Privacy dreigt gemeenten lelijk op te breken

'SUWINET SLECHTS TOPJE VAN DE IJSBERG'

De meerderheid van de gemeenten heeft de beveiliging van persoonsgegevens niet op orde. Grote kans dat uw gemeente er daar een van is. Dan gaat het niet alleen om Suwinet, maar om álle systemen waarmee persoonsgegevens worden verwerkt. De risico's: rondzwervende gegevens, hoge boetes, reputatieschade en afsluiting van Suwinet.

TEKST: DORINE VAN KESTEREN, BEELD: HAJO DE REIJGER

Suwinet is al vijftien jaar lang een bron van onrust. In dit digitale systeem staat gevoelige informatie over burgers, bijvoorbeeld over arbeidsverleden, opleiding, alimentatie, uitkering en boetes. Gegevens die niet in verkeerde handen moeten vallen, daarover is iedereen het eens. Toch slagen gemeenten, UWV en SVB er niet in om Suwinet structureel afdoende te beveiligen. D66-Kamerlid Steven van Weyenberg kwam vorig jaar juni dan ook met een concreet actieplan met harde deadlines. Als voorbeeld van de falende beveiliging noemde hij vrouwen die door hun partner werden gevonden in een blijf-van-mijn-lijf-huis, nadat die hun adres in Suwinet had opgezocht.
Onderdeel van het aanvalsplan is een uitgebreid onderzoek van de Inspectie SZW (zie kader), waarbij alle gemeenten worden doorgelicht. Als daaruit blijkt dat de boel nog steeds niet op orde is, geldt afsluiting van Suwinet als ultimum remedium. "Het laat zich raden wat daarvan de gevolgen zijn voor de bedrijfsvoering. Of het daadwerkelijk tot afsluiting gaat komen, is nog onbekend. Feit is wel dat staatssecretaris Klijnsma van SZW de hete adem van de Tweede Kamer in haar nek voelt", zegt Wiljan de Jong van Stimulansz, die een platform heeft opgericht van gemeentelijke koplopers op het gebied van privacy (zie kader).

GIGANTISCHE BOETES

Niet alleen de Inspectie SZW, maar ook de Autoriteit Persoonsgegevens (voorheen College Bescherming Persoonsgegevens) dreigt met sancties. Deze autoriteit heeft een zelfstandige onderzoeksbevoegdheid (zie kader) en handhaaft de Wet bescherming persoonsgegevens (Wbp). Bij overtredingen kan de autoriteit sinds 1 januari 2016 boetes opleggen die oplopen tot 820.000 euro. De Boetebeleidsregels 2016 van de Autoriteit Persoonsgegevens somt verschillende categorieën boetes en tekortkomingen op. De Jong: "Er geldt bijvoorbeeld een meldplicht voor datalekken. Als je je daar niet aan houdt, kan de boete 500.000 euro bedragen. Dergelijke boetes zijn nog niet opgelegd, maar het wachten is tot het moment dat het wel gebeurt. En maar weinig ambtenaren weten dat zijzelf ook financieel aansprakelijk gesteld kunnen worden, althans de verantwoordelijke directeur of wethouder."
Ook de Europese regelgeving wordt strenger. Op de bescherming van persoonsgegevens is op dit moment nog de Europese Privacyrichtlijn van toepassing. De EU is echter druk bezig om deze verouderde richtlijn te vernieuwen en te vervangen door de zogenoemde Algemene Verorde-

ning Gegevensbescherming. Deze voorziet bijvoorbeeld in boetes tot maximaal 1 miljoen euro of 2 procent van de wereldwijde omzet bij overtreding van de regels.
Naast de dreiging van sancties is het voorkomen van reputatieschade een reden om Suwinet goed te beveiligen. De Jong: "Het is zeer vervelend als in de krant komt te staan dat een gemeente niet in staat is om de privacy van haar burgers te waarborgen. Dat is nooit het héle verhaal, maar dat is wel de boodschap die blijft hangen bij de mensen."

BEVEILIGINGSPLAN

De Inspectie SZW verwacht dat iedere gemeente een plan opstelt met concrete maatregelen om Suwinet te beveiligen; maatregelen die ertoe leiden dat medewerkers louter gegevens kunnen inzien die ze voor hun werk nodig hebben. >

‘Een beveiligingsplan van tientallen pagina’s met tig verboden schiet zijn doel voorbij’

Renze Zijlstra is informatiemanager bij een gemeenschappelijke regeling voor zeven gemeenten in Noordwest-Friesland. Hij schreef het informatiebeveiligingsplan voor de organisatie. “Daarin staat bijvoorbeeld dat elk half jaar steekproefsgewijs de logfiles van Suwinet worden gecheckt: welke medewerker heeft op welk moment welke gegevens opgevraagd? Vervolgens controleren we of er een directe link is met een zaak van die bewuste medewerker. Bij een onrechtmatige opvraging volgt een waarschuwing, bij herhaling volgen disciplinaire sancties. De medewerkers weten dat er over hun schouder wordt meegekeken. Dat is geen wantrouwen, maar een logische, noodzakelijke waarborg als er met persoonsgegevens wordt gewerkt.”

Een andere maatregel is dat slechts een zeer beperkt aantal medewerkers in Suwinet kan zoeken op andere sleutels dan het burgerservicenummer. Zijlstra: “Zoeken op adres of geboortedatum is veel laagdrempeliger. Denk aan een medewerker die net gescheiden is en het adres kent van de nieuwe vriend bij wie zijn ex is ingetrokken. Die verleiding moet er niet zijn.”

OP STRAAT

Suwinet is niet de enige database met persoonsgegevens waarover gemeenten beschikken. Dat zijn er veel meer: registraties van kentekenscanners en camera’s – bijvoorbeeld uit parkeergarages of onveilige buurten – en de applicaties met gegevens over personeel of leveranciers. Daarom verplicht de Wbp gemeenten om organisatiebreed een beveiligingsplan op te stellen. De Jong: “Maar weinig gemeenten zijn zich ervan bewust dat Suwinet het topje van de ijsberg is.” Zijlstra: “Niet alleen voor Suwinet, maar voor álle applicaties en databronnen zijn toegangsbeveiliging en veilig verzenden de pijlers van onze beveiliging.”

Ook de harde schijven van computers, laptops en kopieerapparaten verdienen speciale aandacht. Formeel moeten deze door de shredder voordat een externe partij – een reparateur of softwarespecialist bijvoorbeeld – toegang tot de apparaten krijgt. Zijlstra: “Na de migratie naar een shared service center hebben wij alle hardware die werd afgeschaft ontdaan van de datadragers die we vervolgens gecertificeerd hebben laten shredderen. En voordat we kopieerapparaten en printers vervangen, verwijderen we daarvan alle gegevens.” Smartphones zijn een andere risicofactor. “Talloze medewerkers ontvangen de werkmail op hun mobiele telefoon of tablet. Als ze dat apparaat verliezen, liggen de persoonsgegevens letterlijk op straat. Hetzelfde geldt natuurlijk voor usb-sticks”, zegt De Jong.

DISCIPLINE

Een beveiligingsplan schrijven is een ding, ernaar handelen een tweede. Dat vergt discipline en permanente aandacht, weet Zijlstra. “Ook van het

Het koplopersplatform

Bewustwording, onderzoek en beleidsontwikkeling op het gebied van privacy en informatiebeveiliging, dat zijn de hoofddoelen van het koplopersplatform dat Stimulansz heeft opgericht. Het platform wil snel slagen maken, want gemeenten lopen eigenlijk al ver achter. Bij het platform zijn regionale samenwerkingsverbanden en zowel grote als kleine gemeenten aangesloten, waaronder de gemeente Utrecht en de twee samenwerkingsverbanden ISD Brabantse Wal en de Dienst Sociale Zaken en Werkgelegenheid Noordwest Fryslân.

Meer informatie? wiljan.dejong@stimulansz.nl.

Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens legde vorig jaar dertien gemeenten langs de privacymeetlat: Delft, Eindhoven, Enschede, Nunspeet, Zutphen, Baarle-Nassau, Brielle, Brummen, Heerenveen, Midden-Drenthe, Moerdijk, Werkendam en Woudenberg. Afgelopen januari volgde de conclusie: de beveiliging van persoonsgegevens is verbeterd, maar een aantal gemeenten voldoet nog niet aan alle normen. De komende tijd beoordeelt de Autoriteit Persoonsgegevens of de gemeenten in kwestie verbeteringen hebben doorgevoerd. De vicevoorzitter noemde het onacceptabel dat niet alle gemeenten de zaken op orde hebben. "Als dit niet verandert, is het onvermijdelijk dat wij gaan handhaven."

Onderzoek Inspectie SZW

De Inspectie SZW onderzoekt de beveiliging van Suwinet bij gemeenten. In 2013 en 2014 deed zij dit steekproefsgewijs. Daaruit bleek dat respectievelijk 96 en 83 procent van de onderzochte gemeenten niet aan de zeven essentiële beveiligingsnormen voldeed. Tussen 1 september 2015 en 1 januari 2016 heeft de Inspectie álle gemeenten aan een onderzoek onderworpen. De uitkomsten hiervan worden in april verwacht.

De zeven essentiële beveiligingsnormen zijn:

- **Heeft de gemeente een beveiligingsbeleid en een plan met maatregelen ter bescherming van de beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid van persoonsgegevens en informatiesystemen, waaronder Suwinet?**
- **Draagt de gemeente het beveiligingsbeleid en plan actief uit binnen de organisatie?**
- **Worden het beveiligingsbeleid en plan regelmatig geëvalueerd en geactualiseerd?**
- **Zijn de taken, verantwoordelijkheden en bevoegdheden ten aanzien van Suwinet beschreven en neergelegd bij de juiste personen?**
- **Heeft de gemeente iemand aangesteld die eindverantwoordelijk is voor de beveiliging van Suwinet?**
- **Heeft de gemeente een procedure met criteria om toegang te krijgen tot Suwinet?**
- **Controleert de gemeente meerdere keren per jaar de verleende toegangsrechten?**

management. Ondanks dat er bij ons niet gevraagd werd om een rapportage van de logfiles, heb ik die toch opgesteld. Zo kwam het onderwerp onder de aandacht." Medewerkers ervaren privacy weleens als een belemmering, merkt hij. "Het kost tijd als je voor iedere applicatie apart moet inloggen in plaats van dat je met één wachtwoord overal toegang tot hebt. Het kost ook tijd als het systeem na tien of vijftien minuten geen gebruik automatisch uitlogt. En niet alle medewerkers hebben toegang tot elke applicatie. Daardoor ontstaat spanning tussen de beveiligingseisen en de wens om snel en efficiënt te kunnen werken; een wens die gezien de werkdruk legitiem is." Niet iedere maatregel hoeft veel tijd te kosten, werpt De Jong tegen. "Het is bijvoorbeeld heel simpel om altijd als je even wegloopt, je scherm te locken met de toetscombinatie windowstoets + L."

Bewustwording is een belangrijk doel van het koplopersplatform van Stimulansz. De Jong: "Pas als gemeenten zich bewust zijn van de gevaren en risico's rond privacy kunnen zij een beveiligingsplan opstellen. De tweede stap is om de organisatie hierop in te richten. En daarna moeten ze zorgen dat ze in control blijven, door het plan en de uitvoering daarvan te verbeteren met behulp van de *'plan, do, check, act'*-cyclus. Daarvoor bestaan handige hulpmiddelen, zoals een beveiligingsmonitor om het beveiligingsplan door te lichten en een bewustwordingsmonitor om het privacybewustzijn van de medewerkers in beeld te brengen."

Gemeenten hoeven niet allemaal zelf het wiel uit te vinden en mogen best hun voordeel doen met goede praktijkvoorbeelden, maar Zijlstra – zelf ook aangesloten bij het platform – vindt het niet verstandig om blind het beveiligingsplan van een andere organisatie over te nemen. "Iedere gemeente moet zelf nadenken over haar eigen valkuilen en de oplossingen die daar in de eigen praktijk het beste bij passen." Hij waarschuwt ook voor een wedstrijdje 'Wie is de strengste?'. "Een beveiligingsplan van tientallen pagina's met tig verboden schiet zijn doel voorbij. Het is nu eenmaal niet mogelijk om alles voor 100 procent te beveiligen. En dat hoeft ook niet. De Wbp biedt ruimte voor verstandige afwegingen, dus benut die ruimte ook." *