SPECIAL

INFORMATIEBEVEILIGING MAGAZINE

THEMA: PRIVACY

- Privacy in tijden van pandemie
- Hoe creëer je bewustwording bij medewerkers?
- Column - De ultieme privacy-oefening

JAARGANG 20 - 2020 - EDITIE 3

Privacy special

Rachel

Deze privacy special kwam tot stand onder bijzondere omstandigheden. De coronacrisis houdt ons momenteel in haar greep en samen proberen we er thuis het beste van te maken. Dat gaat met vallen en opstaan, het tempo is wat lager, maar tegelijk biedt het ook weer mooie momenten voor nieuwe verbinding. Er is rust en ruimte om elkaar beter te leren kennen en wat meer bij onze buren naar binnen te gluren om te vragen of het nog wel goed met ze gaat.
Omdat ik nog geen idee heb of we al wat meer bewegingsvrijheid hebben als deze editie op de mat valt, stel ik me zo voor dat een mooie dikke privacy special een welkome afleiding kan zijn. Verschillende onderwerpen komen aan bod en uiteraard ontbreekt de huidige virale crisis daarin niet. Maar er is ook geschreven over privacy in de zorg, bewustwording, DPIA's en Citrix. Meer dan genoeg om een aantal uren leesplezier mee te vullen.

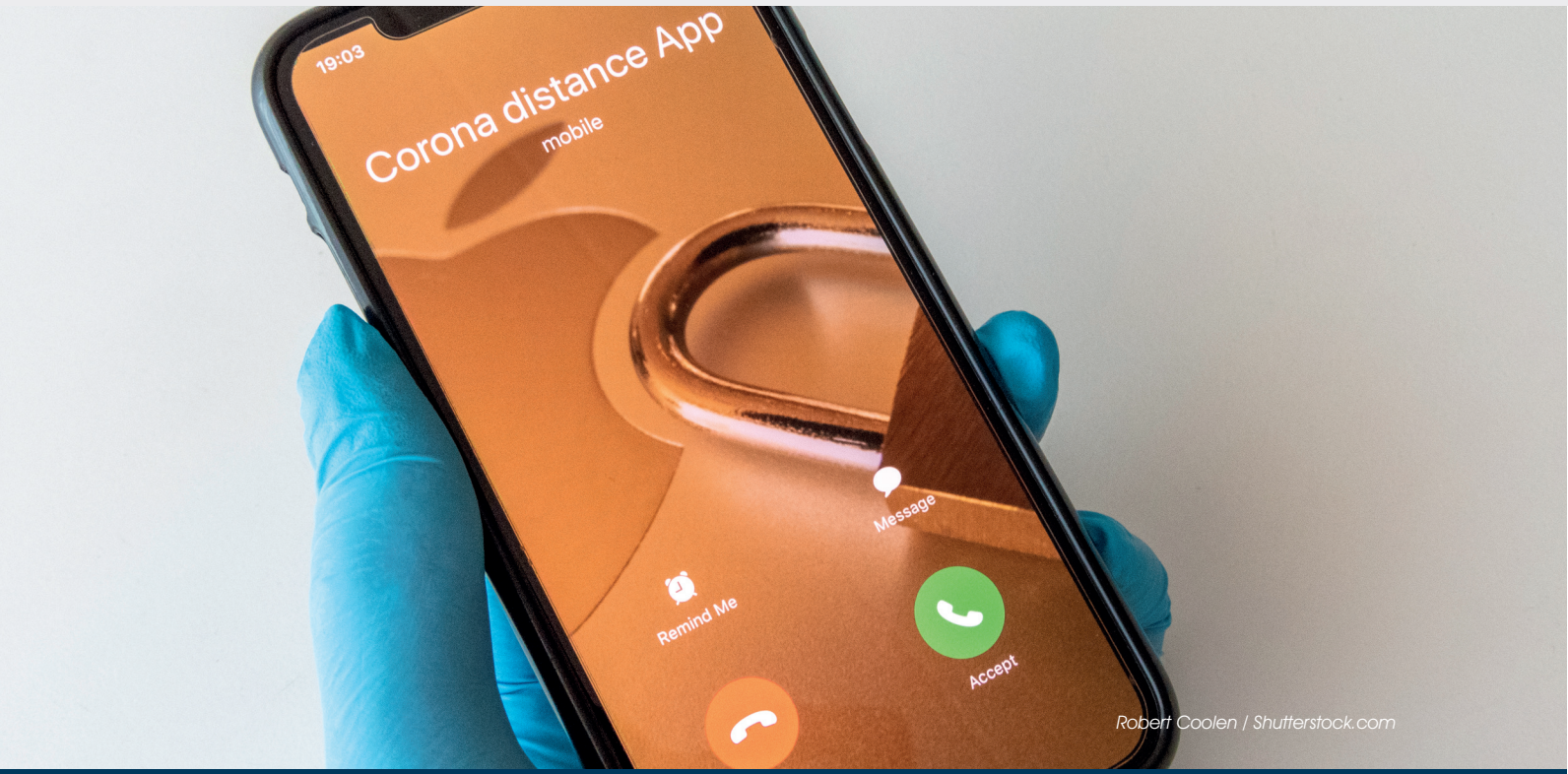
Ik hoop dat alle lezers in goede gezondheid zijn en veilig kunnen genieten van dit speciale nummer. En voor wie zijn geliefden verloor en moest begraven: ik wens jullie ontzettend veel sterkte en liefde tijdens deze periode van rouw.

Was je handen, houd afstand en zorg voor elkaar.

Rachel Marbus

IN DIT NUMMER

Auteur: Rachel Marbus, Lead Privacy Aegon Nederland, bereikbaar via Rachel.Marbus@aegon.nl



Robert Coolen / Shutterstock.com

Privacy in tijden van pandemie

Rechten en vrijheden

De wereld bevindt zich in zwaar weer. Grote groepen mensen worden ziek, zijn het al (geweest) of overlijden. Landen sluiten de grenzen, burgers sluiten hun deuren. Het virus is zo besmettelijk dat iedereen die het onder de leden krijgt ogenblikkelijk wordt afgezonderd. Dit is het scenario voor een humanitaire ramp, maar kan tevens een voorbode vormen voor een totalitaire maatschappij waar het 'goede voor allen' blijvend ten koste gaat van 'de vrijheid van eenieder'.

We weten nog te weinig over het virus en de werking ervan en we zijn naarstig op zoek naar een vaccin. Wat we wel weten is dat het virus heel erg besmettelijk is en daardoor makkelijk overgedragen wordt door onder meer niezen en hoesten. Om het virus te beheersen wordt daarom zoveel mogelijk informatie vergaard. Daarnaast moeten mensen geïsoleerd worden als ze ziek zijn en mogen anderen niet meer samenkomen. Als mensen toch buiten komen, moeten ze zorgen voor ten minste anderhalve meter afstand tot elkaar. Het vergaren van informatie en het ervoor zorgen dat personen zich aan isolatie en afstand houden, zijn beide noodzakelijk om het aantal ziektegevallen in tijd te spreiden. Zodat de zorg niet overbelast raakt en het virus hopelijk op den duur met een vaccin en/of medicatie te bestrijden valt. Dat hiermee rechten en vrijheden onder druk komen te staan, is een gegeven en is tot in bepaalde mate ook niet meer dan logisch en zelfs geheel geoorloofd. Maar waar liggen nu eigenlijk de grenzen? Wanneer is de noodzakelijke inbreuk op de privacy van personen niet meer noodzakelijk en gaat het de grenzen van het betamelijke te buiten? Juist nu, in tijden van nood op wereldschaal, is het zaak om die spanning te benoemen en aan te wijzen. Omdat ook juist nu het heel makkelijk is om over de grenzen van het betamelijke heen te stappen en wellicht zelfs wel permanente schade aan te richten.

Corona-volg-apps

Het voert te ver om in het kader van dit artikel alle apps en andere volgsystemen die wereldwijd ingezet zijn of ingezet gaan worden te benoemen. Temeer daar we, ten tijde van het schrijven, nog volop in de coronacrisis zitten en veel landen nog niet eens in de ernstigste situatie zijn aangekomen. Om toch een beeld te schetsen geef ik een aantal voorbeelden van methodes om mensen te volgen in tijden van corona. In praktisch alle gevallen gaat het om het volgen van personen door de overheid, al dan niet in samenwerking met bedrijven die dit volgen mogelijk maken. Europese wetenschappers gaan een app maken waarmee coronapatiënten gevolgd kunnen worden. Dat wordt gedaan door gebruik te maken van de locatiedata gegenereerd door mobiele telefoons. Een en ander zou op een privacyvriendelijke manier moeten worden ingericht; het project heeft dan ook de hoopvolle naam Pan-European Privacy Preserving Proximity Tracing (PEPP-PT) gekregen (1). Middels de app wordt in de gaten gehouden bij welke andere mobiele telefoons de telefoon van een besmette persoon in de buurt is geweest. De Ierse overheid zal haar eigen app gaan uitrollen, waarbij het gebruikers vrijstaat deze al dan niet te gaan gebruiken. De app houdt bij of je bij iemand in de buurt bent (of bent geweest) die positief getest is op COVID-19. De app die in Moskou ingezet wordt, volgt alle bewegingen van mensen die daar verplicht thuis moeten blijven. Deze app volgt dus weliswaar iedereen, maar wordt tot nu toe specifiek ingezet voor mensen die woonachtig zijn in een bepaald gebied. Daarnaast gaat Moskou een systeem met een QR code inzetten waarbij iedere burger een unieke code krijgt toegewezen. Critici doopten de maatregelen in Moskou al tot een `digital concentration camp'(2).
De Singaporese app, TraceTogether (sic!), zorgt ervoor dat iemand die de app op zijn telefoon heeft, een waarschuwing krijgt zodra hij of zij in de buurt is geweest van een persoon bij wie corona is vastgesteld. De app werkt door middel van bluetooth tracking en hoeft niet verplicht geïnstalleerd te worden, hoewel de overheid wel degelijk aanstuurt op het gebruik ervan. Zuid-Korea doet het weer net even op een andere manier. Daar maakt de overheid gebruik van het verzenden van pushberichten naar iedereen die in de buurt is geweest van iemand die positief heeft getest. Leeftijd, geslacht en reisgeschiedenis van de patiënt worden in het pushbericht genoemd. Amerikaanse wetenschappers werken aan een app genaamd `Private Kit: Safe Paths'(3). Bij het gebruik van die app kunnen patiënten ervoor kiezen om hun locatiegeschiedenis te verstrekken aan de zorgverlener. Die zorgverlener ontdoet de informatie dan van identificerende gegevens waarna de wandelgangen in het systeem worden ingeladen. Iedereen die in de buurt is geweest van deze patiënt krijgt dan een waarschuwing.

Nederlandse maatregelen en initiatieven

In Nederland is het LUMC (Leids Universitair Medisch Centrum) begonnen met een initiatief om zoveel mogelijk informatie te verzamelen via een app genaamd Covid Radar. Deze app heeft tot doel om gegevens over de verspreiding en de context te verzamelen. Aan de hand van de uitkomsten daarvan wordt beleidsadvies gegeven. De Covid Radar wil ook in de gaten houden in hoeverre gebruikers zich houden aan social distancing en wat de effecten zijn van interventies in bepaalde bevolkingsgroepen. De gegevens worden opgeslagen in Nederland en voor vijf jaar bewaard. Gebruikers geven in de app zelf toestemming voor het verwerken van de gegevens. Zij vullen de postcode in en beantwoorden per persoon in het

huishouden een aantal vragen. Bij de persoonskenmerken gaat het om een naam, leeftijdscategorie en of je al dan niet werkzaam bent in de gezondheidszorg. Daarna volgt een lijst met gezondheidsvragen, vragen over reisbewegingen en nabijheid van (zieke) mensen. De app maakt alleen gebruik van vragenlijsten.

Vooralsnog heeft Nederland zich nog niet bij andere initiatieven aangesloten, maar gezien de ontwikkelingen op wereldschaal is het niet denkbeeldig dat dergelijke volgapps die gebruik maken van locatiegegevens ook bij ons op zijn minst een onderwerp voor discussie zijn. Nederlandse telecomproviders hebben immers al verzoeken gekregen voor het delen van de locatiedata van hun klanten om zo onder meer groepsvorming in kaart te brengen (4). Daarnaast heeft Google de bewegingen van Nederlanders in kaart gebracht door de locatiegegevens van haar gebruikers te analyseren (5). In een artikel van de Volkskrant geeft het RIVM aan vooralsnog geen heil te zien in het in stelling brengen van apps die Nederlanders continue gaan volgen. Echter geeft ze daarbij ook aan dat die stelling op later moment best eens zou kunnen veranderen (6). Overigens worden lokaal al zogenaamde coronascreeners gebruikt, aan corona aan te passen versies van de Questmanager van Philips (7). Het gaat daarbij om het online screenen van mogelijke zieken door middel van vragenlijsten en daar waar nodig in samenwerking met callcenters. Patiënten worden op basis van de vragenlijst in een risicoklasse ingedeeld. De antwoorden op de vragenlijsten zullen voor langdurig wetenschappelijk onderzoek gebruikt gaan worden. De coronascreeners worden nu alleen nog door zorgverleners gebruikt, maar het is niet uitgesloten dat de resultaten op den duur ook gedeeld zullen worden met de overheid.

Kliklijnen

Daarnaast worden op lokaal niveau andere middelen ingezet die een vrijheidsbeperkende werking kunnen hebben. De gemeentes Purmerend en Beemster hebben een kliklijn geopend waar burgers kunnen aangeven als ze mensen in een groep op straat zien lopen. Ook andere overtredingen van de maatregelen die door het kabinet genomen zijn, kunnen gemeld worden (8). Tevens worden drones ingezet om te kijken of mensen zich – vooral in kustplaatsen – wel aan de vereiste anderhalve meter afstand houden (9). Dat gaat nog redelijk onschuldig, mensen die dicht bijeen lopen, krijgen een waarschuwing met de vraag om meer afstand te houden.

In België doen ze er nog een schepje bovenop en zijn de drones voorzien van een hittesensor waarmee gecontroleerd wordt of er niet mensen 'illegaal' in vakantiehuisjes verblijven (10). Maar ook Nederland is niet vies van een controle achter de voordeur. De provincie Zeeland wil dat alleen ingezetenen met een hoofdverblijfplaats in de provincie blijven. Iedereen die op vakantieparken of in zijn eigen tweede huis verblijft, mag daar niet langer blijven. De veiligheidsregio Zeeland heeft dit geregeld middels een noodverordening. Boa's zijn vervolgens ingezet om achter voordeuren te gaan controleren (11).

Ondertussen pleit het kabinet ervoor om medische gegevens van besmette patiënten makkelijker vrij te geven, ook als zij daar zelf geen toestemming voor hebben gegeven. Niet iedereen heeft in Nederland een keuze gemaakt betreffende inzage in het medisch dossier. Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) werkt momenteel aan een plan daartoe. Zij geven aan eventuele aanbevelingen van de Autoriteit Persoonsgegevens mee te zullen nemen. Daarnaast is in opdracht van VWS gewerkt aan een database waarin het ziekteverloop door COVID-19 bij verstandelijk gehandicapten wordt vastgelegd. (12)

Anonimiseren en big data

Praktisch alle oplossingen voor mobiele telefoons die op dit moment worden uitgerold of bedacht, maken gebruik van grote bergen data. In veel gevallen gaat dat gepaard met het gebruik van de locatiedata van de gebruiker. Zeker daar waar er sprake is van locatiedata en het tracken van personen is er eigenlijk praktisch geen optie om dat anoniem te realiseren. Alleen wanneer je eventuele groepsvorming zou willen monitoren, zou je een individu nog kunnen laten wegvallen in de massa. Overigens kunnen drones net zo goed ingezet worden om gebieden te overvliegen om groepen in kaart te brengen. Dat is immers ook al succesvol gebleken in de Nederlandse kustgebieden. De vraag is of het dan ook echt nodig is om daarvoor locatiedata van telecomproviders in te zetten. Het probleem bij het gebruik van locatiedata is dat deze data toch altijd weer redelijk makkelijk naar een individu terug te leiden is, zeker nu praktisch alle Nederlanders bij voortduring achter de eigen voordeur zitten. Daar komt bij dat, wil het gebruik van de app zinvol zijn, een (vermoed) besmet persoon op de een of andere manier geregistreerd moet worden en nauwgezet gevolgd moet worden, inclusief de personen die in de buurt komen van deze patiënt. Hoe makkelijk het is om met behulp van locatiedata heel veel over een persoon te achterhalen bewees de New York Times nog niet zo lang geleden met een prachtige visual (13). Er waren 50 miljard datapunten

van 12 miljoen Amerikanen verzameld over een periode van een paar maanden. Binnen die bak data was het een koud kunstje om zeer gedetailleerde gegevens van personen te achterhalen. "Yes, the location data contains billions of data points with no identifiable information like names or email addresses. But it's child's play to connect real names to the dots that appear on the maps," aldus de NYT. Data in grote hoeveelheden kennen unieke patronen en die leiden vaak zeer makkelijk naar personen. En bij het gebruik van locatie is maar zeer weinig nodig om terug te kunnen leiden naar een unieke persoon. "Of the many digital traces we leave in daily life, location metadata may be the most revealing. Our real world movements are so distinctive that most people can be identified from a few data points within a single data set" (14).

Noodverordeningen en het democratisch deficit

Inmiddels zien we veel lokale maatregelen opkomen naast de maatregelen die de Rijksoverheid oplegt. Dat gaat via noodverordeningen van de voorzitters van de Veiligheidsregio's. Zij ontlenen deze bevoegdheid aan de crisissituatie en artikel 39 van de Wet veiligheidsregio's. De voorzitter van de veiligheidsregio neemt daarmee alle bevoegdheden van de burgemeesters over. Het bestuur van een veiligheidsregio bestaat uit alle burgemeesters uit die veiligheidsregio. Een van deze burgemeesters wordt bij Koninklijk Besluit benoemd tot voorzitter van de veiligheidsregio. Meestal is dit de burgemeester uit de grootste gemeente. De noodverordeningen laten in verschillende bepalingen nog veel ruimte om op basis van de algemeen vastgelegde regels concrete besluiten te nemen. Bijvoorbeeld door specifieke gebieden aan te wijzen waar het verboden is te komen. Toezicht en handhaving wordt in handen gelegd van politie, gemeentelijke opsporingsambtenaren en ook militairen. Wie de noodverordening (of de regels die eruit voortkomen) overtreedt kan een gevangenisstraf van ten hoogste drie maanden opgelegd krijgen of een geldboete in de tweede categorie (maximaal € 4350). De geldigheid van de verordening wordt gelijkgetrokken met de termijnen die het kabinet stelt. De gemeenteraden staan door deze noodverordeningen buiten spel en hebben geen democratische macht meer in het stellen, laat staan het becommentariëren, van de regels. De besluiten die genomen kunnen worden door de voorzitter van de veiligheidsregio kunnen zelfs (tijdelijk) wetten opzij zetten. Aan de democratische legitimatie van de besluiten kan dan ook zeer getwijfeld worden. De legitimerende controle door de gemeenteraad is immers door artikel 39 van de Wet veiligheidsregio's goeddeels weggevallen.

(On)vrijwillige keuze

Verschillende initiatieven om informatie te vergaren over corona en persoonlijke omstandigheden werken op basis van vrijwillig te verstrekken informatie. Het principe van vrijwilligheid in het geven van toestemming (zonder vrijwilligheid is er onder de AVG geen juridisch tot stand gekomen toestemming) is iets wat al vaker bediscussieerd is in het licht van hiërarchische relaties. Zo is het al tijden usance, en later ook in richtlijnen van de toezichthouders vastgelegd, dat het vragen om toestemming aan werknemers door de werkgever geen valide optie is om persoonsgegevens te verwerken. Er kan namelijk geen sprake zijn van vrijwillig gegeven toestemming omdat de werknemer mogelijk vreest voor nadelige behandeling als "nee" gezegd wordt. In de voorbeelden van gebruikte volg-apps kwam bij Singapore naar voren dat de overheid een sturende hand heeft in het stimuleren van het gebruik ervan. Nu kan een scepticus zeggen dat dit sturend optreden wellicht gebruikelijker is in Aziatische landen, maar hoe denkbeeldig is het nu echt dat onze eigen overheid ons zou vragen om medewerking door onze (medische) gegevens te delen om het coronagevaar te bestrijden? En, indien dit het geval is, hoeveel blijft er dan nog van de vrijwilligheid in het delen over? Sociale druk, maar zeker ook druk uitgeoefend door overheidsinstellingen, kan ertoe leiden dat weigeraars niet getolereerd worden. Zie bijvoorbeeld ook hoe maatschappij en opsporingsinstanties reageren op personen die weigeren mee te werken aan grootschalige DNA-onderzoeken (15).

Wat vindt de AP?

De Autoriteit Persoonsgegevens heeft al vrij snel in de coronacrisis aangegeven dat ze verantwoordelijken meer ruimte geeft om vragen en verzoeken van de toezichthouder te beantwoorden. Privacy moet goede zorg niet in de weg staan, zo stelt het AP, en daarom zal zij ook niet ferm optreden in die gevallen dat bijvoorbeeld oud-zorgmedewerkers benaderd worden om bij te staan in de zorg. Ze geeft voorts aan wel alert te blijven op gevallen waar de grenzen overschreden worden. "De AP is er als hoeder van het grondrecht op privacy en zal ook in deze tijden ingrijpen wanneer de privacy echt in gevaar is. Daar heeft de burger recht op. Zodat iedereen straks als vrij burger in een vrij land weer vrij kan leven" (16). De lezing van vooral het laatste gedeelte van het citaat, geeft al aan dat ook onze toezichthouder beseft dat in vrijheid leven momenteel eigenlijk al niet meer mogelijk is. De AP wijst nog op de Telecommunicatiewet waarin staat dat locatiegegevens alleen gedeeld kunnen worden indien deze geanonimi-

seerd zijn of daarvoor nadrukkelijke toestemming van de betrokkene is verkregen. Beide opties lijken de toezichthouder in de huidige scenario's praktisch niet haalbaar voor zover het gaat over landelijke voorzieningen voor het volgen van burgers. Over het gebruik van locatiegegevens zegt de AP dat dit alleen kan als daarvoor een wettelijke voorziening bestaat. De toezichthouder stelt dat een en ander gerealiseerd kan worden met een spoedwet waarbij democratische controle van het parlement essentieel is (17).

Kritisch en alert

Het staat absoluut niet ter discussie dat in tijden van crisis soms ingrijpende maatregelen moeten worden genomen die een tijdelijke beperking van de rechten en vrijheden van burgers inhouden. Maar juist in tijden dat vitale belangen op het spel staan, moeten we alert blijven dat rechten en vrijheden niet met voeten getreden worden. We moeten ervoor waken dat de discussie niet ontaard in de valse tegenstelling 'onze gezondheid in ruil voor privacy'. Misschien nog wel het meest pregnante probleem waar we als maatschappij en burgers straks voor komen te staan is het fenomeen van Pandora's doos. De doos, zoals hierboven aangegeven, is opengezet en het is nog maar de vraag of het ons gaat lukken alles weer terug te krijgen naar een status quo zoals we die kenden voor de coronacrisis. Vooral het uitbreiden van bevoegdheden brengt het gevaar met zich dat deze naderhand ofwel in stand blijven ofwel in andere situaties ingezet gaan worden omdat zij toch immers zo effectief bleken te zijn. Vergelijk bijvoorbeeld ook eens de discussies over het inzetten van ANPR (Automated Number Plate Recognition) waarbij in de loop van de jaren de doeleinden steeds verder uitgebreid zijn en de effectiviteit niet altijd aanwijsbaar is, laat staan dat vragen over proportionaliteit en subsidiariteit afdoende aan de orde komen. Een ander voorbeeld is het massaal inzetten van camerasurveillance in stedelijke gebieden waarbij binnen Europa de UK een grote voorloper is en inmiddels zelfs in Londen realtime gezichtsherkenning toegevoegd gaat worden. Ook daar is het hellende vlak toegenomen, elk klein stapje voorwaarts in de erosie van privacy brengt het vertrekpunt van privacy als onschendbaar recht verder weg. Om te voorkomen dat we straks in een onomkeerbare situatie terechtkomen, moeten we juist nu al zeer kritisch zijn en de discussie over het behoud van privacy in crisistijd hardop voeren.

Naschrift: Kort na het schrijven van dit artikel kondigde de Nederlandse overheid aan dat ze apps gaat inzetten om met corona besmette personen te gaan volgen. Daarbij gaf ze tevens aan dat het gebruik van dergelijke apps mogelijk zelfs verplicht gesteld gaat worden.

Referenties

(1) https://www.pepp-pt.org/

(2) Reuters, Putin takes coronavirus precautions as Moscow unveils tracking app, 1 april 2020, https://www.reuters.com/article/us-health-coronavirus-russia/moscow-unveils-coronavirus-tracking-app-as-national-lockdown-widens-idUSKBN21J4W8

(3) https://covidsafepaths.org/

(4) NRC, Ook Nederland wil Telecomdata inzetten tegen verspreiding Coronavirus, 27 maart 2020, https://www.nrc.nl/nieuws/2020/03/27/ook-nederland-wil-telecomdata-inzetten-tegen-verspreiding-coronavirus-a3995128

(5) Google, Helping public health officials combat COVID-19, 3 april 2020, https://www.blog.google/technology/health/covid-19-community-mobility-reports

(6) de Volkskrant, Nederlandse app-makers klaar voor corona-app, 27 maart 2020, https://www.volkskrant.nl/nieuws-achtergrond/nederlandse-app-makers-klaar-voor-corona-app~bb2019b4/

(7) Philips, Philips biedt ziekenhuizen en huisartsen de mogelijkheid patiënten op afstand te screenen en te volgen tijdens de uitbraak van COVID-19, 21 maart 2020, https://www.philips.nl/a-w/about/news/archive/standard/about/news/press/2020/20200321-philips-biedt-ziekenhuizen-en-huisartsen-de-mogelijkheid-patienten-op-afstand-te-screenen-en-te-volgen-tijdens-de-uitbraak-van-covid-19.html en https://www.philips.nl/healthcare/sites/vitalhealth/products/questlink

(8) De Telegraaf, Purmerend en Beemster openen 'corona-kliklijn', 26 maart 2020, https://www.telegraaf.nl/nieuws/1145740436/purmerend-en-beemster-openen-corona-kliklijn

(9) https://www.nhnieuws.nl/nieuws/264542/drones-gaan-dit-weekend-controleren-of-mensen-wel-voldoende-afstand-houden

(10) NH Nieuws, Drones gaan dit weekend controleren of mensen wel voldoende afstand houden, 27 maart 2020, https://www.nieuwsblad.be/cnt/dmf20200328_04905506

(11) Omroep Zeeland, Boa's controleren of toeristen weg zijn, 30 maart 2020, https://www.omroepzeeland.nl/nieuws/119039/Boa-s-controleren-of-toeristen-weg-zijn

(12) Zorgvisie, Nieuwe database biedt inzicht in Covid-19 bij verstandelijk beperkten, 3 april 2020, https://www.zorgvisie.nl/nieuwe-database-biedt-inzicht-in-covid-19-bij-verstandelijk-gehandicapten/

(13) NYT, One Nation Tracked, 19 december 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

(14) Columbia University, Location Data on Two Apps Enough to Identify Someone, Says Study, 13 april 2016, https://datascience.columbia.edu/location-data-two-apps-enough-identify-someone-says-study

(15) Joop, Bedenkingen bij het grootschalige DNA-onderzoek in de zaak Nicky Verstappen, 27 oktober 2017, https://joop.bnnvara.nl/opinies/bedenkingen-bij-het-grootschalige-dna-onderzoek-in-de-zaak-nicky-verstappen

(16) Autoriteit Persoonsgegevens, AP geeft organisaties meer tijd vanwege coronacrisis, 20 maart 2020, https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-organisaties-meer-tijd-vanwege-coronacrisis

(17) Autoriteit Persoonsgegevens, Gebruik telecomdata tegen corona kan alléén met wet, 1 april 2020, https://autoriteitpersoonsgegeven

COLUMN PRIVACY

Mr. Rachel Marbus
@RACHELMARBUS OP TWITTER

De ultieme privacy-oefening

Thuiszitten. Op het moment van schrijven doe ik dat al zes en een halve week. Ietsje meer dan de gemiddelde Nederlander omdat ik al eerder een klein virusje had en ik een week of drie voorsprong heb op corona. En hoewel in week vier de muren echt ontzettend op me afkwamen, vind ik thuis kunnen zitten nog steeds een voorrecht. Het is namelijk de ultieme oefening in privacy met een vleugje voyeurisme.

Ik woon in een klein appartement in een statige wijk in Den Haag, niet zo heel ver van de zee. Op de derde verdieping van een herenhuis bevindt zich mijn domein. Ik heb een woonkamer annex keuken, een slaapkamer, een slaapkamer voor mijn dochter (die dezer dagen ook vaak bij haar vader is) en een ieniemienie rommelkamertje. Met de nadruk op rommel. Er is zelfs een balkon waarop nog niet zoveel zon staat omdat we wat vroeg in het zonseizoen zijn, maar frisse lucht is mooi meegenomen.

Ik doe momenteel verplicht aan privacy. Misschien iets meer dan de meesten van ons omdat ik risicopatiënt ben, maar ik hoop tegelijk dat velen met mij deze oefening ter harte nemen. Ik zie niemand buiten mijn dochter, zelfs niet op anderhalve meter afstand omdat het risico mij groter is dan het eventuele kortstondige welbevinden. En natuurlijk wringt dat, want de mens is een sociaal dier en ik hou ervan om te knuffelen. Maar nu even niet. Als ik buiten kom om eten te kopen, dan doe ik dat incognito met mondkap en wegwerphandschoenen. Omdat mijn bril beslaat met mondkap op, laat ik die thuis. De mensen die ik tegenkom lopen met een grote boog om me heen. Niemand die me herkent; ik voel me waarlijk anoniem in mijn toch altijd zo gezellige en sociale buurt.

Bij thuiskomst in mijn appartement kijk ik vanachter het glas naar mijn buren. Ze hebben ineens een gezicht gekregen. Ik zie gezinnen bewegen in hun dagelijks ritueel. De zo Hollandse gordijnen wagenwijd open, mij een blik gunnend in de kleine huiselijke biotoop. Mijn overbuurvrouw is weer begonnen met roken. Ik had gehoopt dat het haar zou lukken om daar vanaf te blijven. Ze heeft onlangs een kleintje op de wereld gezet en ik had haar al lang niet meer op het balkon zien paffen. Ook heb ik ineens een buurman die niet alleen maar om zes uur in de ochtend aanwezig is, maar die nu zelfs voor het raam een heus geïmproviseerd kantoor gemaakt heeft. Hij maakt er ‘s ochtends vaak een foto van en gaat dan weer in bed liggen.

Ik heb er ook aan moeten wennen hoor, aan al dat gluren naar mijn buren. Ergens na mijn derde week thuis, bleef ineens heel Nederland ook achter de eigen voordeur. Daar had ik even geen rekening mee gehouden toen ik in mijn adamskostuum mijn bed uitkroop en naar de woonkamer annex keuken liep om wat thee te zetten. Zaten ineens al mijn buren op het balkon. De zon was net even gaan schijnen.

Rachel

Auteur: Tamara Brandt, onafhankelijk informatiebeveiliging en privacy adviseur bij haar eigen bedrijf Privara. Tamara Brandt is bereikbaar via tamara@privara.eu

Maken en delen van foto's onder privacywetgeving is complex

Het verwerken van persoonsgegevens begint met het beantwoorden van de vragen: mag het? En: kan het? En als het mag en kan, wil ik het dan? In meer technische termen, voldoet de verwerking aan de grondbeginselen inzake gegevensverwerking? Daarvoor ga je onder meer op zoek naar een juridische verwerkingsgrondslag. Je kunt je in een situatie bevinden waarin de verwerking mag en kan, maar je het ethische vraagstuk niet zo eenvoudig opgelost krijgt.

Privacywetgeving geeft richting en geeft personen handvaten om eigenaarschap te nemen

De AVG geeft ons zes juridische grondslagen ter verwerking van persoonsgegevens (artikel 6, lid 1, AVG). Een veelbesproken grondslag is de verwerking op basis van toestemming. Met enige regelmaat wordt er via scholen, sportverenigingen en zelfs kinderfeestjes met een formulier gevraagd om toestemming voor het nemen van foto's. An sich geen verkeerde reflex, het lijkt hiermee inmiddels tot het grotere publiek doorgedrongen dat foto's een persoonsgegeven (kunnen) zijn. Je zult dus na moeten denken over de vraag of deze verwerkt kunnen worden en onder welke voorwaarden.

Misvatting

De misvatting is dat dit onder toestemming moet en enkel en alleen onder toestemming kan. Er zijn gevallen waarin dit tot in het extreme wordt doorgetrokken. Zo is er een geval bekend van een ouder wiens dreumes enkele dagen in de week naar het kinderdagverblijf gaat. De kleine spruit was jarig en mocht dit heuglijke feit met vriendjes en vriendinnetjes op het kinderdagverblijf vieren. De gebruikelijke festiviteiten zoals het zingen, trakteren en felicitaties werden op het eind onderbroken. De ouder werd uitgenodigd een foto te maken voor het plakboek, maar pas nadat alle kinderen zich hadden omgedraaid en alleen de eigen jarige job met het gezichtje naar de camera gedraaid stond. "Dit moest van de AVG", was het antwoord van de leidster op het verbijsterde gezicht van de ouder. Andere situaties bevatten voorbeelden met mensen die een rode stip op het voorhoofd krijgen zodat ze later bij de fotobewerking onherkenbaar gemaakt kunnen worden. Kinderen op de basisschool waarbij de hele klas onherkenbaar gemaakt wordt op de klassenfoto, behalve het kind waar de foto voor bestemd is. Gele hesjes betekenen dat jouw ouders wel toestemming hebben gegeven dat je op de foto mag tijdens het schoolreisje, oranje hesjes betekenen dat jouw ouders geen toestemming hebben gegeven dat je op de foto mag tijdens het schoolreisje. Zal de huidige generatie kinderen, geboren in het tijdperk dat privacy een steeds prominenter rol speelt in de samenleving, later leiden aan het 'AVG-complex'? Iedereen mag op de foto, behalve ik. Sterker nog, ik krijg een uiterlijk kenmerk toebedeeld op basis waarvan ik word uitgesloten om te worden gefotografeerd.

Privacywetgeving geeft richting

Eng? Ja, best wel. Het paradoxale hieraan is dat de AVG er juist gekomen is om de fundamentele vrijheid die men heeft ten aanzien van privacy te ondersteunen, handel en vrij verkeer in data mogelijk te maken. Mogelijk, mits voldaan aan de juiste voorwaarden. Je kunt altijd besluiten alsnog van de verwerking af te zien, hoewel het wellicht puur juridisch waterdicht is. Privacywetgeving geeft richting en geeft personen handvaten om eigenaarschap te nemen over het verwerken van persoonsgegevens. Hierdoor ben je beter in staat keuzes te maken en jezelf te beschermen in de toenemend digitale wereld waarin we leven. Velen hebben niets te verbergen, maar iedereen heeft iets te beschermen. Het maken en delen van foto's onder privacywetgeving is complex.

Huishoudelijk gebruik

Specifiek onder de AVG is een uitzondering voor de verwerking van persoonsgegevens mogelijk puur voor persoonlijke en huishoudelijke activiteit (artikel 2, lid 2, sub c, AVG). De ouder die een foto van haar verjaardag vierende kind met zijn of haar vriendjes en vriendinnetjes maakt voor in het plakboek mag dit gewoon doen, zonder toestemming in de zin van de AVG. De zaak verandert wanneer deze foto gebruikt wordt door het kinderdagverblijf op de eigen website ter promotie van haar activiteiten. Ook delen via social media is niet zonder meer toegestaan. Dan is er geen sprake meer van puur persoonlijk en huishoudelijk gebruik. Laten we niet te ver doorslaan en onze kinderen behoeden voor het zogenaamde 'AVG-complex'. Zoek bij twijfel advies en start elke verwerking met de vragen gesteld aan het begin van dit artikel. Kan het, mag het en is het ethisch en juridisch verantwoord, maak dan leuke herinneringen voor later in de vorm van fotomateriaal.

Auteur: Nico Mookhoek is privacy jurist en schrijver van het boek 'Lean privacy, efficiënt werken met de AVG'. Nico is bereikbaar via info@deprivacyguru.nl

Hoe creëer je bewustwording bij medewerkers?

Overheden en bedrijven spenderen kapitalen aan informatiebeveiliging en treffen legio technische maatregelen. Om te voldoen aan de AVG worden documenten en procedures opgesteld. De menselijke factor waarmee de uitvoering staat of valt, wordt daarbij helaas vaak over het hoofd gezien. In dit artikel geef ik tips hoe je mensen meer bewust maakt op dit gebied.

Bij ongelukken lezen we vaak dat de oorzaak is ontstaan door een menselijke fout. Bij informatiebeveiliging is dit niet anders. Het merendeel van de incidenten wordt veroorzaakt door menselijk handelen. In een organisatie kan de technische beveiliging nog zo goed op orde zijn, als een (ingehuurde) monteur een onbeveiligde laptop bij een klant achterlaat (KPN) is dat hele beleid in een klap waardeloos. Als de medewerker een boodschappenlijstje maakt op de achterkant van een dienstoverdracht en deze na de boodschappen achterlaat in een winkelwagentje (zoals gebeurde bij een medewerker van het Haga ziekenhuis), zijn al de technische maatregelen nutteloos.

Een goed informatiebeveiligings- en privacybeleid (IBP-beleid) is een noodzakelijke voorwaarde. De technische maatregelen zijn voldoende voorwaarden maar de effectiviteit in de praktijk staat of valt met de mensen. Met mensen die zich bewust zijn dat ze gegevens verwerken die privacygevoelig (kunnen) zijn en die zich bewust zijn van de risico's die zij en hun organisatie met betrekking tot deze gegevens lopen.

Aandachtspunten bij de ontwikkeling

1. **Bedenk wat het startpunt is**
   Hoe volwassen is de organisatie op het gebied van privacy en informatiebeveiliging? Is er een cultuur waarin medewerkers zich bewust zijn van IBP-risico's of is de cul-

tuur meer gebaseerd op vertrouwen? We kennen elkaar toch, dus het is gewoon handig dat we de wachtwoorden voor onze e-mail met elkaar delen. Stem de acties af op de mate van volwassenheid van de organisatie. Een organisatie met een hoog bewustzijn vraagt om andere acties dan eentje waar IBP nog in de kinderschoenen staat.

Let bij grotere organisaties ook op of het privacybewustzijn overal hetzelfde is. Vaak is het management, in AVG-termen: de verwerkersverantwoordelijke, doordrongen van de noodzaak, maar dat betekent nog niet dat het onderwerp op de werkvloer leeft.

2. **Geen eenmalige actie maar een programma**

   Herhaal de boodschap in verschillende vormen op verschillende tijdstippen. Maak daarom op basis van de inventarisatie een programma. Wanneer plannen we een actie en in welke vorm? Met een programma kan voorkomen worden dat acties er in de hectiek van alle dag bij inschieten.

   Pas een mix van communicatiekanalen toe. Gebruik zowel bestaande als nieuwe communicatiekanalen. Benut de nieuwsbrief voor het personeel om IBP onder de aandacht te brengen. Vraag een podium tijdens een personeelsbijeenkomst en vertel over de nieuwe ontwikkelingen. Wissel mondelinge en schriftelijke communicatie af. Sommige mensen lezen liever iets, anderen zijn meer auditief ingesteld. Om de boodschap zo breed mogelijk gedragen te krijgen, moeten beide groepen aangesproken worden. Maak bijvoorbeeld een poster met privacytips en hang die op strategische plekken (koffieapparaat, kopieerapparaat).

   Betrek ook het online element in je programma. Er zijn verschillende e-learning applicaties om medewerkers aan te bieden. Sommige koppelen daar ook nog een toets met een certificaat aan. Zet de medewerkers die het certificaat hebben behaald in het zonnetje tijdens een personeelsborrel.

3. **Houd rekening met de vier fasen bij het eigen maken van nieuwe kennis en vaardigheden**

   Abraham Maslow, een Amerikaanse psycholoog, heeft vier leerfasen onderscheiden. Hoewel hij dit inzicht al in 1954 ontwikkelde, is het nog steeds actueel.

   Fase 1 onbewust onbekwaam: men is zich niet bewust dat men iets niet weet of beheerst.

   Fase 2 bewust onbekwaam: men weet dat men iets mist, dat men iets bij moet leren.

   Fase 3 bewust bekwaam: men gaat bewust aan de slag met het eigen maken van nieuwe kennis en/of nieuwe vaardigheden.

   Fase 4: onbewust bekwaam: men denkt niet meer over de nieuwe kennis of vaardigheden na maar past die automatisch toe.

   Iedere fase vraagt om een andere manier van begeleiden of aansturen. Achterhaal in welke fase een medewerker is, dan kan op het goede niveau ingestoken worden. En begeleid de medewerker naar zijn/haar volgende stap in zijn/haar leren.

Bewustwording is een gemeenschappelijke verantwoordelijkheid

Het maken van IBP bewuste medewerkers is niet alleen een taak van de Information Security Officer (ISO) of de Data Protection Officer (DPO). Het dient een gemeenschappelijke inspanning te zijn, ook voor het management. Zij hebben een belangrijke voorbeeldfunctie: door het naleven van de regels onderschrijven zij impliciet het belang van de regels. Richt het programma ook op de hele organisatie. Betrek ook medewerkers van HRM en de facilitaire afdeling. Bedenk daarbij dat zij andere vragen en issues hebben dan er op de werkvloer leven. Zorg er voor dat je als Information Security Officer of Data Protection Officer in de organisatie zichtbaar bent. Ga dus de organisatie in. Houd interviews met medewerkers over IBP gerelateerde onderwerpen, ze verschaffen waardevolle inzichten. Als dat nog niet de gewoonte is: schuif aan bij het managementoverleg. Praat het management regelmatig bij, ook dat houdt hen betrokken.

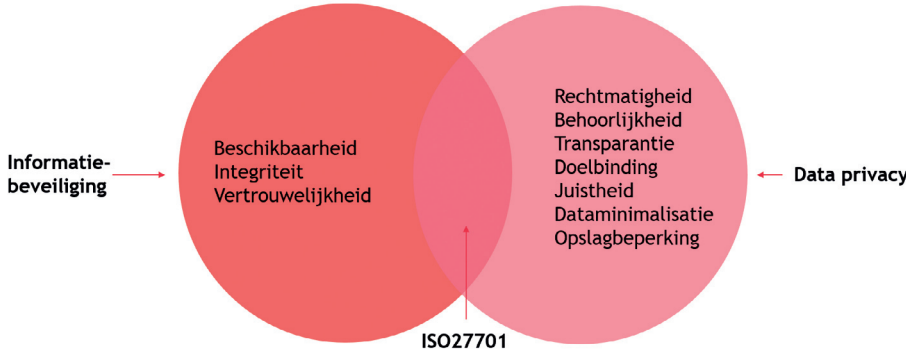
Documenteer en veranker

De AVG gaat, geheel in de geest van de tijd, vooral om transparantie en aantoonbaarheid. Maak de inspanningen dan ook aantoonbaar. Schrijf een verslag van de verplichte analyse van het register: 'datalekken'. Hetzelfde geldt voor bevindingen bij de privacy-audits: maak een advies met voorgestelde maatregelen. Laat bij trainingen en andere bijeenkomsten een presentielijst tekenen. Wanneer de medewerkers bewust bekwaam zijn geworden op het gebied van IBP, blijf dan nog steeds een aantal instrumenten uit het bewustwordingsprogramma gebruiken. Zoals een jaarlijkse IBP-training voor alle nieuwe medewerkers. Blijf via de personeelsbijeenkomst en het personeelsblad de nieuwe ontwikkelingen delen. Behoud draagvlak bij het management: IBP moet een vast agendapunt zijn tijdens het managementoverleg. En net zoals de technische maatregelen steeds geüpdatet moeten worden, vraagt ook bewustwording bij de medewerkers continu aandacht. Het zijn immers de mensen die het (moeten) doen.

Mr. Ruben Tienhooven is expertiseleider privacy binnen BDO Advisory. Ruben is hoofdauteur van de richtlijn 'Best practice voor Privacy in Ketens' van het CIP (Centrum Informatiebeveiliging en Privacybescherming). Ruben is te bereiken via ruben.tienhooven@bdo.nl

ISO 27701: van privacy compliance naar privacy assurance?

Informatiebeveiliging is al lang niet meer weg te denken uit de moderne bedrijfsvoering. Maar de bescherming van privacy komt met de Algemene Verordening Gegevensbescherming (AVG) eigenlijk pas net om de hoek kijken. De vraag naar handvatten om privacy te kunnen beschermen, is de laatste tijd flink toegenomen. Daarvoor is er nu de ISO 27701: de standaard waarmee privacybescherming onderdeel wordt van het Information Security Management System (ISMS). Inclusief het achterliggende Plan-Do-Check-Act (PDCA)-cyclus.



Afbeelding 1 - De verschillen en samenhang tussen informatiebeveiliging en privacybescherming.

Dat de twee vakgebieden overlappen, was al bekend maar de informatiebeveiligings- en privacydeskundigen wisten dit in de praktijk onvoldoende tot uiting te brengen in een geïntegreerde aanpak. Het beschermen van persoonsgegevens gaat, anders dan weleens gedacht, verder dan alleen het inrichten van technische en organisatorische beveiligingsmaatregelen. In de AVG staat in artikel 32 opgenomen dat er een 'passende beveiliging' moet zijn, en ISO 27001 en -2 kennen alleen een paar verwijzingen en algemeenheden over voldoen aan (privacy)wet- en regelgeving. Maar toen was er de ISO 27701, die juist is bedoeld om de verbanden tussen de AVG- en ISO-wereld te leggen.

Structuur: clausules invoegen

Anders dan de AVG, kent de ISO 27701 bijvoorbeeld wel een PDCA-cyclus waarmee privacy in het ISMS wordt geïntegreerd. Op die manier wordt deels invulling gegeven aan het juridische begrip 'passend', zoals in artikel 32 van de

AVG. Werken via een PDCA-cyclus dwingt een organisatie er namelijk toe om continu verbeteringen door te voeren – en daarmee beter aan te sluiten bij – wat de AVG 'de stand van de techniek' noemt. En uiteraard is er ook aandacht besteed aan specifieke onderwerpen als de verplichtingen voor de Verwerkingsverantwoordelijke, de Verwerker en de Functionaris voor de Gegevensbescherming (FG).

Allereerst wordt met twee algemene clausules de indruk gewekt dat slechts een tekstuele wijziging nodig is in het huidige ISMS. Overal waar informatiebeveiliging staat, moet nu ook iets over privacy komen te staan. Echter, er zijn nog 32 specifieke aanvullingen met meer inhoud, gebaseerd op zowel de AVG alsook de ISO 27001 en -2, als de ISO 27002. In onderstaand voorbeeld een willekeurige greep:

Bij ISO 27001 clausule 4.2 geeft ISO 27701 clausule 5.2:

- The organization shall determine its role as a PII controller (including as a joint PII controller) and/or a PII processor (…)
- The organization shall determine external and internal factors that are relevant to its context and that affect its ability to achieve the intended outcome(s) of its PIMS. For example, these can include: legislation, regulations, decisions, organizational context, governance, policies and procedures, applicable administrative decisions, contractual requirements.
- Where the organization acts in both roles (PII controller and a PII processor), separate roles shall be determined, each of which is the subject of a separate set of controls.

Bij ISO 27002 clausule 6.1.1 geeft ISO 27701 clausule 6.3.1.1:

- The organization should designate a point of contact for use by the customer regarding the processing of PII. When the organization is a PII controller, designate a point of contact for PII principles regarding the processing of their PII. (…)

The responsible person should, where appropriate:

- be independent and report directly to the appropriate management level of the organization in order to ensure effective management of privacy risks;
- be involved in the management of all issues which relate to the processing of PII;
- be expert in data protection legislation, regulation and practice;
- act as a contact point for supervisory authorities;
- inform top-level management and employees of the organization of their obligations with respect to the processing of PII;
- provide advice in respect of privacy impact assessments conducted by the organization.

Wet op Behoud van Ellende

Dit soort verbijzonderingen klinken voor sommigen misschien eenvoudig te implementeren, veel organisaties zullen nog wat stappen moeten zetten om privacy op deze wijze te borgen - laat staan de organisaties met vestigingen buiten Europa. Dit confronteert sommige organisaties ook wellicht met een tekort. Voor certificering of alleen maar een conformiteitsverklaring afgezet tegen de ISO 27001 is er in wezen redelijk wat ruimte om de invulling à la Annex A of de ISO 27002, naar eigen believen vorm te geven. Voor de ISO 27701 is de ruimte dus flink minder. Dat is misschien lastig, maar aan de andere kant misschien ook wel een voordeel. Bij veel privacy-compliance implementaties komt regelmatig de vraag naar voren of men wel zo 'ver' moet gaan met detailinvullingen. Het is lastig om vast te stellen wat 'minimaal' nodig is of waar een interne of externe toezichthouder tevreden mee is. In het geval van ISO 27701-implementatie komt men door de clausules te adopteren in huidige beleidsstukken, procedures en werkinstructies, vanzelf een stap verder. Natuurlijk geldt dan wel de Wet op Behoud van Ellende: er is minder denkwerk en overleg nodig, maar meer doe-werk.

Certificering

Als het bovenstaande aan implementatie allemaal is gebeurd, dan kan tegen de ISO 27701 worden gecertificeerd. Betekent conformiteit met deze standaard dan ook gelijk dat er sprake is van AVG-compliance of zelfs certificering? Helaas, daar is toch nog wat meer voor nodig (zie afbeelding 1). Momenteel zijn er wel initiatieven om certificeerbaarheid mogelijk te maken, maar het zal nog een tijd duren voor we daar zijn. De laatste stand van zaken is dat, zoals de AVG dit mogelijk maakt, de certificering per proces plaats zou moeten vinden. Overigens zal deze certificering vooral voor verwerkers interessant zijn, omdat zij tegenover (potentiële) klanten met zekerheid kunnen aantonen AVG-conform te werken.

ISO 27701 is niet niks

Hoe dan ook, het is wel duidelijk dat zowel Verwerkingsverantwoordelijken als Verwerkers een grote stap op weg zijn naar AVG-compliance met de implementatie van de ISO 27701. Hiermee wordt een zekere privacyvolwassenheid duidelijk voor burgers, zakelijke partners en - niet geheel onbelangrijk - de Autoriteit Persoonsgegevens. Door reeds met de ISO 27701-implementatie te starten, kan een voorsprong worden behaald op de concurrentie. Ook wordt voorkomen dat er later in alle haast inhaalslagen gemaakt moeten worden. Kortom: de ISO 27701 is niet moeilijk, niet heel nieuw, maar zeker niet niks.

DE WERELD STAAT BIJNA STIL... OF TOCH NIET?

Hoe snel en gek kan het lopen. In januari schreef Evert dat de digitale samenleving continue en in een rap tempo verandert. Maar dat we in paar maanden tijd in een intelligente lock-down zouden 'zitten' is natuurlijk onwerkelijk. Toch is het zo en hebben we ermee te dealen. Juist binnen onze beroepsgroep weten wij hoe we moeten omgaan met (bedrijfs)risico's alsmede de black swans die ons overkomen.

Vanmorgen belde Jessica mij of ik 'haar' artikel voor dit nummer kon overnemen, omdat ze letterlijk de handen vol had aan een ransomware-aanval bij Cognizant. Natuurlijk doe ik dat, niet zoveel is veranderd ... ahum.

Begin maart zijn er signalen vanuit vooral Italië die hebben geleid tot het annuleren van ons Awareness-event van 10 maart. Deze proactieve actie was ingegeven dat dit nog kosteloos kon. Kijk, dat vind ik als penningmeester natuurlijk erg mooi om te horen. Toch was er toen nog verbazing over het vroegtijdig afblazen van ons event ... en nu dan? Intussen ontkwamen we ook in Nederland niet aan maatregelen die ons allen raken. In eerste instantie privé, je gezin, je ouders, familie en vrienden. Allerlei gevoelens spelen nu mee en dan moet je net doen alsof je met alle risico's goed kunt omgaan. Tja, dat is ons werk toch?

De activiteitencommissie - in afstemming met bestuur - heeft de alternatieven bekeken. En ja, ook wij waren al geruime tijd bezig om een webinar-achtig format uit te proberen. Nou dat ging ineens snel. Het CISO-33 event van 1 april werd de try-out van onze webinar-opzet, waarbij we gebruik maakten van een opnamestudio bij ons verenigingsbureau MOS met de software van SkillsTown die in februari van dit jaar van start is gegaan.

Dit was letterlijk een live try-out met een mooi resultaat, hoewel niet alles helemaal liep zoals het hoort. De leerpunten werden meegenomen voor het volgende event: onze activiteit van 16 april werd ook omgezet naar een webinar: 'Oeps, gehackt door het Red Team ...', nu ook in een PvIB-look and feel. Ik was zelf ook kijker/chatter en ik was bijzonder trots dat wij met bijna 220 webinar-deelnemers een leuk en interessant event hebben kunnen organiseren.

Wat gaat de toekomst ons brengen? Op dit moment is duidelijk dat het organiseren van grote events on-site nog wel even duurt. Kortom wij gaan door met de ingeslagen weg van webinars. Dit biedt in ieder geval een prachtige aanvulling juist ook voor de toekomst van onze vereniging om met elkaar in verbinding te komen en te blijven.

Wat ik vooral zie, is dat - naast de echte concrete problemen waar wij persoonlijk mee worden geconfronteerd - de samenleving zich als geheel opnieuw moet uitvinden: in een vorm van een intelligente en open-up maatschappij. Dan wel in de nieuwe anderhalvemetermaatschappij of hoe we het verder ook gaan noemen. Dit wordt volgens mij ons nieuwe normaal voor ons leven en hoe we met elkaar omgaan. Dat leidt tot verrassende (mooie) initiatieven, tot iets voor elkaar krijgen dat een paar maanden geleden nog ondenkbaar was. Kortom, wij als leden moeten elkaar kunnen vinden en helpen waar dat nodig is. Laat je dan ook horen met je ideeën en je vragen. Mail naar penningmeester@pvib.nl

Met elkaar zijn we sterker!

Henk de Ruiter

Auteur: drs. Ruud Buurma is als adviseur informatiebeveiliging en AVG werkzaam voor HODARI B.V.

AVG in relatie tot informatiebeveiliging

In mei 2018 ging in de gehele Europese Economische Ruimte (EER) de General Data Protection Regulation 2016/679 (GDPR) van kracht. In Nederland vertaald naar de Algemene Verordening Gegevensbescherming (AVG). Wat hebben organisaties in de afgelopen twee jaar geleerd? Een antwoord hierop halen we uit het nieuws. Naast een relatie die direct is te leggen met de AVG, is er ook een relatie met de beveiliging van informatie in het algemeen en persoonsgegevens in het bijzonder.

Een greep uit het nieuws:

juni 2018: uitspraak van Autoriteit Persoonsgegevens rondom gebruik van BSN- en BTW- nummers van zelfstandigen.
juni 2019: gemeente Deventer moet € 500 schadevergoeding betalen aan een man die een aantal WOB-verzoeken had ingediend.
juli 2019: eerste boete van € 460.000 opgelegd op grond van de AVG aan het Haga Ziekenhuis vanwege de onzorgvuldige omgang met patiëntgegevens.
januari 2020: flinke stijging online-fraude.
februari 2020: Universiteit Maastricht betaalt € 197.000 nadat ze het slachtoffer waren geworden van ransomware.
februari 2020: gegevens van 80.000 passagiers Transavia gestolen.
maart 2020: tennisbond KNLTB krijgt een boete van € 525.000 voor het verstrekken van gegevens van leden aan twee sponsoren.
maart 2020: privacy van bestuurders van (veelal elektrische zelfrijdende) auto's niet goed geregeld.

Zit de Autoriteit Persoonsgegevens stil?

Wat opvalt is dat het nieuws ten aanzien van de AVG, als het gaat om boetes, nog te overzien is. Het aantal boetes is tot nu toe nog letterlijk op een hand te tellen. Dat wil niet zeggen dat de Autoriteit Persoonsgegevens (AP) stilzit.

- Zelf geeft de AP in haar 'Toetsingskader 2018-2019' aan dat zij in die jaren 'guidance' willen bieden aan de invoering, en de bekendheid met de AVG willen vergroten. Een groot deel van 2018 en 2019 is dan ook gebruikt om organisaties en particulieren te informeren over hun rechten en plichten.
- Daarnaast heeft de AP een onderzoek gedaan bij dertig organisaties, groot en klein en uit diverse sectoren, naar de naleving van de AVG bij die organisaties. Dit onderzoek was voornamelijk gericht op verwerkersovereenkomsten en verwerkingsregisters. De uitkomsten van die onderzoeken zijn overigens niet publiekelijk bekend gemaakt.
- Ook onderzocht de AP of overheidsorganisaties, ziekenhuizen, verzekeraars en banken een functionaris voor de gegevensbescherming hebben. Tevens is de Autoriteit Persoonsgegevens in een groot deel van 2019 bezig geweest de eigen organisatie op sterkte te krijgen. Deze was nog niet voorbereid op het grote aantal meldingen die zij hebben ontvangen: 27.000 in 2019 tegenover ruim 8.000 in 2018.
- Uit 'Focus Autoriteit Persoonsgegevens 2020-2023', de opvolger van het 'Toetsingskader 2018-2019', blijkt dat de nadruk onder meer zal komen te liggen op illegale datahandel en gebrekkige beveiliging.

Wat eveneens opvalt is dat het nieuws in toenemende mate wordt gevuld met aspecten van cybercrime. Het gaat daarbij om zaken als hacking, identiteitsfraude, phishing, pinpasfraude en ransomware, Niet alleen particulieren worden hier in toenemende mate het slachtoffer van, maar ook organisaties.

De dagelijkse praktijk

Wat is de ervaring van HODARI in de praktijk? Wij zien een opvallende inzet op informatiebeveiliging sinds de invoering van de AVG. Door de toenemende rol van privacy staat voor veel grote organisaties het inzetten op informatiebeveiliging nu nog hoger op de agenda ter voorkoming van schade aan de financiële positie, de reputatie en het imago.
Voor kleinere organisaties gold vaak dat informatiebeveiliging veelal tot een minimum werd beperkt om op die wijze de hoogste risico's (zoals bijvoorbeeld uitval van systemen en verlies van data) te vermijden. Blijkbaar kwam dit doordat de bewustwording voor eventuele andere gevolgen er nog niet was. Met de invoering van de 'melding datalekken', als onderdeel van de Wet bescherming persoonsgegevens, werd een eerste kentering zichtbaar. Geleidelijk groeide het besef dat er meer moest worden gedaan om de IT-omgeving te beveiligen en zo de rechten ten aanzien van de privacy van natuurlijke personen te waarborgen.

Invloed van de AVG op informatiebeveiliging

Waarom is de AVG een belangrijke aanjager geworden voor het optimaliseren van informatiebeveiliging?

Naast de AVG is er ook vanuit andere invalshoeken aandacht voor informatiebeveiliging

Het antwoord op die vraag ligt besloten in de AVG zelf. Teneinde de privacy van natuurlijke personen optimaal te beschermen heeft men in de AVG enkele bepalingen opgenomen die betrekking hebben op informatiebeveiliging. Het gaat daarbij onder meer om de artikelen 5, 5f, 25 en 32 waarin is vastgelegd dat een organisatie passende organisatorische en/of technische maatregelen neemt teneinde persoonsgegevens te beveiligen tegen van buitenaf komend onheil. Ook wordt aangegeven dat een organisatie prudent dient om te gaan met het verlenen van toegang tot systemen waarin persoonsgegevens zijn vastgelegd (toegangsautorisatie).

Rol van certificering

Naast de AVG is er ook vanuit andere invalshoeken aandacht voor informatiebeveiliging. In ISO 27001, ISO 27002, NEN 7510 en voor de overheid de BIO, wordt expliciete aandacht gegeven aan informatiebeveiliging.

In relatie tot de AVG kan hier nog het volgende over worden vermeld: artikel 42 AVG spreekt over certificering als een middel om aantoonbaar te maken dat aan de AVG wordt voldaan. Het mechanisme van certificering is niet verplicht maar kan een organisatie een (concurrentie)voordeel en haar klanten zekerheid opleveren indien zij gecertificeerd is.

Genoeg werk

Concluderend stellen wij vast dat de AVG een aanjager is voor informatiebeveiliging. Gezien het feit dat we vrijwel dagelijks worden geconfronteerd met vormen van cybercrime, datalekken en dergelijke, kan worden gesteld dat er nog genoeg werk is om informatiebeveiliging naar het juiste niveau te brengen en daarmee onder andere aan de AVG te voldoen. Houd hierbij rekening met het feit dat kwaadwillenden niet stilzitten en een permanente bedreiging vormen. De Autoriteit Persoonsgegevens zal met argusogen de vorderingen volgen die organisaties maken. Met name de inspanning die organisaties aantoonbaar hebben gemaakt om hun persoonsgegevens te beschermen, en zo te voldoen aan de in de AVG vastgelegde eisen, zal bepalend zijn voor de mate waarin tekortkomingen worden bestraft.

Maatregelen en risico in balans

Bovenstaande tips zijn beperkt. Iedere specifieke casus vraagt om een goede analyse van de actuele situatie. Op basis van die analyse kan vervolgens worden bepaald welke noodzakelijke maatregelen er genomen dienen te worden om te voldoen aan de AVG en om voldoende beschermd te zijn tegen calamiteiten. Maatregelen dienen qua inzet van middelen in balans te zijn met het risico dat wordt gelopen.

Neem minstens de volgende stappen:

- Draag zorg voor een actueel informatiebeveiligingsbeleid, inclusief de daarbij behorende procedures, en toets deze regelmatig.
- Koppel het informatiebeveiligingsbeleid aan de eisen van de AVG.
- Zorg dat je medewerkers bekend zijn met het beleid en procedures.
- Stuur op houding en gedrag zodat de zwakste schakel (de mens) de risico's herkent en erkent.
- Test frequent of je beveiligingsmaatregelen (nog) werken (via zogenoemde pentest).
- Houd de in de loop van de jaren verzamelde data eens tegen het licht, veel 'unstructured' data bevat mogelijk gegevens die organisaties volgens de AVG niet langer in bezit mogen hebben.
- Draag zorg voor passende organisatorische en technische maatregelen waaronder de verleende toegang tot systemen.

Private

The Attributer had the privilege of serving on the Jericho Forum during the period leading up to its closure (‘sunsetting’) in November 2013. During that period, we wrote paper to set out the principles for protecting the privacy of personal data. Recently, during the time of lockdown to control the Coronavirus pandemic, The Attributer was reminded of some of the problems that we encountered in that work. The issues were concerned with the use of photography to document our daily lives in the form of ‘selfies’ and other types of personal images.

Consider the following scenario: a family or a group of friends are on holiday in a foreign city. They visit famous landmarks such as the Taj Mahal, the Eiffel Tower, the Sydney Opera House or the Lincoln Memorial. They want to say to their friends and relatives that they were there and here’s the photo to prove it. It’s part of socialising.

That’s all well and good unless, in the background there are other people not intended to be part of the visual record, but just there by accident. The person who took the picture posts it on Facebook and there for all the world to see are the ‘extras’, in that place, at that time, and possibly in the company of other people whose association is an embarrassment. Suddenly a private outing becomes public on a global scale as they are recognised and reported in gossip columns around the world. We mean here of celebrities whose lives are examined in minute detail by the public. Politicians and public servants are amongst this group.

There is no malice or intent on the part of the people who take those photos and publish them on popular web sites. They own the copyright to the images and are unaware of the potential embarrassment that publication might cause. So, what can be done to protect the privacy of those ‘extras’? Whose responsibility is it to make sure that such unwanted publications do not take place? Can there be privacy protection for those individuals? Is it all at their own risk?

In the Jericho discussions we never quite found an answer to that last question, but the current trend in setting up new ‘home office’ facilities raises the closely related question again. If you sit at home with a video image of your virtual workplace, then what materials might be displayed in the background that give away personal private details about you and your family life that you really should not display? In these emergency situations people have often not given sufficient thought to the consequences of well-intented actions.

Then there is the issue of government intervention to control the spread of the virus. Governments are leveraging modern technology to help ensure that those ordered to self-isolate actually stay at home. In Hong Kong, new arrivals from abroad are required to wear electronic bracelets to track their movements, while in Singapore those self-isolating are contacted several times a day and required to send photographic proof of their whereabouts. In Taiwan, school children are automatically scanned as they approach the school building to monitor their body temperature and if it shows up as too high, they are turned away for detailed testing and possible quarantine.

The legal enforcement of these measures can be accompanied by heavy penalties. For example, Singapore can use jail terms for anyone who breaks a ‘stay at home’ order. It stripped one offender of his residency rights. Many countries in the West will find it hard to adopt such measures due to their larger populations, and greater civil liberties. However, to whatever extent a country introduces strong measures, there is also the question of how long those will remain in place and whether governments will seize an opportunity to weaken personal privacy legislation.

As with all risk management scenarios, what we see here is a complex interaction of risk factors: public health versus public freedom and personal privacy. SABSA is the framework that allows these risk factors to be played against one another with a view to optimising the outcomes, but it will also require the agreed definition of who are the policy makers and whose interests are being protected when policy is made.

The Attributer

Auteur: Robert-Jan de Vries is mede-eigenaar van Privacy Control Center - een GRC-tool voor privacy- en IB-professionals. Robert-Jan is bereikbaar via rdevries@privacycontrolcenter.com.

Sterker in je rol beleef je meer lol

Als functionaris gegevensbescherming bekleed je een ondankbare positie in je organisatie. Collega's ervaren gegevensbescherming als lastig en belemmerend, terwijl bestuurders het beschouwen als een eenmalig 'moetje' en liever investeren in de groei van de onderneming. Aan jou de schone taak om het management te overtuigen van nut en noodzaak van privacy- en informatiebeveiliging en bovendien de rest van de organisatie mee te krijgen. Een tool kan helpen om jouw positie te versterken, de kosten omlaag te brengen en aantoonbaar meer te bereiken.

De positie van de functionaris gegevensbescherming is verankerd in de AVG. Het management hoort erop toe te zien dat de FG wordt betrokken bij alle aangelegenheden die verband houden met gegevensbescherming én dat hij wordt voorzien van de benodigde middelen om zijn taak te kunnen vervullen. De FG rapporteert aan de 'hoogste leidinggevende', maar mag niet geïnstrueerd worden over de uitvoering van zijn taken. Hiërarchisch gezien is de plaats van de functionaris dan ook als onafhankelijk adviseur en toezichthouder náást het hoger management.

AVG-compliance is work in progress

In de praktijk hebben veel FG's de grootst mogelijke moeite om de bescherming van persoonsgegevens bij bestuurders onder de aandacht te brengen. Ze worstelen dagelijks met de vraag hoe zij noodzakelijke beleidswijzigingen en beschermingsmaatregelen geagendeerd en gebudgetteerd krijgen. Het wenselijke doel is om over de gehele linie aantoonbaar in control te zijn, maar sinds de komst van de AVG bevinden veel organisaties zich nog altijd in een meer of minder gevorderd stadium van implementatie. Dat betekent dat AVG-compliance op veel vlakken nog een 'work-in-progress' is en dat de FG zich als duizendpoot bezighoudt met velerlei verschillende ad hoc zaken die in een ideale wereld bij een privacyofficer of procesverantwoordelijke belegd is. Pas wanneer het privacybeleid zich in alle gelederen van de organisatie heeft gezet, kan de FG een passende afstand nemen en groeien in zijn rol als onafhankelijk toezichthouder. Tot het zover is, moet de organisatie – en met haar de FG – zich de nodige groeipijnen getroosten.

De uitdaging

Voor menig FG is het een uitdaging om verantwoordelijkheden rond gegevensbescherming te beleggen bij de mensen die verantwoordelijk zijn voor het betrokken proces of systeem. Zij zijn immers in the lead als het gaat om besluitvorming rond verandertrajecten en andere zaken die een mogelijke invloed hebben op de bescherming van persoonsgegevens. In veel gevallen vergt dit tijd en aandacht. Voor jouw collega's is gegevensbescherming een nieuw kennisdomein en zij zullen daarom gerichte ondersteuning en uitleg nodig hebben om privacy als vanzelfsprekend in hun besluitvorming mee te nemen. Het is daarbij zaak om veranderingen stapsgewijs te introduceren om te voorkomen dat men overvoerd wordt en gedemotiveerd raakt. Met een risico gebaseerde benadering geef je prioriteit aan de maatregelen die de grootste pijn wegnemen en het best aansluiten bij de dagelijkse praktijk. Zo kun je de inspanningen van collega's beperken tot de zaken die het meest bijdragen aan gegevensbescherming. Dit vergt een gestructureerde aanpak en beschikbaarheid van de kennis die nodig is om een gefundeerde inschatting te kunnen maken van de privacyrisico's in de organisatie.

Van risico's naar doelstellingen

Een FG die alleen reactief met maatregelen strooit om incidenten en datalekken te bestrijden zal eindeloos bezig zijn met het blussen van brandjes. Om afstand te kunnen nemen van de operatie is het noodzakelijk om een doelgericht beleid uit te stippelen, dat de organisatie stapsgewijs naar een hoger volwassenheidsniveau tilt. Een hoger volwassenheidsniveau betekent daarbij een hogere mate van verankering van gegevensbescherming in de processen van de organisatie. Basis voor dit beleid is een plan van aanpak, waarin de doelstellingen rond gegevensbescherming op hoofdlijnen zijn bepaald en waarin de voorgenomen maatregelen zijn afgestemd op reële risico's en echte praktijksituaties. De doelstellingen dienen door het hoger management onderschreven te worden en daarom is het zaak om deze te presenteren op een manier, die voor de bestuurder begrijpelijk is en een verband legt tussen de langetermijnvisie en benodigde middelen. Het gepresenteerde (jaar)plan zal daarom gekoppeld zijn aan risico's voor de organisatie, zodat het management in staat is om op grote lijnen nuances aan te brengen zonder daarvoor de maatregelen in detail te kennen.

Taakgestuurd werken

Het vertalen van doelstellingen naar concrete en behapbare taken brengt de onderneming daadwerkelijk naar een hoger volwassenheidsniveau. Dit is maatwerk: voor optimale werking zijn taken afgestemd op het kennis- en volwassenheidsniveau van de afdeling en de mensen die ze moeten uitvoeren. De beste methode is om deze taken dan ook in overleg met (vertegenwoordigers van) afdelingen uit te werken. Alleen zo krijgt de FG de mensen mee om verantwoordelijkheid te nemen voor gegevensbescherming binnen hun eigen processen of systemen, zodat hij kan ondersteunen vanuit zijn rol als intern toezichthouder.

Schaken op verschillende borden

Zoals uit voorgaande blijkt, moet je als FG op verschillende borden schaken om te komen tot een situatie waarin je jouw rol als adviserend toezichthouder optimaal vervult. Het juiste instrumentarium kan je helpen om de benodigde kennis bijeen te brengen, te structureren en te interpreteren. Met de juiste tooling word je ondersteund bij het identificeren van risico's en het vertalen van doelstellingen in passende maatregelen en de bijbehorende taken. Voor het inrichten van maatregelen is er overigens een ruim aanbod aan normen en sectorale toetsingskaders, die als leidraad en benchmark kunnen dienen. Met het oog op mogelijke certificering, nu of in de toekomst, is het raadzaam om bij deze best-practices aan te sluiten. Of in ieder geval te werken 'in de geest van'. De inzichtelijke, realtime rapportages die een online werkomgeving levert, zijn cruciaal voor het overtuigen van het management van de urgentie van voorgenomen maatregelen. Tot slot dient het complex van maatregelen en taken, en de voortgang daarvan, bij te dragen aan de verantwoordingstructuur, die in- of extern getoetst kan worden. Ondersteuning met het juiste instrumentarium helpt bij het gericht kennis en informatie aanbieden aan de verschillende belanghebbenden en hun rollen: what you see is what you need. Zo versterkt een goede GRC-tool jouw positie als FG (of CISO) en draagt deze bij aan het zalige gevoel van 'in control' zijn.

Auteur: Maria Genova, onderzoeksjournalist en schrijfster van het boek 'Komt een vrouw bij de h@cker'

Coronahackers slaan toe

Afbeelding 1 - Smartphone-app coronatracker. Illustrator: André Versteeg

Investeren in cyber awareness, een menselijke firewall, wordt steeds belangrijker. Vooral nu veel mensen thuiswerken op niet goed beveiligde netwerken slaan coronahackers toe. Maria Genova, schrijfster van het boek 'Komt een vrouw bij de h@cker', vindt dat ICT'ers meer aan voorlichting moeten doen om hacks en datalekken te voorkomen.

Geld spenderen aan dure ICT-tools is geld over de balk gooien als medewerkers niet begrijpen hoe hackers werken. Of zoals een bevriende hacker ooit zei: 'A fool with a tool is still a fool'. Een voorbeeld. Een medewerker van een bedrijf is toevallig op vakantie tijdens een phishingmailtest. De vakantieganger ziet de phishingmail te laat en mailt: "Ik was de afgelopen week niet aanwezig, kun je de link nog een keer sturen, want die werkt niet meer." Een andere reactie was: "Kan ik dit downloaden of is dit spam?" De medewerker kreeg netjes een antwoord van de hacker terug: "Ja hoor, download gerust!"

Momenteel zien de antivirus-providers een gigantische stijging van het aantal gevallen van spam, phishing en malware met gebruik van 'coronavirus' en 'COVID-19'.

Op welke manieren proberen cybercriminelen de computers en de mobiele telefoons over te nemen? En wat voor tips kun je de thuiswerkers geven?

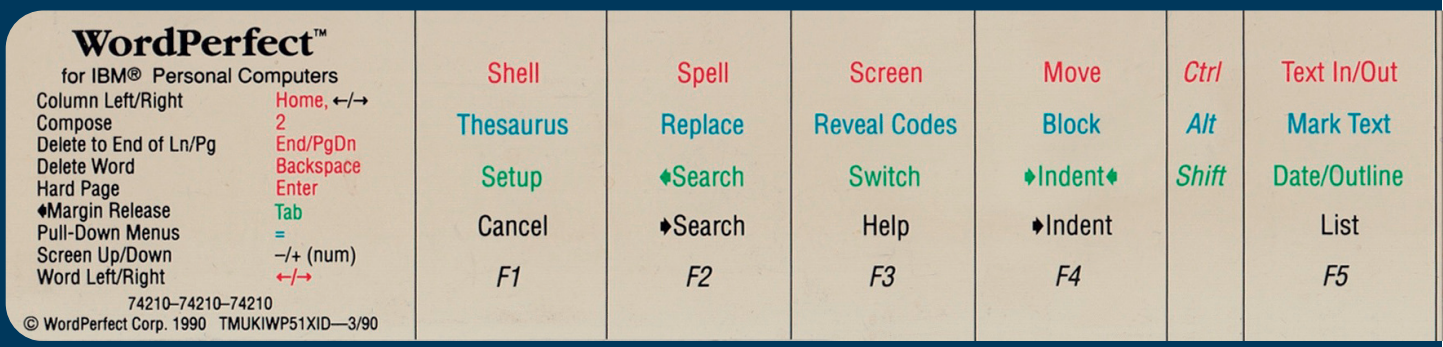
- Hackers maken gebruik van kwetsbaarheden in programma's die niet zijn geüpdatet. Veel thuiswerkers realiseren zich niet dat ze ook hun router en IOT-apparaten moeten updaten.

Houd een coronacyberquiz met recente voorbeelden uit de praktijk om de awareness van thuiswerkers te vergroten

- Fraudeurs doen zich voor als IT-helpdesk en bieden aan een probleem op te lossen. Als je jouw inloggegevens doorgeeft, kunnen ze veel schade aanrichten.
- Cybercriminelen sturen je een 'corona-update' namens jouw organisatie of namens het RIVM.
- Veel thuiswerkers gebruiken zwakke wachtwoorden of steeds hetzelfde wachtwoord voor al hun programma's. Concrete tips of een leuk webinar over wachtwoorden kunnen enorm helpen.
- Mailtjes van je bank met de mededeling dat je je bankpas moet inleveren in verband met corona-quarantaine.
- Valse e-mails, sms'jes of whatsapp-berichten van de overheid over extra toeslagen voor thuiswerkers in verband met corona.
- Valse e-mails van pakketbezorgers doen het ook goed, nu veel winkels gesloten zijn en alleen online bezorgen.
- Valse whatsapp- of sms-berichten van een bekende wiens identiteit is gestolen.
- Werknemers nemen met hun laptops ook vertrouwelijke bedrijfsgegevens mee naar huis. Hoe gaan ze daarmee om? Wat printen ze en hoe vernietigen ze de gegevens vervolgens?
- Het wifi-wachtwoord van thuisnetwerken is vaak niet sterk genoeg.
- Updates van slimme apparaten worden vaak niet uitgevoerd. Mensen weten niet dat die apparaten een springplank naar hun computer of mobiel kunnen zijn.
- De wachtwoorden voor Dropbox en iCloud zijn niet lang genoeg en twee-factor identificatie staat vaak niet aan.
- Er zijn kwaadaardige apps over corona die mobiele telefoons overnemen.
- Hackers hebben inmiddels ontelbare websites met informatie over corona geregistreerd. Soms klopt de informatie wel, maar probeert de website de computer van de bezoeker met malware te besmetten.
- Kwaadwillenden verstoppen computervirussen in een advertentie om bijvoorbeeld je bankrekening te plunderen.
- Pas op met het doorsturen van zakelijke informatie naar privémails en Gmails. Verander eenmalig het wachtwoord van je e-mail en kies voor minstens 14 karakters, bijvoorbeeld een zin.
- Weet je zeker dat de mail van jouw bedrijf komt? Klik op de afzender en zweef even met je muis boven de link in de e-mail om de betrouwbaarheid te checken.
- Let vooral op e-mails waarin gevraagd wordt om in te loggen op tools die de organisatie gebruikt. Vaak krijg je een nepinlogscherm dat professioneel nagemaakt is.
- Let op e-mails die afkomstig lijken van een leidinggevende met het verzoek om met spoed geld over te maken of gegevens door te sturen. Bedrijven raken op deze manier enorme bedragen kwijt.
- Cybercriminelen richten zich op ouders en voogden, bijvoorbeeld met nepmails over onderwijs op afstand.
- Pas op voor oproepen om te helpen bij het vinden van een geneesmiddel voor COVID-19. Een paar initiatieven komen van echte wetenschappers, maar hackers proberen je ook te verleiden tot deelname.
- Er is veel onduidelijkheid over wat wel en niet gemeld moet worden bij de IT-afdeling. Veel medewerkers melden niets als ze per ongeluk ergens op geklikt hebben. De meeste organisaties ontdekken te laat dat ze hackers in het systeem hebben.

Wees als organisatie duidelijk over de manieren waarop thuiswerkers kunnen worden aangevallen en wat wel en niet gemeld moet worden. Houd een coronacyberquiz met recente voorbeelden uit de praktijk om de awareness van thuiswerkers te vergroten. De quiz bestaat uit tien vragen en mag zonder verdere toestemming intern gebruikt worden: https://forms.gle/yRucH35FbQpJWNT79 .

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



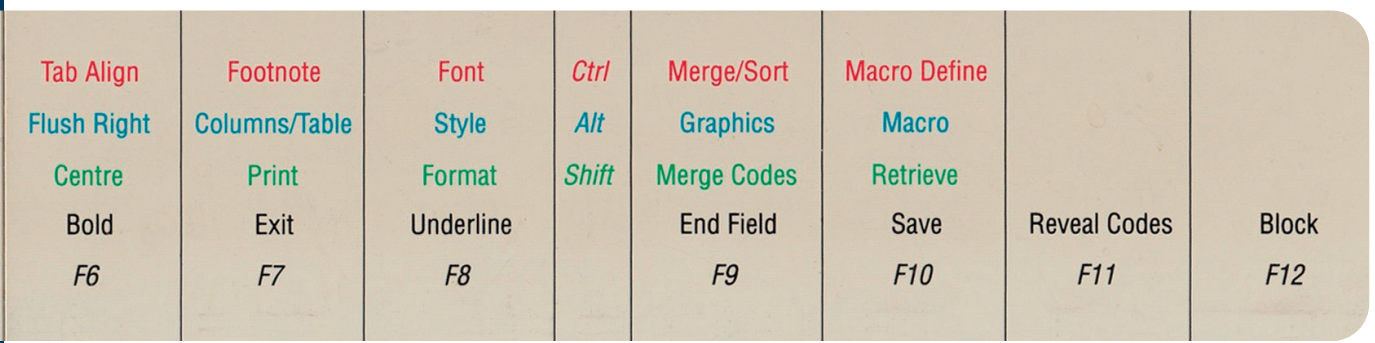
BLOG

Kiezen voor goedkoop en snel levert geen goed resultaat

In militaire dienst bezocht ik elke week de fotokopieerafdeling van de luchtdoelartilleriekazerne in Ede. Daar hing een bordje met: 'Klanten willen het goed, goedkoop en snel. Kies er twee en kom dan terug.' Dat geldt voor kopieeropdrachten, maar ook voor het ontwikkelen van computercursussen, wat ik toen deed. En, bleek later, ook voor het invoeren van information security controls (beheersmaatregelen) in organisaties.

Als Reserve Officier Academisch Gevormd was ik 'als hoogste in rang' verantwoordelijk voor OCMA Ede-West, een kleine dependance van het Opleidingscentrum Militaire Administratie in Middelburg. Ik werd na de militaire basisopleiding ingedeeld bij het dienstvak Technische Dienst of de Intendance en meteen benoemd tot vaandrig. De vaktechnische officiersopleiding van vier maanden zoals bij de wapens der artillerie, cavalerie of van de verbindingsdienst, verviel. We hadden immers net een studie aan een universiteit afgerond. Het mes sneed zo aan twee kanten. De ROAG kreeg werkervaring in het eigen vakgebied en ik had een plezierige diensttijd. Leuker dan een tank drie keer overschilderen of schuttersputten graven en meteen weer dempen. En werkgever Defensie beschikte zo in door haar uitgekozen studierichtingen over een overzichtelijke soldij en de actuele kennis van net-afgestudeerden.

Enfin, ik had een kopieeropdracht omdat we als klein team (vier dienstplichtigen en een beroepsmilitair) elke week zestien cursisten moesten opleiden in algemeen computer- en printergebruik; hanteren van het operating system en ontwikkelen van spreadsheets, relationele databases (acht personen) en tekstverwerken met WordPerfect (de andere acht). Het was toen MS-DOS 3.20. De 5,25 inch floppy diskettes met 360 kB opslagruimte waren nog slap en cursisten moesten ze zelf formatteren voor gebruik. We hadden wel ook al harde 3,5 inch diskettes. Die zie je nog steeds in Windows als icoon voor 'bestand opslaan'. Op het witte vierkantje bovenaan de diskette schreef je welke gegevens erop stonden: data labeling pur sang. Zonder Windows en computermuizen ging alle bediening met toetscombinaties, functie- en cursortoetsen. Een papieren strookje toonde de



werking van alle WordPerfect toetscombinaties van ctrl, alt en shift met de twaalf functietoetsen bovenaan op het keyboard.

PC's met 640 kB geheugen

Matrixprinters hadden mechanische dipswitches. Daarmee kon je met een lucifer of potlood het lettertype wisselen. Dozen met papier met witte en lichtblauwe banen, zigzag gevouwen, om na elke printopdracht af te scheuren en inktcartridges die cursisten zelf konden verwisselen. NLQ, Near Letter Quality, door elke regel twee keer te printen met iets verschoven pixels. En verder Bernoulli-schijven van 10 of zelfs 20 MB voor de verwisselbare massa-dataopslag. In elke PC maar liefst 640 kB intern geheugen! Met de editor van Norton Utilities konden we op byteniveau gegevens aanpassen in software, databases of de File Association Table. Zoals de scorelijst van videospelletjes of de mogelijke kleurcombinaties van spreadsheets. Of in de file attributes een file hidden maken. Mooie tijd man. Werken bij defensie met de state of the art computertechnologie van toen, die nu vrijwel verdwenen of vergeten is. Maar wat zullen we over tien of twintig jaar lachen om een touchscreen met Android 9 of een 'mobiele app'.

Elke dag voegden we als instructeurs onze ervaringen samen. In tien weken veranderden we zo stapsgewijs - of 'agile' zoals we dat onder elkaar voor de grap noemden - de geprogrammeerde instructie van Defensie in een mininaslagwerk. Met ook een uitleg waarom bepaalde toetsen nodig waren en toelichtende cartoons, zodat de cursisten het cursusdocument op de eigen werkplek konden blijven gebruiken. En ook omdat we zo veel minder, laten we zeggen, 'overbodige' vragen hoefden te beantwoorden tijdens elke cursusweek. Nederlandse dienstplichtigen werden namelijk destijds wereldwijd geroemd om hun luiheid, omdat die hen inspireerde tot inventieve oplossingen. Vrije haardracht en afschaffen van de groetplicht leverde Defensie lichtingen dienstplichtigen op die zelf nadachten. Vooral in crisissituaties waarin geïmproviseerd moet worden wanneer er geen militaire leiding (meer) is. Terwijl ik dit schrijf, zijn in Nederland alle kappers gesloten en is er terecht verplichte social distancing. Ik hoop dat de inventiviteit er ook nu weer is.

Goed en goedkoop, maar dan niet snel

Door bovengenoemde aanpak kreeg de Koninklijke Landmacht goedkoop en een bruikbaar lespakket van goede kwaliteit. Het was alleen niet snel beschikbaar. Men had natuurlijk onze studiegenoten kunnen inhuren die door broederdienst, hun eigen platvoeten of een niet-dienstplichtig geboortejaar meteen na hun afstuderen in het bedrijfsleven konden starten als consultant of trainer. Dan was het in korte tijd ook goed geworden, maar wel (veel) duurder uitgevallen. Snel en goed, maar niet goedkoop. Ook bij securityprojecten kun je met goedkope medewerkers een goed resultaat bereiken. Het gaat dan helaas niet snel, heb ik later gemerkt. Als je het goed én snel wilt, zul je als opdrachtgever ook moeten investeren, bijvoorbeeld door meer ervaren medewerkers op te nemen in het team. Als je bij de start van een security-project uitsluitend eisen stelt aan de maximaal acceptabele levertijd en prijs (dus snel en goedkoop), krijg je aan het eind zeker iets geleverd. Maar de B-I-V-kwaliteit van het eindresultaat zal je tegenvallen. Zoals wanneer je videoconferencing tool het wel steeds doet (Beschikbaarheid-Integriteit-Vertrouwelijkheidr) en nuttige functionaliteit biedt die goed werken (integriteit), maar dat de privacy (vertrouwelijkheid) ervan helaas veel te wensen overlaat. Als we hierop inzoomen, geldt ook in dit geval: two out of three is bad.

Auteurs: Robbin Begeer is security consultant bij Tesorion. Robbin is bereikbaar via robbin.begeer@tesorion.nl. Lex Borger is security architect en docent bij Tesorion en oud-hoofdredacteur van IB-magazine. Lex is bereikbaar via lex.borger@tesorion.nl.

Duidelijke en eenvoudige taal. Hoe beoordeel je die?

De AVG wordt nu bijna twee jaar gehandhaafd en elke organisatie heeft inmiddels wel een privacystatement. Maar hoe zit het met de kwaliteit daarvan? In The Privacy Project van de New York Times (1) deden ze er al onderzoek naar. Hierdoor geïnspireerd vroegen we ons af hoe het in Nederland gesteld is met de privacyverklaringen. Is de kwaliteit hiervan tastbaar te maken? Waar moet je op letten? We doen met dit artikel een poging.

Over de communicatie van bedrijven naar personen zegt de AVG (2): `… Voor natuurlijke personen dient het transparant te zijn dat hen betreffende persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt en in hoeverre de persoonsgegevens worden verwerkt of zullen worden verwerkt. Overeenkomstig het transparantiebeginsel moeten informatie en communicatie in verband met de verwerking van die persoonsgegevens eenvoudig toegankelijk en begrijpelijk zijn, en moet duidelijke en eenvoudige taal worden gebruikt.' Inderdaad, als het doel is om eenvoudig toegankelijk en begrijpelijk te zijn, is duidelijke en eenvoudige taal een goed middel. Meer staat er dan eigenlijk niet in de AVG. Deze tekst wordt nog een paar keer herhaald en daar blijft het bij. De privacyverklaring is niet de enige tekstsoort die de noodzaak heeft toegankelijk en begrijpelijk te moeten zijn. Dat moet gelden voor alle communicatie van de overheid. Over dit onderwerp moet dus wel meer informatie te vinden zijn.

Duidelijke taal

Als we het hebben over eenvoudige taal, dan hebben we het in de wandelgangen over Jip-en-Janneke taal, maar dat is eigenlijk niet correct. Annie M.G. Schmidt was een expert in het beschrijven van uiteenlopende onderwerpen in zeer eenvoudige taal, geschikt voor zelfs de beginnende lezer. Het is moeilijk om op dit niveau volwassen onderwerpen zoals privacy goed genoeg uit te leggen. De overheid heeft zelf de norm te communiceren met de burger op een hoger niveau, dat aangeduid wordt met het Europees ReferentieKader-niveau B1 of het onderwijsniveau 2F. Dit komt overeen met het minimum taalniveau van iemand met een mbo-2/mbo-3 opleiding (3). Bevestiging dat de auteurs van de AVG er ook zo over denken komt in de volgende passage over communicatie specifiek gericht op kinderen:
`… Aangezien kinderen specifieke bescherming verdienen, dient de informatie en communicatie, wanneer de verwerking specifiek tot een kind is gericht, in een zodanig duidelijke en eenvoudige taal te worden gesteld dat het kind deze makkelijk kan begrijpen.'

Het niveau van de tekst alleen is natuurlijk niet zaligmakend, daar is genoeg discussie over (4), maar het is desondanks een concreet fundament waar we mee kunnen werken. Dus werd het zaak om middelen te vinden die ons een indicatie geven van het ERK-niveau of het onderwijsniveau van een tekst. Dat bleek echter moeilijk. De beschrijvingen van de ERK-niveaus zijn kwalitatief en hebben het oordeel van een taalkundige nodig. Het CITO heeft een programma om de onderwijsniveaus te bepalen op basis van een Cito LeesIndex voor het Basisonderwijs-score, maar dat programma is niet publiekelijk beschikbaar. Uiteindelijk hebben we twee middelen gevonden die ons geholpen hebben de teksten op eenvoud en duidelijkheid te analyseren, zie het kader 'Middelen'.

Middelen

Het CITO-programma P-CLIB bepaalt het onderwijsniveau van een tekst door een leesbaarheidsscore te bepalen. De informatie over de bepaling van deze score is te summier en niet consistent. Wel wordt het duidelijk welke tekstkenmerken gebruikt worden in die beoordeling (5):

- GWL = gemiddelde woordlengte in letters
- PFREQ = percentage hoogfrequente woorden
- TTR = type-token-ratio (aantal verschillende woorden gedeeld op het totaal aantal woorden)
- GZW = gemiddeld zinslengte per woord

Om een idee te geven: als we naar de volledige tekst van de Universele Verklaring van de Rechten van de Mens (UVRM) kijken (10984 letters, 1987 woorden, 95 zinnen), vinden we dat de gemiddelde woordlengte 5,52 letters is, en de gemiddelde zinslengte 20,9 woorden is. Het gebruikt 573 unieke woorden (28,8%). De meeste van deze kenmerken zijn objectief te meten voor een tekst via een aantal tools/services. Wij konden geen middel vinden dat specifiek gericht is op het Nederlands, dus hebben we ons gericht op tools voor de Engelse taal en kozen WebFX' Readability Test Tool (6). De uitzondering die moeilijker te meten valt is PFREQ, het percentage hoogfrequente woorden. Dit meetpunt zegt ook meer over de duidelijkheid van het taalgebruik, daarom schuiven we dit kenmerk door naar het andere aspect waar we naar moeten kijken.

Tekstlengte

Eerst is er nog iets te zeggen over een ander kenmerk: de tekstlengte. Ook dit raakt de begrijpelijkheid, want een lange tekst doornemen kost meer tijd. Een (vlotte) lezer leest ongeveer 250 woorden per minuut. Een langere tekst vergt langere concentratie en vermoeit de lezer dus meer. Dit speelt voor de universele bepaling van eenvoud geen rol, maar in onze context wel. Net zoals een toespraak, hoort een privacyverklaring lang genoeg te zijn om alles te omvatten en kort genoeg om de aandacht vast te houden. De verklaring moet kort zijn, maar ook een bepaalde inhoud dekken en zal dus een bepaalde lengte moeten hebben. Hier is dus sprake van een optimum dat gevonden moet worden tussen deze twee aspecten. Eerder hebben we gezien dat de UVRM ongeveer 2000 woorden bevat. Onze verwachting is dat een privacyverklaring vergelijkbare eenvoudige taal moet hebben, met een vergelijkbare lengte en dus eenvoudig in tien minuten door te lezen is. En dit is nog maar het eerste aspect waarop we de gebruikte taal moeten beoordelen. Er moet ook nog duidelijke taal gebruikt worden. Hiervoor dien je naar het woordgebruik te kijken. Woorden zijn eenvoudig objectief te tellen en woordfrequenties ook. Dus ook hier gingen we op zoek naar een tool. We zijn uitgekomen op een initiatief van een Nederlandse wiskundedocent (7), vooral omdat de resultaten eenvoudig copy-paste-baar zijn. Op deze eenvoudige woordtellingen kunnen additionele analyses uitgevoerd worden om te bepalen hoe duidelijk de taal is, bijvoorbeeld door de waarde van het PFREQ-kenmerk te bepalen. Hiervoor is wel een lijst nodig van de meest gebruikte Nederlandse woorden. Deze is beschikbaar, maar er is geen formele standaardlijst. Als we een lijst kiezen en vastleggen is het percentage frequente woorden in een tekst objectief te bepalen. Een ander kenmerk dat in beschouwing genomen wordt in de WebFX Readability Test Tool is het aantal lettergrepen per woord. Het gebruik van woorden met meer lettergrepen maakt de tekst minder begrijpelijk. Gevoelsmatig klinkt dit correct. Kijken we weer naar de UVRM, dan zien we dat (naar schatting) veel frequente woorden worden gebruikt, ongeveer 95%. Het percentage complexe woorden (drie lettergrepen of meer) is 25,2%. WebFX is geschikt voor de Engelse taal. We verwachten echter dat als we WebFX gebruiken om een lettergreeptelling op een Nederlandse tekst uit te voeren we desondanks een betrouwbaar resultaat krijgen door de gelijkheid in de talen. Onze testen wijzen uit dat er zelfs een direct verband is tussen gemiddelde woordlengte en het percentage complexe woorden. Het is dus niet nodig de lettergreeptelling apart mee te nemen. De duidelijkheid van een tekst bepalen blijkt dus moeilijker dan de eenvoud ervan bepalen, maar het is mogelijk dit redelijk objectief te doen, door te letten op het percentage unieke woorden per tekstlengte en de gemiddelde woordlengte. Daarnaast is de duidelijkheid ook gediend bij het gebruik van duidelijke woorden. Hierbij verwachten we geen vaagheden, minder algemene woorden en meer specifieke woorden. Voor het domein privacy en de context privacyverklaring denken wij dat de volgende klassen indicaties kunnen geven van groepen gerelateerde specifieke woorden:

- basistermen: persoonsgegevens, gegevens, informatie;
- online-activiteiten: profiel, account, social media, website, cookies;
- organisatieactiviteiten: verwerken, gebruiken, bewaren, opslaan;
- juridisch: privacy, wetgeving, recht(en), belang, toestemming.

Hoe doen Nederlandse bedrijven het?

Met de middelen om privacyverklaringen te analyseren in de hand hebben we de gelegenheid om een aantal Nederlandse organisaties onder de loep te nemen. We doen niet zo'n breed onderzoek als de New York Times deed, we voeren slechts een steekproef uit. We kozen representanten uit verschillende sectoren. Zo kwamen we tot een lijst van zestien bedrijven:

- Supermarkten: Jumbo, Albert Heijn en Lidl;
- Onderwijsinstellingen: Universiteit van Amsterdam en Avans Hogeschool;
- Zorginstellingen: Erasmus MC en Parnassia Groep
- OV-bedrijven: Nederlandse Spoorwegen, Connexxion en GVB;
- Banken: ING, Rabobank en ABN AMRO;
- Verzekeraars: Nationale Nederlanden, Achmea
- Winkelketen: IKEA

De privacyverklaring die we gebruikt hebben is de eerste volledige verklaring die we via een verwijzing op de homepage van de organisatie vonden. We hebben geen samenvattingen gekozen en geen deelverklaringen, als bijvoorbeeld een cookieverklaring apart aangeboden werd.

Lengtekenmerken

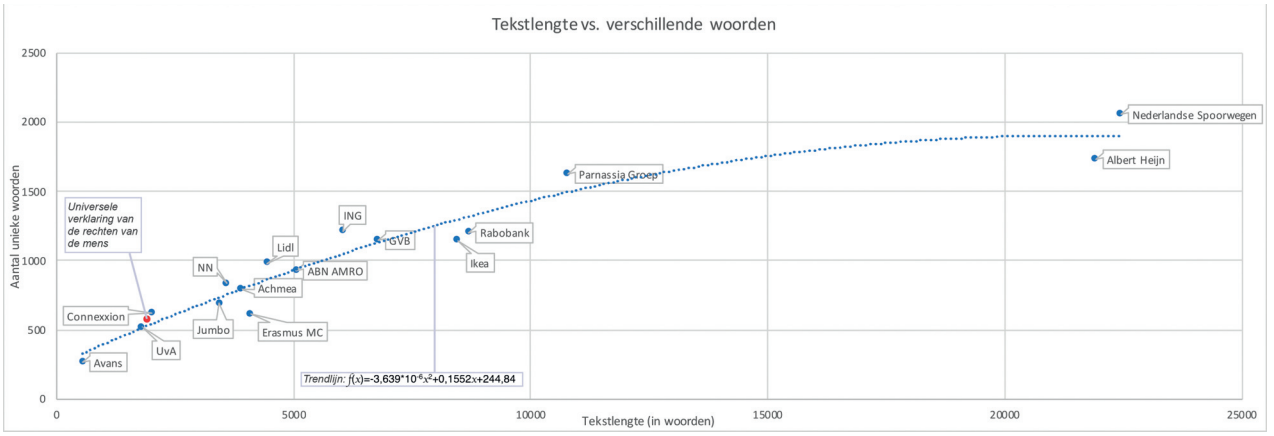
Om de eenvoud van het taalgebruik te beoordelen kijken we naar de lengtekenmerken: woordlengte, zinslengte en tekstlengte. Deze elementen zijn opgenomen in tabel 1.

Woordlengte

Als we kijken naar de woordlengte van de bekeken privacyverklaringen, dan is er niet zoveel verschil te zien. Dit varieert van 4,9 tot 6,2. Binnen deze bandbreedte valt wel op dat onderwijsinstellingen en gezondheidszorg langere woorden gebruiken. De teksten hebben een gemiddelde woordlengte van 5,9 letters. Twee voorbeelden uit de privacyverklaringen van Avans en Parnassia om een gevoel te geven hoe dat leest: 'Avans Hogeschool draagt zorg voor een adequaat beveiligingsniveau. Er is voorzien in passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.' (6,8 letters per woord).
'De gegevensverwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met de AVG voor de rechten en vrijheden van de betrokkene.' (6,1 letters per woord).

		Eenvoudige taal				Duidelijke taal		
Bedrijf	**Branch**	**Leestijd (min.)**	**Tekstlengte**	**Woordlengte**	**Woorden per zin**	**Verschillende woorden**	**Afwijking van trendlijn**	**Percentage complex**
Jumbo	Supermarkt	14	3427	5,5	17,0	692	-6%	25%
Albert Heijn	Supermarkt	88	21915	5,2	12,4	1732	-9%	21%
Lidl	Supermarkt	18	4436	5,5	14,4	985	14%	23%
Universiteit van Amsterdam	Onderwijs	7	1800	5,9	17,1	517	1%	29%
Avans Hogeschool	Onderwijs	2	545	6,2	15,9	262	-20%	31%
Erasmus MC	Gezondheidszorg	16	4097	5,6	18,9	615	-25%	28%
Parnassia Groep	Gezondheidzorg	43	10772	6,0	18,6	1627	9%	29%
Nederlandse Spoorwegen	Openbaar vervoer	90	22452	5,5	17,3	2062	9%	26%
Connexxion	Openbaar vervoer	8	2010	5,9	15,4	622	15%	29%
GVB	Openbaar vervoer	27	6776	5,8	20,2	1152	2%	26%
ING	Financiele dienst	24	6050	5,4	14,5	1213	15%	26%
Rabobank	Financiele dienst	35	8695	5,4	12,4	1201	-9%	25%
ABN AMRO	Financiele dienst	20	5055	5,4	13,4	931	-1%	23%
Nationale Nederlanden	Verzekeraar	14	3583	5,7	13,4	834	11%	26%
Achmea	Verzekeraar	16	3890	5,7	16,0	791	0%	27%
Ikea	Winkelketen	34	8454	4,9	15,8	1148	-11%	19%
Universele verklaring van de rechten van de mens	*Voorbeeld*	*8*	*1987*	*5,5*	*20,9*	*573*	*6%*	*25%*
	gemiddelde	28	6820	5,6	16,1	997	NVT	26%
	minimum	2	545	4,9	12,4	262	-25%	19%
	maximum	90	22452	6,2	20,9	2062	15%	31%
	variatie	190,5%	NVT	22,8%	50,8%	NVT	NVT	48,8%

Tabel 1 - Overzicht Eenvoudskenmerken.



Figuur 1 - Scatter-diagram Lengte vs. Unieke woorden.

Supermarkten en banken gebruiken kortere woorden. IKEA spant de kroon met een gemiddelde woordlengte van slechts 4,9 letters. Lees ter vergelijking een passage uit hun verklaring: 'We gebruiken aankoopgegevens om beter inzicht te krijgen in onze klanten en de manier waarop ze winkelen. Dit doen we om het aanbod in onze winkel te verbeteren. De gegevens voor deze analyses bewaren we twee jaar.' (4,7 letters per woord).
De zinslengte geeft een afwisselender beeld, deze waarde varieert van 12 tot 20 woorden. Dit is opvallend, omdat in dit geval de privacyverklaringen allemaal onder de gemiddelde zinslengte zitten van de verklaring van de rechten van de mens (20,9 woorden per zin). Kennelijk is het gebruik van korte zinnen een eenvoudig toepasbare maatregel om taal te vereenvoudigen.

Tekstlengte

Bij tekstlengte zien we grote verschillen. De verklaring van de rechten van de mens mag in tien minuten te lezen zijn, weinig privacyverklaringen halen dat: alleen die van de UvA, Avans en Connexxion. Neem voor de gemiddelde privacyverklaring maar een half uur en voor de langste anderhalf uur (Albert Heijn en de Nederlandse Spoorwegen). Misschien zijn die lange versies niet bedoeld om van voor tot achter door te lezen. Zo heeft Albert Heijn een interactieve versie op haar website staan, waar je kunt kiezen over welk onderwerp je meer wil lezen. Anderen kiezen bijvoorbeeld om een samenvatting naast de verklaring aan te bieden, zoals de Parnassia Groep en het GVB. Voor de meeste verklaringen duurt het lezen ervan flink langer dan het lezen van de verklaring van de rechten van de mens, tussen een kwartier en een ruim half uur. Dat is te doen, maar je moet er wel voor gaan zitten. We vermoedden al dat er een afweging gemaakt moest worden tussen woordlengte en tekstlengte. De korte verklaringen hebben relatief een langere woordlengte. Over het geheel heeft IKEA een mooie prestatie geleverd met een hele korte woordlengte bij een tekstlengte net boven gemiddeld (+19%).

Duidelijke taal

Om de duidelijkheid van de taal in de privacyverklaringen te bepalen kijken we naar het gebruik van verschillende woorden en specifiek woordgebruik (zie kader 'Middelen'). In een verklaring kun je verwachten dat het aantal unieke woorden hoger is naarmate de tekst langer is. Tegelijkertijd zal de groeitrend hiervan afnemen bij langere teksten, zie figuur 1. Deze figuur toont hoe de bekeken verklaringen voldoen aan deze verwachting door teksten te plotten op basis van hun lengte en aantal unieke woorden.

Het was mogelijk om over de punten in de figuur statistisch een passende curve te vinden waar de bekeken verklaringen minimaal van afwijken. Op dit punt zijn de teksten kennelijk goed vergelijkbaar. Teksten boven de curve gebruiken relatief meer verschillende woorden (bijvoorbeeld Lidl, Connexxion, ING), teksten onder de curve gebruiken relatief minder verschillende woorden (bijvoorbeeld Avans Hogeschool en Erasmus MC). Mogelijk is de verklaring hiervoor dat boven de curve de meer gevarieerde teksten staan en onder de curve meer gestructureerde teksten.
Als laatste kijken we naar specifiek woordgebruik en de consistentie daarvan. We hebben vier klassen van specifieke woorden gedefinieerd (zie kader 'Middelen') en bekijken hoe de verklaringen woorden uit die klassen gebruiken. Dit geeft ons de duidelijkheid van de taal in de context van een privacyverklaring en daarmee dus inzicht in de helderheid van die verklaring.
In vrijwel alle privacyverklaringen vallen de basistermen 'gegevens' en 'persoonsgegevens' onder de meest voorkomende woorden. Persoonsgegevens slaat echter op geïnterpreteerde of interpreteerbare gegevens, dus informatie. Lees wat persoonsgegevens nu precies zijn, volgens de AVG (2): '… alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon …' De term 'gegevens' lijkt dus juist niet duidelijk genoeg. Dat het toch overwegend gebruikt wordt, komt wellicht doordat deze basisterm als definitie is overgenomen uit de wet. Opvallend genoeg

Woordfrequentie	Gegevens en informatie			Social media en online					Organisatie	Juridisch				
Bedrijf	Gegevens	Informatie	Persoons-gegevens	Profiel(en)	(gebruikers)account	Social(e) + media	website	cookies	Verwerken Verwerking	privacy	recht(en)	belang	toestem-ming	wet/wet-geving
Jumbo	6	88	22	2	25	x	x	8	9	24	15	10	8	5
Albert Heijn	304	88	27	169	8	11	79	13	114	37	6	7	22	1
Lidl	47	13	37	x	12	11	37	54	12	17	12	6	15	5
Universiteit van Amsterdam	7	7	70	x	1	1	4	1	21	7	1	4	7	5
Avans Hogeschool	6	1	9	x	x	x	1	x	4	5	2	2	x	2
Erasmus MC	65	7	95	x	x	x	1	1	61	10	11	10	9	13
Parnassia Groep	71	44	150	x	x	3	2	x	87	10	29	17	27	38
Nederlandse Spoorwegen	377	83	190	2	14	6	28	32	110	68	16	39	51	13
Connexxion	30	7	25	x	x	6	8	8	9	17	3	3	5	2
GVB	48	20	122	x	7	3	5	3	27	13	10	3	7	8
ING	76	26	63	7	x	2	5	§	20	54	29	3	10	10
Rabobank	196	19	78	4	x	4	12	3	53	44	21	27	20	15
ABN AMRO	19	5	124	6	x	3	12	3	8	17	14	11	11	24
Nationale Nederlanden	66	7	54	1	2	x	5	3	19	20	10	5	6	7
Achmea	90	5	11	x	x	2	5	2	10	20	12	5	4	9
Ikea	175	19	9	40	33	17	20	42	12	54	8	7	15	4

Tabel 2 - Overzicht Woordfrequenties.

lijken de communicatiemedewerkers bij Jumbo het met ons eens te zijn. Zij prefereren als enige duidelijk het woord 'informatie' (88 keer gebruikt) boven 'gegevens' (6 keer gebruikt).

Veel tekst in verklaringen heeft betrekking op online-activiteiten. De supermarkten Albert Heijn en Lidl en winkelketen IKEA verwijzen vaak naar woorden in deze klasse. Komt dit doordat hun aandacht voor commerciële online-activiteiten de laatste jaren flink zijn toegenomen? Dit is waarschijnlijk in mindere mate ook het geval bij de Nederlandse Spoorwegen en Connexxion. De banken doen veel online-activiteiten, maar daar is het gebruik meer essentieel dan commercieel. Wellicht heeft dit daarom voor hen geen specifieke aandacht nodig in de privacyverklaring.

Onder de organisatieactiviteiten valt vooral op dat een privacyverklaring geschreven is met vormen van het woord 'verwerken' (Albert Heijn, Parnassia Groep, Nederlandse Spoorwegen, Rabobank) of juist alternatieven daarvan ('gebruiken', 'bewaren', 'opslaan'). Zien we hier nog een schim van de jurist in de tekst van de verklaring?

Woorden in de juridische klasse scoren over het geheel genomen laag. Dit geeft aan dat men kennelijk de moeite heeft genomen om de formele, juridische termen niet te vaak te noemen. Albert Heijn spant hier de kroon, buiten het woord 'privacy' worden slechts 36 juridische termen gebruikt in hun lange verklaring.

Om de duidelijkheid van een privacyverklaring te beoordelen is het kijken naar het woordgebruik het meest bepalend. Een duidelijke keuze maken en dan consistent zijn met het woordgebruik is waarschijnlijk de beste strategie. Dan gaat ook het percentage unieke woorden ten opzichte van de tekstlengte omlaag, wat verder bijdraagt aan de duidelijkheid.

Bevindingen

Harde conclusies kunnen we niet trekken op basis van wat we gezien hebben met deze kleine steekproef onder privacyverklaringen. Wel kunnen we zeggen dat het aantoont dat het best goed gesteld is met de leesbaarheid van deze teksten. Zonder de eenvoud taalkundig te hebben laten beoordelen lijken de tekstkenmerken overeen te komen met ERK-niveau B1, soms wat lager (IKEA) en soms wat hoger (Universiteit van Amsterdam en Avans Hogeschool). Voor wat betreft de duidelijkheid is het taalgebruik consistent, soms wat formeel, zoals het gebruik van de wetsterm 'verwerken'. Een grote uitzondering vonden we in de variëteit in lengte. Meer vergelijkingen zijn nodig om te zien of dit een afwijking is in de steekproef, of dat deze verscheidenheid doorzet. Meer vergelijkingen geven ook meer inzicht in de trends in het woordgebruik. Met name de sectoren die nog niet opgenomen zijn in onze steekproef (zoals overheden, industrie, MKB) kunnen wellicht geheel nieuwe sectorale inzichten verschaffen.

Referenties

(1) New York Times - We Read 150 Privacy Policies. They Were an Incomprehensible Disaster: https://www.nytimes.com/interactive/-2019/06/12/opinion/facebook-google-privacy-policies.html

(2) AVG: https://autoriteitpersoonsgegevens.nl/sites/default/-files/atoms/files/verordening_2016_-_679_definitief.pdf.

(3) Staatsexamens Nt2: https://www.staatsexamensnt2.nl/veel-gevraagd/met-welk-cefr-erk-niveau-komen-de

(4) Volkskrant - Pleidooi voor duidelijke taal niet altijd even helder: https://www.volkskrant.nl/gs-b1a4332e.

(5) Begrijpelijke taal - Begripsvoorspelling: http://www.kennisbank-begrijpelijketaal.nl/begripsvoorspelling/ned_formules.

(6) Readability Test Tool: https://www.webfx.com/tools/read-able/.

(7) Woord en letterteller: http://home.wxs.nl/~hklein/zipf/zipf.htm

Auteur: mr. drs. Judith van Schie is legal director bij Considerati www.consideratie.com

Het Citrixlek: hoe kwetsbaar was uw organisatie nu echt?

Iedereen wordt momenteel geacht zoveel mogelijk thuis te werken. Gelukkig is dit technisch goed mogelijk. Dat was begin dit jaar wel anders. Voor veel Nederlandse organisaties was thuiswerken tijdelijk uitgesloten, en op de snelwegen stonden 'Citrixfiles'. Aanleiding hiervoor was een beveiligingslek bij het Amerikaanse bedrijf Citrix. Dit artikel gaat dieper in op de risicoafweging die gemaakt moest worden en waarom het belangrijk is dat de DPO (Data Protection Officer) bij deze afweging wordt betrokken.

Afbeelding 1 – Tijdlijn.

Eerst een overzicht van de belangrijkste gebeurtenissen in januari 2020.

Op 17 december 2019 maakt Citrix publiekelijk bekend dat er een kwetsbaarheid in haar Citrix ADC en Citrix Gateway toepassingen (voorheen bekend als Netscaler) is geconstateerd. Deze thuiswerktoepassingen zijn wereldwijd veelgebruikt. Ongeveer 1800 Nederlandse organisaties, waaronder Rijksoverheidsorganisaties, gemeentes, ziekenhuizen en grote bedrijven, werken met Citrix en werden hierdoor (potentieel) geraakt. Er is op dat moment nog geen definitieve, afdoende oplossing beschikbaar. Wel publiceert Citrix een aantal mitigerende maatregelen die organisaties kunnen treffen. Op 11 januari is er een exploitcode beschikbaar. Deze code maakt het voor kwaadwillenden bijzonder gemakkelijk om van de kwetsbaarheid van de Citrixsystemen misbruik te maken. Al snel blijkt dat deze exploitcode door diverse aanvallers gebruikt wordt. Dat wil zeggen: er is geconstateerd dat actief wordt gezocht naar kwetsbare systemen. Het Nationaal Cyber Security Centrum (NCSC) adviseert Rijksoverheidsorganisaties en vitale organisaties om zo snel mogelijk de door Citrix geadviseerde mitigerende maatregelen te nemen.

Op 13 januari constateert het NCSC dat er nog altijd veel Citrixsystemen in Nederland kwetsbaar zijn. Het NCSC plaatst

daarom een bericht op haar website en social media om hier voor te waarschuwen. Zij geeft aan dat deze kwetsbaarheid qua ernst wordt ingeschaald op 9,8 op een schaal van 1 tot 10. Vele Nederlandse Citrixservers zijn kwetsbaar voor aanvallen (1).
Op 17 januari adviseert het NCSC om de Citrixsystemen uit te schakelen, tenzij een organisatie aan alle volgende drie voorwaarden voldoet:

1) wanneer uitschakeling disproportionele gevolgen heeft voor bijvoorbeeld de veiligheid en gezondheid; en
2) er afdoende extra monitorings- en beveiligingsmaatregelen kunnen worden genomen; en
3) systemen effectief gecompartimenteerd of in quarantaine gezet kunnen worden, er voldoende detectiemogelijkheden zijn en contaminatie (besmetting) van de eigen systemen en die van anderen uitgesloten kan worden.

Een groot deel van de Nederlandse organisaties besluit daarop om hun Citrixsystemen uit te schakelen. Deze beslissing heeft 'Citrixfiles' tot gevolg; doordat thuiswerken plotseling onmogelijk wordt voor een groot deel van werkend Nederland, is het een stuk drukker op de weg (2).

Op 20 januari stelt Citrix patches (reparaties) beschikbaar die een oplossing bieden voor 50% van de kwetsbare Citrixsystemen in Nederland. Door deze patches werkt de exploitcode niet meer. Er zitten wel programmeerfouten in deze nieuwe patches, blijkt uit onderzoek. Dat gebeurt vaker als er patches worden uitgevoerd, maar de programmeerfouten zaaien wel twijfel of deze patch 100% waterdicht is. Er blijft hierdoor een restrisico over. Als een organisatie niet als een testcase voor deze patch wil fungeren, kan de organisatie beter wachten op de laatste patch, die 24 januari beschikbaar komt. Op 24 januari publiceert Citrix de laatste patches, die een oplossing bieden voor de kwetsbaarheden in de Citrixsystemen. Het NCSC geeft in deze cruciale week van 17 tot en met 24 januari bij haar doelgroepen aan dat het onduidelijk is of de tussentijdse mitigerende maatregelen van Citrix 100% effectief zijn om misbruik van de kwetsbaarheden te voorkomen. Het NCSC wijst erop dat het belang van de continuïteit van de primaire processen van organisaties moet worden afgewogen tegen eventuele negatieve gevolgen. Dit advies stelt organisaties voor de taak om deze risicoafweging te maken.

Fout in de webserver

Maar wat zijn deze eventuele negatieve gevolgen? Om daar inzicht in te krijgen is het nodig eerst de werking van de Citrixsoftware en de kwetsbaarheid die zich openbaarde, wat meer in detail te beschrijven. De toepassingen Citrix ADC en Citrix Gateway maken het mogelijk om op afstand op een organisatienetwerk te werken. De bedoeling is dat de gebruiker via Citrix een veilige toegang tot het organisatienetwerk krijgt.
De kwetsbaarheid, die in december aan het licht kwam, is niet nieuw. In de jaren '90 kwam deze fout al voor. Het gaat om een fout in de webserver. Er waren directories bereikbaar die eigenlijk gesloten zouden moeten zijn. In een van de directories stond programmatuur die het mogelijk maakte om elk gewenst commando af te vuren op de server en daarmee ook het systeem over te nemen. De kwetsbaarheid van Citrixsystemen was eerder publiek bekend dan dat er een patch beschikbaar was. Dat heet een zero day. Maar ook de exploitcode waarmee misbruik kon worden gemaakt van de kwetsbaarheid was beschikbaar, voordat er mitigerende maatregelen of patches bekend waren.
De beschikbaarheid van de exploitcode betekent een aanzienlijk groter risico. Met de exploitcode is het ook zonder al te veel technische achtergrond of kennis simpel om misbruik te maken van de kwetsbaarheid; dit kan al via de volgende drie eenvoudige stappen: je klikt het exploitprogramma aan, je klikt het adres aan van de Citrixserver die je wilt misbruiken en je tikt het commando in dat je wilt uitvoeren. Vervolgens is het mogelijk om binnen te dringen bij een organisatie.

Risicoafweging

Terug naar de situatie in Nederland aan het begin van dit jaar. Op 20 januari publiceert het NCSC een stroomschema dat organisaties kan helpen bij het maken van hun risicoafweging. Als een organisatie tussen 17 december 2019 en 9 januari 2020 de door Citrix geboden mitigerende maatregelen niet heeft getroffen, is de kans zeer groot dat de organisatie is gecompromitteerd. Dit komt met name door de beschikbare exploitcode. Maar ook als een organisatie wel mitigerende maatregelen heeft getroffen, is het nog mogelijk dat kwaadwillenden die beschikking hebben over geavanceerde middelen, misbruik hebben gemaakt van deze kwetsbaarheid. Met alle risico's van dien. Het NCSC adviseert deze organisaties om eerst een herstelplan op te stellen waarmee het mogelijk is te achterhalen of, en op welke wijze de systemen zijn gecompromitteerd en op welke wijze dit te herstellen is. Daarna dienen de patches te worden doorgevoerd.
Ondanks de geschetste risico's zijn er verschillende organisaties die al voor de laatste patch van 24 januari hun Citrixtoepassingen weer zijn gaan gebruiken. Daarbij is door

Het is voor organisaties daarom zaak om de invulling van de DPO-rol goed te overwegen en uit te laten voeren

de betreffende organisaties kennelijk de afweging gemaakt dat het belang van de continuïteit van de primaire processen opweegt tegen het (rest)risico van mogelijke aanvallen. Voor een deel van de organisaties was dit relatief eenvoudig; door de exploitcode goed te bestuderen en vergelijken met het effect van de patch, was op basis van de gebruikte Citrixversie en de informatie van Citrix in te schatten of de workaround effectief was. Met een pentest was dat ook te bevestigen. Voor sommige organisaties was er echter een blijvende onzekerheid, bijvoorbeeld omdat zij hun Citrixomgeving al langere tijd niet van patches hadden voorzien waardoor de gebruikte software te oud was om de workarounds te laten functioneren.

Datalekken in Nederland

Tot op heden zijn er nog geen concrete Nederlandse gevallen openbaar gemaakt waaruit blijkt dat de kwetsbaarheden hebben geleid tot lamlegging van organisaties. Dat betekent echter niet dat er geen organisaties zijn getroffen. Zo heeft de Autoriteit Persoonsgegevens (AP) 29 meldingen van mogelijke datalekken ontvangen, die gerelateerd zijn aan de Citrixkwetsbaarheden (3).

Bekend is dat er wereldwijd tientallen organisaties zijn aangevallen via de kwetsbaarheden in Citrix. Dan gaat het om banken, defensiebedrijven, universiteiten, advocatenkantoren, mediabedrijven, farmaceutische bedrijven en telecombedrijven. Zo opereren er volgens securitybedrijf FireEye aanvallers vanuit China, die zich richten op cyberspionage en aanvallen voor persoonlijke financieel gewin (4). Ook is bekend dat er groepen actief zijn die de kwetsbaarheid als springplank hebben gebruikt om de organisatiesystemen binnen te dringen en ransomware te plaatsen. De ransomware versleutelt bestanden en vraagt vervolgens losgeld voor het ontsleutelen van de data. Wanneer organisaties niet binnen vijf dagen betalen, dreigen de aanvallers alle data te verwijderen en op internet te publiceren (5). Niet zelden bevatten deze data (gevoelige) persoonsgegevens, zoals bijvoorbeeld gezondheidsgegevens.

Rol DPO

Daarom is het van belang dat de Data Protection Officer (DPO) van de organisatie wordt betrokken bij het maken van de eerder genoemde risicoafweging. In de meeste gevallen zal de DPO ook de aangewezen persoon zijn binnen een organisatie om het datalek te melden bij de AP. Om die melding accuraat en zorgvuldig te kunnen doen, en ook te kunnen adviseren over mitigerende maatregelen ten aanzien van risico's voor de betrokkenen van wie de organisatie persoonsgegevens verwerkt, is het belangrijk dat de DPO en de IT-medewerkers goed samenwerken.

In de Algemene Verordening Gegevensbescherming (AVG) is het wettelijke vereiste opgenomen dat de DPO professionele kwaliteiten bezit op het gebied van gegevensbescherming. Dat vereist ook enige kennis van de in de organisatie gebruikte IT-systemen en IT-beveiliging. Wanneer deze kennis ontbreekt, kan de DPO in geval van een kwetsbaarheid zoals recent bij Citrix, mogelijk niet goed beoordelen of er daadwerkelijk persoonsgegevens zijn gelekt, welke maatregelen nu getroffen moeten worden, en of er sprake is van een meldplichtig datalek. Het is voor organisaties daarom zaak om de invulling van de DPO-rol goed te overwegen en uit te laten voeren. Voor de IT-afdeling is het raadzaam om de DPO steeds vroegtijdig te betrekken bij dit soort kwetsbaarheden. Een datalek moet namelijk binnen 72 uur na ontdekking gemeld zijn bij de Autoriteit Persoonsgegevens. Zowel de wijze waarop de melding van een datalek wordt gedaan, als het verzuimen om een datalek op tijd te melden, kan grote gevolgen hebben voor de hoogte van eventuele sancties (bijvoorbeeld boetes). Ook moet in bepaalde gevallen een datalek gemeld worden aan de betrokkenen wier persoonsgegevens het lek betreft. Deze meldingsplichten kunnen grote financiële en reputationele gevolgen hebben. Een goede afstemming is dus cruciaal.

Referenties

(1) https://www.ncsc.nl/actueel/nieuws/2020/januari/13/vele-nederlandse-citrix-servers-kwetsbaar-voor-aanvallen.

(2) https://www.nu.nl/binnenland/6024912/verkeer-moet-rekening-houden-met-mist-gladheid-en-citrix-files.html.

(3) https://www.nrc.nl/nieuws/2020/01/22/29-mogelijke-datalekken-gemeld-na-hackpoging-citrix-software-a3987714.

(4) https://www.security.nl/posting/649418/FireEye%3A+cyberspionage+via+lekken+in+Cisco%2C+Citrix+en+Zoho.

(5) https://www.security.nl/posting/641101/Ransomware-aanval+combineert+Citrix-+en+EternalBlue-exploit.

COLUMN Berry

Van het woord privacy krijg ik pukkeltjes

Zoals mijn trouwe lezers weten ben ik van de oude stempel. Een van de eerste gebruikers van internet en de man die nog weet hoe je met een analoog lijntje in moet bellen bij je provider. Vrijheid blijheid. Als je zelf niet aan de gegevens kon komen om je werk een beetje te kunnen doen dan vroeg je dat aan je buurman, die zocht het dan wel even op. Was de buurman een dagje vrij? Geen probleem, het wachtwoord kon je wel vinden onder zijn toetsenbord. Of je pakte het lijstje van de afdeling waar alle userids en wachtwoorden op stonden.

Tegenwoordig ondenkbaar, want je moet je vaak niet alleen inloggen met een wachtwoord maar ook met een code op je telefoon. Ik heb eens bij een bedrijf gewerkt waar ik mijn pasje in een apparaat moest schuiven om te kunnen werken. Wilde je naar de wc of naar de kantine? Pasje mee, anders kon je het toilet niet in, je koffie niet halen of je broodje gezond afrekenen. Dan gaat de lol er toch snel af. Ik heb mij laten vertellen dat dit allemaal te maken had met de waarborging van de privacy van onze klanten.

Alleen van het woord privacy krijg ik al pukkeltjes. De herhaalmedicatie van mijn vrouw mag ik niet doorgeven, dat moet mijn vrouw doen. Ik mag niet samen met mijn vrouw naar de huisarts; we moeten eerst plechtig zweren dat we dat allebei willen. Op zich is het allemaal ook wel terecht en ben ik er blij mee dat we daar strenger op zijn geworden.

Toch is het vreemd dat de overheid dingen mag die wij niet mogen. Waarom mag iedere politieagent nazoeken of de auto waarin ik rijd van mij is zonder enige verdenking? Waarom krijg ik geen melding als mijn telefoontjes worden afgeluisterd zonder dat daar een reden voor is? Waarom behoort mijn telefoongesprek tot een van de 2500 afgeluisterde gesprekken per dag? Waarom mag de belastingdienst straffeloos etnisch profileren? Waarom doet de overheid dat? Omdat overheidsorganisaties en vele anderen lak hebben aan privacy en gewoon misbruik maken van hun kennis - of vermeende - kennis. En ondanks het feit dat dit aantoonbaar is, wordt er niet ingegrepen door de overheid. Zelfs de Tweede Kamer laat de etnisch geprofileerde slachtoffers van de kinderopvangtoeslag eindeloos in onzekerheid bungelen. Etnisch profileren is een van de grofste overtredingen van de privacywetgeving, en toch wordt dit openlijk toegestaan.

Berry

Auteur: Beaubine Adriaansen is consultant Governance, risk & compliance bij Strict. Zij is bereikbaar via b.adriaansen@strict.nl De scriptie is te lezen op: http://www.ubvu.vu.nl/pub/fulltext/scripties/14_2626160_0.pdf

SCRIPTIE

De privacy van rechters en advocaten in de wereld van Legal Tech

Of hebben zij dit recht hier niet?

De afgelopen jaren maken nieuwe technologieën een opmars en dit gaat niet voorbij aan de juridische sector. Het begrip Legal Tech verwijst naar al deze technologie die het werk van de juridische dienstverlener raakt en de innovatieve toepassingen die daardoor ontwikkeld worden. De digitalisering die plaatsvond binnen de juridische sector maakt het mogelijk om steeds meer data te verzamelen, te verwerken en te bewaren. Zo is een groot deel van alle rechterlijke uitspraken in Nederland elektronisch beschikbaar gemaakt via www.rechtspraak.nl. De beschikbaarheid van deze grote hoeveelheid data biedt de mogelijkheid om deze data te analyseren via Artificial Intelligence. Er zijn inmiddels Legal Tech bedrijven op de markt die hier creatief mee aan de slag zijn gegaan en het mogelijk maken om meer inzicht te krijgen in dat wat gepubliceerd is in rechterlijke uitspraken. Door machine learning leert software zichzelf patronen te herkennen in juridische data en daarmee wordt het mogelijk om als het ware 'juridisch te Googlen' op naam van een advocaat of rechter. Zo kun je op detailniveau inzicht krijgen in de prestaties van advocaten en rechters op basis van specialisaties, win- en verlies ratio's, procesduur en proceskosten bij vergelijkbare zaken. Er kan op die manier van iedere professional een profiel worden getoond met het aantal gewonnen zaken per advocaat, hoeveel eisen de advocaat aanvoert en hoeveel er daarvan door de rechter worden toegewezen. Oordeelt deze rechter anders bij werkgevers of bij werknemers? Is de billijke vergoeding bij bepaalde omstandigheden hoger dan normaal? Heeft de betreffende advocaat vaker een zaak gewonnen die vergelijkbaar is met die van mij? Door de werkwijze van rechters en advocaten in vergelijkbare zaken te analyseren, kan er kortgezegd vooraf-gaand aan een proces een betere inschatting worden gemaakt over de procesaanpak en over de kansen die een partij heeft in een gerechtelijke procedure.

Op het eerste gezicht lijken toepassingen als deze van toegevoegde waarde voor rechtspraktijk. En wie ben ik om dat te ontkrachten? De Raad voor de rechtspraak geeft ook zelf aan dat digitalisering nodig is om het werk van rechters en advocaten gemakkelijker en sneller te maken. Maar waar we bij dit soort nieuwe toepassingen kritisch naar moeten blijven kijken, is wat het effect is op de privacy van de rechters en advocaten zelf. En daarbij ga ik in het bijzonder in op de mogelijkheid om via Artificial Intelligence op detailniveau meer inzicht te krijgen in de manier waarop zij hun beroep uitoefenen.

Rechterlijke uitspraken als open data

In de Nederlandse Grondwet is openbaarheid van de rechtspraak een fundamenteel recht. De gedachte achter deze openbaarheid is het volk een transparant rechtssysteem te bieden, waarin publieke controle en daarmee vertrouwen in het recht mogelijk worden gemaakt. Rechterlijke uitspraken worden daarom online gepubliceerd en zijn voor het publiek toegankelijk op www.rechtspraak.nl. Deze uitspraken worden bestempeld als 'open data' van de Nederlandse overheid. Deze data heeft als eigenschap dat deze voor iedereen gratis toegankelijk én herbruikbaar is. De Wet hergebruik overheidsinformatie vormt de wettelijke grondslag voor het hergebruik van deze data. Met de mogelijkheid tot hergebruik van overheidsinformatie wordt gestimuleerd dat zowel commerciële als niet-commerciële partijen deze data gaan gebruiken voor innovatieve en creatieve toepassingen. Neem bijvoorbeeld Buienradar, dat is ontwikkeld met het onder andere open data afkomstig van het KNMI. Terugkomend op de ontwikkeling van

Beaubine Adriaansen is in augustus 2018 als juriste afgestudeerd aan de Vrije Universiteit van Amsterdam. Daar volgde zij na haar bachelor Nederlands recht en ICT-recht aan de Rijksuniversiteit Groningen, de master Internet, Intellectueel eigendom & ICT-recht. Door haar grote interesse in privacy bij de ontwikkeling van nieuwe technologieën, besloot zij haar scriptie te schrijven over 'De privacyrechtelijke aspecten van de analyse van publiek toegankelijke rechterlijke uitspraken via Artificial Intelligence'. In dit artikel gaat zij dieper in op de inzichten die deze onderzoeksvraag haar bracht.

Legal Tech, biedt het gebruik van open data uit de rechtspraktijk dus ook mogelijkheden voor de juridische sector.

Persoonsgegevens juridische professionals openbaar

Maar als deze grote bulk aan data ook persoonsgegevens bevat, mogen die dan ook zomaar hergebruikt worden voor ieder ander doel? Vanuit het oogpunt van de privacy zag ik reden om daar dieper in te duiken. De hoofdregel uit de Wet openbaarheid van bestuur, in samenhang met de Algemene Verordening Gegevensbescherming (hierna: AVG), is dat persoonsgegevens in Open data niet voor hergebruik in aanmerking komen. Die hoofdregel neemt bij de publicatie van rechterlijke uitspraken een iets andere vorm aan, hetgeen is af te leiden uit de Anonimiseringsrichtlijn van de Raad voor de Rechtspraak. In deze richtlijn is het algemene uitgangspunt dat alle gegevens van een natuurlijke personen die niet ambts- of beroepshalve bij een rechtszaak betrokken zijn geanonimiseerd worden. Dit ter bescherming van de persoonlijke levenssfeer van betrokkenen. Zo zal er geen naam of adres van een natuurlijk persoon zichtbaar zijn in de publicatie van een rechterlijke uitspraak. Er wordt echter een uitzondering gemaakt op de publicatie van persoonsgegevens van juridische professionals. Diens namen worden gewoon gepubliceerd en zijn dus raadpleegbaar voor het publiek als open data. Die uitzondering heeft als gevolg dat die gegevens wél herbruikbaar zijn en verwerking daarvan dus in lijn dient te zijn met de AVG. De reden dat de namen van rechters en advocaten worden gepubliceerd, is kortgezegd het feit dat zij in de uitoefening van hun functie een maatschappelijke, onafhankelijke rol vervullen en dat daar een bepaalde vorm van openbaarheid bij hoort. Het kan worden gezien als een onderdeel van de openbaarheid van de rechtspraak. Deze openbaarheid heeft mede als gevolg dat de professionals zich in beperkte mate kunnen verzetten tegen de openbaarmaking van diens namen en het hergebruik daarvan.

Privacyrechtelijke hobbels op de weg

Nu maken nieuwe technologieën het hergebruik van die persoonsgegevens, afkomstig uit rechterlijke uitspraken, op allerlei manieren mogelijk. Daarbij mogen we niet voorbij gaan aan de vraag wat het gebruik van die gegevens in innovatieve toepassingen voor effect kan hebben op de privacy van rechters en advocaten. Maakt dit niet een te vergaande inbreuk op hun privacy? Het gebruik van Artificial Intelligence maakt het nu al mogelijk een profiel om een persoon heen te creëren. Er wordt immers méér informatie uit bestaande informatie gehaald. Dit kan een patroon in de werkwijze van een rechter of advocaat laten zien. Komt dit misschien in de buurt van profiling? Is wel voldoende transparant hoe deze algoritmes werken en mogen we hier blind op vertrouwen? Zou dit het beroep van rechter misschien minder aantrekkelijk maken? Zijn of haar hele werkwijze kan immers in detail op een presenteerblaadje aan de andere partij worden voorgeschoteld. Of hoort dit nou eenmaal bij die publieke functie? Dit zijn vragen die in mijn onderzoek voorbij kwamen en stof tot nadenken geven. Het is hoe dan ook duidelijk geworden dat we kritisch moeten blijven wanneer het aankomt op het hergebruik van persoonsgegevens van rechters en advocaten binnen de wereld van Legal Tech. Enerzijds kan de analyse van deze juridische data van grote toegevoegde waarde zijn voor de juridische sector. Anderzijds moeten we ons blijven afvragen of we op een verantwoorde manier met al deze gegevens omgaan. De ontwikkeling van Legal Tech zal hoe dan ook zorgen voor een verandering in het werk van rechters en advocaten en het is een onontkoombaar feit dat er in deze ontwikkeling zeker nog wat privacyrechtelijke hobbels op de weg zitten.

Auteur: Chris de Vries is redacteur van iB-Magazine. Chris is bereikbaar via impuls@euronet.nl.

Cyberveiligheid, de overheid en Schiphol - een signalering

Vers van de pers: het Rekenkamerrapport met de titel: 'Digitalisering aan de grens' (1).

Hoe je er ook instaat, als het gaat om al of niet vrije toegang tot Europa en dus tot Nederland. En wat je er ook van vindt dat de wereld nu zucht en kreunt onder een pandemie en het reizen aan banden is gelegd: grenzen zijn een feit en digitalisering een gemak.

Het zal dus wel zo zijn dat de overheid er alles aan doet om onze grenzen veilig te houden en dat digitalisering daarvan het Walhalla is. Althans, dat vertelt de overheid ons regelmatig. Zo ook met de apps die ons in de gaten moeten houden inzake coronarisico's en die absoluut privacyveilig zouden zijn, zodra de overheid ons die voorschotelt, al of niet verplicht.
Tja, en dan de Rekenkamer met haar harde conclusie: 'Maatregelen voor beveiliging IT-systemen grenstoezicht nauwelijks genomen.' Van de paspoortbalie, de selfservice tot de pre-assessment worden er drie maatregelen (goedkeuring voor gebruik en uitvoering beveiligingtesten en aangesloten op detectiecapaciteit) geïnventariseerd; in totaal negen metingen dus.

Resultaat:
- 7 maatregelen niet uitgevoerd,
- 1 gedeeltelijk en
- 1 wel uitgevoerd.

Eigenaren van de systemen zijn het Ministerie van Defensie en het Ministerie van Justitie & Veiligheid.
In ons komend nummer (iB-magazine nummer 4) kom ik er uitgebreider op terug.

Referenties

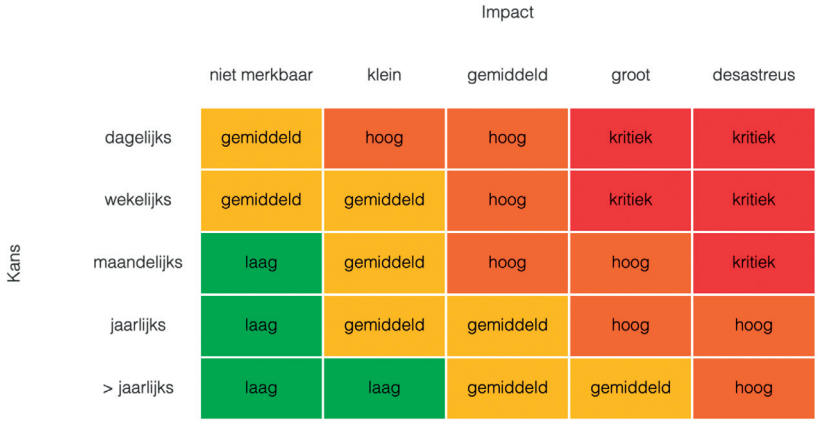
(1) Bron:
https://www.rekenkamer.nl/publicaties/rapporten/2020/04/20/digitalisering-aan-de-grens

Auteurs: Frans Dondorp en Hugo Leisink. Beiden zijn werkzaam in de informatiebeveiliging, maar schrijven dit artikel op persoonlijke titel. Ze zijn bereikbaar via info@privacy-friendly.nl.

Risico-inschatting tijdens de DPIA

Naar ons idee worden de methoden voor risicoanalyses voor informatiebeveiliging en die voor DPIA's te veel door elkaar gehaald. Wat niet bijdraagt aan een goede bescherming van persoonsgegevens.

Risicoanalyse is binnen informatiebeveiliging een bekend begrip. In een risicoanalyse worden risico's in kaart gebracht, waarbij een inschatting wordt gemaakt van de kans dat een risico leidt tot een incident en een inschatting van de impact van zo'n incident. Deze ingeschatte kans en impact worden doorgaans tegen elkaar uitgezet in een risicomatrix (zie figuur 1). Van elk risico kan volgens een eigen waardering bepaald worden of deze acceptabel is of niet en wat de benodigde maatregelen zijn.



Figuur 1 – Risicomatrix.

Risico's binnen de perken

De AVG beschrijft ook een risicogebaseerde aanpak. De kern daarvan staat in overwegingen 76 en 75, waar het ook gaat over risico, met als assen waarschijnlijkheid (kans) en ernst (impact) . Deze risicoafweging is vervolgens weer een element in de DPIA uit artikel 35. De AVG verwacht van de verantwoordelijke een objectieve bepaling van het risico (overweging 76) en verwacht vervolgens passende en effectieve maatregelen (overweging 74) om die risico's binnen de perken te houden.
Dat klinkt bekend en het lijkt dus aantrekkelijk om die AVG-risicoanalyse op dezelfde manier te doen, of zelfs te combineren, met die voor informatiebeveiliging. Dat leidt echter niet tot het juiste resultaat. Ten eerste leidt dat tot een DPIA die zich vooral richt op de beveiliging van persoonsgegevens, ofwel het voorkomen van datalekken. Gegevensbescherming is natuurlijk veel meer dan dat. Ten tweede, en dat is waar dit artikel hoofdzakelijk over gaat, blijkt dat de risicomatrix voor gegevensbescherming eigenlijk helemaal niet in te vullen is. Hierdoor kan getwijfeld worden aan de waarde van de uitkomst. Er zijn namelijk de nodige verschillen tussen de vakgebieden informatiebeveiliging en gegevensbescherming. We benoemen nu alleen de voor dit artikel relevante verschillen.

Informatiebeveiliging versus gegevensbescherming

Het eerste verschil is wie de benadeelde is. In informatiebeveiliging richt de risicoanalyse zich op incidenten binnen de eigen organisatie. Informatiebeveiliging doet u immers voor uzelf, om schade voor uw eigen organisatie te voorkomen. Bij gegevensbescherming gaat het (artikel 35 lid 1) om het risico 'voor de rechten en vrijheden van natuurlijke personen'. Dat doet u dus vooral voor de betrokkene. Dit is dus een andere benadeelde, want iemand anders draagt de feitelijke schade (afgezien van reputatieschade en boetes).
Het tweede verschil is wanneer er sprake is van een inbreuk. Binnen de informatiebeveiliging gaat het om het maken van een inschatting van mogelijke incidenten in de toekomst. Bij gegevensbescherming gaat het om het beoordelen van de mate waarin de rechten en de vrijheden van de betrokkene wordt gerespecteerd. Daar is geen inschatting van iets in de

toekomst voor nodig. Dat is simpelweg het beoordelen van de huidige of geplande processen en maatregelen die daarvoor moeten zorgen. Die processen en maatregelen heeft u op orde of niet. Daar komt geen 'kans' aan te pas. Ook de impact werkt anders in de DPIA. Bij informatiebeveiliging bepaalt de organisatie wat 'erg' is en daarmee wat acceptabel is. Bij de rechten en vrijheden in de DPIA kunt u ook die as niet kwantificeren, want hoe erg is het als u discrimineert? Ook al doet u dat maar een beetje? Waar een inbreuk bij informatiebeveiliging een incident is, is dat bij gegevensbescherming dus het niet respecteren van iemands privacy of de bijbehorende wetgeving (AVG). Het derde verschil is de acceptatie. Vanuit de informatiebeveiliging zijn we gewend om te denken in gradaties, van klein naar groot, met ergens op de assen een acceptabel niveau. De organisatie is meer of minder risico-avers en kan een afweging maken tussen de kosten van de te verwachten schade en de kosten van de maatregelen. Voor gegevensbescherming kunt u die acceptatie niet bepalen. Ten eerste omdat u niet degene bent die de schade draagt. Ten tweede omdat u onvoldoende kennis hebt van de leefsituatie van degene voor wie de schade is, waardoor u niet kan bepalen wat de impact daarop is. Ten derde omdat een bedreiging van rechten en vrijheden van anderen eigenlijk altijd onacceptabel is.

Zou u toch een risicomatrix hanteren, dan is de daarbij horende waardering heel simpel. Alleen de risico's die bijna nooit plaatsvinden en amper impact hebben zou u kunnen accepteren. De conclusie die u daar naar ons idee uit kan trekken, is dat de risicomatrix voor gegevensbescherming niet zinvol is. De aanpak voor informatiebeveiliging is dus niet efficiënt voor gegevensbescherming.

Kans \ Impact	niet merkbaar	klein	gemiddeld	groot	desastreus
dagelijks	gemiddeld	hoog	hoog	kritiek	kritiek
wekelijks	gemiddeld	gemiddeld	hoog	kritiek	kritiek
maandelijks	laag	gemiddeld	hoog	hoog	kritiek
jaarlijks	laag	gemiddeld	gemiddeld	hoog	hoog
> jaarlijks	laag	laag	gemiddeld	gemiddeld	hoog

Figuur 2 – Risicomatrix.

Welk model voor welke inschatting?

Een goede omgang met de risico's voor persoonsgegevens vraagt dus om een andere aanpak. Het maken van een inschatting van de kans op een datalek en de impact daarvan op de organisatie doet u tijdens een risicoanalyse voor informatiebeveiliging. Beoordelen of u met de huidige mate van informatiebeveiliging, waarbij u uitgaat van een hoge impact voor een betrokkene, de rechten en de vrijheden voor de betrokkenen in voldoende mate respecteert, doet u tijdens de DPIA. In bestaande DPIA modellen zien we invullingen die deze aanpak niet volgen. In het Model Gegevensbeschermingseffectbeoordeling Rijksdienst wordt in vraag 16 gevraagd om 'de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen' te beschrijven en te beoordelen. Wij horen dat mensen daarin vastlopen en dat begrijpen wij volkomen, gezien de hierboven geschetste drie verschillen.

In het DPIA model van Commission nationale de l'informatique et des libertés (de Franse toezichthouder) wordt gevraagd om een inschatting te maken van de kans en impact van een aantal inbreuken op de privacy, namelijk oneigenlijke toegang tot persoonsgegevens, onbedoelde aanpassing van persoonsgegevens en verlies van persoonsgegevens. Daar zien wij dus een incident-gedreven risicoanalyse die eigenlijk gericht is op informatiebeveiliging. U kunt deze analyse natuurlijk apart doen voor persoonsgegevens. Echter, omdat beveiliging bijna nooit specifiek en apart voor persoonsgegevens is ingericht, maar meestal voor bedrijfsinformatie in het algemeen, is dat niet echt efficiënt. Zoals eerder aangegeven is de impact van deze incidenten voor een ander niet goed te bepalen en al helemaal niet zonder zicht op de persoonlijke levenssfeer van die ander.

Eigen DPIA-model

Om een antwoord te bieden op deze tekortkomingen, zijn wij enige tijd terug zelf begonnen met het ontwikkelen van een eigen DPIA-model. Met alle reacties daarop, aangevuld met onze eigen evaluaties, zijn we inmiddels op versie drie aangekomen. Het is een DPIA-model waarin alle facetten van gegevensbescherming aan bod komen, waarin het voorkomen van datalekken dus niet de boventoon voert en waarin de rechten en vrijheden van de betrokkenen centraal staan. Onze gratis en open DPIA-model is te vinden op www.privacy-friendly.nl, waarbij wij onze uiterste best hebben gedaan om ook de uitvoering van de DPIA zelf zo veilig en privacyvriendelijk mogelijk te houden.

Auteur: Frans Kersten RE RA is Staffunctionaris Informatiebeveiliging en Functionaris Gegevensbescherming bij het Admiraal De Ruyter Ziekenhuis. Hij is bereikbaar via kersten210@msn.com. Dit artikel is geschreven op persoonlijke titel.

Privacy in het ziekenhuis is meer dan alleen AVG

In ziekenhuizen speelt er meer dan alleen de AVG wanneer het gaat over privacy. Als informatiebeveiliger in de zorg is kennis van AVG en andere wet- en regelgeving noodzakelijk bij het werken aan passende beveiligingsmaatregelen. De naleving van deze wetten kan in het uiterste geval zelfs bepalen of een mensenleven wel of niet gered wordt.

Dit artikel geeft eerst een overzicht van relevante de wet- en regelgeving. Ik bespreek een aantal punten waarop verschillende regels elkaar soms aanvullen en soms tegenwerken. Hopelijk is na lezing duidelijk waarom deze relevant zijn voor een informatiebeveiliger in de zorg. Voor de leesbaarheid van dit artikel zijn details en nuances uit de wetten weggelaten. Bij voorkomende dilemma's over welke wet van toepassing is, is het aan te raden een jurist te raadplegen.

Naast de AVG en bijbehorende Uitvoeringswet kennen we nog andere wetten:

- De Wet op de geneeskundige behandelovereenkomst (Wgbo);
- De Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvp) en bijbehorende besluiten;
- Besluit elektronische gegevensverwerking door zorgaanbieders.

De AVG

De hoofdlijnen van de AVG zijn bij de meeste informatiebeveiligers wel bekend. De AVG classificeert gegevens betreffende de gezondheid (medische gegevens) tot bijzondere gegevens. Deze gegevens mogen niet zonder meer verwerkt worden. Daarom is in de Uitvoeringswet AVG (UAVG) vastgelegd dat en onder welke voorwaarden medische gegevens verwerkt mogen worden. De UAVG bevat ook bepalingen over gebruik van medische gegevens in het kader van de bedrijfsvoering van zorginstellingen en voor wetenschappelijk onderzoek en statistiek.

De Wgbo

De Wgbo is een onderdeel van het Burgerlijk Wetboek, Boek 7, Titel 7 afdeling 5, Overeenkomsten. Het richt zich op de geneeskundige zorg (behandeling, genezing). De Wgbo regelt samen met de Wet BIG het medisch beroepsgeheim. De Wgbo verplicht de hulpverlener om een medisch dossier aan te leggen dat alleen toegankelijk is voor degenen die betrokken zijn bij de behandeling (een behandelrelatie hebben).

De patiënt heeft rechten, waaronder:

- recht op informatie of om geen informatie te willen delen;
- toestemmingsvereiste voor een medische behandeling;
- recht om het medisch dossier in te zien en recht op een kopie daarvan (art. 456) mits de persoonlijke levenssfeer van een ander niet geschaad wordt;
- recht op herstel van fouten;
- recht om een eigen verklaring aan het medisch dossier toe te laten voegen (art. 454);
- recht om (een deel van) het medisch dossier te laten vernietigen (art. 455).

De patiënt heeft ook plichten. Zo moet hij alle informatie verstrekken die van belang is voor de behandeling én de zorgverlener voor de behandeling betalen.

Medisch beroepsgeheim

De hulpverlener heeft een medisch beroepsgeheim. Er zijn situaties waarin de hulpverlener ondanks toestemming van de patiënt kan besluiten om gegevens toch niet te verstrekken. Er zijn ook situaties waarin de hulpverlener kan besluiten om zijn beroepsgeheim te doorbreken en toch informatie te verstrekken (art. 449) als dat in het belang is van de patiënt of anderen. De Wgbo regelt ook wanneer nabestaanden het dossier van een overledene mogen inzien.

De Wgbo bevat bepalingen inzake wetenschappelijk onderzoek en statistiek (art. 458). Onderzoek is toegestaan mits het een algemeen belang dient, zonder de desbetreffende gegevens niet kan worden uitgevoerd en voor zover de patiënt niet uitdrukkelijk bezwaar heeft gemaakt. Hieronder vallen ook de zogenaamde trials voor onderzoek samen met leveranciers naar nieuwe medicijnen, stagiairs en anderen in opleiding.

De hulpverlener mag de gegevens uit patiëntdossiers in beperkte mate gebruiken voor eigen onderzoek, bijvoorbeeld om de effecten van de eigen behandeling te onderzoeken. In andere gevallen is de meest gewenste oplossing om de patiëntgegevens eerst te anonimiseren en dan pas te gebruiken voor onderzoek. Er worden hoge eisen gesteld aan dit anonimiseren (1). De andere grondslag voor onderzoek is expliciete toestemming.

De Wabvpz

De Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg heeft betrekking op uitwisselingssystemen waarmee gegevens tussen verschillende zorgaanbieders beschikbaar gesteld en opgevraagd kunnen worden. Centraal staat het gebruik van een elektronisch uitwisselingssysteem: een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken. Het interne informatie systeem in een ziekenhuis valt hier niet onder. Vanaf 1 juli 2020 moet de patiënt langs elektronische weg inzage kunnen krijgen in zijn dossier en het gebruik ervan.

Zorgverzekeraars hebben geen toegang tot individuele dossiers van patiënten en ook geen toegang tot elektronische uit-

wisselingssystemen (art 15f lid 1 Wabvpz). Zij hebben wel de bevoegdheid om materiële controles en fraudeonderzoeken uit te voeren. Hiervoor is een protocol opgesteld. In dit protocol staat dat pas in laatste instantie – als andere controlemiddelen aantoonbaar geen soelaas boden – controle van zorgverzekeraars door inzage in patiëntdossiers mogelijk is; echter ook dan alleen als de betrokken patiënt toestemming geeft.

1.4 Besluit elektronische gegevensverwerking door zorgaanbieders

Dit besluit regelt het verplichte gebruik van NEN 7510, NEN 7512 en NEN 7513 in de zorg. NEN 7510 deel 1 is het equivalent van ISO 27001, deel 2 van ISO 27002. NEN 7512 gaat in over gegevensuitwisseling in de zorg. NEN 7513 stelt eisen aan de logging van mutaties op het elektronisch patiëntdossier. Het gaat hierbij om het aantoonbaar voldoen aan de norm (certificering is geen eis, maar maakt het wel gemakkelijker). De Autoriteit Persoonsgegevens en de Inspectie Gezondheidszorg en Jeugd zien hierop toe.

Dilemma's bij het verwerken en delen van gegevens

1.Verstrekken van gegevens

Verstrekken van gegevens uit het patiëntdossier aan derden mag alleen met toestemming van de patiënt. Hierbij worden twee situaties onderkend: de 'impliciete' en de 'expliciete' toestemming. Van impliciete toestemming is bijvoorbeeld sprake wanneer de huisarts met de patiënt bespreekt om hem voor verdere behandeling door te verwijzen naar het ziekenhuis. Als de patiënt instemt, volstaat het om in het dossier vast te leggen dat dit met de patiënt besproken is en de patiënt hiermee instemt. In andere gevallen is meestal sprake van 'expliciete' toestemming, bijvoorbeeld aan de apotheek om gegevens over medicatie te delen met de behandelaar in het ziekenhuis. Hierop zijn de eisen van de AVG van toepassing.

De AVG definieert toestemming van de betrokkene als elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt. In de EU Richtlijnen is vastgelegd dat dit in het bijzonder geldt in de zorg (2) en (3). Vastgelegd is dat het ontbreken van toestemming niet mag leiden tot het onthouden van essentiële zorg of het aanbieden van zorg die zwaarder belastend is voor de patiënt. Voor wetenschappelijk onderzoek geldt voorts dat de toestemming per onderzoek of zelfs onderzoeksdoel gegeven moet worden.

2. Leven boven privacy

In de zorg kan de vraag ontstaan wat te doen als een patiënt niet in staat is vragen te antwoorden. De medici en ziekenhuizen hebben een zorgplicht. Uiteenlopende ministers hebben aangegeven (zie jurisprudentie) dat niet wettelijk geregeld hoefde te worden dat in dat geval van beschikbare gegevens gebruik gemaakt mag worden om de patiënt te behandelen, ook zonder dat de patiënt toestemming heeft gegeven. De AVG geeft in artikel 6 lid 1 onder e de mogelijkheid indien de verwerking noodzakelijk is om de vitale belangen van de betrokken te beschermen. Artikel 15b lid 3 geeft de mogelijkheid om als gegevens beschikbaar zijn via een elektronisch berichtwisselingsysteem terwijl het vragen van toestemming niet mogelijk is, toch de gegevens te raadplegen voor zover noodzakelijk voor richting de patiënt te verrichten handelingen. Bij de coronapandemie zie je dit terug. De Autoriteit Persoonsgegevens heeft een standpunt (2) ingenomen over de aanlevering van medische gegevens vanuit huisartsen richting huisartsenposten en de spoedeisende hulp van ziekenhuizen voor de eerste beoordeling van coronapatiënten. Als de patiënt toestemming heeft gegeven, mag deze informatie gegeven worden. Geeft de patiënt geen toestemming, dan mogen deze gegevens niet aangeleverd worden: dit kan dus levens kosten! Heeft de patiënt niet eerder toestemming gegeven (positief of negatief) dan mag worden onder voorwaarden worden uitgegaan van veronderstelde toestemming.

Het hiervoor gestelde komt overigens in een ander daglicht te staan als betrokken patiënt een niet-behandelverklaring heeft. Dan zou behandelen van de patiënt in strijd kunnen worden geacht met diens uitdrukkelijke wens. In de praktijk blijkt hier dan een onbedoeld privacy aspect aan vast te zitten. Het ontbreekt aan een systematische (centrale) vastlegging van dergelijke verklaringen. Het is dus zeer goed mogelijk dat als patiënt een verklaring bij zijn huisarts heeft afgegeven, deze niet bekend is in het ziekenhuis. Het beste advies is dan ook om een dergelijke verklaring altijd bij je te dragen.

3. Bekwaamheid en kinderen

Voor een behandeling is toestemming nodig. De Wgbo (art 450-451) behandelt wie bevoegd/handelingsbekwaam is. Voor kinderen tot 12 jaar zijn dit de ouders. Voor kinderen van 12 jaar, de kinderen samen met de ouders. Kinderen vanaf 16 jaar worden geacht zelfstandig bekwaam te zijn. Dit werkt door qua privacy omdat ouders dan geen inzage meer hebben in de dossiers.

Deze leeftijdsgrenzen blijken in de praktijk de nodige aandachtspunten op te leveren. Denk enerzijds aan situaties van gescheiden ouders (wat als de ene wel en de andere geen toestemming wil geven), kindermisbruik of ontzetting uit de ouderlijke macht. Anderzijds ontbreekt het nog aan technische voorzieningen op het gebied van machtigen (zie proef met

DigID machtigingen). Dit maakt het lastiger om kinderen elektronisch inzage te geven in hun gegevens en hun gegevens elektronisch uit te wisselen.

4. Wgbo versus AVG

De Wgbo heeft als specifieke wetgeving op een bepaald gebied (juridische term: lex specialis) in voorkomend geval voorrang op de AVG - een meer algemene wetgeving (lex generalis) -.

Een voorbeeld is het recht op vernietiging van het patiëntdossier. De AVG geeft de betrokkene het recht om te vragen om vernietiging van zijn persoonsgegevens (i.c zijn medisch dossier). De Wgbo (art. 455 lid 2) bepaalt dat hiervan kan worden afgeweken als bewaring van belang is voor een ander dan de patiënt. Dit is bijvoorbeeld wanneer vernietiging niet in het belang is van de patiënt zelf met het oog op toekomstige behandelingen of bij het volgen van erfelijke ziekten. De hulpverlener beslist.

5. Gebruik BSN

Artikel 87 van de AVG geeft een grondslag om bij lidstatelijk recht specifieke voorwaarden te stellen aan de verwerking van een nationaal identificatienummer. Artikel 46 van de UAVG regelt dat een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts gebruikt wordt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald. Voor de zorg voorziet de Wabvpz hierin. Gebruik is onder meer voorgeschreven bij facturatie aan zorgverzekeraars en bij doorverwijzingen. Doel is het voorkomen van patiëntverwisseling. De wetgeving is echter complex. Gebruik van een BSN is alleen toegestaan bij zorgverleners die in een in de wet benoemd register voorkomen. Voor de gemiddelde medewerker in de zorg is dat niet uit te leggen dat ze vrijwel altijd het BSN moeten gebruiken, maar soms niet, bijvoorbeeld bij verwijzing naar een audicien.

Gestapelde wetgeving

Het voorgaand heeft als het goed is duidelijk gemaakt dat diverse onderwerpen in verschillende wetten aan de orde komen. Inzage van patiënten in hun dossier komt bijvoorbeeld voor in zowel de AVG, de Wgbo als de Wabvpz. Hierbij worden dan verschillende termen gebruikt. Soms zijn er nuances die het verschil maken. Dat maakt het zeer lastig voor hen die in de zorg werken. Zo is er geen formele definitie van wat er onder 'patiëntdossier' valt. Het Ministerie heeft op haar website beschreven wat wel en niet tot het medisch dossier gerekend wordt. 'Persoonlijke aantekeningen van de arts' vallen daar bijvoorbeeld niet onder. Een vriendelijk voorbeeld van zo'n aantekening: het is nauwelijks mogelijk rechtstreeks met patiënt te praten, partner komt altijd mee en doet steeds het woord. In het verleden was het gebruikelijk om deze in het EPD bij de patiënt zelf vast te leggen. Met de mogelijkheden tot digitale inzage en opvragen van kopieën was het dus voor veel artsen een leermoment om deze gegevens toch op een apart plekje vast te leggen. Het ZIS/EPD voorziet hier in. De gestapelde wetgeving kan zorgen voor verrassende zaken. Op grond van de Wgbo hoeven de persoonlijke aantekening niet verstrekt te worden. Als ze verwerkt worden met het ZIS/EPD is echter sprake van een verwerking van persoonsgegevens die ook onder de AVG valt. Is het dan mogelijk om met een beroep op de AVG toch inzage te krijgen in die persoonlijke aantekeningen? De rechter zal dan uitspraak moeten doen.

De toekomst

Het Ministerie van VWS heeft een duidelijke agenda waarbij de patiënt meer regie moet krijgen over zijn gegevens én gegevens eenvoudiger gedeeld moeten kunnen worden tussen zorgverleners. Dit moet er voor zorgen dat medische gegevens (m.n. medicatie) op ieder moment en voor iedere zorgverlener beschikbaar zijn. Hierover is momenteel een internetconsultatie gaande. Omdat niet iedere zorgverlening onder de Wgbo valt, kan dit volgens sommigen het begin van het einde van het medisch beroepsgeheim betekenen. Daarnaast is nog onduidelijk wat de coronapandemie voor effect zal hebben. Op het moment van afronden van dit artikel wordt gesproken over apps waarmee gevolgd kan worden of iemand in contact is geweest met iemand die corona bleek te hebben. Vanuit diverse kanten (Bits for Freedom) is direct aandacht gevraagd voor privacy. De EDPB heeft ook aangekondigd dat er Europese regels moeten komen voor dit soort apps. De angst is dat dit geen tijdelijke oplossing zal zijn, maar een volgende stap in de ontwikkeling dat de overheid steeds meer grip krijgt op haar burgers.

Referenties

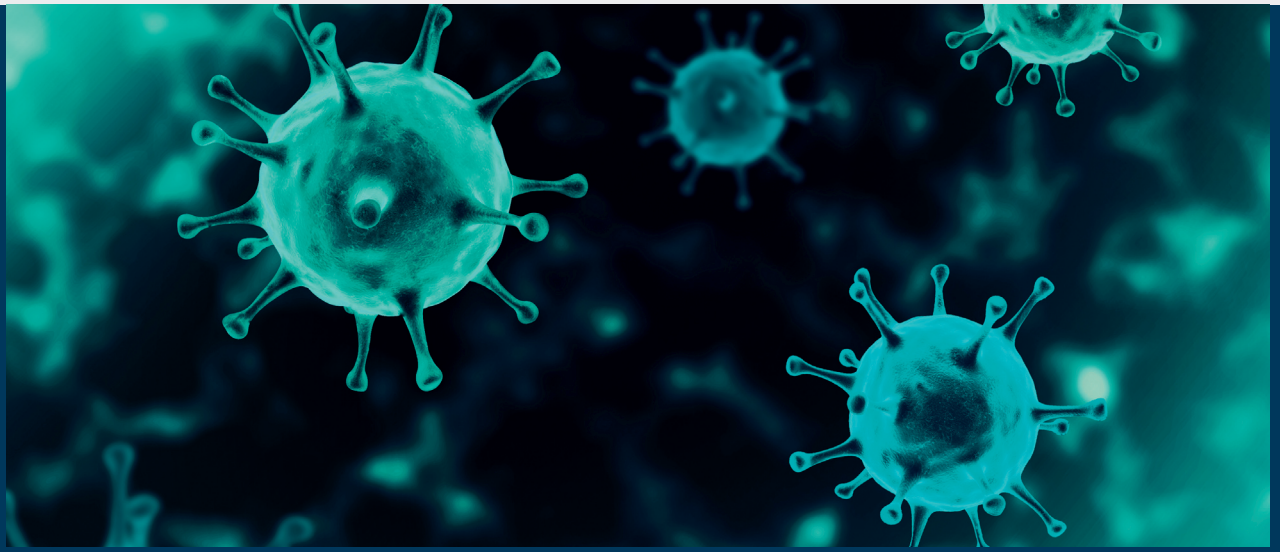
(1) Opinion 05/2014 on Anonymisation Techniques, WP216

(2) Opinion 15/2011 on the definition of consent, WP 187

(3) Working Document on the processing of personal data relating to health in electronic health records (EHR), WP131

(4) https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/-files/brief_medisch_dossier_corona.pdf

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



COVID-19, veiligheid en misdadigers

Er kan geen ramp in de wereld plaatsvinden of er zijn mensen die eraan willen verdienen door oplichting van slachtoffers en angstige mensen. Niets is minderwaardiger dan dat.

Nu maakt de pandemie slachtoffers op het net. Weliswaar niet door bacteriën, maar door niet minder dodelijke software-packets verborgen in phishing-mails, op malicieuze websites en door social engineering geïnstalleerd gekregen. Doelwit o.a. de telewerkinfrastructuur, de in de haast gerealiseerde VPN's en natuurlijk populaire communicatie platforms als Zoom en MS Teams. En ook nu weer waarschuwen de autoriteiten: de Nederlandse politie (1) en de samenwerking tussen de V.S. (DHS/CISA) en het V.K. (NCSC) (2).

Dat roept de vraag op: zijn gebruikers zo dom of zijn ontwikkelaars ongeïnteresseerd in het ontwikkelen van veiliger software? Want dom zijn die toch niet? In een artikel (3) van ICT-jurist Arnoud Engelfriet slaat hij de deur dicht voor het Amerikaanse denken: niet nadenken over privacy en grondrechten, maar iets voortbouwen en zeggen dat dit modern en handig is. Met in het achterhoofd de gedachte: als het maar commercieel handig is. Zijn conclusie: misschien alleen nog maar Europese videovergadersoftware gebruiken. Moeten wij allen niet eens terugkeren naar het oude adagium: 'Koop en gebruik Europees!'

Zelf kiezen - Fook Hwa Tan

We werken inmiddels alweer weken thuis, in de nabijheid van on ons gezin. Soms misschien iets te nabij. Nu we alleen nog online werken, zoeken we naar nieuwe mogelijkheden om samen te werken. Dit creëert naast nieuwe mogelijkheden vaak ook weer nieuwe kwetsbaarheden. Wat moet je nu kiezen? Europees, Chinees, Amerikaans, Russisch of zelf bouwen? Wat is het risico?

Fook Hwa Tan | Chris de Vries | Lilian Knippenberg

Als economie zijn we de laatste jaren steeds meer gaan specialiseren. Dit betekent, dat verschillende landen zich toeleggen op bepaalde specialiteiten. Verder zien we door de drang naar groei steeds meer bedrijven die andere bedrijven overnemen waardoor steeds minder keuze is in de markt. Door minder partijen wordt ook een veel grotere afhankelijkheid gecreëerd. Vooral op digitaal vlak, waarbij diensten bijna direct afgenomen en gebruikt kunnen worden, is door het gemak bijna geen reden meer om de eigen IT-afdeling te raadplegen.

Wat kun je doen? Wat moet je doen? Het is belangrijk in deze tijd iedereen bewust te maken van de gevaren van het gebruik van digitale middelen. De mens is vaak de laatste schakel. Vervolgens is het van belang zelf een inschatting te maken wat acceptabel is qua risico. Waar risico gelopen wordt, kun je ook niet-technische maatregelen implementeren. Al met al is het van belang zelf te weten wat je risicobereidheid is om daarbij een goed afgewogen keuze te maken wat je wel of niet wilt gebruiken. Als laatste is het voor elke organisatie van belang te kunnen monitoren wat er op het netwerk plaatsvindt.

Sleutel tot succes: mensen en samenwerking - Lilian Knippenberg

Mensen zijn vindingrijk, passen zich nog een keer aan nieuwe omstandigheden en zijn op zoek naar manieren om in een nieuwe werkelijkheid zo goed mogelijk door te gaan. In deze tijd kun je als organisatie hopelijk de vruchten plukken van awareness campagnes aan medewerkers uit het verleden en een heldere visie en IT-uitwerking van de (C)ISO/IT-afdeling. Haastige spoed is zelden goed, maar soms helaas noodzakelijk als er in de omgeving dingen gebeuren die we niet konden voorzien. Mensen maken het verschil, gelukkig zijn er een hoop organisaties waar medewerkers zelf vragen om veilige toepassingen en bijvoorbeeld beveiligde verbindingen of applicaties. Ook daar waar medewerkers er niet zelf om vragen, maar de IT-afdeling zelf al veilige toepassingen voor bijvoorbeeld videobellen levert/leverde gaat veilig werken in veel gevallen goed. Maakt het dan echt iets uit in welk land een toepassing gebouwd is?
De (C)ISO weet dat het niet de vraag is of, maar wannéér je aangevallen wordt. Uiteindelijk is samenwerking het sleutelwoord. In deze onzekere tijden is het juist van belang om te bouwen op de samenwerking met je leveranciers (waar deze zich dan ook bevinden), klanten en nieuwe initiatieven zoals https://techtegencorona.nl/. Natuurlijk is het van belang om dan niet naïef te zijn: in de basis is een richtlijn die stelt 'Europe first' wellicht het meest passend voor jouw organisatie. Als deze pandemie weer wat afgezwakt is, kunnen we de voorbereiding op de volgende crisis voor onze organisatie(s) verder optimaliseren en ervoor zorgen dat onze medewerkers hun gedrag aanpassen op de risico's van de organisatie (zowel in gebruik als in levering van toepassingen).

Hoe actueel kunnen wij zijn ….? – Chris de Vries

Op het moment dat wij de laatste hand leggen aan de 'upload' van dit magazine en in afwachting zijn van het bestuursartikel, worden we verrast dat ons 'bestuurslid van dienst' in opperste staat van paraatheid is vanwege de Maze Ransomware'-aanval op de Amerikaanse IT-services gigant: Cognizant. Op internet lezen wij dat Cognizant intern en extern actief stappen onderneemt om dit incident in te perken en dat zij alle gebruikelijke, defensieve maatregelen opgestart heeft. Haar klanten ervaren in ieder geval disruptie in hun werk en leven in vrees met betrekking tot hun vertrouwelijke informatie.
Wij zien dus dat ook de groten der aarde (en dan bedoel ik niet de dinosauriërs) niet vrij zijn voor aanvallen op hun infrastructuur en slachtoffer kunnen zijn van dodelijke software-packets e/o phising-mails e/o social engineering trucs. Hoe moeten wij eenvoudige gebruikers ons dan beschermen?
Ik denk dat 'security- & privacy-by-design' niet enkel iets is voor het papier, als theorie in mooie beleidsstukken, maar nu echt structureel moet worden aangepakt. Commercie mag niet het enige criterium blijven; zeker niet in deze onzekere tijd van pandemieën, virtuele en niet-virtuele virussen. Het is dus aan de tijd dat de 'user' met zijn voeten de richting aangeeft en wel: 'secure design & privacy first!'

Referenties

(1) https://www.politie.nl/nieuws/2020/maart/31/cybercriminelen-spelen-in-op-coronavirus.html
(2) https://www.us-cert.gov/ncas/alerts/aa20-099a
(3) https://blog.iusmentis.com/2020/04/07/misschien-is-nu-het-moment-om-gewoon-alleen-nog-europese-videovergadersoftware-te-gebruiken/

COLOFON

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

PvIB
Platform voor InformatieBeveiliging

HOOFDREDACTEUR
Nicole van Deursen

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

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

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

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
VDR druk & print

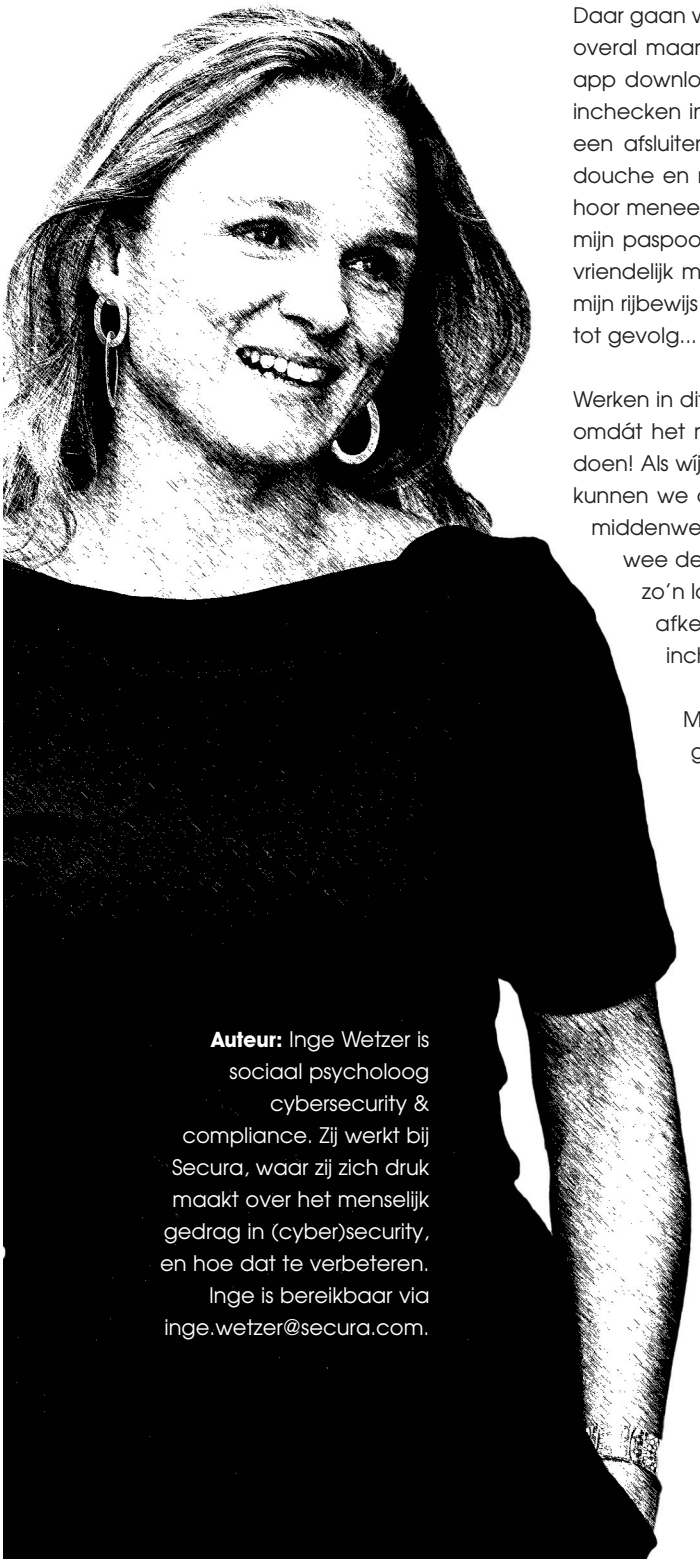
UITGEVER
Platform voor Informatiebeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
E secretariaat@pvib.nl
W www.pvib.nl

ABONNEMENTEN
De abonnementsprijs in 2020 bedraagt € 118,50 (exclusief btw), prijswijzigingen voorbehouden.

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

ISSN 1569-1063

Hotel Geen Idee



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

Daar gaan we weer. Noem het beroepsdeformatie, maar ik heb dus moeite met het overal maar achterlaten van mijn gegevens. Registeren voor een klantenpas, een app downloaden waar ik meteen met een bestaand account op moet inloggen, inchecken in een hotel. Vandaag is het dat laatste. Na een dag hard werken met een afsluitend diner, ben ik blij dat ik in mijn hotel aankom. Ik verlang naar een douche en mijn bed. Of ik de gegevens op mijn reservering even wil checken. Ja hoor meneer, die zijn helemaal in orde. Handtekening, klaar. Oh nee, toch niet. Of ik mijn paspoort of rijbewijs even wil tonen. Braaf vis ik mijn rijbewijs uit mijn tas. Als ik vriendelijk meewerk, gaat het altijd sneller, heb ik gemerkt. Tot de receptionist met mijn rijbewijs naar het kopieerapparaat loopt. Onmiddellijke kortsluiting in mijn hoofd tot gevolg...

Werken in dit vak doet iets met je. Security is namelijk altijd en overal aanwezig. Juist omdát het mijn vak is, probeer ik er niet in door te slaan, maar wel het goede te doen! Als wíj als security professionals het al niet zo nauw nemen met de regels, hoe kunnen we dan ooit de rest van de wereld meekrijgen? Dus probeer ik de gulden middenweg te vinden. Niet te krampachtig, maar wat niet mag, dat mag niet. Dus wee de persoon die de taak heeft mij in te checken bij een hotel. Want ik ben zo'n lastig mens dat haar ID niet afgeeft voor een kopie. Een minachtende en afkeurende blik van de receptionist tot gevolg: "Dan kan ik u niet inchecken."

Moeheid en mijn principes strijden om de aandacht. Maar het is ook gewoon tegen de regels dat hij een kopie maakt! Dus ik probeer nog: "AVG", maar de receptionist houdt voet bij stuk: "Wij maken altijd van elke gast een kopie-ID, mevrouw. Daar doen wij verder niks mee hoor." Aaargh. Waarom dóe je het dan?! Het nummer overschrijven vindt hij onvoldoende. Daar sta ik dan, met de regels aan mijn zijde maar met mijn rug tegen de muur. Ik bedenk de oplossing door de KopieID-app van de overheid in de strijd te gooien. Ik maak voor hem een foto van mijn ID waarin ik alle niet-relevante informatie doorstreep en waarop ik groot markeer dat deze kopie alleen geldig is voor vandaag en voor Hotel Geen Idee. Zuchtend en overduidelijk afkeurend verleent de beste man mij medewerking en overhandigt me – nadat ik tien minuten heb staan prutsen op mijn telefoon – mijn kamersleutel.

In de kamer neem ik eerst een warme douche en dan plof ik op het bed. Pak mijn telefoon en open LinkedIn. Een persoon bekeek uw profiel. Deze persoon is werkzaam bij Hotel Geen Idee. Ik zucht. En lach. Misschien vindt hij me nu zo stom niet meer.

Inge

ALS HET GOED IS, IS HET GOED.

Maar verbetering zit in een klein hoekje.

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/certificering

ONLINE BESCHIKBAAR

WAT IS EEN ISMS?

Wilt u meer weten over het opzetten van een information security management system?

Download de whitepaper via

www.dnvgl.nl/whitepaper