iB
INFORMATIEBEVEILIGING
jaargang 17 - 2017
#5

PRIVACY

De nieuwe privacy-verordening zet de rechten van kinderen onder druk

Eén zekerheid in onzekere tijden

AVG GAP-analyse

Interview Paul Samwel en Reinder Wolthuis: Samen ten strijde

Certificeren? Dan moet u voldoen aan de norm. DNV GL toetst u snel en goed. Maar iedereen houdt van opstekers, niet van standjes. Daarom kijken we bij certificering ook naar wat goed gaat en zelfs nog beter kan. Op die gebieden die voor uw bedrijf of organisatie belangrijk zijn. Aandachtspunten waarop u zélf beoordeeld wilt worden. Certificering die net even verder voert. Want verbetering zit in een klein hoekje.

U kunt ons bereiken via 010 2922 700 of www.dnvgl.nl

Stappenplan ISO 27001/NEN 7510

Download kosteloos de whitepaper 'Stappenplan naar informatiebeveiliging'

www.dnvgl.nl/whitepapers

EEN IEDER HEEFT RECHT OP ZIJN PERSOONLIJKE LEVENSSFEER

Over privacy raak ik nooit uitgepraat. Het is een recht wat door de tijd heen mee verandert met de mensen, techniek en de maatschappij. Het is daarmee een fluïde recht, het beweegt heel prachtig mee met de mores en de mogelijkheden die in onze maatschappij gezien worden. Privacy is iets wat je vooral ook moet voelen. Het nadeel is dan weer wel dat je het vaak pas écht gaat voelen als er een inbreuk op je privacy wordt gemaakt. Doorgaans niet het meest aangename moment. In onze rubriek Achter Het Nieuws lees je hoe onze redacteuren een privacyinbreuk ervaren.
Gelukkig ben ik niet de enige die er niet over uitgepraat raakt. Het was dan ook niet heel lastig om auteurs te vinden die in de pen wilden klimmen om hun gedachten op papier te zetten. De onderwerpen die je in dit nummer tegenkomt, zijn ook enorm divers, van praktische implementatie van nieuwe wetgeving tot een beschouwing over de onzekerheden in die nieuwe wetgeving. Een verhaal over de rechten van kinderen in relatie tot privacy en een over informatiebeveiliging en privacy. En dat is nog slechts een bloemlezing. Dit is tegelijkertijd waarom privacy voor mij niet alleen razend interessant blijft, maar ook telkens voor nieuwe verwondering zorgt. Een ding dat onveranderd blijft, is dat privacy gaat over het goede doen voor mensen. En over datgene wat goed is, kunnen we onverminderd met elkaar in gesprek blijven. Veel leesplezier!

Rachel Marbus

In dit nummer

DE NIEUWE PRIVACY-VERORDENING ZET DE RECHTEN VAN KINDEREN ONDER DRUK

Vorig jaar is de Algemene Verordening Gegevensbescherming (AVG) aangenomen die op 25 mei 2018 van kracht wordt. Deze verordening zal de inmiddels verouderde privacy-richtlijn uit 1995 vervangen en is vanaf het moment van inwerkingtreding rechtstreeks van toepassing in de Europese Unie. De AVG moderniseert het huidige privacyrecht en verstevigt het fundamentele recht op bescherming van persoonsgegevens. De AVG introduceert belangrijke vernieuwingen (waaronder het beginsel van privacy by design) in het privacyrecht die ervoor moeten zorgen dat de weegschaal meer richting bescherming van burger en consument uitslaat in een wereld waarin persoonsgegevens ook wel `de nieuwe olie' worden genoemd. Of dat gaat lukken, hangt af van de juridische inkleuring van deze regels en hun praktische implementatie die wordt bemoeilijkt doordat de AVG vooral veel vragen oproept. Een van de terreinen waarop onduidelijkheid heerst, is die van de bescherming van de persoonsgegevens van kinderen.

De AVG beoogt kinderen extra te beschermen tegen overheden en bedrijven, omdat zij zich niet bewust zouden zijn van de risico's van de verwerking van hun persoonsgegevens (zie overweging 38). Overigens is dat laatste niet gefundeerd met empirische inzichten, maar geheel onwaarschijnlijk lijkt het niet.

Ouderlijke toestemming…

Wat is dan de oplossing? Dat is er niet slechts één, maar de belangrijkste is wel dat ouderlijke toestemming een vereiste wordt voor de verwerking van de persoonsgegevens van hun kinderen onder de 16 jaar voor online diensten die rechtstreeks aan kinderen worden aangeboden (artikel 8 AVG). Dat leidt meteen tot de vraag welke diensten in deze categorie vallen? Specifiek op kinderen gerichte diensten? Daarmee zouden veel generieke diensten die juist door kinderen worden gebruikt -denk aan Snapchat, WhatsApp, Instagram, YouTube- dus niet binnen het bereik van de bepaling vallen. Of gaat het om online diensten die –mede- worden gebruikt door of toegankelijk zijn voor kinderen? Of: online diensten die populair zijn onder kinderen? Het antwoord kennen we nog niet, maar gelet op het onderliggende rechtsbelang is een ruime uitleg gepast. Daarnaast roept de bepaling allerlei praktische vragen op: Hoe ga je als bedrijf verifiëren dat je met een kind onder de 16 te maken hebt en of het inderdaad de ouder was die toestemming heeft gegeven? Met welke technische tools heb je als bedrijf op zijn minst voldaan aan je inspanningsverplichting om te verifiëren?

… vormt een inbreuk op de privacy

Een volgende vraag is: hoe kan worden voorkomen dat de verificatieverplichting een privacy-inbreuk oplevert? Paradoxaal genoeg is het welhaast onmogelijk om deze bepaling uit te voeren zonder -tegen de geest van de AVG in- meer persoonsgegevens van zowel ouder als kind te verwerken dan noodzakelijk was geweest zonder deze verplichting. Op zijn minst zal steeds moeten worden geverifieerd of iemand al dan niet de leeftijd van 16 is gepasseerd en zo niet dan zal de ouder -dan wel een ander die de ouderlijke verantwoordelijkheid draagt of gemachtigd is om voor het kind te handelen- zich als zodanig kenbaar moeten maken. Markant is dat ouders ingevolge dit vereiste in feite moeten instemmen met het online mediagebruik van hun kinderen, althans zolang ze onder de 16 zijn. Zodra dochter- of zoonlief een account wil openen op Snapchat of Musical.ly zal dat de goedkeuring van ouders moeten krijgen. Tieners die het vervelend vinden als ouders op de hoogte raken van hun hele online doen en laten, hebben dus een probleem als bedrijven dit vereiste strikt gaan implementeren. De bepaling staat daarmee merkwaardig genoeg op gespannen voet met het recht op privacy van kinderen in de relatie tot hun ouders. Voor kinderen, ook reeds op jonge leeftijd, is die privacy echter enorm belangrijk (1). De vrijheids- en ontwikkelingsrechten van kinderen zijn niet -of in ieder geval niet nadrukkelijk- meegenomen in de overwegingen bij de AVG en dat leidt ook tot andere zorgen bij de uitvoering en implementatie ervan.

… zet ook andere vrijheidsrechten onder druk

Indien voor kinderen ouders de wettelijk verplichte toegangspoort tot de digitale wereld worden, kan het zomaar zo zijn dat een groep kinderen die -voor hen buitengewoon relevante- toegang wordt ontzegd. Hetzij omdat ouders niet willen meewerken, hetzij omdat ze dit niet kunnen omdat ze bijvoorbeeld niet 'in the picture' zijn. Maar zelfs als ouders meewerken, dan nog kan kinderen de toegang tot online diensten worden ontzegd. Bedrijven kunnen ervoor kiezen om kinderen die ouderlijke toestemming nodig hebben te weren van hun platform. Zo blokkeert Google diensten waarbij zij persoonsgegevens verzamelen, zoals Gmail, als ze erachter komen dat iemand onder de 16 is om aan deze namelijk reeds in de Wet bescherming persoonsgegevens opgenomen wettelijke verplichting te voldoen (2). Veel scholieren gebruiken Gmail en het is dus zuur als je ineens geen toegang meer hebt tot je berichten en wellicht huiswerk. Google houdt zich natuurlijk gewoon aan de privacywet, maar als de, nog strengere, AVG ertoe leidt dat meer bedrijven zich zo strikt opstellen en veel diensten ontoegankelijk worden voor kinderen, dan raakt dat direct aan de vrijheids- en

Prof. mr. Simone van der Hof is Hoogleraar Recht en Digitale technologie, directeur van het Centrum voor Recht en Digitale Technologie (eLaw) en programmadirecteur van de Advanced Master Law and Digital Technologies, Faculteit Rechtsgeleerdheid, Universiteit Leiden. Ze is bereikbaar via s.van.der.hof@law.leidenuniv.nl.

ontwikkelingsrechten die zij hebben op basis van het VN Verdrag voor de Rechten van het Kind 1989: het recht op vrijheid van informatie en meningsuiting, het recht op toegang tot de media, het recht op privacy en vereniging, het recht om te spelen en het recht op onderwijs (3).

... schiet zijn doel voorbij

Maar de privacywetgeving beoogt kinderen toch te beschermen? Heiligt dat lovenswaardige doel dan niet het goedbedoelde middel? Nog steeds vereist de holistische benadering van het kinderrechtenverdrag -waarbij alle rechten in beschouwing moeten worden genomen- dan dat ook andere dan beschermingsrechten van kinderen dienen te worden meegewogen bij het vaststellen van adequate maatregelen (3). Nemen we voor het gemak echter even aan dat we daar wel uitkomen, dan veronderstellen we bij een positieve beantwoording van voornoemde vraag dat het middel (ouderlijke toestemming) werkt en daarvan weten we inmiddels dat dit buitengewoon twijfelachtig is (4). Het meer algemene idee achter het toestemmingsvereiste is dat je zelf de controle houdt over je persoonsgegevens en kunt kiezen, of op zijn minst weet, wat ermee gebeurt. Die controle hebben we echter allang niet meer en het is volkomen ondoorzichtig hoe persoonsgegevens onder de motorkap van het internet worden verwerkt. Privacyverklaringen zijn te vaag om daarover uitsluitsel te geven, worden doorgaans niet gelezen en de meeste mensen klikken er zelfs gedachteloos aan voorbij (4). Veel apps zijn bovendien niet voorzien van een privacyverklaring (5). Bedrijven bepalen bovendien de regels van het spel en als individu kun je enkel nog beslissen om mee te spelen, geen waarlijk autonome keus dus zoals het toestemmingsvereiste veronderstelt (en zelfs verlangt, zie artikel 7 AVG). Als we kinderen echt willen beschermen tegen surveillance-praktijken dan zijn andere maatregelen noodzakelijk, maar welke en hoe we die gaan implementeren zijn twee andere vragen waar de AVG niet direct een antwoord op geeft.

Hoe nu verder?

Dat neemt niet weg dat de AVG wel degelijk interessante mogelijkheden biedt om het toestemmingsvereiste te ondersteunen met andere beschermingsmechanismen. Zo suggereert de AVG bijvoorbeeld dat kinderen vooral extra bescherming nodig hebben in het geval van geautomatiseerd online profileren van mensen (overwegingen 38 en 71). Het is best denkbaar dat bedrijven zich geheel onthouden van het online volgen van kinderen, wat per saldo de omvang van de verwerking van hun persoonsgegevens flink reduceert en voorkomt dat ze worden geprofileerd. Bovendien voegt de AVG zoals gezegd belangrijke vernieuwingen aan het privacyrecht toe die juist ook voor kinderen en de bescherming van hun rechten interessant en relevant zijn. Het voorgaande is een voorbeeld van de implementatie van het beginsel van privacy by default (artikel 25): de standaardinstelling is dat het online gedrag van kinderen niet geobserveerd, vastgelegd en geanalyseerd wordt voor commerciële of andere doeleinden. In diezelfde bepaling wordt ook het beginsel van privacy by design geregeld dat bij online diensten die door kinderen worden gebruikt voor innovatieve toepassingen kan leiden. Zo moeten bedrijven kinderen op een voor hen begrijpelijke en gemakkelijk toegankelijke wijze informeren over de verwerking van hun persoonsgegevens (artikel 12) en die transparantie zou bijvoorbeeld gevisualiseerd en met spelelementen gerealiseerd kunnen worden. Geen eenvoudige klus (6) maar voor creatieve en innovatieve geesten niettemin een mooie uitdaging. Een andere vorm van privacy by design is pseudonimisering om minimale gegevensverwerking te realiseren. Daarmee zijn we er nog geenszins. Als er sprake is van geautomatiseerde online profilering van individuele personen dan zullen bedrijven een privacy impact assessment moeten uitvoeren om de risico's in te schatten en adequate maatregelen te bepalen. Het Comité voor de Rechten van het Kind laat er geen misverstand over bestaan dat op basis van het kinderrechtenverdrag tevens een kind impact-assessment en -evaluatie vereist is als regelgeving effect heeft op kinderen (7). Zo'n assessment houdt in dat de impact op kinderen en hun rechten moet worden voorspeld en geëvalueerd. Het mag duidelijk zijn geworden dat een dergelijk onderzoek geen overbodige luxe is en met zich mee kan brengen dat ook binnen de AVG naar een holistische benadering moet worden gezocht om te voorkomen dat met de bescherming van persoonsgegevens van kinderen niet onverhoopt juist inbreuk wordt gemaakt op de rechten van kinderen.

Referenties

(1) B Shmueli, A Blecher-Prigat, Privacy for children, 42 Columb Human Rts L Rev 2011, available at: http://bit.ly/2xC4XVR.
(2) R Pijpers, Waarom heeft Google de Gmail van mijn zoon afgesloten?, http://bit.ly/2iKSewF.
(3) S van der Hof, ? – A rights-based analysis of the law on children's consent in the digital world, 34 Wis. Int'l L.J. 409 2016-2017.
(4) B.W. Schermer, B. Custers, S. van der Hof, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, Ethics Inf Technol (2014) 16:171–182.
(5) APPFAIL — Threats to Consumers in Mobile Apps, Norwegian Consumer Council, March 2016, available at: http://bit.ly/2jntEyG.
(6) B van den Berg, S van der Hof, What happens to my data? First Monday, Volume 17, Number 7 - 2 July 2012.
(7) Committee on the Rights of the Child, General Comment No. 5, 2003, CRC/GC/2003/5, paras. 12, 45-47.

HET GOEDE DOEN

Wie op dit moment binnen bedrijf of overheid bezig is met privacy, weet dat er maar één topic is waar het om draait: alles is AVG – de Algemene Verordening Gegevensbescherming. Normaal toch wel nieuws waar elke privacyliefhebber blij van zou moeten worden, maar ik heb gemerkt dat het me de laatste twee jaar toch wel een beetje met pijn in het hart achterlaat. Want privacy gaat eigenlijk helemaal niet over de AVG. En al helemaal niet over het implementeren van allemaal administratieve systemen die je gegevensverwerkingen registreren. Laten we eerlijk zijn… een groot deel van de tijd is dat toch exact waar we nu mee bezig zijn, nietwaar?

We zijn nu zo met het microniveau van privacy bezig – het volgen van de kleine lettertjes van de wet – dat we totaal voorbij gaan aan privacy. Want privacy gaat eigenlijk simpelweg over het goede doen. Je kunt de letters van de wet volgen en denken dat je het correct doet wat betreft privacy, maar als je vergeet te vragen of het ook echt deugt wat je doet, dan loop je tegen een enorme (terechte) muur van verzet aan als de regeltjes letterlijk het enige zijn waar je aan dacht. Zoals recentelijk bleek bij de camera's in reclameborden op treinstations. Maar ook eerder bij ING en het willen analyseren van bankrekeninggegevens. En dat zijn echt niet de enige voorbeelden. Telkens als ik de publieke verontwaardiging over een dergelijke privacy-nono hoor, denk ik aan de titel van een van de boeken van Terry Pratchett: 'Wij pikken het niet langer!'. Want als je alleen maar klakkeloos de regeltjes tot de letter volgt (of misschien zelfs wel een beetje in je eigen voordeel oprekt) en aan je eigen belang denkt, dan vergeet je de belangrijkste speler in het geheel: de persoon om wiens privacy het gaat. En ja, dan komt er verzet.

Het goede doen, heeft vooral ook te maken met dat klanten, burgers, jij en ik niet willen dat er over onze ruggen wordt verdiend aan onze private gegevens. Dat een bedrijf jouw gegevens wil uitnutten waardoor het dubbel aan jou verdient, je betaalt ze immers al voor hun diensten en dan nogmaals doordat je gegevens voor het bedrijfsgewin worden ingezet. Het gaat om de overheid die vaak in het kader van 'pak-ze' van alles en nog wat bij elkaar harkt. Denk bijvoorbeeld aan de Belastingdienst die telkens maar weer gegevens opvraagt waarvoor zij geen enkele wettelijke grondslag heeft (en dus ook al meerdere malen door de rechter op de vingers is getikt). Om die gegevens vervolgens allemaal bij elkaar te mikken en daarmee allerhande nieuwe inzichten te kunnen verwerven in ons doen en laten. Fruit from a poisonous tree. Het is juridisch niet in orde en het deugt ook van geen kant.
Maar ja… hoe lukt het in deze tijden van implementatiegekte dan wel om toch te blijven kijken naar waar het echt om gaat? Dat is in meer normale tijden ook al een flinke uitdaging, omdat doorgaans privacymensen binnen organisaties toch gewoonweg kampen met te veel vragen en te weinig mankracht om die allemaal te beantwoorden. Het enige antwoord is: door er ondanks alles toch standaard tijd voor vrij te blijven maken. Door samen met andere spelers in jouw organisatie te gaan zitten en te bedenken hoe je recht kunt doen aan de privacy van de burger, klant, van jou en mij. Hoe je jouw doelen kunt bereiken met respect voor privacy. En geloof me, als je een beetje slim nadenkt, kun je privacy ook uitnutten. Let maar op; ik zeg het je dat het gaat gebeuren. In ieder geval in het bedrijfsleven.

Mr. Rachel Marbus
@rachelmarbus op Twitter

ÉÉN ZEKERHEID IN ONZEKERE TIJDEN

We stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another. In its scale, scope, and complexity, the transformation will be unlike anything humankind has experienced before" (1). Niet alleen Klaus Schwab, oprichter en voorzitter van het World Economic Forum, voorspelt een ongekende technologische ontwikkeling, ook wetenschappers als Erik Vermeulen (2) en vader en zoon Susskind wijzen op de enorme impact die technologie al heeft en nog zal hebben op onze maatschappij.

Het recht kan deze ontwikkelingen niet meer bijhouden en dus moeten we aldus Vermeulen zoeken naar andere nieuwe regulerings-arrangementen. Vader en zoon Susskind waarschuwen ons dat robots het werk van vele professionals, waaronder juristen, zullen overnemen (3). Anderen zijn meer sceptisch en voorspellen dat het niet zo'n vaart zal lopen en technologie vooral ondersteunend en complementair aan de mens zal zijn (4). Wat de toekomst precies zal brengen, is lastig te voorspellen zonder glazen bol. Maar dat veranderingen snel gaan en een enorme impact hebben, kunnen we eenvoudig aflezen uit het succes van de 'frightfull five' en nieuwe bedrijfsmodellen zoals Uber en Airbnb en de ontwikkelingen in fintech.

Het is juist in deze turbulente en moeilijk voorspelbare tijden waarin een traditioneel reguleringsinstrument, een Europese Verordening, bescherming moet gaan bieden tegen de risico's van gegevensverwerking. En hoewel de meeste bedrijven en organisaties zich voornamelijk afvragen of de hoge boetes die in de Algemene Verordening Gegevensbescherming (AVG) zijn opgenomen ook daadwerkelijk opgelegd zullen worden, is dit slechts een van vele vragen en onzekerheden die de AVG met zich

meebrengt. De geschetste context, een tijd waarin technologie de maatschappij op ongekende wijze zal beïnvloeden, roept de vraag op: kan de AVG hier überhaupt een rol spelen? Nu al buigen wetenschap en praktijk zich over de vraag: hoe zijn beginselen van Big Data te verenigen met de beginselen van gegevensbescherming (5)? Ook roepen ontwikkelingen in Artificial Intelligence allerlei vragen op in relatie tot automatische beslissingen (6). Deze problemen ontstaan overigens niet alleen in relatie tot het Europese juridische kader, maar ook in relatie tot de wettelijke kaders van andere landen. Deze kaders zijn gebaseerd op vergelijkbare beginselen van gegevensbescherming, zoals de Canadese wet PIPEDA (7). Over de problematische verhouding tussen deze wet en het Internet of Things is zeer recent nog een artikel verschenen van Trosow, Taylor en Haman (8). Maar zelfs als we uitgaan van een toekomst waarin wel degelijk een belangrijke rol is weggelegd voor de AVG, zijn we niet verlost van uitdagingen en onzekerheden.

Interpretatie

Hoewel gekozen is voor een verordening om zo meer harmonisatie binnen Europa te bewerkstelligen, zal dit instrument zeker niet gaan leiden tot 28 identieke gegevensbeschermingsarrangementen. Ten eerste laat de verordening hiertoe veel te veel discretionaire ruimte aan de lidstaten. Ten tweede zal de interpretatie van de verordening, in eerste instantie door de nationale rechters, leiden tot de nodige verschillen. Zelfs binnen één land kunnen rechters van mening verschillen over de interpretatie van de rechten en plichten zoals neergelegd in de AVG. In Nederland werd dit recentelijk duidelijk in relatie tot het veel besproken 'recht op vergeten worden'. Twee rechters moesten zich buigen over de vraag: verwerkt Google strafrechtelijke persoonsgegevens wanneer de links die verschijnen na het intypen van een zoekvraag in Google, verwijzen naar bronpagina's waarop strafrechtelijke persoonsgegevens staan? Indien van oordeel dat er inderdaad sprake is van een verwerking van strafrechtelijke persoonsgegevens door Google, moet dit leiden tot het honoreren van een verzoek tot verwijdering van de link door Google. Hoewel een Rotterdamse rechter inderdaad oordeelde dat er sprake is van een dergelijke verwerking en Google dus sommeerde de links te verwijderen, komt een rechter uit Den Haag tot een compleet tegengesteld oordeel (9). Ook de opinies van de Artikel 29 Groep bieden niet altijd uitkomst bij de uitleg van de AVG. Hoewel over het recht op data-portabiliteit in 2017 een twintig pagina's tellende opinie is verschenen (10), is er nu al flinke kritiek op de gegeven uitleg omdat de reikwijdte van dit recht door de Artikel 29 Groep veel te ver zou zijn opgerekt (11).

Privacy by Design en Privacy by Default

En dan zijn er ook nog nieuwe rechten in de AVG waarvoor zowel de Artikel 29 Groep als de rechter nog nauwelijks enige richting hebben gegeven omtrent de nadere inkleuring hiervan. Zo kan bijvoorbeeld gewezen worden op de concepten 'Privacy by Design' en 'Privacy by Default'. Wat de reikwijdte en precieze verplichtingen zijn die volgen uit 'gegevensbescherming door ontwerp en door standaardinstellingen', zoals neergelegd in artikel 25 AVG, lijkt vooralsnog overgelaten aan onze eigen verbeelding. En juist hier wil ik, uit pure persoonlijk interesse, wat langer bij stilstaan. Naar mijn mening kunnen deze concepten namelijk van zeer grote waarde en betekenis zijn. In algemene zin is er consensus over de betekenis van de concepten, maar de vraag is: hoever reiken verplichtingen nu eigenlijk? Bij Privacy by Design gaat het om het 'inbakken' van privacy in het design van producten en diensten. Al in een vroeg stadium van ontwikkeling van een product of dienst moet worden nagedacht over het afdwingen van een behoorlijke en zorgvuldige omgang met persoonsgegevens, door middel van technische en organisatorische maatregelen. Het vereiste van Privacy by Default, als onderdeel van Privacy by Design, vereist dat bij een product of dienst de standaardinstellingen altijd zo privacy-vriendelijk mogelijk zijn ingesteld. In theorie klinkt dit veelbelovend en lijken deze beginselen zeker een bijdrage te kunnen leveren aan meer en betere bescherming van privacy: ingebouwde normen zijn over het algemeen moeilijker te negeren of te omzeilen

Dr. Colette Cuijpers is Associate Professor bij het Tilburg Institute for Law, Technology, and Society van de Universiteit van Tilburg. Ze is bereikbaar via cuijpers@uvt.nl.

dan de letter van de wet. Hoeveel er van deze beginselen verwacht kan worden, hangt echter af van hoe strikt deze beginselen in de praktijk toegepast moeten worden. Iets dat uiteindelijk af zal hangen van de interpretatie van de rechter. In de zaak FBI tegen Apple kun je je bijvoorbeeld afvragen of Privacy by Design en Privacy by Default een argument kunnen vormen tegen het inbouwen van een zogenaamde achterdeur in de technologie (12). Indien deze beginselen strikt uitgelegd worden, moet deze vraag naar mijn mening positief beantwoord worden. Andere voorbeelden waarbij een strikte uitleg van het beginsel van Privacy by Design en Privacy by Default echt verschil zouden kunnen maken, zijn bijvoorbeeld het afdwingen van ouderlijke toestemming bij kinderen en de ontwikkeling van een privacyvriendelijke Nederlandse elektronische identiteitskaart.

Zowel vanuit de wet als uit de algemene voorwaarden van bijvoorbeeld WhatsApp en Facebook volgt dat kinderen onder een bepaalde leeftijd niet zonder toestemming van de ouders gebruik mogen maken van deze diensten. De naleving van deze regel, uit eigen ervaring met twee (pre)pubers in huis, is een wassen neus. Er is geen enkele serieuze organisatorische of technische drempel ingebouwd die er toe leidt dat kinderen inderdaad alleen gebruik kunnen maken van deze diensten met toestemming van een ouder. Mijn vraag is: zou een dergelijke verplichting niet moeten volgen uit de beginselen van Privacy by Design en Privacy by Default? Ervan uitgaande dat zulke technische en organisatorische drempels in te bouwen zijn, zonder onredelijke inspanning en kosten voor de aanbieders van deze diensten.

In relatie tot de ontwikkeling van een elektronische identiteitskaart in Nederland, vraag ik mij af: hadden Privacy by Design en Privacy by Default niet moeten leiden tot de keuze van een systeem waarbij gebruik wordt gemaakt van attribute-based credentials (ABC)? Een technologie waarmee je op betrouwbare wijze alleen relevante eigenschappen (attributen, zoals 'ouder dan 18') van jezelf aan anderen kunt bewijzen, zonder onnodig persoonsgegevens vrij te geven (13). Hierbij gaat het om de vraag: hoeveel vrijheid laten de beginselen van Privacy by Design en Privacy by Default om te kiezen voor minder privacyvriendelijke oplossingen bij de ontwikkeling van producten en diensten, wanneer bekend is dat er reeds oplossingen bestaan die de privacy beter beschermen?

Hoewel deze bijdrage kort inzoomt op een aantal onzekerheden in relatie tot de AVG, wil ik graag afsluiten met een zekerheid uit persoonlijke overtuiging. Zolang de AVG van toepassing is, zal er meer dan genoeg werk zijn voor juristen met kennis en ervaring op het gebied van privacy en gegevensbescherming. Met alle uitdagingen, onzekerheden en de noodzaak tot afweging van een veelheid aan belangen, maak ik me voorlopig nog niet al te druk over het Susskind-scenario van robotisering in de juristerij.

Referenties

(1) K. Schwab, 'The fourth industrial revolution what it means, how to respond' (WEF 2016), http://bit.ly/1ULs72D, geraadpleegd 15 augustus 2017
(2) http://bit.ly/2eQ76VS
(3) Daniel Susskind en Richard Susskind, 'The Future of the Professions. How Technology Will Transform the Work of Human Experts' (Oxford University Press 2016)
(4) Frank A. Pasquale, 'Book Review: Automating the Professions?' (L.A. Review of Books, March 15, 2016; U of Maryland Legal Studies Research Paper No. 2016-21), http://bit.ly/2ePzasn, geraadpleegd 15 augustus 2017
(5) Bijvoorbeeld Moerel en Prins, 'Privacy voor de homo digitalis: Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van big data en Internet of Things' (Preadvies voor de Nederlandse-Juristenvereniging 2016), http://bit.ly/2vOnGvV, geraadpleegd 15 augustus 2017
(6) Wachter, Sandra and Mittelstadt, Brent and Floridi, Luciano, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (December 28, 2016). International Data Privacy Law, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2903469
(7) http://bit.ly/2cDg5a1
(8) S. Trosow, L. Taylor and A. Hanam, 'The Internet of Things: Implications for Consumer Privacy under Canadian Law', Working paper 2017, beschikbaar via: http://ir.lib.uwo.ca/lawpub/91/.
(9) Rechtbank Rotterdam 29 maart 2016, RBROT:2016:2395 en Rechtbank Den Haag 27 januari 2017, RBDHA:2017:264.
(10) http://bit.ly/2gs7BE2
(11) D. Meyer, European Commission, experts uneasy over WP29 data portability interpretation, zie: http://bit.ly/2pE0XCr
(12) C. Cuijpers en S. van Schendel, 'Data Protection by Design als argument in het FBI vs. Appledebat', in: 'Nieuwe technologieën in opsporing en veiligheidszorg', Justitiele Verkenningen 2016/3.
(13) Hierover valt meer te lezen op de website: https://privacybydesign.foundation/ waar verwezen wordt naar het project IRMA onder leiding van professor Bart Jacobs waarin gebruikt wordt gemaakt van deze technologie.

PRIVACY AWARENESS - PRIVACY CORE® (E-LEARNING)

Naast onze certificerende privacy trainingen en workshops, kunt u ook bij TSTC terecht voor een complete, bedrijfsbrede privacy awareness oplossing die bruikbaar en geschikt is voor audits. We maken hiervoor als exclusieve Nederlandse partner gebruik van het e-learning programma van IAPP (de internationale vakvereniging voor privacy professionals): Privacy Core®.

Privacy Core® bestaat uit een zeer groot aantal privacy awareness modules die u middels een licentie kunt integreren in uw eigen Learning Management System (LMS). Deze oplossing is SCORM compliant en daarmee toepasbaar in vrijwel elk LMS. Assessment functionaliteit biedt de beheerder de gelegenheid om de prestaties van medewerkers en teams te monitoren en via de bedrijfslicentie krijgt u toegang tot het complete aanbod van modules.
Privacy Core® modules zijn leverbaar in een groot aantal talen (waaronder een aantal in het Nederlands) en te customizen naar uw organisatie's branding.

IAPP maakt als vakvereniging bij de samenstelling van de modules gebruik van internationale FG's die bekend zijn met de specifieke problematiek binnen overheid, grote (internationale) organisaties, diverse afdelingen en AVG/GDPR eisen. U bent daarmee gegarandeerd van een kwaliteitsprogramma dat door experts is samengesteld en geschreven.

Waarom Privacy Awareness voor uw medewerkers?

Klant- of andersoortige persoonlijke data wordt door een groot aantal mensen in de organisatie ingezien, aangepast en verspreid. Om de risico's op onjuist gebruik of lekken te verkleinen is het van belang dat al deze medewerkers bewust zijn van wat privacy wet- en regelgeving van ze verwacht, wat gevoelige informatie is en aan welke grenzen zij gebonden zijn in hun dagelijkse werkzaamheden. Denk bijvoorbeeld aan uw afdeling marketing, klantenservice of Human Resources (HR).
Ook de AVG zelf legt letterlijk op dat deze medewerkers bewust gemaakt dienen te worden en opgeleid.

AVG/GDPR Artikel 39 lid 1 sub b geeft aan:
"De functionaris voor gegevensbescherming vervult ten minste de volgende taken:
b) toezien op naleving van deze verordening (....) met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;"

Privacy Core® modules

Het beschikbare aanbod modules wordt steeds verder uitgebreid en vertaald. We sturen u graag een actueel overzicht van de mogelijkheden. Een greep uit het aanbod:

- Waarom is privacy belangrijk?
- Wat is persoonlijke informatie?
- Hoe om te gaan met persoonlijke informatie?
- Herkennen en voorkomen van social engineering.
- Privacy by design.
- Vendor Management en privacy.
- Privacy beschermen in een call center.
- Privacy beschermen bij het inhuren en aannemen van personeel.
- Privacy afwegingen bij het monitoren van personeel.
- Klantinformatie verzamelen in het kader van marketing.
- Tracking technieken en privacy.
- Loyalty programma's en de bescherming van de privacy van deelnemende klanten.

Neemt u vooral contact met ons op voor verdere uitleg of een demonstratie van de mogelijkheden.

TSTC
ICT en Security Trainingen

e-PRIVACYCORE®
Privacy Training Essentials

WWW.TSTC.NL of telefonisch 0318-581480.

PRIVATE

The introduction of GDPR (General Data Protection Regulation) in 2018 in the EU raises some new challenges for those involved in controlling and processing personal data, but it is also a great case study in risk ownership and governance. It demonstrates some concepts and principles that have long been central in the SABSA way of thinking. In this article we shall explore those principles using the GDPR as an example.

SABSA has an approach to risk ownership that recognises different players with different roles. There is the risk owner, whose job it is to determine how much risk can be taken and who is ultimately accountable. There is the risk custodian, who is responsible for looking after the management of the risk on behalf of the owner, according to policies and procedures laid down by the owner, often in the form of a contract and service level agreement. There are also other third parties who have no say in the policies and have no part to play in the management of the risk, but who can be impacted by the outcome of risk-related events.

SABSA also embraces the concept of policy domains, each with a policy authority that owns the domain and makes security and risk management policy within the domain. A domain is sometimes physical in nature but more often logical, being a population of entities subject to the same security and risk management policy. These entities may be human individuals, groups of individuals, organisations or even machine devices. There is a hierarchy of domains – domains within domains, called sub-domains. The higher-level domains that contain sub-domains are known as super-domains. The super-domain / sub-domain model can be deeply nested, in which some domains are sub-domains to higher domains, but also super-domains of lower ones.

Let's see how all this relates to the GDPR model.

The highest-level super-domain is the EU itself, setting policy for personal data protection in the form of an EU Directive. Nation states within the EU are sub-domains. They are all subject to the policy guidelines in EU Directives. The development of these guidelines for personal data protection is actually carried out by a small sub-domain of the European Commission called the Article 29 Working Party, which comprises representatives from all the participating nation states and is run by the EC. However, the material (opinions, working documents, letters etc.) issued by the Article 29 Working Party reflects the views only of the working party, which has an advisory status and acts independently. They do not reflect the position of the EC, although the EC will develop its position based on the advice it receives. Authority behind any Directive comes from the EU Parliament. Each nation state is an autonomous lawmaker and must implement the Directive in national law, but there may be local variations according to cultural differences. Each nation state will also have a dedicated government office and officer with responsibility for policing compliance with the law. Already we see some complexity in the policy domain model.

GDPR talks about 'controllers' and 'processors'. The controller says how and why personal data is processed and the processor acts on the controller's behalf. So we see the roles as being risk owner (controller) and risk custodian (processor). However, the processor is also a risk owner because GDPR introduces specific legal obligations that significantly increase the accountability of the processor. In many cases the controllers and processors will be organisations of some considerable size, although the regulations apply equally to small and medium sized organisations, including sole traders and practitioners, where both the roles are combined in one party.

As before there are data subjects about whom the personal data has been collected. They are clearly 'at risk' from breaches in the regulations and could be heavily impacted by a breach, but they have no official authority for risk ownership or custody. It is worth noting that the definition of 'personal data' has also been extended under GDPR to include such items as IP addresses and other online identifiers, in line with the growth of the digital economy and the change in the ways that organisations collect information about people.

Some personal data is also classed as 'special categories of personal data' such as genetic information and biometric information in which the objective of the processing is to identify an individual uniquely for identification purposes. There are exceptions too, such as personal data collected under the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

So there we have a complex and deeply nested set of policy authorities that inherit policy from higher-level authorities and must implement those policies in their own lower-level policy-making activities. It is the strength of SABSA that it provides the tools with which to model such complexity, something that is essential in the development of security architectures.

The Attributer

AVG GAP-ANALYSE

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Op dat moment beschermen wij de privacy van onze gegevens niet meer op basis van de Nederlandse Wet bescherming persoonsgegevens (Wbp), maar op basis van een Europese privacyverordening.

Veel van de wetgeving die is opgenomen in de AVG is al onderdeel van de Wbp. Maar op diverse onderwerpen introduceert de AVG veranderingen of nieuwe verplichtingen. Zo hoeven persoonsgegevens verwerkende organisaties geen melding meer te doen van hun verwerking bij de Autoriteit Persoonsgegevens (voorheen het CBP), maar dienen zij wel zelf een verwerkingsregister bij te houden. De AVG verandert de (passieve) registratieplicht hiermee in een (gedetailleerdere en continu te onderhouden) documentatieplicht waarmee organisaties actief moeten aantonen de privacyregels na te leven. In eerste instantie naar zichzelf toe, maar bij controle ook richting de Autoriteit Persoonsgegevens (AP). Ook krijgen betrokkenen (de personen van wie gegevens worden verwerkt en beschermd) met het van toepassing worden van de AVG meer rechten. Bijvoorbeeld daar waar het om het verwijderen, bevriezen, corrigeren en porteren van de over hen verwerkte persoonsgegevens gaat. De gewijzigde rechten van de betrokkenen hebben tezamen met de documentatieplicht vermoedelijk de grootste impact op organisaties.

Checklist

Om een goede pragmatische start te maken met de nieuwe wetgeving is bij dit artikel een checklist gevoegd die voor een GAP-analyse kan worden gebruikt. Als je als organisatie reeds eerder aandacht besteedde aan de Wbp, weet je op basis van de checklist snel aan welke onderwerpen nog aandacht moet worden besteed bij het van toepassing worden van de AVG. Van deze checklist is op classity.nl ook een online versie beschikbaar, inclusief verwijzingen naar de relevante AVG-artikelen voor meer informatie. De resultaten zijn bij het gebruik van de site na het invullen als pdf te downloaden. Deze pdf bevat bij een zorgvuldige beantwoording ook meteen een goede start voor het opzetten van het verplichte verwerkingsregister.
Voldoe ik hiermee volledig aan de AVG? Nee. Het is niet mogelijk om met een enkele actie volledig aan de AVG te voldoen. De AVG vereist dat je controle hebt én houdt over je verwerking. Dit vereist een continue proces. Je voldoet dus niet aan de AVG als je eenmalig een activiteit voltooit, maar pas als je aan kunt tonen over een langere periode verantwoord met persoonsgegevens om te kunnen gaan.

Daarnaast is er geen 'one size fits all'-aanpak voor het voldoen aan de AVG. Hiervoor laat de wet teveel ruimte voor interpretatie. De wet zal de komende tijd verder gepolijst worden met zienswijzen (waarin de Europese toezichthouders uitleggen hoe zij de wet interpreteren) en jurisprudentie. Organisaties die een zeer behoudende koers varen, zullen de teugels op basis van deze ontwikkelingen in de toekomst mogelijk een beetje kunnen laten vieren. En organisaties die de wet heel vrij interpreteren moeten vermoedelijk naderhand een tandje bijzetten. Kortom, de GAP-analyse is bedoeld om een vliegende start te maken met de belangrijkste onderwerpen. Voor organisaties die nog niet zijn gestart, kan dit vermoedelijk geen kwaad. Want het is 25 mei 2018 voor we er erg in hebben.

Maarten Hartsuijker is consultant en ethisch hacker bij Classity en helpt organisaties in de volle breedte met informatiebeveiliging (en privacy). Maarten is tevens redacteur bij IB-Magazine. Hij is bereikbaar via m.hartsuijker@classity.nl.

Checklist

Doelstelling	GAP?	Benodigde actie	Benodigde resources
WETTELIJKE GRONDSLAG			
De wettelijke grondslag voor de verwerking is vastgesteld en vastgelegd (bijv.: vanuit overeenkomst, toestemming, gerechtvaardigd belang)			
Persoonsgegevens worden alleen verwerkt voor het doel waarvoor ze primair zijn afgestaan. Voor andere doelen is aanvullende ondubbelzinnige toestemming verkregen en vastgelegd, tenzij er andere grondslagen zijn die een verwerking rechtvaardigen (zoals een gerechtvaardigd belang of een wettelijke plicht). Bij het vragen van ondubbelzinnige toestemming zijn klanten goed geïnformeerd over waarvoor zij exact toestemming verlenen.			
DOCUMENTEREN			
Bij de verwerking van persoonsgegevens wordt geregistreerd: - wie er verantwoordelijk is; - wat het doel van de verwerking is; - welke categoriën betrokkenen er zijn (klanten/medewerkers/etc.); - welke categoriën persoonsgegevens er verwerkt worden (NAW/Financieel/locatie/etc.); - welke derden er betrokken zijn bij de verwerking, - of er persoonsgegevens worden doorgegeven aan 'derde landen' buiten de EU; - wat de bewaartermijnen zijn; - welke technische-organisatorische beschermingsmaatregelen er getroffen zijn.			
Bij het vragen van toestemming voor een specifieke verwerking wordt geregistreerd: - Waar toestemming voor is gegeven; - Waar en wanneer de toestemming is gevraagd; - Hoe de toestemmingsvraag is gesteld (en waarover is geïnformeerd).			
Indien de verwerking van bijzondere categorieën van persoonsgegevens (medisch/etniciteit/geloofsovertuiging/etc.) noodzakelijk en gerechtvaardigd is, is altijd een uitdrukkelijke (expliciete) toestemming gevraagd en vastgelegd (de uitdrukkelijke toestemming is tevens ondubbelzinnig).			
Er ligt vast voor welke gegevens een specifieke wettelijke bewaarplicht geldt. Deze bewaarplicht wordt bij een verzoek tot gegevenswissing niet uit het oog verloren.			
Van gegevens van kinderen is de toestemming van de ouder of voogd vastgelegd. Met alle partijen waarmee wordt samengewerkt is (in samenspraak met de juristen) een verwerkersovereenkomst afgesloten.			
De organisatie is transparant over de wijze waarop de persoonsgegevens worden verwerkt, o.a. door goede communicatie via het privacy statement.			
RECHTEN BETROKKENEN			
De gegevens die over een persoon verzameld zijn kunnen op verzoek binnen 4 weken worden gewist.			
Op verzoek kan binnen 4 weken een kopie van de over iemand verwerkte persoonsgegevens worden aangeleverd, inclusief de doelen waarvoor de gegevens verzameld zijn.			
Aan te leveren kopieën zijn in een uniform, voor machines leesbaar formaat, beschikbaar. Gegevensverwerkingen kunnen voor specifieke personen (binnen 4 weken) worden opgeschort op het moment dat daar recht op is ('blokkeren' van mutaties / bevriezen van de gegevens). Doorgegeven actualisaties of correcties van persoonsgegevens kunnen binnen 4 weken worden doorgevoerd.			
Voordat persoonsgegevens worden verstrekt (geldt ook voor: corrigeren/actualiseren/ verwijderen/blokkeren) wordt altijd de identiteit van de persoon die dit verzoekt vastgesteld. Hierbij wordt rekening gehouden met eventuele uitzonderingen en vastgelegde machtigingen.			

Doelstelling	GAP?	Benodigde actie	Benodigde resources
Verzoeken tot correctie/actualisatie/ verwijdering/opschorting van (het gebruik van) persoonsgegevens kunnen overal worden doorgevoerd, ook als verwerkingen aan andere afdelingen, organisatieonderdelen of derden zijn uitbesteed. Hierbij wordt rekening gehouden met verplichtingen uit andere / meer zwaarwegende regelgeving. Denk aan langere bewaarverplichting als gevolg van belastingwetgeving voor specifieke financiële gegevens.			
Binnen systemen en processen waarin geautomatiseerd wordt geprofileerd is het mogelijk om specifieke personen (die dit aangeven) van deze geautomatiseerde verwerking uit te sluiten. We spreken van profilering indien beslissingen enkel op een geautomatiseerde verwerking zijn gebaseerd (data analytics, big data).			
Er is gefaciliteerd dat een verstrekte toestemming voor het verwerken van persoonsgegevens door een persoon net zo makkelijk kan worden ingetrokken als dat hij is afgegeven.			
PRIVACY BY DESIGN / DEFAULT			
Persoonsgegevens verwerkende systemen en processen zijn privacy-vriendelijk ontworpen en standaard staan verwerkingsinstellingen (waaronder toestemmingen) zo privacy-vriendelijk mogelijk ingesteld. (privacy by design, privacy by default).			
Er is een PIA uitgevoerd indien de verwerkingsactiviteiten een hoog risico voor de betrokkenen met zich mee kan brengen. Dit is het geval indien: - nieuwe technologie wordt geïmplementeerd; - er grote hoeveelheden persoonsgegevens worden verwerkt; - er bijzondere persoonsgegevens worden verwerkt - wanneer er gebruik wordt gemaakt van geautomatiseerde besluitvorming en deze een aanzienlijk effect teweeg kan brengen voor betrokkenen.			
Gegevens worden niet langer dan noodzakelijk is bewaard.			
Indien het voor een specifieke verwerking niet noodzakelijk is dat gegevens tot op de persoon herleidbaar zijn, zijn anonimisatietechnieken toegepast.			
Gegevens die worden ingezet om de dienstverlening te optimaliseren, te testen en om producten te verbeteren, worden daarvoor geanonimiseerd. (Indien het met geanonimiseerde data niet mogelijk is om dit doel te bereiken kan het met de juiste privacywaarborgen ook te verantwoorden zijn om geen anonimisatie- maar pseudonimisatietechnieken in te zetten).			
Alle maatregelen die volgen uit het beveiligingsbeleid (en de daarvan afgeleide baseline) zijn toegepast.			
PRIVACYORGANISATIE			
Er is een privacy officer aangesteld met voldoende kennis en steun en mandaat van het bestuur om de verantwoordelijkheid voor het borgen van een passende bescherming van persoonsgegevens op zich te nemen.			
Het privacybeleid houdt rekening met de uitgangspunten uit de AVG en beschrijft hoe de privacyrollen en verantwoordelijkheden in de organisatie zijn belegd.			
Het beveiligingsbeleid houdt rekening met de uitgangspunten uit de AVG en beschrijft hoe de beveiligingsrollen en verantwoordelijkheden in de organisatie zijn belegd Er is vastgelegd op welke wijze een datalek kan worden afgehandeld. Er is vastgelegd op welke wijze er invulling wordt gegeven aan werkzaamheden die gerelateerd zijn aan betrokkenen die gebruik maken van hun rechten (inzien/verwijderen/muteren/bevriezen/bezwaar tegen profilering).			

PRIVACY EN INFORMATIEBEVEILIGING WORDEN SAMEN VOLWASSEN

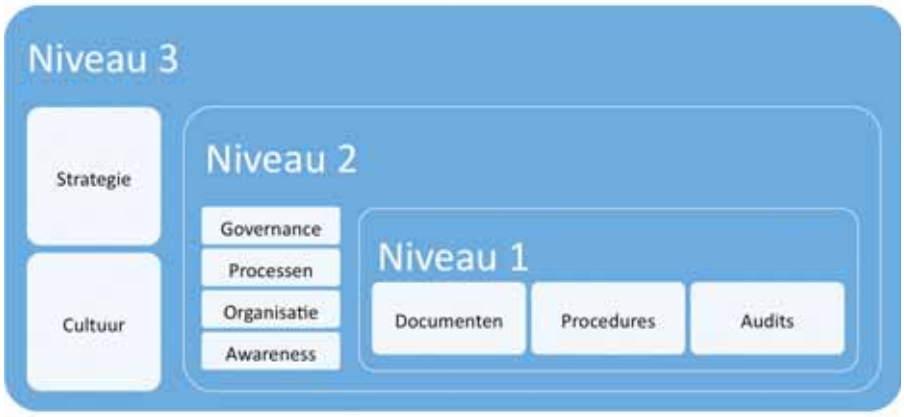
Veel lezers van dit blad zijn inmiddels drukdoende met de voorbereiding op 25 mei 2018, de datum waarop de Algemene Verordening Gegevensbescherming (AVG) van toepassing wordt. De hoogte van de mogelijke boetes, en de aansprakelijkheid voor bestuurders, is voor veel organisaties de voornaamste reden om het onderwerp privacy nu echt serieus op te pakken. De achterliggende reden van de AVG biedt organisaties echter ook een kans: een uniforme wetgeving voor heel Europa waarmee de open markt verder gestimuleerd zal worden.

De AVG benadrukt het belang van een goede beveiliging van persoonsgegevens, maar vooral: stelt het belang van de betrokkene centraal. De AVG legt ook nadruk op accountability en op het aantoonbaar in control zijn. Verantwoording kunnen afleggen over dit onderwerp is uiteraard nodig. Aantoonbaar in control zijn, stimuleert organisaties om de beheersing van de levensloop van data en de kwaliteit van data te verhogen. Een te sterke nadruk op in control zijn, kan helaas wel leiden tot de creatie van een papieren tijger. Een organisatie legt dan het zwaartepunt op allerlei controles om zeker te zijn dat er geen missers worden gemaakt. Deze nadruk op in control zijn en compliance kan leiden tot het invoeren van allerlei extra processen en overhead die de normale bedrijfsvoering kan gaan hinderen. Dit kan zeker ontstaan als voor privacy losstaande processen en functies worden ingericht. De aandacht voor privacy, waarbij informatiebeveiliging voor persoonsgegevens uitdrukkelijk onderwerp is, kan ertoe leiden dat door het gebrek aan middelen, tijd, geld enzovoorts de informatiebeveiliging van andere type gegevens minder aandacht kan krijgen.

Een organisatie kan immers maar een beperkt deel van haar middelen inzetten voor activiteiten die niet direct bijdragen tot de primaire activiteiten van de organisatie. De oplossing voor dit probleem is de additionele processen ten behoeve van de AVG zodanig in te richten dat optimaal gebruikgemaakt kan worden van reeds bestaande processen voor informatiebeveiliging en deze zoveel mogelijk in te bedden in de bestaande bedrijfsprocessen. In het verleden (WBP-tijdperk) werden informatiebeveiliging en privacy vaak als twee verschillende 'losstaande' disciplines gezien. Zowel privacy als informatiebeveiliging kunnen echter beschouwd worden als disciplines die zich richten op de beheersing van risico's geassocieerd met de kwaliteit van de informatievoorziening van een organisatie. Managementsystemen voor risicomanagement vormen daarmee een aanknopingspunt voor het samenvoegen van de activiteiten (integratie) voor deze disciplines. De integratie ondersteunt de volwassenheidsgroei van beide disciplines. Gebaseerd op dit uitgangspunt gaan we eerst in op de wijze waarop verschillende risicomanagementdisciplines kunnen worden geïntegreerd. We beschrijven vervolgens voor- en nadelen van integratie van privacy en informatiebeveiliging. Tenslotte gaan we in op een aantal praktische voorbeelden van integratie.

Modellen voor integratie

Privacy en Informatiebeveiliging zijn niet de enige risicomanagementdisciplines waar een organisatie aandacht aan moet besteden. Een organisatie van enige omvang zal aandacht besteden aan een waaier van risicomanagementdisciplines, zoals kwaliteitsmanagement, arbeidsomstandigheden, milieuzorg en informatiebeveiliging. Het is daarom niet verwonderlijk dat er nogal wat onderzoek gedaan is naar het integreren van managementsystemen voor het beheersen van risico's. Op



Figuur 1 – Niveaus van integratie.

basis van dergelijk onderzoek (1) zijn er vier niveaus van integratie te onderscheiden:

- Niveau 0: Geen integratie, losstaande managementsystemen.
- Niveau 1: Integratie op basis van structuurovereenkomsten veelal tot uitdrukking komend in de integratie van documenten, procedures en audits.
- Niveau 2: Integratie op basis van procesovereenkomsten veelal gebaseerd op de onderliggende PDCA-cyclus van de managementsystemen.
- Niveau 3: Integratie op basis van organisatie waarbij de onderliggende waarden en normen van de managementsystemen ingebed zijn in de strategie en de cultuur van de organisatie.

De niveaus 1 tot en met 3 zijn weergegeven in figuur 1.

De bovenstaande niveaus geven aan welke aspecten van managementsystemen kunnen worden geïntegreerd. Voor het uitvoeren van deze integratie zijn er in principe twee verschillende, voor de hand liggende, wegen:

- Eerst een afzonderlijk systeem opstellen voor een van de onderwerpen en deze vervolgens integreren met systemen voor de andere onderwerpen.
- Een enkel geïntegreerd systeem ontwikkelen en dit vervolgens implementeren.

De eerste vorm van integratie is veelal gebruikt door organisaties die vanwege commerciële of wettelijke redenen beginnen met een enkel onderwerp. Veel organisaties zijn bijvoorbeeld eerst begonnen met managementsystemen voor kwaliteit en hebben daar later milieuzorg en arbeidsomstandigheden aan toegevoegd.

De daadwerkelijke integratie van privacy en informatiebeveiliging kan uitgevoerd worden op basis van de achterliggende managementsystemen. Voor informatiebeveiliging ligt het gebruik van het managementsysteem beschreven in ISO 27001 (2) voor de hand. Voor privacy is er zover bekend nog geen breed gedragen standaard voor het te hanteren management-systeem. De managementsystemen opgesteld binnen ISO bevatten allen vergelijkbare elementen. De elementen uit ISO 27001 kunnen daarom gebruikt worden voor het identificeren van elementen die in een management-systeem aanwezig moeten zijn. De managementsystemen zijn daarnaast ook gebaseerd op een PDCA-cyclus. Die cyclus kan daarmee ook gebruikt worden voor integratie.

Joseph Mager, MISM, is Information Security Officer bij de Nederlandse Spoorwegen en vervult daarnaast een brugfunctie als Privacy Officer om synergie tussen privacy en informatiebeveiliging te creëren. Dit artikel is geschreven op persoonlijke titel en borduurt voort op zijn Master Thesis (5). Hij is bereikbaar via joseph.mager@ns.nl.

Renato Kuiper is security architect bij Verdonck, Klooster en Associates en vervult verschillende rollen op het snijvlak van architectuur, security en privacy. Hij is bereikbaar via renato.kuiper@vka.nl.

Figuur 2 - Managementsysteem en PDCA-cyclus.

Figuur 2 combineert die twee invalshoeken en geeft een aantal elementen van een managementsysteem weer in de PDCA-cyclus.

Het samenvoegen van de managementsystemen gebaseerd op de PDCA-cyclus leidt tot een integratie van niveau 2: de integratie op basis van procesovereenkomsten. De stap naar niveau 3, integratie op basis van organisatie, lijkt voor de meeste organisaties nog een brug te ver. Overigens kan door gebruik te maken van achterliggende waarden en normen het uiteindelijk eenvoudiger zijn om meerdere disciplines gezamenlijk naar niveau 3 te tillen. Veel risicomanagementdisciplines zijn gebaat bij het creëren van een open cultuur waarbij fouten in alle vrijheid kunnen worden besproken en een lerende organisatie die deze fouten gebruikt om haar processen te verbeteren. Hierbij wordt de PDCA-cyclus op het onderwerp ook daadwerkelijk doorlopen. Qua aanpak ligt het voor een organisatie die al ISO 27001 hanteert voor de hand om daar het managementsysteem voor privacy aan toe te voegen. Dit zal vooral in de IT-industrie, waar ISO 27001 veel wordt gebruikt, een geschikte aanpak zijn. Als ISO 27001 nog niet wordt gehanteerd, ligt het opzetten van een geïntegreerd systeem meer voor de hand. In beide gevallen dient de integratie projectmatig te worden opgepakt. Voor het opzetten van een dergelijk project kan het ISO-handboek voor de projectmatige integratie van managementsystemen (3) gebruikt worden.

Voor- en nadelen van integratie

Een organisatie kan ervoor kiezen om losstaande managementsystemen voor informatiebeveiliging en privacy in te voeren. De integratie bevindt zich in dit geval op niveau 0, geen integratie. Het voordeel van deze aanpak is dat er geen inspanning nodig is voor integratie en daarmee kunnen initieel de managementsystemen sneller worden opgezet. Deze aanpak kent echter ook nadelen. Er zullen daarna twee afzonderlijke systemen en bijbehorende processen in stand moeten worden gehouden. De informatie en rapportages over de bedrijfsprocessen en informatiesystemen benodigd voor beide disciplines zal twee keer worden opgesteld. De cultuurverschillen tussen beide disciplines worden niet aangepakt waarmee concurrentie om aandacht en middelen kan ontstaan. De genoemde aspecten leiden tot overhead in communicatie, tragere uitwisseling van informatie en verspilling van menselijk kapitaal. Het belangrijkste nadeel is dat medewerkers in de primaire processen van de organisatie opgezadeld worden met vergelijkbare activiteiten ten behoeve van het beheersen van de risico's voor beide disciplines.

Integratie op niveau 1 vereist dat bij het opstellen van documentatie en procedures structurele overeenkomsten voor beide disciplines worden gecreëerd. Denk hierbij bijvoorbeeld aan het creëren van documenten met eenzelfde opzet en indeling. Dit minimaliseert de inspanning die nodig is voor het opstellen van geïntegreerde documentatie en het bijhouden van administratie. Deze aanpak leidt tot een reductie van bureaucratie, waarmee additionele personeelskosten worden beperkt. De geïntegreerde documentatie vereenvoudigt daarnaast de uitvoering van interne en externe audits.

Een succesvolle integratie op niveau 2 vergt de betrokkenheid van het (top) management, gelijkvormige processen en het gebruik van gemeenschappelijke middelen, zoals informatiesystemen en mensen. Bij dit niveau van integratie is er aandacht voor en focus op de relatie tussen de beiden gebieden en de relatie van de gebieden met de bedrijfsvoering. Het belang van beide onderwerpen kan daarmee beter worden aangetoond. Daarnaast is het mogelijk prioriteiten te bepalen over beide gebieden heen en kunnen maatregelen worden geoptimaliseerd. De organisatie en verantwoordelijkheden kunnen op een enkele plek worden gedefinieerd. Een mogelijk obstakel voor integratie is dat de benodigde onafhankelijkheid van de functionaris gegevens-bescherming (FG) wellicht niet kan worden gerealiseerd. De privacy-rol ingevuld door een FG is een onafhankelijke rol.

De FG moet zich vrijelijk kunnen bewegen in de organisatie, geniet ontslagbescherming en rapporteert aan het hoogste managementniveau of zelfs aan de AP (Autoriteit Persoonsgegevens). Daarnaast vergt dit niveau van integratie een team waarin beide disciplines afdoende vertegenwoordigd zijn en teamleden voldoende affiniteit hebben met de andere discipline. Integratie van de CISO-rol en FG biedt grote voordelen voor informatiebeveiliging, immers een van de belangrijkste privacy principes gaat over de bescherming van de persoonsgegevens. Op dat vlak, lees principe, is maximale integratie te realiseren. Voor alle andere privacyzaken (lees basisprincipes), heeft een CISO ook baat bij bijvoorbeeld de transparantie over de gegevensverwerking.

Integratie in de praktijk

Het model voor integratie zoals weergegeven in figuur 1 en de onderdelen van het ISMS zoals weergeven in figuur 2 bieden aanknopingspunten voor integratie. Een aantal aspecten komen we daarvan al in de praktijk tegen en beschrijven we hieronder. Andere aspecten kunnen gebruikt worden om aanvullende kansen voor integratie te identificeren en te realiseren.

Governance en strategie

Met het model van een managementsysteem als uitgangspunt begint integratie van privacy en informatiebeveiliging aan de top. De besturing van beide disciplines is op het hoogste niveau van de organisatie belegd. Gezien het toenemend belang van informatiebeveiliging en privacy vormt dit aspect tegenwoordig geen al te grote uitdaging meer. Hierbij geldt wel dat de bestuurders moeten inzien dat informatiebeveiliging geen IT-feestje is. Het onderwerp risicomanagement moet in de volle breedte (lees Enterprise Risk Management) als portefeuille belegd worden in de Raad van Bestuur (RvB). De RvB bekrachtigt principiële uitspraken over het nut en de noodzaak van beide onderwerpen, zoals ze dit ook doet voor de uitgangspunten voor maatschappelijk ondernemen van de organisatie. Een zorgvuldige omgang met persoonsgegevens en een goede beveiliging is immers een maatschappelijke verplichting van elke organisatie, zoals ook naar voren komt in het rapport over zorgplicht opgesteld door Cyber Security Raad (4). Deze situatie kan dan ook alleen werken vanuit de inherente behoefte om zorgvuldig om te gaan met persoonsgegevens met een risico gebaseerde aanpak als uitgangspunt en geen compliance gedreven aanpak, het moetje…

Organisatie

De organisaties voor informatiebeveiliging en privacy kunnen geïntegreerd worden. Het is daarbij nodig om het betreffende team zo samen te stellen dat recht gedaan wordt aan de kennis en vaardigheden die nodig zijn voor beide disciplines. De medewerkers gericht op privacy zullen veelal een juridische achtergrond hebben. Enig begrip en kennis van IT is daarbij zeer zinvol, en in feite onontbeerlijk. De medewerkers gericht op informatiebeveiliging zullen veelal een IT-achtergrond of management-achtergrond hebben. Hierbij is uiteraard aanvullende kennis op juridisch gebied onontbeerlijk. Idealiter bevat het team ook een of meerdere personen die thuis zijn in beide disciplines, misschien vraagt dat om een SPA (Security en Privacy Architect). Zij zijn in staat om bruggen te bouwen tussen de disciplines en met de business en bestuurders en spelen een cruciale rol in opzetten van een enkel geïntegreerd managementsysteem.

Processen

Privacy en informatiebeveiliging kunnen beide beschouwd worden als risicomanagementdisciplines. Het ligt daarom voor de hand om de risicomanagementprocessen van beide disciplines te integreren. Een van de randvoorwaarden hiervoor is dat er ook nagedacht is over de risicobereidheid op beide gebieden. Informatie-beveiliging maakt vaak gebruik van een Business Impact Assessment (BIA) om de waarde van de informatie voor de organisatie te bepalen. Hierbij wordt nagegaan wat de gevolgen voor de bedrijfsvoering zijn als de informatie niet beschikbaar, juist, actueel of volledig (integer) is of de vertrouwelijkheid wordt geschonden. In de AVG staat het uitvoeren van een Privacy Impact Assessment (PIA) voor risicovolle verwerkingen centraal. Een dergelijke PIA is vaak ook benodigd als de verwerking plaatsvindt op basis van de grondslag van gerechtvaardigd belang. In die situatie moeten de belangen van de organisatie afgewogen worden tegen de belangen van de betrokkenen, de personen van wie de gegevens worden verwerkt. Het belang van de informatie voor de bedrijfsvoering wordt al bepaald in de BIA. Ten behoeve van de PIA moet dan nog aanvullend de belangen van de betrokkenen worden bepaald.

Nadat de BIA en PIA opgesteld zijn, kan door middel van een risicoanalyse bepaald worden welke maatregelen genomen dienen te worden om de risico's afdoende te beheersen. De AVG noemt expliciet beveiliging van de persoonsgegevens als uit te voeren maatregelen. Logischerwijs dragen de maatregelen genomen op basis van de risicoanalyse voor informatiebeveiliging daarmee bij aan de maatregelen voor privacy. Aanvullend kunnen

maatregelen vanuit de AVG ertoe leiden dat er minder zware maatregelen voor het beveiligen van persoonsgegevens nodig zijn. Indien bijvoorbeeld dataminimalisatie wordt toegepast, wordt de impact van het uitlekken van persoonsgegevens verlaagd. Deze verlaging van impact geldt daarbij ook nog eens voor de gevolgen voor de betrokkenen en voor de gevolgen voor het bedrijf.

Integratie van de BIA en PIA is mogelijk. Een organisatie is vrij om te kiezen op welke wijze zij het proces voor het bepalen van informatiebeveiligingsrisico's en risico's met betrekking tot verwerking van persoonsgegevens uitvoert. In de AVG worden wel minimale eisen gesteld, bijvoorbeeld dat er onder andere een risicoafweging gedaan moet worden. Beide processen zijn simpel te integreren, maar moeten wel met brede kennis ter ondersteuning integraal met de business worden gedaan. De business wordt nu voor een nieuw informatiesysteem slechts eenmaal bevraagd op zowel de BIA- als de PIA-vragen.

Het risicomanagement van beide disciplines moet daarnaast ook ingebed worden in de bedrijfsprocessen. Omdat beide disciplines risico's in de informatievoorziening van de organisatie behandelen, is het zinvol om aan te sluiten bij de ontwikkelprocessen van deze informatie-voorziening. Als er een standaard voortbrengingsproces is met bijvoorbeeld Quality Gates, kan zowel het bepalen van de maatregelen als de controle op implementatie daarvan in dit proces worden ingebed. Bij een organisatie waar informatiemanagement goed is ingevoerd, wordt daarnaast op dit niveau aangesloten op de informatie-planning. Het is zoals altijd zinvol om zo vroeg mogelijk aangesloten te zijn op nieuwe ontwikkelingen. Op deze wijze kan het beste invulling worden gegeven aan het principe van privacy by design.

Een andere mogelijkheid voor integratie van processen betreft het afhandelen van incidenten. Het proces voor informatiebeveiligingsincidenten is vrij eenvoudig uit te breiden met een proces voor het melden van datalekken. De uitbreidingen richten zich op het bepalen van de impact van een datalek voor betrokkenen, het op tijd melden bij de AP, de juistheid van de melding en de afweging of er gemeld moet worden bij de betrokkenen. De integratie betreft overigens niet enkel het melden en afhandelen van incidenten. Deze strekt zich uit tot de evaluatie, de check- en act fase, van een managementsysteem van incidenten en op basis daarvan het bijstellen van maatregelen. Op deze wijze wordt pas echt een meerwaarde gecreëerd voor de bedrijfsvoering.

Awareness en communicatie

De belangrijkste aspecten waarop de disciplines kunnen integreren zijn bewustwording, opleiding en communicatie. Deze aspecten dragen bij aan de stap naar integratie op niveau 3. Door het belang van beide aspecten te benadrukken, kan het zorgvuldig omgaan met de persoonsgegevens onderdeel gaan uitmaken van de cultuur van de organisatie. Het is daarbij van belang dat de activiteiten op deze aspecten zorgvuldig op elkaar afgestemd zijn en uiteraard toegesneden op de verschillende doelgroepen in de organisatie.

Conclusie

Invoering van de AVG biedt kansen om privacy en informatiebeveiliging verder te integreren. In de praktijk gebeurt dit al binnen veel organisaties. Door gebruik te maken van de achterliggende managementsystemen kunnen ook andere mogelijkheden voor integratie worden geïdentificeerd en gerealiseerd. Een organisatie die gebruikmaakt van alle mogelijkheden, zal in staat zijn om de risico's op beide gebieden efficiënter te beheersen. De benodigde inspanning zal uiteindelijk lager zijn dan wanneer beide gebieden afzonderlijk worden ingericht. Daarnaast zal de bedrijfsvoering minder belast worden. Afhankelijk van de rol en ophanging van zowel de CISO als de FG is dit eenvoudig of lastiger in te voeren.
Informatiebeveiligingsmaatregelen die getroffen worden op basis van de AVG worden gezien de compliancedruk van mei 2018 nu sneller geïmplementeerd. De CISO kan zich in een later stadium daarom gaan focussen op de beveiliging van andere typen informatie: financieel, intellectueel eigendom en operationele IT.

Als privacy gezien wordt als een zorgplicht om goed om te gaan met gegevens van betrokkenen en niet als een moetje, en er wordt er een risico gebaseerde aanpak voor privacy als basis gebruikt, dan is deze goed te integreren met de PDCA-cyclus van informatiebeveiliging. Zo kunnen beide disciplines gezamenlijk in volwassenheid groeien.

Referenties

(1) How integrated are environmental, quality and other standardized management systems. An emperical studgy. Merce Bernardo et al. 2008, Journal of Cleaner Production.
(2) ISO. ISO 27001:information security management system, www.iso.ch, 2013.
(3) The integrated use of system management standards. sl : Internatial Organisation for Standardization, 2008.
(4) CSR. Ieder bedrijf heeft digitale zorgplichten. sl : Cyber Security Raad, 2017.
(5) Mager, Joseph. Het succes van risicomanagement. 2010.

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

People matter, results count.

Transform uncertainty into trust

Intelligent Cybersecurity Services

Find out more:

www.nl.capgemini.com/oplossingen-voor-cyberbeveiliging

DO'S & DONT'S BIJ PROFILING

In onze gedigitaliseerde samenleving worden steeds grotere hoeveelheden en soorten data gegenereerd en verzameld. Samen met de geautomatiseerde wijze van informatieverwerking via software zorgt de exponentiële groei van Big Data-analyses voor uiteenlopende en veelal vergaande toepassingen (1). Profilering is een van die toepassingen.

De geavanceerde technologische ontwikkelingen maken het voor bedrijven en organisaties mogelijk om aan de hand van verzamelde, gecombineerde en geanalyseerde (persoons)gegevens individuele (risico)profielen op te stellen, verbanden te leggen en voorspellingen te doen die gebruikt kunnen worden voor commerciële doeleinden of als een vorm van risicomanagement (2). Deze gerichte profilering kan bijzonder efficiënt en waardevol zijn, maar kan tevens grote risico's met zich meebrengen voor de rechten en vrijheden van betrokken natuurlijke personen, denk aan stigmatisering en discriminatie. Door de gevoeligheid van dit soort thema's speelt dit onderwerp een zeer belangrijke rol in de maatschappelijke discussie rondom privacy en staat dit onderwerp hoog op de agenda's van de toezichthouders. Om de betrokkenen te beschermen, zijn ruim twintig jaar geleden in de Richtlijn 95/46/EG (Privacyrichtlijn) en later in de Wet bescherming persoonsgegevens (Wbp) regels vastgelegd aangaande individuele besluiten die op geautomatiseerde wijze tot stand komen. De term profilering als zodanig is echter pas geïmplementeerd onder de Algemene Verordening Gegevensbescherming (AVG), die vanaf 25 mei 2018 van toepassing wordt en dan de Privacyrichtlijn en de Wbp gaat vervangen. In dit artikel sta ik stil bij het wettelijke kader voor de geautomatiseerde individuele besluitvorming, in het bijzonder profilering onder de AVG, en welke aandachtspunten dit kader met zich meebrengt voor de organisaties.

Huidig wettelijk kader

Ten aanzien van geautomatiseerde individuele besluiten voorzien zowel de Privacyrichtlijn als de Wbp al in het regelgevende kader. De hoofdregel is daarbij dat geautomatiseerde individuele besluiten die bestemd zijn om een beeld te krijgen van (bepaalde aspecten van) iemands persoonlijkheid (3) verboden zijn indien aan die besluiten voor een natuurlijke persoon:

1) rechtsgevolgen zijn verbonden, of
2) deze persoon in aanmerkelijke mate treffen (4).

Een dergelijk besluit is alsnog toegestaan indien het besluit, met passende beschermmaatregelen omkleed,

a) wordt genomen in het kader van een overeenkomst of
b) zijn grondslag vindt in een wet waarin beschermende maatregelen zijn vastgelegd.

In beide situaties moet de verantwoordelijke aan de betrokkene kunnen uitleggen waarom zijn gegevens geautomatiseerd worden verwerkt (5).

Nieuw wettelijk kader: wat wijzigt er?

Definitie

De AVG introduceert in artikel 4 lid 4 een vaste definitie van de term profilering (waarbij de reikwijdte van de bepaling ten opzichte van Privacyrichtlijn is uitgebreid): "elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen".

Met andere woorden: profilering gaat over het evalueren van geautomatiseerd opgestelde persoonlijke profielen met het doel om voorspellingen te doen en beslissingen te

nemen over iemands voorkeuren, gedragingen enzovoorts.

Hoofdregel en uitzonderingen

Wat betreft de profilering staat het belangrijkste wettelijke kader in artikel 22 lid 1 AVG. Dit artikel borduurt voort op de regels over de geautomatiseerde individuele besluiten uit de Privacyrichtlijn. Het biedt het recht 'niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.' Dat houdt in dat:

1) de verwerking die niet uitsluitend geautomatiseerd gebeurt buiten de werking van artikel 22 AVG valt, en dat
2) besluitvorming gebaseerd op profilering is toegestaan zolang de betrokkene daar geen rechtsgevolgen van ondervindt noch in aanmerkelijke mate wordt getroffen. Wat een dergelijke rechtsgevolg concreet inhoudt en hoe de aanmerkelijke mate precies wordt gemeten blijkt niet uit de wet. Ook de AVG licht deze twee begrippen summier toe door zich te beperken tot twee voorbeelden: de automatische weigering van een online ingediende kredietaanvraag of een verwerking van sollicitaties via internet zonder menselijke tussenkomst (6).

De hoofdregel kent drie uitzonderingen, waarbij profilering dus wel mag:

a) de uitdrukkelijke toestemming van de betrokkene;
b) als het noodzakelijk is voor de totstandkoming of uitvoering van een overeenkomst en
c) toestemming voortvloeiend uit een wet (7).

In de eerste twee gevallen moet de verantwoordelijke passende maatregelen nemen om de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene te beschermen. Van de genoemde uitzonderingen is alleen de eerste nieuw.

Profilering op basis van bijzondere persoonsgegevens (denk aan gegevens over iemands ras of etnische afkomst, politieke of religieuze overtuigingen, gezondheid, seksuele geaardheid of strafrechtelijk verleden (8)) mag alleen

1) met uitdrukkelijke toestemming, of
2) omdat verwerking noodzakelijk is door zwaarwegend algemeen belang, én passende maatregelen zijn getroffen om de grondrechten en de fundamentele belangen van de betrokkene te beschermen.

De AVG zegt overigens niet hoe in situatie van zwaarwegend algemeen belang de evenredigheid met het doel dient te worden gewaarborgd en hoe de wezenlijke inhoud van het recht op bescherming van persoonsgegevens kan worden geëerbiedigd.

Let op als het gaat om besluitvorming over kinderen in het kader van marketing en profilering. Het komt erop neer dat kinderen specifiek worden beschermd en daarom niet aan profilering mogen worden onderworpen (9).

Rechten betrokkene

De beginselen van behoorlijke en transparante verwerking nemen een centrale plaats in in de AVG. De transparantie en de zeggenschap over de manier waarop persoonsgegevens worden verwerkt, dragen bij aan de bescherming daarvan. In het kader van profilering voorziet de AVG, naast de bestaande rechten van betrokkenen (10), in een aantal aanvullende rechten:

Zo heeft de betrokkene het recht:

a) op specifieke informatie,
b) op menselijke tussenkomst van de verantwoordelijke,
c) om zijn standpunt kenbaar te maken,
d) om uitleg over de na een dergelijke beoordeling genomen besluit te krijgen en
e) om te allen tijde (11) het besluit aan te vechten (12).

De expliciete vermelding in de AVG dat de betrokkene recht heeft om bezwaar te maken tegen profilering is nieuw ten opzichte van de Privacyrichtlijn. Dit bezwaar mag alleen worden afgewezen indien sprake is van dwingende gerechtvaardigde gronden voor de profilering die zwaarder wegen dan de belangen van de betrokkene. Dat geldt echter niet in geval van profilering ten behoeve van direct marketing (13).

Verder geldt dat de betrokkene bij het verzamelen van zijn gegevens of binnen een redelijke termijn dient te worden

Ksenia Kondratova is bedrijfsjurist bij KPN. Zij is bereikbaar via ksenia.kondratova@kpn.com.

geïnformeerd over het (bestaan van) profileren, de onderliggende logica en de verwachte gevolgen daarvan voor de betrokkene (14). Degene die profileert moet dus helder kunnen uitleggen wat, waarom en hoe hij verwerkt.

Plichten verantwoordelijke

De verantwoordelijke heeft de verplichting om een voor de betrokkene behoorlijke en transparante verwerking te garanderen. Hij moet:

- de betrokkene goed informeren;
- de passende wiskundige en statistische procedures gebruiken;
- technische en organisatorische maatregelen nemen;
- zorgen dat de gegevens kloppen;
- zorgen voor goede bescherming van de gegevens;
- voorkomen van discriminerende gevolgen voor de betrokkene.

Als extra verplichting geldt dat in geval van profilering of als er sprake is van verwerking van bijzondere persoonsgegevens (en voor overige grote verwerkingen) een zogenaamde gegevensbeschermings effectbeoordeling (DPIA) moet worden gemaakt (15).

Conclusie

Profilering waarbij profielen worden opgesteld, correlaties worden gelegd, voorspellingen en beslissingen worden gemaakt op basis van iemands persoonlijke kenmerken kan waardevol zijn. Zo kan de betrokkene aantrekkelijke persoonlijke aanbiedingen ontvangen, kan de overheid misdaden voorspellen en kan een verzekeraar een passende premie berekenen. Indien besluiten worden genomen op basis van profilering is het echter niet zonder risico voor de privacy van betrokkenen. Geautomatiseerde verwerking en vooral de besluitvorming over profielopstelling gebeurt vaak door een computer zonder menselijke tussenkomst. Daardoor bestaat de kans op bijvoorbeeld een onjuist of achterhaald profiel of kan het incorrect toerekenen van bepaalde eigenschappen of gedragingen aan iemand hem of haar stigmatiseren.

Om natuurlijke personen te beschermen, zijn de regels rondom de profilering expliciet vastgelegd in de AVG. De AVG verschaft een groot aantal (nader uitgewerkte) regels als het gaat om profilering. Bijvoorbeeld de definitie, aanvullende regels voor bijzondere gegevens en voor besluitvorming over kinderen en de uitgebreide rechten van de betrokkene. Ik wijs daarbij in het bijzonder op het recht op bezwaar, dat ondanks de eerder verleende uitdrukkelijke toestemming kan worden ingeroepen. De AVG heeft wat dat betreft een grote optimaliseringsslag gemaakt ten opzichte van de Privacyrichtlijn. De rechten en de zeggenschap van betrokkenen bij profilering zijn enorm verbeterd ten opzichte van de huidige wetgeving. Tegelijkertijd roept de wet nog steeds vragen op. Immers, feit blijft dat de niet uitsluitend op geautomatiseerde verwerking gebaseerde besluiten buiten artikel 22 AVG vallen. Dit is een belangrijk punt omdat de desbetreffende regels relatief makkelijk kunnen worden omzeild door de verwerking niet uitsluitend geautomatiseerd in te richten.

Een ander punt van onduidelijkheid is de concrete invulling van de vereisten van artikel 22 AVG waarin de hoofdregel voor de profilering is neergelegd. Ondanks de introductie van een expliciete definitie blijft de formulering van de hoofdregel vaag (16). Je kan je namelijk afvragen om welke concrete aan een besluit verbonden rechtsgevolgen het gaat en hoe de aanmerkelijke mate, waarmee de betrokkene bij profilering eventueel wordt getroffen, gemeten wordt. Beperken dergelijke rechtsgevolgen en ernstige beïnvloedingen zich tot de situaties van kredietverstrekking en het personeelsmanagement of zijn andere gevallen denkbaar? Deze twee voorbeelden lijken opnieuw te suggereren dat het recht om niet te mogen onderwerpen aan profilering ontkracht kan worden door het element van uitsluitend geautomatiseerde verwerking weg te halen. Bij gebrek aan heldere richtlijnen (17) blijft er dus ruimte over voor interpretatie. Hoe bedrijven en organisaties deze interpretatieruimte in de praktijk gaan benutten, zal moeten blijken.

Met het oog op een behoorlijke en transparante verwerking zijn de plichten van de verantwoordelijke onder de AVG verzwaard. Om de behoorlijke en transparante verwerking te kunnen borgen, dient de verantwoordelijke veel procesevaluaties en -wijzigingen door te voeren en moet hij blijven toetsen aan de niet altijd eenduidige normen van de AVG. Daarmee zijn er in ieder geval meer kaders, spelregels en definities gegeven, die enerzijds het individu beter moeten gaan beschermen en anderzijds organisaties in de gelegenheid stellen hun profileringsactiviteiten te ontplooien.

De uitleg van de nieuwe regels rondom profilering en de belangenafweging die daarbij moet worden gemaakt, zou wat mij betreft niet gestuurd moeten worden door het willen voorkomen van een boete, maar daarbij zou ook de ethische kant van profilering voor ogen moeten worden gehouden.

Aanbevelingen

Indien uw bedrijf of organisatie geautomatiseerde besluitvorming, waaronder profilering, toepast of laat toepassen in het kader van de verwerking van (bijzondere) persoonsgegevens is het van belang om te onderzoeken in hoeverre de interne (IT-)processen voldoen aan de vereisten van de AVG en deze, zo nodig, tijdig aan te passen. Hieronder volgt een opsomming van aanbevelingen die als checklist kan worden gebruikt.

- Ga na of de huidige geautomatiseerde besluitvorming en profilering rechtsgevolgen hebben voor de

betrokkene dan wel hem in aanmerkelijke mate (kunnen) treffen;
- Zo ja, implementeer in de processen (inclusief de registratie, afhandeling en vastlegging verzoeken alsook gelegenheid tot menselijke interventie), de mogelijkheid voor de betrokkene om zijn rechten uit te oefenen door:
  - menselijke tussenkomst te verkrijgen; en
  - zijn standpunt te uiten; en
  - het besluit aan te vechten
- Stel vast of beroep kan worden gedaan op de uitzonderingen van artikel 22 AVG:
  - noodzaak voor het aangaan of uitvoeren van een overeenkomst; of
  - een wettelijke bepaling die dat toelaat; of
  - een uitdrukkelijke toestemming van de betrokkene.
- Als sprake is van bovengenoemde uitzonderingen geldt dat deze besluiten geen betrekking mogen hebben op kinderen en niet gebaseerd mogen zijn op de (verwerking van) bijzondere categorieën van persoonsgegevens.
- Tenzij:
  - de betrokkene uitdrukkelijke toestemming heeft gegeven; of
  - de verwerking noodzakelijk is om redenen van algemeen publiek belang; en
  - er passende maatregelen ter bescherming van de gerechtvaardigde belangen van de betrokkene zijn genomen.
- Neem als verantwoordelijke de navolgende maatregelen in acht bij het verwerken van persoonsgegevens voor profileringsdoeleinden (privacy by design en privacy by default):
  - Voer vóór de verwerking een DPIA uit wanneer de geautomatiseerde individuele besluitvorming en in ieder geval profilering, gelet op de aard, de omvang, de context en de doeleinden daarvan, waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen;
  - Hanteer voor het profileren passende wiskundige of statistische procedures;
  - Introduceer passende technische en organisatorische maatregelen in processen om onjuistheden te corrigeren en het risico op fouten te minimaliseren;
  - Voorkom dat de verwerking voor de betrokkene discriminerende gevolgen zou hebben op grond van ras of etnische afkomst, politieke overtuiging, godsdienst of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische of gezondheidsstatus, of seksuele gerichtheid;
- Zorg ervoor dat de verwerking behoorlijk en transparant is:
  - Informeer de betrokkene over het bestaan van profilering bij het verzamelen van de gegevens bij de betrokkene of, indien de gegevens uit een andere bron zijn verkregen, binnen een redelijke termijn, die afhangt van de omstandigheden van het geval;
  - Voorzie de betrokkene van alle noodzakelijke en nuttige informatie omtrent profilering, zoals de onderliggende logica en het belang en de verwachte gevolgen van de verwerking;
  - Geef de betrokkene nadere uitleg omtrent het genomen besluit en implementeer de mogelijkheid om te allen tijde bezwaar in te stellen tegen het besluit en op verzoek de op profilering gebaseerde verwerking te beëindigen.

Referenties

(1) Working Party 29, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013, p. 35 e.v.
(2) www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-en-tv/profiling.
(3) Zoals beroepsprestatie, kredietwaardigheid, betrouwbaarheid, gedrag, enz.
(4) Artikel 15 lid 1 Privacyrichtlijn, artikel 42 lid 1 Wbp.
(5)Artikel 42 lid 2,3 en 4 Wbp en artikel 15 lid 2 Privacyrichtlijn.
(6) R.o. 71 AVG.
(7) Onder meer ten behoeve van de controle en voorkoming van belastingfraude en -ontduiking overeenkomstig de regelgeving, normen en aanbevelingen van de instellingen van de Unie of de nationale voor oversight bevoegde instanties, en om te zorgen voor de veiligheid en betrouwbaarheid van een dienst die door de verwerkingsverantwoordelijke wordt verleend, zie r.o. 71 AVG.
(8) Artikel 22 lid 4, artikel 9 en r.o. 71 AVG.
(9) R.o. 38 en 71 AVG.
(10)Denk o.a. aan het voorafgaand informeren over het feit dat er verwerking plaatsvindt en van de doeleinden daarvan, volledigheidshalve zie Hoofdstuk 3 AVG.
(11)Artikel 21 lid 1 AVG.
(12) Artikel 22 lid 3 AVG en r.o. 71.
(13) Artikel 21 lid 2 en 3 AVG.
(14) Artikel 13 lid 1 (f) en artikel 15 lid 1 (h) AVG, en r.o. 60 en 61.
(15) R.o. 91 AVG. Voor DPIA zie artikel 35 AVG.
(16) Deze conclusie wordt gedeeld door B. van der Slot, De nieuwe consumentenrechten in de Algemene verordening gegevensbescherming: vergeten worden, data-portabiliteit en profilering, Tijdschrift voor Consumentenrecht en handelspraktijken 2012-6, p. 257.
(17) Volgens de AVG dient de Working Party 29, die onder de AVG het Europees Comité voor gegevensbescherming gaat heten, de mogelijkheid te krijgen om met betrekking tot profilering nadere richtsnoeren op te stellen, zie r.o. 72 AVG.

Interview Paul Samwel en Reinder Wolthuis

SAMEN TEN STRIJDE

Tegen 'het onheil dat nooit zou komen'

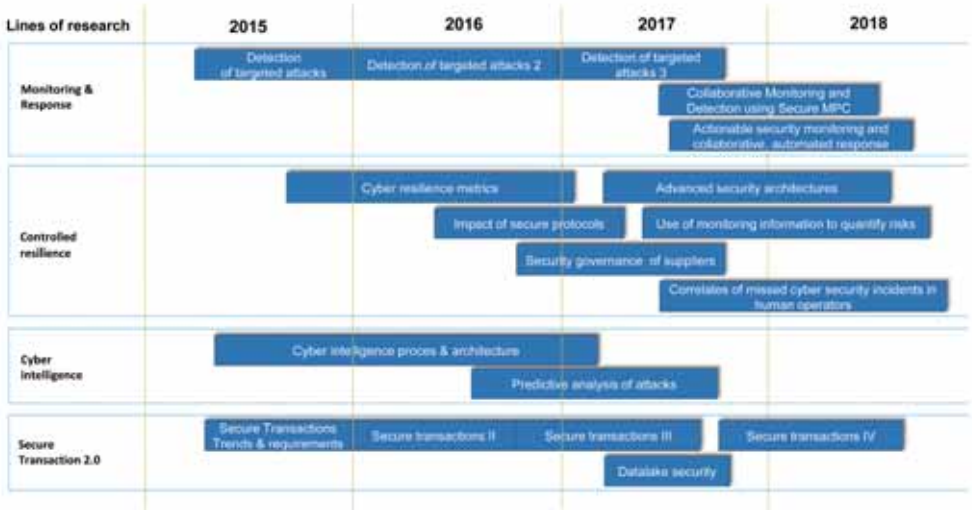
Gijzelsoftware legde in juni tientallen bedrijven wereldwijd plat. Een aanval die grote gelijkenis vertoonde met de grote Wannacry-aanval ruim een maand eerder. Aanvallen die laten zien hoe kwetsbaar we als maatschappij zijn voor cyberaanvallen. IB-Magazine sprak hierover met Paul Samwel, hoofd security architectuur & -innovatie bij Rabobank, en Reinder Wolthuis, senior projectmanager en consultant cybersecurity van TNO. "Waren we jaren geleden als security-specialisten nog weleens bezig met 'het ons wapenen tegen onheil dat nooit zou komen', inmiddels is dit echt anders", concludeert Samwel. Hij roept daarom op tot samenwerking.

De genoemde aanvallen laten volgens Samwel zien dat het aantal businesscases voor cyberaanvallers alleen maar toeneemt. En die businesscases creëren we met zijn allen door de steeds verdergaande digitalisering van de maatschappij. Waarbij daders volgens hem niet alleen uit zijn op geld of informatie, maar zeker ook op ontwrichting van de samenleving. "We moeten daarom alles in het werk stellen om ons te wapenen tegen de ransomwares van de toekomst", stelt hij. En dat vraagt om samenwerking. Reden voor Samwel om in dit gesprek de aandacht te vestigen op het Shared Research Program Cybersecurity.Een programma waarin TNO met drie grootbanken (Rabobank, ABN AMRO en ING) en Achmea samenwerkt om de Nederlandse samenleving te wapenen tegen cyberaanvallen van vandaag en morgen. "Met als doel een veilige en veerkrachtige digitale samenleving", vult Reinder Wolthuis aan.

Beide heren zijn sinds de start in 2014 nauw bij het Shared Research Program (SRP) betrokken. Een samenwerking die vanuit de grootbanken is ontstaan. "We concurreren als banken in Nederland niet op informatiebeveiliging", zegt Samwel. "We hebben te maken met dezelfde dreigingen. Zouden klanten bovendien het vertrouwen in mobiel- of internetbankieren verliezen dan geldt dat niet voor één, maar voor alle banken. Voor ons als banken is het dus niet meer dan logisch om gezamenlijk te acteren om cybercriminaliteit te bestrijden."

Interesse om aan te sluiten?

De ambitie van de deelnemers aan het Shared Research Program is nu om het programma uit te breiden met andere partijen. "We zijn op zoek naar partijen met een behoorlijk volwassenheidsniveau op het gebied van cybersecurity", legt Wolthuis uit. "Bedrijven die bovendien onderdeel zijn van



'SRP Cybersecurity Roadmap july 6th'

de kritieke infrastructuur in Nederland. Denk bijvoorbeeld aan telecom- en energiebedrijven. Hen nodigen we graag uit zich aan te sluiten." "Ze lopen tegen dezelfde kwetsbaarheden aan als wij. Kwetsbaarheden waarvoor nog geen goede bescherming is. Ik zie het als onze taak hier gezamenlijk een duurzame oplossing voor te vinden." Samwel: "De samenleving wordt steeds afhankelijker van ICT. Dat zorgt voor nieuwe kwetsbaarheden, maar ook voor nieuwe motieven voor cybercriminelen. Denk alleen maar aan Internet of Things (IoT). Cybercriminelen zullen hierin 'kansen' zien voor crimineel ingrijpen in de fysieke wereld. We kunnen dus verwachten dat de acties van cybercriminelen zich verder zullen uitbreiden naar de fysieke wereld." "(Nieuwe) dreigingen waartegen we ons gezamenlijk moeten weren door kennis, ervaring en (geanonimiseerde) data te delen. Om cybercriminaliteit tegen te gaan, is samenwerken meer dan ooit noodzakelijk. Het uitgangspunt binnen ons programma."

De onderzoeksthema's

Onderzoek binnen het SRP vindt plaats in de onderzoekslijnen: Monitoring & response, Controlled resilience, Cyber Threat Intelligence en Secure transactions. Daarbinnen kunnen deelnemers zelf onderzoeksvragen aandragen. "Het programma is op deze manier heel praktisch en deelnemers kunnen echt zelf sturen. Meer dan wanneer ze ervoor kiezen samen te werken met universiteiten", legt Samwel uit. "Hoewel het één het ander uiteraard niet uitsluit. Zo werken we als banken, maar ook binnen het SRP, weer samen met universiteiten wanneer dat gewenst of nodig is."

"Ons uiteindelijke doel is innovatieve kennis en kunde opbouwen om de samenleving beter te beschermen tegen cyberaanvallen", vat Wolthuis samen. "Waarbij het zeker ook de bedoeling is te komen tot Nederlandse productinnovaties. Leveranciers van kennis en concrete innovatieve producten en diensten die ons verder kunnen helpen om de cyberaanvallen van de toekomst het hoofd te bieden, nodigen we dan ook uit zich aan te sluiten. Zo kunnen we samen iets toevoegen aan de markt. Niet voor niks is het uitgangspunt voor elk onderzoek binnen ons programma dat er na een jaar zicht op valorisatie moet zijn."

Waar het tegengaan van fraude met internetbankieren zo'n drie jaar geleden het startpunt was voor de samenwerking binnen het SRP, zijn sindsdien veel meer onderwerpen aan bod gekomen. De onderstaande SRP roadmap geeft hiervan een duidelijk beeld:

DNS Ninja: breed toepasbaar

Een onderzoek dat Samwel en Wolthuis eruit willen pikken, is dat op het vlak van targeted attack detection. "Er is als het gaat om beveiliging van de perimeter al heel veel te koop", weet Samwel. "Aangezien wij niet als ambitie hebben om de markt te kopiëren, hebben wij onze focus gelegd op wat er gebeurt als een aanvaller eenmaal binnen is, de zogenoemde lateral movement." "Uitkomst van dit onderzoek is onder meer een snelle waarschuwingsmethode die kijkt naar afwijkend gedrag in het interne netwerk op 'concentrators' in het netwerk. DNS is zo'n concentrator waarbij op één plek informatie samenkomt vanuit heel het netwerk. De hypothese was dat je daarmee op een efficiënte wijze afwijkingen in het netwerk zou kunnen detecteren. Uiteindelijk hebben we aangetoond dat dit inderdaad mogelijk is door DNS-verkeer te analyseren met behulp van clustertechnieken."

De methode, die bekend is geworden onder de naam DNS Ninja, is volgens beide heren 'krachtig, breed toepasbaar en eenvoudig te integreren in bestaande IT-architecturen'. Klaar dus voor alledaags gebruik. Een goed voorbeeld van hoe het SRP bijdraagt aan het op basis van wetenschappelijk onderzoek ontwikkelen van producten en diensten voor de markt.

Sandra Kagie is freelance tekstschrijver/journalist. Als ervaren tekstschrijver en eindredacteur verricht zij uiteenlopende werkzaamheden op het gebied van tekst & taal. In het verleden is zij als eindredacteur nauw betrokken geweest bij 'Informatiebeveiliging'. Haar website is www.sanscriptproducties.nl en op Twitter is zij actief als @SanSanscript.

Meten van cyberweerbaarheid

Een tweede voorbeeld van een onderzoek dat beide heren willen belichten, is dat van het meten van cyberweerbaarheid, measuring cyber resilience. De meeste 'metrics' meten volgens hen het functioneren van een maatregel. Maar daarmee is niet gezegd dat deze maatregel een risico goed afdekt. Ook wordt geen rekening gehouden met veranderingen in het inherente risico. Het genoemde onderzoek heeft aangetoond dat het absoluut mogelijk is om 'metrics' te definiëren die inzicht geven in de weerbaarheid en het resterende risico. In het door de deelnemers uitgebrachte magazine 'Innovating in Cyber Security – Shared research 2017 (zie kader) wordt onder meer dieper ingegaan op de 'metrics'. Daarbij belooft Samwel dat er binnen afzienbare tijd een losse publicatie komt over dit onderwerp. "We willen daarmee stimuleren dat anderen ermee aan de slag gaan zodat het verder kan evolueren."

Voordelen van samenwerking

Niet elk onderzoek leidt overigens tot direct toepasbare oplossingen in de praktijk. Het is soms een kwestie van lange adem, waarschuwt Wolthuis. "Onderzoek is en blijft een kwestie van zaaien en oogsten. Wat we echter heel nadrukkelijk hebben gemerkt in de eerste drie jaar van deze samenwerking, is dat we als deelnemers nadrukkelijk evolueren in denken. We dagen elkaar continu uit waardoor onderzoek veel effectiever en creatiever is." "Wat we bovendien terugkrijgen van de deelnemers is dat de mindset van hun medewerkers die meedoen aan het programma is veranderd. Niet alleen binnen het programma, maar ook in hun dagelijkse werkzaamheden denken ze veel meer out-of-the-box. En heel praktisch, wanneer er een bepaalde investering moet worden gedaan in het kader van it-security zijn ze veel beter in staat de juiste vragen te stellen."
Een individueel bedrijf zou volgens Wolthuis nooit zulke stappen hebben kunnen zetten als de deelnemers de afgelopen drie jaar gezamenlijk hebben gedaan. Zo is het volgens hem een heel belangrijk voordeel dat deelnemers binnen de onderzoeken gebruik kunnen maken van gezamenlijke, (geanonimiseerde) actuele data om ontwikkelde methodieken te verifiëren.

Bijkomend voordeel voor deelnemers is dat het programma vanuit het topsectorenbeleid financiële steun krijgt vanuit Den Haag. "De financiële bijdrage van deelnemers is hierdoor te overzien. Wel wordt ook een investering in menskracht gevraagd", vult Samwel aan. "Wanneer we worden gevraagd naar de belangrijkste voordelen van deze samenwerking voor deelnemers, noemen we dan ook de combinatie van: shared workload, shared data en shared funding." "Deelnemers zijn uiteraard als eerste op de hoogte van ontwikkelde concepten en proofs of concept. Ze bepalen vervolgens zelf hoe zij deze willen gebruiken in de eigen organisatie", gaat Wolthuis verder. "Ook kunnen deelnemers besluiten onderzoeksresultaten te kapitaliseren door ze, al dan niet samen met anderen, te ontwikkelen tot producten en toepassingen voor de markt."

De toekomstige ontwikkeling

Natuurlijk vragen we de betrokkenen bij het SRP niet alleen terug te kijken. We horen ook graag in welke richting ze denken dat het programma zich de komende tijd zal ontwikkelen. Wat Wolthuis betreft wordt onder meer aandacht voor het automatiseren van de verdediging tegen aanvallen belangrijker. "Wat we zien, is dat aanvallers steeds meer gebruikmaken van geautomatiseerde tools om hun aanvallen op te zetten; aanvallen gaan dus sneller en worden grootschaliger. Dit is op de wijze die we nu hanteren (veel menselijke handelingen) niet meer te verdedigen. We zien dus dat het onderzoek zich meer richt op automatisering van de verdediging. Met technieken als Software Defined Networking en Network Function Virtualization." Dit betekent volgens Wolthuis een veranderende rol voor security professionals: "Ze zullen wellicht op een ander abstractieniveau hun werk moeten doen." Op dat vlak komt wat hem betreft dan ook de menselijke factor steeds prominenter in het onderzoek naar voren. Dat laatste geldt volgens hem ook zeker voor de gebruikerskant van securitydiensten en -producten. "Je moet op dit vlak beyond awareness denken en fundamentele inzichten uit psychologie en sociologie gebruiken om mensen zover te krijgen zich digitaal veiliger te gaan gedragen. Denk bijvoorbeeld aan het betrekken van gedragswetenschappers bij onderzoek", geeft hij een voorbeeld.

"We moeten bovendien nog veel beter in het hoofd van aanvallers kunnen kruipen", vult Samwel aan. "Zij zijn vaak weken, soms maanden en misschien wel jaren bezig met het plannen van een aanval. Daar valt dus winst te behalen als het gaat om tijdige herkenning." Informatie over wat er omgaat in de hoofden van kwaadwillenden is wat hem betreft dus cruciaal. "Samenwerking met politie en justitie is dan ook zeker gewenst. Een mogelijkheid die we momenteel onderzoeken. Waarbij we uiteraard bekijken hoe we onderling informatie kunnen uitwisselen, zonder álles te delen. Dit in het kader van privacywetgeving en de bescherming van persoonsgegevens."

Kat-en-muis-spel

Hoe meer partijen betrokken zijn bij het SRP, hoe meer de resultaten van het programma tot wasdom kunnen worden gebracht. Daarvan zijn de deelnemers overtuigd. Wolthuis en Samwel doelen hierbij niet alleen op de ontwikkeling van daadwerkelijke producten en diensten voor de markt, maar bijvoorbeeld ook op standaarden gebaseerd op SRP-onderzoek. Om dit te bewerkstelligen, roepen ze bedrijven en organisaties nogmaals op mee te doen. "Onze tegenstanders worden steeds innovatiever", waarschuwen ze. "Cybersecurity is een kat-en-muisspel. Het kennisniveau van de kwaadwillenden stijgt waardoor de dreiging toeneemt. Om ons afdoende te beschermen, moeten we wel samenwerken."

Deelnemen of magazine downloaden
Ben je geïnteresseerd in deelname aan het Shared Research Program Cybersecurity, neem dan contact op met Reinder Wolthuis: reinder.wolthuis@tno.nl. Dit geldt ook wanneer je geïnteresseerd bent in de resultaten van het onderzoek van het SRP en wanneer je hier iets mee wilt doen. Het magazine Innovating in Cyber Security – shared research 2017 is beschikbaar via http://bit.ly/2wjVZKZ.

ACCESS42
Cybersecurity

tenable™

Niemand is in staat om inzicht en focus te bieden om het

CYBER EXPOSURE GAP

te dichten

TOT NU TOE

Access42 en Tenable kunnen u helpen met het noodzakelijke inzicht en de focus om het Cyber Exposure Gap te dichten. Cyber Exposure bouwt verder op de beginselen van Vulnerability Management voor traditionele IT applicaties, endpoints en systemen door de identificatie van bugs en misconfiguraties uit te breiden met het volgende:

Wilt u meer weten over de mogelijkheden voor uw organisatie? Neem contact met ons op voor een vrijblijvende afspraak en demonstratie.

Access42 B.V.

E-mail: info@access42.nl
Telefoon: +31(0)880002000
Website: https://www.access42.nl

OPINIE

BIG BROTHER, GRAND CHILDREN

Op 11 juli 2017 is de Eerste Kamer akkoord gegaan met de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv). Inlichtingen- en Veiligheidsdiensten mogen nu volgens het sleepnetmodel informatie verzamelen en vervolgens gedurende drie jaar accumuleren en analyseren. Kortom, een zeer privacygevoelige activiteit. Met het oog op ons aller veiligheid en onder het motto: alles heeft zijn prijs. Maar gaat het zo goed? Of kan het ook anders?

NSA-klokkenluider William Binney (1) zei over het surveillanceprogramma van de VS na 9/11 "it's better than anything that the KGB, the Stasi, or the Gestapo and SS ever had" (2). Met de ontwikkeling van ThinThread (3) toonde Binney vervolgens aan dat privacyprotectie heel goed samen kan gaan met het terughoudend verzamelen van data. Sterker nog, slimme en tijdige dataminimalisatie bevordert juist de effectiviteit van opsporingsactiviteiten. In de VS was er geen vruchtbare bodem voor dit idee. Maar in Wenen wordt op dit moment door Jan van Oort een oplossing ontwikkeld die - toevallig - sterke gelijkenissen met ThinThread van Binney vertoont. Van Oort en Binney zijn hierover inmiddels met elkaar in gesprek. Waar het op neerkomt, is dat dataminimalisatie en veiligheid heel goed samengaan.

De Europese Algemene Verordening Gegevensbescherming (AVG) heeft mede tot doel surveillanceprogramma's zoals die van de KGB, de Stasi, de Gestapo en de SS - of erger - te voorkomen. Ofwel, democratic governance is een centrale doelstelling. Data governance is een kritische succesvoorwaarde daarvoor, niet een eindpunt. Vergelijk het met een auto waarbij iemand de juiste kant op moet sturen. Of met de rode knop, waarmee al dan niet een atoomwapen gelanceerd zal worden. Zonder bekwame, democratische bestuurders raken we van de wal in de sloot.

Maar de vergelijking gaat mank. Want zelfrijdende auto's, robots en drones - al dan niet bewapend of van sensoren voorzien - met een handelingsmandaat zijn in opmars, net als analysetools die meer over ons te weten kunnen komen dan wijzelf. Data-ijsbergen groeien onder water aan en data-lakes dijen ongecontroleerd uit. Steven Hawking wijst erop dat robots sneller kunnen evolueren dan mensen. Hij waarschuwt zelfs voor een opstand van "schurk-robots" (4). Chatbot 'Tay', een creatie van Microsoft, evolueerde al - binnen een tijdsbestek van 24 uur - van teksten als "humans are super cool" tot "Hitler was right" (5). Zonder regie tuimelt Tay in het ravijn.

AGConnect tenslotte schreef op 18 februari: "politieke partijen hebben te weinig aandacht voor digitalisering en de gevolgen daarvan voor de Nederlandse samenleving" (6). Dit geldt in het bijzonder voor privacy & democratic governance. Het is aan de politiek om zich te informeren en met kennis van zaken digitale handen en voeten te geven aan democratische waarden en daarmee aan een effectieve privacyprotectie. De IT-sector heeft een maatschappelijke verantwoordelijkheid om kennis en inzicht te delen. Als IT-professional ben ik daar zelf in ieder geval graag toe bereid. U ook?

Referenties

(1) https://en.wikipedia.org/wiki/William_Binney_(U.S._intelligence_official))
(2) https://www.thenation.com/article/obamas-crackdown-whistleblowers/
(3) https://en.wikipedia.org/wiki/ThinThread
(4) http://www.dailymail.co.uk/sciencetech/article-3664076/Artificial-intelligence-evolve-faster-human-race-Professor-Stephen-Hawking-warns-rogue-robot-rebellion.html#ixzz4rolUyrEY).
(5)https://www.infowars.com/microsofts-ai-bot-goes-from-benevolent-to-nazi-in-less-than-24-hours/
(6) https://agconnect.nl/artikel/politieke-partijen-ontberen-visie-op-it-revolutie

Elisabeth de Leeuw is Principal Architect Identity & Privacy bij KPN. Ze is bereikbaar via (info volgt nog)

NETWERK- EN INFORMATIEBEVEILIGING EN BUSINESS CONTINUITY MANAGEMENT

Het Europees Parlement heeft in juli 2016 de nieuwe Europese cybersecurityrichtlijn aangaande Netwerk- en InformatieBeveiliging (de NIB-richtlijn/NIS-Directive) gepubliceerd, die gericht is op het creëren van een gemeenschappelijk niveau van netwerk- en informatiebeveiliging binnen Europa. Elke lidstaat dient in het kader van het maatschappelijk belang te zorgen voor betrouwbaar, betaalbaar en veilig netbeheer. Op dit moment wordt in Nederland gewerkt aan de Cybersecuritywet (Csw) met als doel invulling te geven aan de NIB-richtlijn. Uiterlijk 9 mei 2018 moet de richtlijn zijn omgezet in wetgeving. We kunnen gerust stellen dat na de recente cybercrime-incidenten, met onder andere hacks en ransomware, dit geen overbodige luxe is. Een gezamenlijke Europese aanpak wordt toegejuicht, zolang dit maar geen lokale doublures en verwarring tot gevolg heeft. In dat kader zal op het moment dat de Cybersecuritywet is aangenomen, de Wet gegevensverwerking en meldplicht cybersecurity weer worden ingetrokken. Spannend blijft wel de link met de Algemene Verordening Gegevensbescherming (AVG of GDPR) die gepland staat voor 25 mei 2018.

De NIB-richtlijn is van toepassing op door de lidstaten aan te wijzen 'aanbieders van essentiële diensten' (AED's). Deze aanbieders bevinden zich binnen de in de richtlijn specifiek genoemde sectoren (energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, levering en distributie van drinkwater en digitale infrastructuur) en op 'digitale dienstverleners' (DSP's): aanbieders van onlinemarktplaatsen, onlinezoekmachines en cloudcomputerdiensten. Je kunt fronsen bij de keuzes, maar deze zijn specifiek benoemd. De verplichtingen van deze richtlijn gelden niet voor eventuele andere diensten die deze organisaties aanbieden. De lidstaten dienen die AED's uiterlijk 9 november 2018 te hebben aangewezen. De NIB-richtlijn regelt de verbindingsfunctie tussen lidstaten en per lidstaat de meldplicht van cyberrisico's en incidenten bij het CSIRT (voor Nederland bij het NCSC, onderdeel van het NCTV). Het regelt ook toezicht bij de bevoegde autoriteit, het betreffende Ministerie of De Nederlandsche Bank, per eerdergenoemde sector. Veel stof om over na te denken, Wie betreft dit? Wat betekent dit inhoudelijk voor mij? En wellicht ook; wat gebeurt er wanneer ik het niet doe, hoe worden sancties opgelegd?

Continuïteit

In de richtlijn wordt op diverse plaatsen melding gemaakt van het fenomeen 'Continuïteit' en dat, kun je gerust stellen, is dan ook één van de doelstellingen (naast vanzelfsprekend mogelijk misbruik van toegang en/of buitgemaakte gegevens te voorkomen). Continuïteit van de benoemde essentiële productlevering en dienstverlening. Je kunt daar begrip voor opbrengen wanneer je je bedenkt wat er zou geburen wanneer deze producten en diensten niet beschikbaar zijn. De technische invulling laten we hierbij even voor wat het is, maar de gevolgen, wanneer informatiebeveiliging faalt, voor de bedrijfscontinuïteit niet. De richtlijn spreekt van "Bij de beoordeling van de mogelijke gevolgen, wat betreft omvang en duur, van een incident op economische en maatschappelijke activiteiten of op de openbare veiligheid moeten de lidstaten ook inschatten hoe lang het zal duren voordat de discontinuïteit een negatief effect begint te sorteren". Veel onderdelen hierbinnen zijn niet gedefinieerd en dat kan op zich alweer tot verschillen leiden tussen lidstaten en hun wetgeving, helaas. Hoe wordt het 'beoordeeld', wat is 'te lang' in het kader van 'negatief effect' en wat wordt bedoeld met 'begint te sorteren'. Ook wanneer gesproken wordt over "De lidstaten zorgen ervoor dat aanbieders van essentiële diensten passende maatregelen nemen om de gevolgen van incidenten die de beveiliging van de voor de verlening van die essentiële diensten gebruikte netwerk- en informatiesystemen aantasten, te voorkomen en te minimaliseren zulks om de continuïteit van deze diensten te waarborgen", komen weer termen voor als 'passend', 'voorkomen' en 'minimaliseren' die best wel enige verduidelijking behoeven. Laten we er echter positief naar kijken. Deze richtlijn moet worden omgezet in wetgeving en we gaan er vooralsnog van uit dat verduidelijking waar gewenst of vereist wordt ingevuld door onze wetgever.

Invalshoeken

Vanuit het perspectief van de eindgebruiker, de klant (u en ik dus), wordt aandacht geëist voor netwerk- en informatiebeveiliging vanuit verschillende invalshoeken met in ieder geval als doel te voorkomen dat we zonder deze essentiële diensten komen te zitten. Er wordt gesproken over het nemen van preventieve maatregelen, alsook wat te doen wanneer 'hét' gebeurt, in dit geval benoem ik dat als aantasting van de netwerk-informatiesystemen en onze gegevens door ongeoorloofd handelen. Dit is volledig gericht op bedreigingen/risico's gerelateerd aan netwerk- en informatiesystemen, waardoor kritische ICT-diensten (afhankelijkheid van gegevenstoegang, applicaties, …) niet beschikbaar zijn voor kritische activiteiten. Deze vormen tevens een onderdeel van de Business Continuity Management Bedreigingen Analyse wanneer het gaat om de benoemde bedreigingen/risico's en de bepaling van de kritische activiteiten middels de Business Impact Analyse.

Gert Kogenhop (1958) is directeur van bcm+, een bedrijf dat is gespecialiseerd in training, consultancy en implementatie van Business Continuity Management Systemen conform de norm ISO 22301. Gert heeft een financieel economische achtergrond en is onder andere werkzaam geweest als Regional Finance Director Northern Europe bij DELL en is tevens een gecertificeerd trainer op het gebied van leidinggeven. Gert is bereikbaar via www.bcmplus.nl of per e-mail: gk@bcmplus.nl.

‘Bekwaamheid om met behulp van de ter beschikking staande middelen een gesteld doel te bereiken. Plan van handelen’

Op deze wijze is dan ook het onderwerp informatie-beveiliging onlosmakelijk verbonden met Business Continuity Management. Organisaties dienen zich te realiseren dat uitval van ICT als gevolg van een technische oorzaak (hardware uitval, software- of netwerkproblemen) al jarenlang in de spotlights staat, en nog, en dat alle mogelijke opties en technische faciliteiten ter voorkoming een enorme ontwikkeling hebben doorgemaakt. Het kan echter zijn dat de gebruikers geen toegang hebben tot ICT-systemen. Bijvoorbeeld doordat er een beveiligings-incident is en men (nog) niet heeft kunnen vaststellen wat de omvang is. Om dientengevolge geen risico’s op escalatie of verspreiding te nemen, kan vervolgens de toegang tot gegevens, systemen en applicaties onmogelijk worden gemaakt. Dan komt de vraag naar boven ‘En wat nu?’. Hoe afhankelijk zijn we van ICT? Hebben we alternatieven? Wie gaat wat, hoe doen? Wat kunnen we nog wel? Hoe en wanneer informeren we derden die afhankelijk zijn van wat we hier doen? Allemaal legitieme vragen die binnen Business Continuity Management dienen te worden beantwoord conform de daarbinnen vooraf vastgestelde strategie.
Bij Business Continuity Management gaat het uiteindelijk om het managen van de situatie tijdens en direct na een ernstig incident, een verstoring van de `business as usual’-situatie. In dit geval het niet beschikbaar zijn van (betrouwbare) ICT-systemen of gegevens. We moeten voorbereid zijn en zorgen dat we weten wat we moeten doen om de levering van onze producten en/of diensten aan onze afnemers zo optimaal mogelijk te waarborgen. Het is ook belangrijk om indien nodig over bijvoorbeeld de (on)mogelijkheden en prioritering van tevoren afspraken te maken met álle belanghebbenden.

Strategie

Het komt er simpelweg op neer dat de gekozen strategie in deze situatie van het grootste belang is. Strategie, volgens Van Dale: `Bekwaamheid om met behulp van de ter beschikking staande middelen een gesteld doel te bereiken. Plan van handelen’. Wat is dan dat gestelde doel? Wat zijn dan de te verrichte handelingen in deze `business as not usual’-situatie? Om het niet te ingewikkeld te maken, stel ik hier vast dat het overgrote deel van de bedrijven door middel van bepaalde activiteiten bepaalde producten en/of diensten levert aan bepaalde afnemers (markten, klanten). In het geval van ICT-problemen kunnen we onder andere te maken hebben met activiteiten en processen met betrekking tot systemen, gegevens of applicaties. Dit leidt er automatisch toe dat er drie ingangen zijn voor de continuïteitstrategie, namelijk de activiteiten, de producten en/of diensten en de afnemers. Er zullen strategische keuzes moeten worden gemaakt over wat het eerst hersteld moet zijn en wat wellicht helemaal (of nu nog even) niet. Indien de gekozen strategie is dat alle activiteiten in een bepaalde volgorde worden hersteld, dan heeft dat direct invloed op welke producten en/of diensten vervolgens geleverd kunnen worden. En daardoor aan welke afnemers wel en niet geleverd kan worden. Indien de producten en/of diensten bepalend zijn voor de volgorde, dus eerst dit product en vervolgens dat product, dan heeft dat directe gevolgen voor de te herstellen activiteiten die daarvoor nodig zijn. En aldus is dat bepalend voor aan welke afnemers wel en niet geleverd kan worden. Echter, indien de afnemers leidend zijn tijdens de continuïteitsinspanning, dus eerst deze klant en dan die en die (nog even) niet, dan is vervolgens bekend welke producten gemaakt moeten worden en/of diensten geleverd dienen te worden. Daaruit kan direct afgeleid worden welke activiteiten in welke volgorde hersteld dienen te worden. Deze strategische keuzes zijn bepalend voor de tactische (management) handelingen en de inspanningen op de werkvloer, de operationele kant. Een niet te onderschatten beslissingstraject dat regelmatig wordt vergeten en tijdens een ernstig incident leidt tot chaos en kans op verkeerde keuzes en beslissingen. Wellicht in dit geval nog versterkt door het feit dat het hier gaat om essentiële producten en diensten binnen de sectoren energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, levering en distributie van drinkwater en digitale infrastructuur.

Voor wie te maken krijgt met NIB-richtlijn en volgend jaar de Csw het advies om verder te kijken dan de informatiebeveiligingsimpact en het ICT-continuïteitsplan, plus eventueel separaat het Disaster Recovery Plan. Zoek aansluiting met het Business Continuity Management System van de organisatie.

EXPONENTIËLE GROEI AAN SLEUTELS EN CERTIFICATEN VRAAGT OM ANDERE DENKWIJZE EN AANPAK

Encryptie was lange tijd een zaak van het leger en wiskundigen. Met de komst van de computer werd het mogelijk de versleuteling (cryptografie) zeer snel uit te voeren en voor verschillende doeleinden in te zetten. Dezelfde computer bood ook weer uitkomst voor het kraken van de versleuteling.

Pasqualle Verwoerdt Business Manager High Grade Security bij Avensus

In ons moderne digitale leven is encryptie niet meer weg te denken. Dagelijks hebben we ermee te maken, denk aan internetbankieren, pinnen, slimme meters, IoT, auto's, OV-chipkaart, websites en online shopping. Kortom; we ontkomen er niet aan, al zouden we dat soms graag willen. Nu onze samenleving op alle vlakken verder digitaliseert en onze privacy een steeds groter goed wordt; is de afhankelijkheid en noodzaak voor cryptografie exponentieel toegenomen. Data (al dan niet met persoonsgegevens) wordt het best beschermd door deze te versleutelen; dit wordt door overheid en bedrijfsleven onderstreept. Het NCSC en ook Enisa hechten steeds meer waarde aan versleuteling en sleutelbeheer.

Sleutels en certificaten

Meer encryptie betekent meer afhankelijkheid van sleutels en certificaten. Helaas vertrouwen de meeste organisaties de opslag en uitgifte van deze cruciale sleutels en certificaten aan software toe. Dit is geen verstandige keuze als je bedenkt dat sleutelmateriaal in software pseudo random wordt gegenereerd. Er zijn tal van voorbeelden waarbij crypto-analisten en cybercriminelen in staat zijn om vrij eenvoudig delen van een sleutel in software aan te vallen, waardoor uiteindelijk de hele sleutel kan worden achterhaald. De gevolgen zijn niet te overzien en het melden van de security breach aan de autoriteiten is wellicht nog wel datgene waar je je op dat moment het minst zorgen om maakt: de continuïteit van het bedrijf staat dan op het spel. Door (gecertificeerde) hardware te gebruiken voor sleuteluitgifte en -opslag kunnen we dit voorkomen. Bij het gebruik van een Hardware Security Module (HSM) staat het sleutelmateriaal namelijk onder het regime van de HSM. Buiten de HSM staat alleen een 'associatie' en NIET de sleutel zelf; deze sleutel zit ten alle tijden veilig opgeslagen in de gecertificeerde hardware. Zo wordt elk risico tot een minimum beperkt.

Vanuit 'goed huisvaderschap' is het gebruik van HSM's in deze tijd eigenlijk een no-brainer. Daarnaast biedt het ook uitkomst om te voldoen aan regelgeving als de AVG en GDPR. In de AVG en GDPR gaat het over dataprotectie, waarbij securitytermen als antivirus, ips/ids, siem, security intelligence, soc en firewalling NERGENS voorkomen in deze specifieke regelgeving, terwijl er zeker 19 keer gesproken wordt over Encryption of Pseudonimisatie. Er wordt dus sterk de nadruk gelegd op protectie van de data zelf. De definitie van data protectie die men aanhoudt is: pseudonimisatie / encryptie + key management + access control. Dat is ook logisch als je bedenkt dat het pseudonimiseren of encrypten van data een veel betere strategie is dan het koortsachtig voorkomen van een lek. De impact van een inbreuk of lek wordt geminimaliseerd omdat de data encrypted is en niet meer bruikbaar voor onbevoegden. In combinatie met goed key management en access control kan worden aangetoond dat men 'in control' is aan de interne organisatie en aan de externe autoriteiten.

In het kader van goed huisvaderschap en aangescherpte regelgeving moeten we bouwen aan een fundamentele en effectieve security basis door de HSM centraal te stellen binnen de infrastructuur als Trust Anchor. Vanuit deze gedachte kunnen alle verschillende toepassingen die we kennen en certificaten of sleutels die we gebruiken of genereren, gecentraliseerd in de HSM worden beheerd (met name de private keys). De toepassing van een HSM is voor elke organisatie haalbaar, maar begin laagdrempelig of op de plek waar de meeste pijn zit. Van daaruit kan de HSM stap voor stap gaan dienen als Trust Anchor voor allerlei toepassingen (we moeten meer gaan denken in de richting van HSM-as-a-Service, die we in onze interne omgeving kunnen inzetten). Encryptie toepassen is altijd de beste keuze, maar maak dan ook de juiste keuze als het gaat om aanmaak en beheer van onze sleutels en certificaten. Met HSM als Trust Anchor kunnen we de exponentiële groei aan sleutels en certificaten op het allerhoogste niveau beveiligen.

Bronnen en naslag:

- NCSC: ICT Beveiligingsrichtlijnen voor Transport Layer Security (TLS); met name H3, H4 en Appendix :Verdere overwegingen
- NCSC: Postkwantum-cryptografie;
- Enisa: Privacy and Data Protection by Design – From Policy to engineering
- Enisa: Algorithms, Key Sizes and Parameters Report

Avensus
HIGH GRADE SECURITY

WHO STILL DARES TO SHARE?

Aandachtspunten bij gebruik van filesharing

Iedereen maakt vandaag de dag privé gebruik van diensten als Dropbox, OneDrive of Google Drive voor het opslaan en vooral ook delen van foto's en documenten. Deze tools zijn heel erg handig, intuïtief en werken ook goed op mobiele apparaten. Als werknemer is de verleiding groot om deze tools ook te gaan gebruiken voor zakelijke samenwerking. Hier kleven echter risico's aan. Hoe vind je als bedrijf een balans tussen in control blijven en voldoen aan compliance eisen en aan de andere kant om mee te gaan met medewerkerswensen en te komen tot een acceptabele en werkbare oplossing? Wat zijn de uitdagingen en aandachtspunten hierbij, in het bijzondere voor onderwijs- en onderzoeksinstellingen?

Onzorgvuldig gebruik van filesharingdiensten zorgt voor een aanzienlijk risico op het lekken van gegevens. Zeker met de nieuwe privacywetgeving AVG (Algemene Verordening Gegevensbescherming) is het lekken van vertrouwelijke persoonsgegevens zeer onwenselijk en kan aanzienlijke reputatieschade opleveren. Vaak wordt onderschat hoeveel data al als persoonsgegevens geclassificeerd moeten worden. Persoonsgegevens zijn alle informatie die direct dan wel indirect te herleiden is tot een natuurlijk persoon. In essentie is filesharing vaak net zo risicovol als het gebruik van reguliere e-mail, waarin alle mogelijke persoonsgegevens ook (in bijlagen) verstuurd worden. Aan de andere kant, kan een goed ingerichte en gebruikte filesharing ook veiliger zijn dan reguliere e-mail.

Er ligt dus nu een uitdaging, maar ook kans voor organisaties om dit passend te gaan inregelen. Enerzijds in technische zin, maar vooral ook: welke begrijpbare en werkbare spelregels spreek je met medewerkers af ten aanzien van het opslaan en delen van met name vertrouwelijke en geheime informatie? Kies je voor een onwerkbare oplossing, dan zijn de eindgebruikers vaak creatief genoeg om alternatieven te bedenken die meestal nog onwenselijker zijn. Bijvoorbeeld opslag op losse harde schijven of memory sticks, versturen van bestanden als bijlage naar privé e-mailadressen of het gebruik van een persoonlijke Dropbox of OneDrive.
In de academische wereld is samenwerken binnen de universiteit, met andere kennisinstellingen in Nederland, de EU dan wel wereldwijd en met commerciële bedrijven cruciaal om als kennisgenerator en als partner van het bedrijfsleven te kunnen optreden. Hierbij is het veilig en laagdrempelig kunnen delen van informatie en samenwerken met verschillende soorten partijen dus een must. Elke deelnemer heeft hierbij vaak zijn eigen systemen en beleidskaders.

Binnen de academische wereld bestaat, in tegenstelling tot bijvoorbeeld banken met een vergaande informatieclassificatie, een niet zo sterk gereguleerde omgeving. Hierbij zijn meestal geen maatregelen genomen als data loss prevention (DLP) en Enterprise Digital Rights Management (EDRM) tooling zoals in sterk gecontroleerde omgevingen. Het toezicht op de verspreiding van informatie is hierdoor lastiger.
Gebruik van filesharingdiensten wordt door een aantal aanbieders actief gepromoot binnen de onderwijswereld en daarbuiten. Zo promoot Microsoft het gebruik van OneDrive onder scholieren, studenten en academisch personeel door 'gratis' 1 TB opslag aan te bieden en heeft ook Dropbox promotiecampagnes (Dropbox Campus Cup) en speciale

aanbiedingen voor studenten. De verleiding is dus groot om van deze diensten gebruik te maken doordat het niks of weinig lijkt te kosten in vergelijking tot corporate opslagdiensten, zeker bij grotere hoeveelheden data. Maar boven kosten speelt het intuïtieve en bekende gebruikersgemak een doorslaggevende rol voor het gebruik.

Scope

Gartner (1) definieert filesharing ofwel 'enterprise file synchronization and sharing' (EFSS)-diensten als: "a range of on-premises or cloud-based offerings that enables individuals to synchronize and share files (such as documents, photos and videos) among mobile devices and PCs. Sharing can happen among people (for example, partners and customers) within or outside the organization, as well as among applications. Smooth search, retrieval and access of files stored in multiple data repositories (e.g., file servers or content management platforms) from different client devices complement these offerings, as well as security, data protection and collaboration capabilities."
Grofweg zijn er volgens Gartner drie functionele gebieden te onderscheiden voor de inzet van EFSS (2). De eerste is de verhoging van de productiviteit van medewerkers door middel van de mogelijkheid om vanaf een willekeurig apparaat en vanaf elke locatie bestanden eenvoudig te kunnen benaderen en aan te passen. De tweede is de mogelijkheid om bestanden intern dan wel extern te kunnen delen. Hierbij zijn aspecten als versiebeheer en notificaties van wijzigingen belangrijk. Het laatste gebied zijn de mogelijkheden om bestaande interne opslagdiensten (waaronder FTP) te verplaatsen naar EFSS. Zodoende kan eenvoudig voorzien worden in passende redundantie en bijbehorende hoge beschikbaarheid en back-up met eenvoudige restore mogelijkheden. Aanvullend op bovenstaande punten neemt het gebruik van apps sterk toe en vereisen diverse apps integraties met één of keuze uit meerdere specifieke EFSS-diensten vereisen voor toegang tot data.
Afhankelijk van de specifieke organisatiebehoeftes zal de uiteindelijke keuze voor een EFSS-dienst dan ook verschillend zijn. Kosten per medewerker zullen ten alle tijden een cruciaal aspect blijven tijdens het selectietraject. Daarnaast dient er ook rekening gehouden te worden met de organisatievoorkeur ten aanzien van public, hybrid of private cloud dan wel alles on-premise. Recent worden er zelfs peer-to-peer blockchain-achtige oplossingen aangeboden met bijbehorende encryptie en compartimentering (3).

Uitdagingen en aandachtspunten

Hieronder een nadere uitwerking van een aantal uitdagingen en aandachtspunten bij de selectie en het gebruik van EFSS-diensten. Deze punten kunnen organisaties helpen om passende keuzes te maken bij de selectie en het gebruik van deze diensten.

Security versus functionaliteit

Waarschijnlijk zal al snel duidelijk worden dat het niet haalbaar is om aan alle securityeisen te voldoen in combinatie met de vereiste businessfunctionaliteiten. Men zal dus een balans moeten zoeken tussen de hoeveelheid controle en toezicht vanuit security en het toelaten om innovatie en wendbaarheid van de organisatie te ondersteunen. Geen richting geven aan EFSS-diensten en het oogluikend toestaan of gedogen van andere opslagmedia is nog risicovoller.

Synchronisatie

Voor gebruik van filesharingdiensten is het belangrijk om te kiezen voor diensten die gewijzigde bestanden enkel als delta synchroniseren in plaats van het hele bestand opnieuw te synchroniseren. Dit is niet alleen nuttig voor gebruikers met een trage internetverbinding (bijvoorbeeld bij gebruik van mobiel netwerk op platteland in het buitenland) maar voorkomt ook dat de zakelijk internetverbinding traag wordt door honderden gebruikers die gelijktijdig hun data synchroniseren. Een ander voordeel van delta synchronisatie is dat version history mogelijk is en dat bij ransomware infecties makkelijk terug gegaan kan worden naar een oudere versie. Verder is het belangrijk dat er bijvoorbeeld door een checksum te vergelijken van bestanden voor en na synchronisatie gevalideerd wordt dat de bestanden niet aangepast zijn.

Raoul Vernède is Security Officer bij Wageningen University & Research. Hij is bereikbaar via raoul.vernede@wur.nl.

Sterke authenticatie
Wachtwoorden als authenticatie bieden maar een zeer beperkte bescherming van gegevens. Sterke authenticatie door middel van een tweede factor is noodzakelijk voor de bescherming van vertrouwelijke data. Voor EFSS-diensten is twee factor authenticatie echter lastig in gebruik en bij diverse aanbieders zelfs afwezig. De tweede factor is meestal een mobiel apparaat dat zelf ook toegang heeft tot de via EFSS gedeelde bestanden, waardoor juiste initiële registratie noodzakelijk is om effectief te zijn.

Exit strategie
Denk al tijdens het selectietraject van een EFSS-dienst na over het moment dat men geen gebruik meer wil maken van de dienst. Bepaal een strategie voor het migreren van bedrijfsdata naar een andere dienst. De wetgeving m.b.t. privacy ontwikkelt zich constant en marktontwikkelingen gaan vaak nog sneller. De kans dat men na enige tijd een andere dienst wil of moet gebruiken is aanzienlijk.

Delen van data
Een standaard functionaliteit is het kunnen delen van documenten en mappen met externe personen. Dit gebeurt met behulp van zakelijke of persoonlijke dan wel sociale e-mailadressen waarbij er beperkte zekerheid is dat de eigenaar van het e-mailadres ook daadwerkelijk de beoogde ontvanger is. Verder is de authenticatie enkel op basis van wachtwoorden waarbij men als eigenaar van de informatie geen wachtwoordbeleid of twee factor authenticatie kan afdwingen bij de ontvanger waardoor de kans op een security incident groter wordt.
In geval van het lekken van vertrouwelijke persoonsgegevens is het maar de vraag of de Autoriteit Persoonsgegevens het delen van persoonsgegevens enkel op basis van een e-mailadres en bijbehorend wachtwoord als voldoende passende beveiliging zal beoordelen. Een mogelijke toekomstige oplossingsrichting zou kunnen zijn om bepaalde domeinen van organisaties waarmee men contractuele afspraken heeft en die men vertrouwt, te kunnen white-listen om zo met deze externe medewerkers van die organisatie te kunnen samenwerken. Voordeel hierbij is ook dat indien een medewerker van zo'n samenwerkingspartner vertrekt het account wordt dichtgezet en deze persoon dan geen toegang meer heeft tot de gedeelde data. Dit in tegenstelling tot filesharing accounts die gekoppeld zijn aan privé e-mailadressen.

Toegang data
Filesharingdiensten zijn persoonsgebonden en niet team of afdeling gebonden. Toegang tot bedrijfsdata bij een normaal einde dienstverband dan wel bij een (security)incident vereist daarom toegang of minimaal het op afstand kunnen verwijderen (remote wipen) van data. Zijn hiervoor eenvoudige en transparante tools voor aanwezig in de geselecteerde EFSS-dienst? Bepaal de bewaartermijn van de EFSS-data na contractbeëindiging van een medewerker, anders bestaat het risico dat data en bijbehorende back-up verwijderd zijn op het moment dat de vertrokken medewerker toch nog niet gedeelde documenten had.

Logging
Makkelijk toegankelijke en gedetailleerde logging over een langere periode is cruciaal om onder andere in geval van een mogelijk datalek te kunnen aantonen dat de data niet is gelekt. Denk bijvoorbeeld aan de situatie dat een wachtwoord gecompromitteerd is. Verder kan logging ook inzicht geven in het gebruikersgedrag, wat bijsturen mogelijk maakt op ongewenst gedrag. Rechtstreekse koppeling naar een eigen SIEM om correlaties te ontdekken, kan wenselijk zijn.

Verspreiding data
Doordat gebruikers sync-clients en apps installeren op eigen niet zakelijk beheerde apparaten (BYOD) zoals laptops, tablets als ook smartphones en data synchroniseren, zal zakelijke data gefragmenteerd worden over meerdere en vooral ook beperkt beheerde locaties. Diefstal of verlies van privé apparaten zonder passende beveiliging zoals dataencryptie dan wel het ongewild peer-to-peer delen van te veel datamappen kan tot datalekken leiden. Bij sommige diensten is het mogelijk als beheerder op afstand gesynchroniseerde bestanden te verwijderen (in geval van verlies/diefstal dan wel einde dienstverband) op het moment dat het apparaat weer op het internet komt. Het niet toestaan van sync-clients haalt veel handige en door de gebruikers gewenste functionaliteit weg en is in veel gevallen bijna geen optie. Als alternatief zouden de bestanden dan enkel via een webbrowser te benaderen en te bewerken zijn. Of men moet ervoor kiezen BYOD geheel onder beheer te nemen door middel van EMM (Enterprise Mobility Management) met bijbehorende aanzienlijke kosten.

Fysieke locatie data
Voor diverse organisaties is het onwenselijk en onacceptabel indien bedrijfsinformatie buiten het eigen land dan wel de EU (of Europese Economische Ruimte) opgeslagen wordt. Dit ondanks het vernieuwde Privacy Shield als opvolger van Safe Harbour. Sommige aanbieders bieden daarom Europese datacentra aan. Het blijft echter vaak de vraag (4) in hoeverre de data in transit dan wel de metadata en indexering van de bestanden buiten de EU komt en zo makkelijk af te tappen is. Navraag bij de EFFS-aanbieder kan hier mogelijk deels inzicht in geven op basis van certificeringen, transparency reports en government data requests principles.

Samenwerking
Voor interne dan wel externe collaboratie binnen projecten bieden organisaties vaak ook specifieke samenwerkingsomgevingen aan (denk hierbij bijvoorbeeld aan Microsoft SharePoint teamsites). De functionaliteit hiervan is meestal uitgebreider en omvat vaak zaken als actielijsten en agendabeheer. Doordat er echter overlap met EFSS-diensten bestaat is het belangrijk om als organisatie te bepalen in welke situaties van welke hulpmiddelen gebruik gemaakt kan worden en wanneer niet. Veel organisaties redeneren van binnen naar buiten toe als het gaat om de keuze en inrichting van externe samenwerkingshulpmiddelen. Hierdoor moet bij samenwerking onderling besloten worden welke dienst gebruik gaat worden. In samenwerkingsverbanden (bijvoorbeeld EU-onderzoeksprojecten) met diverse of veel partners is dit bijna onmogelijk. Vaak wordt er daarom door gebruikers als een soort connectiviteitslaag gebruik gemaakt van een cloud gebaseerde breed verspreide EFFS-dienst (meestal Dropbox of Google Drive).

Encryptie
Sommige aanbieders van EFSS-diensten bieden naast encryptie van de verbindingen ook encryptie van eigenlijke data aan. Dit beschermt echter niet tegen vordering van data door wettelijke instanties (in het buitenland). Een extra laag van encryptie van de brondata waarbij de cryptografische sleutels binnen het eigen bedrijf worden opgeslagen en beheerd heeft als nadeel dat zaken als zoeken op basis van indexering niet meer werken. Lokaal gesynchroniseerde data is standaard niet versleuteld en is zo potentieel een bron voor een datalek bij verlies of diefstal.

Gebruikersgedrag
Doordat veel medewerkers privé al consumenten filesharingdiensten gebruiken, zullen zij terughoudend zijn om mogelijke, net iets minder handige, zakelijke EFSS-diensten te gaan gebruiken. Gebruikersgemak en -bewustwording is cruciaal om medewerkers te verleiden naast heldere en werkbare gebruiksvoorwaarden en beleidskaders. Maar al te vaak zullen er anders privéfoto's en bestanden opgeslagen gaan worden als back-up voor thuis. Gebruikersfouten, zoals het abusievelijk delen van een hele map in plaats van een enkel bestand, zijn natuurlijk ook aandachtspunten. Daarnaast moeten de gebruikskaders van andere losse opslagmedia zoals USB-memorysticks dan wel losse harde schijven helder zijn voor de gebruikers.

Identiteiten en authenticatie
Integratie van EFSS-diensten met de eigen directory services (zoals AD) is eigenlijk een must om accounts makkelijk te kunnen beheren en het wachtwoordbeleid te kunnen afdwingen. Het gaat hierbij dus om provisioning van accounts en authenticatie met behulp van bijvoorbeeld het SAML v2 protocol. In geval van claim based authenticatie kan men ook gebruikmaken van de eigen IDP (identity provider zoals ADFS of SecureAuth) met eigen toegangsregels, inclusief het afdwingen van twee factor authenticatie. Door federatieve afstemming en afspraken tussen organisaties wordt het delen van data makkelijker. Binnen de Nederlandse onderwijs- en onderzoeksinstellingen biedt SURF een gezamenlijke EFFS-dienst SURFdrive aan waarbij alle medewerkers van de aangesloten instellingen federatief kunnen inloggen (5).

Digital rights management
Inzet van een EDRM-systeem (Enterprise Digital Rights Management) om te voorkomen dat specifieke documenten gedeeld worden, is in specifieke gevallen noodzakelijk. Implementatie en gebruik van EDRM-systemen is echter complex en werkbaarheid voor medewerkers is een cruciaal aandachtspunt. Eventueel zou ook besloten kunnen worden om via geo-fencing (op basis van IP-gegevens) de toegang vanuit bepaalde landen tot EFFS-dienst te beperken. De bescherming hiervan is echter beperkt omdat dit door gebruik van VPN-verbindingen omzeilt kan worden.

Conclusie

Inzet van EFFS-diensten is complex en omvat veel aspecten variërend van security, privacy tot gebruikersgemak waarmee rekening gehouden zal moet worden. Geen keuzes maken als organisatie is erger dan richting geven, ook al zijn het soms suboptimale oplossingen. Ongecontroleerd gebruik of niet gebruikmaken van de functionele mogelijkheden van EFFS-diensten is een gemiste kans. Dus ja, voor onderwijs en onderzoek geldt zeker: dare to share! Intensieve en veilige samenwerking met partners en in productieketens en netwerken is cruciaal. Neem indien mogelijk, als sector of keten, hierin het initiatief en vorm federaties waarbinnen informatie veilig gedeeld kan worden.

Referenties

(1) Magic Quadrant for Enterprise File Synchronization and Sharing door Monica Basso, Karen A. Hobert, Jeffrey Mann – 2016 – Gartner
(2) The Top 10 Best Practices for Choosing and Deploying an Enterprise File Sync and Sharing Solution door Charles Smulders, Monica Basso, Karen A. Hobert – 2016 – Gartner
(3) Zie https://storro.com/
(4) How to Mitigate the Risks of Public Cloud EFSS and Storage door Raj Bala, Monica Basso – 2016 – Gartner

EEN KWESTIE VAN DEFINITIE

Precies één jaar na de bloedige aanslag in mijn woonplaats Apeldoorn bezocht ik als echte risicomijder om die reden op Koninginnedag de Warsteiner-bierbrouwerij in Duitsland. De radio speelde juist 'Happiness is Just Around the Bend' toen mijn vriendin en ik het landgoed opreden en zo was het ook.

Metershoge, wit-geel-gouden vlaggen wapperden in wind en zon. Het gebouw met de voor het bedrijfskritieke proces o zo belangrijke koperen ketels ('kroonjuwelen') wees fier de lucht in. Vlak daarnaast het hoekige bezoekerscentrum dat als een hypermoderne gebruikersschil om de brouwerij (als legacy systeem) heen was geplaatst. Ook de speciale wasstraat voor de vrachtwagens van het merk was goed zichtbaar. Er is namelijk slechts één Warsteiner-brouwerij op de wereld, dus alle transport vertrekt vanaf dit punt als centrale hub. Daar worden de vrachtwagens gewassen en indien nodig voorzien van nieuwe belettering wanneer het logo (ongeveer iedere eeuw) verandert. Vroeger ging dat vervoer met paard en wagen. En paarden staan er nog steeds in hoog aanzien, zoals blijkt uit sponsoring van wedstrijden en concoursen. De brouwerij waardeert de dieren nog steeds als werknemers en in ruil voor hun representatieve en sportieve arbeid wordt er goed voor ze gezorgd in ruime weilanden rondom de brouwerij. Deze weilanden zijn wel omheind; niet met schrik- of prikkeldraad maar met grote, houten witgelakte hekken. JR Ewing's ranch en landerijen uit de tachtigerjaren tv-serie Dallas. Men heeft op zich wel vertrouwen in het veiligheidsbewustzijn van de medewerkers, maar biedt vriendelijke hulp bij het naleven van de essentiële regels.

We checkten in bij het Warsteiner Gästehaus op het landgoed en brachten de weekendtas naar onze kamer, waar in de minibar reeds enkele gratis biertjes gekoeld stonden te wachten. De fabriek produceert alleen van maandag tot donderdag. Daarna wordt er gepoetst. Ook op vrijdag kun je met een elektrisch treintje door de fabriek rijden, terwijl er die dag dus niets gebeurt. Het gevoel van: na maandenlang plannen komt de directie eindelijk eens kijken op het SOC en net die middag is het zeer rustig, qua incidenten.

Na de rondleiding door de fabriek en proeverij (twee stuks) liepen we over het landgoed en vonden een restaurant op het bedrijfsterrein. Helaas voor mijn vriendin en mij was er een besloten feest aan de gang: een kersvers echtpaar vierde daar hun huwelijksfeest in een bierbrouwerij! Alle

twee waren we aangenaam verrast door dit buitengewoon goede idee (zij het elk met een andere klemtoon). We verlieten het landgoed en kwamen in het aanliggende stadje terecht. Daar zagen we achtereenvolgens een Warsteiner Café, een Warsteiner Konditorei, een Warsteiner Apothek, een Warsteiner Zeitung en een Warsteiner Rathaus . Al snel werd duidelijk dat het niet ging om een totaal uit de hand gelopen sponsoring door de zo geliefde brouwer. Het waren allemaal verwijzingen naar de plaatsnaam Warstein, waar ook de brouwerij en haar bier naar waren vernoemd. Het bleek dus een kwestie van definitie: wat is Warstein?

Zo is het natuurlijk ook met security. Dat is ook overal, hoort overal bij, kan of moet overal aan worden toegevoegd. Zeker als je er als echte liefhebber naar kijkt: dan zie je overál toepassingsgebieden en mogelijkheden. Met name op plaatsen waar je collega's van andere afdelingen juist nog helemáál niet aan security hebben gedacht. Bij security speelt definitie en scopebepaling steeds een grote rol. Wie kent als securityprofessional niet het voorbeeld van de projectleider die oprecht denkt voldoende aandacht te hebben gegeven aan security in zijn project, door aan een dagelijkse backup van de ingevoerde gegevens te denken. Terwijl wij als security-experts meteen zien dat daarbij de integriteit en vertrouwelijkheid vergeten zijn. Of zoals ik ooit in een auditrapport mocht lezen: "dat de kwaliteitsaspecten integriteit en vertrouwelijkheid in het onderzochte aandachtsgebied en in de prioritering en implementatie van de requirements in dier voege onvoldoende aandacht hebben gekregen".

Wanneer in een organisatie geen gezamenlijke, gedeelde definitie en scope bestaat van wat 'security' voor die organisatie precies inhoudt, kunnen er twee groepen ontstaan. De ene groep (de business) denkt dat de andere teveel aan security doet en wil uitgeven; de andere groep (de security-afdeling) doet alsof de eerste groep te weinig aan security denkt en wil besteden.

Hoe kom je eenvoudig tot een werkbare (of betaalbare) definitie van security? Spreek als aanpak bijvoorbeeld af:

- Dat in de security-paragraaf van de Project Start Architectuur, altijd aandacht moet worden gegeven aan beschikbaarheid, integriteit èn vertrouwelijkheid van de betrokken data.
- Dat de vereiste niveaus voor deze B+I+V kunnen variëren van 1 t/m 3 en dat bij V=3 meer mitigerende maatregelen nodig zijn dan bij 1. Geef als handreiking een lijst met bijvoorbeeld de beheersmaatregelen uit de ISO 27002 (Code of Practice for Information Security) en geef aan welke maatregelen altijd nodig zijn (al bij niveau 1) en welke alleen of pas bij BIV-niveau 2 of 3.
- Dat er een bruto risico te bepalen is voor elk van de aspecten B+I+V en dat de security-maatregelen die werkelijk worden geïmplementeerd, dit mitigeren tot een lager netto risico. Sommige maatregelen (vooral de preventieve) verlagen de kans van optreden, andere beperken de impact (als het toch gebeurt) van het risico (met name de detectie en response maatregelen). Veel interne discussie is te vermijden, door per beheersmaatregel eenmalig te besluiten of deze de kans, of juist de impact beperkt en dit in een extra kolom te vermelden.

Heel soms (bijvoorbeeld net na een groot security-incident met veel media-aandacht) zijn de security-budgetten voldoende groot om alle bedachte maatregelen uit te voeren. Dan kan het netto risico zelfs nul worden. Maar in de meeste gevallen geldt: 100% veiligheid bestaat wel, maar is onbetaalbaar. Wanneer er dus nog wel (netto) rest-risico's zijn, worden die vastgelegd in een risico-analyse met een duidelijke motivatie waarom die restrisico's qua kans èn impact aanvaardbaar zijn voor het verantwoordelijk management. Waarbij datzelfde management dan weloverwogen kan tekenen bij het kruisje.

Drs. Robert Metsemakers RA RE CISSP heeft een rijk arbeidsverleden bij Achmea en diens voorgangers in verschillende security en audit functies. Dit artikel is op persoonlijke titel geschreven. Robert is bereikbaar via metsemakers@live.com.

Titel:	**Grip op de AVG**
Ondertitel:	**De nieuwe privacywet voor niet-juristen**
Auteurs:	**- Koen Versmissen CIPP/E**
	- mr. drs. Jeroen Terstegge CIPP-E/US
	- Natalja Krijgsman MSc CIPM
Taal:	**Nederlands**
Pagina's:	**120**
Uitgever:	**Wolters Kluwer, Deventer**
Datum:	**18 mei 2017**
ISBN:	**9789013139204**
Prijs:	**€ 39,95 (incl. btw)**

BOEKREVIEW

EEN GOEDE HOUVAST VOOR DE BEVEILIGER

Volgend jaar wordt de nieuwe Europese privacywetgeving van kracht. Internationaal bekend als GDPR (General Data Protection Regulation), in Nederland ook bekend als AVG (Algemene Verordening Gegevensbescherming). Deze wetgeving vergt extra organisatie rondom de verwerking van persoonsgegevens, waar bedrijven nu al voorbereidingen voor moeten treffen om klaar te zijn voor de invoering. Deze voorbereidingen vragen vooral ook overleg en afstemming met partners en leveranciers, wat maakt dat GDPR en AVG dus op dit moment hype-begrippen zijn in de ICT-markt. Dit boek richt zich op de professionals die niet zozeer een juridische achtergrond hebben en heeft tot doel de taaie juridische materie begrijpelijk en behapbaar te maken.

Samenvatting

Het boek 'Grip op de AVG' is geschreven onder beheer van Privacy Management Partners (1) en het lijkt een tweede deel te zijn uit een serie, gepositioneerd als opvolger op 'Grip op datalekken'. Het bevat negen hoofdstukken, de eerste twee hoofdstukken geven inleiding en context, het derde hoofdstuk beschrijft de AVG in het kort. De volgende vijf hoofdstukken diepen een aantal onderwerpen uit. In hoofdstuk 9 wordt afgesloten met de beschrijving van een aanpak voor de implementatie. Elk hoofdstuk wordt afgesloten met een korte samenvatting, onder de koppen 'Tips & Tricks' en 'Wat verandert er?'

Het voorwoord is geschreven door Bas Eenhoorn, de digicommissaris van Nederland. Dit geeft het boek zeker een formeel cachet.

Er is ook een werkboek beschikbaar en de auteurs verwijzen naar de blog van over onderwerp (2).

Evaluatie

Het boek leest makkelijk weg. Het is verrassend vrij van juridische taal, waarbij de essentiële juridische elementen uitgebreid en duidelijk worden uitgelegd. De opbouw is logisch en structureel, wat maakt dat het als gids in zijn

geheel gelezen kan worden, en het ook als handboek gebruikt kan worden waarin snel een detail terug te vinden is in de inhoudsopgave en het trefwoordenregister. In deze zin is het een uniek boek, niet alleen op de Nederlandse markt, maar ook internationaal. Als ik de whitepapers van leveranciers over dit onderwerp buiten beschouwing laat, kan ik maar twee Engelstalige boeken vinden die wellicht vergeleken mogen worden met dit boek.

Op één punt kan het lastig zijn voor grotere bedrijven dat de auteurs grotendeels besloten hebben vast te houden aan de Nederlandse terminologie. Ik begrijp het vanuit taalpurisme, maar de praktijk op de werkvloer is vaak anders, de Engelse terminologie raakt eerder ingeburgerd in een internationale omgeving.

Het is verrassend dat de auteurs in hoofdstuk 9 tot een handreiking voor de praktijk komen van slechts twaalf pagina's. Hier verworden wettelijke eisen tot de dagelijkse praktijk van managers, operationele uitvoerders en technische experts. De auteurs gebruiken een gefaseerde aanpak van drie stappen: uitdenken, implementeren en beheren. Storend hierbij vind ik dat er niets genoemd wordt over ontmanteling van systemen. Zeker, in eerste instantie zal dit nog niet aan de orde zijn, maar ik ga ervan uit dat dit boek de tand des tijds zal doorstaan en ook als handreiking gebruikt gaat worden in een tijd dat er onder AVG-beheer systemen ontmanteld moeten gaan worden.

En zoals vaak gedaan wordt bij beheer, wordt in fase 3 onder andere de Deming PDCA-cyclus gebruikt. Dat is prima, maar dan moet je elke stap wel een relevante inhoud geven. In de beschrijving van de auteurs krijgt de stap 'act' een hele magere invulling. Ze verzuimen bij 'act' het noemen van het permanent maken van de procesverandering die onder 'do' ingezet was.

Al met al een boek dat ik op mijn boekenplank wil hebben staan, want ik zal er regelmatig op teruggrijpen. Het lijkt me ook een goed boek voor managers om door te nemen, omdat zij hier in hun domein mee te maken gaan krijgen. Dit boek zal ze helpen om door de boodschap te prikken van hypende leveranciers en consultants die AVG-compliance out-of-the-box gaan proberen te verkopen.

Referenties

(1) https://www.pmpartners.nl/grip-op-avg/
(2) https://www.pmpartners.nl/grip-op-avg/blogserie/

Opmerkelijke quotes

2.4.3 Meerdere betrokken partijen
"Hoe dan ook is het zo dat niet de formele, maar de feitelijke situatie doorslaggevend is bij het bepalen van de rolverdeling."

3.5.3 Voorafgaande raadpleging
"Wij kunnen niet beter adviseren dan dat u in voorkomend geval de AP raadpleegt of die vindt dat zij geraadpleegd moet worden."

4.2 Doelbinding
"In deze tijden van sociale media, big data en het internet of things worden er steeds meer gegevens vastgelegd over ons, onze persoonlijkheid en ons gedrag zonder dat vooraf precies duidelijk is wat er allemaal voor moois of minder moois met die gegevens gedaan kan worden."

4.5.6 Toestemming
"Met name in een internetcontext moet het verzoek kort en bondig zijn, zodat het beoordelen ervan het afnemen van de betreffende dienst niet onnodig stoort."

5.1 Informeren van de betrokkene
"Hoe kunt u al die informatie geven, en tegelijkertijd voldoen aan de in paragraaf 5.7 besproken eisen van 'beknopt, transparant, begrijpelijk en gemakkelijk'?"

5.7 Algemene regels, onder Heldere communicatie
"Bij voorkeur zijn de teksten dan ook niet geschreven door juristen."

9.1.2 Kapstokbeleid
"Het toepassen van de voorschriften van de AVG is niet one size fits all, en zult u juist moeten toesnijden op uw organisatie."

9.2.2 Doen, onder Procesniveau
"Begin idealiter al in de ontwikkelingsfase van de verwerking met het uitvoeren van de DPIA."

Nawoord

"Bij wijze van uitgeleide willen we nogmaals beklemtonen dat het van groot belang is dat u het doel van de AVG niet uit het oog verliest doordat u krampachtig haar regels probeert te volgen."

Door Lex Borger, hoofdredacteur IB-Magazine, security consultant bij i-to-i en docent security aan de Hogeschool Utrecht. Lex is te bereiken via l.borger@i-to-i.nl.

PRIVACY, IK WEET HET ALS IK HET VOEL

Je kunt welhaast geen (online) krant meer openslaan of een broadcastmedium aanzetten of het gaat over privacy. Gedreven door een nieuwe wet, maar ook door allerlei incidenten, is er niet alleen steeds meer aandacht bij pers en politiek maar ook bij het 'lijdend' voorwerp zelf. De burger, klant, - gewoonweg jij en ik - maken zich steeds meer zorgen of er wel goed met onze gegevens wordt omgegaan. We trekken ook makkelijker aan de bel bij bedrijven en overheden om verhaal te halen. Gelukkig worden we ook steeds beter te woord gestaan. Maar toch blijven er zaken waar we ons enorm over opwinden omdat ze ons in ons persoonlijke (privé)leven raken. Zo is er die moeder die zich vreselijk druk maakt over de app die de school gebruikt op de iPads van haar kinderen. Met die app kan de camera van de iPad worden overgenomen en de school ziet er geen kwaad in. Of die werknemer die zich afvraagt waarom de volgapparatuur in zijn auto niet uit kan als hij pauze neemt en die zich afvraagt waarom het überhaupt nodig is dat zijn baas hem overal en altijd maar kan volgen. Iedereen heeft wel van die momenten dat de privacyharen recht overeind gaan staan. En beste redactie, waar hebben jullie je de laatste tijd enorm druk over gemaakt als het om privacy gaat?

Tom Bakker

Er zijn vele privacyzaken geweest waar je je enorm druk over kunt maken. Zo lijkt het wel dweilen met de kraan open: elke dag is er ergens wel een lek geweest, veroorzaakt door hackers of door menselijk falen (of beiden). Ik noem dat meer zorgelijk dan druk maken. Iets nieuws was laatst de verborgen camera's in reclameborden op NS-stations die reizigers stiekem bespioneren. Normaal gesproken moet je dat wel via stickers of bordjes bekend maken, net als bij CCTV-bewaking.

Dan de 'sleepnet' wet. Hier is het argument steeds weer: security (veiligheid) versus privacy. Net of die elkaar uitsluiten. Daar word je nu wel een beetje moe van. Waar ik me niet zo zeer druk over maak maar meer nieuwsgierig naar ben, is de impact van de AVG volgend jaar. Hoewel veel bedrijven nog flink achterlopen met de te nemen maatregelen, als ik de persberichten mag geloven, is het min of meer wel duidelijk wat er moet gebeuren. Het gaat straks echt interessant worden hoe bedrijven als Google en Facebook hun compliancy gaan regelen. Hun businessmodel is immers het verzamelen en


Maarten Hartsuijker


Tom Bakker


Lex Borger

verkopen van onze persoonsgegevens. Het voldoen aan de AVG zal voor hen moeilijk zijn of misschien zelfs wel onmogelijk. En wat te denken van die profiling-bedrijven, die we niet eens kennen omdat die stiekem zonder onze toestemming ons surfgedrag verkopen aan adverteerders.

Lex Borger

Ik vind het knap hoe creatief sommige mensen zijn in het herkennen van privacyproblemen, zoals het voorbeeld van de iPad in de inleiding. Het vervelende van privacyproblemen is dat ze geleidelijk aan binnensluipen. Wij zijn dan de kikker in het geleidelijk warmer wordende water. Waar heb ik me druk om gemaakt? Hierover denkend zijn het eigenlijk geen zaken met brede maatschappelijke impact: de toename aan aanbiedingen van loyaliteitsprogramma's bij winkels waar ik weinig kom. Als ik een tuinproject doe, kom ik bij een aantal vakhandels waar ik me 'moet' registreren om aanbiedingen te krijgen. Kijkend naar de blauwe bouwmarkt zie ik dat ik mijn huid goedkoop verkoop: ik schat mijn besparing op een tientje jaarlijks. Laatst bleek mijn loyaliteitskaart bij een andere vakhandel niet meer geldig te zijn. Toch maar de gelegenheid gepakt om door te vragen. Konden ze zien dat hij bestond en niet geldig was, of kwam ik niet meer voor in hun bestand? "U komt niet meer voor", wisten ze me te vertellen. Hebben ze nog informatie over mij? "Nee", was het antwoord. Kan ik dit vertrouwen? Is dit te controleren? Ik dacht even na. "Houden zo", besloot ik. Een ander geval: na vakantie wil je graag een fotoboek samenstellen. Op de website kun je prachtig hele ladingen foto's uploaden en een opmaak maken, maar bij bestellen gaat er wat mis. Nu zweven mijn vakantiefoto's wellicht als wezen (orphans) rond in een fotocloud van een fotobewerkingsdienst, zonder dat ze aan mij gelinked zijn. Ik ben benieuwd hoe dat werkt als ik een opvraag doe over mijn gegevens.
Waar maak ik me dus kennelijk druk om? Niet zozeer om de informatie die ik 'moet' afgeven, waarbij de verwerking goed gaat. Maar wat gebeurt er met de snijverliezen die niet aan een persoon gekoppeld zijn? Worden die netjes opgeruimd? Of op een hoop geveegd en bekeken? Onder het mom van ... (vul in)?

Maarten Hartsuijker

Het beschermen van je privacy wordt steeds moeilijker. Retailers willen het gebruik van contant geld ontmoedigen. En tegelijk zien steeds meer banken jouw digitale transacties als handelswaar. Als de Wet zeggenschap lichaamsmateriaal er komt, kun je op termijn geen bloed meer laten onderzoeken zonder in een DNA-databank terecht te komen. Ongetwijfeld vanuit de beste bedoelingen. Maar hoe waarborg je goede bedoelingen op het moment dat nieuwe regeringen een dataverzameling minder ethisch in besluiten te zetten? Je kunt geen website meer bezoeken zonder dat je gedrag op de achtergrond wordt vastgelegd en verkocht. En daar waar de gegevens volgens de verzamelaar `geanonimiseerd' zijn of worden, blijken ze vaak relatief eenvoudig te repersonaliseren. Als ik zelf terughoudend ben met het delen van informatie met bijvoorbeeld Google, dan ontvangt die organisatie toch informatie over mij omdat anderen hun mobiel met Google hebben gekoppeld.

De techniek om beeldmateriaal aan persoonsgegevens te koppelen wordt steeds beter. En apparatuur in je huis (bedoeld voor gemak of als speelgoed voor de kinderen) blijkt beelden en persoonlijke gegevens terug te sturen naar de fabrikant.
Steeds meer ambtenaren gebruiken de Algemene Wet Bestuursrecht om persoonsgegevens te vorderen. De toegang tot dataverzamelingen die vroeger onder veel protest voorzien van privacywaarborgen zijn opgezet wordt, continu verder opgerekt. En de camera's van politiehelikopters bleken recent ook uitermate geschikt om naturisten te filmen.
Bestel je op internet nu nog zo anoniem mogelijk? Als het eID-stelsel breed geaccepteerd en ingezet wordt dan zal ook dat stukje privacy tot het verleden horen. En komen je echte personalia bij veel meer organisaties terecht dan je mogelijk zelf wenselijk acht.

Is dit dan waar ik mij druk over maak? Nee, om heel eerlijk te zijn maak ik mij niet over al deze onderwerpen even druk. Als ik aan privacy denk, gaat het voor mij om mijn keuzevrijheid om iets wel of niet te delen. Online zou dat heel eenvoudig kunnen, bijvoorbeeld door bedrijven te verplichten de `do not track' keuzes van individuen te respecteren. Maar die wil is er niet. De handel in kennis over mij is een industrie geworden. En ik zie dat de industrie nog niet staat te springen om mij mijn recht op privacy makkelijk te laten uitoefenen.

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
Lex Borger (hoofdredacteur, werkzaam bij i-to-i)
e-mail: hr@pvib.nl
MOS bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Tom Bakker (Digidentity BV)
Kas Clark (NCSC)
Lex Dunn
Maarten Hartsuijker (Classity)
Rachel Marbus (KPN)
Bart van Staveren

ADVERTENTIE-ACQUISITIE
e-mail: adverteren@pvib.nl;
of neem contact op met MOS
T (033) 247 34 00
ibmagazine@pvib.nl

VORMGEVING EN DRUK
VdR druk & print, Nijkerk
www.vdr.nl

UITGEVER
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
e-mail: secretariaat@pvib.nl
website: www.pvib.nl

ABONNEMENTEN 2017
De abonnementsprijs in 2017 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

PvIB abonnementenadministratie
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl

ISSN 1569-1063

CURIEUZE PRIVACY

Mijn hele werkzame leven heb ik doorgebracht in de IT en later in de informatiebeveiliging. Veel nieuwe woorden en nieuwe begrippen zijn afkomstig uit die wereld en worden nu gebruikt alsof het al jaren bestaat, denk hierbij aan WiFi, USB-stick, muis en zo kan ik nog wel even doorgaan. Iedereen is nu aan die woorden gewend. Ondanks het feit dat we niet allemaal weten hoe het precies werkt, gebruiken we het gewoon.

Datzelfde geldt voor het begrip privacy, eenieder geeft daar een eigen invulling aan. Een voorbeeldje. Mijn vader moest laatst verhuizen en ik moest een nieuw paspoort aanvragen. Dus ik dacht deze twee zaken wel even te kunnen combineren. Machtiging laten schrijven door mijn vader, zijn identiteitsbewijs meegenomen en ook zijn inloggegevens van DigiD gekregen. Mijn eigen identiteitsbewijs ook meegenomen en fluitend ging ik naar het gemeentehuis. De aanvraag van mijn paspoort was zo klaar, die kon ik over vijf werkdagen ophalen. De adreswijziging van mijn vader werd iets lastiger. Het aardige meisje achter de balie zei mij dat ik de adreswijziging niet kon doorgeven. Ik liet mij niet uit het veld slaan en legde triomfantelijk het identiteitsbewijs van mijn vader op de balie.

De glimlach van het meisje werd minder uitbundig en wederom moest ik aanhoren dat het niet kon zoals ik wilde, omdat "iedereen wel een identiteitsbewijs op de balie kon leggen". Mijn humeur werd nu wel heel snel minder. Ik zei tegen het nog steeds aardige meisje dat zij wel wist dat ik niet 'iedereen' was en dat ze in haar administratie wel kon zien dat ik één van de zonen was. Inmiddels was de glimlach bij haar helemaal verdwenen toen ik de handgeschreven machtiging op de balie legde. Ze las de machtiging aandachtig door en schudde haar hoofd tijdens het lezen. Ze begon haar zin met "meneer Berry", de rest heb ik niet gehoord want zo'n aanhef belooft niet veel goeds. Het aardige meisje keek mij aan en zag mijn teleurstelling. "U kunt wel op onze website het adres van uw vader wijzigen, dan heeft u alleen maar de DigiD inloggegevens van uw vader nodig" meldde ze. Haar glimlach verdween snel toen ik haar vriendelijk bedankte en opstond. Ze besefte kennelijk zelf hoe krom het klonk. De adreswijziging was kort daarna ook voor elkaar.

Een tweede voorbeeldje is het uitvoeren van een zogenaamd 'Medewerker Tevredenheid Onderzoek'. Deze onderzoeken vinden plaats onder volstrekte anonimiteit zodat iedere medewerker zonder enige terughoudendheid kan aangegeven wat hij of zij vindt van de organisatie, management werkinhoud en dergelijke. De uitnodigingen worden per mail gezonden en in deze mail wordt nogmaals verzekerd dat het onderzoek volstrekt anoniem is. Wanneer je het onderzoek niet invult krijg de medewerker een melding per mail dat het onderzoek nog niet is ingevuld. Of erger nog, je manager spreekt je aan op het feit dat je in gebreke bent gebleven. Ik blijft dit curieus vinden, want men weet dus wel wie het niet heeft ingevuld. Zou de organisatie dan geen inzicht hebben in de antwoorden van degenen die het onderzoek wel hebben ingevuld? Misschien neemt niet iedereen het begrip privacy serieus.

Berry

SECURITY ACADEMY

SECO-Institute DPO track: dé privacy certificering

Behaal de officiële Internationale S-DPF en S-DPP certificering van het **SECO-Institute**, zodat u en uw bedrijf optimaal voorbereid zijn op de algemene verordening gegevensbescherming (**AVG**) / de General Data Protection Regulation (**GDPR**). Zowel voor de beginnende (S-DPF) als de gevorderde privacy functionaris (S-DPP). Bij de Security Academy kunt u de juiste opleidingen volgen ter voorbereiding op de examens.

Tijdens de opleidingen leert u welke impact de wet- en regelgeving op het gebied van privacy heeft op de processen, rollen en verantwoordelijkheden in uw organisatie.

Privacy & Data Protection FOUNDATION | S-DPF

Startdata: 13 nov, 6 dec, 19 feb

Privacy & Data Protection PRACTITIONER | S-DPP

Startdata: 21 nov, 6 maart, 31 mei

* Op dit moment biedt Security Academy de Foundation- en Practitioner opleiding in deze track, waarmee u de DPO functie kunt uitoefenen.

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