GDPR VEREIST ZOEKEN EN CONTROLEREN

BEDRIJFSPROCESSEN MOETEN ANDERS WORDEN INGERICHT

Het ongebreideld koppelen van databestanden is voorbij

Veel overheden en bedrijven denken dat het met de nieuwe privacywet (GDPR) niet zo'n vaart zal lopen. Maar weten zij waar ze alle data bewaren? En wat ermee gebeurt? Het rondslingeren van data is een groot probleem, zeggen Hans Henseler en Geert-Jan van Bussel. Bedrijven en overheden hebben hun information governance en informatiewaardeketen niet onder controle.

door Hans Henseler en Geert-Jan van Bussel beeld Shutterstock

DE GDPR (GLOBAL DATA PROTECTION REGULATION) KOMT ERAAN. Volgens de nationale privacybenchmark van 30 november 2017 is 80 procent van de Nederlandse bedrijven en overheden nog niet klaar voor de nieuwe privacywet; 60 procent van de bedrijven en overheden weet zelfs niet waar de gegevens van burgers of klanten zijn opgeslagen.

Overheden en bedrijven lopen achter, maar willen daar niet openlijk over praten. Veel overheden denken, vreemd genoeg, nog steeds dat het zo'n vaart niet zal lopen. Bij velen leeft het beeld dat deze wet vooral wat moet doen aan data die door een incident op straat komen te liggen, bijvoorbeeld door een digitale inbraak of dataverlies door eigen medewerkers.

In werkelijkheid ligt het probleem iets ingewikkelder. De GDPR gaat, net als de Wbp (Wet bescherming persoonsgegevens), die al sinds 2000 van toepassing is, veel verder. Bedrijven en overheden moeten zich afvragen met welk doel zij over bepaalde gegevens beschikken en in hoeverre deze gegevens ook voor andere doelen gebruikt mogen worden. Zolang organisaties niet weten waar de persoonsinformatie van hun relaties, zoals klanten, patiënten, leden, abonnees en anderen, zich bevindt en wie toegang tot deze data heeft, is het lastig om te controleren hoe de gegevens worden gebruikt.

Daarbij komt dat het laten 'rondslingeren' (zie kader) van informatie meer nadelen heeft. Wat er rondslingert, zijn in bijna alle gevallen kopieën van de bron, die snel 'verouderen' en niet meer de actuele gegevens in de bron weerspiegelen. Het gevolg is dat medewerkers met 'oude' informatie werken, iets wat vooral bij persoonsgegevens nogal kwalijke gevolgen kan hebben. Daarnaast is het voor eventuele digitale inbrekers niet moeilijk zoeken als data zich overal bevinden.

Er zijn ook voorbeelden van organisaties die de fout ingaan bij het gebruik van data die in hun bezit zijn voor doeleinden waarvoor geen toestemming is ver-

REACTIES EN BIJDRAGEN

Voor reacties en nieuwe bijdragen van IT-experts:
Henk Ester
020-2356415
h.ester@agconnect.nl

Het identificeren van persoonsgegevens is de eerste stap

ZWERF-INFORMATIE

Rondslingerende informatie (ook wel 'zwerf-informatie' genoemd) kan gaan om prints of USB-sticks die achterblijven op de werkplek. Of om laptops, mobieltjes of tablets die werknemers in de auto laten liggen. Bij diefstal komt bedrijfsinformatie in verkeerde handen. Het levert ook een datalek op als er persoonsgegevens bij zijn betrokken. Het gaat echter ook om 'oude' lijstjes die overal te vinden zijn in spreadsheets, Word-documenten et cetera. Namen, adressen en telefoongegevens die nooit worden gecontroleerd met authentieke registraties. Het veroorzaakt berichten aan personen die al zijn overleden. Dit is niet alleen pijnlijk voor de ontvangers, maar ook een onacceptabele handeling van de verzender. Denk hierbij aan e-mails met een bijlage met salaris- en/of klantgegevens die per ongeluk naar de verkeerde personen worden gestuurd. Maar ook aan het delen van privacygevoelige gegevens via publieke diensten als Dropbox en WeTransfer of aan databases in websites waar klanten hun gegevens achterlaten, aan factuur- of creditcardgegevens, bewaard buiten de financiële administratie, en aan kopietjes van een paspoort die buiten het personeelsdossier worden bewaard.

eist. Vorig jaar legde de Autoriteit Persoonsgegevens nog een dwangsom op aan de gemeente Arnhem vanwege een privacyschendende afvalpas. Begin vorig jaar werd in de media uitgebreid bericht dat de Hoge Raad had geoordeeld dat de fiscus beelden van snelwegcamera's niet mag gebruiken voor het controleren van leaseauto's. Het ongebreideld koppelen van databestanden is dus voorbij.

EERSTE STAP

Bedrijven en overheden die zich ervan bewust zijn dat ze eigenlijk niet weten waar hun gegevens zich bevinden, doen in toenemende mate een beroep op consultants die E-Discovery-diensten aanbieden. E-Discovery wordt normaal gesproken ingezet bij het zoeken naar digitaal 'bewijs' in verband met intern onderzoek of onderzoek uitgevoerd door of namens een toezichthouder. Technische E-Discovery-tools kunnen uitstekend helpen bij het lokaliseren van privacygevoelige data in de IT-infrastructuren van bedrijven en overheden. E-specialisten doen dat door het informatielandschap van een bedrijf in kaart te brengen door middel van onderzoek en interviews en door het doorzoeken van databases, e-mail- en fileservers op persoonsgevoelige data. Zij doen dit aan de hand van vooraf gedefinieerde patronen, die telefoonnummers, bankrekeningnummers, paspoortnummers of creditcardnummers kunnen herkennen. In sommige gevallen worden zelfs geavanceerde technieken zoals 'entity extraction' ingezet om namen van personen te herkennen in ongestructureerde data.

Het in kaart brengen van het informatielandschap en het identificeren van persoonsgegevens door een organisatie zijn in feite de eerste stap in de voorbereiding op de GDPR. Deze stap levert een snapshot op van de organisatie. Maar informatie verandert constant en mensen krijgen onder de GDRP ook het recht op inzage in en correctie van de persoonsgegevens die door een organisatie worden verwerkt. Ook voor dit doel kan E-Discovery-software worden ingezet als enterprise search engine, waarmee via één loket door alle verschillende gegevensbronnen op een uniforme wijze gezocht kan worden. Die toepassing is overigens niet nieuw. Met name overheidsorganisaties hebben in het verleden ook al interesse getoond in E-Discovery-technieken om zo beter (en vooral sneller) te kunnen reageren op Wob (Wet openbaarheid bestuur)-verzoeken. Ook in het geval van deze verzoeken bleek relevante informatie zich in allerlei verschillende (en vooral onverwachte) computersystemen te bevinden.

RONDSLINGEREN

Maar met het in kaart brengen van het informatielandschap en het vinden van

SYMPOSIUM E-DISCOVERY

Op 26 april vindt het 9de Symposium E-Discovery in Nederland plaats in Leiden. Het thema dit jaar is de Global Data Protection Regulation (GDPR). Het symposium wordt georganiseerd door het lectoraat Digital Forensics & E-Discovery van de specialisatie Forensisch ICT van de Hogeschool Leiden. Tijdens het symposium wordt ingegaan op E-Discovery-oplossingen en -technieken die organisaties kunnen helpen bij het in kaart brengen van gegevens in hun organisatie, die relevant zijn in het kader van de nieuwe GDPR. Met name de eerste fasen van het E-Discovery Reference Model, Information Governance en Identification, zijn relevant. Naast technische E-Discovery-oplossingen wordt ook aandacht besteed aan digitaal archiveren, aan het juridische spanningsveld tussen E-Discovery en de GDPR en de legitimatie voor de inzet van E-Discovery.
Voor meer informatie: hsleiden.nl/symposium-ediscovery-2018.
Deelname is gratis, maar registratie is vereist.

de data zijn de problemen niet opgelost. Ze kunnen dan wel ingezien, vernietigd, geanonimiseerd of in een betrouwbare bron worden opgeslagen, maar dat is niet voldoende om te voorkomen dat het 'rondslingeren' weer begint. De oorzaak van het rondslingeren moet aangepakt worden, anders blijft het dweilen met de kraan open. Bedrijfsprocessen moeten anders worden ingericht, bewustzijn van goed omgaan met (persoonlijke) gegevens moet worden gestimuleerd en er moet beter en meer worden gecontroleerd op het uitvoeren van procedures inzake de verwerking van persoonlijke gegevens.
Daarmee komen we op het terrein van information governance: de wijze waarop organisaties regels, besliskaders en verantwoordelijkheden vaststellen en onderhouden voor de effectieve creatie, de verzameling, de analyse, de distributie, het gebruik, het behoud en de vernietiging van informatie. Het betreft dus de wijze waarop de informatiehuishouding wordt ingericht om de verantwoording en de performance zo effectief, efficiënt en compliant mogelijk in te richten. In essentie komt het neer op het realiseren van de informatiewaardeketen, de keten van informatieprocessen die ervoor zorgt dat informatie te allen tijde vindbaar, beschikbaar en toegankelijk is in de context waarin die informatie is vastgelegd (www.vbds.nl/2017/12/13/).
De informatiewaardeketen zou voor overheden het realiseren van de Archiefwet veel eenvoudiger maken. Die informatiewaardeketen is het laatste decennium echt een hoofdpijndossier. Zowel bedrijven als overheden hebben hun information governance en de daaraan gerelateerde informatiewaardeketen niet onder controle, met alle gevolgen van dien. Het draait voor een groot deel om bewustzijn dat digitaal werken een fundament als information governance met een ingerichte informatiewaardeketen vereist om de performance van Enterprise Information Management te verhogen. Op die manier worden archivering, privacy, security en duurzame toegankelijkheid van informatie geïntegreerd benaderd en wordt GDPR onderdeel van een gestructureerde en verantwoorde aanpak van informatiemanagement en -beheer. Door de vereiste procedures onderdeel te maken van de information governance, wordt GDRP-compliance geborgd in de informatiewaardeketen van de organisatie.

AUTEURS

HANS HENSELER
is lector Digital Forensics & E-Discovery bij de specialisatie Forensische ICT aan de Hogeschool Leiden. Hij is tevens CEO en medeoprichter van Tracks Inspector, dat software ontwikkelt voor opsporingsinstanties (henseler.h@hsleiden.nl).

GEERT-JAN VAN BUSSEL
is oprichter en directeur van Van Bussel Document Services en docent/onderzoeker aan de Universiteit en Hogeschool van Amsterdam.