CSR Magazine schreef: "Nederland moet onveiliger worden voor criminelen, óók in de digitale wereld". Maar de aanpak van de veel voorkomende cybercriminaliteit is lastig. Hoewel de specialistische kennis op het gebied van cybercriminaliteit aanwezig is bij de landelijke eenheid (Team Hightech Crime) en bij de regionale eenheden (de cyberteams), wordt vrijwel alleen ingezet op de grotere, complexere zaken. Terwijl het gros van de meldingen 'simpele' marktplaatsfraude betreft. Hoe de politie zich kan organiseren op het gebied van veel voorkomende cybercriminaliteit wordt momenteel mee geëxperimenteerd.

Een casus

Een gezin met vier kinderen wil in de herfstvakantie graag naar Disneyland. Op Marktplaats zien zij kaarten staan voor een gereduceerd tarief. De marktplaatsverkoper heeft al 11 jaar een account en een goed verhaal over waarom de kaarten beschikbaar zijn gekomen. Na enig contact en onderhandeling zijn ze tot een akkoord gekomen. De verkoper geeft aan dat hij de kaarten zal opsturen op het moment dat hij de betaling heeft ontvangen, en geeft daarbij ook aan geen goede ervaringen te hebben met de betaalmogelijkheid via Marktplaats. Het gezin maakt het geld over maar ontvangt de toegangsbewijzen niet. Vanaf het moment van betalen is de verkopende partij niet meer te bereiken. Via een vriendin proberen ze uit of de verkopende partij wel opneemt als er een nieuwe klant komt. Dat blijkt het geval. Nu zijn ze er zeker van: ze zijn opgelicht. Een gevoel van boosheid overheerst, maar er is ook veel schaamte. Dit hadden ze wellicht kunnen zien aankomen…

Wie pakt het op?

De melding van dit gezin zou bij de politie niet de prioriteit krijgen. De melding behelst een schadebedrag van 'slechts' 150 euro, wat voorkomen had kunnen worden door gebruik te maken van de betalingsregeling. De enige opsporingsindicatie is het rekeningnummer waarvoor de politie een vordering zou moeten doen bij de bank. Maar welke bewijslast van oplichting is er eigenlijk? Deze ene melding in deze eenheid maakt nog niet dat de verkopende partij willens en wetens mensen oplicht. Terwijl hij mogelijk wel door het hele land slachtoffers maakt.

Landelijk Meldpunt Internet Oplichting (LMIO)

Een belangrijk instrument in de aanpak van veel voorkomende cybercriminaliteit is het Landelijk Meldpunt Internet Oplichting (LMIO). In 2010 hebben de politie, het OM en Marktplaats het LMIO opgericht. Later sloten bij de samenwerking ook de banken, Betaalvereniging en de Autoriteit Consument en Markt aan. Dit publiek-privaat samenwerkingsverband (PPS) heeft als doel om de bestrijding en aanpak van online handelsfraude te coördineren en daarmee efficiënt en effectief te maken. Het LMIO is begonnen als proeftuin waarin werd geëxperimenteerd met een meldpunt voor slachtoffers van aan- en verkoopfraude. In het PPS zijn afspraken gemaakt over te treffen repressieve en preventieve maatregelen, adequate voorlichting en snelle gegevensuitwisseling in gevallen van fraude.

Bij het LMIO worden landelijk bij benadering 160 meldingen per dag gedaan van internetoplichting, bijna allemaal (92%) via de website van de politie. De meldingen komen vervolgens terecht bij de landelijke eenheid van de politie en bij het LMIO voor de intake, analyse en veredeling van informatie. Een deel van de informatie uit die meldingen wordt direct doorgezet naar de partners, zodat zij direct benodigde acties tegen de rekeninghouder en/of accounthouder kunnen opstarten, zoals het blokkeren van de rekening of het loskoppelen van frauduleuze webwinkels. Belangrijk aspect van gegevensdeling is het voorkomen van fraude door te frustreren, blokkeren en barrières op te werpen. Onderdeel hiervan is ook de creatie van de checkfunctie op politie.nl waarbij de consument de mogelijkheid heeft om, voor dat hij tot een aankoop overgaat, te controleren of er al eerder meldingen zijn gedaan tegen een 'wederpartij'. Deze controle blijkt zeer succesvol te zijn gezien het feit dat er circa 160.000 views per maand zijn.

Door het centraliseren van intake, analyse en veredeling bij het LMIO, wordt informatie bij elkaar gebracht en voorkomen dat taken dubbel of ongestructureerd worden uitgevoerd. Hierdoor wordt capaciteit in de regionale eenheden bespaard. De activiteiten binnen het LMIO resulteren bijvoorbeeld in een lijst van rekeninghouders waar minimaal drie meldingen over zijn binnengekomen: de oplichters/katvangerslijst. Deze lijst verspreiden zij weer over de regionale eenheden zodat ieder basisteam de betreffende rekeninghouder uit zijn wijk kan opsporen. Het is aan de regionale eenheden om de zaken op te pakken voor vervolging.

De uitdaging

De grote uitdaging ligt echter in het regionaal oppakken van de zaken voor vervolging. De opsporingscapaciteit en de strafrechtketen staan onder druk. Voor een capaciteit- en tijdrovend strafrechtelijk proces wordt in het stuur- en weegproces vaak prioriteit gegeven aan andere, grotere zaken: van de 33.000 meldingen die opgepakt zouden kunnen worden, worden er zo'n 5.000 daadwerkelijk opgepakt. De zaken van online handelsfraude zijn immers klein (het gemiddelde schadebedrag in 2019 was 250 euro) en het slachtofferschap is niet dringend (men is niet in onveilige situaties terecht gekomen). Omdat de zaken nu nog initieel bij het landelijk meldpunt terecht komen, en niet bij de regionale eenheden, worden regionale eenheden niet gestimuleerd om de zaken op te pakken. Zij voelen geen eigenaarschap over de meldingen. Zaken blijven hierdoor liggen en dit leidt onder andere tot onbegrip van burgers.

Hoe verder?

Het LMIO gaat op korte termijn vernieuwen en verbeteren via een combinatie van een lokale en landelijke aanpak. In deze nieuwe vorm van het LMIO komen de meldingen van internetoplichting nog steeds binnen bij het landelijk meldpunt maar óók bij de regionale eenheden waar de verdachte woont. Dit bevordert de aanknopingspunten voor de opvolging omdat verdachten in het hele land (en daarbuiten) slachtoffers kunnen maken. De voordelen van deze aanpak zijn tweevoudig: De eenheden worden gestimuleerd de meldingen op te pakken en het LMIO krijgt door het wegvallen van de coördinatie van meldingen meer tijd en capaciteit voor de analyse van de grotere netwerken, projectvoorbereiding en de vernieuwing van het huidige samenwerkingsverband.

In de tussentijd

Om de regionale eenheden te ondersteunen bij een efficiënte en effectieve opvolging van meldingen heeft het LMIO geëxperimenteerd met twee alternatieve afdoeningen: het stopgesprek en de buitengerechtelijke afdoening. Deze zijn ontstaan in basisteams die aan de slag zijn gegaan met de oplichterslijsten. Deze uitvoeringspraktijken geven handelingsperspectief aan enerzijds de wens om de vele meldingen die binnenkomen op te pakken, en anderzijds de schaarste in de capaciteit van de opsporing en vervolgingsketen maar waarbij tóch sprake is van een 'betekenisvolle' afhandeling.

Het stopgesprek is een alternatieve afdoening waarin een civielrechtelijke procedure wordt voorgesteld: verdachte betaalt de schade zelf terug aan zijn/haar slachtoffer(s). Wanneer de schade is terugbetaald, zullen de meldingen ingetrokken worden. Op deze manier wordt geen justitiële documentatie opgesteld. Bij de buitengerechtelijke afdoening wordt er wel justitiële documentatie opgemaakt. Er wordt een kort dossier opgesteld en na ondertekening van de verdachte zal het Centraal Justitieel Incassobureau (CJIB) het schadebedrag bij de verdachte innen. Vervolgens draagt het CJIB zorg voor de terugbetaling aan slachtoffers. Beide alternatieve afdoeningen dragen, zonder dat het een grote belasting is voor de opsporing en vervolgingsketen, bij aan de primaire wens van slachtoffers: het schadeloosstellen. Vanuit het LMIO worden beide uitvoeringspraktijken geëvalueerd (wat zijn succesfactoren), zodat ook hierop doorontwikkeld kan worden.

Conclusie

Het reeds behaalde succes van LMIO komt voor een groot deel door de publiek-private samenwerking. Daarnaast zijn 'vernieuwen' en 'verbeteren' onder meer door het uitvoeren van pilots en evaluaties de codewoorden van het LMIO. Op korte termijn wordt onder andere ingezet op het verbeteren van het LMIO via een combinatie van een lokale en landelijke aanpak. De veel voorkomende cybercriminaliteit zal blijven stijgen de komende jaren en het is een moeilijk grijpbaar fenomeen. Immers, de bedragen zijn klein en de oplichters verschuilen zich vaak achter een netwerk van katvangers. Echter, door vroegtijdig in te grijpen in de vorm van stopgesprekken, buitengerechtelijke afdoeningen of een andere toekomstige (nog te ontwikkelen) afdoening wordt de criminele carrière vaak gestopt. Het LMIO vormt daarbij een belangrijke 'motor' en aanjager voor de eenheden. Door deze centrale veredeling/analyse van de meldingen worden de eenheden op een efficiënte wijze gevoed met informatie om zaken op te pakken.

Dit artikel is tot stand gekomen in samenwerking met Gijs van der Linden van het LMIO.

[1]Bron: https://www.computable.nl/artikel/nieuws/overheid/6866769/1277202/registraties-cybercrime-en-onlinefraude-fors-omhoog.html

[2]Bron: Cijfers LMIO

Over de auteurs

Jolien van Aar werkte ten tijde van het schrijven van het artikel als onderzoeker/consultant bij Capgemini Invent en richtte zich daarbij op effectmetingen en evaluaties in de publieke sector.

martine.middelveld@capgemini.com

Martine Middelveld is managing consultant bij Capgemini Invent en focust zich op ketensamenwerking, monitoring van effecten en privacyvraagstukken binnen de publieke sector.

erik.hoorweg@capgemini.com

Erik Hoorweg is vice president bij Capgemini Invent en verantwoordelijk voor de sector openbare orde en veiligheid.

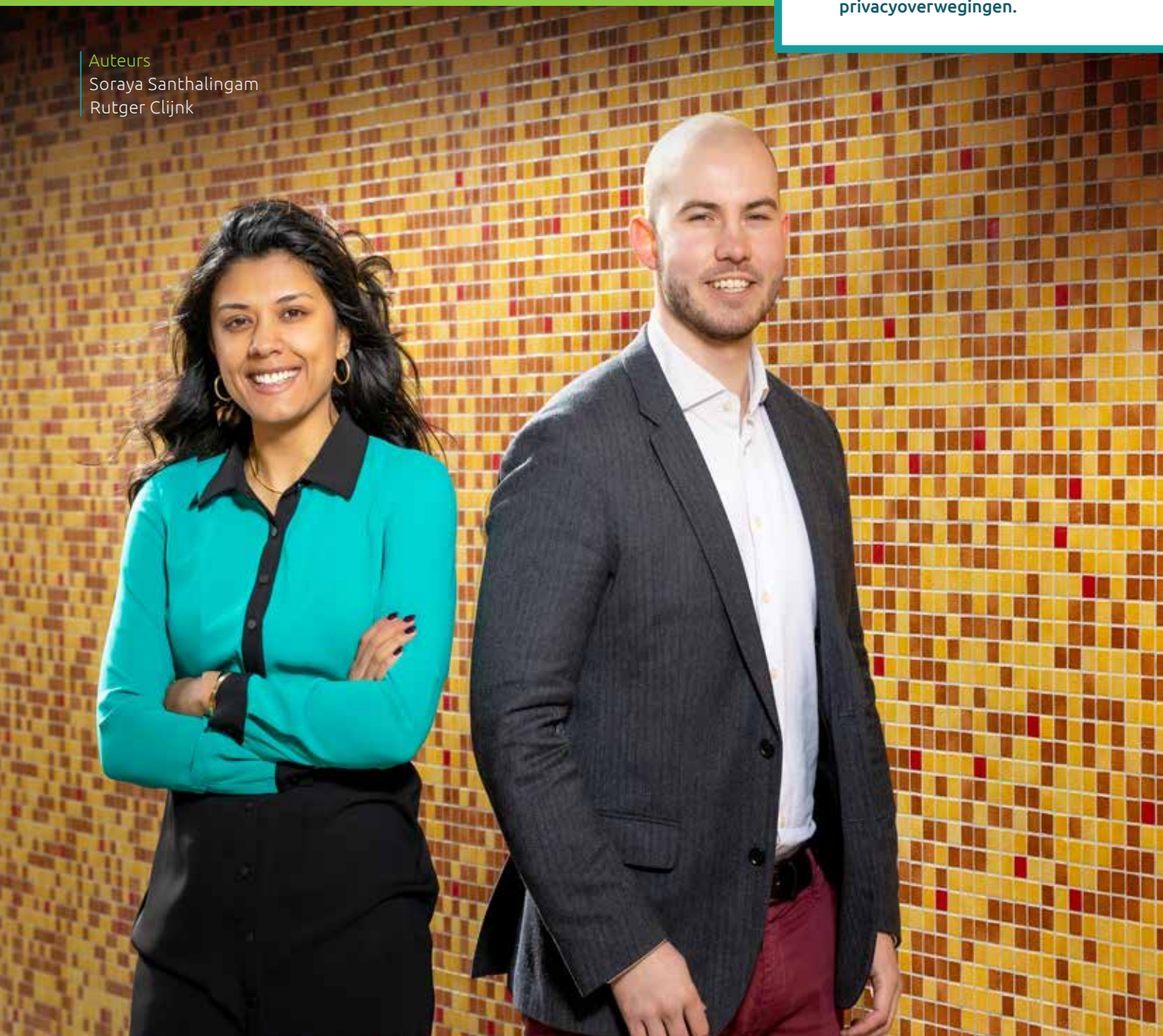
Een gewaagde technologie in de kinderschoenen: experimenteren met artificial intelligence binnen de jeugdzorg

Wat is de huidige visie op het effectief inzetten van AI in de keten van jeugdzorg, ter preventie van jeugdcriminaliteit- en recidive?

Highlights

- De 'Adolphe Quetelet' van onze tijdgeest is een kunstmatige intelligentie.
- Leidt innovatie met kwantitatieve methoden binnen de jeugdzorg tot minder jeugdcriminaliteit?
- Van ketensamenwerking naar holistische samenwerking binnen de jeugdzorg.
- 'Garage2020' is een voorbeeld van experimenteren met data science & artificial intelligence.
- Uitdagingen: het koppelen van datasets en privacyoverwegingen.

Auteurs
Soraya Santhalingam
Rutger Clijnk



In mei 2019 bepleitte minister Grapperhaus tijdens een evenement van het ministerie van Justitie & Veiligheid om meer aan te sturen op informatievoorziening in de keten, om samenwerking binnen het veiligheidsdomein te bevorderen. De ketensamenwerking in de jeugdzorg kwam hier specifiek aan de orde in een aansluitend panel met Mariënne Verhoef van SpiRit. Hierbij was de rol van data één van de hoofdthema's. Voorkomen is beter dan genezen en aangezien artificial intelligence (AI) steeds meer in staat lijkt te zijn om voorspellingen over de toekomst te maken, lijkt het belang van data science en het uitwisselen van informatie tussen ketenpartners ook steeds belangrijker. Aangezien er middels analysemethoden als AI steeds meer mogelijkheden lijken te zijn om data te gebruiken, rijst de vraag: wat is de huidige visie vanuit de jeugdzorg op de inzet van AI ter preventie van (zware) jeugdzorgtrajecten? Wat zijn de uitdagingen van deze toepassingen in de ketensamenwerking? Hoe zit het met privacyoverwegingen?

De oorsprong van criminaliteit verklaren vanuit de statistiek

In 1827 was het de Franse overheid die voor het eerst een rapport met criminaliteitscijfers uitgaf. Dit rapport heette de Compte Général[1]. Het publiceren van deze statistieken luidde het begin van de positivistische criminologie in. Deze criminologische school was voornamelijk gericht op het verklaren van de oorzaken van criminaliteit[2]. Adolphe Quetelet maakte in 1842 gretig gebruik van deze cijfers, ondanks de kwalitatieve beperkingen van de statistieken. Hiermee werd hij één van de eersten die statistische methoden toepaste op de sociale wetenschappen. Jeugdigheid en geslacht bleken de twee belangrijkste predictors van criminaliteit. Waar de statistische analyse van Quetelet beperkt bleef tot het vaststellen van de ratio tussen twee variabelen, is de huidige maatschappij tegenwoordig echter aan het experimenteren met het inzetten van AI om grote hoeveelheden variabelen en datapunten met elkaar in verband te leggen. Het lijkt erop dat niet een individuele intelligentie, maar een kunstmatige intelligentie de potentie heeft om de Quetelet van onze huidige tijdgeest te worden.

Huidige kennis over voorspellende factoren jeugdcriminaliteit

> **Het lijkt erop dat niet een individuele intelligentie, maar een kunstmatige intelligentie de potentie heeft om de Quetelet van onze huidige tijdgeest te worden."**

Quetelet schreef in 1842 al dat van alle factoren die een neiging naar criminaliteit zouden voorspellen, de variabelen leeftijd en geslacht met stipt de meest voorspellende waarden vertegenwoordigden. Verder bleek uit zijn statistische analyse dat de voorspellende waarde van deze variabelen het sterkste was voor mannen tot de leeftijd van 25 jaar. Na het bereiken van deze leeftijd zou volgens hem de ontwikkeling van het redenerende vermogen een inhaalslag maken op de ontwikkeling van de fysieke kracht en emotie3. Bijna twee eeuwen verder sinds Quetelet zijn baanbrekende onderzoek publiceerde, zijn er vandaag de dag nog veel parallellen te trekken met het verleden. Zo lijkt het haast geen toeval dat Politie.nl (2020) jeugdcriminaliteit nog steeds definieert als strafbare gedragingen, gepleegd door jongeren tot en met 24 jaar. Tevens blijkt uit recente literatuur dat het effect van risicofactoren af zou nemen, naarmate de leeftijd toeneemt[3,4].

Gelukkig hebben we tegenwoordig wel beter zicht op wat deze risicofactoren daadwerkelijk betekenen, dan enkel die van 'statische factoren', zoals leeftijd en geslacht. In de literatuur zijn tal van contextuele en dynamische factoren te vinden die een verhoogde kans op jeugddelinquentie zouden kunnen geven. Over het algemeen vallen ze onder te verdelen in vijf domeinen: school, gezin, vrienden, alcohol/drugs en vrijetijdsbesteding[3]. Met AI zouden we meer inzicht kunnen krijgen op de invloed van deze contextuele en dynamische factoren.

Deze kennis is nuttig voor wetenschappers die zich richten op de jeugdzorg. Echter blijkt het in de praktijk nog moeilijk om vroegtijdig te voorspellen welke jongeren crimineel gedrag zullen gaan vertonen. Daarnaast blijft het lastig om in te schatten welke criminele jongeren tevens crimineel gedrag zullen vertonen in de latere adolescentie[4]. Dit gebrek aan voorspellend vermogen lijkt dus een preventieve strategie ter bestrijding van zowel jeugdcriminaliteit, als criminaliteit gepleegd door volwassenen, in de weg te staan.

Casus: Garage2020. Een voorbeeld van (keten-)samenwerking in de jeugdzorg en het verkennen van AI.

Om beter te begrijpen hoe AI werkt in de praktijk hebben we gesproken met deskundigen uit de branch. Garage2020[5] is een voorbeeld van samenwerking binnen de jeugdzorg om door middel van onder andere data science tot een verbetering van de jeugdzorg te komen. De vestigingen van Garage2020 zijn autonome broedplaatsen. Per locatie wordt gewerkt aan verschillende vraagstukken omtrent jeugdzorg, waarbij de projectgroepen verschillen afhankelijk van het onderwerp. Denk bijvoorbeeld aan een mix van projectleiders, designdenkers en datascientists die hierbij zijn aangesloten.

> **Garage2020 probeert met een multidisciplinaire benadering de jeugdzorg efficiënter in te richten middels het gebruik van AI in hun processen."**

Een voorbeeld van een project is 'Extra Team-Lid' in Amsterdam. Dit project is bedoeld om de betrokken professionals te ondersteunen bij het maken van keuzes, om passende hulp in te zetten voor jongeren. Het gaat hier dus niet om analyses van risicofactoren, maar om een ondersteuning bij het keuzeproces op basis van het verleden van een jeugddelinquent. Dit product bestaat uit een interactief 'blokkenspel'waarbij het verleden van jeugdhulp van de jongere in kwestie weergegeven wordt op een bord. Een foto van het bord wordt geüpload naar de bijbehorende app. Vervolgens worden uit de data mogelijke vervolgtrajecten van jeugdzorg gehaald, die tenslotte worden weergegeven in de app. Zo kan efficiënt en nauwkeurig een vervolgtraject gecalculeerd worden.

Uitdagingen en de zoektocht naar alternatieven

Roeland de Koning en Fokko Dijksterhuis stelden in de vorige editie van Trends in Veiligheid dat het veiligheidsdomein meer zou moeten experimenteren met de inzet van AI om de methode verder te ontwikkelen[6]. Initiatieven als Garage2020 zijn een mooi voorbeeld hiervan. Echter benoemden zij ook een aantal uitdagingen bij de implementatie van deze techniek.

Ten eerste geeft Garage2020 aan dat zij rondom 2017 een verschuiving zien in het gebruik van de datasets, mede door herinrichting van de jeugdzorg. De sets van voor die tijd zijn makkelijker te gebruiken omdat die bepaalde categorieën van jeugdzorg weergaven, die in latere datasets zijn losgelaten vanwege een andere manier van sturen. De datasets anno 2020 zijn te beperkt om robuuste analyses uit op te maken. Van jeugdhulpverleners wordt verder verwacht dat ze maatwerkgericht en preventief werken. Hierom worden er alternatieven van zware jeugdhulptrajecten aangeboden in de app van Extra Team-lid, die aansporen om 'outside the box' na te denken.

> **Niet alleen AI, maar outside-of-the-box denken is belangrijk in de huidige, complexe datagedreven samenleving."**

Echter de grootste uitdaging die Garage2020 ziet is de beperking vanuit privacywetgeving. Het koppelen van datasets zou enorme inzichten kunnen bieden, maar daar durft niemand zich echt aan te branden. De Algemene Verordening Gegevensbescherming (AVG) stelt dat geautomatiseerde besluitvorming, waaronder profilering, in combinatie met het koppelen van datasets een hoog risico kan opleveren voor de rechten en vrijheden van betrokkenen[7]. Zo dient er voor de beoogde gegevensverwerking een Data Protection Impact Assesment (DPIA) plaats te vinden om deze risico's in kaart te brengen. In sommige gevallen is dit zelfs verboden. Zo oordeelde de Rechtbank Den Haag in februari 2020 dat het Systeem Risico Indicatie (SyRI) van het ministerie van Sociale Zaken en Werkgelegenheid in strijd is met privacywetgeving en het Europees Verdrag voor de Rechten van de Mens (EVRM). Dit systeem koppelt datasets van verschillende overheden aan elkaar, analyseert deze en maakt profielschetsen om fraude op te sporen[8]. Het lijkt erop dat de samenleving dus nog wat ethische vraagstukken moet beantwoorden, voordat initiatieven als Garage2020 volop kunnen profiteren van de voordelen die AI kan bieden.

> **De Rechtbank Den Haag oordeelde in februari 2020 dat het Systeem Risico Indicatie (SyRI) van het Ministerie van Sociale Zaken en Werkgelegenheid in strijd is met privacywetgeving en het Europees Verdrag voor de Rechten van de Mens EVRM."**

Conclusie

Het combineren van datasets afkomstig van verschillende partners binnen de jeugdzorgketen lijkt op het eerste gezicht een veelbelovende techniek die deuren openzet voor het gebruik van AI. De toename van de hoeveelheid data in de samenleving zou ons middels het gebruik van geavanceerde analysemethoden meer inzicht kunnen verschaffen in de complexiteit van factoren die kunnen leiden tot (zware) jeugdzorgtrajecten. Hiermee zou kunstmatige intelligentie een nieuwe doorbraak kunnen inluiden voor ons begrip van jeugdcriminaliteit, net zoals Quetelet deed in 1842 toen hij begon te experimenteren met statistische methoden. Er zijn al initiatieven gaande binnen de jeugdzorg om te experimenteren met de toepassing van AI binnen jeugdzorg processen. Een voorbeeld hiervan is Garage2020, die met een multidisciplinaire benadering de jeugdzorg efficiënter probeert in te richten middels het gebruik van AI in hun processen. Echter zijn er ook nog beren op de weg te zien. De komst van wetgevingen zoals de AVG maken het ingewikkelder om datasets van verschillende ketenpartners met elkaar te koppelen. Dit maakt het moeilijker om geavanceerde AI-analysemethoden toe te passen, omdat de kwantiteit en kwaliteit van de data te beperkt blijft. Alvorens er verder geëxperimenteerd zal worden met het toepassen van AI binnen de jeugdzorg, dient onze samenleving nog wat prangende ethische vraagstukken te beantwoorden. Deze gewaagde technologie staat immers nog in haar kinderschoenen.

Over de auteurs

rutger.clijnk@capgemini.com
Rutger Clijnk

soraya.santhalingam@capgemini.com.
Soraya Santhalingam

Rutger Clijnk, Msc MA en **Soraya Santhalingam,** LL.M. zijn werkzaam bij Capgemini Nederland, binnen de Cybersecurity Unit. Zij adviseren organisaties om hun weerbaarheid te vergroten op het gebied van cybersecurity of over een zorgvuldigere omgang met hun data en persoonsgegevens.

[1]Beirne, P. (1987). Between Classicism and Positivism: Crime and Penalty in the Writings of Gabriel Tarde. Criminology.

[2]McLaughlin, E. & Muncie, J. (2013). Criminological Perspectives: Essential Readings. SAGE Publications Ltd.

[3]Sampson, R. J. and J. H. Laub. (1992). Crime and Deviance in the Life Course. Annual Review of Sociology 18:63-84.

[4]Het CCV, gepubliceerd op 31-12-2019. Secondant: voorspellen van delinquentie op jonge leeftijd. https://hetccv.nl/nieuws/secondant-voorspellen-van-delinquentie-op-jonge-leeftijd/ .

[5]Interview Bastiaan Bervoets, 22 januari 2020; Interview Jeroen de Vries- 28 januari 2020, 09:30u; Interview John Komen 11 februari 2020, 17:00u.

[6]Dijksterhuis, F. & Koning, R. de. Vertrouwen in artificial intelligence voor het veiligheidsdomein begint met experimenteren https://www.trendsinveiligheid.nl/rapport/2019-slimmer-samenwerken-aan-een-veiliger-nederland/vertrouwen-in-artificial-intelligence-voor-het-veiligheidsdomein-begint-met-experimenteren/.

[7]Artikel 35 AVG, zie ook Handreiking V&J. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[8]Rb. Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865.

Schiet uit de privacykramp! Hoe technologie privacy eenvoudiger kan maken

Hoe maken we privacyprocessen slimmer en efficiënter?

Auteurs
Albert Holl
Natasja Pieterman
Michail Theuns

Highlights

- Ruim 39% van de bevolking heeft geen vertrouwen in hoe de overheid met hun persoonsgegevens om gaat.
- Privacy wordt regelmatig gezien als belemmering, waardoor men risicomijdend wordt terwijl privacy juist voor meer vertrouwen zou kunnen zorgen.
- Technologie voegt steeds meer intelligentie toe aan privacyprocessen om repetitieve activiteiten te automatiseren.

Mag je tegenwoordig nog wel persoonsgegevens delen? Hoe houdt u dan grip op dit delen van persoonsgegevens zonder in een privacykramp te schieten? Slimme automatisering helpt om privacy duurzaam te waarborgen.

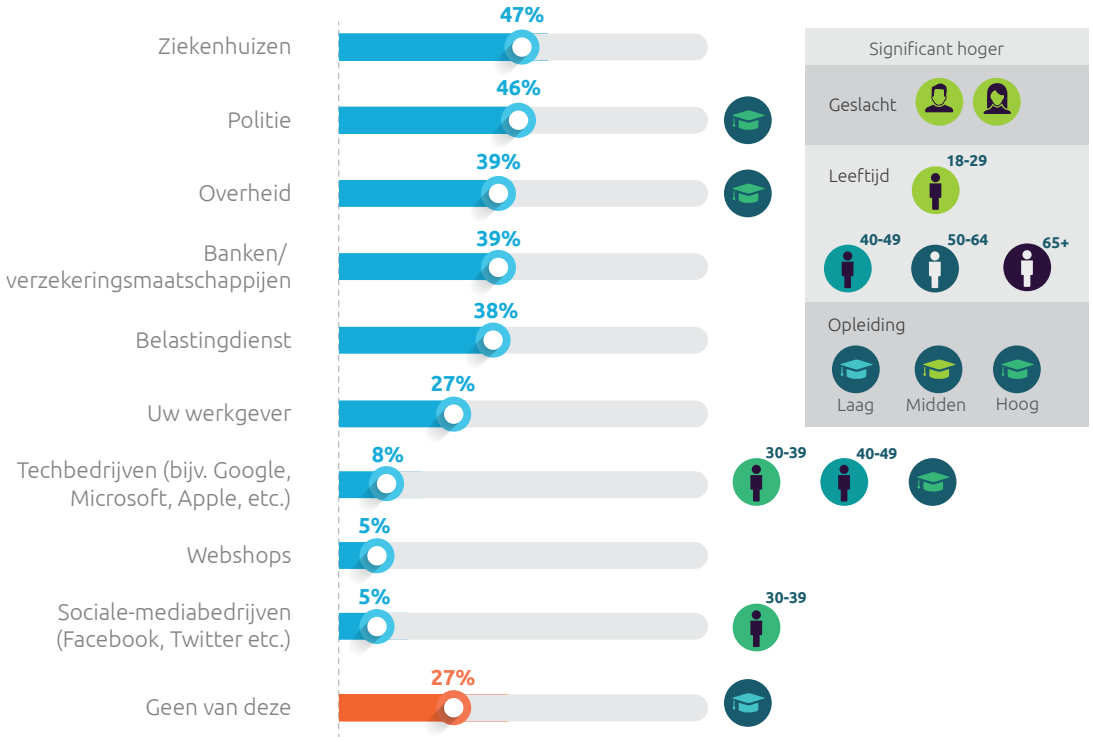
Privacykramp!

Privacykramp lijkt een nieuw woord in de Van Dale te worden. Het hebben van verwerkingsregisters, cookie-regels, wel of geen gegevens uitwisselen? Allemaal vragen die zijn gaan leven na de invoering van de Algemene Verordening Gegevensbescherming (AVG). Al jaren voor de inwerkingtreding van de AVG was er aandacht voor het onderwerp privacy. Met als gevolg dat veel organisaties aan de slag zijn gegaan om persoonsgegevens beter te beschermen. Bijvoorbeeld door goed in kaart te brengen waar alle persoonsgegevens zijn opgeslagen en waarvoor ze nodig zijn.

De invoering van de AVG heeft tot gevolg gehad dat organisaties gegevens niet meer delen uit angst en onwetendheid voor de AVG. Als gevolg hiervan lopen organisaties tegen problemen aan in de dagelijks uitvoering van hun taken. Denk aan de overheid als het gaat om toezicht en handhaving, maar ook in de zorg ("mogen we de kamernummers van patiënten nog verstrekken aan familieleden?"[1]). Met de boetes die wereldwijd worden uitgedeeld, is die zorg niet geheel onterecht[2]. Uit onderzoek uitgevoerd door Ipsos in opdracht van Capgemini in 2020 blijkt dat 39% geen vertrouwen heeft in hoe de overheid met hun persoonsgegevens om gaat.

Van welke van de volgende instanties/bedrijven heeft u er vertrouwen in dat ze veilig met uw gegevens omgaan?

Vertrouwd veilig om te gaan met persoonsgegevens



Organisaties zijn fanatiek aan de slag gegaan om te (blijven) voldoen aan de lokale wet- en regelgeving. Net zoals informatiebeveiliging zou de AVG de bedrijfsdoelen niet moeten hinderen, maar juist ondersteunen zodat deze op een veilige manier behaald kunnen worden. De compliance-uitdagingen die de AVG met zich meebrengt moeten ondergebracht worden in de huidige organisatie en integreren met het bestaande landschap.

Bij grote organisaties zien we dat voor deze inventarisatie software werd gekocht, maar bij kleinere organisaties komen we nog regelmatig handmatige administraties in Excel tegen. Het invoeren van wet- en regelgeving en kaders wordt echter vaak gezien als een kwestie van 'vinkjes halen'. Of het nu gaat om het implementeren van maatregelen uit de Baseline Informatiebeveiliging Overheid (BIO), de ISO 27001 serie of de AVG, vaak zien we dat het behalen van compliance belangrijker is dan het echt verbeteren van de veiligheid van gegevens. Compliance is bovendien een arbeidsintensief proces, voornamelijk bij handmatige administraties. Het vroegtijdig detecteren, corrigeren en voorkomen van afwijkingen of overtredingen van wet- en regelgeving op het gebied van privacy en informatiebeveiliging kan hierdoor lastig zijn.

De uitdagingen in de praktijk

Organisaties in het veiligheidsdomein werken met gevoelige informatie zoals gegevens uit de vreemdelingen- of de strafrechtketen. Wanneer dit soort gegevens uitlekken kan dit ernstige gevolgen hebben voor de betrokkenen. Niet voor niets heeft minister van Justitie en Veiligheid Ferdinand Grapperhaus de Tweede Kamer vorig jaar geïnformeerd over de verbetering van de centrale aansturing en beheersing van informatiebeveiliging binnen het ministerie van Justitie en Veiligheid[3].

Als mensen beperkingen ervaren in het delen van noodzakelijke gegevens of bang zijn voor boetes, zijn ze geneigd om de meest veilige weg te bewandelen. Het gevolg daarvan is risicomijdend gedrag. Op zichzelf is dat geen kwalijke zaak, tenzij het een belemmerende werking heeft in de uitvoering. Ook ons veiligheidsdomein loopt hier tegenaan bij handhaving, fraudeonderzoek en opsporing. Het niet of juist overmatig voldoen aan de verschillende richtlijnen kost capaciteit, tijd en geld.

Kijkend naar handhaving en toezicht zijn de belangrijkste leveranciers van gegevens de overheidspartijen. Juist deze partijen ervaren problemen met het uitwisselen van data en het creëren van overzicht. Zo bleek recent ook met de dossiers van de Belastingdienst inzake de kinderopvangtoeslag[4]. Niet enkel met betrekking tot handhaving in het sociaal domein is deze data tussen deze partijen relevant, maar ook voor landelijke opsporing.

In de Kamerbrief van Ferdinand Grapperhaus is de ambitie uitgesproken om op het gebied van informatiebeveiliging te groeien van een volwassenheidsniveau van 2,9 nu naar een 4,2 op een vijfpuntschaal in 2021. Dat is een stevige groei, terwijl niet alle organisaties in het veiligheidsdomein de mogelijkheid en capaciteit hebben om een fulltime CISO of functionaris gegevensbescherming in dienst te nemen. Dat betekent dat organisaties slimmer te werk moeten gaan door repetitieve taken te automatiseren.

Door het automatiseren van tijdrovende bedrijfsprocessen kan efficiëntie gewonnen worden. Medewerkers kunnen zich focussen op hun kerntaken in plaats van afgeleid te worden door 'uitzoekklusjes' zoals het bij elkaar zoeken van persoonsgegevens in het kader van verzoeken tot inzage. Daarnaast kunnen doorlooptijden van aanvragen verkort worden, en de uitkomsten worden voorspelbaarder, waardoor uiteindelijk de klanttevredenheid kan worden verbeterd.

Automatisering van privacyprocessen

De politie werkt in de dagelijkse praktijk samen met andere overheidspartijen en derde partijen zoals woningbouwverenigingen. Hierbij willen ze structureel gegevens uitwisselen voor de uitvoering van hun taak. Deze gegevensuitwisseling leggen zij vast in convenanten om de samenwerking zo duidelijk en transparant mogelijk te maken. In deze gevallen zijn er extra privacyzorgen, want waar ligt de verantwoordelijkheid, wie moet een datalek melden en wie moet welk register bijhouden? Het overzicht houden van de verwerkingen, de datastromen en convenanten is cruciaal om het behapbaar te houden.

Wat daarbij kan helpen is een centraal platform in de organisatie. Geen versnippering van datastromen, geen verwerkingsregister per afdeling, niet zoeken naar eventuele informatieverzoeken die privacy-gerelateerd zijn, maar alle informatie overzichtelijk op één plek. Software kan helpen door slimme automatisering van specifieke AVG-processen. In de markt zijn verschillende softwarepakketten beschikbaar die organisaties hierin ondersteunen. Denk aan geautomatiseerde afhandeling van datalekken en melding van datalekken aan de Autoriteit Persoonsgegevens, of het geautomatiseerd aanmaken van privacyrisico's. Zo is het mogelijk om via deze kunstmatige intelligentie vragen en klachten van betrokkenen af te handelen en alleen indien nodig menselijke interventie in te schakelen. Dit soort innovaties zorgen ervoor dat organisaties efficiënter beveiligingsmaatregelen kunnen doorvoeren en daarmee meer vertrouwen van klanten en burgers kunnen winnen.

Het toevoegen van intelligentie in procesautomatisering

Zoals eerder aangegeven bestaan er al diverse automatiserings-oplossingen voor specifieke AVG-processen zoals voor het uitvoeren van een privacy-risicoanalyse, het vastleggen van verwerkingen in een verwerkingsregister en het melden en mitigeren van een datalek. Dit soort privacymanagementsoftware automatiseert workflows zodat iedere rol in deze workflow automatisch zijn of haar taak toebedeeld krijgt.

Onze verwachting is dat de markt voor privacymanagement-sofware in 2020 steeds volwassener gaat worden en dat softwarepakketten een combinatie gaan vormen met partijen die zich meer op content en uitvoering richten. Neem het privacymanagement softwarebedrijf OneTrust het DataGuidance platform overnam in maart 2019[5]. Het privacymanagementplatform van OneTrust werd hierdoor verrijkt met honderden internationale privacywetten en kon daardoor ook meer content-gerelateerde zaken automatiseren. Bijvoorbeeld een geautomatiseerde analyse van de verschillende wetgevingen die van toepassing kunnen zijn op één specifieke casus (zoals de Wet Politiegegevens en de AVG die beide van toepassing kunnen zijn in een opsporingszaak). De politie en andere overheidsdiensten krijgen regelmatig te maken met onderzoeken die de landsgrenzen overschrijden. Privacysoftware kan hier een uitkomst bieden doordat alle internationale privacywetten zijn geïntegreerd. De software maakt een eerste analyse die later door de verantwoordelijke privacy officer als uitgangspunt gebruikt kan worden voor het definiëren van maatregelen of het opzetten van een verdere analyse. Op deze manier faciliteert de software het efficiënter doorvoeren van de diverse maatregelen.

Innovatieve niche-oplossingen

Naast toevoegingen van automatisering zien we ook dat er nieuwe partijen de markt zullen betreden met zeer specifieke niche oplossingen. Zo biedt de start-up Privaci.ai een platform om compliancetaken te automatiseren door gebruik van kunstmatige intelligentie[6]. Deze start-up heeft recentelijk 31 miljoen dollar aan investeringen opgehaald en heeft als doel om verzoeken van betrokkenen te faciliteren, toestemming voor verwerken te verzamelen en organisaties te helpen bij het uitvoeren van data protection impact assessments. Met name het gebruik van kunstmatige intelligentie is interessant. Middels machine learning (zie kader) leert het platform om verschillende datatypes in kaart te brengen, te classificeren en te onderscheiden van elkaar. Vervolgens kan het deze datatypes koppelen aan een betrokkene die reeds geïdentificeerd is. Het platform kan hierdoor een volledige afhandeling van het verzoek van een betrokkene doen: identificatie van de betrokkene, koppelen van de juiste data aan deze betrokkene en het koppelen van alle betrokken stakeholders (zoals de privacy officer of de servicedesk die dit verzoek moet behandelen).

Machine learning is een breed onderzoeksveld binnen de kunstmatige intelligentie dat zich bezighoudt met de ontwikkeling van algoritmes en technieken waarmee computers kunnen leren door op geautomatiseerde wijze patronen en relaties te zoeken in grote hoeveelheden gegevens.

Tot slot

Hoewel op dit moment veel organisaties in een zogenaamde 'privacykramp' schieten, zijn andere organisaties naarstig aan de slag gegaan om de privacy op orde te brengen. Sommige organisaties gebruiken voor de ondersteuning van deze werkzaamheden specifieke privacysoftware maar bij kleinere organisaties komen we ook nog regelmatig administraties in Excel tegen. Verder zien we een toename van automatisering van privacyprocessen met als doel het bereiken van een betere efficiëntie binnen deze AVG-processen. Onze visie is echter dat naast deze efficiëntieslag de technologie zich ook in de richting van intelligentere privacysoftware zal ontwikkelen. Voorbeelden van dit soort intelligentie zijn: een pre-analyse van de verschillende wetten die van toepassing kunnen zijn op een bepaalde casus of het afhandelen van bepaalde verzoeken in het kader van de rechten van betrokkenen door middel van kunstmatige intelligentie. Dit kan nu nog gezien worden als een niche maar zal door verdere doorontwikkeling meer volwassen worden. Uit de kramp dus.

Over de auteurs

albert.holl@capgemini.com

Albert Holl FIP is managing consultant bij Capgemini Cybersecurity en richt zich op vraagstukken op het gebied van privacy en digital trust.

michail.theuns@capgemini.com

Michail Theuns MSc CISSP CISM CIPP/E is managing consultant bij de Capgemini Cybersecurity Unit en is gespecialiseerd in cybersecurity en privacy-management.

natasja.pieterman@capgemini.com

Natasja Pieterman is senior consultant bij de Capgemini Cybersecurity Unit en richt zich met name op privacy in het publieke domein. Daarnaast is zij trainer bij de Capgemini Academy.

[1]https://www.ad.nl/amersfoort/meander-draait-privacy-beleid-terug-baliemedewerkers-mogen-wel-kamernummer-geven~a9192961/

[2]https://www.enforcementtracker.com/

[3]https://www.rijksoverheid.nl/documenten/kamerstukken/2018/10/29/tk-plan-van-aanpak-verbetering-centrale-sturing-en-beheersing-informatiebeveiliging-jenv

[4]https://www.rtlnieuws.nl/nieuws/nederland/artikel/4951601/kinderopvangtoeslag-dossier-belastingdienst

[5]https://www.prnewswire.com/news-releases/onetrust-acquires-dataguidance-integrates-hundreds-of-privacy-laws-into-onetrust-privacy-management-technology-300809704.html

[6]https://iapp.org/news/a/platform-uses-ai-bots-to-automate-compliance-practices/

De noodzaak van de digitale brandoefening

Hoe zorgen we dat Nederland goed voorbereid is op maatschappij-ontwrichtende ontwrichtende cyberincidenten?

Highlights

- De grootste dreigingen zijn spionage, verstoring en sabotage.
- De overheid heeft onvoldoende middelen om adequaat te handelen op een incident.
- Toenemende digitalisering en geopolitieke spanningen maken de schaal, verspreiding en impact van cyberincidenten groter.
- Improvisatie op mandaat en samenwerking heeft de overhand.
- Door een gesimuleerd cyberincident te oefenen en ervaren werken we aan een betere voorbereiding.

Auteurs
Lisa Soldaat
Maaike Vermeulen

Een cyberincident heeft de mogelijkheid om de maatschappij te ontwrichten: verstoring en uitval van digitale infrastructuur kan grote gevolgen hebben voor onze economie en samenleving. De toenemende digitalisering maakt de mogelijke schaal, verspreiding en impact van incidenten alsmaar groter. Maar hoe aannemelijk is het plaatsvinden van een grootschalig cyberincident? En hoe kunnen we ons hierop voorbereiden?

"Overheid waarschuwt: honderden Nederlandse bedrijven kwetsbaar door ernstig lek". "Cyberaanval ontwricht haven". "Nederlandse bedrijven slachtoffer van geavanceerde gijzelsoftware". "Chinese hackersgroep spioneert jarenlang in het geniep in Nederland". Dit zijn recente krantenkoppen die eens te meer wijzen op de noodzaak om ons te weren tegen geavanceerde cyberincidenten. Nederland behoort tot de voorlopers op het gebied van cybersecurity[1] en heeft een belangrijke digitale infrastructuur[2]. We hebben vele en snelle internetverbindingen in combinatie met een open samenleving en we worden steeds afhankelijker van ICT. Tegelijkertijd worden aanvallers steeds slimmer en neemt de dreiging toe door geopolitieke spanningen en digitale verwevenheid van apparaten. Het aantal serieuze cyberincidenten is in 2019 bijna verdrievoudigd ten opzichte van 2018[3]. Sinds het begin van de coronacrisis is er een enorme toename van cyberincidenten[4]. Van de stijging in phishing e-mails tot gerichte, ontwrichtende aanvallen op ziekenhuizen. Ziekenhuizen zijn in deze tijd belangrijker dan ooit en worden tegelijkertijd fysiek en digitaal onder vuur genomen. Waar het ziekenhuispersoneel zich met verschillende scenario's voorbereidt en elkaar via samenwerkingsverbanden helpt om instrumenten en patiënten uit te wisselen, zou dit ook digitaal moeten plaatsvinden. De Nederlandse overheid heeft echter bij een incident onvoldoende middelen om adequaat te handelen, vooral wanneer verstoringen ontwrichtende consequenties hebben voor de fysieke wereld en het vertrouwen in de rechtstaat[5]. Maar hoe aannemelijk is het plaatsvinden van een grootschalig cyberincident? En hoe kunnen we ons hierop voorbereiden?

In dit artikel zullen we ingaan op wat nodig is om ons voor te bereiden op grootschalige cyberincidenten: de digitale brandoefening.

Het huidige dreigingsbeeld

De grootste dreigingen zijn spionage en sabotage vanuit statelijke actoren en verstoring van vitale systemen. Waar de motivatie van niet-statelijke actoren vaak gericht is op financiële- en reputatieschade, is de motivatie van statelijke actoren specifiek gefocust op het bereiken van geopolitieke en economische doelstellingen ten koste van Nederlandse belangen. Door spionage worden politieke inlichtingen ingewonnen, (bedrijfs)geheimen gestolen en (dissidente) groeperingen of individuen gevolgd. Om binnen te dringen bij het doelwit wordt vaak gebruik gemaakt van leveranciers die op legitieme wijze toegang hebben tot een infrastructuur. Hierdoor is het ecosysteem zo sterk als de zwakste schakel en kleinere leveranciers hebben niet altijd het budget of de skills om de organisatie weerbaar te houden.

Storing en uitval van (informatie)systemen zijn daarnaast een dreiging door de potentiële impact. De uitval van één systeem of netwerk kan voor storing of uitval op andere plekken zorgen. Dit geldt zeker wanneer het plaatsvindt op een centraal informatieknooppunt of bij vitale processen. Denk bijvoorbeeld aan de 112-storing in juni 2019. Het noodnummer was urenlang onbereikbaar door een storing op het netwerk van KPN.

Daarnaast is er nog digitale sabotage waarbij (vitale) systemen en processen opzettelijk worden beschadigd, verstoord of vernietigd. Aanvallen op bedrijven en instellingen gebeuren bijna wekelijks[6], maar in de meeste gevallen blijft het buiten het nieuws. Een voorbeeld is de NotPetya aanval van 2017. Deze aanval legde heel Oekraïne plat en trof ook de haven in Rotterdam. Twee grote containerterminals in de haven werden twee weken platgelegd en de schade was enorm. Deze hack heeft gezorgd voor een reality check: één zwakke plek kan de maatschappij al ontwrichten en er zijn hackgroepen die niet alleen deze potentie kennen, maar ook bereid zijn om hun tegenstander daar te raken.

Hoe reageert Nederland?

De reactie op grootschalige incidenten wordt gekenmerkt door improvisatie, met name op het gebied van mandaat en samenwerking: de overheid heeft geen duidelijke bevoegdheden om in te grijpen en daarnaast hebben overheden, organisaties en bedrijven vaak geen goed beeld van de partijen van wie ze afhankelijk zijn. Omdat systemen die bijvoorbeeld telefoonverkeer, betalingen, beveiliging en transport regelen volledig geautomatiseerd zijn, onderling verbonden en opereren in een web met

allerlei leveranciers en tussenbedrijven, is er amper overzicht. Een bijkomend probleem is dat als de digitale ramp uitbreekt het vaak te lang duurt voordat hulptroepen aan de slag kunnen. Toen met de NotPetya aanval de systemen in de Rotterdamse haven lam waren gelegd, kon de veiligheidsregio eerst niets doen toen ze informatie wilden. Ondanks dat er veel lessen zijn getrokken uit deze incidenten, bestaan er geen duidelijke en voldoende ingekaderde bevoegdheden om cyberincidenten te bestrijden. De focus ligt nu op het adviseren en ondersteunen van organisaties binnen de vitale infrastructuur. Maar wanneer organisaties weigeren mee te werken, "is het onduidelijk welke middelen de overheid heeft om in te grijpen en op welke gronden dat dient te gebeuren", aldus de Wetenschappelijk Raad voor het Regeringsbeleid[7].

En het Nationale Cyber Security Centrum (NCSC) dan? Het NCSC heeft de wettelijke taak om vitale aanbieders en onderdelen van Nederland te informeren, adviseren en bij te staan bij dreigingen en incidenten. Echter, veel organisaties in de semipublieke- en private sector vallen niet onder de wettelijke taakstelling van het NCSC. Hierdoor kan het nauwelijks invloed uitoefenen op bijvoorbeeld organisaties zoals zorg- en onderwijsinstellingen.

De digitale dreiging neemt toe

Gezien de sterke groei in digitalisering van de wereldwijde samenleving zal de dreiging alleen maar toenemen. Tegenwoordig zijn niet alleen PCs, laptops en mobiele telefoons aangesloten op het internet, maar ook onderdelen van onze vitale infrastructuur, hele fabrieken, systemen in het openbaar vervoer, medische apparaten en energienetwerken. Dit in samenloop met het 5G-netwerk dat naar verwachting in 2020 wordt uitgerold. Volgens KPN maakt 5G het mogelijk om vrijwel de gehele samenleving onderling te verbinden[8]. De toenemende complexiteit en connectiviteit kunnen negatieve effecten hebben op de weerbaarheid en het vermogen van hackers om schade aan te richten neemt toe. Het is evident dat 5G de wijze waarop wij problemen met cyberbeveiliging aanpakken in de toekomst zal veranderen.

Daarnaast zullen we ook rekening moeten houden met de oplopende geopolitieke spanningen tussen met name de VS, de EU-lidstaten, Rusland, China, Iran en Noord-Korea. Dit is te merken aan de recent geëscaleerde situatie tussen de VS en Iran, de toenemende assertiviteit van China en Rusland en de toenemende nucleaire onzekerheid en verslechterde trans-atlantische relaties. Deze oplopende spanningen beïnvloeden cybersecurity.

Het zal een uitdaging blijven om de weerbaarheid dusdanig op peil te houden dat we de toenemende afhankelijkheid en veranderende dreiging het hoofd kunnen bieden. Er zijn essentiële maatregelen die getroffen moeten worden om ons voor te bereiden op een cyberaanval. Er staat immers teveel op het spel om de voorbereiding op en aanpak van digitale ontwrichting op zijn beloop te laten.

De digitale brandoefening

Voorkomen is beter dan genezen. Cybersecurity-maatregelen binnen de overheid zijn dan ook met name gericht op het voorkomen van cyberincidenten. Echter, in het digitale domein valt een incident nooit 100% uit te sluiten. Daarbij komt het feit dat cybercriminelen altijd voorop zullen lopen op de overheid en veel andere organisaties.

Er zijn stappen te ondernemen bij het voorkomen van een cyberincident: uitwijkmogelijkheden of terugvalopties zijn bijvoorbeeld vaak onvoldoende aanwezig[9]. Daarnaast zijn veel maatschappelijke kernprocessen sterk afhankelijk van het doen en laten van grote, monopolistische, buitenlandse aanbieders van digitale voorzieningen. Dit maakt onze maatschappij kwetsbaar voor wisselende intenties van deze aanbieders en landen[10].

Aangezien het onmogelijk is om alle cyberaanvallen te voorkomen, is het noodzakelijk dat organisaties zich meer gaan focussen op oefenen: door gesimuleerde cyberaanvallen daadwerkelijk te ervaren, is het voor organisaties mogelijk om zich beter voor te bereiden. Een digitale brandoefening.

Hierbij staan ons inziens drie onderdelen centraal:

1. **Incident response:** een term die wordt gebruikt om het proces te beschrijven waarmee een organisatie een cyberincident afhandelt (zowel technisch als met betrekking tot bedrijfsprocessen). Dit heeft als doel om de schade, hersteltijd en -kosten zoveel mogelijk te beperken. Naast het oefenen op de bedrijfsprocessen is het tegenwoordig ook steeds beter mogelijk om te oefenen op technische componenten[11]. Dit is uitermate belangrijk voor het trainen van de technische capaciteiten van medewerkers.

2. **Samenwerking:** bij een grootschalig cyberincident is het onvermijdelijk dat verschillende organisaties met elkaar moeten samenwerken op nationaal niveau. Niet alleen heeft de overheid geen duidelijke, gecentraliseerde bevoegdheden om in te grijpen. Ook is er vaak samenwerking nodig tussen verschillende sectoren voor de uitwisseling van de juiste (technische) expertise. Daarbij komt dat er samenwerking vereist is op Europees en internationaal niveau: het digitale domein kent geen nationale grenzen.

3. **Communicatie:** besluitvorming ligt bij het management. Bij cyberincidenten moet het niet-technische management echter vaak de technische expertise inschakelen van specialisten. Het oefenen op communicatie binnen een organisatie is daarom ook fundamenteel: hoe lopen de communicatielijnen? Is het management voldoende op de hoogte van de ernst van een cyberincident en de te nemen stappen? Daarnaast is het oefenen op externe communicatie ook van belang. Hoe communiceren we naar onze stakeholders? Hoe gaan we om met media, zonder onze reputatie te schaden?

Een succesvolle cybersimulatie-oefening kent bovenstaande aspecten en oefent enerzijds op managementniveau en anderzijds de technische experts binnen de organisatie. Door crisissituaties na te spelen, wordt de gehele organisatie zich bewust van de digitale dreigingen, de eigen rol, verantwoordelijkheden en risico's/consequenties van het eigen handelen.

Conclusie

Door de hierboven genoemde ontwikkelingen is het niet de vraag óf er een grootschalig cyberincident met nog ongekende gevolgen voor maatschappelijke ontwrichting zal plaatsvinden, maar wanneer. Juist omdat een cyberincident nooit volledig te voorkomen is, is het noodzakelijk dat niet slechts de focus wordt gelegd op preventieve maatregelen maar dat organisaties zich gaan bezighouden met welke stappen er gezet moeten worden wanneer er een cyberincident plaatsvindt. Door een gesimuleerd cyberincident te oefenen en te ervaren, kunnen we werken aan een betere voorbereiding. Kortom, we moeten ons voldoende bewust zijn van hoe we de volgende grote 'digitale brand' kunnen bestrijden.

[1]De Global Cybersecurity Index (2018) positioneert Nederland op de 12e plek (8e in Europa) van de 175 landen wereldwijd; gemeten op o.a. wettelijke maatregelen, technische capaciteiten en samenwerking.

[2]In Amsterdam ligt het op een na grootste internetknooppunt ter wereld – de Amsterdamse AMS-IX. Dit knooppunt bestaat uit enorme datacentra en is in veel opzichten vergelijkbaar met Schiphol en de Rotterdamse haven.

[3]Channel Connect (2019) Aantal serieuze cyberincidenten in een jaar bijna verdrievoudigd.

[4]Trouw (2020) Europol: De coronacrisis serieuze bedreiging voor de digitale veiligheid.

[5]De Wetenschappelijke Raad voor het Regeringsbeleid (sept. 2019), 'Voorbereiden op digitale ontwrichting', p.10.

[6]NOS (nov. 2019), Nederlandse bedrijven slachtoffer van geavanceerde gijzelsoftware.

[7]De Wetenschappelijk Raad voor het Regeringsbeleid (2019), 'Voorbereiden op digitale ontwrichting', p. 66

[8]KPN (april, 2019), wat kunnen we met 5G?

[9]Voorbeelden hiervan zouden zijn: een variëteit in aanbieders, toepassingen of infrastructuren; netwerkscheiding (het plaatsen van 'schotten' tussen verschillende systemen om verstoringen een halt toe te roepen of verdere verspreiding van besmetting te voorkomen) of terugvallen op analoge systemen.

[10]The Hague Security Delta (2019), CSAN 2019, p. 7.

[11]Bijvoorbeeld door middel van een 'Cyber-Range-in-a-Box' (CRIAB): een speciale computer voor het ontwikkelen, testen en experimenteren van cybertooling en -technieken.

Over de auteurs

Maaike Vermeulen was ten tijde van schrijven van dit artikel management consultant bij Capgemini. Ze is gespecialiseerd in cybersecurity en privacy. Maaike focustte zich op de publieke veiligheidssector en heeft ervaring met bewustwordingsprogramma's, innovatie en procesoptimalisatie.

lisa.soldaat@capgemini.com

Lisa Soldaat is management consultant bij de Cybersecurity Unit van Capgemini. Ze is gespecialiseerd in cybersecurity en crisisbeheersing. Lisa focust zich op de publieke veiligheidssector en richt zich op vraagstukken rondom nationale veiligheid en de digitale weerbaarheid van organisaties.

Meer misdaden oplossen met minder politiemensen

Hoe kunnen we anders (samen)werken om de capaciteitsuitdaging bij de politie het hoofd te bieden?

Auteurs
Jeroen Oosterwal
Lisa Marie Brouwer

Highlights

- Onder andere door demografische ontwikkelingen heeft de politie capaciteitsuitdagingen, zo zijn er in 2040 nog maar 2 werkenden op 1 gepensioneerde.
- Om toekomstbestendig te zijn moet de politie op een andere manier gaan werken.
- Wij stellen voor om Informatie Gestuurd te gaan optreden, in een snelkookpan omgeving het gebruik van nieuwe technologieën echt te realiseren en digitale triage te gaan toepassen.
- Door op deze vernieuwende manieren te gaan werken, kan de politie meer zaken oplossen en het vertrouwen in de politie versterken.

De politie moet anders gaan werken om met minder menskracht meer zaken op te lossen. In dit artikel stellen wij drie vernieuwende manieren van werken voor.

Actuele cijfers van het CBS over de bevolkingsprognoses geven een ontluisterend beeld:

- De Nederlandse bevolking vergrijst in een hoog tempo. Van ruim 19% 65 plussers in 2020 naar 25% in 2040.
- De hoeveelheid mensen die kan werken (grofweg tussen 20 en 65 jaar) neemt af. Van 59% in 2020 naar 32% in 2040.
- In 2020 zijn er 3 werkenden op 1 gepensioneerde. In 2040 zijn er nog maar 2 werkenden op 1 gepensioneerde.
- De grijze druk neemt tussen 2020 en 2040 toe met 15%.

Bovenstaande effecten versterken elkaar en dat betekent dat er een grote druk komt te staan op de maatschappij. Dit heeft uiteraard ook gevolgen voor het veiligheidsdomein, en meer specifiek, op het aantal mensen dat werkzaam is bij de politie. Terwijl er eigenlijk meer mensen nodig zijn omdat de totale omvang van de bevolking toeneemt en, niet onbelangrijk, de samenstelling van de bevolking verandert.

Eén ding is zeker. De komende tijd gaan veel politiemedewerkers met pensioen[1] en de instroom van nieuwe agenten blijft achter ondanks maatregelen zoals het verkorten van de opleiding[2]. Hierdoor loopt het tekort aan agenten en rechercheurs nog harder op. Dit betekent dat de huidige manier van (samen) werken onder druk komt te staan. Om toch voldoende blauw op straat te houden, voldoende zaken te kunnen oppakken én op te lossen moeten er innovatieve oplossingen komen. Omdat het werk in de veiligheidsketen, en dan met name in het operationele domein, veelal mensenwerk is, zijn er vooral op dit gebied grote veranderingen nodig om met minder mensen minimaal hetzelfde te kunnen doen.

Traditioneel is automatisering bij de politie vooral gericht geweest op administratieve en registratieve processen. Dit heeft er niet toe geleid dat agenten minder tijd kwijt zijn aan het verwerken van aangiften, het opstellen van een proces-verbaal en het afhandelen van andere meldingen. Integendeel, er zijn juist veel administratieve lasten bijgekomen omdat steeds meer geregistreerd moeten worden vanuit een behoefte aan maakbaarheid. Kortom, de huidige automatisering is voornamelijk gericht op bestaande processen; wat vroeger op papier werd gedaan wordt nu via een app of via een registratiesysteem gedaan.

Er is echter een acute noodzaak om een andere manier van werken te adopteren. De tijd van stapsgewijs en vrijblijvend andere, innovatieve oplossingen bedenken is voorbij. Samenwerking in de ketens zal moeten veranderen om zinvol en effectief te zijn. In dit artikel stellen wij drie manieren van anders werken voor.

Dit zijn dé drie manieren waarop de politie het capaciteitsprobleem kan aanpakken:

1. Informatie Gestuurd Optreden
2. Een Snelkookpan Omgeving politie (SOP)
3. Digitale triage toepassen

1. Informatie Gestuurd Optreden

Het is helaas zo dat veel zaken niet worden opgepakt door gebrek aan capaciteit waardoor het vertrouwen van de burger in de politie op termijn afneemt. Doordat de pakkans afneemt, neemt de criminaliteit toe. Beide gevolgen zijn desastreus en zorgen voor een negatieve spiraal.

Traditioneel is de manier om meer misdaad op te lossen het inzetten van meer mensen. Wanneer dat niet mogelijk is vanwege schaarse capaciteit, is het alternatief om in te zetten op andere manieren van misdaden oplossen of zelfs nog beter, om misdaden te voorkomen. Eén van die manieren is Informatie Gestuurd Optreden (IGO). Op deze manier optreden start met de basis en dat is Informatie Gestuurd Werken.

Informatie Gestuurd Werken (IGW) is het gebruiken van data om het primaire proces bij de politie beter, sneller en effectiever te laten verlopen. Het komt er op neer dat je op basis van beschikbare data beslissingen neemt, zoals in de dagelijkse operatie mensen of teams inzetten op basis van de uitkomsten van data-analyses. Voorbeelden hiervan zijn PredPol en CAS (Criminaliteits Anticipatie Systeem in gebruik bij de Eenheid Amsterdam). Met behulp van IGW[3] kun je dus slimmer omgaan met de al beschikbare data en daarmee een betere informatiepositie verkrijgen, waardoor je:

- Sneller en beter kunt reageren (wendbaarheid);
- beter kunt sturen op resultaten en de samenhang (effectiviteit);
- meer resultaten kunt leveren tegen lagere kosten en met een kortere doorlooptijd (efficiëntie);
- beslissingen beter kunt onderbouwen (transparantie);
- betere keuzes kunt maken (beleidsontwikkeling).

Nu is de politie traditioneel al een organisatie die heel veel informatie verzamelt. Zo wordt elke melding die bij de politie binnenkomt vastgelegd, samen met de acties op de melding. Bij het opmaken van een proces-verbaal worden alle benodigde gegevens nauwkeurig vastgelegd en in grotere onderzoeken worden vele meters aan dossiers gevuld met informatie. Tel daar alle informatie bij op die wordt verzameld op basis van sensoren (zoals camerabeelden, ANPR-registraties, interceptie van telefoongesprekken en internetgebruik) en er ontstaat een beeld waarbij een heleboel data bij kan dragen aan het oplossen van misdaad in ons land[4].

Hierbij moet ook niet het belang van uitwisseling met ketenpartners (zoals de Kmar, gemeenten, veiligheidsregio's etc.) worden onderschat. Op dit moment wordt er nog maar mondjesmaat informatie uitgewisseld maar ook hier kan het delen van meer informatie zorgen voor nieuwe inzichten.

De kunst is nu om met behulp van moderne technologie deze data te verwerken, te interpreteren én er sturingsinformatie uit te halen ten behoeve van de operatie. De politie is al langer bezig om de mogelijkheden van Business Intelligence & Analytics (BI&A) te onderzoeken. Er is echter nog geen overkoepelende visie en aanpak om IGW door de hele organisatie heen te operationaliseren en op basis van deze analyses informatie gestuurd te gaan optreden (IGO).

2. Snelkookpan Omgeving Politie (SOP)

Wendbaarder worden om met steeds sneller gaande veranderingen mee te gaan is een belangrijke reden waarom organisaties wereldwijd anders gaan werken. Echter, organisaties in het veiligheidsdomein zoals de politie werken vaak nog op een traditionele manier. Het wordt tijd dat de politie slimmer gaat samenwerken. Ook al kunnen technologische innovaties het veiligheidsdomein in staat stellen om efficiënter te werken, de uitdaging blijft om mensen bereid te krijgen om deze ook daadwerkelijk in te zetten, schreven Daalmijer en Bruin al in hun artikel over elektronisch ondertekenen[5]. De manier waarop er samengewerkt wordt in het veiligheidsdomein kan efficiënter en effectiever. Ondanks dat er al veel technologie beschikbaar is om processen te versnellen, blijft de organisatie achter. Het daadwerkelijk inzetten van nieuwe technologieën vergt wel een totaal andere mindset en de bereidheid om te leren.

Om nieuwe technologieën te ontwerpen en realiseren stellen wij een snelkookpan voor. Hierin worden kleine en wendbare teams van professionals ondersteunt door business- en data analisten en softwareontwikkelaars. Die teams werken samen om oplossingen te ontwikkelen die morgen al ingezet kunnen worden. Een dergelijke snelkookpanomgeving moet worden voorzien van de benodigde tooling en state-of-the-art ICT-voorzieningen. Er moet daarbij ook een fysieke omgeving gerealiseerd worden waarin deze partijen gefaciliteerd worden om met elkaar samen te werken en resultaten te boeken.

De resultaten uit deze snelkookpanomgeving moeten getoetst worden in de praktijk binnen bestaande basis- of onderzoeksteams. In de vorm van kortlopende pilots kunnen de resultaten snel gevalideerd worden. Als de pilot succesvol is dan kunnen de resultaten overgedragen worden aan de IV-organisatie die de ontwikkeling van de oplossing verder vormgeeft en uitrolt in de politieorganisatie. Als een pilot niet succesvol is moeten de uitkomsten terug de snelkookpan in en kan er, na een goede analyse, een volgende poging worden gedaan. Lukt het dan nog niet dan moet de ontwikkeling gestaakt worden.

Wij denken dat op deze manier processen versneld worden, en belangrijker nog, dat met behulp van snelle oplossingen in een SOP het mogelijk wordt om met minder mensen meer zaken te behandelen én op te lossen.

3. Digitale triage gaan toepassen

Als je buiten normale kantooruren spoedzorg nodig hebt, ga je naar de huisartsenpost. We zijn gewend dat we dan eerst even moeten bellen om een afspraak te maken. De goed opgeleide assistente aan de andere kant van de lijn bepaalt dan hoe spoedeisend jouw klacht is. Afhankelijk daarvan krijg je een afspraak op de post. In de zorg is daar een bekend begrip voor: triage. Het is het proces dat wordt gebruikt om onnodige druk op hulpverleners te voorkomen door hulpvragen te kanaliseren en waar nodig meteen door te verwijzen naar de juiste specialist. Het belangrijkste doel is het vinden van de juiste balans tussen veiligheid en efficiëntie: de middelen in de zorg eerlijk verdelen aan degenen die het nodig hebben.

In de zorg wordt nu geëxperimenteerd met digitale triage[6]. In plaats van telefonische assistentie praat je dan met een chatbot die jou op afstand kan adviseren, doorverwijzen of een afspraak voor je inplant. Er is een vergelijking te trekken tussen de uitdaging in de zorg en die in het veiligheidsdomein: veel vragen verwerken met een beperkte capaciteit. Als we naar de politie kijken, dan speelt deze uitdaging door de hele organisatie. Of het nu gaat om het rijden van een spoedhulpdienst of welke onderzoeksmiddelen worden ingezet door de recherche. Het oplossingspercentage van de politie ligt al jaren rond de 25%[7]. Dit percentage kan verbeterd worden als de politie gerichter inzet op die zaken die een hoger oplossingspotentieel hebben. Digitale triage, op basis van het vergelijken van data kan dit potentieel berekenen en helpen om een beredeneerde keuze te maken welke zaken onderzocht gaan worden. Of, in een extremer geval, die keuze voor je maken. Dat scheelt mensenwerk en voorkomt dat er 'op gevoel' keuzes gemaakt worden die in theorie niet per se de voorwaarden hebben om opgelost te worden. Daarnaast gaat triage er ook over dat vragen door de juiste persoon/afdeling worden opgepakt, wat dubbel werk voorkomt.

Het invoeren van triage kan op allerlei vlakken van het politiewerk. Feit is wel dat hiervoor de juiste software ontwikkeld moet worden en dat er een duidelijk proces ingericht moet worden. Dat is natuurlijk een complex vraagstuk, waar verschillende stakeholders bij betrokken moeten worden zodat er ook voldoende draagvlak is voor de oplossing. En dat kan dan weer perfect in de eerder beschreven SOP.

Afsluiting

De politie heeft een enorme capaciteitsuitdaging en deze wordt alsmaar groter door onder andere demografische ontwikkelingen. De uitdagingen zijn zo groot, dat incrementele, stapsgewijze aanpassingen de problemen niet kunnen oplossen. Er is een compleet andere manier van denken en doen nodig. Door op korte termijn echt Informatie Gestuurd te gaan werken en op te treden, door in een snelkookpan nieuwe technologieën echt te realiseren en door digitale triage toe te passen kan de politie vernieuwen. De politie zal zo in staat zijn om de uitdagingen aan te gaan en anders, maar vooral efficiënter en effectiever te gaan werken en daardoor Nederland veilig te houden.

Over de auteurs

jeroen.oosterwal@capgemini.com

Ing. Jeroen Oosterwal is Principal Consultant bij Capgemini. Jeroen is werkzaam als Architect en Business Developer bij de marktgroep Openbare Orde en Veiligheid.

lisa-marie.brouwer@capgemini.com

Lisa Marie Brouwer is werkzaam bij Capgemini Invent en ontwerpt en faciliteert interactieve werksessies waar complexe multi-stakeholder uitdagingen worden opgelost.

[1]Volkskrant 29 november 2017. "Groot tekort aan agenten dreigt: komende jaren 14.000 politiemensen met pensioen."

[2]https://nos.nl/artikel/2330816-politieopleiding-een-jaar-korter-in-strijd-tegen-tekort-aan-agenten.html

[3]https://www.trendsinveiligheid.nl/rapport/2019-slimmer-samenwerken-aan-een-veiliger-nederland/effectief-informatiegestuurd-werken-igw-in-een-wereld-met-5g-sensing/

[4]De auteurs doen hier geen uitspraken over de beperkingen die mogelijk worden opgelegd vanwege wet- en regelgeving.

[5]https://www.trendsinveiligheid.nl/rapport/2019-slimmer-samenwerken-aan-een-veiliger-nederland/elektronisch-ondertekenen-een-kleine-stap-in-techniek-een-grote-sprong-voor-de-strafrechtketen/

[6]Voorbeeld: https://praktijkvoorbeeldenanw.lhv.nl/nieuwe-pilots/nieuwe-pilots/zelftriage-met-een-chatbot

[7]https://www.politie.nl/nieuws/2018/maart/1/veiligheidsgevoel-verbetert-misdaadcijfers-dalen.html

Kennis en kansen van artificial intelligence in het veiligheidsdomein

Tussen science en fiction: welke stappen moet het Nederlandse veiligheidsdomein ondernemen om vertrouwd en veilig artificial intelligence (AI) toe te passen?

Highlights

- Artificial intelligence (AI) is voor velen nog nieuw en onbekend - en het onbekende is eng.
- AI is alles wat machines nog niet kunnen.
- Nuanceer 'science' en 'fictie' van AI.
- Spiegel performance van AI met performance van de mens.
- Zet in op kennis en voorkom een digital skill gap.

Auteurs
Mehrnaz Pour Morshed
Jasper van Buren
Marijn Markus

Trends in Veiligheid 2019 beschreef hoe artificial intelligence (AI) geen hype meer is, maar blijvende technologie. Ook de Covid-19 pandemie toont de waarde van data, algoritmes en AI voor de veiligheid van onze samenleving. Overheden en ketenorganisaties, met name in het veiligheidsdomein, experimenteren internationaal met toepassingen van AI. Het gaat dan om toepassingen zoals beeldherkenning, fraudedetectie en criminaliteitvoorspellingen. Ontwikkelingen van nieuwe technologie als AI wekken echter ook onzekerheid en angst op onder de bevolking. AI is voor velen nog nieuw en onbekend. Het onbekende is eng, zeker als dit zowel het persoonlijke leven van burgers als de nationale veiligheid beïnvloedt. Dit wordt versterkt door verhalen in de media over AI-toepassingen die bijvoorbeeld inbreuk maken op privacy – zoals het inzetten van gezichtsherkenning om burgers te monitoren in China. Daarom is het binnen Nederland des te belangrijker dat de overheid introductie en adoptie van AI binnen het veiligheidsdomein in goede banen leidt.

Het publieke debat over AI wordt gevoerd door twee tegenpolen. Enerzijds is technologie als AI noodzakelijk om de samenleving veiliger te maken. Anderzijds heerst de angst dat AI onze vrijheid en veiligheid beperkt – hetzij door privacy-schendende multinationals, hetzij via big brother-achtige overheden. De werkelijkheid is complexer. Nuance verdwijnt wanneer de bevolking dagelijks wordt gebombardeerd door Hollywood films en (AI-gestuurde) media. Om nog maar te zwijgen over misinformatie en doemscenario's over het Corona virus of alle misinformatie omtrent Corona Apps en hun mogelijke werking. Slecht nieuws krijgt nu eenmaal meer aandacht. Door alle verhalen over algoritmes en 'foute' AI die onze vrijheid en veiligheid bedreigen is het moeilijk de science van de fictie te onderscheiden.

> **AI als spiegel van de mens: een set aan technieken om het menselijk denken en doen na te bootsen."**

Artificial intelligence is een snel ontwikkelende tak van wetenschap, gericht op het ontwikkelen van algoritmes en machines die menselijk gedrag kunnen nabootsen. Doorbraken in machine learning en data-opslag stellen ons in staat om slimme algoritmes te ontwikkelen. Veel organisaties (publiek en privaat) binnen het veiligheidsdomein passen deze technologieën dagelijks toe om processen te optimaliseren, te voorspellen en kosten te besparen.

Het is belangrijk dat we ons realiseren dat AI werkt op basis van data(sets) en algoritmes – beiden worden door mensen geproduceerd. Met deze data en algoritmen kunnen machines menselijk gedrag nabootsen, zie het als een digitale medewerker.

AI leert snel door goede data, maar deze afhankelijkheid heeft ook een keerzijde. Zonder data van voldoende kwaliteit én kwantiteit zal een AI-toepassing niet erg nauwkeurig zijn. AI bevat in de beginfase veel kinderziektes. Wanneer ingevoerde data bijvoorbeeld niet volledig of representatief is, zie je al snel dat AI tot discriminerende resultaten komt. Dit is extra problematisch binnen het veiligheidsdomein, vanwege de gevoelige data en de impact op het individu. Dergelijke berichten leiden tot wantrouwen in de samenleving. De oorzaak van dit probleem ligt echter niet in de technologie, maar in de (mogelijk onethische) toepassing ervan door mensen.

Ontwikkelaars én bestuurders moeten zich bewust zijn van ethische complicaties om de toepassing van AI te verbeteren en tegelijkertijd verwachtingen te managen. Enerzijds dient de performance van AI goed gemonitord te worden. Dit kan bijvoorbeeld via het 'vier ogen principe', waarbij mensen de besluitvormingsprocedure van de machine controleren en verifiëren. Anderzijds dienen organisaties in het veiligheidsdomein te accepteren en te anticiperen op het feit dat AI fouten kan maken, zeker in het begin. Bovendien is AI nooit 100% foutloos, zoals mensen dat ook niet zijn.

Transparantie is een ander groot onderwerp binnen AI. Besluitvorming van AI over bijvoorbeeld de correctheid van je belastingaangifte, risicoprofielen voor fraude of het voorspelde brandgevaar van je woning, dienen verklaarbaar en uitlegbaar te zijn. Ook hier is AI te spiegelen met onszelf. Menselijke (of bestuurlijke) besluitvorming is vaak niet transparant maar achteraf wel uitlegbaar. Hetzelfde geldt voor AI, die beslissingen niet maakt op basis van regels (deterministisch) maar via kansberekeningen. Deze berekeningen zijn vaak moeilijker uit te leggen aan mensen dan een beslisboom. Een uitleg vergroot het vertrouwen en daarmee de acceptatie van AI door de gemiddelde burger. Evalueren hoe een AI presteert in vergelijking met de menselijke medewerker, met andere woorden wiens bias minder duidelijk is, nuanceert het debat. De vraag moet niet zijn hoe goed of slecht een AI-toepassing is, maar hoe goed de AI is in vergelijking met de mens.

Impact van AI op maatschappelijke veiligheid

Veel mensen vrezen dat AI een gevaar zal vormen voor de maatschappij. Maar momenteel speelt AI geen zichtbare rol in levensbedreigende situaties binnen het veiligheidsdomein[1]. Waar AI momenteel wél impact heeft is de economie en werkgelegenheid. Onrust en gebrek aan vertrouwen voorkomt investering in nieuwe technologie, maar juist hier kan het veiligheidsdomein niet achterblijven.

Door criminelen wordt steeds meer gebruik gemaakt van AI. Stel je voor dat ransomware alle ziekenhuizen in een land platlegt – zoals WannaCry in het Verenigd Koninkrijk deed in 2017[2]. Of denk aan de cybercriminelen die 220.000 euro buit maakten door stem en spraak van een CEO na te bootsen (Wall Street Journal, 2019[3]). Bedrijven tonen weinig initiatief om de markt en maatschappij over deze risico's in te lichten.

Informeren over risico's zoals datalekken, het binnendringen van accounts of het doorverkopen van persoonlijke data worden gezien als bijzaak. Dit maakt het gebrek aan 'awareness' over data, digitale veiligheid en AI in de maatschappij tot een groot probleem. Want het is diezelfde maatschappij die het grootste veiligheidsrisico loopt.

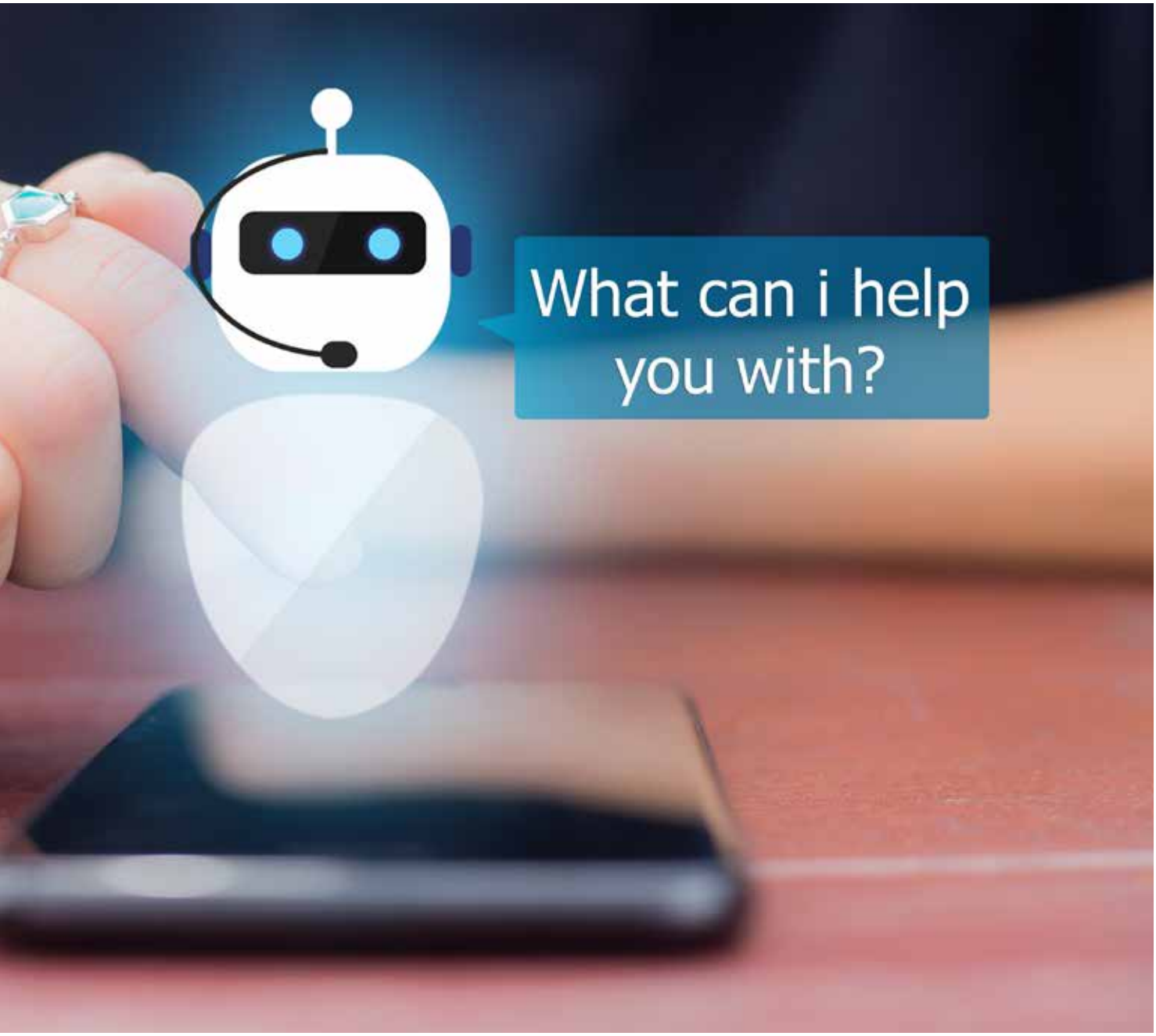
Het veiligheidsdomein dient hier het voortouw te nemen. Door preventief te communiceren en op te leiden (in samenwerking met academica) om bijvoorbeeld data- en security-bewustzijn te creëren en door in te grijpen wanneer dit fout gaat. In hedendaagse opleidingen zien we weinig data, statistiek of cybersecurity terugkomen. Terwijl de arbeidsmarkt hier wel steeds meer om vraagt. Dit 'digital skill gap' (het ontbreken van digitale vaardigheden in personeelsbestanden[4]) is een van de grootste uitdagingen voor het veiligheidsdomein én de maatschappij. Een goed voorbeeld hiervan is het grootschalig thuiswerken tijdens de Covid-19 pandemie, waarbij werknemers én bedrijven zonder digitale skills of middelen achterbleven.

Beeldvorming van AI in de samenleving

Wanneer AI ethisch de fout in gaat bereikt dit al snel het nieuws, zoals Tay, de chatbot van Microsoft die extreemrechtse leuzen aanleerde, of de recruitment engine van Amazon, die een voorkeur had voor blanke mannen. Goed functionerende AI krijgt weinig aandacht. In tegendeel: goede AI noemen we al snel geen AI meer, maar wordt deel van ons dagelijks bestaan. Zie: Google, het weerbericht en zelfrijdende auto's. "AI is alles wat machines nog niet kunnen", aldus Tesler (1979). Wat zou bijvoorbeeld de reactie zijn wanneer AI succesvol bosbranden

kan voorspellen waardoor de brandweer preventief kan handelen? Binnen een paar jaar zouden we er niet meer van opkijken.

In onze optiek heeft de maatschappij in plaats van focus op de buzz meer belang bij uitleg; over het functioneren van AI, het besluitvormingsproces en waar de besluiten op gebaseerd zijn. Enerzijds dient de besluitvorming van AI transparant en uitlegbaar te zijn aan zowel een CIO als een gewone burger. Anderzijds dient het begrip van AI binnen de maatschappij vergroot te worden. Alleen met een combinatie van deze twee elementen kunnen we AI een plaats geven in onze huidige samenleving en het imago van AI positief beinvloeden. Het is mede aan het veiligheidsdomein om de negatieve beeldvorming om te draaien: door frequenter en overtuigender de kansen van AI te laten zien en om nuance te aan te brengen. Geen zwart/wit discours, maar een maatschappelijk debat over hoe AI verantwoord in te zetten is. Op dezelfde manier als dat we eerder discussies voerden over de komst van technologie als radio, TV en het internet. Hier ligt een grote taak voor de Nederlandse overheid. De AVG, het AI-Actieplan van de Europese Commissie en de vele gratis digitale opleidingen aangeboden in quarantainetijd zijn stappen in de goede richting.



Nuancering van AI-ontwikkeling

Dit gaat niet alleen over AI, algoritmes en technologie maar ook over de mensen en bedrijven als Google en Amazon, of overheden zoals de VS en China. Enerzijds verwerpen we hoe bijvoorbeeld China via cameratoezicht AI toepast voor doeleinden als 'social ranking'. Anderzijds is de Nederlandse overheid zelfs in tijden van grootschalig thuiswerken niet in staat om sommige papieren processen te digitaliseren. Hierdoor ontstaat een breuk in de discussie over AI, tussen de mogelijkheden en de gevaren.

De technieken ingezet voor negatieve doeleinden, om te spioneren of rekruten te filteren, worden ook gebruikt om mensen te helpen zoals bij routeplanning, kankeronderzoek of het voorspellen van oogst voor boeren. Sterker nog, de AI-methoden om bijvoorbeeld rekruten te filteren (wat leidde tot discriminatie) waren oorspronkelijk juist ontwikkeld om discriminatie aan te tonen. Toch voert negatieve aandacht de boventoon, wat resulteert in een technofobische trend in de samenleving. AI heeft zowel kosten als baten die zorgvuldig geëvalueerd moeten worden. Maar het proces van technologische vooruitgang is niet omkeerbaar.

Ons advies

1. Faciliteer een brede discussie over AI en nieuwe technologie, waarin zowel de kosten als baten belicht worden. Juist hierdoor kan de maatschappelijke angst voor nieuwe technologie genuanceerd en deels weggenomen worden.

2. Overheden moeten inzetten op een goede interne (data) infrastructuur om de adoptie van nieuwe AI-technieken te versnellen. Dit is een investering voor de lange termijn. Veel (legacy) systemen binnen overheden zijn niet klaar voor nieuwe technologie als AI, zowel qua snelheid als datakwaliteit. Het updaten van zulke systemen gebeurt vaak reactief, bijvoorbeeld wanneer er grote persaandacht of onrust ontstaat. Wees proactiever. Op dit moment vormt het gebrek aan moderne ICT-infrastructuur de grootste bottleneck voor het adopteren van nieuwe AI-technieken binnen de overheid.

3. Investeer in het opleiden van intern personeel in de omgang met nieuwe technologie. Veel overheidsmedewerkers hebben weinig kennis van data, statistiek, cybersecurity of eenvoudige digitale skills. Dit vormt onderdeel van het digital skills gap: hoe om te gaan met niet-technisch personeel binnen een arbeidsmarkt die steeds meer technisch van aard wordt? Dit is een van de grootste uitdagingen voor de komende jaren.

4. Zowel leveranciers van software en technologie als afnemers moeten proactief handelen in het begrijpen van technologie en diens (veiligheids)risico's. Deel best practices en lessons learned! Ook is het de taak van de overheid om middelen als opleidingen en platformen beschikbaar te stellen. Samenwerking tussen overheid, verzekeraars, ontwikkelaars en afnemers is per slot van rekening cruciaal voor een veilig Nederland.

Conclusie

De AI-discussie wordt gevoed door te veel woorden en te weinig daden. Naast wetgeving en beleid is het van belang ook actief onderzoeksresultaten om te zetten in productie. Experimenten en 'Proof of Concepts' met AI hebben weinig betekenis voor de maatschappij totdat deze op schaal toegepast worden. Het verschil wordt gemaakt door ethische inzet van AI en het belichten van de kansen die het biedt. Technologie is een middel, geen doel op zich. Als mensen hebben wij vaak moeite met verandering en AI is hier ook onderdeel van. Zie erop toe dat AI goed ingezet wordt, voor de veiligheid van het individu én de maatschappij.

[1]https://www.security.nl/posting/644499/Grapperhaus%3A+AI+gaat+politieagenten+op+straat+niet+vervangen

[2]https://www.bbc.com/news/technology-41753022

[3]https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

[4]https://www.capgemini.com/nl-nl/bronnen/de-kloof-in-digitaal-talent-doen-bedrijven-voldoende/

Over de auteurs

mehrnaz.pour.morshed@capgemini.com

Mehrnaz Pour Morshed heeft een Msc in artificial intelligence en is werkzaam als cybersecurity consultant binnen Capgemini. Ze heeft veel interesse in het menselijk gedrag. Dit is een belangrijk en relevant thema in het cybersecuritydomein, waar zij zich graag bezighoudt met vraagstukken rondom beleid en gedrag. Tijdens haar project binnen een grote Europese luchthaven zet ze zich in voor een verhoogde digitale weerbaarheid van het ecosysteem van deze luchthaven. Om dit te kunnen realiseren werkt ze veel samen met lokale autoriteiten uit het veiligheidsdomein zoals de marechaussee maar ook met private partijen.

jasper.van.buren@capgemini.com

Jasper van Buren is actief binnen de Cybersecurity Unit van Capgemini en focust zich op het vergroten van digitaal vertrouwen (digital trust) in de samenleving. Daarbij richt hij zich op vraagstukken rondom de security, privacy en (data) ethiek van nieuwe technologieën en innovaties. Jasper helpt klanten bovendien bij het versterken van de organisatie om het digitaal vertrouwen ook op langere termijn te borgen. Cybersecurity levert hiermee toegevoegde waarde voor de organisatie.

marijn.markus@capgemini.com

Als AI Lead en senior data scientist is **Marijn Markus** al drie jaar een leider in de AI-inspanningen van Capgemini. Hij past zijn brede kennis van machine learning, menselijk gedrag en beleid toe binnen publieke, private en veiligheidsorganisaties in verschillende landen om inzicht te creëren met data. Daarnaast is Marijn actief als publiek spreker en zet hij zich in voor 'AI for Good' bij diverse NGO's.

Hoe grote gemeentes slim kunnen bijdragen aan een veiliger Nederland

Hoe zorgen we dat decentralisatie van verantwoordelijkheden op het gebied van openbare orde niet in de weg komt te staan van de informatievoorziening in de veiligheidsketen?

Auteurs
Joop Koster
Tijmen Patist
Wouter Bal

Decentralisatie van toezicht op Openbare Orde en Veiligheid leidt tot fragmentatie van informatie, waardoor een integraal veiligheidsbeeld kan verdwijnen.

Highlights

- Verantwoordelijkheden van de politie verschuiven steeds meer naar de gemeentelijke BOA's.
- Vastlegging van gegevens in gemeentelijke systemen doet afbreuk aan de vorming van een integraal veiligheidsbeeld.
- Een waardevollere en slimmere informatievoorziening kan leiden tot vroegtijdige inzicht en signalering, en mogelijke preventie van criminele activiteiten in de toekomst.
- Communicatie tussen de instanties blijft belangrijk. Vooral om informatie, kennis en 'buikgevoel' te delen omtrent potentiële delinquenten.

In de afgelopen drie decennia zijn in de grote steden handhavende diensten zoals parkeerpolitie, milieupolitie en stadswacht samengevoegd tot een overkoepelend orgaan: Handhaving, onder verantwoordelijkheid van de gemeente. De taken die toebehoren aan Buitengewone Opsporingsambtenaren (BOA's) in de gemeente zijn met de jaren steeds verder uitgebreid. In de grote steden hebben Handhavers Toezicht en Veiligheid de status van BOA's gekregen om zo meer middelen te hebben om hun taken goed uit te voeren.

De Handhavers Toezicht en Veiligheid dragen bij aan het handhaven van de openbare orde en veiligheid binnen de gemeente waarbij zij de Politie ontlasten[1]. Dit houdt in dat zij vaak betrokken zijn bij mistanden in de wijken en buurten van een stad in plaats van de Politie. Het gevolg hiervan kan zijn dat de handhavers een beter beeld hebben van de zaken die spelen in bepaalde buurten of wijken van een stad dan de politie. In dat geval zullen zij degene zijn die de verschillende veiligheidsfenomenen zoals radicalisering, drugsgebruik/handel en overlast in de wijken en buurten beter in beeld hebben en wie daarbij betrokken zijn. Dit soort overlast beperkt zich meestal niet enkel tot de leefomgeving van deze personen maar zijn gemeentegrensoverschrijdend.

In steden zoals Rotterdam, Amsterdam en Utrecht heeft de Handhaving een eigen registratiesysteem waarin zij informatie opslaan. Het gebruik van verschillende systemen zonder onderlinge koppelingen zorgt voor een fragmentatie van de vastgelegde informatie over gebeurtenissen en de betrokken perso(o)n(en). Het gevolg hiervan is dat het lastiger wordt om tijdig te signaleren dat er een interventie nodig is voor iemand. Terwijl juist het vroeg signaleren van de samenloop van bepaalde gebeurtenissen rondom een persoon van groot belang is om tijdig in te kunnen grijpen in de ontwikkeling van een criminele loopbaan.

Wat is het belang van het vroeg signaleren?

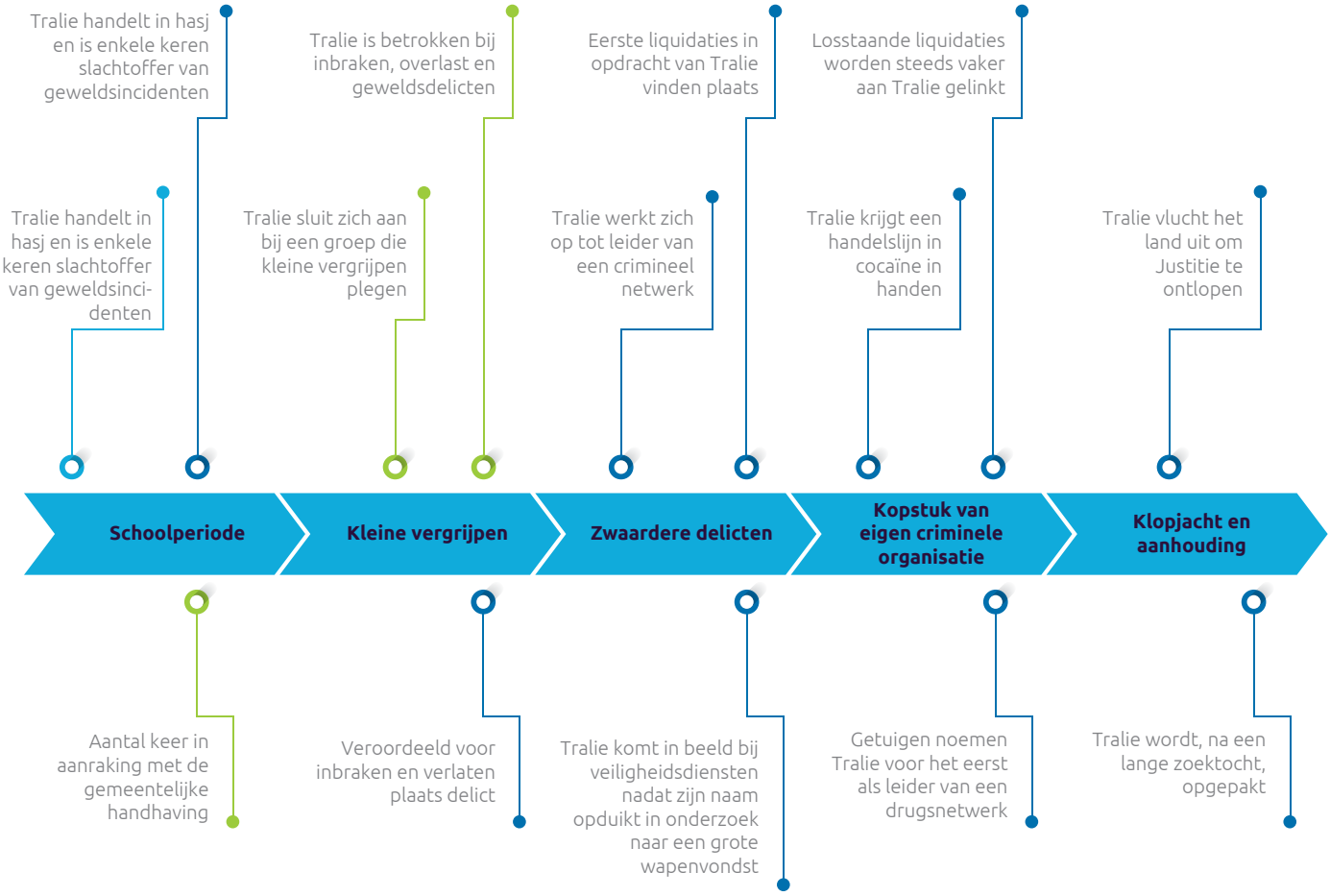
Laten we stellen dat een potentiële crimineel in Nederland wordt geboren. Remi Tralie groeit op in de het midden van het land. Hij heeft een handeltje in hasj, maar wordt vaak in elkaar geslagen door andere jongens. Hij sluit zich daarom aan bij een groep jongens met kwaad in de zin. Samen zetten ze de handel voort en raken ze betrokken bij kleine inbraken, overlast en geweldsincidenten. Pas later, als hij beetje bij beetje berucht wordt, duikt zijn naam op in verschillende onderzoeken. Uiteindelijk weet men hem in te rekenen, na de inzet van veel mankracht en financiën.

Remi is in zijn jeugd, in verschillende gemeentes, al een aantal keer in aanraking geweest met het gemeentelijk handhavingsapparaat. In de tijd dat hij in zijn eigen gemeente ingeschreven stond, beging hij al enkele kleine vergrijpen. Zo wordt hij eens aangesproken omdat hij met een groep rondhangt op straat, krijgt hij een waarschuwing na wildplassen tegen een kerk en worden in de buurt van zijn school meerdere meldingen gemaakt van geluidsoverlast. Op een bepaald moment besluit Tralie zich uit te schrijven bij de basisregistratie voor personen om zo minder op te vallen. Hoewel er verschillende vergrijpen op zijn naam staan in zijn eigen gemeente, is het voor andere gemeentes, bij nieuwe incidenten, niet te achterhalen wat deze voorgeschiedenis inhoudt.

Omdat de incidenten los staan van elkaar, wordt hij telkens weer uit het oog verloren. Telkens een andere ambtenaar die zijn zaak behandelt, en ja, dan weet je het wel. Het verhaal staat toch in het systeem waar híj mee werkt? Geen reden om daar meer aandacht aan te besteden. Maar wat hij niet wist, en misschien ook wel niet had moeten weten, om de simpele reden dat het niet bij zijn taakomschrijving hoort, is dat Remi zal uitgroeien tot de moorddadige leider van een criminele organisatie. Juist in de fase waarin de ontwikkeling naar deze zware criminaliteit plaatsvindt, kan nog veel gewonnen worden door informatie centraal en eenduidig te verzamelen. Wellicht kan daarmee de volgende Tralie op tijd geïdentificeerd worden en preventief worden opgetreden.

Zoals blijkt uit bovenstaande fictie, zijn er veel aspecten aan de levensloop van een crimineel die vroege aanwijzingen kunnen geven van serieuzere vergrijpen. En dan kunnen we dat als samenleving maar beter op tijd doorhebben.

Figuur 1: Incidentengeschiedenis en verloop.



De toekomst van informatievoorziening

De huidige opslag van 'handhavingsinformatie' door de verschillende instanties en organisaties is erg versnipperd. Informatie ligt vast in meerdere en van elkaar verschillende systemen. Het gaat hier om systemen die soms erg verouderd zijn en in bepaalde gevallen zelfs niet meer voldoen aan de huidige wetgeving. Ook de wijze van vastlegging loopt uiteen van ongestructureerd in een document of bestand (denk hierbij aan brieven, geluidsfragmenten en beeldopnames en dergelijke) tot gestructureerd in een applicatie, in de vorm van velden en transacties.

Dit alles opgeteld maakt het erg complex, zo niet onmogelijk, om relevante informatie tussen de verschillende diensten te delen. Veel situationele kennis omtrent een gebeurtenis en de gerelateerde omstandigheden en personen gaat hierdoor verloren. Gezamenlijke diensten verliezen daarmee inzicht- en preventiemogelijkheden bij latent groeiende criminele activiteiten. We missen hier zicht op potentieel betrokken (veel)plegers en het ontstaan van nieuwe criminele organisaties. De decentralisatie van bepaalde vormen van 'handhaving' naar gemeentes kan dit probleem alleen maar groter maken maar tegelijkertijd ook een kans bieden om hier verbetering in aan te brengen. Als er meer ogen bijkomen in de vorm van handhavingsdiensten kan er, mits centraal en op gecoördineerde wijze gedocumenteerd, een beter integraal veiligheidsbeeld worden gevormd bij delinquenten.

De vraag is: hoe zorgen we bij gedecentraliseerde verantwoordelijkheden van gemeentes dat versnipperde registraties van gebeurtenissen en betrokken personen worden tegen gegaan?

Daarbij: op welke manier kunnen we dit doen zodat informatie beter en vertrouwelijk met elkaar gedeeld kan worden zonder de privacy- en securitywetgeving te overtreden?

De huidige wetgeving rond privacy is gebaseerd op de rechten van een persoon en laat vrije uitwisseling niet zomaar toe. Persoonsgegevens mogen pas gedeeld of uitgewisseld worden als er voldoende aanleiding of reden toe is. Dat is goed en dat moet ook zeker zo blijven. We moeten niet in een situatie komen die vergelijkbaar is met de tijden van de Koude Oorlog waarin de overheid van het voormalig Oost-Duitsland voor iedere burger een persoonlijk dossier bijhield (Big Brother is watching you). Maar hoe dan wel?

Van kattenkwaad tot zwaar delict

Een oplossing is een centrale vastlegging waarbij de verantwoordelijkheid decentraal kan worden ingeregeld. Bij het vastleggen moet de focus in eerste instantie op gebeurtenissen komen te liggen en minder op personen. Bij gebeurtenissen speelt privacy een minder grote rol en mogen zonder al te veel regels worden gedeeld. Belangrijk uitgangspunt is wel dat de gebeurtenissen en de bijbehorende omstandigheden eenduidig, consistent maar vooral regionaal of nationaal worden vastgelegd waardoor ze eenvoudig(er) breed gedeeld kunnen worden over de gehele keten. De gebeurtenis-gerelateerde persoonsgegevens die immers ook vastgelegd dienen te worden, zijn hierin secundair en ondergeschikt, en mogen alleen ingezien worden door diegene of die instantie (gemeente, politie en dergelijke) die ze heeft vastgelegd en daartoe gemachtigd is. Ook voor de registratie van de gebeurtenis-gerelateerde persoonsgegevens en de relatiegegevens tot de gebeurtenis geldt dat deze in dezelfde centrale omgeving eenduidig en consistent wordt vastgelegd. Hierdoor wordt het mogelijk om met nieuwe en moderne technologie gebeurtenissen met elkaar in verband te brengen. Bijvoorbeeld door een analyse gebaseerd op artificial intelligence (AI) kunnen onderlinge gebeurtenis relaties, patronen en/of 'trends' worden gedetecteerd die de moeite zijn om nader te onderzoeken.

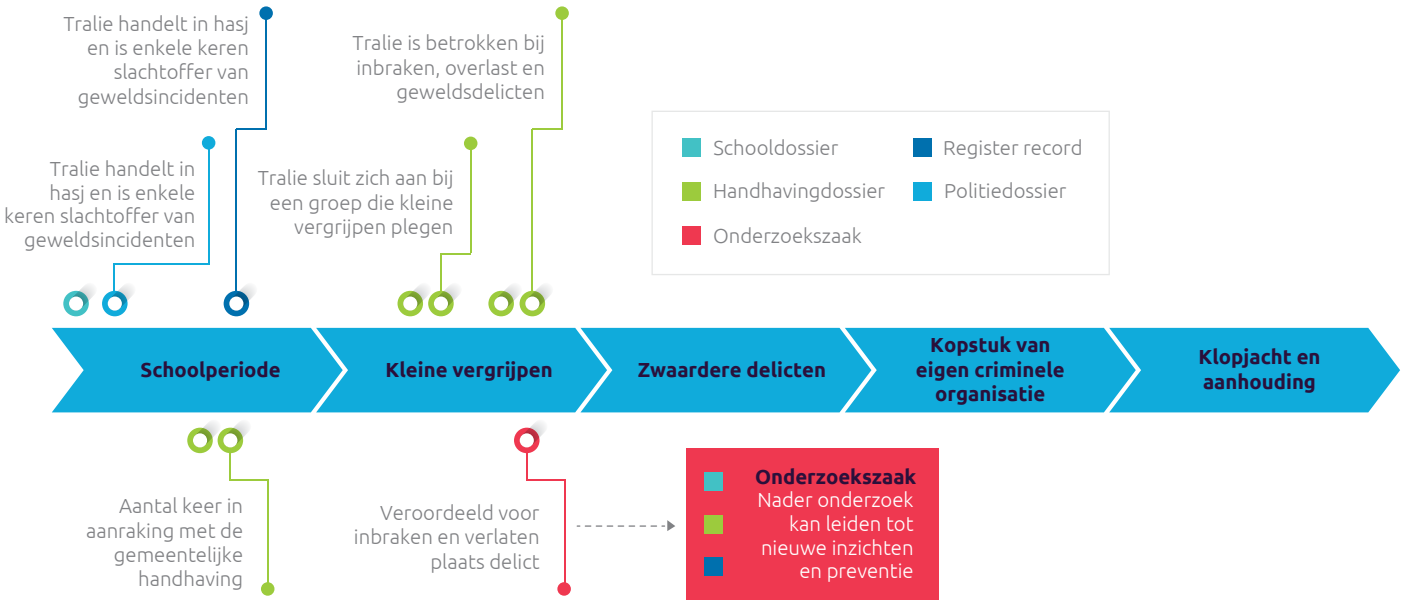
Er kunnen meerdere redenen zijn waarom gebeurtenissen met elkaar in verband gebracht worden. Een combinatie van één of meerdere gebeurtenissen kan leiden tot één of zelfs meerdere zaken. Verschillende en/of combinatie van analyses kunnen aanvullend leiden tot bepaalde notificaties/signalen dat bepaalde instanties met elkaar om de tafel moeten (veiligheidshuizen).

Een voorbeeld uit het leven van Remi Tralie. In de jongere jaren van Remi hebben een aantal gebeurtenissen plaats gevonden die los van elkaar zijn vastgelegd (zie de groene punten in onderstaande afbeelding) in verschillende gemeentes. Bij een centrale vastlegging zou middels analyse(s) de gebeurtenissen kunnen worden gebundeld. Deze analyses kunnen zowel handmatig (bijvoorbeeld met een netwerkanalyse) als automatisch (AI) worden uitgevoerd. Aansluitend kan dan een onderzoekszaak worden geïnitieerd, waarbij door middel van notificaties de verschillende instanties op de hoogte worden gebracht om in overleg te gaan.

De uitkomst van het overleg tussen de instanties kan voldoende aanleiding en meer bevoegdheid geven tot nader onderzoek waarbij ook meer persoonsgegevens (gemeente registers, politiedossiers etc.) kunnen worden uitgewisseld en of geanalyseerd.

De hierboven beschreven situatie biedt stappen naar een waardevolle en slimmere informatievoorziening, die kan leiden tot vroegtijdige inzicht en signalering, en mogelijke preventie van criminele activiteiten in de toekomst.

Figuur 2: Vroegtijdige signalering en inzichten ten behoeve van preventie.



Conclusie

Door decentralisatie van de verantwoordelijkheden rondom handhaving worden misstanden in de openbare ruimte geregistreerd op gemeentelijk niveau. Dit zorgt voor een fragmentatie van informatie tussen de verschillende gemeentes, wat kan leiden tot het uiteenvallen van het integrale veiligheidsbeeld. Door eenduidig en op nationaal niveau te registreren kan een beter integraal veiligheidsbeeld in stand worden gehouden.

Bronnen

https://www.politie.nl/themas/buitengewoon-opsporingsambtenaar.html

https://haagsehanden.nl/mensen-weten-niet-dat-handhavers-veel-bevoegdheden-hebben

https://www.rotterdam.nl/wonen-leven/handhaving/

https://www.amsterdam.nl/bestuur-organisatie/organisatie/stadsbeheer/toezicht-handhaving/

Over de auteurs

joop.koster@capgemini.com

Joop Koster is een Solution Architect met meer dan 25 jaar ervaring in het implementeren van bedrijfssystemen in verschillende industrieën, met een specialisatie in basisvoorziening-oplossingen in de openbare orde en veiligheidsdomein. Zijn thought leadership is ontstaan uit vele interacties met politie- en inlichtingenorganisaties wereldwijd.

tijmen.patist@capgemini.com

Tijmen Patist is business analist in het veiligheidsdomein, waar hij zich binnen de Community of Practice Intelligence specialiseert in Informatie Gestuurd Werken en intelligence. Verder werkt hij met verschillende partners van Capgemini aan het versterken van hun processen op gebied van crisisbeheersing en gegevensbescherming.

wouter.bal@capgemini.com

Wouter Bal is Business Analist met ervaring bij (inter)nationale veiligheidsdiensten en toezichthouders. Zijn focus ligt hierbij op Informatie Gestuurd Werken en intelligence in het domein van openbare orde en veiligheid.

Om te kunnen verdedigen, moet je weten hoe je aanvalt!

Hoe kunnen we ons wapenen tegen geavanceerde cybercriminaliteit?

Highlights

- Bestrijden van cybercriminaliteit vereist een offensieve beveiligingsstrategie.
- Detectie van de communicatie van cybercriminelen is de sleutel tot preventie en opsporing van cybercriminaliteit.
- Weerbaarheid tegen cybercriminaliteit vraagt om concrete observatie en aanvalssimulaties.

Auteurs
Henk Brandon
Jameel Nabbo

In de afgelopen jaren is de manier waarop cybercriminelen te werk gaan sterk geëvolueerd. De snelheid waarmee zij tegenwoordig opereren is vooral te danken aan de financiële en technologische middelen die de cybercriminelen inmiddels tot hun beschikking hebben. In het huidige digitale landschap zijn cybercriminelen zwaarbewapend met geavanceerde tools en technieken, zoals Golden Tickets[1], Fully Undetectable Crypters[2] en Domain Fronting[3], waardoor moeilijk te achterhalen is wie er achter een aanval zit. Tevens opereren cybercriminelen veelal van buiten de landsgrenzen, waardoor de invloed en bevoegdheid van de Nederlandse politie en justitie beperkt is. Dit maakt het erg moeilijk om cybercriminaliteit effectief aan te pakken.

Voor de aanpak van cybercriminaliteit is het belangrijk om werkwijze en aanvalspatronen te (her)kennen. Het is daarom zaak om inzicht te hebben (en houden) in de methoden en technieken die cybercriminelen gebruiken. In dit artikel lichten we toe waarom het belangrijk is om een offensieve beveilgingsstrategie te hanteren. Een offensieve beveiligingsstrategie biedt ondersteuning bij het opsporen van cybercriminelen en bij het herkennen, verstoren en voornamelijk voorkomen van geavanceerde digitale criminele activiteiten. In dit artikel bieden we handvatten waarmee veelvoorkomende digitale criminele activiteiten actief kunnen worden bestreden, zoals het ongeautoriseerd verkrijgen van toegang tot vertrouwelijke gegevens, het uitvoeren van op maat gemaakte ransomware-aanvallen en het besmetten van computernetwerken met schadelijke software.

Aanval is de beste verdediging

Tegenwoordig is het vrij eenvoudig om, waar dan ook ter wereld, cyberaanvallen te starten en organisaties binnen onze landsgrenzen aan te vallen. In een toespraak zei secretaris Kelly van het George Washington University Center for Cyber and Homeland Security dat een van de grootste bedreigingen voor cybersecurity kwam van Transnationale Criminele Organisaties (TCO's). "Als je een terrorist bent met een internetverbinding, zoals die op je altijd aanwezige mobiele telefoon, kun je met slechts een paar klikken nieuwe soldaten rekruteren, aanvallen plannen en een video uploaden waarin wordt opgeroepen tot een terroristische aanval"[4]. Overigens kunnen deze organisaties ook in opdracht werken van statelijke actoren die digitale middelen inzetten om geopolitieke en economische doelstellingen te behalen ten koste van Nederlandse belangen[5].

Deze aanvallen kunnen ook nog eens grote impact hebben en komen de laatste jaren steeds vaker voor. De meest recente randsomware-aanval in Nederland staat nog vers in ons geheugen. In december 2019 werd de Universiteit Maastricht zwaar getroffen door de Clop-ransomware[6]. Volgens de universiteit heeft de aanval “een ernstige inbreuk gepleegd op de ICT-systemen van de universiteit en daarmee de continuïteit van de instelling onder druk gezet”.

Net als een misdaad in de fysieke wereld doorloopt ook een ransomware-aanval de volgende drie basis-stappen: activiteiten vóór de aanval, tijdens de aanval en na de aanval. Daarom is het vroegtijdig detecteren van criminele communicatie en het verzamelen van bewijsmateriaal de sleutel tot het mogelijk voorkomen van (digitale) aanvallen. Daar staat tegenover dat het verzamelen van deze informatie steeds moeilijker wordt. Dit omdat cybercriminelen zeer geavanceerde communicatietechnieken gebruiken om hun sporen te verbergen, zoals anonimiseren, steganografie[7], verduistering, maskerade[8] en codering. Om cybercriminelen vroegtijdig op te sporen is het essentieel om je te verdiepen in offensieve beveiligingstechnieken. Hierdoor krijg je inzicht in waar, hoe en wanneer een crimineel toe wil of kan slaan.

Wat is offensieve beveiliging?

Met offensieve beveiliging kruip je als het ware in de huid van een cybercrimineel. Met een criminele mindset verdiep je je in de wereld van malware-ontwikkeling en het gebruik van cryptografie in de communicatie. Kortom, middels offensieve beveiliging heb je beter inzicht in de werkwijze van de cybercriminelen. Hiermee vergaar je informatie over hoe cybercriminelen stap voor stap hun aanval voorbereiden en uitvoeren. Met deze informatie kan je passende tegenmaatregelen nemen en eventueel overgaan tot politieke attributie.

Offensieve beveiliging is tevens een proactieve benadering om de computersystemen van de eigen organisatie te testen door georganiseerde aanvallen en technieken van een indringer te simuleren. En hierbij vanuit een hackersmentaliteit de zwakke punten en de kwetsbaarheden in de systemen en technologieën van de organisatie te ontdekken.

Om als een cybercrimineel te kunnen denken is het belangrijk om onderscheid te maken tussen reguliere offensieve beveiligingsactiviteiten en cybercriminele offensieve beveiligingsactiviteiten. De eerste categorie wordt vaak aangeduid als ethische hackers met een 'white hat-mentaliteit'. De ethische hacker gaat middels zogenaamde penetratietesten op zoek naar kwetsbaarheden in de systemen. Deze heeft hiervoor toestemming van de betreffende organisatie en zal geen schade veroorzaken.

De tweede categorie zijn de ethische hackers met een 'black hat-mentaliteit'. De black hat-mentaliteit houdt in dat deze hackers net als cybercriminelen (binnen de wettelijke bevoegdheden) acties uitvoeren die gericht zijn op financieel of politiek gewin of het verstoren en ontwrichten van de organisatie of samenleving. Ze doen dit echter zonder daadwerkelijk verstoringen te veroorzaken of zaken kapot te maken. Met andere woorden, ze gaan te werk als een cybercrimineel zonder het veroorzaken van schade en met medeweten van de beveiligingsmedewerkers van de betreffende organisaties.

Hoe offensieve beveiliging kan helpen

Door dezelfde activiteiten, middelen en technieken te gebruiken als cybercriminelen kun je je beter wapenen tegen hen en digitale criminaliteit vroegtijdig signaleren. De drie belangrijkste activiteiten die wij zien voor offensieve beveiliging zijn:

1. Social engineering: deze activiteit is gebaseerd op het testen van menselijk gedrag en zwakte door het ontwikkelen van aanvalscenario's. De aanvalscenario's worden op gecontroleerde wijze ingezet tegen de medewerkers van een organisatie. Voorbeelden van social engineering-activiteiten om vertrouwelijk informatie te verzamelen zijn: phishingaanvallen via e-mail, nabootsing van identiteit, proberen toegang te verkrijgen tot afgesloten ruimtes en telefoongesprekken voeren met werknemers.

2. Penetratietesten: het doel van een penetratietest is om voor een beperkte scope in een beperkte hoeveelheid tijd zoveel mogelijk kwetsbaarheden, exploits, configuratieproblemen en risico's in systemen te ontdekken.

3. Red teaming: een red teambeoordeling lijkt sterk op een penetratietest. De activiteiten van een red team gaan echter niet alleen over het vinden van kwetsbaarheden en exploits, maar ook om de detectie- en responsmogelijkheden van een organisatie te testen bij het simuleren van real-world aanvallen.

Om je op weg te helpen met het opzetten van een offensieve beveiliging strategie, geven wij hieronder vijf uitgangspunten.

1. Zorg ervoor dat iemand binnen de organisatie beschikt over de kennis en vaardigheden om malware te reverse-engineeren: het demonteren van de malware. Hierdoor kun je kijken wat de malware doet en welke systemen het beïnvloedt. Alleen door de details te kennen, kun je tot een oplossing komen die de beoogde schadelijke effecten verminderen en kom je erachter waarvoor de malware is ontworpen en welke kwetsbaarheden het wilde misbruiken.

2. Ontwikkel een cybersecuritylab: een faciliteit voor innovatief en experimenteel onderzoek naar kwaadaardige software en netwerkverkeerinspectie waar je een virtuele omgeving kunt bouwen. Hier kun je experimenteren met de effecten van malware op verschillende systemen.

3. Gebruik bronnen zoals de Dark-web-zoekmachines en .onion-domeinen. Voorbeelden zijn Torch en DuckDuckGo. Dit zijn zoekmachines voor het niet standaard toegankelijke deel van het internet. De gegevens uit deze bronnen verschaffen waardevolle informatie over de actuele cyberbedreigingen en tools die worden gebruikt door cybercriminelen zoals Remote Access Trojans (RAT's)[9].

4. Voer aanval-simulatieoefeningen uit op digitale omgevingen. En voer deze oefeningen van zowel het externe als interne dreigingsperspectief uit. Voorbeelden van aanvals-simulatieoefeningen zijn het starten van Phishing campagnes, het uitvoeren van Compromise Assessments[10], het uitvoeren van red teaming-oefeningen en het testen van draadloze netwerken (met tools als HackRF en Pineapple).

5. Om inzicht te krijgen in ransomware-aanvallen die daadwerkelijk plaatsvinden kun je gebruik maken van de 'MITRE ATT&CK-kennisbank[11]. In combinatie met door Lockheed Martin ontwikkelde stappenplan van cybercriminelen (de "Cyber Kill Chain")[12] biedt de MITRE ATT&CK-kennisbank een goede basis voor de ontwikkeling van specifieke dreigingsmodellen en -methodologieën. Hierdoor krijg je beter inzicht in de aanvalsmethoden van cybercriminelen. Van de eerste toegang tot en met volledig controle van de doelsystemen. Het MITRE ATT&CK-raamwerk kan ook worden gebruikt om de technische activiteiten die criminelen gebruiken te analyseren en te begrijpen. Deze kennis kan helpen bij het opbouwen van je technische kennisniveau over de huidige moderne cyberaanvallen.

Conclusie

Cybercriminelen ontwikkelen hun vaardigheden elke dag en lanceren hun aanvallen op alles wat voor hen economisch of politiek waardevol zou kunnen zijn. Om onszelf te beschermen, moeten we in dezelfde wapens investeren als de cybercriminelen. Wij geloven dat een offensieve beveiligingsstrategie de beste manier is om de cybercriminelen een stap voor te blijven. En om cybercriminaliteit beter te detecteren en aan te pakken. De vijf startpunten naar een offensieve beveiligingsstrategie zullen hierbij helpen. Door te beschikken over essentiële- en actuele dreigingsinformatie op basis van daadwerkelijke aanvallen zijn we in staat om de overstap te maken van defensieve naar offensieve beveiliging. Met een offensieve beveiligingstrategie schakelen we de cybercriminele activiteiten uit en bouwen we aan een veiligere digitale samenleving.

Over de auteurs

henk.brandon@capgemini.com

Henk Brandon is Principal Consultant Information Security en Chapter Lead Security Strategy, Governance & Change.

jameel.nabbo@capgemini.com

Jameel Nabbo is Principal Consultant Offensive Security met diepgaande technische kennis van IT-netwerken, offensieve beveiliging, beveiligingsonderzoek, veilige softwareontwikkeling en het beoordelen van cybersecurity zwakke punten en exploits binnen organisaties.

[1]Een Golden Ticket-aanval is wanneer een aanvaller volledige en onbeperkte toegang heeft tot een heel domein - alle computers, bestanden, mappen en vooral het toegangscontrolesysteem zelf.

[2]Fully Undetectable Encrypters worden niet herkend door een antivirus en kunnen worden gebruikt om virussen, RAT's, keyloggers en sommige spyware-tools te coderen. Een doelwit kan hierdoor niet zien dat het een virus is.

[3]Domain Fronting is een techniek dat internetcensuur omzeilt door het domein van een HTTPS-verbinding te overschaduwen. Het biedt een gebruiker de mogelijkheid om verbinding te maken met een service die anders kan worden geblokkeerd door bijv. DPS of IP.

[4]https://www.dhs.gov/news/2017/04/18/home-and-away-dhs-and-threats-america

[5]https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/dreiging

[6]https://nos.nl/artikel/2316120-universiteit-maastricht-kampt-met-ransomware-aanval.html

[7]Steganografie is een methode om informatie op een ongewone plaats maar in het volle zicht te verstoppen: op een locatie opslaan waar niet-ingewijden klakkeloos aan voorbij gaan.

[8]Maskerade is een type aanval waarbij de aanvaller zich voordoet als een geautoriseerde gebruiker van een systeem om er toegang toe te krijgen of grotere rechten te verkrijgen dan waarvoor hij is geautoriseerd.

[9]https://veiliginternetten.nl/themes/situatie/wat-een-remote-access-tool/ Een RAT is software waarmee een ICT'er vanaf één basiscomputer kan inloggen op alle geregistreerde computers en deze op afstand kan beheren. Cybercriminelen maken gebruik hiervan om malware te maken en verspreiden.

[10]https://www.fireeye.com/services/mandiant-compromise-assessment.html / Middels een Compromise Assessment worden sporen van lopende of eerdere aanvallen op IT omgevingen geïdentificeerd.

[11]https://attack.mitre.org

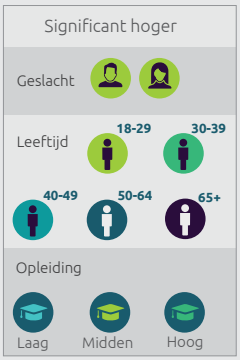
[12]https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Onderzoeksresultaten: Trends in veiligheid in Nederland

Dit onderzoek is uitgevoerd door Ipsos in opdracht van Capgemini Nederland B.V.
Het onderzoek is gedaan in december 2019 en januari 2020.
De steekproefpopulatie is 'de Nederlander' en N>999.

Uitleg legenda

Bij een groot deel van de resultaten uit dit onderzoek zijn ook de grootste significante verschillen per subgroep aangegeven middels iconen. Te weten: leeftijd, geslacht en opleiding. Als een 65+ is weergeven bij een keuze-antwoord, dan is deze groep significant meer vertegenwoordigd in vergelijking met de andere leeftijdsgroepen. Indien er geen andere iconen zijn weergeven, zijn er geen opvallende significante verschillen tussen de andere subgroepen, zoals geslacht en opleidingsniveau.



Veiligheid en cybersecurity

Het aantal Nederlanders dat zich veilig voelt is even groot als het aantal dat zich onveilig voelt, hoogopgeleiden voelen zich vaker onveilig.

Op straat en online is het gevoel van veiligheid vergelijkbaar, ouderen voelen zich online en thuis onveiliger.

Ondanks dat de meeste Nederlanders zelfs geen internetoplichting hebben meegemaakt (ouderen nog minder vaak dan jongeren) geeft een aanzienlijk deel aan slachtoffer te zijn geweest van spam of phishing mail, vooral jongeren en hoger opgeleiden.

De verwachting is dat verschillende vormen van cybercrime zullen toenemen, nagenoeg iedereen neemt dan ook maatregelen om de privacy te beschermen: het up-to-date houden van apps (jongeren), software (ouderen) en verdachte websites mijden. Deze maatregelen worden vaker gehanteerd door hoger opgeleiden.

Een digitale aanval wordt waarschijnlijker geacht dan een fysieke aanval, vooral door hoger opgeleiden. Bijna de helft van de Nederlanders maakt zich hierover weleens zorgen.

Informatievoorziening

Het vertrouwen in traditionele media is minder afgenomen dan dat in nieuwe media en het beeld dat techbedrijven het informatiebeeld beïnvloeden leeft in Nederland, vooral onder jongeren en mannen.

Het grootste deel van de bevolking denkt nepnieuws te kunnen herkennen (vooral jongeren) en een nog groter deel ziet dit nieuws als een gevaar en zien criminele groepen en hackers als de bron van dit kwaad, vooral ouderen.

Digitale veiligheid wordt vooral gezien als een eigen verantwoordelijkheid, toch vindt de Nederlander extra investeringen nodig, vooral in technische middelen en kennis en áls de overheid digitale veiligheid moet waarborgen en dan vooral door het krijgen van meer bevoegdheden.

De stemwijzer en nieuwssites zijn de populairste informatievoorzieningen omtrent verkiezingen, vooral voor hoogopgeleiden. Een groot deel van de Nederlanders is van mening dat andere landen de Amerikaanse verkiezingen beïnvloeden, meer dan die in Nederland.

Privacy versus Veiligheid

In het geval van een misdaad of acuut onveilige situatie vertrouwen de meeste Nederlanders op de politie. Deze bereiken ze bij voorkeur door te bellen. Het leeuwendeel van de bevolking is tevreden met de hulpdiensten.

De Nederlander - vooral de 50 plusser - is bereid om aan privacy in te boeten als het de bestrijding van criminaliteit ten goede komt: camerabeelden mogen gebruikt worden en de helft van alle Nederlanders gaat ermee akkoord dat vingerafdrukken opgeslagen worden. Al heeft minder dan de helft daadwerkelijk vertrouwen in de Nederlandse overheid wanneer het deze opslag betreft.

Bijna alle Nederlanders zijn tevreden over uitwisseling van kennis door inlichtingendiensten.

Ziekenhuizen en de politie worden gezien als de instanties die het meest secuur met persoonsgegevens omgaan, vooral hoger opgeleiden hebben vertrouwen in de wethandhavers.

Belangrijkste inzichten

Veiligheid en cybersecurity

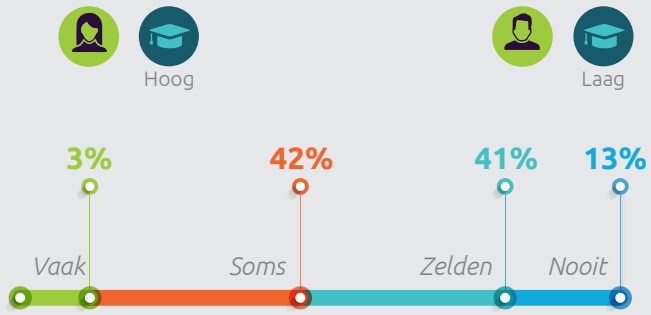
Het aantal Nederlanders dat zich veilig voelt is even groot als het aantal dat zich onveilig voelt. Op straat en online is het gevoel van veiligheid vergelijkbaar.

Ondanks dat de meeste Nederlanders zelfs geen internetoplichting hebben meegemaakt, geeft een aanzienlijk deel aan slachtoffer te zijn geweest van spam of phishing mail. De verwachting is dat verschillende vormen van cybercrime zullen toenemen, nagenoeg iedereen neemt dan ook maatregelen om de privacy te beschermen.

Bijna de helft van de Nederlanders maakt zich wel eens zorgen over een digitale aanval op Nederland.

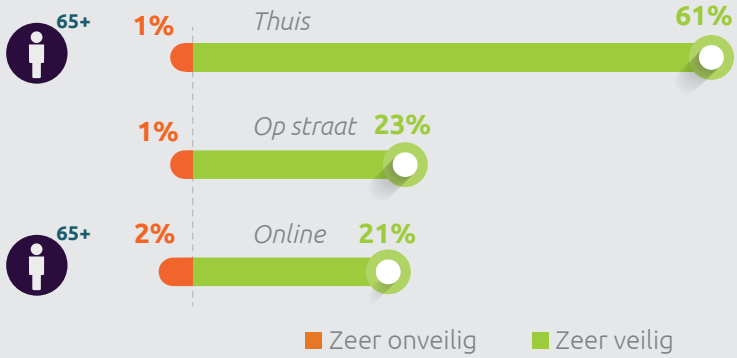
Het aantal Nederlanders dat zich veilig voelt is even groot als het aantal dat zich onveilig voelt, hoogopgeleiden voelen zich vaker onveilig. Op straat en online is het gevoel van veiligheid vergelijkbaar, ouderen voelen zich online en thuis onveiliger.

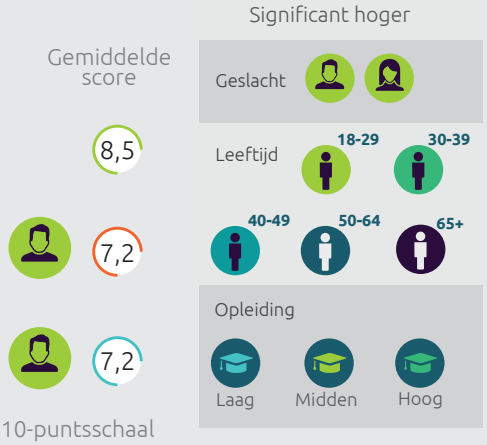
Gevoel van onveiligheid



Q1. Voelt u zich weleens onveilig?

Hoe veilig voelt u zich…

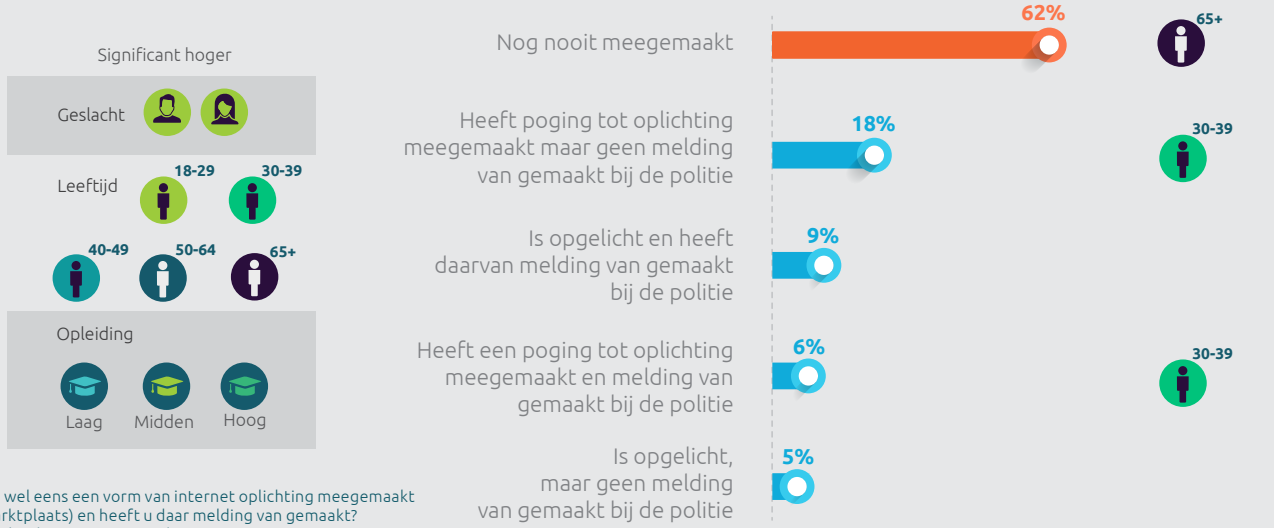




Q2. Hoe veilig voelt u zich… Thuis/Op straat/Online
Basis: Nederlanders 18 jaar en ouder, n=1201

Het merendeel van de Nederlanders heeft geen online oplichting meegemaakt, ouderen nog minder vaak dan jongeren.

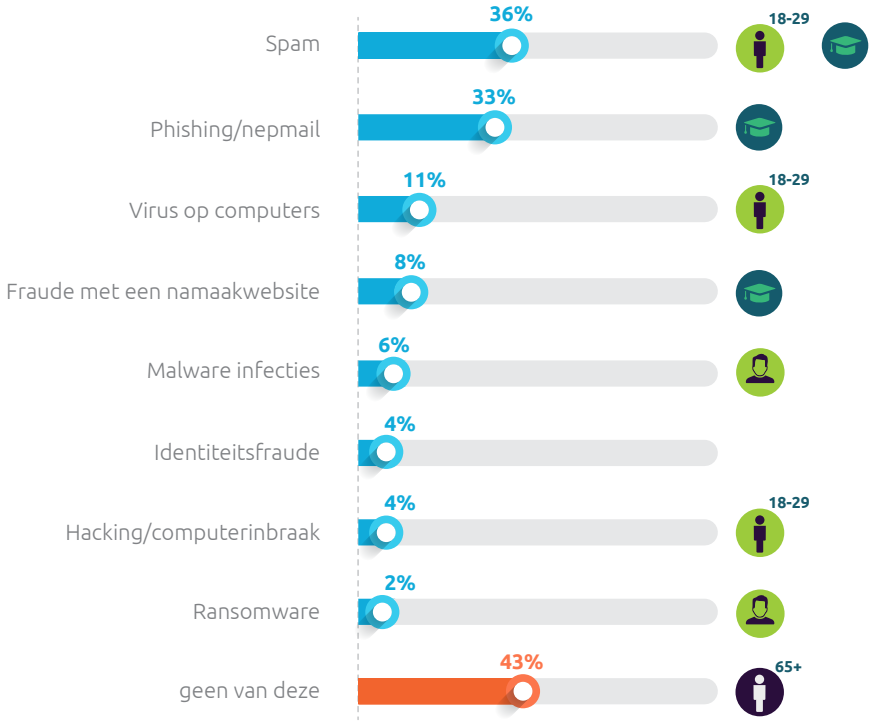
Weleens internetoplichting meegemaakt

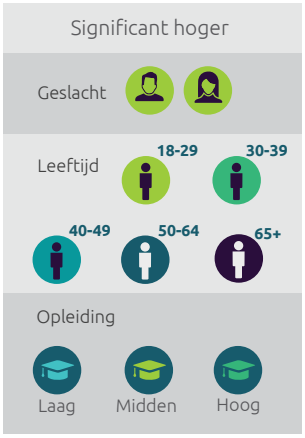


Q3. Heeft u wel eens een vorm van internet oplichting meegemaakt (bijv. via marktplaats) en heeft u daar melding van gemaakt?
Basis: Nederlanders 18 jaar en ouder, n=1201

Spam en phishing mails komen het vaakst voor, vooral bij jongeren en hoger opgeleiden. Men verwacht dat de meeste vormen van cybercrime zullen toenemen, maar de meeste Nederlanders achten zichzelf wel in staat om phishing mail en fake news te blijven herkennen.

In welke vorm slachtoffer van cybercrime geweest





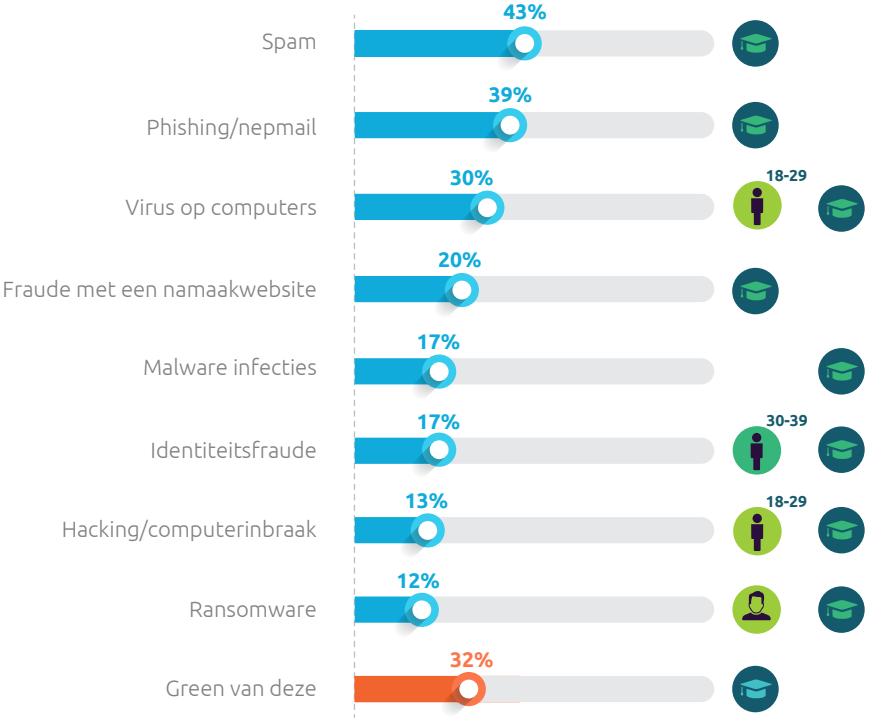
Q4. Van welke vormen van cybercrime bent u de afgelopen 12 maanden zelf wel eens slachtoffer geworden?

Q5. Van welke van de volgende vormen van cybercrime acht u dat er een kans is dat u in de komende 2 jaar slachtoffer kan worden?

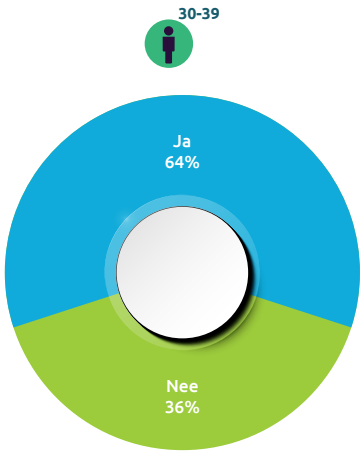
Q5b. Denkt u dat u over 5 jaar tijd nog in staat bent om echte mails van phishing/nepmails te kunnen onderscheiden?

Basis: Nederlanders 18 jaar en ouder, n=1201

Van welke vorm van cybercrime meeste kan om slachtoffer van te worden

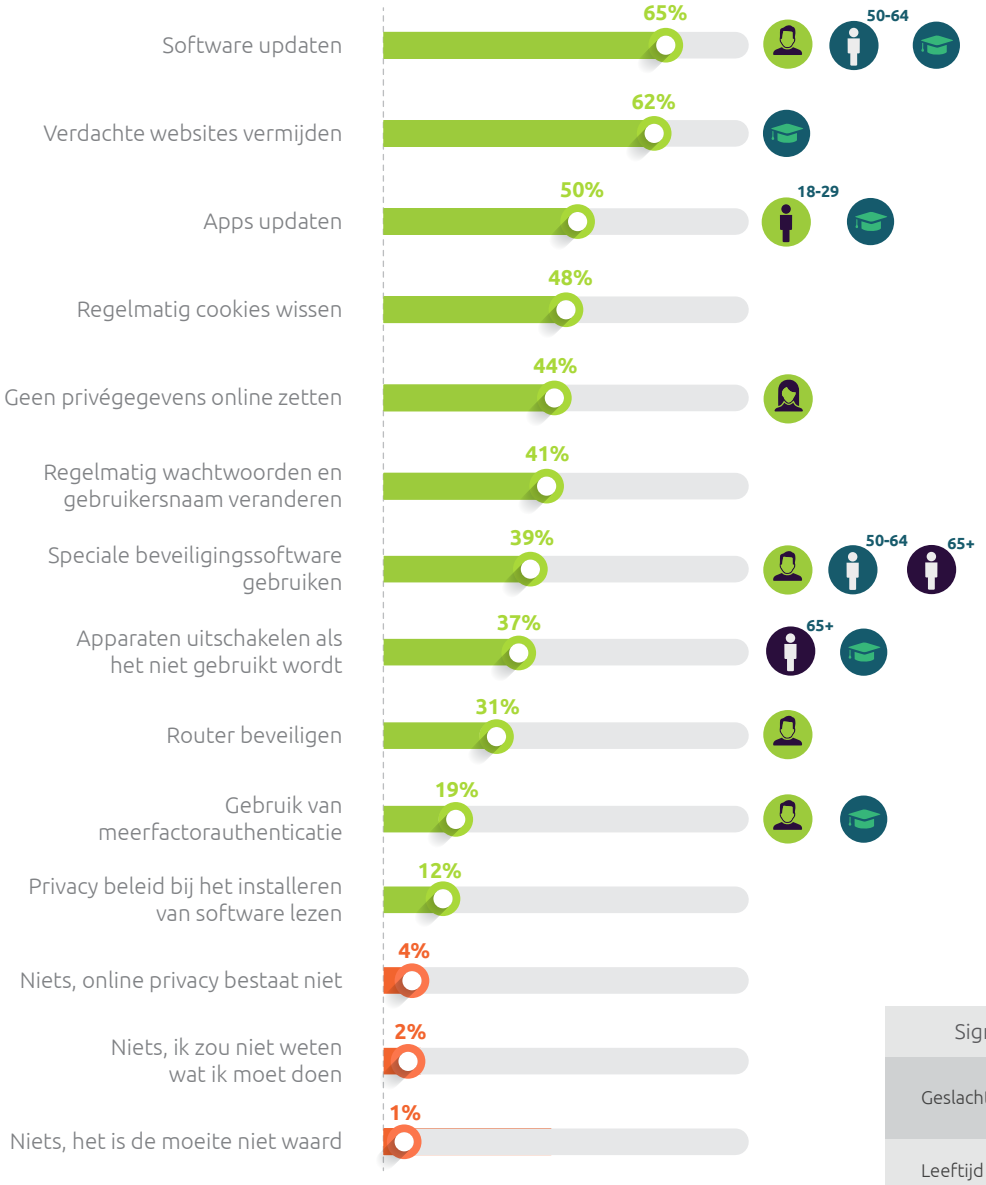


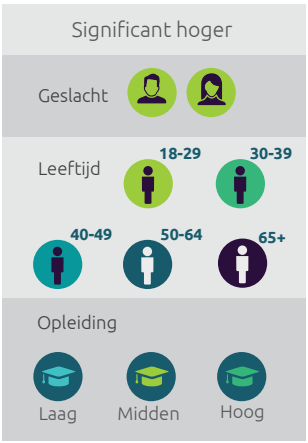
Phishing/nepmails onderscheiden



De meest gebruikte maatregelen om de online privacy te waarborgen zijn het up-to-date houden van apps (jongeren), software (ouderen) en verdachte websites mijden, deze maatregelen worden vaker gehanteerd door hoger opgeleiden.

Maatregelen om online privacy te beschermen

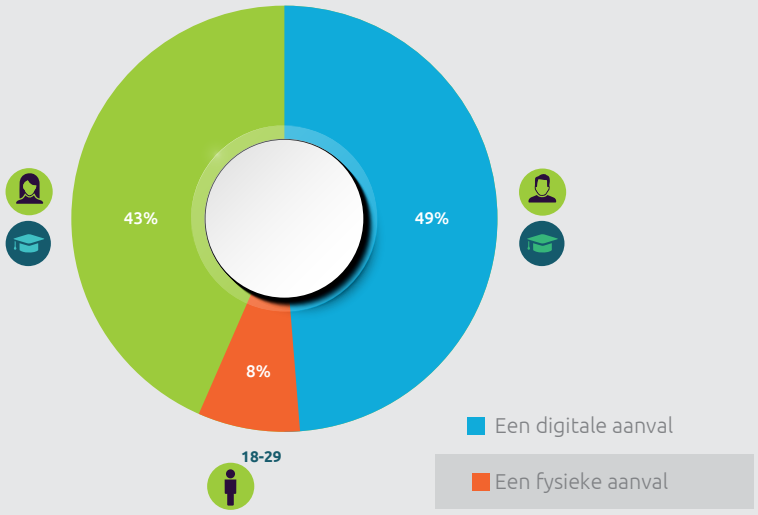


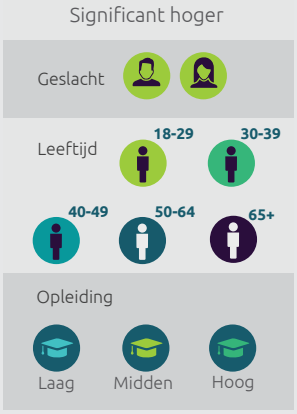


Q6. Welke maatregelen neemt u om online uw privacy te beschermen?
Basis: Nederlanders 18 jaar en ouder, n=1201

Een digitale aanval wordt waarschijnlijker geacht dan een fysieke aanval, vooral door hoger opgeleiden. Bijna de helft van de Nederlanders maakt zich hierover weleens zorgen.

Waarschijnlijker in Nederland…

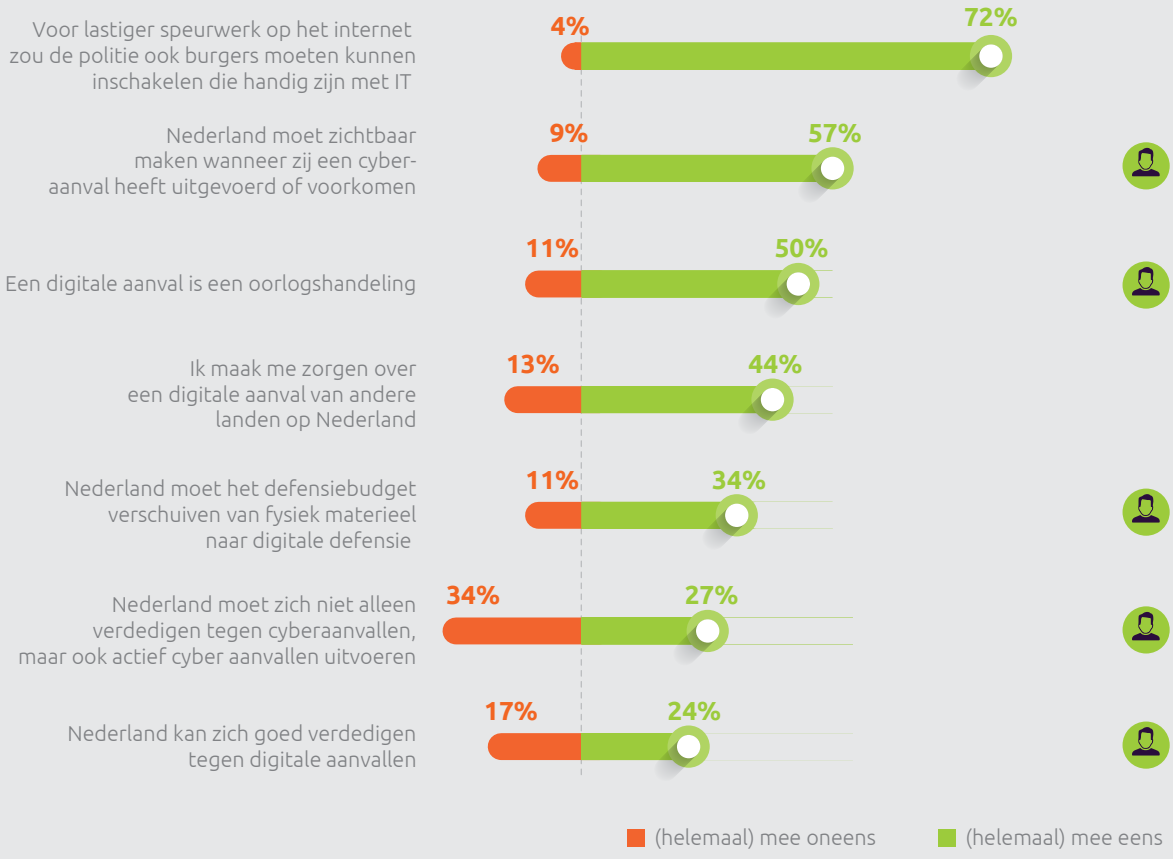




Q7. Welke gebeurtenis acht u waarschijnlijker in Nederland? Q8. In hoeverre bent u het eens met de volgende stellingen?

Basis: Nederlanders 18 jaar en ouder, n=1201

Beleid rond digitale veiligheid



Informatievoorziening

Het vertrouwen in traditionele media is minder afgenomen dan dat in nieuwe media en het beeld dat techbedrijven het informatiebeeld beïnvloeden leeft in Nederland.

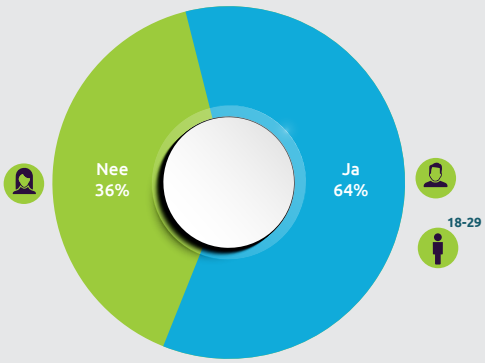
Het grootste deel van de bevolking denkt nepnieuws te kunnen herkennen en een nog groter deel ziet dit nieuws als een gevaar.

Digitale veiligheid wordt vooral gezien als een eigen verantwoordelijkheid, toch vindt de Nederlander extra investeringen nodig. Vooral in technische middelen en kennis en áls de overheid digitale veiligheid moet waarborgen en dan vooral door het krijgen van meer bevoegdheden.

De stemwijzer en nieuwssites zijn de populairste informatievoorzieningen omtrent verkiezingen. Een groot deel van de Nederlanders is van mening dat andere landen de Amerikaanse verkiezingen beïnvloeden, meer dan die in Nederland.

Het vertrouwen in traditionele media is minder afgenomen dan dat in nieuwe media. Het beeld dat techbedrijven het informatiebeeld beïnvloeden leeft in Nederland, vooral onder jongeren en mannen.

Vertrouwen in informatiebronnen



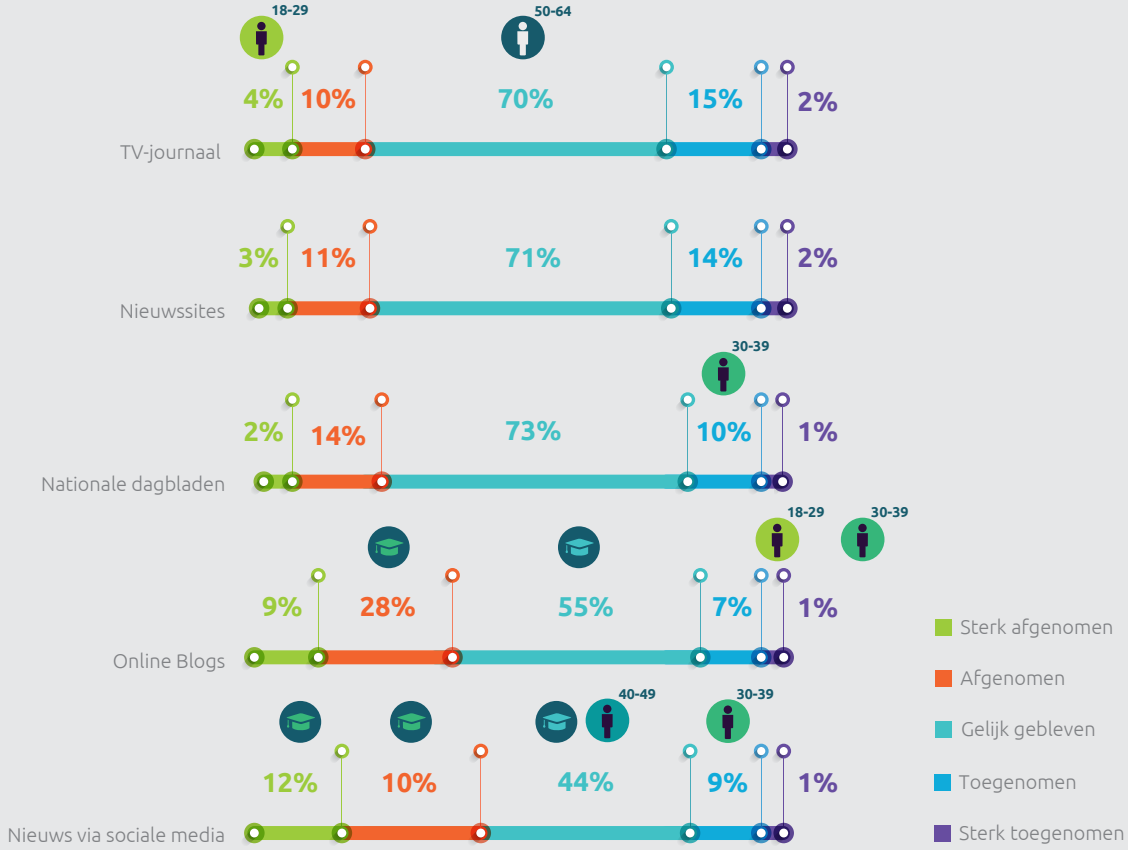
Significant hoger

Geslacht

Leeftijd: 18-29, 30-39, 40-49, 50-64, 65+

Opleiding: Laag, Midden, Hoog

Techbedrijven beinvloeden uw informatiebeeld…



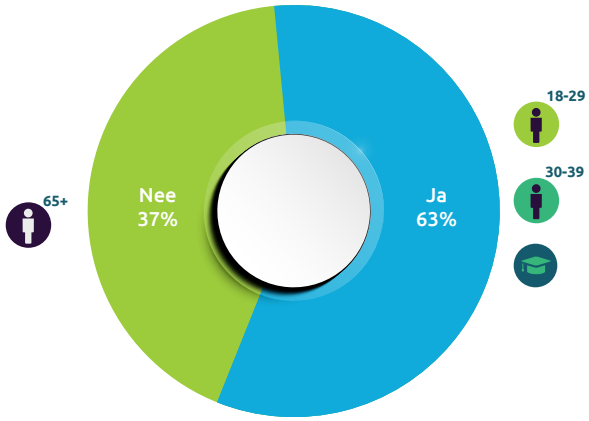
Q9. In welke mate is uw vertrouwen ten aanzien van het nieuws dat de volgende bronnen verstrekken het afgelopen jaar, toe-of afgenomen?

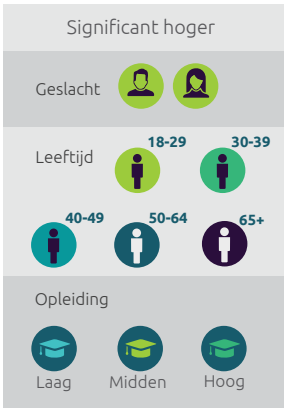
Q10. Heeft u het idee dat uw informatiebeeld wordt beïnvloed (vernauwd) doordat techbedrijven (zoals Facebook, Instagram, etc.) heel gerichte informatie weergeven?

Basis: Nederlanders 18 jaar en ouder, n=1201

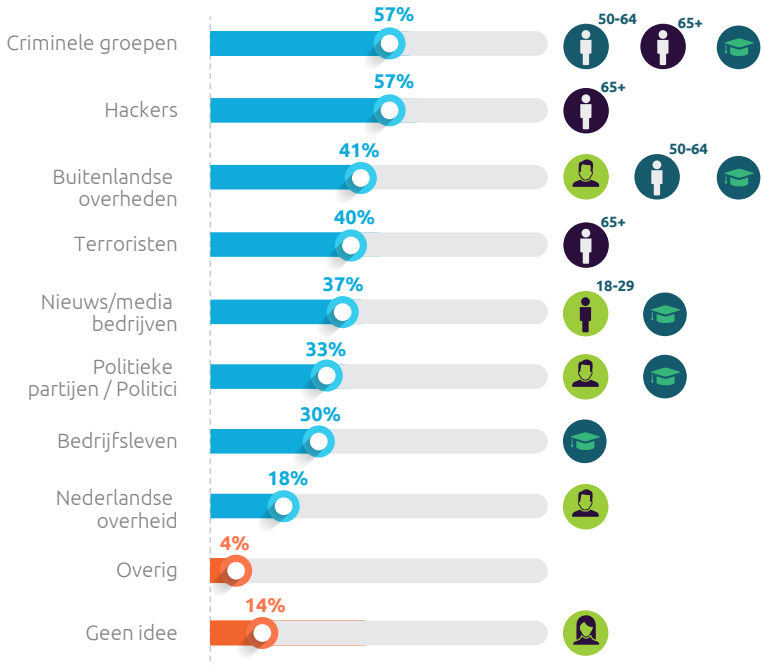
De meerderheid van de Nederlanders acht zichzelf in staat om nepnieuws te herkennen, vooral jongeren. Tevens ziet het overgrote deel het als een gevaar voor de maatschappij, vooral ouderen. De meeste, vooral oudere, Nederlanders zien criminele groepen en hackers als de oorsprong van dit nieuws.

Nepnieuws herkennen

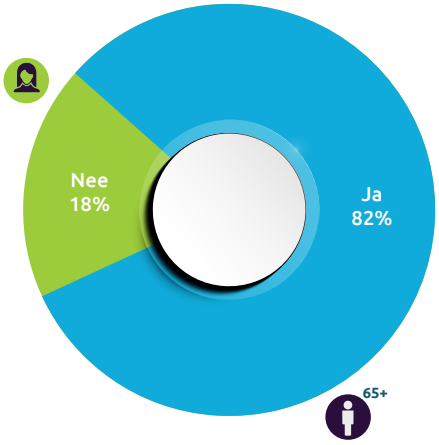




Oorsprong van nepnieuws



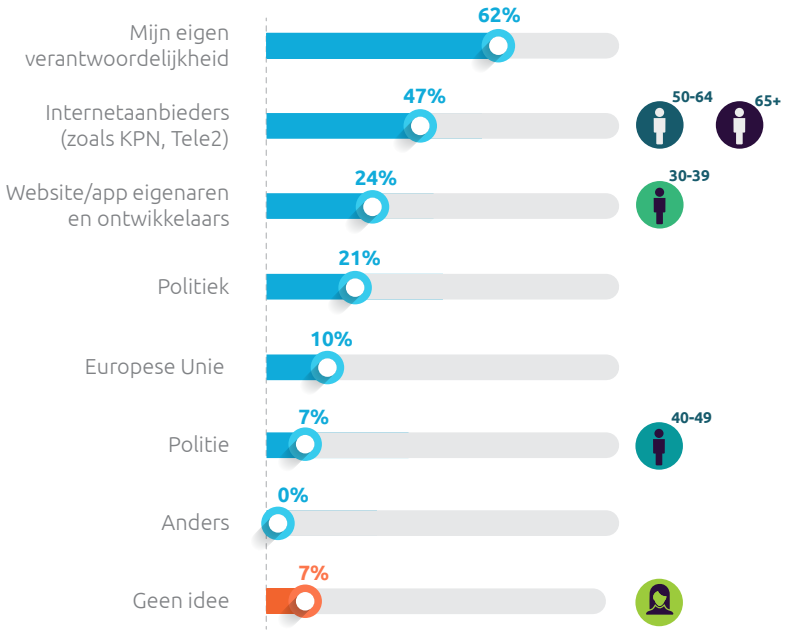
Nepnieuws gevaarlijk?

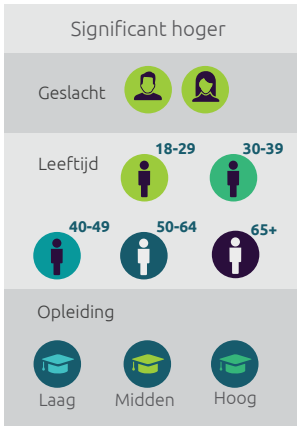


Q11. Denkt u dat u in staat bent nepnieuws te herkennen?
Q12. Waar is nepnieuws volgens u afkomstig van?
Q13. Vindt u dat nepnieuws een gevaar vormt voor de Nederlandse maatschappij?
Basis: Nederlanders 18 jaar en ouder, n=1201

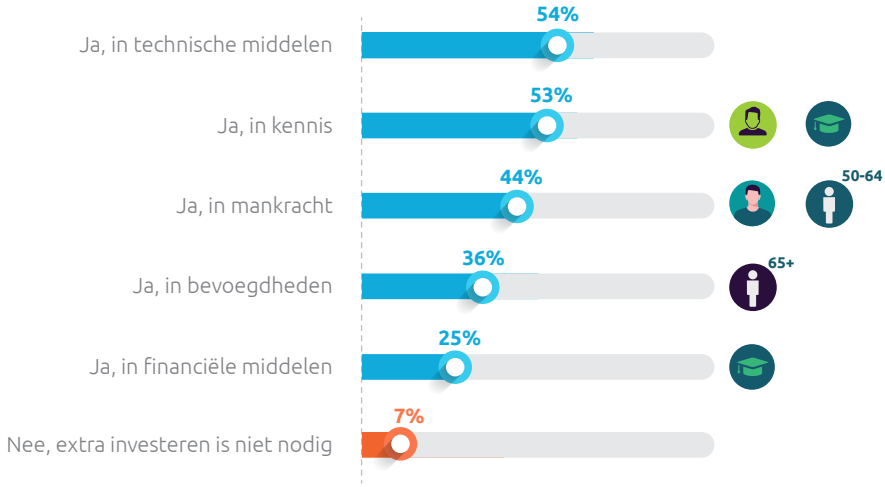
Digitale veiligheid wordt vooral gezien als een eigen verantwoordelijkheid, toch vindt de Nederlander extra investeringen nodig, vooral in technische middelen en kennis.

Verantwoordelijk voor digitale veiligheid





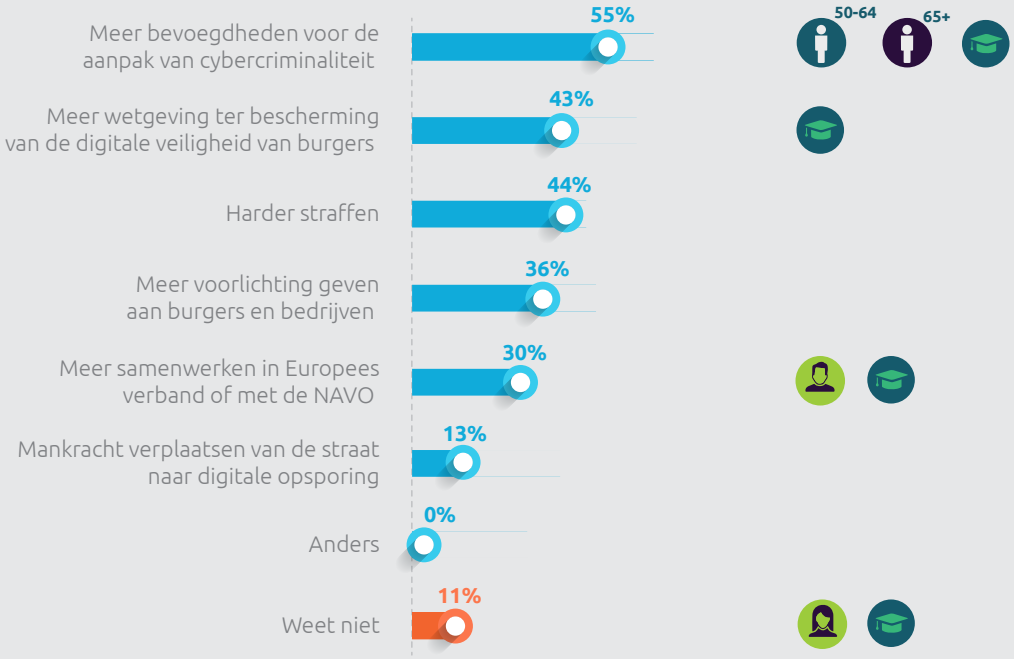
Extra investeringen politie/overheid nodig



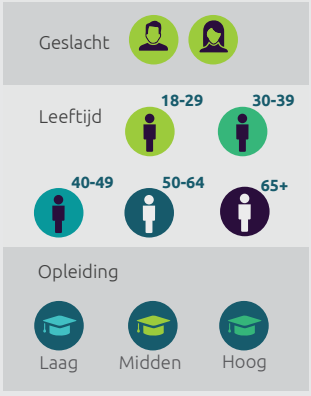
Q14. Wie is volgens u verantwoordelijk voor uw digitale veiligheid?
Q16. Is het nodig dat de politie/overheid extra investeert? Indien ja, waarin?
Basis: Nederlanders 18 jaar en ouder, n=1201

En áls de overheid digitale veiligheid moet waarborgen, dan vooral door het krijgen van meer bevoegdheden.

Digitale veiligheid waarborgen door



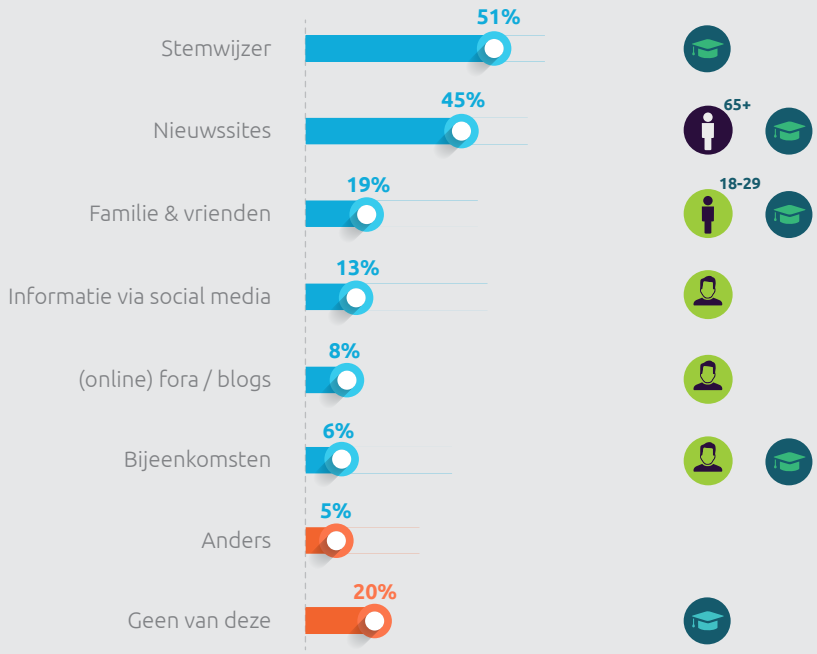
Significant hoger

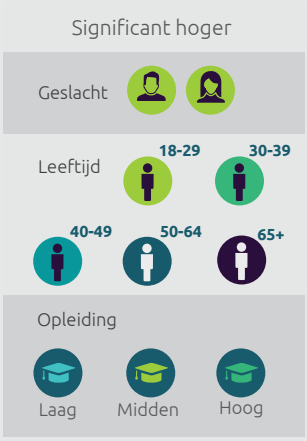


Q11. Denkt u dat u in staat bent nepnieuws te herkennen?
Q12. Waar is nepnieuws volgens u afkomstig van?
Q13. Vindt u dat nepnieuws een gevaar vormt voor de Nederlandse maatschappij?
Basis: Nederlanders 18 jaar en ouder, n=1201

Voor verkiezingen zijn stemwijzer en nieuwssites het populairst voor het inwinnen van informatie, dit speelt vooral onder hoogopgeleiden. Driekwart van de Nederlanders is van mening dat andere landen de Amerikaanse verkiezingen beïnvloeden, tegenover twee derde in Nederland.

Informatiebronnen komende verkiezingen





Invloed andere landen op verkiezingen

Q14. Wie is volgens u verantwoordelijk voor uw digitale veiligheid?
Q16. Is het nodig dat de politie/overheid extra investeert? Indien ja, waarin?
Basis: Nederlanders 18 jaar en ouder, n=1201

Privacy versus veiligheid

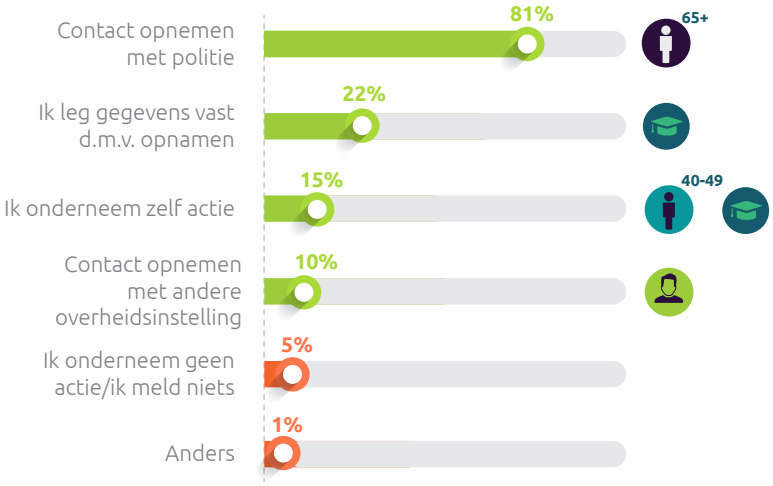
In het geval van een misdaad of acuut onveilige situatie vertrouwen de meeste Nederlanders op de politie. Deze bereiken ze bij voorkeur door te bellen.

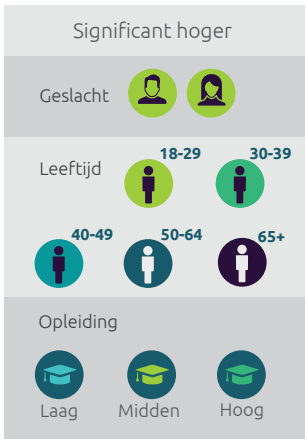
De Nederlander is bereid om op privacy in te boeten als het de bestrijding van criminaliteit ten goede komt: camerabeelden mogen gebruikt worden en de helft van alle Nederlanders gaat ermee akkoord dat vingerafdrukken opgeslagen worden.

Ziekenhuizen, politie en de overheid worden ook gezien als de instanties die het meest secuur met persoonsgegevens omgaan.

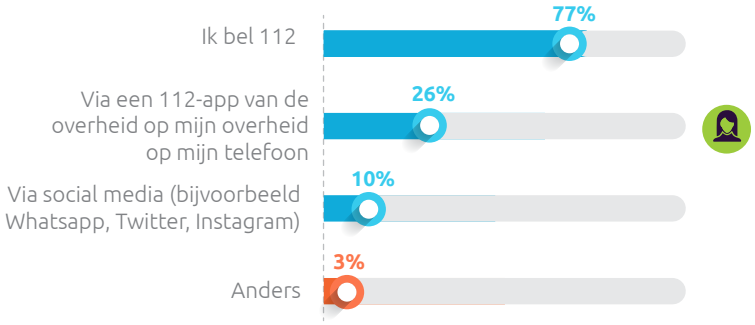
De meeste Nederlanders vertrouwen op de sterke arm der wet voor bescherming en deze opbellen in geval van nood is populairder dan via alternatieve manieren. Het leeuwendeel van de bevolking is tevreden met de hulpdiensten.

Wat doet u als getuige van een voorval?

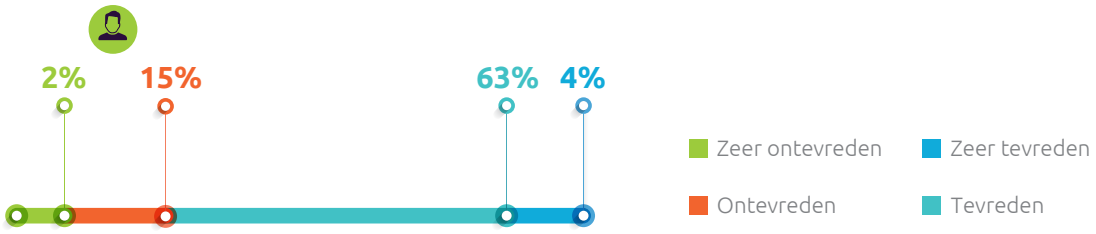




Benaderen hulpdiensten in de toekomst



Tevredenheid delen van informatie met hulpdiensten en overheid



Q18. Wat zou u doen als u getuige bent van een strafbaar feit of acuut onveilige situatie?

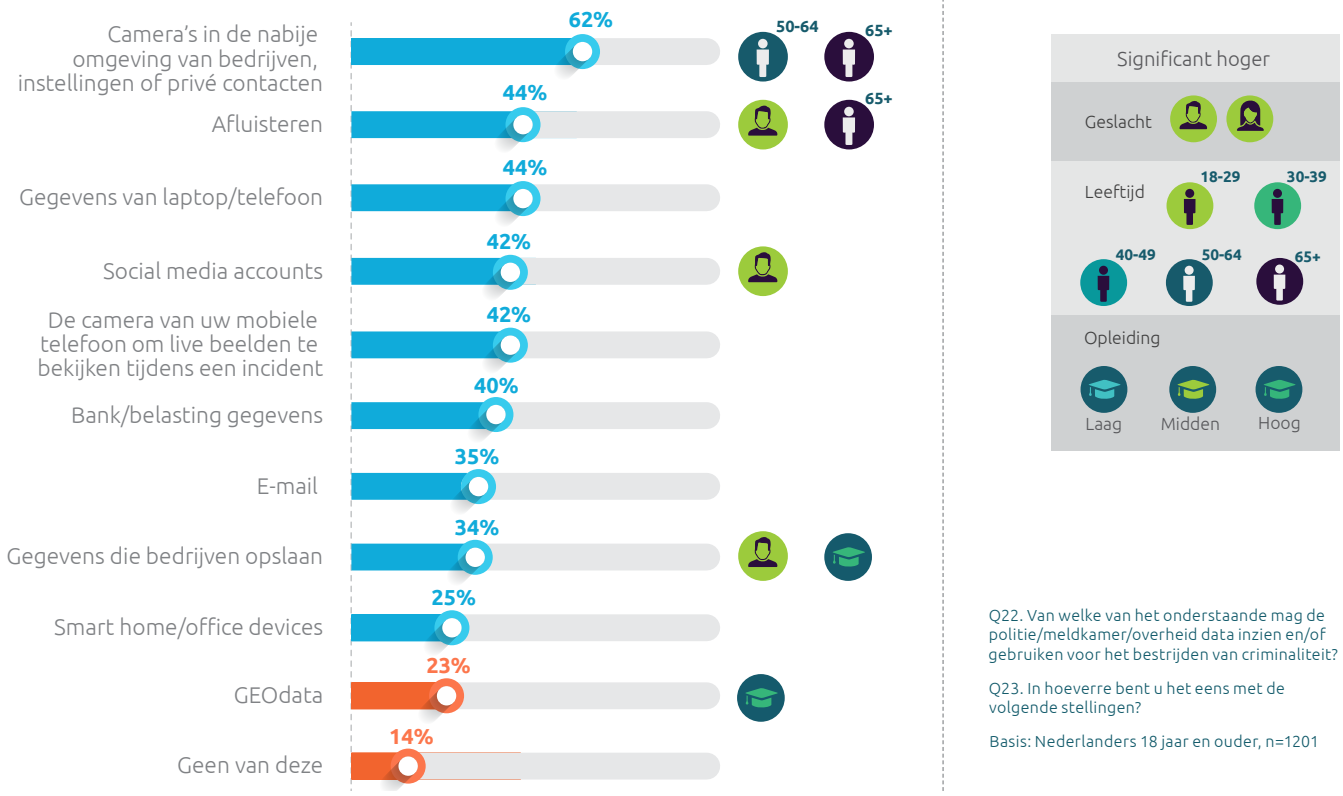
Q19. Op welke wijze zou u in de toekomst melding willen doen van een acute onveilige situatie?

Q21. In hoeverre bent u tevreden met de wijze waarop u informatie kan delen met de overheid, politie, brandweer of ambulance tijdens een incident of aanslag?

Basis: Nederlanders 18 jaar en ouder, n=1201

Als het gaat om het bestrijden van criminaliteit, dan mag de overheid rigoureus handelen en camerabeelden gebruiken van de Nederlandse burger, dit vinden vooral 50-plussers.

Welke data gebruiken voor bestrijding criminaliteit



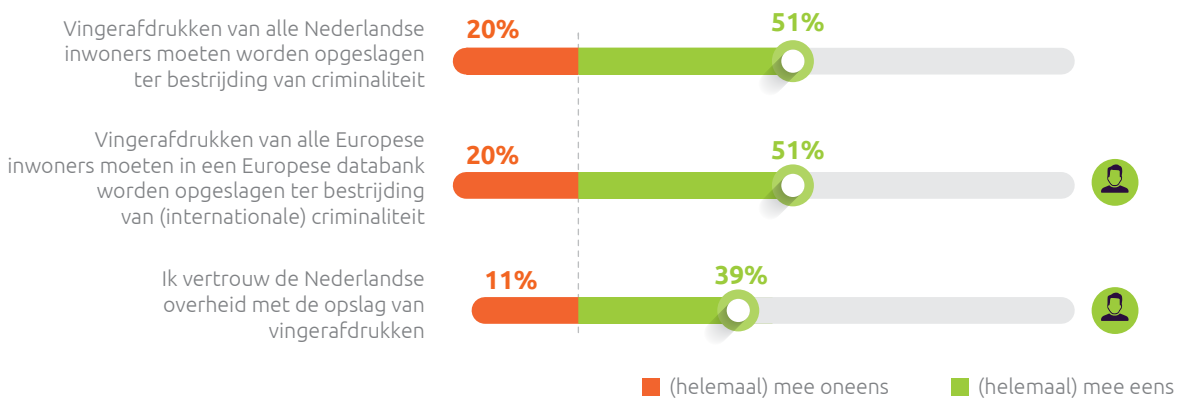
Q22. Van welke van het onderstaande mag de politie/meldkamer/overheid data inzien en/of gebruiken voor het bestrijden van criminaliteit?

Q23. In hoeverre bent u het eens met de volgende stellingen?

Basis: Nederlanders 18 jaar en ouder, n=1201

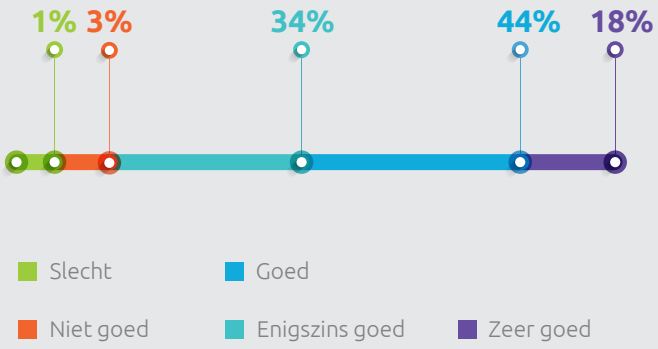
De helft van alle Nederlanders vindt dat vingerafdrukken moeten worden opgeslagen, al heeft minder dan de helft hier daadwerkelijk vertrouwen in.

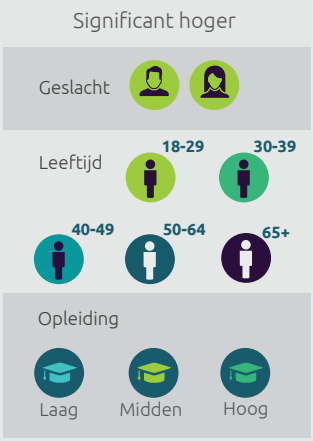
Welke data gebruiken voor bestrijding criminaliteit



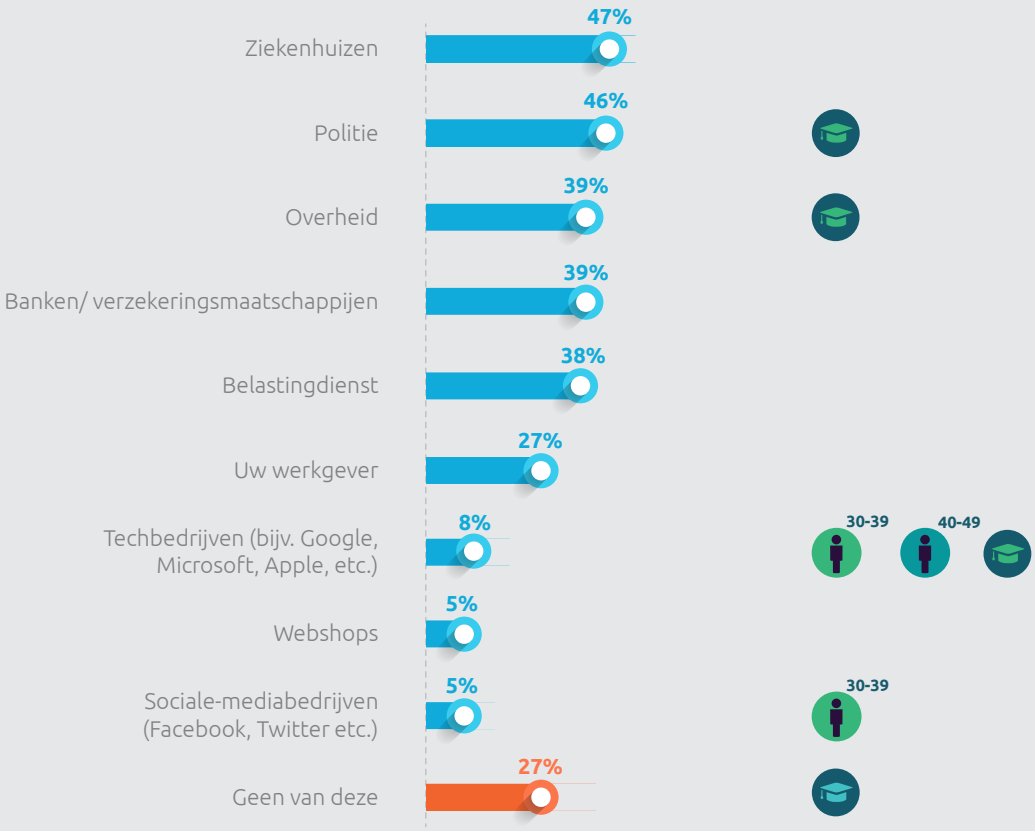
Bijna alle Nederlanders zijn tevreden over uitwisseling van kennis door inlichtingendiensten. Ziekenhuizen en de politie zijn de meest vertrouwde instanties als het omgang met persoonsgegevens betreft, vooral hoger opgeleiden hebben vertrouwen in de wethandhavers.

Uitwisseling inlichtingendiensten





Vertrouwd veilig om te gaan met persoonsgegevens



Q24. Wat vindt u ervan dat verschillende inlichtingendiensten als AIVD, MIVD, NFI voor het bestrijden van bijvoorbeeld terrorisme of fraude gegevens over personen aan elkaar uitwisselen?

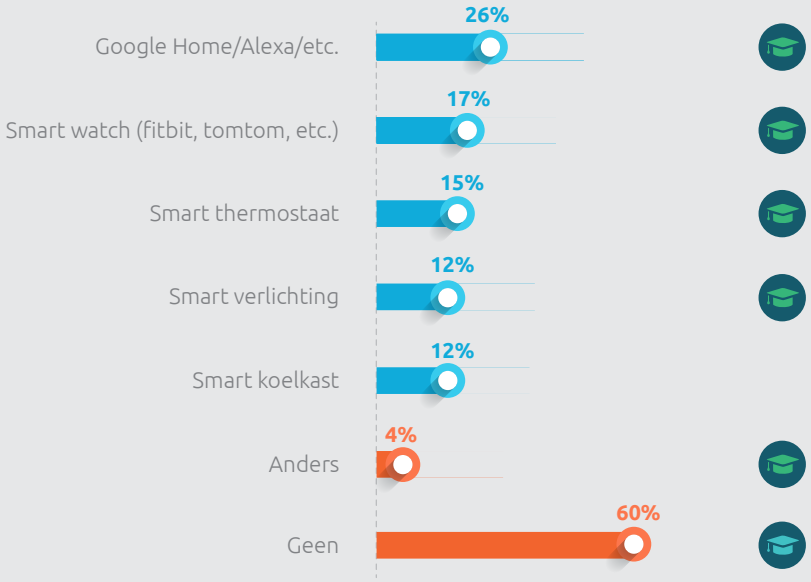
Q25. Van welke van de volgende instanties/bedrijven heeft u er vertrouwen in dat ze veilig met uw gegevens omgaan?

Basis: Nederlanders 18 jaar en ouder, n=1201

Additionele inzichten

Hoger opgeleide Nederlanders maken zich vaker zorgen om privacy wanneer het 'smart home devices' betreft.

Zorgen over privacy tijdens gebruik van deze apparaten



De nieuwe mogelijkheden van een 5G-netwerk interesseren vooral jongere en hoger opgeleide Nederlanders, meer vrouwen dan mannen worden afgeschrikt.

5G…

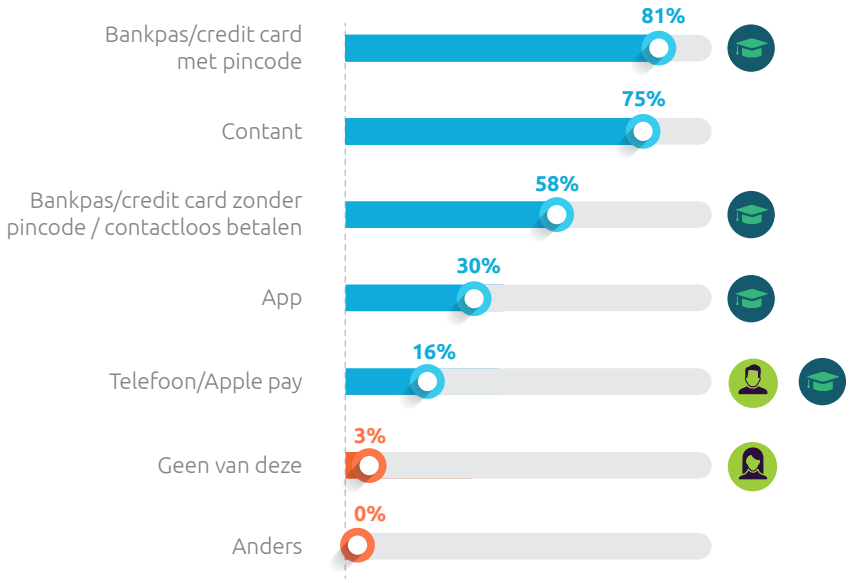
Q26. Van welke van de volgende apparaten die verbonden zijn met wifi of met bluetooth maakt u zich wel eens zorgen over de privacy van deze apparaten en apps?

Q27. De opkomst van 5G zal, als je de hype mag geloven, leiden tot totale connectiviteit waarin alles van auto's tot horloges tot dialysepompen tot koelkasten wordt verbonden. Wat vindt u daarvan?

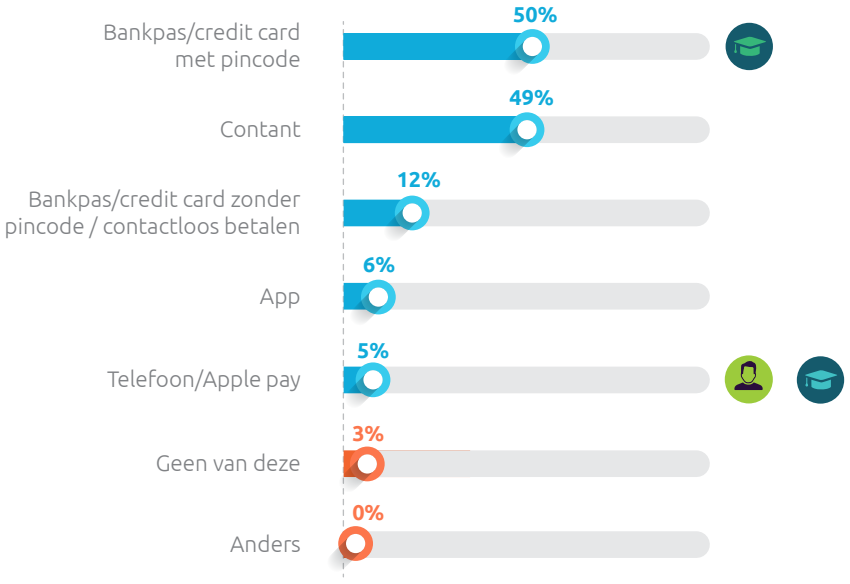
Basis: Nederlanders 18 jaar en ouder, n=1201

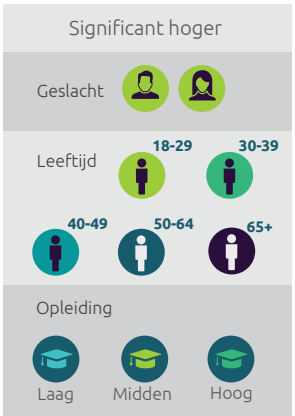
De meeste Nederlanders doen betalingen met hun bankpas of met contant geld en deze manieren van betalen worden ook als de meest veilige methodes ervaren.

Gebruik betaalmogelijkheden



Veiligheid betaalmogelijkheden





Q30. Welke vormen van betalen gebruikt u?

Q31. Welke manier van betalen vindt u het meest veilig?

Basis: Nederlanders 18 jaar en ouder, n=1201

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.

Trends in Tax

"Leuker kunnen we het niet maken, wel makkelijker", dat was lange tijd de slogan van de Belastingdienst. En precies daar lag ook het accent de afgelopen jaren. Niet alleen bij onze Nederlandse Belastingdienst, maar wereldwijd. Digitale ontwikkelingen werden ingezet om het aangifteproces te vergemakkelijken. In Trends in Tax 2020 stelt Capgemini vast dat het nu tijd is om de achterkant van het proces aan te pakken. Het wemelt van de IT-legacy en de papieren processen. Dat komt de agility van de diensten niet ten goede, en juist die beweeglijkheid is cruciaal in een tijd waarin de ontwikkelingen elkaar sneller opvolgen dan ooit.

Trends in Tax 2020 gaat dieper in op deze ontwikkelingen en hoe belastingdiensten erop kunnen inspelen. Uiteindelijk verschijnt een indruk van de belastingdienst van de toekomst, waarin gebruikersvriendelijkheid, agility en verantwoordelijk gebruik van data hand in hand gaan.

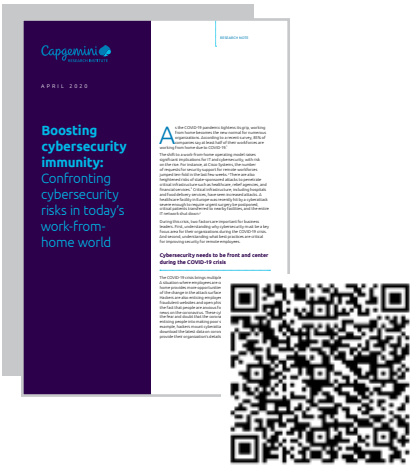
The Great Digital Divide

Covid-19 heeft de manier waarop we leven en werken voorgoed veranderd. Het verloopt meer dan ooit digitaal, en op afstand van elkaar. Althans, voor diegenen die de noodzakelijke middelen tot hun beschikking hebben. We vergeten vaak dat er ook veel 'offline' mensen zijn. Die digitale ongelijkheid is door de pandemie pijnlijk blootgelegd en verder vergroot; openbare diensten verlopen steeds meer online en cruciale informatie is vaak voornamelijk online beschikbaar. In het rapport 'The Great Digital Divide: Why bringing the digitally excluded online should be a global priority', stelt Capgemini het nieuwe normaal aan de kaak. De vinger wordt op de meest pijnlijke plekken gelegd en er worden handvatten gegeven voor vergroting van de 'digitale inclusie'. De belangrijkste slotsom: De digitale ongelijkheid overwinnen we alleen als alle betrokken partijen samenwerken: private sector, publieke sector en burgers.

Boosting cybersecurity immunity

Afkomstig uit de Covid-19 reeks van het Capgemini Research Institute: 'Boosting cybersecurity immunity: Confronting cybersecurity risks in today's work from home world'. Alsof digitale veiligheid onze maatschappij niet al genoeg hoofdbrekens bezorgde, kwam er met het massale thuiswerken een hele dimensie bij. Werken op afstand komt met eigen kwetsbaarheden. We zien nu al dat kwaadwillende actoren die kwetsbaarheden proberen uit te buiten. Ziekenhuizen en andere cruciale organisaties worden bijvoorbeeld steeds vaker geconfronteerd met steeds heftiger cyber-aanvallen. Hoe gaan we daarmee om en wat kunnen we doen om ons beter te wapenen?

In dit rapport maken de onderzoekers de balans op en geven ze richting aan betere cybersecurity in een thuiswerkende maatschappij. Daarbij benadrukken ze dat deze crisis niet alleen maar problemen oplevert, maar ook kansen biedt. De investeringen die bedrijven vandaag doen, stellen hen in staat morgen sterker voor de dag te komen en meer agile te bewegen in een wereld waar thuiswerken er steeds meer bij hoort.



Virtual organizations

Hoe ziet een leidinggevende rol eruit in een tijd waarin iedereen thuis werkt? Dat was de vraag die de onderzoekers van het Capgemini Research Institute stelden voor dit rapport, onderdeel van een reeks onderzoeksnota's over organisaties in tijden van Covid-19. In 'Virtual Organizations need real leadership: Covid-19 and the virtual operating model', kijken ze naar de kwesties waarmee de leidinggevende van nu wordt geconfronteerd. Hoe geef je effectief leiding in een virtuele omgeving? Hoe houd je je medewerkers betrokken en gemotiveerd? En hoe stimuleer je samenwerking en creativiteit in een virtuele werkomgeving? Het rapport concludeert dat anders werken samen moet gaan met ander gedrag, en een andere mentaliteit. Leidinggeven in tijden van Covid-19 vereist vertrouwen, verantwoordelijkheid, empathie, authenticiteit, creativiteit en zorg. Zaken, kortom, die altijd al belangrijk waren en nu hernieuwd in de belangstelling moeten staan.

Blogs

Trends in Veiligheid blogs

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

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

En alle overige Capgemini blogs via:

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

Global: www.capgemini.com/blog

Colofon

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

Lisa Marie Brouwer
Pablo Derksen
Eva Kieft
Thomas de Klerk
Marcel Kordes
Martijn van de Ridder
Erik Staffeleu
Mark de Wit

Advies, ontwerp en productie: Marketing & Communicatie Capgemini Nederland B.V.
Johanna Achterberg, Trina Nandi, Saptadip Dey Sarkar

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 wereldwijd toonaangevend in consulting- en technologiediensten. In de voorhoede van innovatie, helpt Capgemini zijn klanten om de kansen te benutten die ontstaan in de snel veranderende wereld van cloud computing, digitalisering en platformen. Voortbouwend op 50 jaar historie en diepgaande sectorkennis, stelt Capgemini organisaties in staat om hun zakelijke ambities te realiseren via een breed palet aan diensten, van strategie tot uitvoering. Capgemini is sterk doordrongen van de overtuiging dat de zakelijke waarde van technologie van en door mensen komt. Het is een multiculturele organisatie met bijna 270.000 medewerkers verspreid bijna 50 landen. Capgemini Group, met Altran, rapporteerde in 2019 wereldwijd een omzet van EUR 17 miljard.

Bezoek ons op

www.capgemini.nl

www.trendsinveiligheid.nl

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

People matter, results count.

IN/1A-005.20a