FOTO ISTOCK, BEWERKING NRC

DATA

Bedrijven houden lekken vaak voor zich

Sinds een jaar moeten bedrijven en instellingen datalekken aanmelden. De Autoriteit Persoonsgegevens kreeg 5.500 meldingen. Onbeveiligde laptops en zoekgeraakte of besmette usb-sticks. „Naïviteit ten top."

Door onze medewerker
Liza van Lonkhuyzen

DEN HAAG. Ziekenhuizen en andere zorginstellingen melden veruit de meeste lekken van privacygevoelige persoonsgegevens. Dat heeft toezichthouder Autoriteit Persoonsgegevens woensdag bekendgemaakt. Deze instelling maakt de balans op van het eerste jaar dat de meldplicht voor datalekken van kracht was.

Het was onthutsend, zegt de voorzitter van de Autoriteit Persoonsgegevens (AP), Aleid Wolfsen. In de eerste week in zijn nieuwe functie deze zomer bleek dat een organisatie tijdens het verhuizen een kast met persoonlijke dossiers van klanten domweg had achtergelaten in het pand. Tenenkrommend vindt hij het ook als laptops met medische gegevens van patiënten worden gestolen en geen wachtwoord blijkt te zijn ingesteld. „Naïviteit ten top."

Sinds een jaar moeten bedrijven, overheden, universiteiten, ziekenhuizen etcetera ernstige datalekken melden bij de AP, die toezicht houdt op gebruik van persoonsgegevens. Wie zich niet binnen een paar dagen meldt, kan hoge boetes krijgen. Die hangen organisaties ook boven het hoofd wanneer de beveiliging van persoonsgegevens zwaar ondermaats blijkt.

De toezichthouder mag officieel boetes tot ruim acht ton opleggen, of 10 procent van de nationale jaaromzet. In het eerste jaar is nog geen enkele boete uitgedeeld. Wél lopen naar tientallen bedrijven onderzoeken, waar in sommige gevallen volgens de AP ook boetes op kunnen volgen.

De AP heeft in het eerste jaar zo'n 5.500 meldingen binnengekregen, bijvoorbeeld over zoekgeraakte usb-sticks of verkeerd geadresseerde post met gevoelige gegevens. Bijna eenderde daarvan (29 procent) kwam uit de gezondheids- en welzijnssector. Op enige afstand volgen de sectoren financiële dienstverlening (17 procent) en openbaar bestuur (15 procent). Meer dan honderd organisaties kregen een officiële waarschuwing.

Nieuws over datalekken bij gemeenten of ziekenhuizen deed afgelopen jaar vaak stof opwaaien. Je hoeft als klant van zo'n organisatie niet altijd 's nachts wakker te liggen van het lek, zegt Wolfsen - oud-rechter en voormalig burgemeester van Utrecht. „Soms heeft een database met gegevens opengestaan en had iemand met kwade bedoelingen erbij gekund, maar is dat niet gebeurd."

Identiteitsfraude is het doemscenario bij een lek, waarbij criminelen met andermans identiteit aan de haal gaan om bijvoorbeeld een woning te huren voor een wietplantage. „Sommigen denken bij een lek van burgerservicenummers: waar gaat dat nou over", zegt Wolfsen. „Maar je hoeft maar één slachtoffer tegen te komen van identiteitsfraude en je begrijpt hoe ernstig dat is."

De medische sector is op IT-gebied nog weinig volwassen

Dat de medische sector zich het meest heeft gemeld, verbaast beveiligingsexpert Kevin Jonkers van Fox-IT allerminst. De sector is volgens hem „weinig volwassen" op IT-gebied. Medische persoonsgegevens komt zijn bedrijf tegen op laptops zonder versleuteling die mee naar huis worden genomen of onbeveiligde servers. „Robots helpen steeds vaker in operatiekamers, maar die computers worden gewoon aan het algemene ziekenhuisnetwerk gehangen en niet extra beveiligd. Als je op het netwerk weet in te breken, is dat heel gevaarlijk."

Vorig jaar berekende Deloitte dat meer dan de helft van de Nederlandse ziekenhuizen wel eens te maken heeft gehad met een besmetting van medische apparatuur met een computervirus, zoals hartmonitoren, infusie-apparatuur en MRI-scanners. Die zijn dan bijvoorbeeld geïnfecteerd door besmette usb-sticks.

Vaak is er sprake van onzorgvuldig handelen. Het Isala-ziekenhuis deed vorig jaar melding van een datalek nadat een laptop van een coassistent was gestolen met daarop een spreadsheet met gegevens van ruim vijfhonderd patiënten. Zij waren onder behandeling van de afdeling plastische chirurgie voor een syndroom waarbij een zenuw in de pols bekneld is geraakt. „Je eigen lichaam en je geestelijke gezondheidszorg, dat zijn echt privézaken", zegt Wolfsen.

De voorzitter vermoedt dat de bereidheid om te melden in de medische sector groot is, omdat men beseft dat met heel gevoelige gegevens gewerkt wordt.

Opvallend genoeg zijn veel minder datalekken gemeld dan vooraf werd gedacht: experts hadden verwacht dat er zo'n zestigduizend datalekken per jaar zouden boven komen. Beveiligingsexpert Sijmen Ruwhof van Secundity spreekt van *underreporting* in het bedrijfsleven. 5.500 meldingen is volgens hem „extreem weinig" vergeleken met de werkelijke hoeveelheid datalekken. Deels komt het verschil volgens hem door een passieve houding van bedrijven. „Als een virus op een bedrijfscomputer wordt aangetroffen, wordt de computer opnieuw geïnstalleerd. Er wordt meestal niet gekeken of er überhaupt gegevens gelekt zijn naar het internet. Bedrijven houden ook meestal geen technische logboeken bij, waarmee dat makkelijker is na te gaan."

Wanneer bedrijven wel beseffen dat sprake is van een datalek, houden ze dat volgens Ruwhof vaak stil uit angst klanten te verliezen door imagoschade. „Bedrijven hopen simpelweg dat een hack nooit ontdekt wordt." Het schrikbeeld is volgens Ruwhof Diginotar, een bedrijf dat veiligheidscertificaten regelde en failliet ging nadat bekend werd dat het gehackt was.

Ondanks dit verzuim heeft de meldplicht volgens Ruwhof wel voor flink wat opschudding gezorgd in het bedrijfsleven. „Computerbeveiliging wordt opeens een duidelijke business case. Ondernemers beseffen dat ze financieel aansprakelijk zijn."

De zelfverklaarde ethische hacker vindt het „slim" dat nog geen boetes zijn uitgedeeld. „Je wil mensen niet afschrikken door wie zich braaf meldt te straffen wegens belabberde informatiebeveiliging." Wolfsen beaamt dat dit meespeelt. „We zien het liefst dat zoveel mogelijk datalekken worden gemeld, zodat gaten snel worden gedicht."

De AP vraagt expliciet tips en onderzoekt incidenten die in de media komen. Volgens Ruwhof is het nodig dat datalekken die onder de pet worden gehouden veel actiever worden opgespoord, al is dat heikel voor de autoriteit. „Om te beoordelen of er een beveiligingslek is, moet je dit lek vaak uitproberen en dat mag niet zomaar. Het is een spagaat: beveiligingslekken liggen voor het oprapen, maar je mag de wet niet breken door zelf te gaan hacken."

Het is niet verstandig om ongevraagd testen uit te gaan voeren, vindt ook Jonkers van Fox-IT. „Tot op zekere hoogte kan de AP wel zelf gaan zoeken, want soms zijn gelekte databestanden gewoon op internet te vinden."

De AP kampt ook met een ander obstakel. Het kabinet schatte eerder dat 130.000 Nederlandse organisaties met privacygevoelige gegevens werken. Bij de toezichthouder werken gemiddeld zes man fulltime aan het controleren van gemelde datalekken. „We zijn te klein", zegt Wolfsen. „Dat geven de Tweede Kamer, minister Van der Steur van Veiligheid en Justitie en wijzelf toe."

Bedrijven hopen simpelweg dat een hack nooit ontdekt wordt

De voorzitter ziet deze periode als een opmaat naar mei 2018, wanneer Europese wetgeving van kracht wordt. Daarin staat dat bedrijven transparanter moeten zijn over hoe en waarom ze welke data verwerken. Burgers kunnen daarnaast om inzicht in hun eigen gegevens vragen. Boetes worden flink opgehoogd: Europese privacytoezichthouders kunnen tien of twintig miljoen euro opleggen, afhankelijk van de overtreding.

Wij krijgen er mensen bij, zegt Wolfsen. „In de nieuwe Europese regels staat dat elke privacytoezichthouder genoeg mankracht moet hebben." Na mei 2018 wordt het volgens hem „echt menens".

Vijf tips voor wie een datalek ontdekt

Organisaties moeten soms eerlijk zeggen dat er een lek is: namelijk wanneer zij de Autoriteit Persoonsgegevens niet kunnen overtuigen dat betrokkenen hoogstwaarschijnlijk geen last krijgen van het lek. Wat je kan doen als blijkt dat jouw gegevens mogelijk gelekt zijn verschilt per soort datalek, maar beveiligingsexperts Sijmen Ruwhof en Kevin Jonkers hebben toch vijf algemene tips:

- Bedenk goed bij wie je welke gegevens achterlaat en probeer dat zoveel mogelijk tot een minimum te beperken. Wat er niet is, kan ook niet gestolen worden.
- In principe moet de 'lekkende organisatie' burgers ook vertellen welke actie zij het beste kunnen ondernemen als er iets is gelekt. Vraag daar dus naar, als je geen adviezen krijgt.
- Als je wachtwoord is gelekt, wil je dat graag veranderen. Ga vooral na of je hetzelfde wachtwoord niet ook elders gebruikt (sowieso een slecht idee). Het gebeurde de ceo van Facebook dat zijn Twitter-account werd gehackt door een datalek bij LinkedIn.
- Mochten privégegevens zijn gelekt die je niet zomaar kunt wijzigen, wees dan vooral op je hoede voor misbruik. Denk aan vreemde uitgaven op je creditcard of post over abonnementen die je niet hebt afgesloten.
- Wees ook alert op mails die afkomstig zijn van het bedrijf waar het datalek is geweest. Deze kunnen door de aanvaller verstuurd zijn. Niet zomaar op linkjes klikken of bijlagen openen.