INFORMATIEBEVEILIGING MAGAZINE

- Uitreiking Artikel van het Jaar
- Het Data Protection Impact Assessment
- Privacy tool kopen?
- Waarom een privacy-adviseur geen functionaris gegevensbescherming is

JAARGANG 19 - 2019 - EDITIE 3

Uw applicaties goed **beveiligd!**

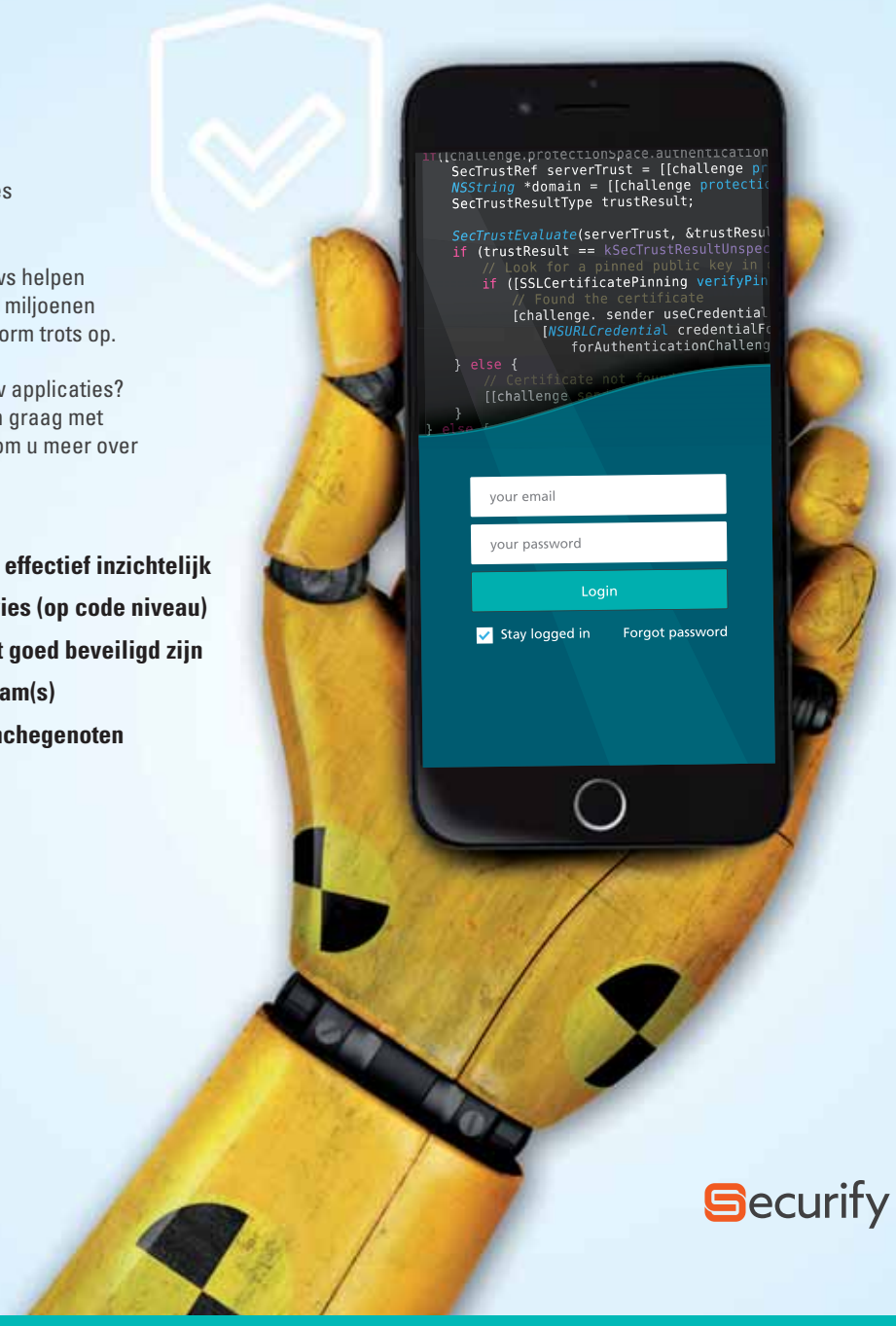
Veel bedrijven - van start-ups tot grote banken - vertrouwen al jaren op Securify om hun applicaties goed te beveiligen.

Met jaarlijks honderden pentesten en code reviews helpen wij achter de schermen mee om de gegevens van miljoenen Nederlanders veilig te houden. En daar zijn we enorm trots op.

Nieuwsgierig naar de beveiligingskwaliteit van uw applicaties? Of waarom Nederlands grootste bedrijven al jaren graag met ons samenwerken? Dan maken we graag kennis om u meer over onze aanpak te vertellen.

- ✓ **Alle beveiligingslekken en verbeterpunten effectief inzichtelijk**
- ✓ **Concreet en direct toepasbaar verbeteradvies (op code niveau)**
- ✓ **Maak aantoonbaar dat uw applicaties écht goed beveiligd zijn**
- ✓ **Een awareness boost voor uw ontwikkelteam(s)**
- ✓ **Leer waar u staat ten opzichte van uw branchegenoten**

www.securify.nl



Securify

Pentesting - Source Code Reviews - Agile Security - Red Teaming

Securify is specialist in web- en mobiele-applicatiebeveiliging en helpt bedrijven met het identificeren, verhelpen en voorkomen van technische beveiligingsrisico's.
Securify is opgericht door voormalig beveiligingsspecialisten van ABN AMRO, Delta Lloyd en Rabobank.

Een jaar later: privacy in volle aandacht

Op 25 mei 2018 stonden de media op hun kop: de AVG (of GDPR) stond voor de deur en vanaf 25 mei zou de wereld er heel anders uitzien. De meningen over de 'nieuwe' wetgeving liepen uiteen. De Autoriteit Persoonsgegevens was in ieder geval de meest besproken organisatie in maanden. Soms leek het heel even alsof we nog nooit eerder privacywetgeving gehad hadden…

En nu? Wat is er in mei 2019 over van alle media-aandacht? De media-aandacht lijkt verschoven te zijn naar schreeuwende koppen met niet altijd evenveel feiten. De verschillende meningen lijken nog niet verdwenen. Maar gelukkig zijn de meeste organisaties wel goed uitgerust met maatregelen om privacy goed te beschermen. En met de komst van de AVG is er een heel nieuw licht gaan schijnen over privacybewustwording. In het artikel van Kim Reijnen, 'AVG: blijf op de hoogte', lichten we 2 concrete zaken toe van recente uitspraken over de AVG. En met alle nieuwe inzichten zijn ook nieuwe functies ontstaan waarvan de functionaris gegevensbescherming wel de bekendste is. Maar we kennen ook de privacy-adviseur en de privacy officer. Waarom het één niet het ander is, licht Simone Fennell toe in haar artikel op pagina 30. En op pagina 32 leest u wat Lynsey Dubbeld vertelt over de ontwikkelingen op het gebied van dataprotectie en het vak van privacy officer.

En vanuit de media naar dichter bij huis: hoe is het gesteld met de privacymaatregelen bij u in de organisatie en hoe staat het er thuis voor? In deze uitgave een inkijkje bij Dré Lameir thuis, een security officer die daar alles over vertelt.

In deze privacy special leest u verder meer over de DPIA, de selectie van een privacy tool en zoals u van ons gewend bent: achtergrondinformatie over informatiebeveiliging & privacy. Want waar het eerst nog verschillende disciplines leken te zijn, blijkt een gelukkig huwelijk tussen de (C)ISO en de privacyfunctionaris ook in de organisatie het recept voor een vlekkeloze (privacy) huishouding.

Bianca Brooijmans en Rachel Marbus

Rectificatie iB-2

In Achter Het Nieuws van iB-2 stond een onjuiste zin: 'In 1958 is de Europe Unie (Verdrag van Maastricht)…'. In 1957 werd in Rome een verdrag gesloten dat in 1958 in werking trad. Dat was het verdrag tot het oprichten van de EC. In Maastricht werd in 1992 ook een treaty gesloten, wat veel meer inhield. Hiermee werd de EU opgericht en afspraken vastgelegd om veel meer samen te gaan doen. Nog weer later werd in de treaty van Lissabon expliciet de ECB vastgelegd.

Hartelijk dank Klaas Pranger!

IN DIT NUMMER

Dré Lameir is information security officer en VP innovation & development bij Enovation bv.
Hij is bereikbaar via: linkedin.com/in/lameir/

Digitale hygiëne

Mijn collega en ik carpoolen naar huis. We luisteren Spotify en ineens stopt de muziek. Op zich niet raar. Ik zet de muziek weer aan, we luisteren even en dan stopt de muziek weer. Hardnekkig als ik ben zet ik de muziek weer op. Dit gebeurt een aantal keer en uiteindelijk stopt de muziek weer, maar nu omdat de telefoon gaat. Op het display zie ik dat mijn vrouw belt. Ik neem op en ben verrast want ik hoor: "Hoi pap." Het is mijn zoon van 7. Leuk, denk ik, even kletsen. "Hee kerel, hoe is het?" Hij: "Ja pap (zucht, boos) … daar heb ik nu even helemaal geen tijd voor! KAN JIJ VAN ONZE MUZIEK AFBLIJVEN!"

Mijn collega en ik barsten in lachen uit en beloven gewoon naar de radio te luisteren. De reden voor de verstoring is ineens duidelijk, de jongste zat met de iPad op de bank en we namen blijkbaar over en weer de sessie over op hetzelfde account. Kleine jongens worden groot, denk ik. Het wordt tijd voor een familie-account bij Spotify. Uiteraard heb ik dat een aantal weken laten liggen en toen het weer gebeurde tijdens de rit naar huis was de maat vol.

Upgraden

Ik ga er in het weekend eens voor zitten en log in bij Spotify. Ik upgrade soepel naar een familie-abonnement en wil mijn oudste zoon (12 jaar) uitnodigen. Vanaf hier begint de ellende. Ik wil zijn account activeren, daarbij moet je aangeven dat je op hetzelfde adres woonachtig bent. Logisch, alleen wordt zijn account consequent geweigerd. Het mailadres is al in gebruik … door Henk, een man van 25 woonachtig in Frankrijk. Raar. Keer op keer loop ik vast.

Is mijn zoons account gehackt? Hoe kan dat? Ik ben toch ingelogd? Ik zie toch dat de adresgegevens kloppen? Ik probeer zijn aandacht te krijgen terwijl hij online met zijn vrienden aan het gamen is. Op zich is dat al een hele klus. Hij weet van niets, heeft ook geen account aangemaakt, weet niets van Henk uit Frankrijk, pa is een zeur, mag ik weer gaan gamen enzovoort.

Digitale vingerafdruk

Ik log in op zijn mailbox, die is ongebruikt … denk ik. Fout, er staan honderden mailtjes in van diverse onlinediensten. Hij heeft allerlei accounts geprobeerd aan te maken. Een kleine bloemlezing:

- 3 Snapchataccounts - "Oh, die gebruik ik niet."
- 1 account om een webshop te bouwen - "Ja, moesten we een keer voor een schoolproject."
- 1 fake Facebookaccount (Henk, Frankrijk, 25 jaar) - "Huh … heb ik Facebook?"
- 4 Instagramaccounts met tientallen dubieuze volgers - "Nou die gebruik ik niet pap, ik gebruik alleen dat laatste account."
- 2 Gmailaccounts op 2 verschillende achternamen - "Ik had even een mailadres nodig om weer een ander account aan te maken."
- Groot aantal profielen bij diverse game leveranciers - "Anders kon ik geen extra X downloaden voor het spel Y." Op de plaats van 'X' kwam: wapens, muntjes, skins, auto's, vliegtuigen. Op de plaats van 'Y' een willekeurig spelletje.
- 1 account op een AutoCad-achtige site - "Voor school moesten we 3D iets maken voor een MakerBotproject".
- 1 Samsungprofiel - "Ik heb toch mama's oude telefoon gekregen? Dat moest, want anders deed 'ie niks … die is trouwens héél sloom! Ik moet een nieuwe!"

En uiteindelijk dus wel een gratis Spotify-account … gekoppeld aan het fake Facebookprofiel van Henk uit Frankrijk. Nee, we wonen gewoon in Nederland en hebben geen vakantiehuis. En mijn zoon heet geen Henk. En dus kan ik het niet activeren, want het adres komt niet overeen en Spotify geeft de vage melding dat het mailadres al in gebruik is.

Nadat ik eindelijk heb kunnen inloggen op zijn Gmail, zie ik nog veel meer profielen die hij bij diverse diensten heeft aangemaakt. Ik schaam me echt. Ik heb gewoon niet goed op zijn digitale leven gelet en had geen idee dat meneer in zo'n korte tijd overal zijn digitale vingerafdrukken had achtergelaten. Hij heeft zich daarbij als volwassene voorgedaan om de leeftijdscontroles te omzeilen.

Actie

De security officer in mij neemt het over en gaat aan de slag. Accounts die hij niet langer gebruikt, gaan we verwijderen. Ik kan bij de eerste natuurlijk al niet inloggen, ik vloek. "Probeer '123konijn' eens", roept hij vanachter de Playstation. Het werkt! Verrek, blijkbaar wist hij dat ene wachtwoord nog, knap van hem … of wacht eens even … "Gebruik je dat wachtwoord dan wel vaker?", vraag ik hem. "Ja best wel vaak, handig toch", krijg ik nonchalant terug.

Ik trek nog net niet wit weg. Een paar uur verder blijkt dat hij voor bijna elke dienst hetzelfde wachtwoord heeft gebruikt. Ik ben de hele middag bezig met het inloggen en verwijderen van accounts en mijn verbazing groeit met de minuut. Schijnbaar achteloos maakt hij aan de lopende band profielen aan. Voor een spelletje, voor een schoolopdracht, omdat hij niet meer bij een account kan en omdat hij van telefoon wisselt. Hij en zijn leeftijdgenootjes verbruiken accounts als boterhamzakjes. Uiteraard probeer ik hem op de gevaren van het internet te wijzen, hem uit te leggen dat hij beter op moet letten. Het komt maar matig binnen, hij gaat wat anders doen en ik ploeter door.
Totdat hij zijn smartphone oppakt en ik hem ineens hoor roepen: "PAP! Ik kan nergens meer bij? Hoe kan dat?"

Awareness

Ik laat hem zien dat ik overal kan inloggen met zijn mailadres en standaard wachtwoord. En dat ik het simpel kan aan-

‘Mijn zoon en zijn leeftijdgenootjes verbruiken accounts als boterhamzakjes’

passen en zo zijn digitale jonge leven kan overnemen. Nu is meneer wél wakker! Hij komt naast me zitten en wil graag alles weten. Let’s go:

- Samen lopen we door al zijn online accounts en verwijderen wat ongebruikt of verdacht is.
- Ik maak een encrypted wachtwoordkluis aan op een gedeelde locatie waartoe we beiden toegang hebben.
- Ik zorg dat hij vanaf zijn telefoon en de andere devices bij die wachtwoordkluis kan met de juiste app.
- Ik leg hem uit hoe dit werkt en dat hij zo maar 1 sterke (grappige) wachtwoordzin moet onthouden. – “Zo! Handig pap!”
- Alle accounts, die hij wil houden, voorzien we van een sterk en vooral lang wachtwoord.
- We bekijken elke applicatie op zijn telefoon en verwijderen ongebruikte en enge zaken. Gelijk ook even de autoupdate aangezet.
- Van de apps die mogen blijven, zetten we de machtigingen goed (geen toegang tot van alles en nog wat zoals mail, gps, microfoon en camera).
- Als klap op de vuurpijl installeren we Google Authenticator en oefenen we met Two Factor Authentication (2FA).

Aan het einde van de middag is zijn telefoon weer supersnel en opgeruimd. Hij is vooral blij met de authenticator. Dit heeft voor hem iets magisch en hij vindt het stoer. Nu wil hij ineens overal QR-codes scannen en 2FA aanzetten. Hij vindt het gek dat dat nog niet bij alle accounts kan. “Maar dat is dan toch onveilig pap?” – ja dat klopt.

We spreken af dat we samen af en toe door zijn telefoon, mailboxen en applicaties lopen en dat we van nu af aan overleggen als hij een account aanmaakt. Ik complimenteer hem, omdat hij nu de veiligste van de klas is en hij moet lachen. En ik? Ik krijg uiteindelijk na veel gedoe zijn Facebookaccount verwijderd. Ik kan een nieuw vers en veilig Spotifyprofiel aanmaken en hem uitnodigen op ons familie-account. Bijkomend voordeel is dat Ronnie Flex, Lil’ Kleine en Rapper Boef eindelijk uit mijn playlists verdwijnen.

Bedrijfsrisico

Informatiebeveiliging is altijd een kwestie van maatregel op maatregel stapelen. En de ketting is zo sterk als de zwakste schakel. Maar wat als we tonnen uitgeven om de informatiebeveiliging op kantoor te waarborgen, terwijl de zwakste schakel eigenlijk thuis rondloopt? Wie van jouw collega’s heeft thuis een aantal pubers met meerdere devices met daarop tientallen accounts met dezelfde wachtwoorden? Of heeft kinderen die doorgeschoven bedrijfsmiddelen zoals een oude smartphone, tablet of laptop gebruiken? Dat zijn schatkisten, mooie aanvalsvectoren voor hackers. Hoe vaak komen kinderen ook op kantoor en pluggen even in op het netwerk? Of kunnen op de ‘echte WiFi’ in plaats van de ‘Gasten WiFi’? Wiens kids doen bij mam op kantoor een sociale stage in groep 8 en brengen dit soort risico’s mee?

Onze pentesters leren me altijd dat ze niet op zoek zijn naar jouw specifieke wachtwoord. Ze proberen gewoon net zolang totdat ze een bedrijfsaccount vinden met ‘Carrera911’ als wachtwoord. Maar misschien is een eenvoudige ingang wel ‘123konijn’ bij onze kinderen. We leren onze collega’s alert te zijn op kantoor, maar wat als thuis bij de CEO de boel wagenwijd openstaat en geïnfecteerd is? Wat zijn dan de risico’s?

Iedereen CISO en FG

Natuurlijk ben ik geschrokken. Als security officer heb ik de hele dag mijn mond vol van informatiebeveiliging en awareness op kantoor. Maar als vader thuis heb ik het een beetje laten lopen, vrees ik. We moeten in de privésfeer allemaal een beetje CISO en een beetje FG zijn. Digitale hygiëne moet net zo gewoon worden als handen wassen en tandenpoetsen. Je leert je kinderen om ze te beschermen tegen virussen. Dat is beter voor onze kinderen en dus uiteindelijk ook voor ons.

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

Wie zijn wij?

Bijna alle grote spelers in het privacyveld organiseren dit jaar een congres of event in het kader van 'een jaar na de AVG'. Dat gaat dan over hoe het ervoor staat (zijn er al veel boetes gevallen, zijn we nog wel aware, voldoen we aan de wet?) en regelmatig ook over de nieuwe figuur die bij vele organisaties rondloopt – de functionaris voor gegevensbescherming (FG/DPO). Ik spreek op verschillende plekken voor verschillende soorten publiek. Toen ik laatst van één van die congressen de sprekerslijst doorlas (toch leuk om te kijken welke oude vrienden ik weer tegenkom) viel het me op dat, hoewel we doorgaans hetzelfde doen in de praktijk, we vaak toch allemaal anders heten.

Ik zag een chief privacy officer, data protection officer, functionaris gegevensbescherming, IT auditor en privacyfunctionaris, chief information security and privacy officer, DPO risk control manager, privacy officer, corporate privacy officer, group data protection officer, privacy information officer, FG & information security officer en een marketing privacy officer. Een gedeelte daarvan oefent de wettelijke taken en bevoegdheden uit zoals die omschreven staan in de AVG bij de functionaris gegevensbescherming, soms met andere taken erbij. Maar wat de rest nu precies doet, is toch wat lastig af te leiden uit de naamgeving. Wat iedereen in ieder geval doet, is privacy-advies geven. Althans, dat hoop ik dus.

Is het nou eigenlijk erg dat we allemaal anders heten? Wel als je een FG/DPO bent, dan lijkt het me goed dat je die titel luid en duidelijk voert, zodat voor zowel klanten als werknemers duidelijk is dat jij de FG bent bij wie ze terecht kunnen voor hun vragen en klachten. Bij de andere namen is het niet zo erg, maar vooral verwarrend. Voor de rest zie ik in de namen soms terug waar iemand in de organisatie geplaatst is: bij legal/compliance, risk, IT audit of infosec. Wat die mensen dan allemaal doen en/of kunnen, is daarmee niet duidelijk. Hoewel ik bij die marketing privacy officer best nog wel een aardig idee heb.

Vroeger - hier spreekt oma Rachel - waren we nog maar met een klein groepje privacyliefhebbers en heetten we eigenlijk allemaal 'gewoon' privacy officer (als we in dienst waren) of privacy-adviseur (als we ingehuurd werden). We kenden elkaar ook bijna allemaal wel, dus we wisten wat voor vlees we in de kuip hadden. Ik houd van eenvoud. Lijkt me helemaal niet gek om te kijken of we een beetje kunnen uniformeren (en daaraan kwaliteitsstandaarden verbinden natuurlijk). Privacy officer als je in de organisatie privacy-advies geeft en chief privacy officer als je dan ook nog eens de baas bent. En dan als FG/DPO de wettelijke titel blijven voeren (luid en duidelijk).

Maar goed, hoe belangrijk is een naam dan eigenlijk echt? Passie voor privacy is volgens mij de belangrijkste drijfveer voor iedereen die op de een of andere manier 'privacy doet'. En als je vanuit passie werkt, dan maakt het ook niet meer zo heel veel uit hoe je heet, als de mensen je maar weten te vinden. Ik ben ook niet de eerste die dit bedenkt natuurlijk. Vele jaren geleden was iemand me al voor: 'A rose by any other name would smell as sweet…' (Shakespeare).

Rachel

Fred van Noord is kwartiermaker cybersecurity hoger onderwijs bij dcypher.
Fred is te bereiken via: f.vannoord@dcypher.nl

Jan Piet Barthel is directeur van dcypher en programmamanager cybersecurity onderzoek bij NWO. Jan Piet is bereikbaar via j.barthel@nwo.nl

Inventarisatie van erkende cybersecurity-opleidingen in Nederland

De afgelopen jaren is in onderzoek bevestigd waar de beroepspraktijk zich al jaren van bewust is: er is een toenemende krapte op de arbeidsmarkt van cybersecurityspecialisten en een tekort aan cybersecuritydocenten om die specialisten op te leiden. Om meer inzicht te krijgen in deze problematiek heeft dcypher in 2018 een inventarisatie uitgevoerd van cybersecurity-opleidingen in het hoger onderwijs.

Het doel voor de korte termijn is het identificeren en beschrijven van erkende opleidingen met een focus op cybersecurity. Het doel voor de langere termijn is het formuleren van aanbevelingen op basis van een verschillenanalyse van de vraag naar goed opgeleide experts en het aanbod van cybersecurity-opleidingen.

Werkwijze

Een klankbordgroep - bestaande uit professionals uit het bedrijfsleven, de overheid en het hoger onderwijs - heeft een sjabloon opgesteld met onderwerpen die relevant zijn voor cybersecurity. Van elk onderwerp kan daarin de onderwijsinspanning (studielast) worden aangegeven. Dit sjabloon is uitgezet in het hoger onderwijs.

De onderwerpen waren onderverdeeld in drie categorieën:

a. Organisatie - zoals governance, risicomanagement en informatiebeveiliging, wet- en regelgeving en compliance, business continuity management, review en audit;
b. Mens en gedrag - zoals awareness, cybercrime, ethiek;
c. Techniek - zoals ICT (computersystemen, netwerken, software, data), ICT-beveiliging, malware-/fraude-/hackingtechniek, cryptografie, monitoring en analyse.

Daarnaast is in het sjabloon de studielast van stage en afstuderen, de keuzeruimte (zoals minoren) en de basiscompetenties (zoals presenteren, vergaderen, onderzoeken, ondernemen enzovoort) ingevuld.

Uitgangspunten bij het in kaart brengen van de opleidingen waren:

1. de opleiding is voor een groot deel gericht op cybersecurity;
2. de opleiding is opgenomen in het CROHO (1);
3. de opleiding leidt op voor de graad Associate degree (2), bachelor of master;
4. het totaal van de studielast aan cybersecurity-onderwerpen in de opleiding is minstens 60 ECTS (3).

De volgende opleidingen kwamen in aanmerking:

a. opleidingen van het bekostigde hoger onderwijs (hogescholen en universiteiten);
b. niet-bekostigde hbo-opleidingen (deze zijn op geen enkele manier door de rijksoverheid gefinancierd);
c. niet-bekostigde post-initiële masteropleidingen (4).

In dit onderzoek zijn alleen de opleidingen meegenomen die daaraan hun medewerking hebben verleend. Onderwijsinstellingen die niet konden meedoen, zijn uitgenodigd hun gegevens alsnog aan te leveren om te worden opgenomen in het online overzicht.

Resultaten

Er worden twintig cybersecurity-opleidingen aangeboden door achttien onderwijsinstellingen. Vijftien hiervan zijn voltijd (vijf master, tien bachelor) en vijf deeltijd (drie master, twee bachelor). Drie van de vijf voltijd masteropleidingen zijn tweejarig (120 ECTS) en twee zijn éénjarig (60 ECTS). Bacheloropleidingen worden grotendeels door hogescholen aangeboden (11 van de 12).

	Master	Bachelor	totaal
Voltijd	5	10	15
Deeltijd	3	2	5
totaal	8	12	20

Tabel 1 - Verdeling van voltijd en deeltijd cybersecurity master- en bacheloropleidingen

Om opleidingen te kunnen typeren, is gekeken hoe in het curriculum de verhouding ligt tussen de categorieën:

Organisatie, Mens en gedrag en Techniek. Als één van de deze categorieën een hoger aandeel heeft dan 60% dan is de opleiding in het onderstaande overzicht aangegeven met een kleurmarkering (oker: Organisatie, oranje: Mens en gedrag, blauw: Techniek). Als de studielast grotendeels verdeeld is over twee dan wel drie categorieën dan is deze niet gekleurd.

Techniek	Organisatie	Mens en Gedrag	Combinatie

In onderstaande tabellen staan de resultaten per master- en bacheloropleiding voor voltijd en deeltijd.

Master – Voltijd

Instelling	Opleiding	Organisatie (%)	Mens & Gedrag (%)	Techniek (%)
Vrije Universiteit (VU)	Computer Systems Security	3	-	97
TRU/e (Radboud/TUe)	Cyber Security	14	5	81
Univ. van Amsterdam	Security & Network Engineering	15	13	72
4TU (TU Delft/TU Twente)	Cyber security	16	16	68
Radboud Universiteit	Security & Privacy	67	11	22

Bachelor – Voltijd

Instelling	Opleiding	Organisatie (%)	Mens & Gedrag (%)	Techniek (%)
Hogeschool Amsterdam	Cyber Security	9	-	91
Radboud Universiteit	Cyber Security	6	4	90
Fontys Hogescholen	ICT & Cyber Security	5	5	90
Hogeschool Leiden	Forensische ICT	5	7	87
De Haagse Hogeschool	Cybersecurity Technology	12	2	86
Hogeschool Rotterdam	Technische Informatica	15	7	78
Arnhem & Nijmegen	Infrastructuur en Security Mgt	37	-	63
NHL Stenden	Cybersafety	34	66	-
Fontys Hogescholen	ICT & Management and Security	26	26	47
De Haagse Hogeschool	Information Security Management	56	24	20

Master – Deeltijd

Instelling	Opleiding	Organisatie (%)	Mens & Gedrag (%)	Techniek (%)
De Haagse Hogeschool (CSA)	Cyber Security Engineering	12	2	85
Univ. Amsterdam	Security & Network Engineering	15	13	72
Univ. Leiden (CSA)	Executive Cyber Security	33	33	33

Bachelor – Deeltijd

Instelling	Opleiding	Organisatie (%)	Mens & Gedrag (%)	Techniek (%)
Fontys Hogescholen	ICT & Management and Security	26	26	47
NOVI	Cyber Security	52	-	48

Tabel 2 - Typering van master- en bacheloropleidingen in voltijd of deeltijd

In onderstaande tabel staat per typering (Techniek, Organisatie en Mens en gedrag) de totalen naar voltijd versus deeltijd en master versus bachelor.

	Voltijd		Deeltijd		
	master	bachelor	master	bachelor	totaal
Techniek	4	7	2	-	13
Organisatie	1	-	-	-	1
Mens en Gedrag	-	1	-	-	1
Combinatie	-	2	1	2	5
totaal	**5**	**10**	**3**	**2**	**20**

Tabel 3 - Het aantal master- en bacheloropleidingen, onderverdeeld naar typering en voltijd en deeltijd

Dertien opleidingen zijn gericht op Techniek, één opleiding richt zich vooral op Organisatie en één opleiding heeft de focus op Mens en gedrag. Vijf opleidingen bieden een mix van Techniek, Mens en gedrag en/of Organisatie.

Minoren en keuzevakken die zijn genoemd, zijn onder andere: pentesting/hacking, Internet of Things (IoT), big data, vulnerability research, sensor technology, mobile development, cybersecurity technology en cybersafety. Het gedetailleerde en geactualiseerde overzicht is te vinden op de website van dcypher: www.dcypher.nl.

Aantallen afstudeerders

In 2018 hebben bijna 400 studenten hun cybersecurity-opleiding afgesloten met een diploma (165 master, 229 bachelor). Het merendeel hiervan (307 studenten) heeft een technische cybersecurity-opleiding gevolgd (130 master, 177 bachelor). Het werkelijke aantal afgestudeerden is hoger, omdat een enkele opleiding niet in het overzicht staat en een paar opleidingen die wel in het overzicht staan geen uitstroomgegevens hebben aangeleverd. Overigens zal de komende jaren het jaarlijkse aantal afstudeerders naar verwachting verder groeien, omdat er dan nieuwe opleidingen bij zijn gekomen.

Docententekort

Aan opleiders is gevraagd naar het huidige of te verwachten docententekort bij hun opleiding. Ook is er gevraagd om welke specifieke expertise het daarbij gaat. Negen opleidingen geven aan dat het vinden van goede docenten niet eenvoudig is. Reacties variëren van 'enigszins moeilijk' tot 'heel moeilijk'/ 'uiterst gecompliceerd'. De expertise waarnaar wordt

"Nederland beschikt over voldoende cybersecuritykennis en -kunde"

gezocht is 'échte IT'er met kennis en ervaring op netwerk/pentesting/security-vlak en ethical hacking'. Vijf opleiders gaven aan geen problemen te hebben met het vinden van docenten.

Hybride docenten

Een ontwikkeling die verbetering kan brengen ten aanzien van het docententekort, is het hybride docentschap (5). Het geeft voordelen aan onderwijsinstellingen, professionals, studenten én werkgevers:

- het docententekort wordt opgelost;
- professionals kunnen met hun up-to-date inzichten en praktijkervaring bijdragen aan de innovatie van het onderwijs;
- professionals krijgen een afwisselende werkweek met de voldoening van het opleiden van jong talent;
- opleidingen worden aantrekkelijker voor (potentiële) studenten, omdat zij les krijgen van ervaren professionals die de praktijk goed kennen en de verhalen uit de praktijk doorgeven;
- werkgevers krijgen meer gemotiveerde medewerkers, vanwege de voldoening van het leveren van een bijdrage aan het urgente maatschappelijke vraagstuk van digitale veiligheid;
- werkgevers komen via hun medewerkers in een vroeg stadium in aanraking met jong talent.

Hoe verder?

1. Het hierboven geschetste beeld is een momentopname. Veranderingen hierin kunnen vele oorzaken hebben: opleidingen worden toegevoegd, vakken worden toegevoegd, vakken worden ingewisseld voor andere vakken enzovoort. Daarom wordt het beeld door dcypher online aangevuld en geactualiseerd. Geïnteresseerden in de meest recente informatie over een opleiding, wordt aangeraden om het online overzicht te bekijken en daarnaast de websites van opleidingen te raadplegen.
2. PvIB publiceert beroepsprofielen (6) die generieke cybersecurityberoepen beschrijven waarnaar op de arbeidsmarkt veel vraag naar is. Deze beroepsprofielen kunnen de basis zijn voor het ontwikkelen van cybersecurity-opleidingen. De beroepsprofielen kunnen bovendien gebruikt worden in een nog te implementeren certificatiestelsel (7).

Het Dutch cybersecurity platform higher education & research werd in 2016 opgericht. Hiermee hebben vier ministeries (EZK, OCW, J&V en Defensie) samen met NWO (Nederlandse organisatie voor Wetenschappelijk Onderzoek) het initiatief genomen invulling te geven aan één van de doelstellingen in de Nationale Cyber Security Strategie: "Nederland beschikt over voldoende cybersecuritykennis en -kunde en investeert in ICT-innovatie om onze cybersecuritydoelstellingen te halen."

Referenties

(1) Het Centraal Register Opleidingen Hoger Onderwijs (CROHO) bevat de lijst van alle in Nederland georganiseerde opleidingen voor hoger onderwijs die door het Ministerie van Onderwijs, Cultuur en Wetenschap worden erkend.

(2) Een associate degree is een tweejarig programma binnen een HBO-bacheloropleiding met een eigen wettelijke graad (Ad). In 2018 bestonden, voor zover bekend, nog geen associate degree (Ad) opleidingen in cybersecurity. De haalbaarheid voor het starten van een Ad-opleiding werd onderzocht door de Hogeschool van Amsterdam en de Hogeschool van Rotterdam.

(3) European Credit Transfer System; 1 ECTS = 28 uur studiebelasting.

(4) Een post-initiële masteropleiding is een opleiding voor personen met een hbo- of universitair diploma en/of met de nodige werkervaring in de beroepspraktijk.

(5) Een combinatie van een baan voor de klas met een andere baan Zie www.hybridedocent.nl

(6) www.pvib.nl

(7) https://www.pvib.nl/veelgestelde-vragen/certificering

Frans Dondorp (CIPP/E, CIPT) is werkzaam bij Decos Information Solutions.
Hugo Leisink (CIPP/E) is werkzaam als senior adviseur cybersecurity binnen de Rijksoverheid.

De auteurs schrijven op eigen titel, representeren met dit artikel geen bedrijf of instantie en streven met dit artikel geen commerciële of politieke belangen na. Voor vragen zijn ze te bereiken via info@privacy-friendly.nl.

Het Data Protection Impact Assessment

Het Data Protection Impact Assessment (DPIA) wordt niet altijd goed uitgevoerd. De nadruk ligt vaak te veel op risico's voor de organisaties en te weinig op de risico's voor de betrokkenen.

De Algemene Verordening Gegevensbescherming (AVG) schrijft voor dat de verwerkingsverantwoordelijke een gegevensbeschermingseffectbeoordeling (DPIA) uitvoert wanneer een verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Dit staat in AVG artikel 35 lid 1, waarbij in lid 3 en lid 7 verder wordt uitgelegd wanneer deze DPIA specifiek vereist is en wat daar in dient te staan. Vooral lid 7 sub b en c zijn voor nu van belang. Daarin staat dat de DPIA 'ten minste' een beoordeling van de 'noodzaak en evenredigheid van de verwerking' moet bevatten, alsmede een 'beoordeling van de risico's voor de rechten en vrijheden van betrokkenen.' Bij een DPIA gaat het dus vooral ook om de betrokkenen en zeker niet alleen om jou als verwerkingsverantwoordelijke. Een DPIA gaat niet alleen om jouw risico's op overtreding van de AVG, een datalek, een boete, imagoschade enzovoort. In de praktijk is dat vaak echter wel de focus.

Natuurlijk zijn die onderwerpen belangrijk, maar de AVG eist meer. Een DPIA kan niet alleen gericht zijn op de belangen van een organisatie. Niet in de laatste plaats omdat de AVG zich richt op de belangen van natuurlijke personen.

De betrokkene, degene wiens privacy in het geding is, heeft immers niets aan zo'n 'interne' DPIA. Iedereen mag verwachten dat jij je aan de AVG houdt. Daarin staat in artikel 5 t/m 11 helder welke verwerking wel of niet mag en in artikel 32 t/m 34 waar de beveiliging aan moet voldoen. Als je een intern gerichte DPIA doet, voeg je niets toe. Zo'n DPIA is weinig meer dan een verklaring dat je zelf vindt dat je je aan de wet houdt. Dat zegt te weinig over wat jouw activiteiten specifiek betekenen voor de rechten en vrijheden van de betrokkenen. Daarom is artikel 35 lid 7 sub c een bepaling die je niet mag missen.

Privacy versus security

De klassieke tegenstelling tussen gegevensbescherming en gegevensbeveiliging komt toch weer aan de orde. Dit zijn twee werelden en dat blijft ook zo. Andere doelgroepen: de gegevensbescherming is primair gericht op de betrokkene en de gegevensbeveiliging primair op de eigen organisatie. Ja, security draagt bij aan privacy. Als je eigen informatiebeveiliging niet op orde is, dan kan je nooit een goede omgang met persoonsgegevens van anderen garanderen. Security is een heipaal. Belangrijk, maar geen huis.

Voor wat betreft de DPIA hebben we het over 'artikel 32 versus artikel 35'. De eisen en inhoud van de DPIA worden specifiek omschreven, met als kern 'bescherming van persoonsgegevens'. Daarvoor is natuurlijk de beveiliging ex artikel 32 nodig, maar dat is niet alles. Het simpelste voorbeeld is dat een risico (geïdentificeerd door de DPIA) ook gemitigeerd kan worden door een wijziging in het proces. Of door gegevensminimalisatie. Niet voor niets moet je in de DPIA ook de 'noodzaak' nadrukkelijk onder de loep nemen. Vraagstukken die breder zijn dan alleen maar het beveiligen van gegevens. Een DPIA kan dus niet alleen een beveiligings-

‘Wij roepen privacy-experts op om met ons mee te doen, om hun mening te delen en bij te dragen aan een betere DPIA’

assessment zijn, zoals je ook niet alleen op een heipaal kunt wonen.

De gegevensbescherming dient gebruik te maken van hetgeen een organisatie met informatiebeveiliging heeft bereikt. Van daaruit is namelijk geregeld dat informatie goed wordt beschermd, welke organisatorische afspraken er zijn en welke technische maatregelen genomen zijn. Daar kan in de DPIA dus naar verwezen worden, zonder daar inhoudelijk op in te gaan. De CISO zit daarbij aan tafel om te beargumenteren of via ‘passende maatregelen’ aan artikel 32 voldaan wordt. De CISO is niet degene die vertelt dat een nieuwe verwerking een verhoogt risico op discriminatie introduceert. Artikel 35 is niet artikel 32.
De AVG sluit aan bij de risicogebaseerde aanpak van informatiebeveiliging. Je denkt dan in ‘kans × impact’, waarbij je waarschijnlijk gewend bent dat je een laag risico kunt accepteren. Daarin zit een verschil tussen gegevensbescherming en informatiebeveiliging. Je kunt immers niet spreken voor een betrokkene en je kunt dus geen uitspraak doen over de acceptatie van een risico.

In de privacywereld is het bestaan van een risico op discriminatie altijd onacceptabel. Je kunt geen kleine kans op discriminatie accepteren, zeker niet ‘namens’ de betrokkenen. Die risicomatrix is er dus niet. Het bestaan van een risico vereist een maatregel, ongeacht hoe je (als niet-betrokkene) dat risico inschat.

Wat een organisatie dus niet moet doen tijdens een DPIA is op zoek gaan naar hoe de verwerking te verantwoorden is onder de AVG. Wat organisaties moeten leren en accepteren is dat een DPIA kan uitwijzen dat een geplande verwerking niet strikt noodzakelijk is of niet eerlijk is naar de betrokkenen en dus geen goed idee is. Zij moeten leren dat, hoe goed de beveiliging ook is, afzien van een geplande verwerking soms de beste en meest eerlijke keuze is.
Een maatregel in de wereld van gegevensbescherming kan dus ook inhouden dat het proces aangepast wordt of niet meer wordt uitgevoerd. Gegevensminimalisatie. Privacy by design. Dat raakt niet per se aan gegevensbeveiliging.

Een nieuwe DPIA

Wij denken dat er een nieuwe, publiek beschikbare DPIA moet komen. Een DPIA die meer stuurt op of de verwerking wel eerlijk is richting de betrokkenen. Een DPIA waarbij je niet kan wegkomen met alleen een antwoord op de vraag of een verwerking wel mag en of de of gegevens wel goed beveiligd zijn. Wat nodig is, is een DPIA die teruggaat naar de kern en gericht is op de vraag wat een verwerking betekent voor een betrokkene. Een extern gerichte DPIA.
Wij vinden dat zo’n DPIA publiek beschikbaar moet zijn. Omdat wij allemaal moeten willen dat die kleine MKB’er ook een DPIA uitvoert. Omdat een DPIA een ‘work in progress’ is en steeds beter wordt naarmate privacy-experts vragen aanscherpen. Omdat DPIA’s herhaald moeten kunnen worden binnen een organisatie. Omdat DPIA’s gedeeld en vergeleken moeten kunnen worden tussen organisaties. Hoe mooi zou het zijn als een andere organisatie een (deel van) jouw DPIA kan gebruiken zodat het voor hen makkelijker wordt en minder werk oplevert en hen dus nog minder excuus geeft om het niet te doen. Hoe mooi zou het zijn als een betrokkene de DPIA kan opvragen en ziet dat zijn belangen ook echt zijn meegewogen.

Wij hebben reeds een eerste aanzet gedaan tot zo’n nieuwe DPIA. Het resultaat van onze inzet is te vinden op www.privacy-friendly.nl. Deze eerste versie is nu nog slechts een PDF, wat dus een handmatige uitvoering van de DPIA vereist. We werken hard aan een gebruiksvriendelijkere mogelijkheid om de DPIA online in te kunnen vullen.
Wij roepen privacy-experts op om met ons mee te doen, om hun mening te delen en bij te dragen aan een betere DPIA. Een ‘community standard’ waarbij iedereen een inhoudelijke bijdrage kan leveren. Een DPIA op die door alle privacy-experts gekend en erkend wordt.

TOM BAKKER

Deze keer is het mijn beurt om mezelf voor te stellen als bestuurslid. De meesten van jullie zullen mij wel kennen, omdat ik al een tijd meedraai in het PvIB. Ik zit in de redactiecommissie van ons iB-Magazine. Ik doe dit alweer 10 jaar, waarvan 8 jaar als commissievoorzitter en vanaf dit jaar ook als bestuurslid. In 1978 begon ik in de IT bij Delta Lloyd Verzekeringen als programmeur (wat was dat ook alweer?). In die tijd heb ik mijn EXIN AMBI-diploma gehaald. Na 12 jaar als ontwikkelaar en later als DBA overgestapt naar IT-audit. Ik heb de postdoc IT-auditopleiding mogen volgen aan de VU. Net als zoveel IT-auditors later in de informatiebeveiliging gerold als CISO. Na 2012 bij Allianz en Digidentity. In september 2017 ben ik met vervroegd pensioen gegaan en neem ik zo nu en dan wat parttime opdrachten aan.

Ik ben altijd al verbonden geweest aan (vak)verenigingen (NGI/KNVI, ISACA, NOREA, ISF, CIOnet), omdat ik de meerwaarde zag in kennisdeling en netwerken. Omdat informatiebeveiliging niet op zichzelf staat, kijk ik vooral ook naar aanpalende specialismen als BCM, privacy, crisismanagement, fraudebeheersing en fysieke beveiliging. Die meerwaarde probeer ik uit te dragen in het iB-Magazine door ook artikelen op die gebieden te organiseren.

Wat mij de laatste tijd is opgevallen, is dat er steeds meer geruchten de ronde doen (Huawei) en incidenten plaatsvinden waarbij al dan niet sprake is van bewust aangebrachte zwakheden in hardware. Voor ons vakgebied wel een lastige, want die zaken zitten vaak diep in (technische) systemen. Niet iedereen heeft daar verstand van. Dat wordt nog een uitdaging.

Ik zie ook een forse toename van gevallen van bedrijfsspionage waarbij IP gestolen wordt. Al dan niet door naties. Denk aan het recente incident bij ASML met een forse schade.

Incidenten zijn er bijna dagelijks en zijn geen nieuws meer. Wat steeds belangrijker wordt, is hoe we met die incidenten omgaan en hoe we die moeten oppakken. 'Resilience' is daarbij het toverwoord geworden. Ik denk dan dat er meer aandacht voor crisismanagement zal en moet komen en dat de professionals en het PvIB daar energie in moeten steken.

Over vijf jaar hoop ik dat ik kan constateren dat we overbodig zijn geworden als het PvIB. Ik heb dat in het verleden altijd gedacht, omdat informatiebeveiliging niet iets is dat 'eraan geplakt moet worden', maar gewoon vanzelfsprekend moet zijn. Security by design dus. Ik ben alleen bang dat dat in die 5 jaar nog niet gaat lukken. Integendeel, gezien de snelle ontwikkelingen zal er juist meer vraag komen naar security professionals. Als ik ergens kom, op IT-beurzen bijvoorbeeld, dan valt het mij op dat er maar weinig mensen van het PvIB gehoord hebben. Zelfs bij security professionals. Dat is wel jammer.

Voor de komende jaren moeten we meer samenwerken met belangengroepen en verenigingen die niet direct met ons vakgebied te maken hebben om het PvIB te profileren. Een mooie taak voor mij, de commissies en het bestuur.

Frank van Vonderen is CEO van WeDoPrivacy en partner bij Verdonck, Klooster & Associates. Frank is bereikbaar via frank.vanvonderen@vka.nl.

Privacy tool kopen?

Dit zijn de 5 vragen die je moet stellen

"Hebben we hier geen tool voor nodig?" Het is een veelgehoorde opmerking bij veel organisaties die aan de slag gaan met complexe onderwerpen als security of privacy. Deze wens komt voort uit de behoefte om grip te krijgen op een moeilijk onderwerp, om de wereld in te kunnen delen in kleuren en om te kunnen vertellen of je als organisatie in control bent.

Maar een ander gezegde is: 'a fool with a tool is still a fool'. Dat geldt ook voor privacy tooling. Op een markt die drie jaar geleden nog nauwelijks bestond, verdringen nu tal van aanbieders zich met tools die je helpen om 'compliant' te raken met AVG / GDPR. Maar over wat voor tools hebben we het dan bijvoorbeeld?

1. Tools die helpen om aan de administratieve verplichtingen van de AVG te voldoen (register, DPIA, inzage, datalekken, verwerkersovereenkomsten).
2. Tools die een beeld geven van de mate van 'compliance' en helpen bij verantwoording (balanced scorecards, risicomanagement en maatregelen).
3. Tools die helpen bij privacy by design (minimaliseren, verwijderen, versleutelen, toegangsbescherming, pseudonimiseren en anonimiseren).
4. Forensische tooling (wat voor gegevens bevinden zich in de infrastructuur en wat hebben hackers kunnen bereiken).

In 2018 is in de AVG-haast geïnvesteerd in privacy en in privacy tooling. Een jaar verder spreek ik veel organisaties die in de praktijk merken dat ze niet alles uit de tooling halen: het vullen is lastig, de tooling is te complex, of gebruikers vinden dat ze dubbel werk moeten doen. En door deze slechte ervaringen aarzelen veel andere organisaties voordat ze tooling aanschaffen… Wat zijn daarom de belangrijkste vragen die je moet stellen als je een (privacy) tool wilt kopen?

Vraag 1: wat zijn de functionele eisen aan de tool?

Dat is makkelijker gezegd dan gedaan, want je hebt vaak wel een verwachting van de uitkomst van de tool (`de heilige graal'), maar nog niet van het gebruik van de tool. Het is in dit geval mogelijk om voor jezelf 'use cases' of gebruiksscenario's te definiëren, of anders gezegd: hoe ben je van plan te gaan werken? Bijvoorbeeld bij een register van verwerkingen: wie zorgt voor de initiële vulling, wie gaat het straks bijhouden en hoe, hoe wil je de actualiteit en juistheid controleren, en hoe ziet het toezicht er uit? Pas als deze gebruiksscenario's duidelijk zijn, kun je bij een demo of kennismaking ook kijken of de tool bij jouw gebruiksscenario's past.

Vraag 2: in hoeverre kunnen we al gebruik maken van bestaande middelen?

Kijk in hoeverre al gebruik kan worden gemaakt van bestaande tools: het is veel makkelijker om taken te beleggen bij collega's als zij daarbij ook gebruik kunnen blijven maken van eigen tooling.

Stel: je krijgt per dag tientallen tot honderden vragen van klanten. Via telefoon, mail of web. Daar kan zo maar eens een inzageverzoek tussen zitten. Als er zoveel klantcontacten zijn, is er vaak ook een professionele werkwijze om klantvragen te categoriseren en af te handelen. Is het dan ook niet slimmer om te kijken of je ook inzageverzoeken via het reguliere klantcontactproces (en de bijbehorende tooling) te laten verlopen? Andere mogelijkheden zijn tools voor inkoop / contractmanagement (inpassen bewaking verwerkersovereenkomst) en tools voor de afdeling ICT (bijhouden incidenten en datalekken).

Vraag 3: wat vinden de beoogde gebruikers van de tool?

Vaak zie ik dat privacy officers en functionarissen voor gegevensbescherming (FG) een tool kopen. Voor hen is de AVG gesneden koek. Maar wat vinden gebruikers? Worden zij blij van wat ze zien? Snappen zij de termen en werkt de tool voor hen intuïtief? Als privacy officer of FG ben je misschien niet de beste om dat te bepalen, betrek daarom ook de mensen die worden geacht met de tool te werken. Want als de tool hen aanstaat, dan is de kans veel groter dat ze het gaan gebruiken. En daar heb je als privacy officer of FG uiteindelijk veel meer aan. Misschien is er wel een proefperiode mogelijk?

Vraag 4: is er hulp bij implementatie / nazorg om het maximale uit de tooling te halen?

Even generaliseren: leveranciers van privacy tools zijn niet goed in het advies er omheen. Hun businessmodel is ontworpen om aan de tool te verdienen en niet aan de implementatie. Maar vaak is steun bij de implementatie wel nodig: om alles uit de tool te halen, moet het niet alleen op de juiste manier worden geïmplementeerd, maar is er ook hulp nodig om de processen te ontwikkelen of een goede gebruikerstraining te geven. Hoe voorziet een tool leverancier hierin? Doet ze dat zelf, of heeft ze een implementatiepartner die je kunt bellen, ook nog een aantal maanden na de implementatie?

Vraag 5: wat doet de leverancier aan beheer en onderhoud?

En dan maar ook de andere kant generaliseren: adviesorganisaties zijn geen goede toolleveranciers. Zij verdienen hun geld aan advisering en niet aan beheer en onderhoud van tooling. Vraag is dan hoe snel en adequaat zij reageren op bugs en foutjes. Wat is de kalender voor doorontwikkeling van de tooling?

Samengevat: *baseer de keuze van de tooling niet zomaar op een demo of dat wat de buren doen. Stel deze vragen, zodat je een beter onderbouwde keuze maakt in privacy tooling.*

Kim Reijnen is freelance privacyrecht adviseur en CIPP/E gecertificeerd. Kim werkt voor Kim Reijnen, Legal Support & Training. Daarnaast is ze coördinator van het privacynieuws bij SDU. Kim is te bereiken via kim@kimreijnen.nl.

Blijf op de hoogte

Data kan niet volledig worden beschermd door alleen technische beveiligingsmaatregelen te nemen. De Algemene Verordening Gegevensbescherming (AVG) verplicht organisaties daarom ook organisatorische en administratieve maatregelen door te voeren. Echter, de AVG bevat veel open normen waardoor niet altijd even duidelijk is hoe de bepalingen uit de AVG moeten worden uitgelegd. De uitkristallisering en onderzoeken door de Autoriteit Persoonsgegevens (AP) zijn ook nog in volle gang. Willen organisaties AVG-proof zijn én blijven dan is het noodzakelijk om ook op de hoogte te zijn van de laatste en meest belangrijke ontwikkelingen. Daarom worden in dit artikel twee belangrijke onderwerpen met interessante ontwikkelingen op dat vlak behandeld.

‘De AVG bevat veel open normen waardoor niet duidelijk is hoe de bepalingen uit de AVG moeten worden uitgelegd’

Eén van de meest besproken verplichtingen uit de privacywetgeving is het sluiten van verwerkersovereenkomsten. Wanneer de verwerking geheel of gedeeltelijk wordt uitbesteed aan een derde partij, de verwerker, moet een overeenkomst gesloten worden. In de praktijk wordt snel aangenomen dat een ontvanger van persoonsgegevens een verwerker is en dat een verwerkersovereenkomst het verplichte middel is om afspraken in vast te leggen. Terwijl het ook mogelijk is dat de andere partij (mede)verantwoordelijk is voor de gegevensverwerking. In dat geval is een verwerkersovereenkomst niet het juiste middel. Daarom moet altijd eerst naar de onderlinge relatie worden gekeken voordat de overeenkomst wordt opgemaakt.

Analyse maken

De verwerkingsverantwoordelijke bepaalt het doel en de middelen. De verwerker verwerkt slechts in opdracht van de verwerkingsverantwoordelijke de persoonsgegevens voor dat doel. Bij het analyseren van het voorgaande, spelen de verantwoordelijkheden van partijen en de feitelijke invloed die partijen uitoefenen een belangrijke rol. Verder moet de opdracht die wordt gegeven gericht zijn op het verwerken van persoonsgegevens. Je gaat immers ook niet met de pakketbezorger een verwerkersovereenkomst afsluiten omdat de pakketbezorger de gegevens over de ontvanger krijgt. Dat gegevens in dit geval worden uitgewisseld, is slechts een voortvloeisel van de primaire opdracht.

Verkeerde kwalificatie

Een verkeerde kwalificatie komt ondanks bovenstaande handvatten vaak voor. Dit aangezien er situaties bestaan waarbij meerdere interpretaties mogelijk zijn en er organisaties zijn die deze analyse niet goed maken. Dit overkwam ook Uber. Uber B.V. (UBV) en Uber Technologies, Inc. (UTI) hebben in 2018 een boete opgelegd gekregen voor het overtreden van de meldplicht datalekken. Bij de beoordeling heeft de AP ook naar de rollen van partijen gekeken. Partijen waren zelf overeengekomen dat UBV verantwoordelijke is en UTI ten behoeve van UBV als verwerker optreedt. Ze hadden daarom een verwerkersovereenkomst gesloten. De AP was het hier niet mee eens en oordeelde dat de partijen als gezamenlijk verantwoordelijken zijn aan te merken. Dit aangezien UTI het privacybeleid en het informatiebeveiligingsbeleid (mede) had opgesteld, beslissingen had gemaakt over de opslag van de gegevens en de Uber-app door had ontwikkeld en aangeboden.

Kortom, partijen hadden hier een verkeerde kwalificatie gemaakt. Verder was dus hetgeen dat op papier stond niet leidend voor het vaststellen van de rollen. UTI bepaalde samen met UBV voor welk doel en met welke middelen de persoonsgegevens werden verwerkt. De feitelijke gedragingen zijn dus doorslaggevend voor de kwalificatie van de rollen.

Verstrekken van persoonsgegevens

Tussen verwerkingsverantwoordelijken en verwerkers en tussen verwerkingsverantwoordelijken onderling worden dus veel persoonsgegevens uitgewisseld (1). Echter, het verstrekken van persoonsgegevens is aan voorwaarden uit de AVG gebonden (2). De algemene regel is dat het verstrekken van persoonsgegevens alleen mag als het verenigbaar is met het doel waarvoor de gegevens zijn verzameld. Om te bepalen of het verenigbaar is met het oorspronkelijke doel, moet naar de concrete omstandigheden gekeken worden. Daarbij spelen verschillende factoren een rol, zoals de aard van de gegevens en de gevolgen van de verstrekking. Wanneer het niet verenigbaar is met het doel, mag het verstrekken als er toestemming wordt gegeven of als de gegevens nodig zijn voor een verwerking. Dit is mogelijk op basis van een unierechtelijke of lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in de AVG bedoelde doestelling van algemeen belang (specifieke wettelijke plicht). Naast het bovenstaande moet het doel ook altijd gerechtvaardigd zijn. Dit houdt in dat het doel gebaseerd moet zijn op één van de zes grondslagen uit de AVG. Ook moet worden gekeken naar de proportionaliteit en subsidiariteit. Verder moet de verwerkingsverant-

‘Jurisprudentie en alle verschillende publicaties van de AP gaan ook de aankomende periode erg waardevol zijn’

woordelijke die de gegevens ontvangt zelf ook een grondslag hebben om de gegevens te mogen verwerken.

Ontvanger zelf verantwoordelijk

Het lijkt dus vrij duidelijk hoe moet worden bepaald of gegevens mogen worden verstrekt of niet. Een duidelijk voorbeeld is die van de situatie waarbij iemand een reis boekt bij een reisbureau. Het reisbureau moet dan de gegevens doorgeven aan de vluchtmaatschappij, anders kan de overeenkomst met de boeker niet worden uitgevoerd.
Toch zullen er altijd grijze gebieden en verschillende interpretaties bestaan rondom de rechtmatigheid van de verstrekking. Voornamelijk in de situatie waarbij er afzonderlijke verwerkingsverantwoordelijken zijn die in principe niet samenwerken. Rechtspraak kan uitkomst bieden voor dit soort situaties. Van deze uitspraken kunnen wij dan leren waar rechters naar kijken bij hun beoordeling over de rechtmatigheid van de verstrekking. Dit kunnen wij weer toepassen in de praktijk.

Belangenafweging

Een recente uitspraak (3) gaat over een situatie die we net noemden. Daarbij was een belangenafweging noodzakelijk om te bepalen of gegevens verstrekt mochten worden. Dutch Filmworks (DFW) wilde namelijk gegevens inzien waarover Ziggo beschikt om mensen die illegaal een film gedownload zouden hebben een ‘downloadboete’ te geven. Aangezien Ziggo dit weigerde, stapte DFW naar de rechter.
De rechter heeft toen een belangenafweging gemaakt om te beoordelen of Ziggo de gegevens moest verstrekken. De rechter stelde voorop dat DFW belang heeft bij het verkrijgen van de gegevens. Dit aangezien het illegaal downloaden van een film verboden is en het daarbij aannemelijk is dat DFW recht heeft op een schadevergoeding als vastgesteld is dat een film illegaal gedownload is. Ook werd verwezen naar het besluit van de AP uit december 2017 waaruit bleek dat de voorgenomen verwerking van DFW rechtmatig is. De rechter stelde daarbij dat dit onder de AVG niet anders is. Verder haalde de rechter aan dat voor DFW geen minder ingrijpende manier bestaat om achter de gegevens te komen.
Echter, DFW had volgens de rechter onvoldoende duidelijk gemaakt hoe zij de gegevens wil gebruiken om de downloaders te benaderen. Daarnaast werd onvoldoende duidelijk of DFW de persoon achter de gegevens als de illegale downloader aanmerkt, omdat de IP-adreshouder niet diegene hoeft te zijn die de film daadwerkelijk heeft gedownload. Ook was het volgens de rechter niet duidelijk of DFW voldoende informatie aan de downloaders over hun rechten zal verstrekken. De rechter vond, gelet op het voorgaande, dat Ziggo de gegevens niet hoefde te verstrekken.

Hierbij moet opgemerkt worden dat het oordeel van de rechter dus anders zou kunnen zijn als DFW het bovenstaande wel duidelijk had kunnen maken. Wees dus altijd concreet in de onderbouwing van onder andere de noodzaak, gevolgen en omstandigheden van de gegevensverstrekking.

Blijf de rechtspraak en de AP volgen

Jurisprudentie en alle verschillende publicaties van de AP gaan ook de aankomende periode erg waardevol zijn. Het is daarom verstandig om op de hoogte te blijven en te anticiperen op de ontwikkelingen. En onthoud dat zelfs de rechtbank en de AP soms nog zoekende zijn.

Referenties

(1) Doorgifte naar buiten de EU wordt in dit artikel niet nader besproken.
(2) Art. 6 lid 4 AVG
(3) Rb. Midden-Nederland 08-02-2019, ECLI:NL:RBMNE:2019:423

Non-conflicted

Within the last 24 hours (as The Attributer writes this on 5th April 2019) the CEO of Boeing, Dennis Muilenburg, has publicly acknowledged that bad data feeding into an automated flight system on the company's popular 737 Max jets played a role in two recent crashes (1). 'With the release of the preliminary report of the Ethiopian Airlines flight 302 accident investigation it's apparent that in both flights the Maneuvering Characteristics Augmentation System, known as MCAS, activated in response to erroneous angle of attack information.' (2) We are beginning to see emergent properties of autonomous (and semi-autonomous) systems, including their human interfaces, that are causing major concerns over the resolution of conflicting requirements. In a much earlier incident, Air France flight 447 (an Airbus 330) crashed on 1st June 2009 over the Atlantic Ocean. In that case ice crystals built up on speed sensors and caused the auto-pilot to disconnect. That convinced the pilots to take erroneous action that led to a catastrophic aerodynamic stall of the aircraft. We might expect that this type of incident is one that will occur again as we roll out more and more autonomous systems for transportation and other industrial applications. It concerns the conflict that can occur between the humans and the technology, and how we resolve these cases in real time to save human lives. If the humans are given false (or fake) data, how should they handle that? How should they 'know' for certain that the data is false? To what extent should an autonomous system insist that it is a better decision maker than the humans? And to what extent should the human operator be considered as an effective backstop for a malfunctioning autonomous system. These are complex issues (3). Resolving design conflict is by no means new. We have had to deal with the need for heavily controlled access and ingress into buildings whilst at the same time making it easy for those inside to escape if the building is on fire. Special fire escape doors have been used, and yet in certain venues, often nightclubs, the management has chained up the escape doors to prevent people getting in through the back without paying. There are many recorded tragedies of hundreds dying in nightclub fires for this very reason. Human behaviour is the key issue; technology attempts to mitigate the worst threats to human life but the designers cannot foresee or forestall every type of future behaviour ... or can they? In an earlier Attributer blog article (Safe, April 2016) we discussed the synergy that exists in the approach taken in SABSA for security architecture and that taken in the safety engineering frameworks: STAMP (System-Theoretic Accident Model and Processes), CAST (Causal Analysis using Systems Theory), and STPA (System Theoretic Process Analysis) (4). These methods are from the team at the MIT Department of Aeronautics and Astronautics led by Dr Nancy Leveson.

The key differentiator between the MIT methods and traditional safety engineering approaches is the emphasis on hierarchical governance that modern thinking embraces. No longer is there a belief that an accident is caused by a linear chain of events, or even by the 'swiss cheese model' where all the 'holes' align. Yet already Mr Dennis Muilenburg has publicly asserted in his video statement that these accidents were caused by a 'chain of events'. No doubt that part of his statement will occupy safety analysts and lawyers for several years to come. Many industry experts are already pointing to poor governance, driven by competitive issues with respect to Airbus and the need to maintain profitability. Perhaps now is the time for The SABSA Institute to reach out again for some joint thinking and working with the MIT team. We are facing the prospect of safety engineering becoming more and more dependent on the quality of digital data feeds and therefore on the security of digital sub-systems. Autonomous piloting systems in all forms of transportation are becoming ubiquitous. Safety authorities in different sectors and jurisdictions are moving to a position that 'a system cannot be safe, if it is not secure'. Both schools of thought (STPA and SABSA) have major contributions to make towards a holistic architectural approach to the design of safety-critical digital systems of all types. What is not yet clear is exactly how to achieve the goals. Further research and development of ideas is needed to move forward. Here's another 'call to arms' from The SABSA Institute. We shall be pleased to hear from anyone interested in working on a joint project to look at these issues in autonomous systems. The Attributer suspects that we might find that designers are too focused upon the behaviour of the technology under stress and not sufficiently attentive to the vast array of possible human behaviours that might accompany technical malfunction. As a starting plan The Attributer suggests the creation of a taxonomy of scenarios including the detailed analysis of possible human interventions. That would give us some insight into the scale of the problem as it emerges in this fast-changing world of digital automation. Contact info@sabsa.org.

The Attributer

Referenties

(1) Lion Air flight 610 on 29th October 2018 and Ethiopian Airlines flight 302 on 10th March 2019

(2) www.boeing.com/commercial/737max/737-max-update.page#/message

(3) www.noop.nl/2008/08/simple-vs-complicated-vs-complex-vs-chaotic.html

(4) www.psas.scripts.mit.edu/home/wp-content/uploads/2016/01/Systems-Theoretic-Process-Analysis-STPA-John-Thomas.pdf

Tim Florack is mede-oprichter van Cubbibu en is actief als IT risk en privacy consultant. Tim geeft workshops en trainingen op het gebied van informatiebeveiliging en privacy, cybersecurity, privacy en IT GRC. Tim is te bereiken via tim.florack@cuccibu.nl.

AVG: pleidooi voor een alternatief stappenplan

Eind januari publiceerde Het Financieele Dagblad een artikel met de pakkende titel 'Angst voor privacywet AVG blijkt ongegrond' (1). Privacyexperts reppen over nieuwbakken consultants die vooral angst inboezemden. Deels terecht. Een andere benadering is dat bij het gros van de organisaties privacy, in het bijzonder de omgang met persoonsgegevens, nauwelijks op de agenda stond en er daarom veel behoefte was aan ondersteuning. De conclusie die in het artikel wordt getrokken, is dat de invoering van de AVG vooral voor een stijging in privacy-bewustzijn heeft gezorgd.

Hoewel daar zeker een kern van waarheid in zit, hoop ik dat bewustzijn niet de enige winst is. Dus rijzen de vragen: waar stonden organisaties voor de AVG en waar staan ze nu? En is er meer bereikt dan enkel bewustwording? Sinds 2011 ben ik actief in het vakgebied, vanuit een achtergrond in IT audit, IT risico management en informatiebeveiliging. In die eerste jaren kwam ik beperkt in aanraking met privacyvraagstukken. De Wet bescherming persoonsgegevens was van toepassing en slechts enkele klanten hadden processen ingericht die aan de eisen van deze wet voldeden. In 2016 kreeg privacy (of eigenlijk gegevensbescherming) in Nederland een eerste boost door de 'Meldplicht Datalekken'. Dit zorgde voor een stijging in het aantal privacy gerelateerde vragen, toen nog vooral gericht op het simpelweg opstellen van een procedure 'omgaan met datalekken'.

Stappenplan AVG

Door de komst van de AVG hebben 2017 en 2018 voor veel organisaties, en dus ook voor onze organisatie, in het teken van gegevensbescherming gestaan. Organisaties zijn druk bezig geweest met de implementatie van allerlei vereisten die uit de wet voortvloeiden. Vaak met als einddoel de implementatie van een bepaalde eis. Hiervoor zijn door allerlei instanties frameworks en stappenplannen aangeboden. Denk even terug aan het 10 stappenplan van de Autoriteit Persoonsgegevens (AP) om te kunnen voldoen aan de AVG (2) (zie hieronder).

In 10 stappen voorbereid op de AVG (Autoriteit Persoonsgegevens):

1. Bewustwording
2. Rechten van de betrokkenen
3. Overzicht verwerking
4. Data Protection Impact Assessments
5. Privacy by design/default
6. Functionaris voor de Gegevensbescherming
7. Meldplicht Datalekken
8. Verwerkersovereenkomsten
9. Leidende toezichthouder
10. Toestemming

Figuur 1 – Basisvereisten

Bewustwording

Stap 1 (bewustwording) zit wel goed, als we het FD mogen geloven. Bewustwording wordt door de AP omschreven als 'het op de hoogte stellen van relevante mensen over de wetgeving'. Bewustwording is cruciaal - dat vinden wij ook - maar wel in een iets bredere context die geborgd dient te worden in de organisatie - en welke periodiek wordt herhaald. Namelijk de context van mensen als belangrijkste schakel zien in de omgang met persoonsgegevens. Dit vereist een proces van continu informeren, opleiden en trainen. Iets dat ook de afgelopen twee jaar benoemd werd in de top 5 'Prioriteiten voor gemeenten in het IBD Dreigingsbeeld' (3) van de Informatiebeveiligingsdienst Gemeenten. Grappig detail is dat in dit stappenplan onder stap 1 ook wordt aangehaald dat de AP sancties kan opleggen. Toch niet enkel het 'legertje van honderden nieuwbakken AVG-consultants' die de angst bij organisaties zouden hebben aangewakkerd zoals in het FD artikel wordt gesuggereerd?

Afvinken checklisten

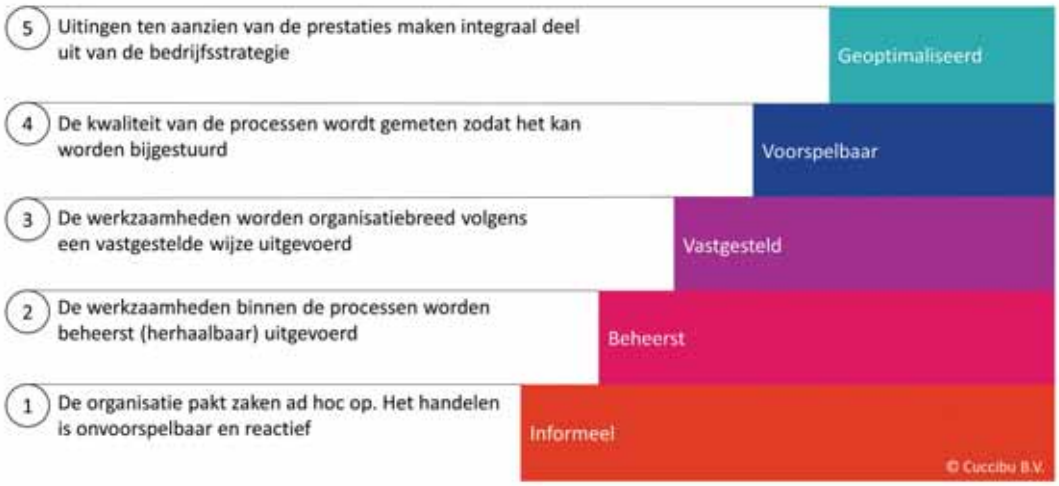
Kijkend naar de stappen 2, 3, 4, 7 en hoger geldt dat dit momenteel de papieren tijgers zijn geworden waar organisaties bang voor waren. Organisaties beschikken over ellenlange beslisbomen voor afhandeling van een datalek of een verzoek van een betrokkene, maar zodra een melding binnenkomt, start de improvisatie. Kortom, de procedure is geschreven, misschien zelfs formeel vastgesteld, maar is niet geborgd in de organisatie. Het punt dat ik hier wil maken, is dat dit een prima stappenplan is (of was) mits organisaties beseffen dat het geen eenmalige 'afvink' stappen zijn. Implementatie stopt niet bij het afvinken van een checklist met documenten.

Borging

Men heeft een privacybeleid geformuleerd (of gekopieerd), bepaalde rollen zijn belegd, procedures zijn beschreven en we hebben met z'n allen een aantal verwerkersovereenkomsten getekend. In veel van die gevallen was die overeenkomst niet nodig op basis van (gedeelde) verantwoordelijkheid, maar die formaliteit is afgevinkt (stap 8). Check! Toezicht op naleving van de overeenkomst? Nee, niet ingericht. Register volledig ingevuld? Check! Proces ingericht om proceseigenaren ook zelf de verantwoordelijkheid te laten voelen om het register actueel te houden. Nee, dat niet.

Kortom, borging in de organisatie van de processen blijft achter. Dit is niet gek, want borging van een proces lukt niet in een paar maanden of een jaar. Helaas is de aanpak in veel gevallen wel gericht geweest op het eenmalig optuigen van al deze formaliteiten en aan de borging daarvan is geen of te weinig aandacht besteed.

Eenzelfde situatie is ontstaan bij het inrichten van governance. Het aanstellen van een Functionaris



Figuur 2 – CIP privacy volwassenheidsniveau

Gegevensbescherming (stap 6) is door organisaties eenvoudig afgevinkt, maar als je het vraagstuk breder trekt, de verantwoordelijkheden van de FG of governance van privacy in een breder perspectief bekijkt, dan loopt het spaak. De vraag aan een FG op welke wijze deze het toezicht gaat houden, of daar een budget aan is gekoppeld, of een planning, wordt regelmatig weifelend beantwoord. Gevolgd door de opmerking dat de FG daar simpelweg nog niet aan toekomt, doordat deze allerlei operationele vragen moet beantwoorden, of - nog erger – door onvoldoende vrijgemaakte tijd. Begin 2019 was een iets rustigere periode na een ontzettende piek aan vragen getriggerd door de inwerkingtreding van de AVG. Dat lijkt te suggereren dat organisaties de inrichting van de AVG op orde hebben. Ik merk in ieder geval dat veel organisaties óf denken dat ze klaar zijn, óf nu de kat uit de boom kijken. De inrichting van AVG-formaliteiten (zie figuur 1) zijn afgevinkt: de basis 'is op orde'.

Hype

Dit strookt niet met het beeld dat ik hierboven schets en in verschillende organisaties zie terugkomen. Als we dan terugkijken op waarom organisaties in eerste instantie in beweging kwamen, waren dat of die mogelijke boetes of het willen nemen van verantwoordelijkheid voor de correcte omgang met persoonsgegevens. Als organisaties gemotiveerd werden door boetes in plaats van door het nemen van verantwoordelijkheid, zijn we dan nu in afwachting van die eerste (schokkende) boete? Of is privacy de 'hype' voorbij en is het nu wachten op ePrivacy of enige andere 'nieuwe' (nee, eigenlijk is ePrivacy ook niet nieuw) wet- en regelgeving? Pas als echt gekeken gaat worden naar de borging van de basisprincipes van de AVG (rechtmatigheid, behoorlijkheid, transparantie, doelbinding, gegevensminimalisatie, proportionaliteit enzovoort) kun je een uitspraak doen over het niveau van gegevensbescherming in een organisatie. In die zin is stap 5 de vreemde eend in de bijt van het AP-stappenplan. Privacy by design en privacy by default verwachten namelijk wel een absolute verankering in de organisatie. Je kunt deze principes niet afvinken als dat gedachtegoed niet tot in de diepste vezels van de medewerkers is doordrongen. Denk maar aan het advies van de Informatie Beveiliging Dienst met betrekking tot het 'versterken van de menselijke schakel' bij informatiebeveiliging.

Privacy Volwassenheidsmodel

Privacy by design is te vergelijken met een bepaalde mate van volwassenheid. Niet eenmalig een actie uitvoeren, maar continu en aantoonbaar werken volgens bepaalde normen en waarden. Volwassenheidsmodellen zijn van alle jaren en ook voor privacy zijn deze modellen beschikbaar. Het Centrum Informatiebeveiliging en Privacy heeft in 2017 het 'Privacy Volwassenheidsmodel' gepubliceerd (4). Een bruikbaar model om de volwassenheid van de organisatie rondom privacy te toetsen. In onderzoeken wordt dit model geplot op de algehele inrichting van privacy (en informatiebeveiliging) in de organisatie en daarnaast op de afzonderlijke formaliteiten zoals is weergegeven in figuur 2. Hiermee ontstaat een helder beeld van de verbeterpunten (lees: de afgevinkte formaliteiten die nog niet bekend en gekend zijn binnen de organisatie). Hoewel het een wat voorzichtige inschatting is,

'De noodzaak van een voortdurende verantwoorde omgang met persoonsgegevens'

denk ik dat de meeste organisaties zich nu ergens tussen niveau 1 en 2 bevinden. Dat is namelijk exact die plek waar organisaties zich bevinden die wel een procedure hebben, maar bij een brandje direct starten met blussen.

Waar zou privacy by design merkbaar zijn? Minimaal niveau 3, maar ook dan kun je nog niet spreken van 'in de vezels', zoals eerder aangehaald is. Bij niveau 4 is meer aannemelijk om écht te kunnen spreken van een volwassen privacy-organisatie. Hierboven haalde ik de angst voor papieren tijgers al aan en om in die metafoor te blijven: als volleerd dompteur hebben organisaties de afgelopen jaren de tijgers de berg van volwassenheid op gedirigeerd. Echter, door enkel stappen af te vinken zijn dezelfde dompteurs daarna weer rustig de berg af gaan lopen, zonder te kijken of de tijgers wel vastzitten. Kwestie van tijd voordat de tijgers dat ook in de gaten hebben en iedereen ineens heel hard de berg afholt.
Minder abstract: als je geen aandacht schenkt aan de borging van processen in de organisatie zal niveau 3 nooit bereikt worden. Sterker nog, het is aannemelijk dat het niveau zonder aandacht ook snel weer zal afnemen. Dit zou zonde zijn van al dat harde werk in de afgelopen jaren. Bewustwording was één van de belangrijkste winstpunten, maar zijn we voldoende bewust geraakt van de noodzaak van deze wet- en regelgeving? En de noodzaak van een voortdurende verantwoorde omgang met persoonsgegevens? Oftewel: de verankering van de principes uit de wetgeving in de organisatie.
Het lijkt alsof het stappenplan van de AP hier onvoldoende toe heeft bijgedragen. Daarom stel ik nu ook een alternatief 10 stappenplan voor. Of 10 aanbevelingen op een deel van de reeds bestaande stappen. Het maakt niet zoveel uit hoe het wordt omschreven, deze aanbevelingen zorgen gegarandeerd voor een borging van privacy en verdere groei van het volwassenheidsniveau.

1. Beschrijf rollen en verantwoordelijkheden in de omgang met (persoons)gegevens, formaliseer deze, definieer een overlegstructuur en bepaal plannen met bijhorende budgetten.
2. Richt een 'privacy en informatiebeveiligingswerkgroep' in met personen uit de organisatie om een breed draagvlak te creëren (privacy/informatiebeveiligingsambassadeurs).
3. Maak proceseigenaren verantwoordelijk voor de verwerking van (persoons)gegevens in hun processen om zo te voldoen aan de beginselen van de AVG.
4. Zorg voor een overzicht van alle processen en voer risicoanalyses (of DPIA's) uit om inzichtelijk te maken welke risico's aanwezig zijn rondom de verwerking van (persoons)gegevens.
5. Automatiseer maatregelen om op een effectieve en efficiënte wijze aan de beginselen van de wetgeving te voldoen.
6. Structureel toezicht door de Functionaris voor de Gegevensbescherming op basis van een vooraf gedefinieerd – en waar mogelijk gecommuniceerd – plan.
7. Maak concrete afspraken over de controle op de naleving van verwerkersovereenkomsten en maak die naleving een onderdeel van het plan van toezicht.
8. Definieer indicatoren van een correcte omgang met (persoons)gegevens, zoals het aantal (gemelde) datalekken, informatiebeveiligingsincidenten en verzoeken van betrokkenen.
9. Informeer betrokkenen over de dienstverlening en de daarbij horende verwerking van persoonsgegevens en meet die middels een organisatiebrede klanttevredenheidsmeting.
10. Maak de omgang met (persoons)gegevens de pijler van een voortdurend bewustwordingsprogramma.

Hierboven wordt het eerste gedeelte van het woord 'persoonsgegevens' steeds tussen haakjes gezet. Simpelweg omdat een verantwoorde omgang met gegevens niet ophoudt bij gegevens die herleidbaar zijn naar een persoon. Het gaat om informatieveiligheid in brede zin!

Referenties

(1) Het Financieele Dagblad, 31 januari 2019, 'Angst voor privacywet AVG blijkt ongegrond'.
(2) Autoriteit Persoonsgegevens, In 10 stappen voorbereid op de AVG
(3) Informatiebeveiligingsdienst Gemeenten, Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2019/2020
(4) Centrum Informatiebeveiliging Privacy - Privacy Volwassenheidsmodel, versie 3.0.9

Robert Metsemakers is als ervaren IT auditor en informatiebeveiligingsexpert beschikbaar voor security-advies en (algemene) schrijfopdrachten via robert.metsemakers@gmail.com.

Lia Koltyrina / Shutterstock.com

Met metadata alleen kom je al een heel eind

In een scène uit een niet-bestaande Nederlandse politieserie geef ik een voorbeeld hoe uit louter metadata over telefoonverkeer toch veel over de gespreksinhoud is af te leiden.

‘Metadata kan in combinatie met openbare data en historische metadata privacygevoelig zijn’

Commissaris van Dalen kwam de vergaderruimte binnen en riep: “Deksels!” Inspecteurs Smid en Pietersen keken elkaar aan: de ouwe was normaal gesproken korter en directer in zijn woordkeus bij tegenvallers. Dit kon alleen maar betekenen dat hij 'boven' bij Jurza of de korpsleiding formeel bot had gevangen en dat het tapverzoek op de telefoon van crimineel K. was afgewezen. “We mogen niet tappen, we krijgen alleen meta”, mopperde Van Dalen. Uit zijn houding en de minachting waarmee hij een USB-stick van zich afwierp, bleek dat hij niet precies wist wat meta was, maar dat de kwaliteit ervan uitermate teleurstellend zou zijn. De USB-stick schoof tollend over de gladde vergadertafel en kwam tot stilstand op de plek waar Cor Maassen had moeten zitten, als data-analist van de afdeling Opsporing.
Net toen Van Dalen wilde opstaan om te kijken waar Cor bleef, kwam deze binnen met in zijn linkerhand een mok hete koffie en Donna in zijn rechterhand. Donna was een 10 inch mini-laptop, volgestopt met intern geheugen, een bloedsnelle SSD en een 8 jaar oude, tragere processor. Maar omdat Cor dat ding altijd bij zich had, dacht hij toch 10 minuten sneller te zijn dan de collega’s die ‘nog even hun laptop moesten halen'. Of zelfs een hele nacht sneller ten opzichte van de collega’s die zeiden: “Shit, ik heb mijn laptop op bureau gelaten. Dan morgen maar.”
Cors ogen glinsterden toen hij de USB-stick zag liggen. Hij stopte het ding in zijn laptop en opende Excel. Cor werd, vanwege zijn voorkeur voor het gelijknamige bestandsuitwisselingsformaat, vaak ‘CSV’ genoemd. Terwijl Cor het bestand omvormde naar kolommen in de eerste tab van een eerder gemaakte spreadsheet, begon Van Dalen te tieren: “We mogen die hufter niet tappen en zijn familie al helemaal niet. Belt hij ook nog met een buitenlands nummer! Sinds de tarieven in heel Europa hetzelfde zijn, kan je net zo makkelijk met een buitenlands nummer in Nederland bellen. We hebben alleen metadata gekregen over de kinderen, daar heb je dus helemaal geen zak aan!”

“Nou”, zei Cor, die niet bekend stond om zijn gevoel voor politieke tact, “dat valt wel mee. Zijn het alleen de belgegevens van afgelopen maand en alleen die van de oudste dochter?”, vroeg hij op basis van wat hij op zijn scherm zag. Gebelde nummers, datum, tijdstip en gespreksduur stonden overzichtelijk in kolommen op de eerste tab van het spreadsheet.

Op de tweede tab waren dezelfde gegevens anders gerangschikt, op totale gespreksduur per gekozen nummer. Op een andere tab waren de nummers per datum gesorteerd en de vierde tap toonde een grafiek van de populaire beluren. Vooral 's avonds werd veel gebeld, van 22.00 tot 23:45 uur was er weinig verkeer en daarna nog één of twee korte gesprekken of WhatsAppjes, kort voor het slapen gaan.

“Bevestigend”, zei van Dalen, terwijl hij de tabel met nummers die vaak gebeld waren bekeek. Hij mopperde toen: “Wie heeft ze eergisteren zo lang gebeld? 70 minuten? Meer dan de meeste mensen in een maand bellen. Mijn hele abonnement is maar 60 minuten per maand.”
Inspecteur Smid vroeg Cor: “Heb je dat nummer al gepleurd?” Pleuren was de term op de afdeling voor het gebruik van PLEUR, een database die Cor had gebouwd op Donna. Alle telecomproviders in Nederland geven maandelijks hun klantbestand door, met telefoonnummer, naam, voornaam, geboortedatum, geslacht, adres en woonplaats van al hun klanten. Doordat Cor bij het inlezen alle records aanvulde met een date-stamp, had hij een historisch bestand opgebouwd in de 10 jaar dat deze informatiestroom bestond. Hij kon zien welke mobiele nummers een persoon op enig moment had of had gehad, op welke adressen die nummers geregistreerd waren en soms zelfs welke gebruikers na elkaar hetzelfde nummer hadden gehad.
Het systeem was niet honderd procent foutloos, want het bevatte alleen maandultimo’s. Ook klopt de omrekening van begincijfers van een mobiel nummer naar de telecomprovider niet altijd, doordat bellers via nummerportabiliteit hun nummer konden meenemen. Maar meestal was PLEUR een handig ‘reverse engineering’-tool.

Cor typte het telefoonnummer over in PLEUR en zei: "Andere achternaam, hetzelfde geboortejaar, andere woonplaats" en zocht die achternaam op Facebook op. Op een foto stonden twee vrouwen in uitgelaten stemming. Uit de Facebookpagina bleek dat ze beiden lid waren van hetzelfde studentendispuut. Op de foto droegen ze een trui met het dispuutslogo. Uit de historie van het gekozen nummer bleek dat beide nummers enkele jaren geleden op hetzelfde adres waren geregistreerd. "Een studievriendin, verhuisd naar andere stad", concludeerde hij.
Uit het rijtje nummers van de afgelopen maand bleek verder dat het nummer vrijwel dagelijks meerdere keren kort werd gebeld, maar nooit 70 minuten. "De meeste vrouwen bellen alleen zo lang met hun moeder", bromde van Dalen. "Die heeft ze óók gebeld", reageerde Cor, "en wel meteen erna." Ongeveer 10 minuten duurde dat gesprek. En daarna was er nóg een gesprek van enkele minuten, naar een nummer dat in de maand ervoor nog geen enkele keer gekozen was. Vreemd om rond 23:30 nog naar een wildvreemde te bellen.
Cor pleurde het nummer en zag dat het een man was, ongeveer 10 jaar ouder dan de dochter. Op LinkedIn zocht hij hem op. De dochter was met hem geconnect. Niet zo vreemd als zijn management-assistent. Opvallend was wel dat hun werkrelatie helemaal niet bleek uit de Facebookaccounts van beiden. Van Dalen maakte zich opeens zorgen. "Zien die lui dat jij hen zoekt op Facebook? Ik krijg zelf weleens een melding dat iemand mij heeft opgezocht." Cor schudde zijn krullen. Nee, want op Facebook was hij Olga en 18 jaar oud. "Ze delen hun relatie niet op Facebook, maar wel op LinkedIn", stelde hij droog vast en vervolgde: "Ik denk dat ze per abuis hem met haar privételefoon op zijn zakelijke nummer heeft gebeld en daarna meteen haar telefoon heeft uitgezet. Althans, er zijn geen gesprekken meer, tot de volgende ochtend 8:00 uur."
Inmiddels stonden de drie mannen over de schouders van Cor mee te kijken naar het minuscule beeldschermpje. Cor pleurde het nummer dat de volgende ochtend om 8:00 gebeld was. Het bleek een geboortebeperkingskliniek. "Misschien wil ze een spreekbeurt houden en zoekt ze informatie", grapte Smid op zijn sardonische wijze die niet altijd door iedereen meteen werd begrepen. Cor keek niet-begrijpend opzij en schudde zijn hoofd. "Nee, want het is niet het algemene informatienummer, ze belde de afsprakenlijn en meteen daarna weer haar moeder." De drie zessen in het nummer waren herkenbaar genoeg, daar was geen PLEUR meer voor nodig.

"Goed", zei inspecteur Cees Pietersen toen. "De zaak is voor mij helder. De oudste dochter van K. heeft, sinds ze daar ongeveer twee jaar geleden ging werken, een buitenechtelijke relatie met haar baas, die volgens zijn Facebook getrouwd is en al twee kinderen heeft. De dochter was zwanger van die vent, heeft uitgebreid besproken met haar BFF wat dit zou betekenen voor haar leven en carrière en nog belangrijker: wat haar pa, die wij allemaal kennen, ervan zou vinden. Daarna heeft ze haar moeder gebeld of die haar naar de abortuskliniek kan brengen en na de ingreep weer kan terugrijden. Toen dat geregeld was, heeft ze die zak gebeld en het telefonisch uitgemaakt. Definitief, want ze heeft daarna de telefoon compleet uitgezet. Ze is in elk geval goed over de emmer, want per ongeluk heeft ze zijn zakelijke nummer gebeld in plaats van zijn privénummer. En ze belden altijd privé om het geheim te houden."
Rudi Smid plaatste een foute grap. "Van 22:00 tot 23:45 belden ze nooit, dan wipte hij zeker eventjes langs?" Niemand lachte. Ondertussen pleurde Cor een ander veel gekozen nummer uit de lijst en dit bleek inderdaad op naam van de man te staan. Volgens de begincijfers was het een kleine provider, dus waarschijnlijk was het een privénummer, want organisaties in Nederland gebruiken zakelijk meestal één van de grotere providers.
"Gisteren ging ze met haar moeder naar die kliniek. Dat verklaart dat het toestel de hele dag uit stond." Cor beaamde dat dit logisch klonk en suggereerde: "We kunnen meer metadata opvragen, want providers weten ook bij welke GSM-paal die telefoonnummers waren tijdens het gesprek. Dan kunnen we via triangulatie helemaal zeker pinpointen waar ze waren."

Maar voor commissaris Van Dalen was het al genoeg. "Kom Pietersen, dan gaan we bij K. langs. Eens kijken hoe hij reageert als hij hoort dat hij toch geen opa wordt. Misschien gaat hij stuk. En anders gaat hij mogelijk zelf op hoge poten naar die manager. Dan laten we een AT hem bij dat adres oppakken voor een 'geweldje'. Zien we wel of hij na een dagje binnen bij ons toch begint te zingen."
Terwijl het duo gehaast naar buiten liep, zei Smid tegen Cor: "Nu een bakkie echte pleur. En eigenlijk niet zo erg dat we vanwege de AVG geen tapvergunning kregen. Met een beetje metadata en jouw aanvullend historisch inzicht kom je als agent ook een heel eind. Meten is weten, maar met ongeveer bereik je méér." Lachend klapte Cor Donna dicht (na het saven van de spreadsheet) en ze kuierden naar de koffieautomaat.

TSTC

ICT en Security Trainingen

Want security start bij mensen!!

Next Generation Cybersecurity Training

TSTC is een gerenommeerd IT opleidingsinstituut en erkend specialist in informatie beveiliging-, cybersecurity en privacy trainingen.

Top 10 Security trainingen

CEH • OSCP • CCSP • CCFP • CISSP • C|CISO • CRISC
Privacy CIPP/E-CIPM • CISM • ISO 27001/27005/31000

Nieuw in 2019

- Extreme Hacking NextGen tm
- Cybersecurity Compliance Officer
- Cybersecurity Specialist
- Certified Chief Innovation Officer
- Red team vs Blue team

Recognition for Best ATC's and CEI's

TSTC Accredited Training Center of the Year 2017

Circle of Excellence Instructor 2017

www.tstc.nl

Simone Fennell is privacy-adviseur van de Gemeente Tilburg en privacytrainer bij Privacy Company. Zij schreef deze bijdrage op persoonlijke titel. Simone is bereikbaar via LinkedIn: www.linkedin.com/in/simonefennell/

Waarom een privacy-adviseur geen functionaris gegevensbescherming is

...én dat ook niet moet willen zijn

"Ah, dus jij bent de FG?" Men kijkt vreemd op als ik zeg dat ik dat niet ben, en nóg vreemder als ik aangeef dat (althans nu) ook niet te willen zijn. Door een veelvoud aan privacyberoepstitels, waarvan de één nog exotischer is dan de ander, wordt het er in ieder geval niet duidelijker op wat iemand doet.

Zomaar even een greep uit de gevoerde titels: functionaris gegevensbescherming (FG), data protection officer, privacy officer, privacy-adviseur, buddy, champion, accenthouder, coördinator, analist, beheerder, consulent en linking pin. Daarnaast hebben we ook nog een handjevol mensen die kennelijk de eindbaas van het geheel zijn door voor- of achtervoegsels als directeur of chief. Wat mensen dan precies doen? Ik heb geen idee.

Ik ben adviseur, dus ik geef advies

Ik weet gelukkig wel wat ik zelf doe. Ik ben adviseur, dus ik geef advies. Ik ben vooral bezig met de gegevensverwerkingsprocessen zelf. Daarbij richt ik me op de vraag hoe iets mogelijk gemaakt kan worden binnen de kaders die mijn organisatie kent. Ik kijk daarbij breder dan het recht. Als adviseur mag ik meedenken over alle zaken die privacy op één of andere manier raken. Onderwerpen als gegevensmanagement, informatiebeveiliging, procesmanagement en ethiek komen ook aan bod bij het geven van privacy-advies. Bijkomend voordeel is dat ik daardoor zelf voortdurend moet leren. Het gaat dus niet zozeer over de vraag of iets mag, maar over de vraag hoe we iets samen mogelijk kunnen maken.

Doordat adviseurs breder kijken dan alleen het recht, is het ook te verklaren waarom veel privacy-adviseurs van huis uit geen jurist zijn. Zij hebben kennis en kunde uit een ander relevant vakgebied. Het is echter wel belangrijk dat een goede kennis van het recht aanwezig is. Al is het maar om de soms ingewikkelde materiewetten te kunnen doorgronden en de onderlinge relatie te kunnen begrijpen. Adviezen hebben immers altijd een juridische component. Adviseurs hebben daarmee zoveel vaardigheden nodig, dat je verwacht dat het schapen met vijf poten zijn (1).

De adviseur zit dichter tegen de werkvloer aan en moet creatief zijn in het verzinnen van oplossingen

Ik houd geen toezicht

Een privacy-adviseur is geen FG, en andersom ook niet. De FG is in een aantal gevallen een bij wet verplichte toezichthoudersfunctie. De adviseur wordt niet genoemd in de wet. Wel wordt gesproken over 'advies' door de FG over gegevensverwerkingsprocessen. Wat mij betreft moet dit uitsluitend in het licht van de toezichthoudende taak gelezen worden. Dat maakt mijn rol als adviseur fundamenteel anders dan die van de FG.

De FG richt zich op effectief toezicht en zal zijn of haar best doen om risico's voor de betrokkene te identificeren en over te brengen aan degene aan wie hij/zij rapporteert. Dit vereist andere vaardigheden dan adviseren. De adviseur zit dichter tegen de werkvloer aan en moet creatief zijn in het verzinnen van oplossingen, soms streng zijn, maar altijd met het oog op de belangen van de betrokkene. Door in gezamenlijkheid met de werkvloer tot oplossingen te komen ben je als adviseur misschien ook wat toegankelijker dan een FG. Vanuit de samenwerking ontstaat (vaak) een kentering in de eigen organisatie. Men gaat beter nadenken over het gebruik van gegevens die er al zijn, wat de kwaliteit is, maar ook wat de effecten zijn van de activiteiten die we doen. Dat is een heel bijzonder onderdeel van het adviseurschap, omdat je daarmee, meer dan de FG, een spin in het web bent. Een adviseur moet misschien dus nog wel veel meer dan een FG een spin in het web zijn. Een soort van liaison tussen de werkvloer en de buitenwereld. Voor mij is het juist zo fijn dat er een FG naast mij staat die kan escaleren. Een advies kun je tenslotte ook in de wind slaan. Dat komt overigens maar zelden voor, omdat dingen vaak best kunnen, maar op een andere manier. Het is mijn taak om de business daarvan te overtuigen.

Ik ben onderdeel van een kudde

Ik mag mezelf gelukkig prijzen dat ik in een privacyteam werk en een fantastische FG naast me heb staan. Ik schrijf hier bewust het woord naast. We staan niet tegenover elkaar, al houdt de FG uiteindelijk ook toezicht op wat ik doe. Samen zorgen we voor de behartiging van de belangen van de burger.

Referenties

(1) https://www.privacycompany.eu/privacy-professionals-blog/

Lynsey Dubbeld is freelance communicatieadviseur, contentstrateeg, trendanalist en copywriter. Ze is gespecialiseerd in de thema's privacy, security en duurzaamheid. Dit artikel kwam tot stand in samenspraak met en in opdracht van Thomas Moons. Voor vragen zijn zij bereikbaar via: t.moons@iir.nl.

Ontwikkelingen in dataprotectie en het vak van privacy officer

De grondslagen van het privacyrecht zoals we dat nu kennen, dateren van de late jaren negentig, toen de Europese Dataprotectie Richtlijn werd ontwikkeld. Parallel aan de evolutie van de privacywetgeving heeft ook de functie van privacy officer de afgelopen decennia een sterke ontwikkeling doorgemaakt. Drie visies op het vak van de privacy officer, toen en nu.

Het is al bijna 25 jaar geleden dat de Europese Dataprotectie Richtlijn van kracht werd. De invoering van de Kaderwet in 1995 staat bekend als een cruciaal moment in de ontwikkeling van het hedendaagse privacyrecht. Inmiddels is met de komst van de General Data Protection Regulation (GDPR) een nieuwe mijlpaal bereikt. De Nederlandse vertaling van de richtlijn, de Algemene Verordening Gegevensbescherming (AVG), bouwt voort op het fundament van de Europese Dataprotectie Richtlijn, maar legt tegelijkertijd meer dan ooit de nadruk op de verantwoordelijkheid van organisaties om aantoonbaar in control te zijn.

Functionaris voor de gegevensbescherming

De AVG heeft het vak en werkterrein van privacy officers en data protection officers een enorme impuls gegeven. Een groter aantal organisaties dan voorheen is verplicht een functionaris voor de gegevensbescherming (FG) aan te stellen. Daarnaast heeft de uitgebreide media-aandacht voor de AVG - en de dreiging van forse sancties van de toezichthouder, de Autoriteit Persoonsgegevens (AP) - het thema privacy stevig op de agenda gezet. Steeds meer organisaties investeren in specialistische kennis en kunde op het vlak van dataprotectie en AVG-compliance. Bijvoorbeeld door een functie van privacy officer te creëren, of vrijwillig een FG aan te stellen.

Aan de basis van de hedendaagse beroepspraktijk van privacy professionals ligt de actuele wet- en regelgeving, waaronder de AVG en de toekomstige ePrivacy Verordening. De basisbeginselen en normen hiervan kennen veel overeenkomsten met de Europese Dataprotectie Richtlijn en de privacyprincipes van de OECD uit de jaren tachtig. Het vak van privacy officer is sinds die tijd sterk veranderd. Welke ontwikkelingen hebben zich in de beroepspraktijk voorgedaan en hoe ziet het vak er nu en straks uit?

Huib Gardeniers

Huib Gardeniers is partner bij Net2Legal Consultants en docent Certified Data Protection Officer (IIR-opleiding CDPO). Hij houdt zich al sinds 1990 bezig met privacyvraagstukken: eerst bij de Registratiekamer (de voorganger van de AP) en bij FENIT (het huidige Nederland ICT), en vanaf 2000 als consultant.

"Ik zie door de jaren heen echt een stijgende lijn als het gaat om de aandacht voor het thema dataprotectie en de functie van privacy officer. Privacy is voor veel organisaties een serieus onderwerp van gesprek en een volwassen onderdeel van de bedrijfsvoering, het beleid en het risicomanagement geworden. Er is ook meer bereidheid om mensen en middelen ter beschikking te stellen om als organisatie in control te zijn op het vlak van dataprotectie."

"Voorheen was dataprotectie vooral een speeltje van juristen. Het vak had ook een hoog theoretisch gehalte. Het onderwerp nodigde ook niet uit om ermee in de praktijk aan de slag te gaan. Nu wordt dataprotectie juist heel praktisch ingestoken, bijvoorbeeld vanuit de informatiebeveiliging en risk & compliance."

"Als privacy officer of FG moet je in teamverband werken en jezelf niet aan het einde van de gang laten zetten. Je moet eigenlijk een soort diplomaat zijn die middenin het primaire proces van de organisatie staat. Mensen moeten je echt weten te vinden, zodat je de juiste informatie krijgt om toezicht uit te oefenen, samen te werken met collega's en afspraken te maken met andere betrokken afdelingen, zoals compliance. De laatste jaren zie ik gelukkig dat steeds meer organisatieafdelingen zich met dataprotectie bezighouden en daarop ook actief monitoren en controleren."

"De toelichting van de EDPS geeft enige uitleg over de kennis en vaardigheden die essentieel zijn voor de FG-functie. Het komt erop neer dat de FG een schaap met vijf poten is. De EDPS besteedt overigens geen aandacht aan de werkervaring waarover data protection officers moeten beschikken. Ik denk dat je wel vier tot vijf jaar in het vak moet hebben meegelopen om een goed beeld te hebben van de veelzijdigheid van het onderwerp."

Rien van Zuijlen

Rien van Zuijlen is FG bij Noordwest Ziekenhuisgroep. Hij werkt sinds 1981 bij het ziekenhuis in de kop van Noord-Holland, eerst als privacy officer en sinds 2017 als FG.

"Niemand maakte zich erg druk over de naleving van de Wet bescherming persoonsgegevens (Wbp). Pas met de komst van de meldplicht datalekken, die sinds 2016 geldt, begonnen veel organisaties zich serieus zorgen te maken over de naleving."

‘Organisaties die denken dat je met een privacy officer zonder budget een heel conglomeraat AVG-ready kan maken’

"Voorheen speelde privacy bij ons vooral binnen de muren van het ziekenhuis. Het ging bijvoorbeeld over de omgang met patiënten die een kamer delen, en de afscherming van gesprekken die worden gevoerd bij de balie. Nu is het vak van de FG vrijwel volledig verschoven naar het management van data die over de grenzen van ziekenhuizen heengaan. Het vak van privacy officer is daarmee gecompliceerder en uitdagender geworden, en de blik is meer gericht op de buitenwereld."

"Het werk van de FG is naar mijn idee alleen maar leuker en spannender geworden. Je werkt bijvoorbeeld veel meer in teamverband. Binnen de organisatie overleggen we regelmatig met de vijf personen van onze privacycommissie over actuele zaken op het snijvlak van privacy en informatiebeveiliging.”

"Ons privacyteam zit bepaald niet verstopt in een kamertje achteraf: we zijn veel op de werkvloer en denken actief mee over nieuwe ontwikkelingen. Als privacyteam staan we voor goede zorg binnen de kaders van de privacywetgeving. Collega's beseffen daardoor in toenemende mate dat dataprotectie echt een voordeel kan zijn, ook voor bijvoorbeeld de nieuwe plannen van zorgprofessionals en ICT-dienstverleners. Door de FG al vroegtijdig aan te haken, is privacy geen remmende kracht, maar juist een slimme strategie die voorkomt dat een project in de uitvoeringsfase stagneert."

Rachel Marbus

Rachel Marbus is sinds 2016 FG bij KPN. Ze startte haar loopbaan in 2004 als onderzoeker aan de Tilburg University en werkte vanaf 2007 als consultant op het vlak van privacy en security. Tot voor kort was ze privacy officer bij de NS.

"Een aantal decennia geleden was dataprotectie vooral een academisch feestje, dat sterk werd gedreven door het werk van wetenschappers. Pas later kwamen er mensen die er in de praktijk mee aan de slag gingen. Langzamerhand zag je in organisaties mensen verschijnen die iets moesten doen met privacy. Het optreden van de toezichthouder en de risico's van nieuwe technologie creëerden een sense of urgency. Maar de functie van privacy officer moest toen nog wel helemaal uitgevonden worden."

"Het bestaansrecht van privacy officers hoeft nu eigenlijk niet meer te worden bevochten. Sterker nog: privacy is sinds de AVG een gigantische hype. Dat heeft niet altijd geleid tot een goed beeld van het vak van data protection officer. Er zijn organisaties die denken dat je met een privacy officer zonder budget een heel conglomeraat AVG-ready kan maken."

"Een FG moet over voldoende professionaliteit beschikken om onafhankelijk toezicht te kunnen houden. Omdat de functie van een data protection officer voor veel organisaties nieuw is, weten collega's niet altijd wat het takenpakket inhoudt. Het is logisch dat collega's het lastig vinden als ze iets niet kunnen doen vanwege de privacywetgeving. Ik benadruk dan dat we allemaal op aarde zijn om het bedrijf verder te helpen. Dat kan uiteraard ook als je goed let op privacy en security."

"De ideale FG of privacy officer bestaat niet - dat is een unicorn. Excellente vakkennis is een vanzelfsprekende basis. Je moet als FG in ieder geval niet bang zijn om autonoom te werken - en ook een beetje lef en een rechte rug hebben. Een multidisciplinaire achtergrond is een pre. Het helpt bijvoorbeeld als je naast een juridische opleiding ook een andere discipline beheerst, zoals informatiebeveiliging. Maar je moet vooral ook goed kunnen communiceren met verschillende doelgroepen, van de CEO tot de receptioniste."

Namens het bestuur en de redactieraad overhandigt Tom Bakker de eerste prijs aan winnaar Rob van Os.

Artikel van het Jaar 2018

Ook dit jaar heeft de jury weer een aantal interessante en leesbare artikelen mogen beoordelen. De onderwerpen betroffen de factor gedrag en cyberveiligheid, risicoanalyse door middel van scenario's, en een aantal artikelen over technische aspecten die het al dan niet lastig maken om cyberveilig te werken. Al met al een mooie compilatie van hedendaagse onderwerpen die momenteel de agenda bepalen.

De artikelen zijn beoordeeld op de volgende aspecten:

- Is de opzet logisch en passend bij het onderwerp?
- Is het artikel prettig leesbaar (toegankelijkheid)?
- Wordt er een duidelijke doelgroep bediend?
- Is het vernieuwend?
- Zet het artikel aan tot denken over de eigen IB-situatie?
- Geeft het artikel concrete handvatten om een probleem aan te pakken?
- Is het artikel inhoudelijk correct?

De jury heeft het artikel 'MagGMa: a framework and tool for use case management' van Rob van Os e.a. tot winnaar verkozen. Een bijzonder goed leesbaar artikel en door het beschikbaar gestelde gereedschap onmiddellijk toepasbaar voor de IB-professional die zich bezighoudt met security operations, en de monitoring van cyberdreigingen.

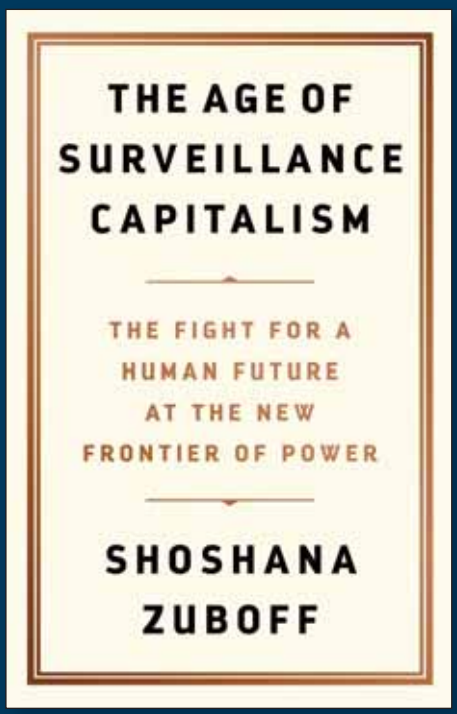
De tweede plek is voor 'Metadata, een onbekend risico' van Wiebe en Auke Zwaan. Een bondig en zeer leesbaar artikel over een onderwerp dat eenvoudig over het hoofd gezien kan worden. Niettemin een potentieel probleem dat aandacht verdient. Na lezing van dit artikel was de jury ervan overtuigd dat dit probleem met spoed moet worden aangepakt. De jury had graag concrete handvatten willen hebben om dit probleem aan te kunnen pakken.

De derde plek is voor 'Catching and Insider spy' van Vincent de Vries. Een spannend artikel over het probleem van de werknemer of partner die zich tegen het eigen bedrijf keert. Lijkt het in eerste instantie daarover te gaan, maar bij nadere bestudering blijkt het vooral een organisatorisch probleem te zijn. De aanpak hiervan is gelegen in preventieve maatregelen. Het is wel de moeite waard om eens te analyseren of de Nederlandse situatie ook zo ernstig is als de Angelsaksische.

De jury was dit jaar gecharmeerd van de kwaliteit van de artikelen over de gehele linie en kijkt vol verwachting uit naar de productie volgend jaar!

Namens de jury,
Ellen Wesselingh (HAN University of Applied Sciences)

Niels Huijbregts waakt als functionaris gegevensbescherming over de privacy van klanten en medewerkers van XS4ALL. Niels is bereikbaar via nielsh@xs4all.net en linkedin.com/in/nielshuijbregts/



Titel: The age of surveillance capitalism - The fight for a human future at the new frontier of power
Auteur: Shoshana Zuboff
Uitgegeven in het Engels door Profile Books, London
ISBN: 9781781256848

The age of surveillance capitalism

The fight for a human future at the new frontier of power

Hoewel Shoshana Zuboff veel voorbeelden beschrijft die ik niet voor het eerst tegenkom, heb ik na het lezen van The age of surveillance capitalism een snerpend alarm in mijn achterhoofd dat maar niet uit wil. Dat privacy in onze tijd onder hoogspanning staat, is geen nieuws. In het gedigitaliseerde leven is alles erop gericht alsmaar meer informatie over ons te verzamelen. Maar in Zuboffs surveillance capitalism is het nog veel erger dan we al dachten.

Het begon zo mooi. Toen het internet in de jaren 90 van de vorige eeuw razendsnel populair werd bij een wereldwijd publiek, was de sfeer uiterst positief. Hoopvol zelfs. Het internet werd geroemd om z'n vrijheid en z'n democratiserende kracht. Er was geen twijfel mogelijk: dit was het begin van een nieuw tijdperk waarin alles beter zou worden. De startups van die jaren barstten van het idealisme.

Google stelde zichzelf de nobele taak de exponentieel groeiende berg informatie die het internet was voor iedereen toegankelijk en bruikbaar te maken. Slim bedachte algoritmes brachten niet alleen alle websites in kaart, maar ook de voorkeuren, zoekpatronen, locaties en een heleboel andere kenmerken van de gebruikers van de zoekmachine. Die informatie werd aanvankelijk gezien als bijvangst, nuttig om de zoekresultaten te verbeteren, maar verder van weinig betekenis. Maar toen in 2001 de internetbubbel barstte en de beurskoersen kelderden, moesten bedrijven als Google opeens laten zien hoe ze echt geld konden verdienen. Het verkopen van advertenties werd het leidende model op internet en het duurde niet lang of het bijproduct was het hoofdproduct geworden: de gegevens over gedrag en voorkeuren van gebruikers werden de meest waardevolle assets van de internetbedrijven.

Daarmee begon een nieuw economisch paradigma, dat Zuboff het 'surveillance kapitalisme' noemt. Daarin zijn mensen niet primair de consumenten van producten en diensten, maar de leveranciers van grondstoffen. Om advertenties zo effectief mogelijk te maken zijn niet de wensen en behoeftes van mensen het belangrijkst, maar het voorspellen van hun gedrag, zegt ze. En hoe mooi de ronkende beloften van de techreuzen ook zijn - vrijheid, gelijkheid, democratisering, universele toegang tot informatie - ze werden ingehaald en uitgehold door de eisen van de markteconomie. Om bestaansrecht te houden moet Google steeds meer informatie verzamelen - en ons als dataleveranciers dus steeds intensiever in de gaten houden - om steeds accuratere voorspellingen te doen. Een ontwikke-

ling die leidt tot onstuitbare datahonger en uiteindelijk tot de wens ons gedrag te beïnvloeden. Dat heeft er bijvoorbeeld toe geleid dat Facebook gedetailleerd de psychische gesteldheid van haar gebruikers in kaart probeert te brengen om ze informatie te kunnen voorschotelen op het precieze moment dat ze daar het meest vatbaar voor zijn.

Zuboff vergelijkt de grootmachten van het surveillance kapitalisme met die van de industriële revolutie. En hoewel Facebook en Google niet direct het beeld oproepen van gore fabrieken en uitbuiting van arbeiders, maken ze zich wel degelijk schuldig aan uitbuiting, vindt de schrijfster:

'Ons gedrag wordt geëxploiteerd, en onze menselijkheid, ons lichaam, ons brein en ons hart worden achteloos weggeworpen. Net als bij de weerzinwekkende jacht op olifanten voor hun ivoor. Iedereen kent inmiddels het cliché 'if it's free, you're not the customer, you are the product' maar vergeet dat maar. Je bent niet het product. Je bent het achtergebleven karkas.'

Die dramatische houding zal sommige lezers misschien met de ogen doen rollen. Maar in de jacht op onze data zijn de oneerlijke machtsverhoudingen tussen bedrijven en mensen wel degelijk te vergelijken met die van jager en prooi. We zitten gevangen in de netten van bedrijven die inmiddels in alle aspecten van ons leven zijn binnengedrongen: in onze computers en telefoons, onze auto's en televisies, onze kantoren en scholen, in onze slaapkamers, en zelfs in het speelgoed van onze kinderen. Overal wordt ons gedrag gedetailleerd in kaart gebracht en in modellen gegoten die vervolgens voorspellingen doen over toekomstig gedrag. En op al die plekken waar we interacteren met onze smart, connected devices, wordt de realiteit die we om ons heen ervaren, en de keuzes die we daarin krijgen voorgeschoteld, beïnvloed door de uitkomsten van die algoritmes. Zo verzamelen ze niet alleen data, maar beïnvloeden ze actief onze levens door ongemerkt ons gedrag te sturen.

De informatie waarop we ons baseren als we een huis kopen, een school zoeken voor onze kinderen, ons informeren over standpunten van politieke partijen tijdens de verkiezingen, al die informatie wordt toegespitst op algoritmische modellen van onze voorkeuren en gedrag. En doordat de algoritmes bepalen welke informatie we te zien krijgen, kunnen ze ook beïnvloeden welke keuzes we maken. Zo ondermijnt het surveillance kapitalisme de vrije democratie en de vrije wil.

Alles met ons medeweten en toestemming natuurlijk. U heeft immers op 'OK' geklikt. Maar wie - zoals ik - bewust besluit alle privacyverklaringen, fair use policies en terms of service voortaan braaf te gaan lezen, komt er al snel achter dat dat gewoon niet kan. Een eindeloze stroom juridische documenten wordt opzettelijk zo vaag en ingewikkeld mogelijk gemaakt om er maar voor te zorgen dat we ze ongelezen accorderen. Die zogenaamd vrijwillig gegeven toestemming voor het gebruik van onze gegevens stelt niets voor: niet alleen willen we al die teksten niet lezen omdat ze saai en ingewikkeld zijn, de hoeveelheid alleen al maakt het praktisch onmogelijk, laat Zuboff zien.

En bijna iedereen lijkt zich daarbij te hebben neergelegd. Privacyvoorvechters blijven waarschuwen voor de macht van Google en Facebook. Maar dat die bedrijven alles van ons weten is voor veel mensen gewoon een gegeven. De waarschuwing komt daardoor niet meer aan. Mensen willen immers maar al te graag informatie over zichzelf ruilen voor gemakkelijke interfaces, gepersonaliseerde informatie, toegang tot vrienden en nieuwtjes. Dat dat gevolgen heeft voor hun privacy hebben ze vaak genoeg gehoord, en ze vinden het wel prima. Ze hebben immers niks te verbergen. Zuboff verschuift de discussie van privacy naar autonomie: het gaat er niet zozeer om dat die bedrijven alles van ons weten en het gaat er niet om of we iets te verbergen hebben. Waar het om gaat is het vermogen om zelf keuzes te maken, zelf te kunnen beschikken over onze toekomst. Dat vermogen is ondermijnd door de data-industrie die niet alleen alle data over ons leven verzamelt, maar ons leven actief beïnvloedt met speciaal geselecteerde informatie en subtiele gedragsbeïnvloedingstechnieken. Zo subtiel is die gedragsbeïnvloeding trouwens niet altijd: in het hoofdstuk 'Make them dance' beschrijft Zuboff prachtig hoe Facebook invloed uitoefent op het opkomstpercentage bij verkiezingen, en hoe Pokemon Go wereldwijd horden mensen de straat op krijgt.

De bezorgdheid die Zuboff in haar quote over de achtergebleven karkassen uitspreekt over onze menselijkheid, lijkt wel eens te wringen met haar harde kapitalistische opstelling in andere delen van het boek. Aanvankelijk las ik veel van de problemen die zij beschrijft als aanklachten tegen het kapitalisme in het algemeen. Maar dat bleek een misvatting - misschien ingegeven door mijn Europese blik. Zuboff protesteert geenszins tegen het kapitalistische systeem, maar tegen de disruptie ervan: het surveillance kapitalisme breekt fundamenteel met de Amerikaanse traditie van het marktkapitalisme. Dat is immers gebaseerd op de vrije markt, waarin consumenten op basis van vrije wil, vrije keuzes maken. En die breuk, vindt Zuboff, is kwalijk. Voor het economische systeem, de democratische rechtsstaat en voor ons als mensen.

The age of surveillance capitalism is met 535 pagina's en ruim 100 pagina's noten en verwijzingen behoorlijk stevige kost. Maar door Zuboffs puntige stijl, aansprekende voorbeelden en heldere inzichten leest het boek als een trein. Van harte aanbevolen.

Romy ter Beek is werkzaam bij Considerati. Romy is bereikbaar via terbeek@considerati.com

Bart Schermer is chief knowledge officer bij Considerati. Bart is bereikbaar via schermer@considerati.com

Inzet van gedrags-herkenning door autoverzekeraars

Wat is de oorzaak van een auto-ongeluk en wie kan hiervoor aansprakelijk worden gesteld? In veel gevallen is dit niet gelijk duidelijk. Data kan een belangrijke rol spelen bij het achterhalen van de toedracht van een ongeluk. Het Verbond van Verzekeraars heeft ook aangegeven vóór het verzamelen van data te zijn om ongelukken te reconstrueren. Veel autofabrikanten verzamelen nu al data over het rijgedrag van automobilisten zoals de snelheid, locatie en zelfs de rijstijl van een bestuurder. Maar er zijn ook andere manieren om de oorzaken van een ongeval te achterhalen.

Hyundai Mobis is één van de autofabrikanten die onderzoekt hoe gezichts-, lichaams- en gedragsherkenning in hun auto's gebruikt kan worden (1). De technologie van de Chinese startup 'Deep Glint', die gespecialiseerd is in gezichts-, lichaams- en gedragsherkenning met behulp van AI, wordt hiervoor ingezet. Een eerste toepassing is biometrische toegangscontrole op basis van gezichtsherkenning. Maar er wordt ook gekeken naar de meer geavanceerde toepassing van Deep Glint. Er wordt bijvoorbeeld gekeken naar de mogelijkheid om auto's te personaliseren op basis van gezichtsuitdrukkingen en naar het bestuderen van de aandacht van de autorijder. Wanneer het systeem bijvoorbeeld detecteert dat de automobilist slaperig is, kan een alarm afgaan, zodat de gebruiker weer op de weg let.

Gedragsherkenning van automobilisten die betrokken zijn bij een auto-ongeluk zou een belangrijke rol kunnen spelen bij het reconstrueren van het ongeluk. De gebruikte technologie van bijvoorbeeld Deep Glint kan verzekeringsmaatschappijen doorslaggevende informatie geven over de oorzaken van een ongeluk. Uit de gedragsanalyse kan de verzekeringsmaatschappij mogelijk afleiden dat een bestuurder afgeleid was of wat de gemoedstoestand van de automobilist was voordat het ongeluk plaatsvond. Het gebruik van gedragsherkenning kan echter op gespannen voet staan met de Algemene Verordening Gegevensbescherming (AVG) (2). In dit artikel wordt nader ingegaan op de voorwaarden die gelden voor de inzet van gedragsherkenning bij auto-ongelukken door verzekeringsmaatschappijen in het kader van de AVG.

Voorwaarden verwerken persoonsgegevens

Welke voorwaarden gelden voor het verwerken van persoonsgegevens? De AVG regelt de voorwaarden voor een zorgvuldige omgang met persoonsgegevens. De verwerking van persoonsgegevens is alleen toegestaan wanneer het een bepaald doel dient en je hiervoor een grondslag hebt. Er zijn in totaal zes grondslagen genoemd in de AVG op grond waarvan de verwerking van persoonsgegevens is toegestaan: toestemming, uitvoering van de overeenkomst, wettelijke verplichting, vitaal belang, publieke taak en gerechtvaardigd belang.

‘Door de inzet van gedragsherkenning worden kenmerken over het gedrag van een bestuurder kenbaar’

De AVG kent een verwerkingsverbod voor bijzondere categorieën van persoonsgegevens. Dit zijn wettelijk bepaalde categorieën van gegevens die extra gevoelig zijn. Het gaat dan onder andere om gegevens over het ras, etniciteit, religie, gezondheid en biometrie. In beginsel mogen bijzondere persoonsgegevens niet worden verwerkt, tenzij hiervoor een uitzondering van toepassing is. Gezien de ‘gevoeligheid’ van bijzondere persoonsgegevens gelden er extra strenge regels.

Biometrische gegevens

Wat voor soort persoonsgegevens worden er verwerkt bij gedragsherkenning? Dat zijn biometrische gegevens. Door de inzet van gedragsherkenning worden kenmerken over het gedrag van een bestuurder kenbaar. Deze gegevens worden ‘biometrische gegevens’ genoemd onder de AVG. Biometrische gegevens zijn gegevens die de unieke, fysieke, fysiologische of gedragsgerelateerde kenmerken van een individu bevatten. Met de komst van de AVG in mei 2018 werden biometrische gegevens als bijzondere persoonsgegevens bestempeld. Voor de verwerking van biometrische gegevens dient er dus een uitzonderingsgrond van toepassing te zijn, anders is het niet toegestaan.

Ras of etniciteit automobilist

Bij gedragsherkenning wordt de bestuurder in beeld gebracht. Hierdoor kunnen mogelijk gegevens die iets zeggen over het ras of de etniciteit van de automobilist worden verwerkt. Ras of etnische gegevens worden niet altijd verwerkt wanneer beeldmateriaal wordt verwerkt. De Autoriteit Persoonsgegevens (AP) heeft beleidsregels gepubliceerd met betrekking tot cameratoezicht (3). In deze beleidsregels staan een aantal criteria omschreven wanneer rasgegevens worden verwerkt bij het verwerken van beeldmateriaal. Hier kwam naar voren dat rasgegevens niet worden verwerkt, indien: 1) het doel niet gericht is op het verwerken van rasgegevens dan wel op het maken van onderscheid op grond van ras; 2) het niet voorzienbaar is dat de verwerking zal leiden tot het maken van onderscheid op grond van ras; en 3) de verwerking van ras-gegevens onvermijdelijk is. Indien alle genoemde omstandigheden van toepassing zijn, worden er geen rasgegevens verwerkt volgens de toezichthouder. In geval van gedragsherkenning is het doel niet gericht op het verwerken van rasgegevens of op het maken van onderscheid op grond van ras. Het is niet voorzienbaar dat er onderscheid wordt gemaakt op grond van ras en het is onvermijdelijk dat rasgegevens worden verwerkt. De mogelijkheid om rasgegevens af te leiden bij gedragsherkenning wordt vermoedelijk niet gezien als de verwerking van rasgegevens, zoals bedoeld wordt bij de AVG.

Strafrechtelijke gegevens

Bij verkeersongevallen is het mogelijk dat een bestuurder wordt veroordeeld doordat deze een strafbaar feit heeft gepleegd. Het zou dus mogelijk kunnen zijn dat er ook strafrechtelijke persoonsgegevens worden verwerkt indien een ongeluk wordt gereconstrueerd. Strafrechtelijke gegevens vallen niet onder de categorie bijzondere persoonsgegevens en worden afzonderlijk geregeld in de AVG. Voor de verwerking van strafrechtelijke persoonsgegevens gelden aanvullende voorwaarden. De discussie wanneer sprake is van een strafrechtelijk gegeven is worden – voor de leesbaarheid van dit artikel - verder buiten beschouwing gelaten. Voor het vervolg van dit artikel is daarom alleen gekeken naar de voorwaarden voor het verwerken van biometrische gegevens.

In de Uitvoeringswet van de AVG (UAVG) zijn een aantal uitzonderingsgronden opgenomen waardoor in bepaalde gevallen bijzondere persoonsgegevens, zoals biometrische gegevens, toch verwerkt mogen worden. In geval van biometrische gegevens komen vier uitzonderingsgronden mogelijk in aanmerking: 1) je krijgt de uitdrukkelijke toestemming van de betrokkene; 2) noodzakelijk voor het kunnen identificeren van een persoon voor authenticatie of beveiligings-

doeleinden; 3) noodzakelijk voor een zwaarwegend algemeen belang; of 4) noodzakelijk voor het instellen, uitoefenen of onderbouwen van een rechtsvordering.

Toestemming

Verzekeringsmaatschappijen zouden het gedrag van bestuurders mogen analyseren indien de bestuurder hier uitdrukkelijk toestemming voor heeft gegeven. Toestemming van de betrokkene betekent een vrij gegeven, geïnformeerd, specifiek en ondubbelzinnige indicatie van de wensen van de betrokkene waarmee hij of zij door een verklaring of duidelijke handeling instemt met de inzet van gedragsherkenning door de verzekeraar om ongelukken te reconstrueren. Verzekeraars zullen hun klanten hier goed over moeten informeren. Lang niet alle bestuurders zullen hiermee akkoord gaan. De resultaten kunnen namelijk ook tegen de bestuurder worden gebruikt.

Verzekeraars koppelen data ook weleens aan het betalen van een lagere premie of het verkrijgen van kortingen. De verzekering 'Veilig Rijden Autoverzekering' van de ANWB is hiervan een voorbeeld (4). Automobilisten kunnen voor een verzekering kiezen waarbij korting wordt gegeven indien de bestuurder goed rijgedrag vertoont. De AP en de Artikel 29-werkgroep (tegenwoordig de European Data Protection Board), waarin de Europese toezichthouders zijn verzameld, lijken de mogelijkheid om toestemming te vragen voor het gebruiken van persoonsgegevens voor dit doel niet uit te sluiten (5).

Er wordt verder geen nadere toelichting gegeven over de voorwaarden voor het vragen van 'toestemming' aan verzekeringnemers om hun data te geven in ruil voor een betere premie. Bij gedragsherkenning worden nog gevoeligere gegevens verwerkt dan bij de verzekering van de ANWB, omdat hier ook bijzondere categorieën van persoonsgegevens worden verwerkt. Dit kan een behoorlijke impact op de privacy van een automobilist hebben. Dergelijke verzekeringen roepen vragen op over de vrijwillige keuze van de betrokkenen. Hoe vrij ben je in de keuze om data te geven aan de verzekeraar als je hier korting voor ontvangt wanneer je bijvoorbeeld in de schuldsanering zit? Er heerst echter nog onduidelijkheid over welke gegevens en hoeveel gegevens mogen worden gevraagd door de verzekeraar om de hoogte van de premie te bepalen indien de bestuurder hier toestemming voor geeft. Deze vragen zullen veelal ook een ethische afweging zijn. Jurisprudentie en richtlijnen van de toezichthouder zullen hier hopelijk in de toekomst nadere toelichting over kunnen geven. Verzekeraars dienen in ieder geval de 'vrije keuze' om persoonsgegevens aan de verzekeringsmaatschappij te verstrekken zo goed mogelijk te waarborgen.

Authenticatie of beveiliging

Het gebruik van gedragsherkenning in een auto door de verzekeraar heeft als doel om bij te dragen aan een goede omschrijving van alle relevante factoren bij een auto-ongeluk. Het controleren van de identiteit van een bestuurder en beveiliging van de toegang tot een auto is in dit geval niet het doel voor de inzet van biometrie. Voor het (mede) vast-

stellen van een ongeluk kan daarom geen beroep worden gedaan door de verzekeringsmaatschappij op de gronden authenticatie of beveiliging.

Zwaarwegend algemeen belang

Het gebruik van gedragsherkenning bij automobilisten door verzekeringsmaatschappijen kan ervoor zorgen dat bestuurders beter op de weg gaan letten, wat de verkeersveiligheid ten goede komt. Het gedrag van bestuurders kan positief worden beïnvloed indien zij weten dat de verzekeringsmaatschappij hun gedrag kan analyseren ingeval van een ongeluk.

Het hoofddoel – het maken van een goede reconstructie van een ongeluk om de aansprakelijkheid vast te kunnen stellen – dient niet zozeer een algemeen belang, maar eerder het belang van de verzekeraar en van het slachtoffer. Gedragsherkenning kan ook een preventieve werking hebben en dat kan de verkeersveiligheid vergroten - wat wel een publiek belang dient.

Stichting Wetenschappelijk Onderzoek Verkeersveiligheid (SWOV) heeft een literatuuronderzoek gedaan naar de pakkans en straf en de invloed hiervan op verkeersovertredingen (6). Uit het onderzoek bleek dat wanneer de bestuurder de pakkans groot acht deze eerder een verkeersovertreding zal nalaten. De pakkans had hierbij vaak meer invloed dan de hoogte van een straf. De vraag is echter of de mogelijke bijwerking van gedragsherkenning op de verkeersveiligheid voldoende is om te kunnen spreken van een zwaarwegend algemeen belang.

Om een beroep te kunnen doen op een 'zwaarwegend algemeen belang' gelden strenge voorwaarden. In de Nederlandse Uitvoeringswet van de AVG zijn enkele beperkingen voor deze uitzonderingsgrond opgenomen. Voor verzekeringsmaatschappijen geldt in deze situatie dat verzekeraars overeenkomstig een volkenrechtelijke verplichting (dat wil zeggen een verplichting in een verdrag) dienen te handelen. Indien dit niet het geval is, kan geen beroep worden gedaan op het hebben van een 'zwaarwegend algemeen belang'. Een dergelijke wettelijke verplichting voor verzekeringsmaatschappijen om de verkeersveiligheid te vergroten, is niet gevonden. De inzet van gedragsherkenning door verzekeringsmaatschappijen kan in dit geval dus waarschijnlijk niet op grond van een zwaarwegend algemeen belang, tenzij hiervoor speciale wetgeving zou komen.

Rechtsvordering

Wanneer een verzekeraar een rechtsvordering instelt, kan het gedrag van de bestuurder relevant zijn voor de verzekeraar om de rechtsvordering te onderbouwen. Op voorhand kan de verzekeraar echter niet weten of het gedrag van de automobilist noodzakelijk is voor het uitoefenen, instellen of onderbouwen van een rechtsvordering. Verzekeringsmaatschappijen kunnen de mogelijkheid om gegevens nodig te hebben voor een toekomstige rechtsvordering niet als grond gebruiken om op voorhand gegevens over iemands gedrag te verzamelen. Het gedrag van bestuurders kan daarom nooit 'standaard' worden geanalyseerd door verzekeringsmaatschappijen voor dit doel. Verzekeraars dienen dus eerst een grond te hebben om deze gegevens in te mogen zien.

Wanneer de verzekeringsmaatschappij de gedragsanalyse legitiem in handen weet te krijgen, zou het mogelijk kunnen worden gebruikt ter onderbouwing van een rechtsvordering. De verzekeringsmaatschappij zal de gegevens waarschijnlijk niet verkrijgen van de autofabrikant. De kans dat een autofabrikant persoonsgegevens voor dit doel aan een verzekeraar gaat geven, is namelijk erg klein. Het verschaffen van persoonsgegevens aan de verzekeraar van een bestuurder zonder diens toestemming zal de relatie tussen de bestuurder en de autofabrikant niet goed doen. Om de eigen reputatie hoog te houden, zal een autofabrikant deze informatie waarschijnlijk niet aan een verzekeraar geven. Daarbij is het ook maar de vraag of de autofabrikant deze gegevens überhaupt mag verstrekken aan een verzekeraar zonder toestemming. In veel gevallen zal er namelijk geen doelbinding zijn (zie het hoofdstuk over 'Is er sprake van een verenigbaar doel?').

De verzekeraar kan dan alleen inzage krijgen in de gedragsanalyse indien de bestuurder zelf de informatie verstrekt of indien de rechter oordeelt dat de verzekeraar recht heeft op inzage. Automobilisten zullen in de meeste gevallen deze informatie alleen verstrekken, indien de gedragsanalyse in diens voordeel spreekt. De kans dat een bestuurder zelf incriminerende bewijsstukken aanlevert, is erg klein. De gedragsanalyse zal in dit geval dus vaak weinig toegevoegde waarde hebben waardoor het niet noodzakelijk is voor het instellen, uitoefenen of onderbouwen van een rechtsvordering. Indien de tegenpartij stelt dat de bestuurder niet zat op te letten en uit het gedrag van de bestuurder blijkt dat de bestuurder wel aandacht voor de weg en

het verkeer had, is het verdedigbaar dat deze informatie noodzakelijk is voor de onderbouwing van de rechtsvordering. In dit geval kan het als bewijs fungeren wanneer er een juridische procedure loopt tussen de verzekeringsmaatschappij en de wederpartij.

Verzekeraars kunnen niet altijd de informatie die volgt uit de gedragsherkenning gebruiken op grond van het instellen, uitoefenen of ter onderbouwing van een rechtsvordering. Er zijn enkele situaties denkbaar dat het wel op grond hiervan mogelijk is, maar dan moet de betrokkene eerst de informatie hebben verstrekt aan de verzekeraar of de rechter moet hebben besloten dat de verzekeraar recht heeft op inzage.

Verenigbaar doel

Persoonsgegevens mogen worden verwerkt indien dit een vooraf bepaald en een uitdrukkelijk omschreven specifiek doel dient. Wanneer persoonsgegevens worden verwerkt voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verzameld, bepaalt de AVG dat dit alleen mogelijk is indien dit doel verenigbaar is met het oorspronkelijke doel. In geval van de inzet van gedragsherkenning door verzekeraars lijkt het erop dat dit alleen mogelijk is indien de bestuurder hier uitdrukkelijk toestemming voor geeft. Doordat de betrokkene toestemming geeft aan de verzekeraar om deze gegevens te verwerken voor een bepaald doel, is het niet noodzakelijk om te beoordelen of dit doel verenigbaar is met het doel van de autofabrikant om gedragsherkenning te gebruiken.

Conclusie

Verzekeringsmaatschappijen hebben een belang bij het maken van een goede reconstructie van een auto-ongeluk indien zij hiervoor moeten gaan betalen. De verzekeringsmaatschappij moet voor de verwerking van deze gegevens een geldige grondslag, uitzonderingsgrond en een gerechtvaardigd doel hebben. De gegevens die zijn af te leiden uit gedragsherkenning zijn in ieder geval biometrische gegevens, omdat gegevens worden verwerkt over de kenmerken van het gedrag van de bestuurder. De verwerking van biometrische gegevens is verboden, tenzij de bestuurder hier uitdrukkelijke toestemming voor heeft gegeven, het bedoeld is ter authenticatie of beveiliging, wanneer het een zwaarwegend algemeen belang dient, of wanneer het noodzakelijk is voor het instellen, uitoefenen of onderbouwen van een rechtsvordering. De inzet van gedragsherkenning door verzekeringsmaatschappijen berust in dit geval niet op een beveiligingsdoel of wordt ten behoeve van authenticatie ingezet. Verzekeraars gebruiken gedragsherkenning alleen om te bepalen wat voor gedrag een automobilist vlak voor of tijdens een ongeval vertoonde, zodat de oorzaken van het ongeluk kunnen worden vastgesteld en de eventuele opzet en schuld van de bestuurder kan worden bepaald.

Daarnaast lijkt het erop dat de inzet van gedragsherkenning in dit geval enkel het belang van de verzekeraar dient en niet het algemeen belang zoals bedoeld in de AVG. Ondanks dat er uit verschillende studies is gebleken dat een grotere pakkans ervoor kan zorgen dat bestuurders minder (bewuste) verkeersovertredingen maken, is niet voldaan aan alle voorwaarden voor een zwaarwegend algemeen belang. De taak om de verkeersveiligheid te bevorderen is namelijk nergens in de wet opgenomen als een taak voor verzekeraars. Zonder deze wettelijk toegewezen taak is het voor verzekeraars niet mogelijk om gedragsherkenning hiervoor in te zetten. Ook is het voor verzekeraars niet mogelijk om een potentiele rechtsvordering in de toekomst te gebruiken als excuus om altijd gegevens te verzamelen van automobilisten. Alleen de uitzonderingsgrond toestemming resteert nu nog. Er zijn situaties denkbaar waarbij de betrokkene toestemming geeft aan de verzekeraar om zijn of haar persoonsgegevens te verwerken door gedragsherkenning toe te passen in de auto. Wanneer een bestuurder hier uitdrukkelijk toestemming voor geeft, de toestemming vrij is gegeven en de bestuurder goed geïnformeerd is over waar toestemming voor wordt gegeven, dan is het mogelijk.

Referenties

(1) https://www.businesswire.com/news/home/20190312005980/en/

(2) https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex%3A32016R0679

(3) AP, 'Cameratoezicht - Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens', 28 januari 2016, p. 26-27.

(4) www.anwb.nl/verzekeringen/autoverzekering/veilig-rijden

(5) www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/-financien/financiele-instellingen?qa=premie&scrollto=1

(6) Dr. eh. Goldenbeid, 'De invloed van pakkans en straf op verkeersovertredingen', Stichting Wetenschappelijk Onderzoek Verkeersveiligheid (SWOV), Leidschendam 1994.

In deze rubriek geven enkele iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over de 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 kunt u sturen naar ibmagazine@pvib.nl.

Dark clouds

Eind maart was het groot in het nieuws: 'Data honderdduizenden patiënten in stilte naar Google verhuisd', kopte een groot dagblad. Patiëntgegevens van grote aantallen Nederlandse burgers zijn verhuisd naar Google Cloud. Zorginstellingen hebben hun patiënten niets gevraagd en niets verteld. Inmiddels zijn diverse privacydeskundigen en politici aan het woord geweest en is er inmiddels vraag om actie vanuit de AP. Is de veiligheid van 'onze' medische data in gevaar of niet?

Chris de Vries

Het patiëntendossier en –geheim: om hoofdpijn van te krijgen. Al jaren mislukt dit dossier, maar wij horen dat medische gegevens ultiem beschermd zijn. Wat is belangrijker dan de eigen medische gegevens? Vrijgave aan commerciële partijen of vreemde overheden is als een arm/beenamputatie. Wat is persoonlijker? In onze moderne samenleving een niet-bestaande barbaarsheid? Recentelijk plaatste men buiten ons om de persoonlijke, medische gegevens in de 'cloud'. De slager (MRDM, Amerikaanse techgigant) oordelende over zijn eigen vlees: "Het is goed dat de discussie wordt gevoerd of het wenselijk is dat een internationale hostingleverancier, met locatie in Nederland, Nederlandse gezondheidsgegevens mag opslaan. (…)" Wij echter: de gegevens zijn op zijn minst open voor de Amerikaanse overheid, zo niet vrijwillig dan via achterdeuren of via de CIA gefinancierde 'startups' (zoals Google)?!

Wederom bezorgde reacties van onze politici en overheid.

Chris de Vries | Maarten Hartsuijker | Fook Hwa Tan

Opnieuw activering van een autoriteit. "Maar of er nu al aanleiding is om een onderzoek te starten, kan ik nog niet zeggen", aldus voorzitter Aleid Wolfsen, die dit aanvult met het belang van de opstelling van het parlement: "De Tweede Kamer bepaalt als wetgever mede de speelruimte voor verwerking van zulke gegevens." Wat betekent dat voor ons? Het kalf ligt in de put en is al verdronken, want voor die Nederlanders, wiens gegevens in de 'cloud' staan, is het te laat. Zij zijn al vereeuwigd. En zo ploegt de boer voort en begraaft hij de botten onder de aarde, want 'wat niet ziet, dat niet deert'. Naïviteit blijkt de norm te zijn.

Maarten Hartsuijker

'Eerste Kamer zet streep door EPD', kopten de nieuwsberichten enkele jaren terug. De Eerste Kamer achtte de toenmalige opzet van het EPD niet veilig genoeg. Tegenwoordig mag iedereen zelf kiezen of zijn zorgaanbieder zijn gegevens mag delen. Maar blijkbaar beperkt deze toestemmingsvereiste zich tot het LSP en zijn patiëntgegevens elders vogelvrij. Het commerciële bedrijf MRDM ontvangt (aldus het AD) per patiënt soms wel 500 'datavelden', waaronder gegevens over de aandoening, opnameduur, zorgverlener en medicatie. Deze set is veel te groot om zo te anonimiseren dat hij in geen geval meer herleidbaar is tot een natuurlijk persoon. Partijen zoals Google, Microsoft en vele andere datahandelaren kunnen immers via opgeslagen zoek- en browsegedrag (om nog niet te spreken over online agenda's waarin ziekenhuisafspraken zijn opgeslagen) precies achterhalen wie er bij een dossier hoort. Wat mij betreft hoort de data zonder toestemming van de patiënt in deze vorm bij niemand behalve de zorgverlener thuis. En zeker niet bij een bedrijf dat de middelen heeft om gevoelige data sets als deze te repersonaliseren.

Fook Hwa Tan

De vraag of vertrouwelijke data of privacygevoelige data naar Google Cloud mag, wordt steeds vaker gesteld. Het begint erop te lijken, dat we juist naar zo'n grote cloudprovider moeten. Waarom? Als we alleen naar Google Cloud kijken, dan kunnen we door de vele eisen van hun grotere klanten stellen dat Google veel doet aan de veiligheid van de gegevens die haar worden toevertrouwd. Het is misschien niet leuk dat de eigenaar van de gegevens, wij, niet op de hoogte worden gesteld en geen invloed hebben, maar het is vaak wel veiliger dan bij de IT-provider om de hoek. Grote cloudpartijen worden vaak nauwlettend gevolgd door toezichthouders (nationaal en internationaal), waardoor ze vaak gedwongen worden om additionele maatregelen te nemen en de standaard hoog te houden. Mijn stelling is dat zelfs hun minimale basisbeveiliging mogelijk hoger zal zijn dan veel kleinere cloudpartijen. Het is vaak moeilijker om onveilige omgevingen in je netwerk toe te staan en deze goed af te zonderen van andere hoger beveiligde omgevingen. Als laatste hebben dit soort organisaties vaak dedicated securityteams om de veiligheid van de toevertrouwde gegevens te borgen. Dit zijn vaak geen kleine teams. Dit zie je bij andere partijen vanwege de kosten niet of nauwelijks terug. De conclusie is dat Google Cloud misschien om vele redenen niet wenselijk is, maar dat veiligheid daar niet één van is!

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

REDACTIE
Tom Bakker
Bianca Brooijmans
Patrick Dersjant
Nicole van Deursen
Maarten Hartsuijker
Lilian Knippenberg
Rachel Marbus
Fook Hwa Tan
Chris de Vries

BLADMANAGEMENT
MOS bv
José Broekhuizen
Lisa Petersen
E ibmagazine@pvib.nl

ADVERTENTIE-ACQUISITIE
MOS bv
Jan van de Vis
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 2019 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

Ik kan het niet geloven

Trouwe lezers van deze column zullen inmiddels wel weten dat ik een soort haat-liefdeverhouding heb met internet en alles wat daarmee samenhangt. De liefdeskant beschrijf ik niet zo vaak, maar neem van mij aan dat het www, e-mail en alle andere handigheden op internet mij bijzonder aanspreken.

Helaas zijn er ook wel zaken te noemen waar ik iets minder blij van word. Daar gaan mijn columns ook vaak over. Dat komt omdat ik mij soms over dingen verbaas. Facebook heb ik vaak genoemd in mijn columns, temeer omdat ze de laatste jaren (of beter gezegd: sinds ze naar de beurs gingen) zo nu en dan een beetje buiten hun boekje zijn gegaan.
Natuurlijk weten zij (net als vele andere datamiljardairs) dat ze hun rijkdom aan de gebruikers te danken hebben. En wij zijn allemaal bereid om die clubs rijker te maken dan dat ze nu al zijn. Wij zijn zelfs bereid onze meest intieme data neer te leggen bij die clubs, hetzij in de vorm van onze mail, hetzij in de vorm van documenten die we gratis ergens in de cloud mogen neerzetten, of door onze foto's die we mogen opslaan.

En dat allemaal voor niets, nou ja … bijna niets.
Het enige wat we weggeven, is de inhoud van onze e-mails. Wat maakt dat nou uit? Alle foto's zetten we ook maar in de cloud, want dan hebben we in ieder geval een back-up.
Ja dat klopt ook, maar we vinden het niet belangrijk dat de foto's gewoon ingekeken mogen worden. Of dat Facebook weet wat we de hele dag gedaan hebben en wie onze vrienden zijn. Wist je dat er ook nog vrienden zijn die nog geen Facebookmaatje van jou zijn? Geen probleem hoor, want Facebook zoekt het gewoon even op in je mail.

Dan heb ik het nog niet eens over al die berichten die verspreid worden, maar helemaal niet waar zijn. Facebook verwijdert iedere dag 1 miljoen accounts (ik herhaal: 1.000.000 accounts) die op de één of andere manier verdacht zijn. Nou mogen er best wat minder accounts zijn, maar als je nagaat dat er in Nederland meer dan 10 miljoen gebruikers zijn, kun je je dan voorstellen hoeveel (on)zinnige dingen gepost worden waar Facebook mee kan doen wat ze maar wil?

Let dus op je gegevens, denk niet dat niemand behoefte heeft aan jouw gegevens, want dat is één van de grootste denkfouten die je kunt maken. We kunnen niet meer zonder internet (herstel, IK kan niet meer zonder internet), maar probeer minimaal scherp te zijn op welke gegevens je deelt met onze Amerikaanse vrienden.

Berry

SECURITY ACADEMY

OPLEIDINGENOVERZICHT

NIEUW IN ONS PORTFOLIO:

Hierboven ziet u een greep uit ons portfolio. Bij de Security Academy kunt u terecht voor het behalen van verschillende internationale titels van **SECO-Institute®**, **IAPP®**, **ISC²®** en **ISACA®**.
Daarnaast biedt de Security Academy een aantal specialistische cursussen en Masterclasses aan. Denk hierbij aan cursussen als Identity and Access Management, Social Engineering of de Masterclass Business Resilience.
Voor het complete overzicht, meer informatie en cursusdata kunt u terecht op onze website.

www.securityacademy.nl
info@securityacademy.nl
+31(0)348-40 80 61