INFORMATIEBEVEILIGING
MAGAZINE

SPECIAL: Privacy

- Wat heeft drie jaar AVG ons gebracht?
- Adequate gegevensbescherming werkt alleen als informatiebeveiliging op orde is
- Interview: Gabriel Bassett pleit voor holistische aanpak cybercrime

JAARGANG 21 - 2021 - EDITIE 5

YOUR CLOUDS.
YOUR DATA.
YOUR KEYS.

OUR DATA PRIVACY SOLUTION.

Maintain the privacy, security, and integrity of sensitive data, systems, and encryption keys across your cloud platforms with Enturst nShield as a Service. Whether you use Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), or Salesforce, you can rely on nShield as a Service to provide complete cryptographic capabilities from FIPS- and Common Criteria-certified hardware security modules, without the need for on-prem maintenance:

- Key generation and protection
- Compliance with industry and regulatory mandates
- Containerized application development

NEW INTEGRATION: Keep your most sensitive data private in Microsoft Azure Information Protection with Entrust Double Key Encryption.

LEARN MORE AT ENTRUST.COM/HSM

ENTRUST

SECURING A WORLD IN MOTION

Drie jaar AVG heeft ons niet onberoerd gelaten

Bianca Brooijmans

Drie jaar geleden werd de AVG privacy echt een begrip. Alle echte gekkies onder ons roepen natuurlijk meteen: 'Ja, maar daarvoor hadden we ook al wetgeving die daarover ging', dat klopt natuurlijk maar de AVG zorgde voor een heus WK-effect; opeens hadden we miljoenen bondscoaches langs de lijn.
We horen allemaal op regelmatige basis 'Dat mag niet van de AVG' of juist 'Dat moet van de AVG'. Laten we met deze special nog eens benadrukken dat de AVG vooral bedoeld is voor passende maatregelen en welke dat dat zijn, is per vraagstuk en situatie verschillend, maar in ieder geval nooit 'omdat het handig is'. Laura de Vries schrijft hierover een duidelijk stuk.

Drie jaar AVG (stiekem al vijf jaar natuurlijk); het heeft ons in ieder geval niet onberoerd gelaten. Maar wat heeft het jou nou daadwerkelijk gebracht en misschien juist wel gekost? Nico Mookhoek blikt terug op de afgelopen jaren en onze vaste redacteurs neemt mee in hun persoonlijke ervaringen.
Laat je ook vooral in deze uitgave weer eens bijpraten over de AVG en do's en don'ts. Niet alleen de AVG staat centraal, maar ook gerelateerde vraagstukken over bijvoorbeeld de eindeloze mogelijkheden van het verwerken van data en de overlap van informatiebeveiliging en bescherming van (persoons)gegevens. Allen geschreven door experts uit het veld, die dagelijks te maken hebben met diverse vraagstukken. Dus als je ook een vraag hebt, lees in ieder geval dit iB5-Magazine door en wellicht wordt jouw vraag al beantwoord. Benader gerust onze auteurs als er daarna nog vragen zijn.

Het was ons weer een genoegen om met zoveel talent een special te maken. Wij hopen dat je het met evenzoveel genoegen zult lezen.

IN DIT NUMMER

03 Voorwoord – Drie jaar AVG heeft ons niet onberoerd gelaten
04 Interview Gabriel Bassett – Co-auteur Data Breach Investigations Report pleit voor holistische aanpak cybercrime
07 Column – Privacy
08 Van BIO naar boa (en weer terug)
14 Handig is geen grondslag
16 Meer met data. Maar wát eigenlijk?
19 Column Inge Wetzer – Klosje tussen de deur
20 Wat heeft drie jaar AVG ons gebracht?
24 Privacy podcasts
26 Adequate gegevensbescherming werkt alleen als informatiebeveiliging op orde is
28 Blog – Overtuigingskracht voor security officers
31 Lekker foppen
32 Best practices in access management (part 2 of 2)
37 Aangestuurd autorijden – deel 2
42 SOCCRATES – Real-time threat, impact analysis and response automation for SOC/CSIRT operations
48 Achter Het Nieuws – 'Wat heeft de invoering van de AVG ons als redactie gebracht of gekost?

Auteurs: Tom Bakker is redactielid van iB-Magazine. Tom is bereikbaar via tombakker@pvib.nl Sandra Kagie is freelance tekstschrijver (Sanscript tekstproducties). Sandra is bereikbaar via info@sanscriptproducties.nl.

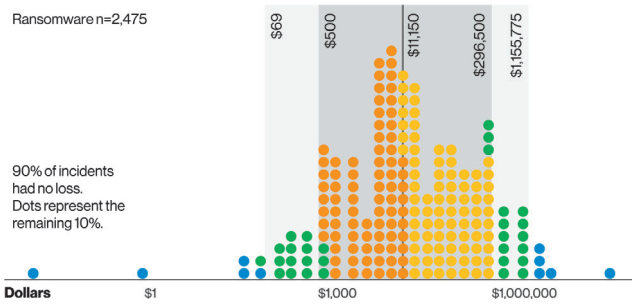
INTERVIEW

Co-auteur Data Breach Investigations Report pleit voor holistische aanpak cybercrime

Op het moment dat we Gabriel Bassett, hoofd data-analist en co-auteur van het in mei gepresenteerde 2021 Data Breach Investigations Report (DBIR) spreken, is ransomware volop in het nieuws. Door een ransomware-aanval op de Amerikaanse software-leverancier Kaseya lagen wereldwijd honderden bedrijven stil. Ook in Nederland werden slachtoffers gemaakt. Termen als 'grootste cyberaanval ooit' domineerden het nieuws. Het geëiste losgeld: 70 miljoen dollar.

Wanneer we Bassett vragen naar het meest positieve nieuws uit het jongste Data Breach Investigations Report (DBIR) verwijst hij direct naar de impact-sectie van het rapport. Daaruit blijkt dat de financiële impact van een ransomware-aanval in veruit de meeste gevallen 'niet exorbitant hoog is', zoals hij het verwoordt.

Hij wijst vervolgens in het rapport op de mediaan van meer dan 11.000 dollar die bedrijven verloren na een ransomeware-aanval. In negentig procent van de gevallen verloren slachtoffers van een ransomware-aanval zelfs helemaal geen geld. "Heel anders dan dat wat we in het nieuws zien", concludeert hij.



Figuur 1 – Verlies per incidenttype. Elke stip vertegenwoordigt 0,5% van de incidenten.

De les die bedrijven uit dit, in zijn ogen, 'goede nieuws' zouden moeten trekken, is dat je als bedrijf kunt dealen met de gevolgen van een ransomware-aanval. "De gevolgen

ervan zijn niet onoverkomelijk. Dit in tegenstelling tot het gevoel dat je zou kunnen krijgen wanneer je berichtgeving over dit type aanvallen in het nieuws volgt."

'Geen Italian job'

"Je kunt als organisatie een fout maken en deze te boven komen", stelt Bassett geruststellend. Aan de andere kant noemt hij het feit dat cybercrime een constante dreiging blijft voor organisaties het slechtste nieuws dat dit keer uit het rapport naar voren komt. "Cybercrime is geen Italian job, maar een business that is here to stay", waarschuwt hij. "Aanvallers hoeven geen experts te zijn, want alles is te koop. Neem ransomware as-a-service. Iedereen die wil, kan ermee aan de slag." Dit maakt volgens Bassett dat elk bedrijf en elke organisatie een potentieel slachtoffer blijft. Ook al denk je 'bij mij valt toch niks te halen'. "Een realiteit waarmee zowel grote als kleine organisaties rekening moeten blijven houden."

"Voor aanvallers is cybercrime nu eenmaal een heel efficiënt businessmodel", waarschuwt Bassett. "Het vergt niet veel investeringen en ze lopen weinig risico. Verdachten slaan immers bij voorkeur toe buiten hun eigen landsgrenzen, wat de opsporing heel moeilijk maakt. Digitaal doen grenzen van landen er niet toe , maar juridisch gezien, als het aankomt op opsporing, is dit een heel ander verhaal. Een tegenstelling die aanvallers in de kaart speelt."

Holistische aanpak

Bassett hoopt dat deze constatering regeringen en bedrijven ertoe aanzet echt na te denken over manieren om dit gunstige businessmodel om zeep te helpen. Vragen die we hiertoe volgens hem gezamenlijk moeten beantwoorden zijn: hoe maken we het businessmodel achter cybercrime minder efficiënt? Hoe verhogen we de drempel zodat het moeilijker is voor aanvallers om zich op het cybercrimepad te begeven? En hoe vergroten we het risico voor aanvallers dat ze gepakt worden? In het verlengde hiervan hoopt Bassett dat het belangrijkste nieuws uit het rapport van volgend jaar zal zijn dat de securitygemeenschap erin is geslaagd cybercriminelen op een 'holistische manier' aan te pakken. "Dat zou ik heel graag opschrijven in het DBIR 2022", geeft hij aan wanneer we hem naar de door hem gewenste headline van dat volgende rapport vragen.
"Dat het ons gezamenlijk is gelukt meer bedrijven en organisaties weerbaar te maken tegen cybercrime aan de ene kant en dat we er aan de andere kant voor hebben weten te zorgen dat cybercrime voor aanvallers minder economisch interessant is geworden en méér risicovol."

Kat-en-muisspel

Wat deze gewenste aanpak betreft zou de securitygemeenschap volgens hem een voorbeeld moeten nemen aan fraudebestrijders. "Die denken niet: wanneer komt er nu eens een eind aan fraude. Het is een kat-en-muisspel en dat

2021 DBIR: de achtergrond

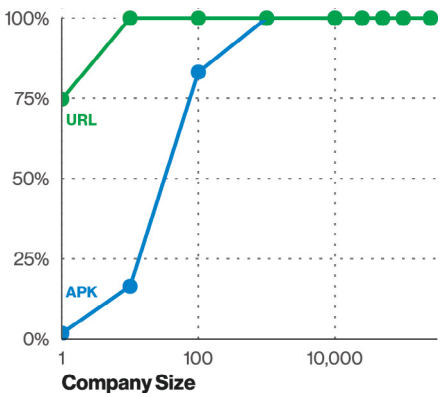
Om te komen tot het 2021 DBIR, alweer de 14e editie van het jaarlijkse onderzoek, heeft een team van analisten, onder wie Gabriel Bassett, 79.635 aan security gelinkte incidenten bekeken. Hiervan bleek het in 29.207 gevallen te gaan om veiligheidsincidenten, waarvan 5.258 bevestigde datalekken. Ter vergelijking: vorig jaar analyseerden ze 3.950 datalekken.
Wie zijn de slachtoffers? Wie zit er achter de cyberaanvallen? Welke tactieken gebruiken cybercriminelen? Slechts een aantal van de vragen die de onderzoekers ook dit jaar in het rapport beantwoorden. Want, zo stellen zij: 'The more you know about the threats you face, the better your chances of keeping your data secure and your name out of the headlines.'
Dit keer is het DBIR gebaseerd op het onderzoek van incidenten afkomstig van 83 bijdragers uit 88 landen. En in het rapport wordt een uitsplitsing gemaakt in elf sectoren, waaronder: de financiële sector, de gezondheidszorg, het onderwijs, de retail en de maakindustrie. Ook wordt een grove regionale analyse gemaakt. Hierbij worden Europa, het Midden-Oosten en Afrika als één regio beschouwd (EMEA).

Benieuwd wat de bevindingen zijn van de onderzoekers over bijvoorbeeld de sector waarin jij werkt?
Het volledige 2021 Data Breach Investigations Report is beschikbaar via Verizon:
https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

accepteren ze. En dat spel spelen ze goed. Iets wat de securitygemeenschap ook moet doen. Perfectie is niet het doel. Nee, het minimaliseren van de dreiging tot deze behapbaar is, moet vooropstaan." Het delen van incidenten is en blijft hierbij volgens Bassett cruciaal. "Help anderen begrijpen wat er is gebeurd in het geval van een cyberaanval, zodat iedereen het beter kan doen", roept hij op. "En stop met het stigmatiseren van slachtoffers, want daarmee bereik je juist het tegenovergestelde."

Menselijke fouten

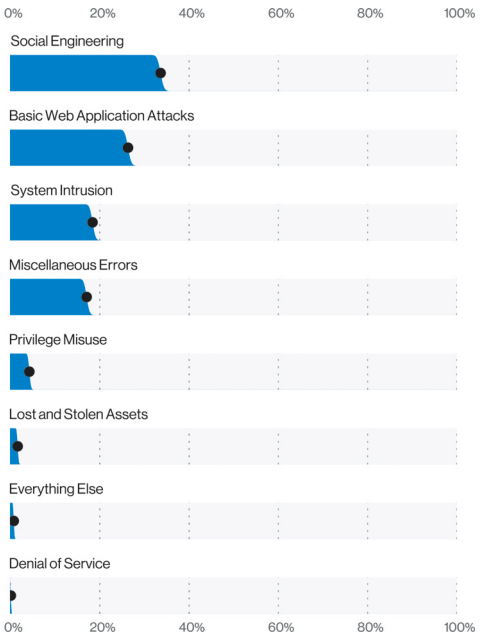
Hij trekt vervolgens de parallel met hoe bedrijven in zijn ogen zouden moeten omgaan met menselijke fouten die gemaakt worden door medewerkers. Nog altijd een belangrijke oorzaak van beveiligingsincidenten en datalekken, zo blijkt uit het rapport. "Why not cultivate your employees to be your early warning system when it can have a great return on investment?", is de opmerking uit het 2021 DBIR die hij in dit kader aanhaalt. "Wanneer iemand binnen je organisatie denkt dat hij bijvoorbeeld heeft geklikt op een verkeerde link dan moet hij of zij zich vrij voelen dit meteen te melden. Zonder dat dit vervelende gevolgen voor diegene heeft", legt hij uit. "Je schamen voor iets wat je verkeerd hebt gedaan, is heel normaal. En het is precies die schaamte waarvan aanvallers profiteren. Een gang van zaken die we kunnen veranderen door de cultuur van angst om fouten toe te geven, te doorbreken. Dat medewerkers fouten maken, zal niet veranderen", stelt hij. "Wat de gevolgen zijn van zo'n fout, hangt echter af van hoe je hier als bedrijf of organisatie mee omgaat. Wat we als security-specialisten nooit moeten vergeten is dat we niet een computer of een systeem beveiligen, maar een organisatie.



Figuur 2 - De kans dat iemand in een bedrijf een foute link ontvangt of een fout APK-bestand (Android app) installeert afgezet tegen de grootte van een bedrijf.

Dat betekent dat je medewerkers altijd moet meenemen in je verhaal."

Terug naar het rapport van dit jaar. In totaal analyseerden Bassett en zijn collega's 29.207 incidenten, waarvan 5.258 bevestigde datalekken vanuit heel de wereld. De belangrijkste conclusies: phishing-aanvallen stegen met 11 procent, aanvallen met ransomware met 6 procent en bij 85 procent van de inbreuken speelde de factor 'mens' een rol. De belangrijkste drijfveer van cybercriminelen is en blijft financieel gewin en daders moeten we zoeken in de wereld van de georganiseerde misdaad.



Figuur 3 – Datalek patronen (n=5275).

Niet veel nieuws onder de zon, zou je kunnen zeggen. En juist dat biedt volgens Bassett voordelen, want voor een belangrijk deel weet je als bedrijf of organisatie dus waar je je op moet voorbereiden. "Engineer for the expected and use operations for the exceptional", adviseert hij daarom. "Je wilt niet dat de afdeling operations binnen je organisatie achter elke phishing-email aan moet die je ontvangt omdat je geen phishing filter service hebt", geeft hij een voorbeeld. "Zorg er daarom voor dat qua workload alles in de juiste emmer terechtkomt. Bewaar met andere woorden de balans tussen engineering en operations, zodat de laatste oog voor de uitzonderingen kan houden", besluit hij.

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Stuur eens een brief

Het kostte wat moeite, maar een paar jaar geleden lukte het om mijn familie over te krijgen naar Signal. De app die nog de meeste garantie biedt op privacy. Whatsapp gebruik ik ook nog steeds, simpelweg omdat veel mensen er nog steeds gebruik van maken. Ook mensen die ik graag eens een bericht stuur. Maar ik blijf het lastig vinden om in die 'users-I-like-lock-in' vast te zitten.

De koppeling tussen WhatsApp en Facebook bekriebelt me en de privacyonvriendelijke gebruiksvoorwaarden durf ik bijna niet te lezen (nee zeggen is niet meedoen en daar zit je dan met je 'users-I-like-lock-in'). De laatste ontwikkeling – het monitoren van de inhoud van de berichten – maakt dat ik echt gruwel. WhatsApp heeft duizend moderatoren ingehuurd om berichten die door gebruikers als 'verdacht' zijn aangemerkt te lezen.

De proef op de som genomen, kijk ik in het profiel van iemand die me onlangs een bericht had gezonden. Onderin vind ik een knop om iemand te rapporteren. Ik druk erop en verwacht dat ik in een keuzemenu terecht kom, of op zijn minst mijn rapport kan toelichten. Dat blijkt niet het geval – na het enkele drukken op de knop wordt direct een rapport verzonden. In dat rapport bevinden zich de laatste paar berichten in leesbare vorm. Dat staat niet in de app aangegeven, maar moet ik ergens in de gebruiksvoorwaarden lezen. Ik word een beetje misselijk en krijg daarnaast het schaamrood op de kaken. Ik heb ten onrechte iemand gerapporteerd aan WhatsApp.

Op dit moment zit er dus iemand met een Amerikaans morele bril naar mijn berichten te kijken. De privacy inbreuk voelt zo draconisch groot en in strijd met de AVG, dat ik me niet kan voorstellen dat dit de toets van welke Europese toezichthouder dan ook zou kunnen doorstaan. De persoon wiens privacy op een wrede manier doorbroken wordt, komt er daarnaast ook nog eens niet achter. Althans, de berichtenapp garandeert dat de persoon die je rapporteert er echt niet achter komt.

De berichtenapp komt praktisch tegelijk met een privacyvriendelijke functie, althans, zo brengt ze het zelf natuurlijk. Het wordt mogelijk om te segmenteren in personen die mogen zien of je online bent geweest en hoe laat dat dan was. Ja, eerlijk is eerlijk, ik durf me niet meer online te laten zien na deze privacyflater. Dan is het maar wat handig dat ik me kan verstoppen achter de boodschap dat ik niet online ben voor de betreffende persoon. Ik denk dat ik een tijdje wat meer offline moet gaan communiceren, ik voel me toch wat beter met pen, papier en een dichtgeplakte enveloppe. Beide extra verzegeld door ons Nederlands grondwettelijke briefgeheim.

Het deed me denken aan de woorden van een rechercheur die ik onlangs sprak op een warme zomeravond bij een fijn glas rum. Hij vertrouwde me toe dat het verreweg het veiligst was om een brief in een gesloten enveloppe aan iemand te zenden. De rest is op de een of andere wijze toch makkelijk leesbaar of leesbaar te maken. Ik nam een slok uit mijn glas en besloot dat ik direct even een paar velletjes postzegels ging bestellen. Via de online winkel van het postkantoor. Dat dan weer wel.

Rachel

Auteurs: Aaf Stuijt LLM en Roswitha Talen LLM zijn beiden ervaren privacy juristen en trainers met een praktische inslag. Ze geven Wpg-trainingen aan boa's, hun beleidsmakers en toezichthouders. Ze begeleiden Wpg-audits en adviseren vaak met succes over complexe samenwerkingsvraagstukken. Voor contact met Aaf en Roswitha mail naar contact@aafstuijt.nl en info@talenjuridischadvies.nl.

Van BIO naar boa (en weer terug)

De bescherming van persoonsgegevens gaat over technische en organisatorische beveiligingsmaatregelen die deze gegevens moeten beschermen tegen onbevoegde, onbedoelde en onnodige verwerking. Andere beschermings-maatregelen zijn van juridische aard en gaan over het hebben van de juiste rechtsgronden, doelbinding en wettelijke basis.

Als we spreken van informatiebeveiliging bij de overheid, komen we al snel uit bij de Baseline Informatiebeveiliging Overheid (BIO). De BIO is de opvolger van zowel de Baseline Informatiebeveiliging Rijk (BIR) als de Baseline Informatiebeveiliging Gemeenten (BIG). De informatiebeveiligers van zowel het rijk als de gemeenten hebben de handen ineengeslagen om gezamenlijk tot één baseline te komen. Hulde voor dit staaltje samenwerken waarmee het bewijs is geleverd dat de weg kan worden gevonden, als de wil er maar is. Alles wat je wil weten over de BIO staat op de website (1).

Hoewel de BIO steeds meer aan bekendheid wint, komt het nog weleens voor dat medewerkers bij de overheid glazig kijken wanneer privacy-adviseurs naar de BIO verwijzen. Wat voor de BIO geldt, geldt ook een beetje voor de Algemene Verordening Gegevensbescherming (AVG). De AVG krijgt steeds meer bekendheid, maar er zijn nog steeds veel mensen die slechts de klok hebben horen luiden, maar nog op zoek zijn naar de klepel. Daarom toch een heel korte introductie.

Pakket uit 2016

Op 25 mei 2016 is er een Europees pakket aan wetgevingsinstrumenten vastgesteld. Dit pakket beoogt uniformering van de bescherming van personen bij de verwerking van gegevens die indirect of direct naar hen herleidbaar zijn. Het pakket bestaat voor zover hier relevant uit de AVG en de Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad (2). Deze wetgevingsinstrumenten samen worden wel aangeduid als het Europese gegevensbeschermingspakket uit 2016. Het is niet toevallig dat ze samen het licht zagen omdat ze eenzelfde doel hebben: ze beogen een uniform beschermingsniveau te bieden aan de betrokkenen van wie de persoonsgegevens worden verwerkt. Hoewel het doel hetzelfde is hebben deze verschillende wetgevingsinstrumenten wel een andere reikwijdte.

AVG reikwijdte

De AVG is een Europese wet die rechtstreeks werkt in de Europese lidstaten maar verrassend genoeg ook daarbuiten. Dat is geregeld in artikel 3 van de AVG waar de territoriale reikwijdte van de AVG wordt bepaald. Zo is de AVG ook van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een organisatie met een vestiging in de Europese Unie, ongeacht of de verwerking in de Unie plaatsvindt. Dat betekent dat alle organisaties die een al dan niet substantiële vestiging hebben ergens in Europa (denk aan de Amsterdamse Zuidas) onder de werking van de AVG zijn gebracht (3).

De tweede uitbreiding van de territoriale reikwijdte is de verwerking van persoonsgegevens van betrokkenen die zich in de Europese Unie bevinden, door een niet in de Europese Unie gevestigde organisatie. Deze uitbreiding is beperkt tot twee situaties. Het moet gaan om verwerkingen van persoonsgegevens die verband houden met het aanbieden van goederen of diensten aan deze betrokkenen al dan niet tegen betaling. Of het moet gaan om het monitoren van hun gedrag, voor zover dit gedrag in de Europese Unie plaatsvindt (4).

De derde uitbreiding van de territoriale reikwijdte van de AVG is meer formeel van aard. De AVG is van toepassing op de verwerking van persoonsgegevens door een verwerkingsverantwoordelijke die niet in de Europese Unie is gevestigd, maar op een plaats waar krachtens het internationaal publiekrecht het lid-statelijke recht van toepassing is. Denk aan een schip dat onder de Nederlandse vlag vaart.

Naast genoemde territoriale uitbreidingen, wordt de materiële reikwijdte van de AVG tegelijkertijd beperkt. Die beperkingen vinden we in artikel 2 van de AVG. Daar staat voor zover hier relevant: 'Deze verordening is niet van toepassing op de verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.' Dat betekent huiselijk gezegd dat de AVG in deze gevallen opzij wordt gezet.

Wpg reikwijdte

De 'verwerking van persoonsgegevens door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten', is in Nederland geregeld in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). De Wpg en Wsjg zijn de Nederlandse implementatie van de genoemde Richtlijn (EU) 2016/680 uit het Europese wetgevingspakket

pakket uit 2016. Persoonsgegevens die worden verwerkt onder de Wpg noemen we politiegegevens, persoonsgegevens die worden verwerkt onder de Wjsg noemen we justitiële of strafvorderlijke gegevens. In dit artikel beperken we ons tot politiegegevens. Het verwerken van politiegegevens kan nooit dus plaatsvinden onder de AVG maar alleen onder de Wpg.

Verwerkingsverantwoordelijke AVG en Wpg

Het verwerken van persoonsgegevens onder de AVG mag alleen in opdracht van een verwerkingsverantwoordelijke. En dat kan volgens de AVG werkelijk iedereen zijn; 'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'. In de Wpg is de verwerkingsverantwoordelijke expliciet benoemd en beperkt tot een klein groepje. Voor de politie is het bijvoorbeeld de korpschef, voor de Rijksrecherche het College van procureurs-generaal (PG's) en voor de Koninklijke Marechaussee (KMar) de minister van Defensie.

Mandaat of bevoegdheid AVG

Je zult begrijpen dat een verwerkingsverantwoordelijke doorgaans niet zelf de persoonsgegevens verwerkt. Via mandaatbesluiten geeft de verwerkingsverantwoordelijke aan welke medewerkers bevoegd zijn om (welke) persoonsgegevens namens hem of haar te verwerken. De verwerkingsverantwoordelijke onder de AVG is helemaal vrij in het mandateren van de verwerkingen aan wie dan ook. Het mooie van mandaat is namelijk dat de bevoegdheden en de aansprakelijkheid altijd in handen blijven van de verwerkingsverantwoordelijke zelf. Anders gezegd: een verwerkingsverantwoordelijke kan de eigen verwerkingsverantwoordelijkheid en de aansprakelijkheid nooit delegeren. Dat is ook de kern van de privacybescherming: iemand is volgens wet verantwoordelijk voor het naleven van de wet en de regels en die kan deze verantwoordelijkheid nooit afschuiven, ontlopen of negeren. Denk aan aansprakelijkheid en boetes.

Houd ook in gedachten dat de AVG niet alleen geldt voor de overheid maar ook voor het bedrijfsleven, private organisaties en zelfs voor onszelf. Immers, elke natuurlijke persoon die persoonsgegevens verwerkt en die zich niet kan beroepen op een beperking van de materiële reikwijdte van de AVG zoals genoemd in artikel 2 AVG is een verwerkingsverantwoordelijke (5).

Mandaat of bevoegdheid Wpg

In de Wpg is dat heel anders geregeld. Bij opsporen en vervolgen mogen er om begrijpelijke redenen grotere inbreuken worden gemaakt op de persoonlijke levenssfeer. Deze ruimere bevoegdheden om inbreuk te maken op de persoonlijke levenssfeer gaan vergezeld van extra privacywaarborgen die expliciet zijn opgenomen in de wet. Een van deze waarborgen is dat deze ruimere bevoegdheden om inbreuk te maken zijn toegekend aan een afgebakende groep mensen. Het primaat van opsporing en vervolging is in Nederland huiselijk gezegd neergelegd bij politie en justitie. Eigenrichting wordt niet zo op prijs gesteld in ons democratische rechtsstelsel. Om die reden zijn de verwerkingsverantwoordelijken voor de Wpg limitatief opgesomd in de wet. Hetgeen hiervoor is opgemerkt over mandaat bij verwerkingsverantwoordelijken geldt ook voor deze limitatieve groep verwerkingsverantwoordelijken.

Daar komt nog bovenop dat de feitelijke verwerking van politiegegevens is voorbehouden aan een selecte groep mensen die in artikel 1 van de Wpg worden aangeduid als 'ambtenaren van politie'. Deze ambtenaren van politie zijn anders dan wat je in het spraakgebruik zou verwachten: 'de ambtenaar, bedoeld in artikel 2 van de Politiewet 2012, alsmede de ambtenaar van de Koninklijke marechaussee voor zover werkzaam ter uitvoering van de politietaak, bedoeld in onderdeel a, en indien artikel 46 wordt toegepast, de ambtenaar, werkzaam bij de in dat artikel genoemde dienst en de ambtenaar, bedoeld in artikel 142, eerste lid, van het Wetboek van Strafvordering'.

Uit bovenstaande volgt dat de Wpg ten opzichte van de AVG de groep verwerkingsverantwoordelijken limiteert en extra eisen stelt aan de personen die politiegegevens daadwerkelijk verwerken.

Mismatch

De oplettende lezer constateert nu een discrepantie. We

hebben hier vier verschillende soorten ambtenaren van politie (Politie, KMar, Bijzondere opsporingsdiensten en Bijzondere opsporingsambtenaren), terwijl we drie soorten verwerkingsverantwoordelijken hebben (korpschef, College van PG's, minister van Defensie). Hoe verhouden deze verwerkingsverantwoordelijken zich tot de genoemde ambtenaren van politie? Er lijkt sprake te zijn van een mismatch.

Deze ogenschijnlijke mismatch is veroorzaakt doordat in de eerdere versies van de Wpg niet alle groepen opsporingsambtenaren waren opgenomen. Opsporingsambtenaren werkzaam bij de bijzondere opsporingsdiensten (bod'en) en buitengewoon opsporingsambtenaren (boa's) zijn later toegevoegd aan het oorspronkelijke rijtje van politie, Rijksrecherche en KMar. In een van de slotbepalingen van de Wpg (artikel 46) is nu bepaald dat de opsporingsambtenaren die daar zijn genoemd ook politiegegevens verwerken. In twee algemene maatregelen van bestuur (dit noemen we een Besluit) is dit nader uitgewerkt. Een Besluit voor de opsporingsambtenaren van de bod'en en een Besluit voor de boa's.

Besluit politiegegevens bod'en

In het Besluit politiegegevens bod'en staat expliciet wie de verwerkingsverantwoordelijken zijn bij de vier Bijzondere opsporingsdiensten die Nederland rijk is:

1. Belastingdienst/Fiscale Inlichtingen- en Opsporingsdienst: onze minister van Financiën;
2. Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport: onze minister van Infrastructuur en Waterstaat;
3. Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit: onze minister van Landbouw, Natuur en Voedselkwaliteit;
4. Directie Opsporing van de Inspectie Sociale Zaken en Werkgelegenheid: onze minister van Sociale Zaken en Werkgelegenheid.

Saillant detail: de ambtenaren van politie werkzaam bij een bod zijn geen bijzondere opsporingsambtenaren maar algemene opsporingsambtenaren in dienst bij een Bijzondere opsporingsdienst (6).

Besluit politiegegevens boa's

De ambtenaar bedoeld in artikel 142, eerste lid, van het Wetboek van Strafvordering is de boa. Om erachter te komen wie de verwerkingsverantwoordelijken van de boa's zijn, moet je naar het Besluit politiegegevens boa's en het Besluit boa. Daarin staat dat de werkgever van de boa de verwerkingsverantwoordelijke is. Het is dus deze werkgever die aan de lat staat om de verplichtingen die voortvloeien uit de Wpg na te leven en niet de boa's zelf. De boa's roeien met de riemen die ze krijgen van hun werkgever. Naleven van de Wpg-verplichtingen door de werkgevers van de boa's heeft ongetwijfeld een positieve invloed op de kwaliteit van de werkzaamheden van de boa's. Dat positieve effect zal zich ook uitstrekken tot de bescherming van de persoonlijke levenssfeer van de betrokkenen van wie politiegegevens worden verwerkt.

Wpg-verplichtingen

De materiële verplichtingen die voortvloeien uit de Wpg zijn grotendeels vergelijkbaar met de verplichtingen die we kennen uit de AVG. Een aantal zaken zijn explicieter geregeld en een aantal zaken zijn echt anders. Naast de materiële verplichtingen kent de Wpg in § 5 en § 7 nog enkele expliciete toezichtbepalingen. In 2019 is het verwerken van persoonsgegevens door boa's onder de Wpg gebracht. Tot die tijd verwerkten boa's persoonsgegevens onder de AVG. Dat betekent ook dat de werkgevers van de boa's vanaf dat moment de Wpg moeten naleven. En dat brengt extra verplichtingen met zich mee. Zoals een auditverplichting waarbij de audit moet worden uitgevoerd door een externe onafhankelijke en ter zake deskundige IT-auditor. De eerste audit moet in 2021 worden uitgevoerd.

Hierna gaan we kort in op enkele van deze verplichtingen met verwijzing naar het normenkader zoals NOREA dat hanteert (7).

Registerplicht

De registerplicht uit de Wpg komt grotendeels overeen met de registerplicht uit de AVG. Zie onderstaande overzicht voor de verplichtingen van de verwerkingsverantwoordelijke ten aanzien van een registerplicht waarbij de relevante wetteksten naast elkaar zijn gezet. Zoek de verschillen:

WPG	AVG	Conform
de naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;	de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;	Ja
de doelen van de verwerking;	de verwerkingsdoeleinden;	Ja
de categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;	de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;	Ja
een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;	een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;	Ja
in voorkomend geval, het gebruik van profilering;		Nee
in voorkomend geval, de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie;	indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;	Ja
een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van		Nee
doorgiften, waarvoor de politiegegevens bedoeld zijn;		
zo mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd;	indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;	Ja
zo mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging, bedoeld in artikel 4a	indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.	Ja
de toekenning van de autorisaties, bedoeld in artikel 6		Nee

Figuur 1 – Registerplicht.

Artikel 32	WPG
1	De verwerkingsverantwoordelijke draagt zorg voor de schriftelijke vastlegging van:
a	de doelen van de onderzoeken, bedoeld in artikel 9, tweede lid;
b	de verstrekking of doorgifte van politiegegevens op grond van paragraaf 3, met uitzondering van de verstrekking, bedoeld in artikel 17 en artikel 24, eerste en tweede lid, indien dit zich niet verdraagt met het belang van de veiligheid van de staat;
c	de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing, bedoeld in artikel 27, eerste lid;
d	een inbreuk op de beveiliging van persoonsgegevens, bedoeld in artikel 33a, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie.
2	Bij de doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie, bedoeld in artikel 17a, tweede lid, onderdeel b, en derde lid, omvat de schriftelijke vastlegging de datum en tijd van doorgifte, informatie over de ontvangende bevoegde autoriteit, de reden van doorgifte en de doorgegeven gegevens zelf.
3	De verantwoordelijke draagt zorg voor de schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de Autoriteit persoonsgegevens.
4	De politiegegevens, bedoeld in het eerste lid, worden bewaard tenminste tot de datum waarop de laatste controle, bedoeld in artikel 33, is verricht.
5	Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld over de wijze van vastlegging.

Figuur 2 - Documentatieplicht.

Documentatieplicht

De documentatieplicht ontbreekt expliciet in de AVG. Impliciet is die er natuurlijk wel. Hoe kan de verwerkingsverantwoordelijke anders voldoen aan de verantwoordingsverplichtingen uit artikel 5 tweede lid en artikel 24 van de AVG?

In de Wpg is de documentatieplicht opgenomen in artikel 32 en bestaat uit de volgende onderdelen:

Loggingsplicht

Daar kunnen we kort over zijn. Deze expliciete verplichting is in Nederland nog niet in werking getreden maar dat zal niet altijd zo blijven. Voor nu laten we het daarom buiten beschouwing. Het is wel goed om je te realiseren dat het niet volledig implementeren van Europese richtlijnen niet geheel vrijblijvend is. De burger die hier last van heeft kan dan bij de rechter een rechtstreeks beroep doen op de richtlijn.

Artikel 33	Audit
1	De verwerkingsverantwoordelijke doet de uitvoering van de bij of krachtens deze wet gegeven regels controleren door middel van het periodiek doen verrichten van privacy audits.
2	De verwerkingsverantwoordelijke zendt een afschrift van de controleresultaten van de privacy audits aan de Autoriteit persoonsgegevens.
3	Indien uit de controleresultaten blijkt dat niet wordt voldaan aan het bij of krachtens deze wet bepaalde, laat de verwerkingsverantwoordelijke binnen een jaar een hercontrole uitvoeren op die onderdelen die niet voldeden aan de gestelde voorwaarden. Het tweede lid is van overeenkomstige toepassing.
4	Eenieder die betrokken is bij een controle als bedoeld in het eerste of derde lid is verplicht tot geheimhouding van de persoonsgegevens waarover hij de beschikking heeft gekregen, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht of zijn taak daartoe noodzaakt.
5	Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld betreffende de inhoud en wijze van uitvoering van de controles, bedoeld in het eerste en derde lid.

Figuur 3 - Auditplicht.

Auditplicht

De expliciete auditverplichting in de Wpg is een groot verschil ten opzichte van de AVG. Waar de AVG volstaat met het sec noemen van de verplichting om verantwoording af te leggen en transparant te zijn gaat de Wpg een stuk verder. De Wpg vult het voldoen aan die verplichting in artikel 33 verder in. Let ook op de actieve rol van de AP bij deze Wpg-audits.

Uitvoering Wpg-audit

Hoe de Wpg-audits precies moeten worden uitgevoerd en door wie, is uitgewerkt in lagere regelgeving. Zie artikel 6:5 van het Besluit politiegegevens en de Regeling periodieke audit politiegegevens. In deze regeling worden de regels voor het uitvoeren van een externe en interne audit vastgesteld. De Wpg-audit is bijvoorbeeld altijd een IT-audit die moet worden uitgevoerd door een daartoe geautoriseerde en gekwalificeerde IT-auditor (Registered EDP Auditors). Kortheidshalve wordt volstaan met de verwijzing naar deze regels.

NOREA

De beroepsorganisatie van IT-auditors (edp-ers of RE's) NOREA heeft enige tijd geleden een normenkader ontwikkeld waarbij invulling kan worden gegeven aan de toets op de naleving van de AVG. NOREA heeft nu ook ingespeeld op de Wpg-auditverplichting voor werkgevers van boa's. In juni 2021 is een NOREA Handreiking Privacy audit Wpg voor boa's gepubliceerd. Deze Wpg handreiking is niet geënt op de al bestaande NOREA Handreiking Privacy Control Framework voor de AVG en kan dus zelfstandig worden gebruikt. Het enige dat nu nog rest is een fit-gap analyse tussen de BIO en de Wpg. Daar wordt al ergens in het netwerk aan gewerkt. Wederom hulde!

De auditverplichting uit de Wpg voor werkgevers van boa's is mogelijk een verrassing voor veel werkgevers. Wanneer het een overheidswerkgever betreft, zal hij moeten voldoen aan de BIO. Dat helpt omdat daarmee de naleving van veel verplichtingen uit de Wpg zullen worden getoetst. De naleving van de extra verplichtingen uit de Wpg kunnen worden getoetst met behulp van de NOREA-handreiking. IT-auditors met kennis van de BIO en de Wpg zullen schaars zijn. Haast is geboden omdat het einde van 2021 snel in zicht komt.

Referenties

(1) https://bio-overheid.nl

(2) De Wet justitiële en strafvorderlijke gegevens (Wjsg) laten we hier buiten beschouwing.

(3) We gaan hier niet in op de precieze afbakening van het Europese territoir in juridische zin.

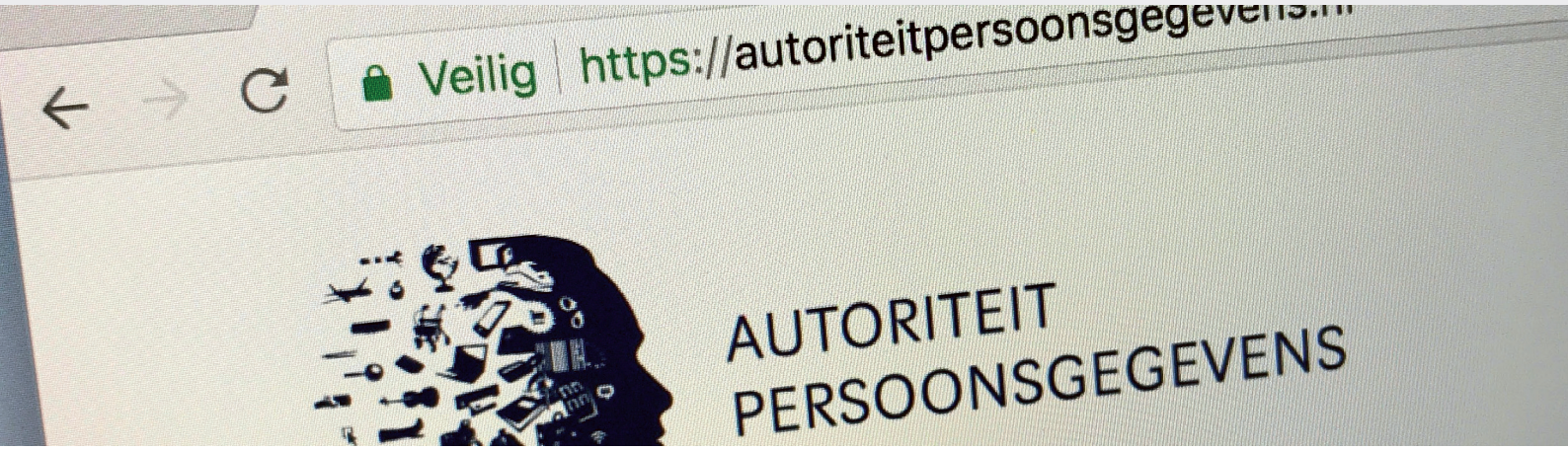
(4) Je kunt je afvragen in hoeverre deze uitbreiding ook van toepassing is op de overheid. Een interessante vraag die te ver strekt voor het doel van dit artikel.

(5) Er staat in artikel 2 AVG nog een beperking van de reikwijdte: door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit.

(6) https://www.justis.nl/producten/boa/BOD/bod.aspx

(7) www.norea.nl

Auteur: Laura de Vries is Privacy & Legal consultant bij Cuccibu. Zij adviseert verschillende organisaties op het gebied van privacy en gegevensbescherming en vertaalt de wettelijke verplichtingen uit onder andere de AVG naar praktische handvatten. Laura is te bereiken via: laura.de.vries@cuccibu.nl.



Handig is geen grondslag

Het is een veelgehoorde uitspraak op de vraag waarom bepaalde persoonsgegevens verwerkt worden: 'dat is handig'. Of: 'dat is misschien handig in de toekomst'. Helaas: handig is geen grondslag. Persoonsgegevens mogen alleen verwerkt worden als er een juridische grondslag voor is en voldaan wordt aan de basisbeginselen uit de AVG. Het blijkt voor organisaties lastig om hun doelen duidelijk te articuleren en daarna stapsgewijs te checken of iets wel mag.

Meer dan drie jaar na de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) blijkt het voor organisaties nog steeds lastig om aan alle verplichtingen te voldoen. Veelal wordt het voldoen aan wet- en regelgeving nog gezien als een checklist: bij elke verplichting een kruisje en dan ben ik klaar. Om aan de AVG te voldoen dienen organisaties echter te zorgen voor het opzetten van processen waarbij constant opnieuw geëvalueerd wordt of wat ze doen nog wel mag.

Register van verwerkingen

De meeste organisaties zijn op basis van de AVG verplicht een register van verwerkingen op te zetten (1). Hierin moet onder andere staan welke verwerkingen er binnen de organisatie plaatsvinden (handelingen dus, zoals het verzamelen, opslaan, gebruiken, wijzigen en vernietigen van gegevens) en waarom (het doel van de verwerking). Dit blijkt vaak een uitdaging. Want waarom verzamel je bepaalde gegevens? Waar gebruik je ze allemaal voor? Heb je deze gegevens wel allemaal nodig? Moet je alle gegevens die je verzamelt ook even lang bewaren? Bij het beantwoorden van deze vragen springen organisaties vaak meteen naar artikel 6 AVG, de grondslagen. In dit artikel zijn zes grondslagen opgenomen op basis waarvan persoonsgegevens verwerkt mogen worden: toestemming, (pre-)contractuele afspraken, wettelijke verplichting, vitaal belang van de betrokkene, algemeen belang/publieke taak en het gerechtvaardigde belang van de verwerkingsverantwoordelijke (of een andere partij). Je ziet het, handig is dus geen grondslag. Je zult expliciet moeten bepalen of 'handig' ook voldoet aan de vereisten uit de AVG.

Artikel 5

Voor artikel 6, komt artikel 5. In dit artikel zijn de basisbeginselen opgenomen van de AVG. Je dient eerst te bepalen of gegevens wel nodig zijn voor het doel dat je voor ogen hebt (dataminimalisatie), of, en hoe lang je deze dient te bewaren (opslagbeperking) en voor welk doel of welke doelen je de gegevens wilt gebruiken (doelbinding) voordat je kijkt naar de grondslag (hoewel dit in de praktijk vaak samenhangt). Daarbij heb je een verantwoordingsplicht, je moet dus kunnen

aantonen dat je aan de vereisten voldoet.
Als je gegevens gaat verwerken en voldoet aan de basisbeginselen, dien je vervolgens de grondslag te bepalen. Heb je bijvoorbeeld een overeenkomst met de betrokkene? Dan mag je de gegevens verwerken die nodig zijn voor het uitvoeren hiervan. Dit klinkt simpel, maar het betekent dus dat je eerst moet bepalen welke gegevens echt noodzakelijk zijn voor het uitvoeren van de overeenkomst. Bestel ik iets in een webshop, dan is het maar de vraag of bijvoorbeeld mijn geslacht een noodzakelijk gegeven is voor het uitvoeren van de overeenkomst. Immers kan ook met enkel naam en adres een pakketje worden bezorgd. Wellicht is dan nog een e-mailadres nodig voor het kunnen versturen van een track & trace code. Vraag je aanvullende gegevens? Dan doe je dat waarschijnlijk op basis van je gerechtvaardigd belang.

Gerechtvaardigd belang

Ik hoor je nu denken, is handig dan niet ook een gerechtvaardigd belang? Misschien wel, maar daarvoor moet eerst het belang van de organisatie worden afgewogen tegenover de rechten en vrijheden van betrokkenen. De inbreuk hierop moet proportioneel zijn en in relatie staan tot het doel.
De Autoriteit Persoonsgegevens (AP) formuleert het als volgt:
`Om uw verwerking te mogen baseren op de grondslag 'noodzakelijk voor de behartiging van een gerechtvaardigd belang', moet u aan drie voorwaarden voldoen. De drie voorwaarden zijn:

1. U heeft daadwerkelijk een gerechtvaardigd belang. Niet elk belang kwalificeert als een gerechtvaardigd belang.
2. De verwerking is noodzakelijk om dit belang te behartigen.
3. U heeft een afweging gemaakt tussen uw belangen en die van de betrokkenen (2).

Maar wat is dan een `gerechtvaardigd belang'? Dit heeft de AP uiteengezet in een normuitleg (3). Enkele voorbeelden zijn: fraudebestrijding, marketing aan bestaande klanten en beveiliging van computersystemen. De reacties op de normuitleg waren niet onverdeeld positief, omdat de AP heeft aangegeven dat een belang in het recht terug te vinden moet zijn, terwijl in principe elk belang dat niet strijdig is aan de wet een gerechtvaardigd belang zou kunnen zijn. Een echte inhoudelijke test voor de rechter moet nog komen, maar de eerste slag is door de AP al verloren. In de zaak tegen VoetbalTV heeft de rechter geoordeeld dat de AP niet voldoende gemotiveerd heeft waarom het gerechtvaardigde belang van VoetbalTV niet voldeed aan de eisen (4). Deze toetsing heeft geheel niet plaatsgevonden omdat de AP enkel aangaf dat `het te gelde maken van persoonsgegevens nooit een gerechtvaardigd belang kan opleveren' (5). De rechter ziet dat toch anders en volgt de redenatie van de AP niet.

Toestemming betrokkene

Wel blijkt uit zowel de normuitleg als deze uitspraak dat alles neerkomt op motivatie. `Handig' alleen zal deze toets vaak niet doorstaan. Heb je geen andere grondslag? Dan kun je nog om toestemming vragen. Deze toestemming moet voldoen aan de vereisten uit artikel 7 en dus vrijwillig, specifiek, geïnformeerd en ondubbelzinnig zijn. Je moet de betrokkene dus goed uitleggen wat je met de gegevens gaat doen, hoe lang je ze gaat bewaren en je mag de toestemming niet verstoppen in een lange lap tekst, of de toestemming aannemen door gebruik van bijvoorbeeld een website.

Let op, verwerk je ook bijzondere persoonsgegevens zoals politieke voorkeur, religie of gegevens over de gezondheid, dan is het hebben van een grondslag niet voldoende. Aanvullend dient de organisatie dan ook nog te vallen onder een uitzondering zoals opgenomen in artikel 9 AVG. Bijvoorbeeld verwerking voor het voldoen aan verplichtingen op gebied van sociale zekerheid, het onderbouwen van een rechtsvordering of een algemeen belang op gebied van volksgezondheid. Val je hier niet onder en wil je de gegevens toch verwerken? Dan dien je expliciete toestemming te vragen aan de betrokkene. Dit betekent dat, in aanvulling op de eisen uit artikel 7 AVG, de toestemming voor het verwerken van de bijzondere persoonsgegevens expliciet moet worden benoemd.

Dus nee, handig is geen grondslag. Als je persoonsgegevens verwerkt, op welke manier dan ook, moet je eerst een concreet doel formuleren en de voorgenomen verwerking toetsen aan de wet. En denk je dat je klaar bent met inventariseren en vastleggen? Dan wordt het daarna tijd om te beginnen aan de review om na te gaan of alles nog steeds klopt en indien nodig aanpassingen te doen.

Referenties

(1) Artikel 30 AVG
(2 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken
(3) https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf
(4) https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2020:5111
(5) https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBMNE:2020:5111

Auteurs: Geoffrey Van den Bergh is Privacy en Data Management Consultant bij CRANIUM Nederland. Hij ondersteunt organisaties in het oplossen van complexe problemen op het gebied van gegevensverwerking. Geoffrey is te bereiken op geoffrey.vandenbergh@cranium.eu. Marloes de Bruin is Privacy, Security en Data Management Consultant bij CRANIUM Nederland. Ze begeleidt organisaties en heeft programma's voor privacy, security en data management gecreëerd en geïmplementeerd. Marloes is te bereiken via marloes.debruin@cranium.eu.

Méér met data.
Maar wát eigenlijk?

De mogelijkheden van data zijn eindeloos. Vooral het analyseren en inzetten van gestructureerde en ongestructureerde data voor bepaalde doeleinden kan een schat aan waarde opleveren voor organisaties. Data in bezit van organisaties leidt naar inzichten en inzichten leiden weer naar kennis. Welke manieren zijn er om data te analyseren onder de Algemene Verordening Gegevensbescherming (AVG) en hoe haal je de meeste waarde uit data?

Het internet der dingen gaat in essentie over 'dingen' of objecten die via het internet met elkaar verbonden zijn. In feite wordt door deze koppeling een model van onze realistische wereld in het internet afgebeeld. Een model waarvan we de elementen kunnen 'voelen' en 'beïnvloeden', onafhankelijk waar wij ons bevinden. In het algemeen zie je dat IoT wordt gebruikt om slimmer om te gaan met alles wat al bestaat, door de eigenschappen te meten en deze waarden naar een platform op het internet te sturen. Dit platform kan vervolgens besluiten hier iets slims mee te doen, bijvoorbeeld de omgeving aan te passen. Vandaar dat de term 'smart' vaak valt in combinatie met IoT. Er gaat geen dag voorbij of je hoort over Smart City, Smart Industry, Smart Home, Smart Energy en ga zo maar door. IoT maakt het mogelijk om steeds meer privacygevoelige data te generen en te combineren. Door de toename van dit soort toepassingen, vormen privacy en security een steeds grotere uitdaging binnen dergelijke ontwikkelingen.

De verwerkingsverantwoordelijke bepaalt de doeleinden waarvoor en de middelen waarmee persoonsgegevens worden verwerkt. Als een organisatie dus beslist 'waarom' en 'hoe' persoonsgegevens moeten worden verwerkt, is zij de verwerkingsverantwoordelijke. De verwerker verwerkt persoonsgegevens uitsluitend namens de verwerkingsverantwoordelijke, en is vaak een derde partij buiten de organisatie.

Organisaties worden niet zozeer beperkt in het doen van data-analyses, maar de manier waarop is wel afhankelijk van de verplichtingen uit de wetgeving. Er zijn inmiddels goede oplossingen beschikbaar om analyses te kunnen uitvoeren zonder dat de gegevens herleidbaar zijn naar individuen en de privacy van de betrokkenen wordt gewaarborgd. Zo kun je gegevens aggregeren waardoor je alleen nog totalen zichtbaar maakt, of je kunt een hele database anonimiseren of synthetiseren. Op deze manier kan een organisatie meer inzicht krijgen in gegevens en verbanden maar kunnen zij ook nieuwe diensten aanbieden of hun huidige dienstverlening verbeteren.

Data is in bits z'n goud waard

Vaak is data-analyse binnen organisaties gericht op het opleveren van managementinformatie zoals omzet- of verzuimcijfers. Maar sommige organisaties willen meer inzicht verkrijgen om nieuwe producten te bouwen en de huidige dienstverlening te verbeteren. Neem als voorbeeld een financiële dienstverlener die o.a. salarissen betaalt en ook verzekeringen aanbiedt. De organisatie die al deze salarissen en verlofaanvragen verwerkt en bijhoudt, heeft een schat aan data opgeslagen. Zo wordt bijvoorbeeld de functie bijgehouden, het salaris geregistreerd en leeftijd bijgewerkt. Maar deze organisaties worden in het kader van de AVG vaak gekwalificeerd als verwerker. Het doen van data-analyses op alle salarisgegevens van de medewerkers van de klant is voor eigen doeleinden vaak niet toegestaan, mits dit contractueel wordt geregeld of de analyses aantoonbaar kunnen helpen bij het onderhoud en verbetering van het systeem.

Ook voor een verwerkingsverantwoordelijke is het interessant om te weten hoe behoeftes van klanten aan elkaar gekoppeld kunnen worden. Zo kan bol.com bijvoorbeeld uit de data van gekochte producten een database opbouwen, en als deze groot genoeg is, op basis van de resultaten behoeften voorspellen van klanten die soortgelijke aankopen doen, en deze met een korting aanbieden.

Wanneer er analyses worden uitgevoerd, wordt data al snel geanonimiseerd, omdat op geanonimiseerde data de AVG niet van toepassing is. Maar het anonimiseren van persoonsgegevens zelf wordt gezien als een verwerking van persoonsgegevens in het kader van de AVG. Derhalve moet deze verwerking worden uitgevoerd op een wijze die in overeenstemming is met de AVG en zich houdt aan de beginselen van gegevensbescherming. Er zijn verschillende methodes om gegevens te anonimiseren. De methode die je kiest, is afhankelijk van het type gegevens dat je wilt anonimiseren.

Analyse op traditionele wijze

Bij klassiek anonimiseren wordt de originele dataset gemaskeerd om te waarborgen dat individuen niet kunnen worden herleid. Een veelgebruikte methode is om gegevens zoals voornaam en achternaam in willekeurige volgorde te 'husselen', zodat je nieuwe voornaam/achternaam combinaties krijgt. Een andere methode om data te maskeren is om een kolom, die je niet nodig hebt voor je test, leeg te maken. Op die manier worden privacygevoelige gegevens en alle risico's ervan letterlijk uit het veld geruimd. Het 'scramblen' van data is een derde methode die data onherkenbaar maakt: het vervangt tekens door x en cijfers door 1. De data kan via vooraf gedefinieerde regels dus worden vervangen.

Een nadeel hiervan is dat de datakwaliteit verslechtert doordat de data wordt bewerkt. Dit komt doordat in het procedé van anonimiseren bepaalde velden ofwel weggehaald worden ofwel gemaskeerd, omdat ze op basis hiervan niet meer herleidbaar zijn tot een individu. Het nadeel hiervan is dat al deze data aan elkaar gekoppeld is. Wanneer een computer deze data niet meer kan lezen, komen er omissies in het profiel van de dataset. Zo kan er in de praktijk geen koppeling meer plaatsvinden tussen historische en toekomstige datasets. Daarnaast blijft de data een bewerkte versie van het origineel waarbij er vaak nog relaties blijven bestaan tussen de oorspronkelijke en geanonimiseerde data. In de praktijk is het dus onvoldoende om identificeerbare gegevens te verwijderen uit bepaalde datasets. Het loskoppelen van (in)direct identificerende persoonsgegevens en de overige gegevens moet onomkeerbaar zijn. Je mag deze gegevens ook in een later stadium niet alsnog aan elkaar kunnen koppelen. Bijvoorbeeld door andere (bijkomende of nieuwe) gegevens of technieken te gebruiken, waardoor je personen toch nog zou kunnen identificeren. Daarom is anonieme data vaak niet echt anoniem. Binnen eenzelfde organisatie is het namelijk relatief eenvoudig te achterhalen op wie de geanonimiseerde gegevens betrekking hebben door intern beschikbare verschillende datasets naast elkaar te leggen. Om gegevens daadwerkelijk volledig te anonimiseren moeten deze datasets geaggregeerd worden over een voldoende grote groep personen.

Een nieuwe speler op de markt: fictieve data

Het nadeel van geaggregeerde gegevens is dat deze gegevens vaak niet geschikt zijn om te gebruiken voor verdere ontwikkeling en testen. Om dit wel mogelijk te maken, kunnen gegevens gesynthetiseerd worden. Dit houdt in dat gegevens worden gegenereerd op basis van fictieve gegevens. Er kan kunstmatige intelligentie worden toegepast om de kenmerken, structuur en waarde van originele data te behouden. Het gevolg is volledig nieuwe, kunstmatig gegenereerde data met een dusdanig hoge kwaliteit dat deze data gebruikt kan worden alsof het originele data is, maar dan zonder te hoeven voldoen aan privacywetgeving omdat er geen relatie meer is tussen de originele data en er dus ook geen sprake meer is van persoonsgegevens. Het gebruik van persoonsgegevens wordt daarnaast geminimaliseerd, hierdoor wordt het risico op datalekken ook drastisch gereduceerd. Daarnaast kunnen organisaties of afdelingen binnen de organisatie, toegang krijgen tot datasets die eerder niet mochten worden gebruikt wegens privacywetgeving.

De datakwaliteit is dusdanig hoog dat zelfs het ontwikkelen van complexe algoritmes en machine-learning modellen mogelijk is op basis van synthetische data. AI gegenereerde synthetische gegevens kunnen worden gebruikt alsof het originele gegevens zijn. Synthetische data biedt het best mogelijke alternatief omdat het de kenmerken, relaties en statistische patronen behoudt, zoals ook in de originele data. Hiermee kan men dus echt datagedreven innovaties realiseren.

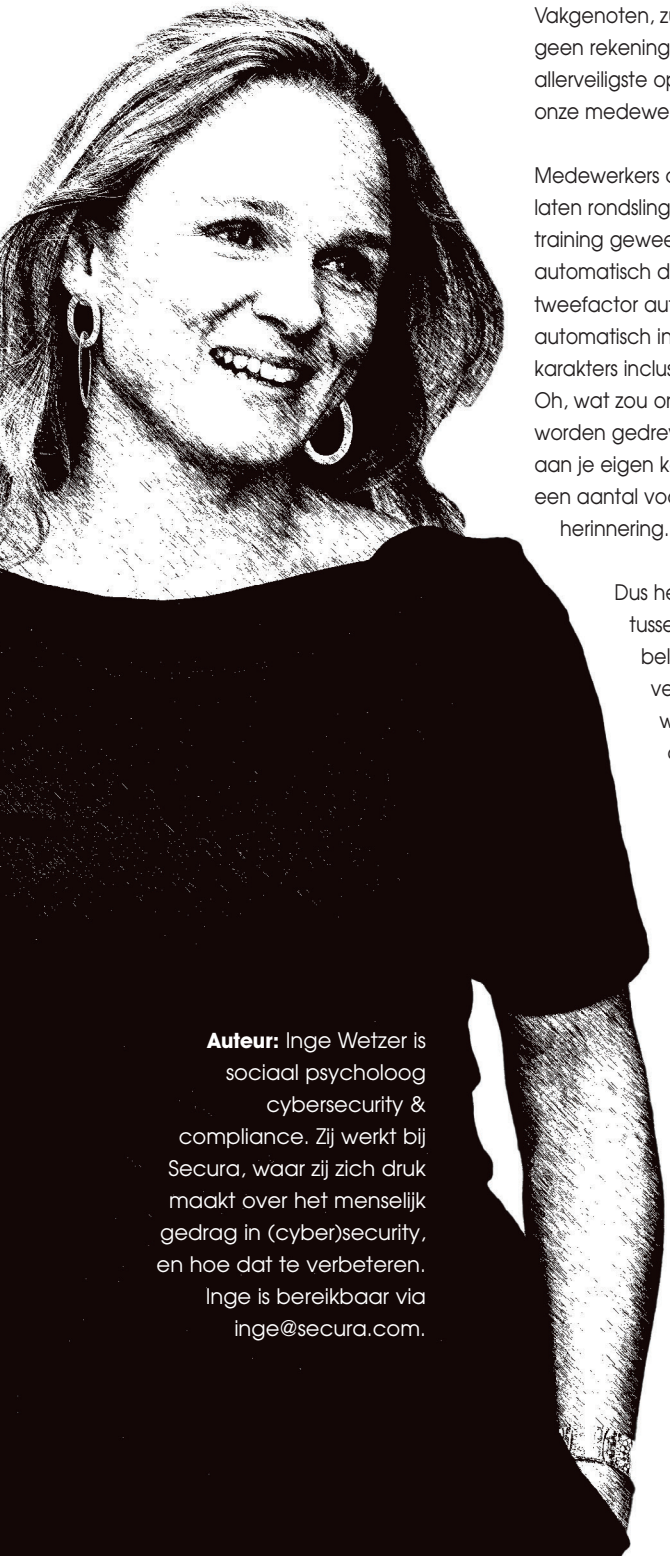
De oorsprong van het gebruik van synthetische data komt uit testmanagement, omdat er door het synthetiseren geen productiedata wordt gebruikt in de testomgeving. Het nadeel is dus dat synthetische data nog niet wordt gezien als een algemene geaccepteerde manier van werken. Andere nadelen zijn dat een kopie van de productieomgeving overzetten naar een ontwikkel- en testomgeving relatief eenvoudig is, hiertegenover is het een stuk ingewikkelder om een goede synthetische dataset te ontwikkelen. Want goede synthetische datasets bevatten weliswaar fictieve gegevens, toch dienen ze bepaalde overeenkomsten te hebben met de originele data. Een voorbeeld hiervan zijn de verhoudingen tussen verschillende data-objecten, deze dienen ongeveer gelijk te blijven aan de originele data. In het geval van de salarisadministrateur, is dit ook van belang. De organisatie maakt namelijk gebruik van meerdere bronsystemen. Wil je dat de verbanden tussen verschillende ID-nummers uit meerdere systemen blijft bestaan, dan dient het gesynthetiseerde ID-nummer ook hetzelfde zijn.

Fictie leidt tot werkelijke waarde

Afhankelijk van wat voor organisatie je bent en hoe datagedreven jouw organisatie wil en kan zijn, is de keuze voor synthetische data ingewikkeld. Wanneer de financiële dienstverlener namelijk de databases in de verschillende systemen synthetiseert, kunnen zij nog steeds de juiste analyses doen en nieuwe diensten aanbieden. Denk bijvoorbeeld aan een salarisvergelijker. De salarisveranderingen die normaal doorkomen van de medewerkers van klanten, worden ook gebruikt om te analyseren wat een marktconform salaris is. Het kan voordelig zijn voor zowel werknemer als werkgever, want een werkgever kan bepalen wie te veel of juist te weinig betaald krijgt, terwijl een werknemer zichzelf kan vergelijken ten opzichte van anderen met gelijke kenmerken.

Met de huidige trends en ontwikkelingen in techniek is het de vraag of klassiek anonimiseren nog echt anoniem is en de kwaliteit van data goed genoeg om analyses te kunnen doen die inzicht geven. Door het gebruik van nieuwere technieken zoals synthetiseren kunnen organisaties analyses doen die niet alleen AVG-compliant zijn, maar ook inzicht geven en waarde creëren voor de organisatie.

Klosje tussen de deur



Auteur: Inge Wetzer is sociaal psycholoog cybersecurity & compliance. Zij werkt bij Secura, waar zij zich druk maakt over het menselijk gedrag in (cyber)security, en hoe dat te verbeteren. Inge is bereikbaar via inge@secura.com.

Vakgenoten, zullen we samen even dromen? Stel je eens voor dat we bij onze oplossingen geen rekening meer hoeven te houden met werkbaarheid. Een walhalla! Overal zouden we de allerveiligste oplossing voor informatiebeveiliging kunnen kiezen, hoe ingewikkeld die ook is voor onze medewerkers!

Medewerkers die een paar maanden na je e-mail toch weer vertrouwelijke stukken printen, laten rondslingeren en mee naar huis nemen? We zetten gewoon de printfunctie uit! Naar een training geweest maar nog steeds locken ze hun computers niet? Na een minuut inactiviteit automatisch dan maar. We kiezen het best beveiligde file exchange program met uiteraard tweefactor authenticatie. Sluiten mensen hun kantoor niet af? Een dranger erop waardoor hij automatisch in het slot valt. En iedereen verplicht een sterk wachtwoord van minimaal 15 karakters inclusief verplichte leestekens, cijfers, etc.
Oh, wat zou ons vak makkelijker worden. Maar de werkelijkheid is dat mensen niet alleen worden gedreven door wat de beste oplossing, en dus het verstandigste is. Even terugdenken aan je eigen keuzes en gedrag: doe je altijd wat het slimste is? Waarschijnlijk niet en heb je zo een aantal voorbeelden paraat. Ik hoef voor mezelf in ieder geval geen week terug in mijn herinnering...

Dus helaas kent iedereen die werkt in de (informatie)beveiliging de precaire balans tussen veiligheid en werkbaarheid. Want mensen vinden veiligheid heus wel belangrijk, maar het moet wel een beetje makkelijk en snel zijn. Als we namelijk de veiligste oplossing willen kiezen voor een probleem, is dit vaak ook meteen de minst werkbare. En mocht je daar niet zo mee zitten... het grote gevaar van oplossingen die slecht werkbaar zijn, is dat de drempel om ze te gebruiken hoger wordt. Met als gevolg dat mensen creatieve manieren gaan vinden om eromheen te werken. Daar gaat je beveiliging...

Want als je op je werk niet meer kunt printen, mail je het gewoon naar je privémail en print je het thuis. Lockt je computer automatisch veel te snel? Dan plak je toch iets op een toets zodat er altijd activiteit blijft en hij nooit meer lockt. En is dat file exchange program te ingewikkeld, dan zijn er gelukkig nog makkelijke (gratis) alternatieven. Valt je deur automatisch in het slot en geen zin om je sleutel steeds mee te nemen? Een klosje ertussen biedt de uitkomt. Iedere vier weken een nieuw wachtwoord? Simpel, dan neem je toch gewoon de naam van je kind met een getal erachter en hoog je dat getal iedere vier weken even op. En zo streven de veiligste oplossingen precies hun doel voorbij.
Dus, zit er voor ons niets anders op dan steeds te blijven koorddansen. Zoeken naar de balans tussen veiligheid en werkbaarheid. De kunst is steeds te kiezen voor díe oplossing die het veiligst is zonder dat de drempel zo hoog is dat mensen workarounds gaan zoeken.
Werkbaarheid is dus net zo cruciaal als veiligheid. Maar het was wel even een mooie droom.

Inge

Auteur: Nico Mookhoek is privacy jurist en oprichter van DePrivacyGuru. DePrivacyGuru helpt organisaties op een pragmatische manier met hun privacyvraagstukken. Van FG as a service tot standaarddocumenten en hoogwaardig advies. Nico is daarnaast jurylid van de Nederlandse Privacy Awards. Nico is bereikbaar via: mookhoek@nmla.nl.

Algemene Verordening Gegevensbescherming

Wat heeft drie jaar AVG ons gebracht?

Afgelopen mei was de Algemene Verordening Gegevensbescherming (AVG) drie jaar van kracht. De nieuwe wet, een implementatie van een Europese Richtlijn, werd samen met de Uitvoeringswet, de UAVG, op 25 mei 2018 van toepassing. Wat heeft de nieuwe wet de eerste drie jaar van haar bestaan opgeleverd?

Bij de invoering werd vooral de nadruk gelegd op de hogere boetes die de toezichthouder, de Autoriteit Persoonsgegevens (AP), op kan leggen. De maximale boete die onder de AVG opgelegd kan worden is 20.000.000 euro of 4% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen. Hoewel dit aspect veel aandacht kreeg, is de kans op een boete voor een gemiddeld bedrijf, klein.

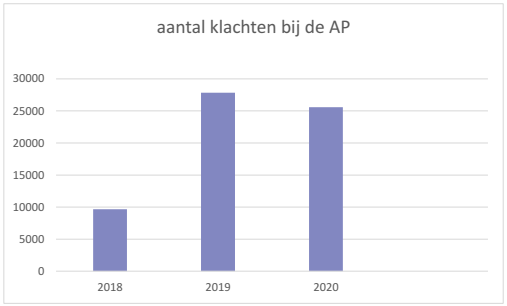
Werden er dan helemaal geen boetes uitgedeeld? Jazeker wel, en vrij forse ook. Bureau Krediet Registratie (BKR) is koploper met een boete van 830.000 euro voor het berekenen van kosten voor een inzageverzoek. Een bedrijf dat vingerafdrukken van haar personeel liet vastleggen voor toegangscontrole kon 725.000 euro boete aftikken. Hekkensluiter van de top 3 is Uber dat al kort na de invoering van de AVG in november 2018 een boete opgelegd kreeg van 600.000 euro voor het niet melden van een datalek. Voor hetzelfde feit kreeg Booking.com afgelopen maart een boete van 475.000 euro.

Het HagaZiekenhuis kreeg in juli 2019 een boete van 460.000 euro opgelegd voor het onvoldoende beveiligen van persoonsgegevens (door de Rechtbank later gematigd tot 350.000 euro). Ook het OLVG kreeg een boete voor slecht beveiligde patentendossiers opgelegd: 440.00 euro. Maar ook kleinere organisaties ontsnappen niet aan het toezicht van de AP. Een orthodontiepraktijk moest 12.000 euro overmaken aan de AP vanwege een onbeveiligde patiëntenwebsite.

Op de site van AP zijn al deze boetes, en ook de andere opgelegde sancties terug te lezen. Het boetebeleid is daarbij gebaseerd op de beleidsregels zoals die in 2019 zijn vastgesteld. Een onderbouwing van de boete gebaseerd op deze beleidsregels is te vinden in het Besluit over de betreffende boete.

Privacy bewustzijn neemt toe

Tweede opvallende ontwikkeling in de drie jaar dat de AVG van kracht is, is het toegenomen privacy bewustzijn bij burgers. Uit een onderzoek van de AP begin 2020 blijkt dat 94% zich zorgen maakt over de bescherming van haar/zijn persoonsgegevens, 32% daarvan maakt zich zelfs ernstige zorgen. De door de AP opgelegde boetes zullen daar zeker aan bijgedragen hebben. Maar ook de zichtbaarheid van de AP als de privacy in het geding is heeft hierbij geholpen, zoals bij de CoronaMelder App. Dat toegenomen privacy bewustzijn bij burgers vertaalt zich ook in het aantal klachten dat de AP



Figuur 1 - Aantal klachten bij AP.

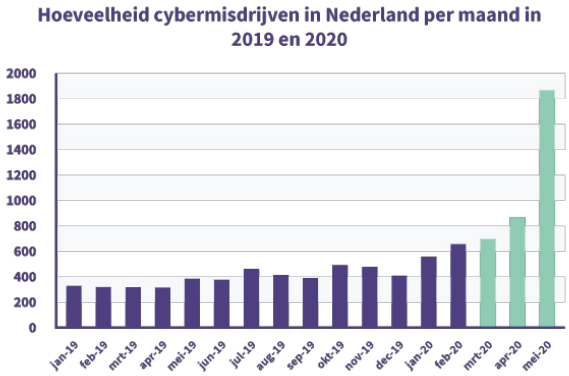
ontving. Sinds de invoering van de AVG hebben burgers het recht een klacht in te dienen bij de toezichthouder als zij niet tevreden zijn over de wijze waarop een organisatie met hun persoonsgegevens omgaat. In 2019 groeide dit explosief naar 27.850 klachten. In 2020 bleef het met 25.590 klachten vrijwel op hetzelfde hoge niveau.

De toename betekende een forse vertraging van de afhandeling van klachten door de AP. In maart 2021 luidde de voorzitter van de AP hierover de noodklok. Gemiddeld duurt het volgens hem zes maanden eer de AP kan beginnen met de behandeling van een klacht. Die signalen van de voorzitter klinken al langer. In een interview met Trouw in november 2020 geeft hij al aan dat er achterstanden zijn en dat uitbreiding van de capaciteit met 182 FTE noodzakelijk is.

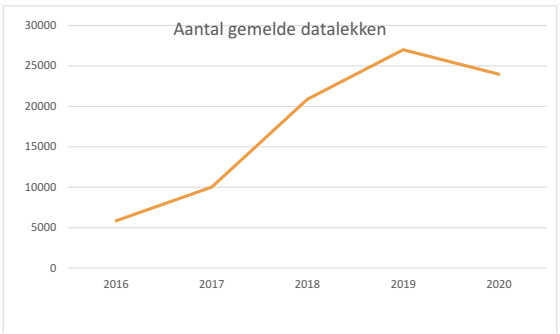
Naar aanleiding van deze signalen liet de minister van Rechtsbescherming, Sander Dekker, door KPMG een onderzoek doen. Uit het onderzoek dat in november 2020 verscheen, blijkt dat de kosten van de AP ten opzichte van andere toezichthouders (ACM, AFM, AT en NVWA) over het algemeen lager zijn. Europees gezien mag de AP volgens het KPMG-rapport niet klagen. Vergeleken met de 31 European Data Protection Board-leden heeft de AP een relatief hoog budget en kent ze een relatief sterke groei in budget en personeel. Tegelijkertijd heeft de AP te maken met relatief meer klachten en meer meldingen van datalekken.

Het rapport signaleert ook dat er nog werk aan de winkel is op het gebied van automatisering en organisatieontwikkeling. 'AP is een organisatie in opbouw. Een aantal functies is nog niet ingevuld, de automatiseringsgraad is laag en bedrijfsvoering staat nog in de kinderschoenen.'

Nadat minister Dekker probeerde de beslissing naar een



Figuur 2 - Aantal Cybermisdrijven in Nederland.



Figuur 3 - Aantal datalekken gemeld bij Autoriteit Persoonsgegevens.

volgend kabinet te tillen, stemde de Tweede Kamer toch in met een motie om de AP uit te breiden. Vanaf 2022 gaat de AP van 184 medewerkers naar 470 voltijdsmedewerkers.

Toename cybercriminaliteit = toename aantal datalekken

Sinds de uitbraak van COVID-19 in 2020 is de cybercriminaliteit fors toegenomen. In mei 2020 is voor het eerst een historische mijlpaal bereikt: er werden meer incidenten op het gebied van cybercriminaliteit bij de politie gemeld dan woninginbraken.

Uit de grafiek blijkt dat maart 2020 een stijging van 119% kende t.o.v. maart 2019. In de maand april werd dat nog overtroffen. Het aantal meldingen van cybercriminaliteit nam in die maand met 174% toe ten opzichte van april 2019.
De cijfers over toenemende cybercriminaliteit zijn ook terug te zien in de rapportage van de AP over datalekken. Een hack, phishing of malware incident leidt altijd tot een datalekmelding. Van een datalek is immers ook sprake als persoonsgegevens gecompromitteerd zijn geraakt, zoals wanneer door een hack het systeem platligt en persoonsgegevens niet meer bereikt kunnen worden. Niet elk beveiligingsincident hoeft dus een datalek te zijn, maar als er persoonsgegevens in het geding zijn, is sprake van een datalek en zal er een melding gedaan moeten worden bij de AP.
De AP geeft jaarlijks een overzicht en analyse van de bij haar gemelde datalekken. De gegevens zijn beschikbaar vanaf 2016.

Sinds de invoering van de AVG is het aantal datalekmeldingen spectaculair gestegen. In 2017 bedroeg het aantal meldingen 10.009, wat al bijna een verdubbeling was ten opzichte van de 5.849 meldingen in 2016. In 2018, het eerste jaar van de AVG werden 20.881 meldingen gedaan, een toename van meer dan 100%. De stijgende lijn zette zich voort in 2019. Het jaar 2020 liet een trendbreuk zien, het aantal meldingen daalde dat jaar rond de 10%. Volgens de toelichting van de AP bij deze cijfers is de oorzaak van deze daling een verminderd aantal meldingen van incassobureaus die een andere werkwijze hebben geïmplementeerd.

Let wel: bovenstaande cijfers betreft het aantal gemelde datalekken. Uit de boetes die aan Uber en Booking.com zijn opgelegd, blijkt dat niet elk datalek ook gemeld wordt bij de AP.

In de rapportage over 2020 licht de AP het aantal datalekken dat verband houdt met cybercriminaliteit extra toe. In 2020 steeg het aantal meldingen over hacking, malware of phishing met 30% ten opzichte van 2019 naar 1.173 meldingen. Opmerkelijk is dat bij 41,5% van de meldingen meer dan 500 personen waren betrokken. Datalekmeldingen met deze oorzaak komen het meest voor in de sector gezondheid en welzijn (13%) gevolgd door onderwijs (11%), ICT-dienstverlening (9%) en handel en autobranche (8%). Op basis hiervan komt de AP tot de conclusie dat vooral grotere organisaties die persoonsgegevens van veel mensen verwerken het doelwit zijn van hacking, malware of phishing.

Het is nu aan de privacy professionals, de Autoriteit Persoonsgegevens maar zeker ook aan de FG's en PO's in het veld om de volgende fase in te gaan.

Toekomst

De eerste drie jaar heeft de AVG in Nederland definitief een plek verworven. Steeds meer organisaties realiseren zich dat privacy een blijvertje is en geen hype. Om de privacy functie te versterken nemen steeds meer organisaties naast een vaak verplichte functionaris gegevensbescherming (FG) ook een privacy officer (PO) aan. Die laatste is meer eerste aanspreekpunt voor de medewerkers bij privacy vragen en issues.

De Autoriteit Persoonsgegevens gaat uitbreiden, wat ruimte geeft om de taken voortvarender uit te voeren. En voor wie dacht dat het allemaal wel weer over zou waaien: de opgelegde boetes zijn niet mals. Ook de burger wordt sinds de invoering van de AVG steeds privacy bewuster en doet meer beroep op zijn rechten uit de AVG.

Kortom, de eerste stappen zijn gezet en het privacy vak groeit naar volwassenheid. Het is nu aan de privacy professionals, de Autoriteit Persoonsgegevens maar zeker ook aan de FG's en PO's in het veld om de volgende fase in te gaan.

Twee zaken zijn daarbij wat mij betreft essentieel. Ten eerste meer betrokkenheid van directie en management bij het onderwerp privacy, daar schort het nu nogal eens aan. De FG is bij uitstek de figuur om dit onderwerp bij hen op de agenda te krijgen zodat het net als Legal en Finance een vaste plek krijgt bij het Bestuur.

Een tweede stap die in het verlengde daarvan ligt is de focus te verbreden van AVG naar privacy. Nu de AVG geïmplementeerd is en wordt onderhouden, wordt het tijd te kijken naar privacy in de brede zin van het woord. Daarbij komen meer beleidsmatige onderwerpen aan de orde. Onderwerpen als: 'Gaan we meer doen met het onderwerp privacy nu we voldoen aan de AVG?' 'Hoe kunnen we een privacy gerichte organisatie worden?', 'Willen we privacy gecertificeerd worden?', 'Hoe kunnen we met privacy waarde creëren?, 'Willen we wat met een onderwerp als data-ethiek?'

Kortom, na drie jaar AVG zijn de eerste stappen gezet, nu ligt de bal bij de privacy professionals om het vak tot volwassenheid te brengen.

Bronnen

https://www.autoriteitpersoonsgegevens.nl/nl/publicaties/boetes-en-sancties

Onderzoek taken en financiële middelen bij de AP, KPMG, 2 november 2020.

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken

Auteur: Lilian Knippenberg is senior information security officer & plaatsvervangend CISO bij de Gemeente Den Haag. Dit artikel is op persoonlijke titel geschreven. Je kunt Lilian bereiken via LinkedIn.

Privacy podcasts

Voor ons werk houden we continu de (technologische) ontwikkelingen in de gaten, bekijken we waar de risico's zitten en proberen we bij te dragen aan innovatie door security by design. Privé ben ik bepaald geen 'early adopter', maar nu ben ik helemaal om! Waarvoor? Voor de podcast!

1: PrivacyHack!

Deze Nederlandse podcast is een hele mooie samenwerking tussen een IT- en privacy-jurist en een ethisch hacker. Ze bespreken technologische onderwerpen met een privacy component, zoals het Internet of Things, VPN, cryptografie en zero-day kwetsbaarheden. De ethisch hacker legt de technische onderwerpen goed uit, de jurist bespreekt de privacy component. Ze stellen elkaar alle vragen, ook de 'domme', die veel vaker gesteld zouden moeten worden. Sinds december 2020 komt er elke maand een aflevering van de podcast online, op het moment van schrijven zijn er negen afleveringen te beluisteren. Deze podcast wordt gemaakt door Marie-José en Martijn.

2: Data privacy podcast

Het onderschrift van deze Amerikaanse podcast is kort en krachtig: 'Real-world insights from privacy thought leaders'. Dit is een professionele, meer journalistiek aandoende podcast, waarin host Tom McNamara met wisselende gasten verschillende onderwerpen bespreekt. Van risicomanagement tot een register van verwerkingen, van effectieve awareness tot meer technische onderwerpen als 'Apple versus tracking'. Daarnaast is er een nieuwe serie 'Leaders in Privacy Tech' opgenomen, waarbij een voorloper in privacy technologie vertelt over zijn/haar visie en product. Dat laatste maakt het wat commerciëler, maar ook juist interessant om te horen hoe er in Amerika door innovators tegen privacy wordt aange-

keken. Meer informatie over de podcast kun je vinden op https://dataprivacypod.com.

3: Data Protection Made Easy

Deze Britse podcast bestaat eigenlijk uit twee onderdelen: de ene week GDPR Radio – News & Views, de andere week een specifiek onderwerp. Beide onderdelen zijn in de basis geen podcast, maar een videocall die daarna gepubliceerd worden als podcast. Je kunt je ook aanmelden voor de sessies en live meedoen en vragen stellen. De GDPR Radio bespreekt informeel het nieuws van die periode en duikt daarin. Hierbij kun je denken aan het certificatieschema dat door de toezichthouder online gezet is. Daarnaast dus de specifieke onderwerpen, zoals over bewaartermijnen, awareness en DPIA's (met de mooie titel 'To DPIA or not to DPIA). De afleveringen zijn vrij lang (60 minuten), maar je kunt de podcast goed in twee of meer keren beluisteren. Ik vind dan ook dat ze de belofte 'data protection made easy' prima waarmaken. Ook deze sessies kun je overigens live bijwonen. Op dit moment staan er 39 afleveringen online. De podcast wordt gemaakt door adviesbureau Data Protection People.

4: GDPR Now!

Britse podcast over wetten gerelateerd aan security en privacy in de praktijk. Telkens komen er meerdere specialisten aan het woord. De gesprekken zijn interessant en goed te beluisteren. Je hoort in deze podcast de Britse cultuur door: niet alleen in de tongval, maar ook in de rust en zakelijkheid. Er staan nu 30 afleveringen online. Deze podcast wordt gemaakt door Karen Heaton (adviesbureau Data Protection 4 Business & Thisisdpo!).

5: Privacy Podcast

Ook dit is een Nederlandse podcast. Gasten gaan met elkaar in gesprek over specifieke privacy onderwerpen met titels als 'de dagelijkse praktijk van de Boa (en de WPG)' en 'de Data Pro Code'. Deze podcast geeft een mooi beeld van specifieke Nederlandse onderwerpen. Helaas is de frequentie niet hoog en niet voorspelbaar; er staan sinds april 2020 nog maar 7 podcasts op Spotify en er zit veel tijd tussen. Deze podcasts worden gemaakt door adviesbureau Verdonck, Klooster & Associates (VKA).

6: Data Protection and ICT

Interessant is de maker van deze podcast: PanelFit. PanelFit is een organisatie die als doel heeft om ethische en juridische problemen (waaronder op het gebied van privacy) als gevolg van ICT te verminderen. Met subsidie van de EU maken zij o.a. een 'mutual learning platform' dat de uitwisseling tussen onderzoekers en innovators moet bevorderen. In de podcast komen vooral onderzoekers aan het woord. Dat geeft een totaal andere invalshoek dan de andere hier besproken podcasts. Eerlijk gezegd is het daardoor soms ook wel erg theoretisch. Meer informatie kun je vinden op www.panelfit.eu.

7: Data Protection Breakfast Club

Wat zijn jouw associaties bij de term 'breakfast club'? Voor mij past deze Amerikaanse podcast daar bij: een gezellig gesprek tussen mensen die overkomen als een stel vrienden. En dat is best knap, omdat in elke podcast andere gasten en uiteenlopende onderwerpen langskomen. De hosts spreken met steeds wisselende gasten over hun functie, het bedrijf waar ze werken en hun visie op privacy. Deze podcast is dus een stuk minder zakelijk en de hosts gaan ook regelmatig off-topic. De hosts zijn privacy professionals Andy Dale (van Alyce) en Pedro Pavon (van Facebook), die op dit moment 34 afleveringen online hebben staan.

8: The Privacy, Security, & OSINT Show

Wekelijkse Amerikaanse podcast over allerhande onderwerpen op het gebied van privacy en security in relatie tot open source intelligence (OSINT). De maker is Michael Bazzell die in de podcast ook sterk zijn eigen mening laat doorklinken. Hij bespreekt onderwerpen in detail met oog voor technologie, wetten en normenkaders en verbindt deze mooi met elkaar. Er komt elke week een podcast online, op het moment van schrijven zijn het er al 232. Wel is dit een éénmansshow, dus je luistert naar een monoloog die soms monotoon wordt. Ik zoek vooral naar specifieke onderwerpen om specifieke dingen te leren. Meer informatie over de podcast kun je vinden op https://www.inteltechniques.com.

Tot slot: Hear GDPR

Wil je de hele GDPR horen? Dat kan met deze 'podcast'. Iedere aflevering is één artikel, letterlijk voorgelezen. Misschien voor de echte liefhebbers onder ons.

Wellicht heb ik jou ook enthousiast gemaakt voor podcasts en weet je nu waar te beginnen. Maak vooral je eigen lijst! Disclaimer: ik heb van de bovenstaande shows overigens niet alle online staande afleveringen beluisterd, wel van elke show minstens twee. In een volgende editie van iB-Magazine zal ik tips over security podcasts, en security & privacy podcasts delen. Tenslotte nog een mooi voordeel: je kunt een beluisterde podcast ook gebruiken voor je CPE-punten.

Auteurs: Peter van Schelven is jurist en arbiter bij BIJ PETER - Wet & Recht en bereikbaar via linkedin.com/in/petervanschelven, Dré Lameir is CISO en CTO bij Enovation Group en is bereikbaar via linkedin.com/in/lameir. Bianca Brooijmans is FG bij Enovation Group en zelfstandige. Bianca is bereikbaar via linkedin.com/in/biancabrooijmans.

Adequate gegevensbescherming werkt alleen als informatiebeveiliging op orde is

Lunch op een willekeurige werkdag, Peter (van Schelven, jurist), Dré (Lameir, CISO) en ikzelf (Bianca Brooijmans, FG). Vlak voor de jaarlijkse audit kijken we terug op het afgelopen jaar, de ontwikkelingen en voorbereidingen. We zitten al jaren in het vak en hebben meebewogen met de ontwikkelingen in de markt.

We werken nauw samen en we zijn er van overtuigd dat we compliance niet voor elkaar krijgen zonder elkaars expertise en zonder het besef van urgentie bij de directie, maar dat is zeker niet zo in iedere organisatie. Peter merkt hierover op: "In de diverse opleidingen die ik als IT-rechtelijk georiënteerde docent verzorg, merk ik vaak dat deelnemers soms tamelijk verkokerd in hun werk zitten. Zo nemen veel privacy-juristen primair de wettelijke regels als vertrekpunt, ze hebben daarbij aanzienlijk minder oog voor bijvoorbeeld de almaar toenemende complexiteit van informatietechnologie en de constante wapenwedloop tussen IT-systemen en de maatregelen om beveiliging daarvan te realiseren. Ik ontken uiteraard het belang van de juridische component niet, maar met een overdreven geloof in regels, baselines, contracten en andere lappen tekst wordt de wereld op zich niet veel mooier en veiliger: papier is geduldig!"

Uitwassen

"Sterker nog, kijk je naar de praktijk van verwerkerscontracten, dan zie je dat er vaak driftig wordt onderhandeld over het afwentelen van financiële risico's van de ene op de andere contractpartij. Het gaat dan helemaal niet meer over de daadwerkelijke bescherming van de persoonsgegevens van de betrokken burgers. Dergelijke uitwassen in de juridische praktijk, mede mogelijk gemaakt door naïeve privacywetgeving en relatieve machtsposities van contractspartijen, zijn 'a part of the problem'. De jurist die wel in het hart van onze digitale samenleving wenst te opereren, zal zich welbewust en in volle kwetsbaarheid moeten bewegen op het raakvlak van vele terreinen, zoals de informatietechnologie, de security-praktijk, data-ethiek, verandermanagement, stakeholdermanagement, maatschappelijke weerbaarheid en het creëren van draagvlak – zowel aan de top als op de werkvloer van organisaties. Dus: géén 'law in the books', maar 'law in action'.

Ja, ook ik herken wat Peter zegt. Ik heb veel contact met collega FG's en we bespreken vaak de 'papieren' kant van het verhaal – de verwerkersovereenkomst, de aansprakelijkheid, maar het gaat (gek genoeg?) bijna nooit over hoe we echt invulling geven aan de verwerkingen waar het over gaat. Een FG dicht bij de organisatie in een gelukkig huwelijk met de CISO zie ik randvoorwaardelijk voor het laten slagen van informatiebeveiliging. Immers het borgen van goede en veilige verwerking van (persoons)gegevens valt of staat met adequate technische maatregelen. We schakelen veel en inhoudelijk met de jurist. Het is immers geen checklist maar
zorgen dat wat je doet past bij de organisatie, de diensten en binnen de kaders van de wettelijke verplichtingen. De AVG (met name) is geen one size fits all.

Dré valt bij: "Het is ook onderdeel van het volwassen worden van een afdeling in de organisatie. Veel organisaties beginnen met inrichten voor de bühne. Het hebben van een FG en/of CISO krijgt vaak het karakter van een extra rol/functie ernaast of als dienstverlening in te huren 'as a service'. Daarbij wordt vergeten om meteen de vertaalslag te maken naar de eigen organisatie. Een template of checklist is goed, maar zorg wel dat het mapt op de eigen organisatie. Vaak is de start een gedownloade set templates en een Excel sheet met standaard risico's. Die sheet gaat dan jaar na jaar mee. Maar kijk nu eens welke risico's je echt loopt in je organisatie op het gebied van privacy en security. Security by design en privacy by default is ook zo'n gebied waar wetgeving soms haaks staat op de praktijk. Het kost energie om daarin stappen te zetten, preventief, want de energie die nodig is om fouten te herstellen is vaak vele malen meer. Welke gegevens heb je echt niet nodig? Wat juist wel maar moet je beter beschermen? Hoe zit het contractueel? Wettelijk? Bewustwording op dit vlak is zeker iets wat Legal, Compliance en DevSecOps samen moeten helpen vergroten."

Eilandjes

Alle drie werken we bijna dagelijks samen aan vraagstukken die bij één van ons binnenkomen. We geloven erin dat adequate gegevensbescherming alleen werkt als informatiebeveiliging op orde is. Wat velen vergeten is dat passende informatiebeveiliging óók betekent dat de juridische zaken op orde zijn; is de verzekering passend, hebben we de klant op de juiste wijze verteld wat we doen en waar ze op mogen vertrouwen? Uiteindelijk dien je hetzelfde belang – zorgen dat de privacy van betrokkenen niet geschonden wordt! Maar met drie jaar AVG op tafel, horen we nog te vaak dat met name op het gebied van informatiebeveiliging en privacy het echt wel eilandjes zijn.

Auteur: Robert Metsemakers schrijft op persoonlijke titel en is als ervaren IT-auditor en informatiebeveiligings-expert beschikbaar voor security-advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.

alleen samen krijgen we corona onder controle

BLOG

Overtuigingskracht voor security officers

Het demissionaire kabinet gebruikt bij de aanpak van corona de zes pijlers van Robert Cialdini's overtuigingstheorie. Die pijlers zijn ook bruikbaar voor security officers die het doen en laten van medewerkers in hun organisaties willen beïnvloeden.

1. **Benadruk uw deskundigheid**
2. **Wees sympathiek**
3. **Laat iemand A zeggen, dan volgt B vanzelf**
4. **Doe concessies**
5. **Maak gebruik van kuddegedrag**
6. **Benadruk wat uniek is**

Volgens Cialdini is overtuigen geen kunst, maar een wetenschap, die iedereen kan leren.

Ad 1. Autoriteit

We zijn sneller geneigd experts te geloven dan leken. Een witte jas voor een acteur in een reclame voor geneesmiddelen heeft een aantoonbaar positief effect. Bij al je besluiten en maatregelen melden dat je ze baseert op adviezen van een (outbreak management) team van experts is ook zoiets. Onderteken daarom je adviezen als security officer met daarbij al je certificaten: de gebieden waarop je werkelijk deskundig bent. En laat je voor een presentatie introduceren als expert door liefst je manager of personal assistent als je zelf 'te bescheiden' bent.

Cialdini schreef zijn eerste boek (1) om het publiek te wapenen tegen misbruik via deze sales- en marketingtrucs. Ook social engineers kunnen deze pijlers toepassen. Het is niet onverstandig te luisteren naar autoriteiten en deskundigen, want meestal hebben ze wel gelijk. Maar Cialdini waarschuwt dat je jezelf steeds moet afvragen of iemand werkelijk deskundig is of slechts doet alsof.

> Gebruik deze technieken alleen om werkelijk bestaande sterke kanten van je boodschap te benadrukken. Doe je dat niet, dan behaal je op korte termijn winst, maar lijd je op lange termijn vrijwel altijd verlies.

Ad 2. Sympathie

Je neemt sneller iets aan van iemand die je aardig vindt en vaak is dat iemand die op je lijkt. De autodealer ziet de golftas in je inruilauto en hoopt daarna hardop dat hij kan golfen dat weekend. Waarop jij de gelijkenis ziet enzovoort. Lachen tijdens presentaties over serieuze, moeilijke problemen. Steeds benadrukken dat we alleen samen een of ander probleem kunnen pareren, dat we van elkaar afhankelijk zijn, cartoons op security awareness posters. Voornamen gebruiken en niet 'afdeling Security' zeggen maar 'Kees en zijn mensen'.

Overeenkomstige normen en waarden doen het qua sympathie goed, dus op de poster staat: 'security is geen afdeling, maar een houding' (= van ons allemaal).

Iemand die na tien minuten gezamenlijk roken op de rookplek bij het naar binnengaan 'weer' haar toegangspas is vergeten, is wel sympathiek. Maar mogelijk geen echte collega en waarschijnlijk bezig met een fysieke penetratietest.

Als je als security officer ervoor zorgt dat je de mensen die jij wilt beïnvloeden aardig vindt, is je invloed veel meer blijvend. Zeker wanneer je complimenten geven en ronduit slijmen als wapens inzet.

Ad 3. Commitment en consistentie

Mensen handelen het liefst in overeenstemming met wat ze eerder hebben gezegd of gedaan. Inconsistentie is een onwenselijke eigenschap, men ziet je snel als een draaikont of warhoofd. Consistentie is een uitstekend beïnvloedingswapen als je kleine stapjes neemt. Als iemand ingaat op een klein verzoek, is hij/zij daarna eerder geneigd 'ja' te zeggen tegen een groter soortgelijk verzoek. Van afstand houden, andere mensen niet in hun gezicht hoesten of niesen, via geen handen geven naar in winkels een mondmasker dragen. Later een mondneusmasker dragen, dan de hele avond en nacht niet meer naar buiten mogen, daarna niet meer naar bepaalde landen mogen. Eerst testen met een stokje, dan inenten met een naald, dan twee keer inenten en vervolgens 'vrijwillig' een halfjaarlijks boosterabonnement nemen. Na drie gratis vaccins, voortaan telkens zelf betalen.

Het consistentieprincipe werkt het sterkst als je mensen hun plannen laat opschrijven en die aan anderen laat lezen. Staat een voornemen eenmaal zwart op wit - of zelfs in kleur in een meerjarige security roadmap met uitklapposter - en weten andere mensen ervan af, dan is het erg lastig om erop terug te komen.

Securitytargets kun je ook voor alle medewerkers in je organisatie heel effectief opnemen in de nieuwe resultaatafspraken in het jaarlijkse beoordelingsgesprek. Te beginnen met één afspraak natuurlijk, zoals: 'security-incidenten die ik zie, zal ik melden bij de Servicedesk'.

Ad 4. Wederkerigheid

Als je bij iemand thuis gaat eten, breng je dan een fles wijn, een 'krabi' (2) of chocolade mee voor de gastheer? Dan ben je gevoelig voor het principe van wederkerigheid. Alles is een kwestie van 'give and take' en je realiseert je dat 'there is no such thing as a free lunch'. Zelfs als je iets krijgt waar je eigenlijk niet op zit te wachten (zoals een van de

Als iemand een concessie doet, is de ander geneigd óók een concessie te doen.

vele experimentele vaccins), voel jij je toch verplicht om de schenker iets terug te geven. Zo blijft je 'relationele bankrekening' in balans. Je vrienden, buren, partner, kinderen en collega's zullen meer openstaan voor je verzoeken als je eerst iets hebt gedaan voor hen. Geschenken en gunsten maken de meeste impact als ze betekenisvol, onverwacht en persoonlijk zijn.

Cialdini noemt een sociaal experiment. Een pepermuntje van de ober bij de rekening levert 3% meer fooi. Twee pepermuntjes van de ober, 14% meer fooi. Eerst één pepermuntje en daarna nog een tweede 'omdat jullie zo'n sympathiek gezelschap zijn': 23% meer fooi.
Wederkerigheid werkt ook met concessies. Als iemand een concessie doet, is de ander geneigd óók een concessie te doen. Willen jullie een totale lockdown? Neen? OK, dan doen we alleen een avondklok. Verbeter de spamfilters om meer goodwill voor security te krijgen.

Een directie wil alle in potentie gevaarlijke websites blokkeren vanwege de risico's van malware besmettingen naar binnen en dataleakage naar buiten. Individuele medewerkers en de ondernemingsraad protesteren. Vervolgens worden alleen de sites met kinderporno en terrorisme en tegelijk alle filesharers (Wetransfer enzovoort) geblokkeerd.
Als security officer iets meer vragen dan wat je eigenlijk nodig hebt, werkt ook met budgetaanvragen bij die directie. Bijvoorbeeld: iedere medewerker moet volgend jaar vijftien security e-learnings doen. Oh, is dat teveel? Dan alleen deze vier cursussen (met een afsluitend examen).

Ad 5. Sociale bewijskracht

Als kuddedieren kijken mensen, vooral in situaties waarin we niet precies weten wat we moeten doen (zoals een wereldwijde pandemie), hoe anderen handelen. Als je iemand wilt overtuigen, werkt het daarom goed te wijzen op anderen die dezelfde keuze maken. Hoeveel personen hebben al een inenting gehad? Als je wilt, mag je de tweede prik al een week éérder halen (= concessie + wederkerigheid), mits je via internet eerst een afspraak maakt (commitment).
Een security-voorbeeld is presenteren dat 90% van de medewerkers na hun zomervakantie hun wachtwoord niet is vergeten en dus de Servicedesk niet hoeft te 'overbelasten' met hun reset-verzoeken. Ook kun je bij een van die verplichte securitycursussen (zie 4) vermelden: 'deze is het populairst'.

Ad 6. Schaarste

'De laatste week', 'op is op', 'maximaal drie per klant', kent u uit de buurtsuper. 'Er zijn te weinig vaccins', van de Jonge. We vinden schaarse zaken waardevoller dan dingen die gemakkelijk verkrijgbaar zijn. Lever nieuwe 'single sign on USB-tokens' dus in batches uit en benadruk dat veel collega's teleurgesteld raakten, omdat ze te laat waren voor de eerste batch.

Verlies is de ultieme vorm van schaarste. Zonder spuit mag je niet meer op vakantie, niet meer uitgaan, niet meer buiten. Dat motiveert enorm.

Referenties

(1) https://nl.wikipedia.org/wiki/Robert_Cialdini

(2) Krabi = krat bier in Arnhemse studentenkringen.

Auteur: Dré Lameir is CISO en CTO bij Enovation Group en is bereikbaar via linkedin.com/in/lameir.

Lekker foppen

Zondagochtend, vroeger wakker geworden dan normaal maar hé... life's good. Want ik ben wakker gemaakt met kussen, knuffels en cadeautjes. Ik ben jarig! Tekening, een nieuwe baseball cap, paar flessen drank (ze kennen me). Ik krijg ook koffie op bed en ondertussen hoor ik de jongste rommelen met papier en plakband.

Tadaaa... nog een cadeau pap! Dit cadeau heeft verdacht genoeg dezelfde afmetingen als het vorige, weegt nu ineens niks en is heel slordig ingepakt. Met veel bombarie maak ik het open... erin zit een klein handgeschreven briefje met de tekst: 'FOPKADO!'.

Als kind vond ik het ook geweldig om tijdens het ontbijt mijn vader te plagen met een leeg omgedraaid eierdopje. Die sloeg dan in een groots gebaar het kapje eraf met zijn mes en reageerde dan altijd even verontwaardigd... held.

Vroeger, toen lekker foppen nog leuk was. Nu is het big business, het begon als slecht ingepakte, te lichte cadeaus maar nu zijn het heel geraffineerde mailtjes, whatsappjes of sms'jes. En ze lijken zoveel van je te weten.

'Ik kreeg een sms'je van de douane, ik verwachtte ook een pakketje van ALI Express, dus…'

of

'Mijn zoons telefoon was ook kapot, ik dacht echt dat hij om wat geld vroeg via de app, dus...'

Maar dit is de wet van de grote getallen. We bestellen massaal online en ja, onze kinderen laten smartphones van een kleine duizend euro op de grond vallen. Er is altijd wel iemand die denkt, dit klopt, dit gaat over mij. Het zit in ons oerinstinct om overal gezichten te herkennen of patronen te zien in vage waarnemingen. Dat heet pareidolia of apofenie, kunnen we niks aan doen. Beter tien keer te vaak weggerend voor een leeuw, dan één keer te weinig.

...eigenlijk zijn we als kind al gewaarschuwd.

Pareidolie of pareidolia is een psychisch verschijnsel, een vorm van illusie waarbij iemand een zodanige interpretatie van onduidelijke of willekeurige waarnemingen heeft, dat hij hierin herkenbare dingen meent waar te nemen.
bron:
https://nl.wikipedia.org/wiki/Pareidolie

Ons vermogen om in phishing te trappen is, denk ik, direct gelinkt aan deze oervaardigheid. Toen hielp het ons te overleven, nu lijkt het onze digitale ondergang te worden. En helemaal een ramp wordt het als de slechteriken gaan spear phishen of whalen. Gerichte aanvallen, waar echt handwerk in is gaan zitten.

Een collega kreeg recent een verzoek tot betaling. Bijgevoegd een certificaat van een notaris uit Zuid-Amerika en een pdf met daarin een gescand inschrijfformulier van een event. Het formulier was echt, vermoedelijk buitgemaakt in een hack bij een ander bedrijf. Daarna was het voorzien van een vervalst voor- en achterblad, de footer was aangepast, er was een ordernummer verzonnen en dit was weer verwerkt in de mail waarin betaling verzocht werd. Die mail was ook nog gericht aan een van onze directeuren. Zijn naam stond niet op het originele formulier.

Ik verbaas me niet over de poging, ik verbaas me over het handwerk. Onderzoek doen, fotoshoppen, bestanden aankopen, fake URL's en maildomeinen opzetten, fake websites, verhaal bedenken. Kijk, 100.000 keer mailen als een Afrikaanse prins of 50.000 keer sms'en als de douane, is schieten met hagel maar weinig arbeidsintensief. Spearphishing of whaling is echt werk. Hoe meer je oefent, hoe beter je wordt. Dat moet dan wel wat opleveren lijkt me.

De lijst met dit soort methodes wordt steeds langer en geraffineerder, vishing (middels voice), clone-phishing, CEO-fraude en uiteindelijk deep fakes. Hier is op termijn niet meer tegenaan te trainen. We zullen als mens nieuwe vaardigheden moeten ontwikkelen. Een soort digitale pareidolia zodat we onechte zaken herkennen. Beter tien keer weggemikt dan een keer echt geklikt.

Misschien komt de tijd dan terug waarin alles nog lekker onschuldig was. Gewoon weer lekker foppen voor de lol. Alhoewel, toen hing er in ons lokale zwembad ook al bovenstaande poster.

Authors: Andres Maurer and Robert Metsemakers have extensive security experience in respectively Swiss and Dutch financial services. They wrote this article together in a personal capacity. They can be reached on andres-maurer@hotmail.com and robert.metsemakers@gmail.com.

Best practices in access management (part 2 of 2)

The first part was published in iB4 and contained best practices for steps 1 to 7 in a generic access management process landscape (see figure 1). This second part describes steps 8 to 13. All steps are based on 'lessons learned' and experience gained by the authors in various implementation projects for access management and through regular line activities.

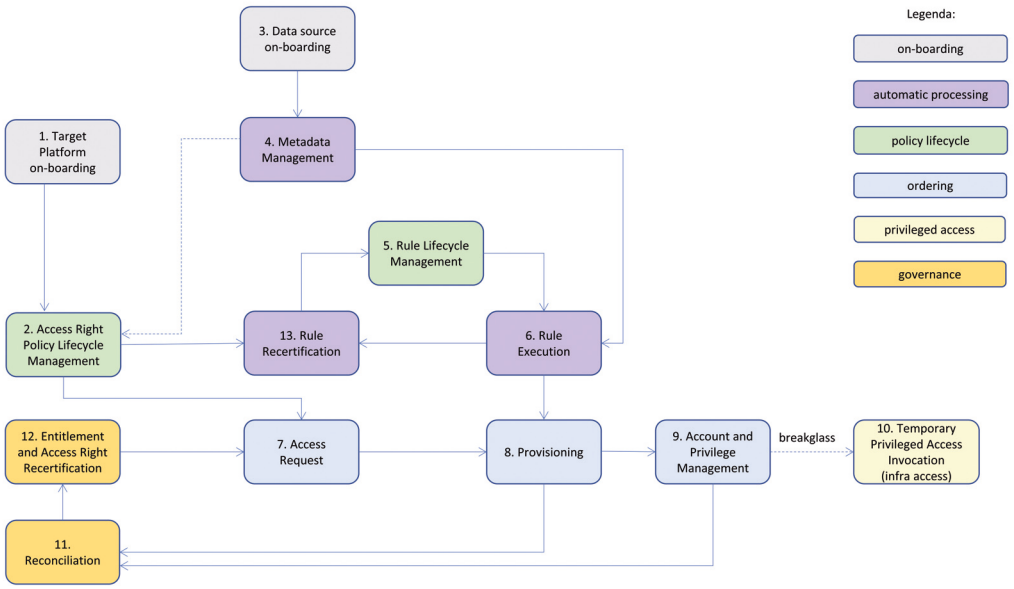


Figure 1 -Steps in Access Management.

8. Provisioning

Description

Once an approved 'access request' (see step 7) will be transferred from the IAM-system to the target system, the entitlement is resolved into provisioning items, i.e. accounts, privileges, profiles, etc. Provisioning can either be automatic or manual because some systems, applications or platforms do not allow automatic creation of accounts.

Best Practices

- Provide a high-level of automation in provisioning and de-provisioning to keep overhead low, minimize errors and speed up the process.
- Error handling in case of failures or conflict should be clear and 'before the fact'.
- You need an ability to handle sequencing of multiple provisioning runs in batch mode, because for instance 'remove

all, add 1, add 2' will have another result than 'add 1, remove all, add 2'.
- Have an SLA (Service Level Agreement) in place that handles speed, time window, quality, time to fix mistakes and reporting for manual provisioning: especially with externally hosted applications.
- Have an ability to temporarily switch off automatic provisioning in case of emergency.
- Have the ability to roll back to a previous (total) snapshot of all access rights - this will be faster than to roll back 'all' access requests from yesterday.
- You need traceability from provisioning items all the way back to the original access request (and name of requestor and a date/time stamp).
- You can use Delta provisioning (= only changes to access are provisioned) or Full Forward provisioning (= when the whole entitlement repository is resolved and provisioned).

9. Account and Privilege Management

Description

The Access Management System must be able to manage the provisioning items efficiently and transparently (add, update, delete) based on the provisioning results. This process ensures that any access management artefacts on the target system can be mapped backed to an entitlement, which can then be mapped back to a request or automated rule.

Best Practices

- You need clear traceability between account name and the owner of the account if SSO (Single Sign On) is not used.
- Maintain single point of entry to manage the entitlement store/database and allow no (or only minimal) manual intervention.
- Bookkeeping of all the entitlement changes (historic ledger) and also the link between the entitlement and the original access request is necessary.
- Provide a clear strategy for handling removal if the provisioning item can be triggered by different access rights/roles. This is about resolving relationships. For instance, if a user has two access rights that are based on one account, then removing one access right should remove only the associated privilege bit, not the account.

10. Temporary Privileged Access Invocation

Description

As only a limited number of users should have access to Production Systems, there has to be an efficient process to grant highly privileged access (like system administrator rights) for only a limited time to Developers or Level 3 supporters to fix incidents. The temporary privileged access should, as the name implies, be automatically revoked after a preset period or sooner when the access is no longer needed.

Best Practices

- Break-glass activation must be provisioned in a very short period. Normally this is done automatically, as in break-glass mode, there is no time to get management approval. So the entitlement should be pre-approved for specific users/roles and can then be activated quickly when needed.
- There has to be traceability between date/time of the break-glass event and of the original initiating incident.
- There has to be a limited ability to prolong the rights in case of emergency (for instance, extend it for 24 hours) and also a limit on the maximum number of extensions to prevent misuse.
- Perform strict JML (joiners, movers, leavers) processing on this selected group of high privileged users (usually system administrators), with timely removal of no longer needed privileged access.
- There must be pre-defined deputies or access groups for allowing these sensitive, high privileged access rights.

11. Reconciliation

Description

This process of comparing the master entitlement repository and the provisioned items on all target systems ensures that there is consistency between the repository and all systems. Changes that are made directly to the target system and hence bypassing the access management process will be detected.

Best Practices

- For a manual reconciliation, it is recommended to have a tool that can show the resolved access rights against the provisioned artefacts from the target system. This will facilitate the operator in doing the comparison faster.
- Define a strategy on how to remediate conflicts that are found during reconciliation.
- The performance of the reconciliation process should not be impacted by the provisioning process, even if they are running in parallel on the same live/production system.
- Reconciliation is done at regular intervals, at a minimum before each entitlement recertification.
- Automatic remediation after reconciliation should not be misused as a workaround for wrongly defined rights or roles.

12. Entitlement and Access Right Recertification

Description

There should be a process in place to ensure that entitlement and access rights/roles are reviewed at regular intervals.

As applications change over time, the access rights and access roles need to be reviewed regularly to ensure that they are still accurate and fit-for-purpose.

To ensure compliance to diverse regulations like Need-to-Know, SOX and so on, a review of user entitlements is required at regular intervals. Normally, only the critical entitlements need to be reviewed.

Entitlement recertification also needs to be an integral part of JML (joiners, movers, leavers).

Best Practices

- Appoint the right person (for instance: department/mandate, knowledge and expertise, personal qualities like precise, inquisitive and attention to detail) to execute the review/recertification.
- Proper context information (like the reason for and criticality of 'temporary' exceptions from the rules that are allowed by management) needs to be presented to the reviewer to allow him/her to do the job well.
- Provide a clear recertification strategy to optimize the scope and the required effort. For instance, recertify only critical access.
- Tools used for the review and recertification need to provide an adequate audit trail that provides enough detail but is also not 'too much information' to store for the required period.
- If an entitlement is judged to no longer be needed, the reason must be given and the affected user must be informed as this judgement may not be correct.
- Reviewer could delegate the task of reviewing, for instance in the holiday season.

13. Rule Recertification

Description

As the rulesets also create entitlements, they also need to be reviewed as well at regular intervals to affirm that the rules are still correct, complete and relevant.

Best Practices

- Metrics and logs of (automatic) rule execution must be available for the reviewer.
- Simulation (testing) environment of the automatic rules is available for the reviewer.
- Changes to external regulations and internal policies with consequences for user rights and entitlements are communicated timely to the rule owners.
- Rule owners needs to be able to simulate the rules to validate the rule behavior.
- Changes in the business process that result in new, extra or superfluous access rights and privileges need to be factored in. The reviewer is usually the rule owner. This provides the opportunity to the owner to review whether the rule is up to date.

Section 2 – Management aspects

Managing Joiners, Movers, Leavers - triggers for the lifecycle of entitlements

A critical factor in ensuring that a corporation's access management is up to date, is to properly manage the Joiners, Movers, Leavers – also known as JML.

There is often the misconception that JML is a process because, from the outside, there are access management activities during a JML event. However, JML only acts as the trigger for such activities.

Joiner (new to organization)

- Manually ordered rights or automatically assigned rights.
- Quick processing time of access requests to reduce unproductive time of users.
- 'Replicate' access rights of the buddy (but keep the buddies clean from 'temporary exceptions' from previous jobs on other departments).
- Roles help reduce the number of items to order, because a new user only has to order for instance a 'banker-set', 'investment broker-set', 'HR-department-set' or 'internal-auditor-set' of access rights.

Mover (changing in organization, department or function)

- Manually ordered rights or automatically assigned rights.
- Manually removed rights (Entitlement recertification) or automatically removed rights.
- Movers seldom move on an absolute date, and usually get questions about their previous work activities, so a 'grace period' for entitlements will help the transition.

- Update Master data repository in the IAM-system. The mover may be an approver or owner of an artefact in the old organization, so a replacement must be defined.

Leaver (leaving organization)

- Remove entitlements automatically (to avoid mistakes, do not leave it to manual process), for instance based on the Human Resources salary administration.
- Deactivating of the registered access rights may be required before actual deletion. For instance, when you need forensics in case of dismissal because of theft or fraud. There can also be approvals etc. in the workflow/pipeline of the leaver that only can be deleted after they have been granted.
- Update the Master data repository (see above).

Section 3 – Architecture

Description

In a large organization, multiple protocols and platforms can (or will) be used, leading to high maintenance overhead. To mitigate this, IAM should be defined on a strategic level that is valid for the whole organization. If the organization is large and extended to different countries, IAM should fulfill all regulatory and compliance requirements for all impacted regions.

Best Practices

- Develop a Master plan for firm-wide Identity and Access Management.
- Publish information on what is supported as well as how to integrate.
- Build/procure based on the supported IAM architecture patterns.
- Select a framework, stick to it and use it consistently, but know when to deviate from it.
- Always do a proper (and holistic!) analysis of new technology and integrate into the master plan.
- Build on standards like OASIS (1) XACML (2) and Zero Trust (3) Framework (4).

OASIS XACML

- XACML is primarily an attribute-based access control system (ABAC). Access is granted on the fly based on attributes matching. For instance, if user is in city "A" and has job function "B", grant write access to Application "C".
- Model that provides common terminology and interoperability between access control implementations.
- Can be used for role-based access control system (RBAC) as well.

Zero Trust Security Model

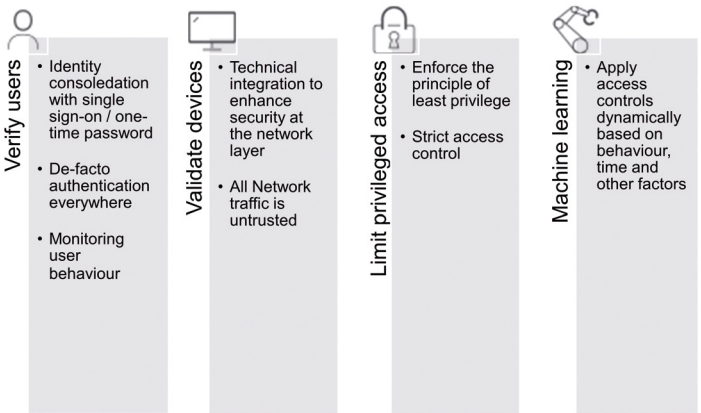


Figure 2 - Zero Trust graphic.

- Change the principle from 'trust, but verify' to 'no trust, always verify'.
- Needs to be implemented holistically but can be implemented in steps.
- Many manufacturers and providers support Zero Trust Security Model.
- Model can also be adopted for Cloud and support micro-segmentation.
- Requires in-depth logging and monitoring.
- Google's implementation (BeyondCorp) is so reliable that VPN is no longer needed for BYOD.

Attackers often try, using the standard command set, to gain administrator privileges to perform highly privileged tasks.

Section 4 – Access management and security monitoring

Description

Attackers often try, using the standard command set, to gain administrator privileges to perform highly privileged tasks. Accounts or permissions that do not match the master repository may indicate malicious activities. So all actual accounts and permissions have to be reconciled with the master repository frequently to allow corrective actions.

An example of such techniques from the MITRE ATT&CK framework (5) are 'Create account', 'Account manipulation' and 'Valid accounts'. Look for more information, for instance on TTP used by (Advanced Persistent Threat groups) APT3 and APT29 (6), on the MITRE website (7).

Misuse of rights or unusual access is often a good indicator of malicious activities and needs to be monitored. For example, look for unusual amounts and quantities, usage time (outside of office hours), place ('work from home' as it was called, pre-Covid), date (during holiday/vacation), frequency of use or speed of input.

- Discrepancies detected during reconciliation, especially superfluous accounts and permissions, are highly suspicious and require further investigation.
- Unusual account activities need to be investigated (e.g. Admin login at Midnight, or during her pregnancy leave).

Best Practices – Preventive control

- Use only one master entitlement repository and a high degree of provisioning automation.
- Do all provisioning automatically from the IAM-system and avoid adding accounts or change permissions manually directly on the target system.
- Deactivate the default admin accounts.
- Do not use non-personal or shared accounts.
- Be aware what groups and permissions are highly privileged and monitor them closely.
- Keep an immutable log of privileged user actions.
- Reconciliation must be in place and executed regularly.
- Have a predefined process in place to deal with reconciliation differences that will appear in the future.

Best Practices – Detective control

- Ensure that necessary logs and information are sent timely to the SIEM (Security Information & Events Monitoring) system in a way that allows no manipulation/changing (both in storage and in transit).
- Define the context of the logs for each detection case.
- To avoid false positives, define proper threshold (the number of security events before an alert is triggered) and use multiple indicators of compromise where possible.
- Also, correlate against the planned maintenance time windows and issued Incident tickets.
- Know the normal usage pattern on the different systems.

References

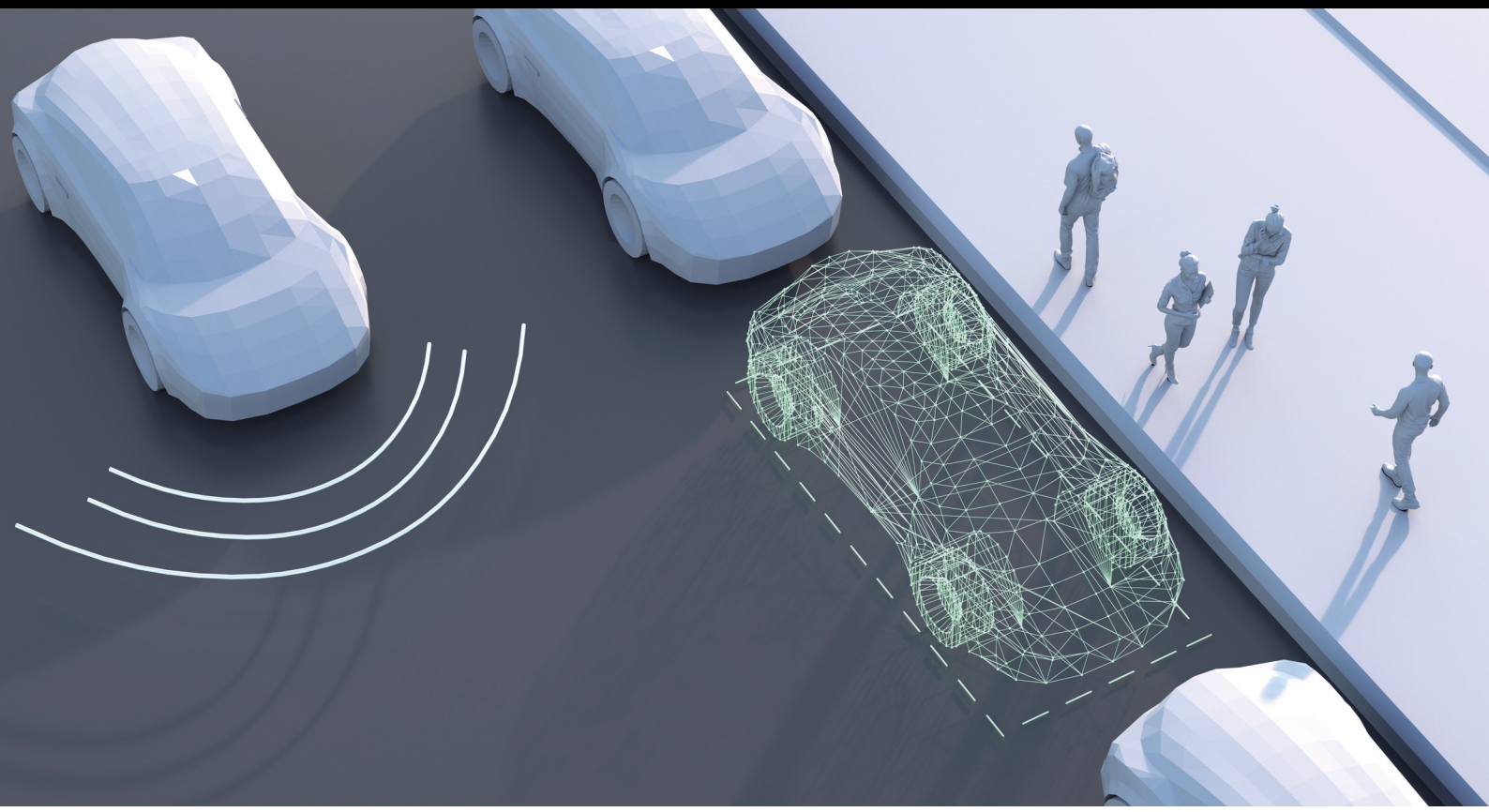
(1) https://www.oasis-open.org/committees/xacml/
(2) https://en.wikipedia.org/wiki/XACML
(3) https://ldapwiki.com/wiki/Zero%20Trust
(4) https://go.forrester.com/blogs/next-generation-access-and-zero-trust/
(5) https://mitre-attack.github.io/attack-navigator/enterprise/
(6) https://www.mitre.org/sites/default/files/pdf/APT3-APT29-software.pdf
(7) https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/attck-101

Auteur: Ir.drs J. van der Vlugt CISA CRISC. Jurgen is zelfstandig professional voor Information governance- en risk management advisering en audit. Jurgen is te bereiken via jvdvlugt@xs4all.nl

Aangestuurd autorijden

In deel 1 van dit drieluik zagen we dat een auto, een zelf automatisch rijdend vervoermiddel, ons op een afgelegen parkeerplaats nog wel van A naar B kan brengen, maar een kwetsbaar (lees: gemakkelijk verstoorbaar) systeem is, in tegenstelling tot de mens als denkende deelnemer in het hedendaags verkeer.
In dit artikel wordt gesproken over de auto als autonoom-rijdend personenvoertuig dat misschien (ooit) beter kan rijden, beter kan omgaan met meer complexiteit dan de mens; maar als de auto faalt dan is het gelijk einde oefening. De vraag die hier wordt gesteld: 'Kan er niet 'iets' centraal aangestuurd worden, vanuit een groot regelsysteem dus?'

Deel 2 van 3: Auto's, besturing en reflexen



In deel 1 kwam het al voorbij: de Central Scrutinizer. Want als dat niet de bestuurder is, kan het dan aan het andere eind van het spectrum worden gevonden, in de vorm van een verkeerscentrale die alle wegverkeer bewaakt en bestuurt? Te denken is aan de Verkeerscentrale Nederland – die al bestaat. Het VCNL is gevestigd in Utrecht Papendorp en bewaakt het verkeer in ons land. Nou ja, de A- en een deel van de N-wegen (1) met daarnaast alleen de bewaking en centrale regie-voering over enkele decentrale centrales rond de grote steden. Wie verzamelt de file-informatie, adviseert alternatieve routes, regelt het stratificeren en vertragen van de gemiddelde snelheid met matrixborden (en het afkruisen van rijstroken)? Juist (2).

> Centralisatie uiteraard in architectuur, niet noodzakelijkerwijs in geografie. Lekker load balancen over een netwerk van systemen van de Nederlandse gemeenten levert best wel wat failover mogelijkheden op tegen pech (4).

Hoe eenvoudig zou het dan zijn om – bijvoorbeeld per stad, als enigszins behapbare eenheid en invulling van een deel van het Smart City-concept (3) –, alle verkeer op camera te vatten en te reguleren? Zeker auto's kunnen hun bestemming wel al rijdende doorgeven, zodat de centrale botsingen kan voorkomen met niet-aanstuurbare verkeersdeelnemers. Zoals die ongure elementen als fietsers en voetgangers met hun zo afwezige stuursoftware in de bovenpan. Ga maar eens in Amsterdam kijken hoeveel fietsers zich aan de regels houden en verbaas u dat de meter door de nul schiet. Een prima idee om auto's dan centraal aan te sturen, zodat individuele bestuurders niet uit nijd fietsers gaan snijden. Met als additioneel voordeel een situational awareness die de routes van auto's kan aanpassen als het ergens te druk dreigt te worden. Daarnaast als grootste voordeel dat economies of scale te bereiken zijn met betrekking tot de benodigde rekencapaciteit.

Nadelen van een verkeerscentrale

Enkele nadelen zijn er ook. Zo zal het lastig zijn om over gemeentegrenzen heen te coördineren. Wellicht bieden Veiligheidsregiokoepels uitkomst. Lastiger wordt het om binnen

gemeenten de juiste expertise te verzamelen. Er nog van afgezien dat ervaringen met decentralisatie – denk aan bijvoorbeeld de jeugdzorg – niet zo hoopgevend zijn. Nu is er hoogstens wat manual verkeersregeling bij lokale evenementen en ligt het verder bij het VCNL.
Maar als we 'dwingend' willen gaan sturen, hoe regelen we dan de mandaten? Wie denkt dat 'de overheid' het wel voor elkaar zal (zou kunnen) krijgen, vergeet dat ons politiek bestel niet geschikt is voor de toekomst (5).

Inbreuk op de AVG

Waarmee we een gevoelig punt raken, want centrale aansturing en identificatie van auto's en hun beoogde route; dat is toch wel een inbreuk op de AVG. Natuurlijk zijn de auto (die zich moet 'identificeren' bij route-doorgave) en de bestuurder niet een en dezelfde, maar de pseudonimisering is in dit geval eenvoudig. En overal camera's, op elke blinde vlek in de openbare ruimte; big brother lijkt overal aanwezig. Vergeet niet dat ook voetgangers en fietsers makkelijk te deanonimiseren zijn.
Er hangen al te veel camera's in gemeenten waarvan de rechtvaardiging twijfelachtig is of door de Autoriteit Persoonsgegevens is afgekeurd. We staan minder ver van repressieve regimes dan we denken, waardoor de druk naar maximale bewegingsvrijheid in de – niet voor niets – openbare ruimte, zal toenemen. Systemen zouden daartoe absoluut en bewijsbaar onmogelijk te deanonimiseren moeten zijn. Als dat theoretisch niet lukt, dan maar gewoon helemaal niet?
De Gemeentelijke Verkeerscentrale is natuurlijk een onoverzichtelijk architectuurcomplex – voor zover 'complex' en 'niet-triviale architectuur' niet al synoniem zijn. Wie beweert dat de beveiliging ervan goed geregeld is, heeft de nodige mislukkingen gedurende de afgelopen vijftig jaar van overheidsautomatisering gemist. Wat continue beschikbaarheid betreft: door ransomware of systeem falen ontstaan simpel problemen door de vele externe connecties. Auto's die dus moeten kunnen vertrouwen op centrale, veilige aansturing of coördinatie zullen dan al snel de weg kwijt zijn. Op dit punt – en de daaronder te rekenen integriteit van uitkomsten – valt ook het nodige toe te voegen met betrekking tot de bepaling hoe en hoeveel 'human in the loop' nodig is (bovenop de Europese minimumvereisten en aan uitlegbaarheid en andere privacyaspecten).
Qua vertrouwelijkheid zal het ook niet zo top zijn. We hebben het over gevoelige gegevens en grote datasets. De vraag is niet of, maar wanneer. Natuurlijk zal niet direct een premier worden ontvoerd als zijn rijroute uitlekt. Lastiger wordt het, als criminele groepen door route-analyses elkaars opslagruimtes weten te lokaliseren, of bij uitrukkende Hermandad de route inclusief eindbestemming uit het systeem weten te plukken. En denk ook aan de natuurwet van scope creep: als de (route)data er is, zal dat een onweerstaanbare aantrekkingskracht hebben op totalitair-bureaucratische lieden (vroom in voorkomen, moreel verschimmeld) die in welke overheid dan ook, onuitroeibaar blijken.

Integriteit

En de integriteit van de data… dat wordt dynamisch-GIS-werk. Naast het stasis-gericht giswerk dat subalterne, semi-, quasi- en overheidsbestuurders nu al wordt verweten, want dan hebben we behalve een enorme verzameling statische informatie over o.a. wegen, stoepen, losliggende tegels (denk aan plots uitwijkende scootmobielen en slingerende fietsers), ook nog een veel grotere verzameling bewegende datapunten (auto's en eventueel 'bussen'). Wat als er iets misgaat in de communicatie? Ruis en vervuiling zullen al snel onwerkbaar overheersen in de database. Verdraaiing (manipulatie) kan ook bewust gebeuren (zie hieronder). Om over de integriteit (juistheid) van de 'uitkomsten' van het systeem maar te zwijgen; wat betekent 'ik raakte in paniek' van het centrale systeem?
De vraag is of het hiermee ooit goedkomt. En als er door niet-integere data iets fout gaat, of door een lek, gaat de gemeente de materiële én immateriële schade dan betalen, zonder dat de belastingbetaler er dan weer voor opdraait? Wat klungelen met een 'Heads I win, Tails you lose' afschuifmentaliteit wordt in het bedrijfsleven (steeds meer, hoewel nog veel te weinig) bestraft met ontslag, clawbacks en VoG-beroepsontzegging. Grove onachtzaamheid zou ook in publieke omgevingen zo kunnen worden aangepakt. Alleen de juiste (sic) skin in the game (Taleb) helpt tegen verkeerd gerichte incentives en moral hazard, blijkt onwrikbaar keer op keer. Summa summarum: ook hier zijn ervaringen uit het verleden geen hoop voor de toekomst.
Als laatste nog een nadeel: door al die ongeleide projectielen als voetgangers, fietsers, en niet te vergeten de vorige keer al genoemde niet-autonoom rijdende auto's (6), zullen de autonoom rijdende auto's zelfs bij centrale aansturing defensief gaan rijden, aan de achterste mem hangen qua praktische voorrangverlening op andere, niet-autonoom rijdende auto's. Dat zal zeker ook gaan spelen bij treintje-rijdende auto's; die zijn minder flexibel dan enkelvoudige auto's én nemen veel (omgevings)beslisruimte in – en zullen dus nog voorzichtiger gaan optreden tegen al die bedreigende losse, relatief kleine,

Zodat eenieder bijdraagt aan een deel van de omgevingsawareness en van het geheel kan profiteren.

projectielen die in de beslisruimte binnen komen zeilen. Overstekende 'mensen', lastig hoor!
Het voornaamste bezwaar zit 'm natuurlijk in het onderbuikgevoel dat we onze vrijheid niet kwijt willen en zeker niet in een achterhaalde utopie van maakbaarheid van de samenleving willen verzanden. De geschiedenis van de mensheid heeft aangetoond dat we daar niets van hoeven te verwachten. Maar wat als we nou eens zouden overschakelen naar het andere uiterste: een anarcho-syndicalistische commune (7)? Een fijnmazig net van overigens zelfstandige maar onderling samenwerkende auto's dus. Die allerlei informatie over het wegverkeer (van het inherente gevaar van de moderne, laat staan de elektrische, fietser tot en met kleine kinderen en ballen (8) op de weg) niet alleen zelf opdoen, maar ook doorgeven aan andere auto's in de buurt. Zodat eenieder bijdraagt aan een deel van de omgevingsawareness en van het geheel kan profiteren.
Misschien dat een gemeente toch iets kan bijdragen? Wilt u het totale meetlussysteem dat ook fietsers en wandelaars registreert? Ja, want wij willen Netflixen achter het stuur! Geen prettig idee. En de centrale is natuurlijk even betrouwbaar als eerder in dit artikel beschreven – of minder, want het belang van integriteit lijkt lager voor de gemeente! Bovendien, wat kost het onderhoud van zo'n zéér fijnmazig meetlusnet wel niet? Dus dit is toch niet zo'n briljant idee.

Knooploos netwerk

Een mesh (knooploos netwerk) zonder centrale database kan uiteraard ook. Het hoeft niet direct een speculatie-speeltje als een blockchain te zijn. Dat is in de benodigde communicatie en computatie te zwaar voor de individuele betrokken auto's, die toch al moeite hadden met het denkwerk voor zelf rijden. Laten we het simpel houden (maar niet simpeler). Wel zal er flink gecommuniceerd moeten worden tussen auto's. Wat nog wat problemen zal geven, want hoe kunnen we die andere auto's vertrouwen (9)? Volgende keer zal het gaan om adversarial attacks; nu al: als onze auto een gemanipuleerd beeld oppikt en doorgeeft aan een andere auto, zijn we dan medeaansprakelijk voor de gevolgen? Mensen zullen de teruggekeken beelden toch als ongemanipuleerd zien, toch, dat was nou net de 'grap' (quod non)?
Ook andere verstoring van al die communicatie is denkbaar. En wat als er weinig auto's op de weg zijn, maar wel andere weggebruikers? Dan is er weinig Vehicle-to-Vehicle (V2V) te babbelen, maar kan het toch druk zijn. Dan heeft de auto relatief veel zelf te zien en te berekenen, maar net met relatief veel te weinig informatie en zal dus des te langzamer gaan rijden. De default zal immers zijn ingesteld op méér informatievergaring voordat tot een moeilijk besluit wordt overgegaan. Met – meestal onwelvoeglijke – reacties van voorbijflitsende fietsers.

Daarnaast kan ik nog wel wat bedenken: mijn auto geeft data door, die andere auto's collectief aan de kant zet . Want ik wil lekker veel ruimte! Dit werkt zelfs als ik op mijn fiets een transponder zou monteren die een vijftigtonner truck met aanhanger simuleert (10). Of een bus – als we data gaan zenden, staat het stoplicht voor mij altijd op groen. Het is hier Almelo niet (11).

Voor nooddiensten zou dit overigens weleens een aardige winst kunnen opleveren. Mits er niet te veel 'overige' weggebruikers zijn die denken handig gebruik te kunnen maken van de plots geboden ruimte. Lastiger wordt het als allerlei maatschappelijk belangrijke beroepsgroepen ook (enige) voorrang krijgen. Zorgpersoneel, vuilophalers, gemeenteplantsoenendienstmedewerkers etc.; in dat geval komen politici nooit uit de parkeerstand. En zullen dan niet velen out-opt'en met betrekking tot opname in de mesh en weer zelf willen rijden?
Sommigen zouden dan weer willen eisen dat álle fietsers en wandelaars (en de kat van de buren) met een transponder de deur uitgaan. Anders is de 'dekking' te laag. Maar, afgezien van een enkeling die zichzelf al hackend boven de regels weet

te verheffen om geen last te hebben van wetten voor de 'hoi polloi' (de anderen), wie zou de totaal gechipte samenleving willen?

Tussenconclusie:

1. Central(e) control(e) gaat niet lukken;
2. Een mesh van samenwerkende auto's kán, maar
2a. is ook (te) kwetsbaar en
2b. voorziet niet in fietsers, wandelaars, niet-autonoom rijdende auto's, juist waar het om ging qua operationele risico's.

Zo zien we: organisatie van het verkeer volgens Stalin of Bakunin (12), beide zijn niet geheel geschikte modellen voor een artificieel-intellectuele voorhoede van bourgeois-auto's.
Qua grand strategy objective ziet de meshed auto er dus wel goed uit, maar gewone strategie is niet die stip aan de horizon maar juist de weg er naar toe en op dat vlak kunnen we maar moeilijk vooruit (13). Want we zullen hoe dan ook naar één of meer tussenfasen moeten waarin niet iedereen een transponder bij zich draagt. Dieren, kleine kinderen, die moeten dan maar met een chip worden geïmplanteerd? 'Het is voor hun eigen veiligheid!', luidt dan het argument. Bovendien is het aantal auto's – van de huidige generatie – nog uiterst beperkt en zal nog zéér fors moeten groeien om serieus baat te krijgen van eventuele mesh-communicatie.
De overige weggebruikers zullen moeten uitfaseren, dat kost generaties.
Als de maatschappij al die kant op wil. Noch 'het zal wel moeten' noch 'maar dat willen de mensen toch' zijn steekhoudend en beide volstrekt belachelijk, zeker in de tijd. Wat we op middellange termijn kunnen voorzien, is misschien niet eens een verdere auto-mobilisering maar juist een slingerweg van auto's, naar fiets, bus (14), trein en wellicht eerder vliegende auto's (ja, eindelijk!). En, met betrekking tot Smart Cities, was het niet de bedoeling auto's én autonoom rijdende auto's daaruit te weren zodat we de laatste 10 km naar onze bestemming kunnen wandelen of fietsen, come rain or shine? De bus duurt te lang, dan zit je nog met al die onwelriekende anderen en je komt nog niet eens voor de deur waar je wilt zijn. En taxi's: dat zijn auto's/autonoom rijdende auto's (sic).
Dus eerst maar eens naar zo'n tussenfase, onduidelijk is welke: mixed-mode rechtuit of uit de auto en dat rekening houdende met gewenste onderlinge disjunctie (veilige afstand).
En ja, dit alles dus nog afgezien van de hackability van de auto en adversarial attacks. Dat was eigenlijk onderwerp voor dit deel twee van dit drieluik 'Auto's, besturing en reflexen' bedoeld. Maar logica gaat boven plan, daarom zal de autonoom rijdende auto zelf in het derde deel alsnog aan bod komen. Misschien zal dan wel blijken dat we, zeker op korte en middellange termijn, met artificial intelligence niet kunnen wat we willen en dan moeten we maar willen wat we kunnen. Ook als dat niet zo veel zal blijken te zijn. Dan krijgen we de 'A' van AI sowieso wel voor elkaar, en gaan we naar een beter begrip van de benodigde 'I' toe. Dat overstijgt het nauwe (?) veld van AI-voor-auto's maar kan via een shift van denkwijze wel een betere toekomst brengen.

Deel 1 van dit drieluik is gepubliceerd in iB-Magazine 3 2021.

Referenties

(1) Was een paar jaar geleden de status. Wellicht is er al wat uitbreiding, maar willen we fileberichten over drukte op de Jan van Galenstraat als we op Vestdijk vaststaan?
(2) (Disclaimer:) Ik heb geen aandelen in het VCNL. Het is een onderdeel van Rijkswaterstaat, maar voor wie een idee wil krijgen wat zo'n centrale zou kunnen betekenen, bijvoorbeeld voor een 'Smart City', zou het PvIB aldaar eens een rondleiding moeten zien te organiseren.
(3) Wie een eenduidige definitie of beeld heeft van wat dat in zou houden; gelieve u te melden. Bestáát dat wel? Anderzijds wordt in dit artikel wel duidelijk dat er nog veel is uit te zoeken voordat eenduidigheid haalbaar is.
(4) Maar niet tegen Acts of Man. Acts of Nature zijn meestal lokaal of hooguit regionaal; Acts of Man (aanvallen) zullen op het systeem als geheel (nationaal) zijn gericht en dus grootschaliger zijn – en dan gecoördineerd moeten worden opgelost met een grote kans op niet-slagen.
(5) https://www.parool.nl/columns-opinie/de-bureaucratie-is-failliet~b3b8a9a6/, ook op https://app.box.com/s/m1uonzbrjuaj5gezlm7babur69vbpjv3
(6) https://maverisk.nl/bring-on-the-future-it-belongs-to-me/ wat die gaan doen…
(7) https://www.youtube.com/watch?v=R7qT-C-0ajI (1:20) en verder – maar de hele clip is top.
(8) Het is de vraag of de LIDARs en vergelijkbare sensorsystemen ooit snel genoeg zo kleine objecten kunnen identificeren.
(9) Voor dit en andere vertrouwensaspecten, zie Vehicle-to-Vehicle communicatie; weg van de privacy? iB-Magazine #4, 2020. Zie tevens Hacker Gehackt, iB-Magazine #5, 2020.
(10) Zoiets als https://tweakers.net/geek/163026/handkar-vol-smartphones-veroorzaakt-nepfiles-in-google-maps.html, maar dan veel vaker uitgevoerd.
(11) Herman Finkers: "Het stoplicht staat op rood / het stoplicht staat op groen / ja in Almelo / is altijd wat te doen."
(12) https://en.wikipedia.org/wiki/Mikhail_Bakunin
(13) https://maverisk.nl/new-category-miss-quotes/
(14) https://newrepublic.com/article/162280/autonomous-vehicles-public-transportation-uber-lyft

Authors: Reinder Wolthuis, senior consultant/project manager cybersecurity at TNO. Can be reached at reinder.wolthuis@tno.nl.
Frank Fransen, senior scientist cybersecurity at TNO. Can be reached at frank.fransen@tno.nl.

SOCCRATES - Real-time threat, impact analysis and response automation for SOC/CSIRT operations

SOCCRATES (SOC & CSIRT Response to Attacks & Threats, based on attack defence graphs Evaluation Systems) is a European innovation project, co-funded by the Horizon2020 program and led by TNO. It brings together some of the best European expertise in the field to develop, implement and evaluate an automated security platform to support SOC analysts. This second article on the project will zoom in on the security automation process and the role of each of the SOCCRATES platform components. The article concludes with some discussion and challenges we encountered.

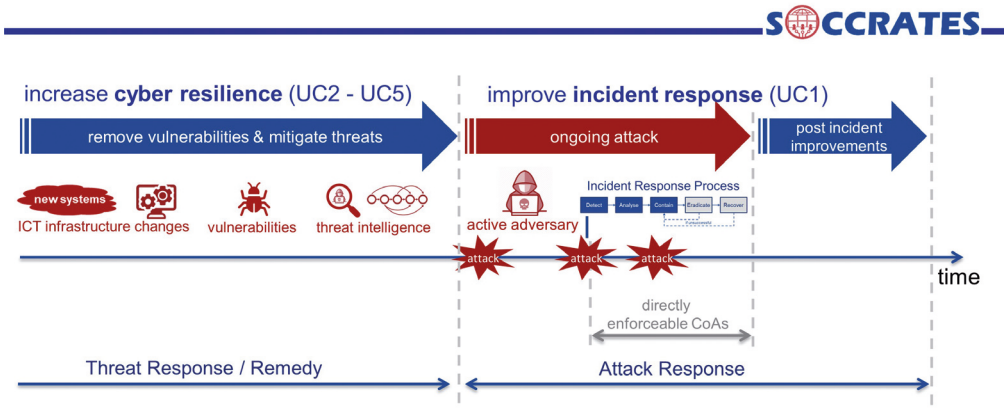


Figure 1 - The SOCCRATES use cases along an incident response time line.

The SOCCRATES project was introduced in the previous article. It gave an overview of the challenges that SOCs and CSIRTs currently face when defending their organisation's complex and continuously evolving ICT infrastructures against complex cyber-attacks and emerging threats, while at the same time there is a shortage of qualified cybersecurity talent. We described how the project addresses these challenges by developing a security automation and decision support platform, 'the SOCCRATES platform'. We will now look in a little more detail to the SOCCRATES platform and its role in the SOC and CSIRT process.

SOCCRATES Use Cases

To guide the development and validate the platform's capabilities, five different use cases have been defined. The use cases have been selected to represent the most relevant situations in which an organisation needs to reassess the security state of their ICT infrastructure, and determine if and how to react in order to protect the organisation's interests. The use cases are characterized by a particular security event that triggers the SOCCRATES platform to analyse and determine the best mitigation or response strategy.

- *Use Case 1: Response on Detected Ongoing Attack*
  Detect ongoing attacks and automatically analyse the attack, automatically determine the best response, and initiate deployment of the selected response.
- *Use Case 2: Response on Newly Received Cyber Threat Intelligence*
  Continuously collect new threat information, automatically analyse the potential business impact and determine best options for proactive mitigation.
- *Use Case 3: Response on Newly Discovered Vulnerable Assets*
  Automatically detect vulnerabilities on assets in the ICT infrastructure, assess if they enable new attack paths, determine and initiate mitigation actions.
- *Use Case 4: Response on Discovered System Configuration Change*
  Automatically detect configuration changes on assets in the ICT infrastructure, assess if they enable new attack paths and determine if action is needed.
- *Use Case 5: Response on Deployment of New Systems in Infrastructure*
  Automatically detect introduction of new systems to the ICT infrastructure. Automatically assess the new situation and determine if (additional) security measures are needed.

There is a crucial difference between use case 1 and the other use cases. In use case 1 the organisation is responding to a detected ongoing attack. That means that an active adversary has access to the organisation's ICT infrastructure and can potentially cause lots of harm. An organisation must be very careful when responding to the attack, as this can tip off the attacker. For use case 1 we thus follow the incident response steps: detection, analysis, containment, eradication, and recovery, as described in NIST SP800 61 (1) and the ISO/IEC 27035 series (2). Within SOCCRATES we decided to focus the automation, that is provided by the SOCCRATES platform, on the first three steps of incident response (detection, analysis and containment).

Use case 2 to 5 are triggered by security events that allow an organisation to improve the security in order to prevent an attacker to make use of it. In other words, these use cases focus on preventing incidents and are focussed on increasing the cyber resilience of the organisation, see figure 1.

General flow

When analysing the automation of these use cases, four common phases can be distinguished that are inspired by the MAPE-K (Monitor, Analyse, Plan, Execute and Knowledge) reference model used in autonomic computing (3) and self-adaptive systems. The four phases are (see figure 2):

1. Monitoring phase (M) – the system monitors for security events specific to the five use cases, and triggers the orchestration function of the SOCCRATES platform.
2. Analysis phase (A) – in this phase the SOCCRATES platform will automatically analyse the security event by collecting additional data, assessing the threat and determine the potential business impact. This is then presented as situational awareness to the SOC analyst. The SOC analyst may at this stage escalate to a CSIRT member.
3. Mitigation & response Planning phase (P) – in this phase the SOCCRATES platform will automatically generate possible responses, so called courses of action (CoAs), to mitigate threats or contain the ongoing attacks. The CoAs are assessed on effectiveness and business trade-off (i.e. costs, operational impact). This is then presented as option awareness for the SOC analyst / CSIRT member.
4. Mitigation & response Execution phase (E) - in this phase the SOC analyst / CSIRT member has selected a CoA and the SOCCRATES platform prepares and initiates the (semi)automated execution of this CoA.

The SOCCRATES platform uses an Orchestration and Integration Engine (OIE) to integrate, manage, and orchestrate all other components through these four phases. The OIE consists of an open source workflow tool, Activiti, and the Cortex framework from the Hive project for easy integration of security tools. In the following sections the role of the SOCCRATES components are described in each of these four phases.

Monitor phase

Based on the five use cases we can easily identify the security events for which we require monitoring capability.

For automating response on detected ongoing attacks (use case 1) it is necessary to detect attacks with high certainty and provide information on the attack stage (e.g. initial compromise, lateral movement, or exfiltration). For this purpose, the SOCCRATES project developed a concept to use an AI based reasoning tool on the events generated by different attack detection tools. The AI based Attack Detection (AAD) component will reduce the false positive rate, improves understanding of the situation, and identifies sequential patterns.
For collecting and triggering the SOCCRATES platform based on new threat Intelligence (use case 2) we use an open source Threat Intelligence Platform (TIP), called ACT. Since we also wanted to trigger new evaluations on threat actor profiles, the platform is extended with tools for creating adversary emulation plans.

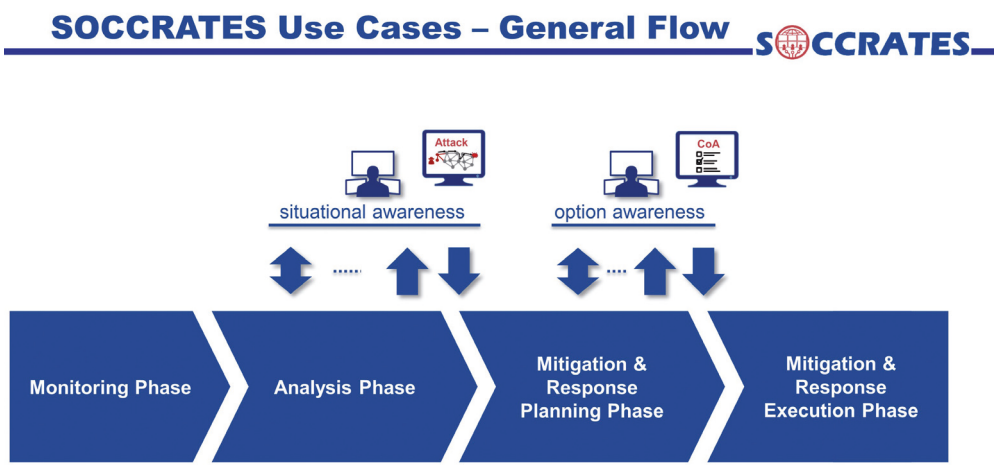


Figure 2 - General flow for the SOCCRATES Use Cases.

After collecting additional data, the SOCCRATES platform performs a threat analysis.

For discovering new vulnerabilities, configuration changes and new systems (use cases 3, 4 and 5) we rely on existing vulnerability scanning, network scanning and asset discovering tools. These scanning tools can also be used to automatically generate models of the organization's ICT infrastructure. To facilitate model generation, the SOCCRATES project developed an Infrastructure Modelling Component (IMC). The IMC provides the SOC and CSIRT with an up to date understanding of the environment they defend. The models can also be used for innovative analysis tools such as automated threat modeling and attack simulation.

Analysis phase

After collecting additional data, the SOCCRATES platform performs a threat analysis. For the threat analysis we use an Attack Defence Graph (ADG) based analysis to predict how attacks propagate over a model of the ICT infrastructure (provided by the IMC). This can for instance be used to determine the potential effect of a new threat, new vulnerability, or changes in a system's configuration. The ADG based analysis can be useful during an ongoing attack to determine if and how other systems can be compromised, or to support root cause analysis. Based on the adversary emulation plan provided by the TIP, the ADG will analyse how a particular adversary (i.e. APT group) may compromise the infrastructure. The ADG is based on research from SOCCRATES partner KTH (Swedish university) (4) (5), that has been transformed in a commercial product securiCAD by the spin-off company foreseeti.

To estimate the operational impact of a new threat or attack on the business, the SOCCRATES project developed a Business Impact Analyser (BIA) component that uses business logic modelling to build a graph representing the dependencies between the technical assets and the business missions, functions and processes. The BIA component will quantify the (potential) impact and provide the terminology of affected business functions and processes, enabling the SOC analyst to communicate more effectively to business owners during a security incident.

The results of the analysis will be provided to the SOC Analyst. Based on this information the SOC Analyst may decide that it is necessary to act, and initiate threat or attack response (e.g. contain an ongoing attack). The SOCCRATES Platform will then proceed to the mitigation & response planning phase.

Mitigation & response planning phase

For use case 1, the main focus of mitigation & response planning is on containing the attack. These attack response actions must be directly enforceable and typically only active during incident response. In a PhD-thesis (6) a term Tactical Response was introduced for the most efficient countermeasure to halt the ongoing attack. Strategic Response aims not only to end the ongoing attack, but also to prevent the occurrence of this attack in the future. Containment CoAs (CCoAs) are typically Tactical Responses. Next to these CCoAs, SOCCRATES platform also can generate attack responses to stop exfiltration, to prevent an adversary to regain access after recovery (root cause CoAs) and to protect critical assets during the attack (Impact Reduction CoAs). The latter two may be strategic responses.

For use cases 2 to 5, the response action could be structural changes, like the introduction of new security measures, changes in network configuration, or deploying software patches. Since deploying such changes takes more time, we refer to them as planned responses. A combination of directly enforceable and planned response is also possible. A software patch is typically deployed after testing and during planned

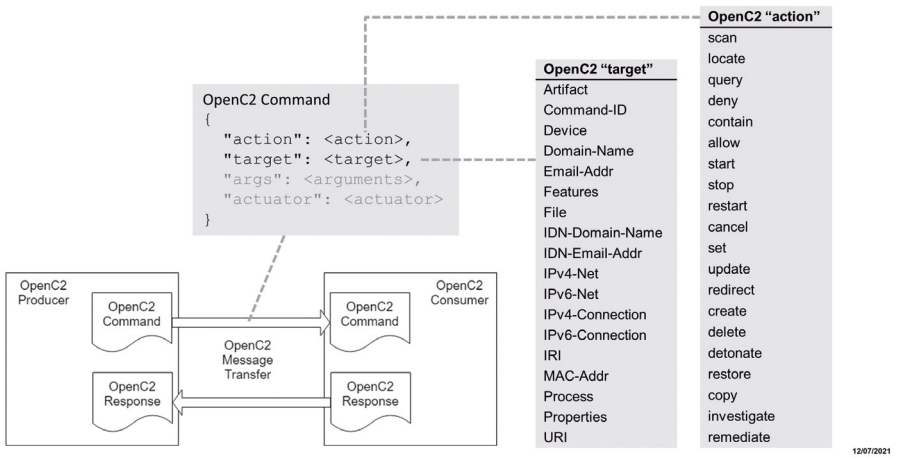


Figure 3 - OpenC2 command structure.

system downtime. An organisation can choose to first block certain traffic to the vulnerable system until the patch is deployed (i.e. directly enforceable response) and later deploy a software patch (i.e. planned response). Post incident response for UC1 may include structural changes based on lessons learned during the analysis and aftermath of the incident.

The SOCCRATES platform has two components that can produce CoAs. The first, the CoA Generator, is based on the use of the ADG. Since the attack languages used by the ADG includes all kinds of different defences, it is possible to turn on certain defences in the model of the ICT infrastructure and analyse the improvement. An algorithm is developed to automatically figure out which defences can best be turned on within a given total cost factor (each defence can be assigned a financial cost and/or deployment time). The second component that produce CoAs is the Response Planner. This component focusses on identification of directly enforceable response actions for e.g. containment of compromised hosts.

As part of the analysis the CoA Generator will provide information on the effectiveness of the recommended CoA. For financial assessment of the CoA, the Response Planner can calculate the Return on Response Investment (RORI). In addition, the Business Impact Assessment component can be consulted to determine if the CoA will have negative consequences for the business functions and processes. The SOCCRATES platform will present the list of generated CoAs with the analysis on effectiveness, RORI and business consequences to the SOC / CSIRT analyst, thereby enabling the analyst to make informed decisions on the response actions.

Mitigation & response execution phase

After the analyst has selected the CoAs to be executed, the SOCCRATES platform will initiate the (semi-)automatic execution of the CoAs. For many organisations automated execution of security responses and reconfiguration of security controls is a new and potential scary concept. An attacker may misuse such mechanisms to perform for instance a denial of service attack. Moreover, for MSSPs it is typically not allowed to perform reconfigurations in their customers network. Therefore, the basic response execution of the SOCCRATES platform is to automatically send IT support tickets or email with the recommended CoAs. This enables the integration of a human in the loop for authorisation of the CoA execution, and to include manual reconfiguration. To further automate the execution of the CoAs, SOCCRATES has adopted two machine readable languages that are being specified by OASIS Open:

- Open Command and Control (OpenC2) (7) – language for the command and control of technologies that provide or support cyber defences.
- Collaborative Automated Course of Action Operations (CACAO) (8) – standard for implementing course of action playbooks for cybersecurity operations.

OpenC2 is used to formulate response actions, such as filter

The SOCCRATES platform has been designed as an open extendable framework.

traffic or contain hosts, in a machine-readable language. CACAO is used to combine multiple response actions (defined with OpenC2) into a playbook and add meta data. An OpenC2 command must contain the 'action' and 'target', and optionally contains the 'actuator' and 'arguments', see figure 3. The actuator executes the command specified with the action and target. Since not many security systems support OpenC2, it is necessary to develop OpenC2 proxies that translate the OpenC2 commands to the proprietary commands of a security systems.

Example OpenC2 command to contain host:

```
{
 "action": "contain",
 "target": {
  "device": {
   "name": "hostname"
   "IPv4-Addr": "1.2.3.4"
  }
 }
}
```

During the SOCCRATES pilots (at MSSP mnemonic and the SOC of Vattenfall), automated execution of CoAs will not or only under specific conditions be allowed. The SOCCRATES platform will have the capability to initiate automatic reconfiguration, but in most cases this will be limited to sending IT support tickets.

Discussion & challenges

The SOCCRATES platform has been designed as an open extendable framework, enabling different security tools to be integrated in an automated platform. In particularly, we expect that in the future more security analysis and reasoning tools will emerge that can provide additional security information for faster and better decision making by the SOC / CSIRT. During the project we identified that some tasks are difficult to fully automate. A typical example of this is assessing the full extent of an incident. This is usually done by a SOC / CSIRT analyst by iteratively searching for evidence in multiple data sources to identify all compromised hosts in an ongoing attack. If security tools do not provide standardised and/or easy to integrate open APIs, further automation of security operations will be difficult. This is why we believe that security automation will not entirely replace human analysts, but automation will support the analysts in making their task more effective and efficient. We do believe that the task of the analyst will change; instead of analysing the details of each individual incident him/herself, the automation platform will take over a lot of the standard analysis steps. The analyst will be provided with option awareness and select CoA's presented by the automated security platforms; the analyst therefore will act on a higher abstraction level and this will require education and training.

Furthermore, the adoption of fully automated reconfiguration or execution of CoAs will take time. Within some domains, however, such as cloud environments, we anticipate that the concept of security automation will be adopted very fast.

This is part two. Part one SOCCRATES – Security automation in SOC & CSIRT environments was published in iB-Magazine 4.

References

(1) Paul Cichonski. Tom Millar, TimGrance, and Karen Scarfone, 'Computer Security Incident Handling Guide', NIST Special Publication 800-61 Revision 2, August 2012.

(2) ISO/IEC 27035-1:2016, Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management.

(3) An architectural blueprint for autonomic computing, IBM whitepaper, June 2005 http://www-03.ibm.com/autonomic/pdfs/AC%20Blueprint%20White%20Paper%20V7.pdf

(4) Pontus Johnson, Robert Lagerström, Mathias Ekstedt, 'A Meta Language for Threat Modeling and Attack Simulations', ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security, August 2018 Article No.: 38, Pages 1–8 https://dl.acm.org/doi/abs/10.1145/3230833.3232799

(5) Sotirios Katsikeas, Simon Hacks, Pontus Johnson, Mathias Ekstedt, Robert Lagerström, Joar Jacobsson, Max Wällstedt, Per Eliasson, 'An Attack Simulation Language for the IT domain', International Workshop on Graphical Models for Security, GraMSec 2020: Graphical Models for Security pp 67-86, https://link.springer.com/chapter/10.1007/978-3-030-62230-5_4

(6) Wael Kanoun, 'Intelligent Risk-Aware System for Activating and Deactivating Policy-Based Response', PhD thesis, 2011

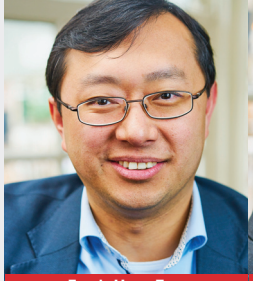
(7) https://www.oasis-open.org/committees/openc2

(8) https://www.oasis-open.org/committees/cacao

In deze rubriek geven enkele iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

‘Wat heeft de invoering van de AVG ons als redactie gebracht of gekost?’

Iedereen herinnert zich nog wel 25 mei 2018. Het was dé datum, in ons vakgebied ‘een moment’. Er was veel media-aandacht, veel rumoer en veel paniek. Om niets? Het ging vooral om de verzwarende administratieve last en de torenhoge boetes die als een zwaard van Damocles boven de hoofden zou gaan hangen. Er werden vinklijstjes afgewerkt en er werd (en wordt!) ‘wij zijn AVG-compliant’ geroepen. Zoals altijd daalde het stof neer, maar in dit geval niet helemaal. De focus op maatregelen is in verhoogde mate gebleven, de AP wordt (langzaam) volwassen en partijen houden elkaar meer dan ooit scherp.


Fook Hwa Tan


Chris de Vries

Onze redactie zit vol experts op het gebied van Informatiebeveiliging & Gegevensbescherming. In deze Privacy special stelt de hoofdredactie hen de vraag 'Wat heeft de invoering van de AVG jullie gebracht of gekost?'

Kansen en bedreigingen van AVG - Chris de Vries

Iedereen heeft met de Algemene Verordening Gegevensbescherming (AVG) te maken. Van overheid via de ondernemers naar de privé persoon. Het grote verschil is de mate van professionaliteit die wij ervaren bij de betrokkenen. Op de vraag 'Wat heeft de AVG ons, als redactie, gebracht of gekost?' kan ik dan ook vanuit mijn ervaring zeggen: 'menig zweetdruppeltje'.

Het lijkt allemaal zo eenvoudig. Je weet wat je doet, je kent je functie (verwerker of niet?!) en er staan modellen, zoals de Privacy Impact Assessment (PIA), gereed. Een kind kan de was doen. Echter, zo eenvoudig is het niet. De wet kent m.i. een groot gat, t.w. de overdracht van gegevens naar het buitenland om goede (?!) redenen. Het Europees Hof stemde in met overdracht van data naar het Verenigd Koninkrijk (wat gelijkstaat aan overdracht naar de Verenigde Staten), terwijl hetzelfde hof de privé-data overdracht naar de Verenigde Staten blokkeert. Bedreiging 1.
Dan hebben wij te maken met vele verenigingen in Nederland. Goedwillende bestuurders, zelden behept met data-management kwaliteiten. Wat moeten die dan doen met hun verantwoordelijkheid, lees aansprakelijkheid, en hun tekortschietende inzichten alsook onbegrip voor de gebruikte terminologie? Ik ben voor verschillende verenigingen bezig deze ver-van-hunbed show acceptabel te maken en het minimum geregeld te krijgen. Zowel bedreiging 2 als een kans. Al met al, een koppijndossier waarbij theoretisch alles klopt, maar in de praktijk de koning naakt is.

Grotere bewustwording, of toch niet? - Fook Hwa Tan

Drie jaar AVG heeft zeker privacy of bescherming van persoonsgegevens een boost gegeven. Maar wat heeft het echt opgeleverd? Waar willen we eigenlijk naartoe?
In de begin jaren was het nieuws vaak, dat grote boetes je organisatie zouden kunnen treffen als je niet voldeed aan deze nieuwe wet. De toezichthouder was in stelling gebracht en had het mandaat om onderzoek te doen en mogelijk je bedrijfsvoering plat te leggen als je niet goed omging met persoonsgegevens. Over de jaren zijn aantallen boetes gegeven door deze toezichthouder, maar de daadwerkelijk hoge bedragen zijn nog niet gezien.

Ook werd initieel gedacht dat klanten zouden verdwijnen en je mogelijk failliet zou kunnen gaan, indien bekend werd dat je niet voldoende zorgvuldig met persoonsgegevens bent omgegaan. Daar hebben we over de afgelopen periode jammer genoeg of gelukkig ook niet veel van gezien. Dit komt vaak, omdat de klanten of misschien zelfs gebruikers geen keus hebben om naar een andere organisatie te gaan.
Als laatste zou deze wet betekenen dat nog meer bureaucratie gecreëerd zou worden om aantoonbaar te maken, dat is voldaan aan adequate omgang met persoonsgegevens. De eerste implementatie drie jaar terug is gedaan om toen te voldoen, maar er zijn genoeg voorbeelden waar het vervolgens niet altijd goed is onderhouden. Of dit goed is of niet, kan ik geen uitspraken over doen.

Wat ik wel had gehoopt, is dat organisaties zich niet alleen bezighouden met privacy door angst, maar dat organisaties inzien hoe belangrijk het is voor eigen personeel of andere stakeholders om zorgvuldig met hun gegevens om te gaan. Laten we hopen, dat de komende drie jaar organisaties zelf de intrinsieke motivatie vinden en het plichtsgevoel krijgen om goed om te gaan met persoonsgegevens!

Lees ook het artikel van Nico Mookhoek in deze uitgave. Daarin blikt hij terug op wat de AVG ons heeft gebracht.

COLOFON

IB is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

PvIB
Platform voor InformatieBeveiliging

HOOFDREDACTEUR
Nicole van Deursen

GASTHOOFDREDACTEUREN
Bianca Brooijmans en Rachel Marbus

REDACTIE
Tom Bakker
Bianca Brooijmans
Maarten Hartsuijker
Lilian Knippenberg
Rachel Marbus
Fook Hwa Tan
Chris de Vries

BLADMANAGEMENT
MOS bv
Caroline Knobbe
Sam Dekkers
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE
MOS bv
E acquisitie@mos-net.nl
T 033 247 34 00

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

UITGEVER
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
E secretariaat@pvib.nl
W www.pvib.nl

ABONNEMENTEN
De abonnementsprijs in 2021 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

ABONNEMENTENADMINISTRATIE
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
E secretariaat@pvib.nl

ISSN 1569-1063

Dataprotectie & Privacy trainingen

Privacy compliant zijn, verantwoord omgaan met data en (cyber)security, AI, algoritmes en machine learning slim inzetten voor uw datagestuurde organisatie. Hoe doet u dat? Met de dataprotectie- en privacyopleidingen van IIR leert u nieuwe competenties en bent u als professional weer volledig op de hoogte.

Een greep uit ons aanbod:

FG in de publieke sector | 4-daagse praktijkcursus

Realiseer een privacy bewuste én compliant organisatie voor het vertrouwen van burger, medewerker en toezichthouder. Haal de benodigde kennis in huis en maak uw organisatie AVG-compliant.

Senior Privacy Professional | 5-daagse specialisatieopleiding

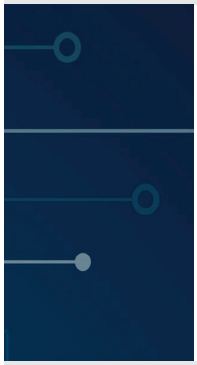
Ga complexe vraagstukken niet uit de weg en maak het verschil. Leer over leiderschap, verhoog uw kennis en vaardigheden op management- en bestuurkundig niveau. Sta sterker in uw schoenen als (senior) professional.

Auditing Privacy | 3-daagse masterclass

Kom in control door uw privacy audits onder de AVG naar een hoger niveau te brengen. Zo ziet u geen privacy risico's over het hoofd!

DPIA's en risicobeheersing | 2-daagse praktijkcursus

Krijg grip op uw privacy risico's en realiseer een bewuste organisatie die aantoonbaar in control is. Ontvang methodes en technieken voor het uitvoeren, opvolgen en inbedden van DPIA's.



Certified Data Protection Officer® | 10-daagse opleiding + examen

De premium beroepscertificering voor Privacy Professionals (PO, FG)

Deze opleiding is speciaal ontwikkeld voor de gevorderde Data Protection Officer (DPO/FG). Met de titel CDPO® laat u zien dat u een deskundig en professioneel Data Protection Officer bent.

» Inclusief diepgaande kennis van privacywetgeving en organisatie
» Beheers relevante aspecten op het raakvlak van informatiebeveiliging en privacy
» Wees in staat om praktisch met datalekken en incidenten om te gaan

Bekijk het volledige aanbod met actuele data op iir.nl/privacy

TSTC

ICT en Security Trainingen

ADVANCE YOUR CAREER WITH SECURITY IN 2021

CSA - Certified SOC Analyst
GSEC - Giac Security Essentials
GPEN - Giac Penetration Tester
EDRP - Disaster Recovery Professional
EHF - Ethical Hacking Foundation
CND - Certified Network Defender v2
CEH - Certified Ethical Hacker v11
CPENT - Certified Penetration Testing Professional

Want security start bij mensen!!

TECHNICAL SECURITY TRAININGEN

CEH - Certified Ethical Hacker
CHFI - Computer Hacking Forensic Investigator
CPENT - Certified Penetration Testing Professional
SSCP - Systems Security Certified Professional
OSCP - Offensive Security Certified Professional

SECURITY MANAGEMENT TRAININGEN

CISSP - Certified Information Systems Security Professional
CISM - Certified Information Security Manager
CISA - Certified Information Systems Auditor
CRISC - Certified In Risk And Information Systems Control
C|CISO - Certified Chief Information Security Officer

PRIVACY TRAININGEN

CIPP/E - Certified Information Privacy Professional / Europe
CIPM - Certified Information Privacy Manager
CIPT - Certified Information Privacy Technologist
CDPO - Certified Data Protection Officer

CLOUD SECURITY TRAININGEN

CCSP - Certified Cloud Security Professional

ISO TRAININGEN

ISO 27001 - Foundation
ISO 27001 - Lead Implementer
ISO 27001 - Lead Auditor
ISO 27005 - Risk Manager
ISO 27701 – Privacy Management

www.tstc.nl

Onze trainingen zijn weer klassikaal of Live Online te volgen