DATALEKKEN

Katalysator die privacy volwassen maakt

Axel Arnbak

Nog niet zo lang geleden was privacy een 'dode letter der wet'. Een abstract grondrecht waar alleen academici en complottheoretici om zouden geven. De recente stortvloed aan datalekken heeft dat voorgoed veranderd. Vraag maar aan advocaat Geert-Jan Knoops die afgelopen vrijdag zijn concept-pleitnota in het Wilders-proces teruglas in de krant. Voor ernstige datalekken baseren Amerikaanse verzekeraars hun datalek-polissen op circa € 200 aan geschatte schadekosten per benadeeld persoon. Een bittere pil als het misgaat en miljoenen datarecords lekken. Ooit dacht niemand iets te verbergen te hebben. In feite heeft iedereen iets te beschermen.

Sinds de wijziging van de Wet bescherming persoonsgegevens op 1 januari 2016 moeten Nederlandse dataverwerkers datalekken binnen 72 uur verplicht melden bij de Autoriteit Persoonsgegevens. De boetebevoegdheid van de toezichthouder is daarbij verhoogd naar geldboetes die kunnen oplopen tot 10% van de netto-omzet van een dataverwerker. Een eerste tussenbalans uit de praktijk leert dat beleidsmakers en toezichthouders gek zijn op datalekken, die het altijd zo abstracte privacy eindelijk handen en voeten geven. In het voetspoor van streng beleid gaan dataverwerkers privacy en beveiliging daadwerkelijk prioriteren. En blijkt dat de meeste datalekken te voorkomen zijn met vrij basale maatregelen.

Beleidsmakers en toezichthouders spinnen garen bij datalekken, omdat incidenten de brug slaan tussen allerlei domeinen die tot voor kort onoverbrugbaar leken. Niet alleen maakt een datalek de abstracte dreiging van privacy-inbreuken concreet, maar de valse tweedeling tussen private privacy en publieke veiligheid is eindelijk doorbroken. Datalekken laten zien dat iedereen baat heeft bij privacy én bij veiligheid. Zelfs de altijd ruziënde Europese en Amerikaanse autoriteiten zijn wat dit betreft ineens de beste vrienden, terwijl zij doorgaans in hun opvattingen over privacy en overheidsregulering totaal verschillen. Zo is privacywetgeving in de VS er alleen voor sommige sectoren, maar in vrijwel elke staat geldt al meer dan tien jaar een meldplicht datalekken met miljoenenboetes tot gevolg. Door een Trans-Atlantische consensus ontwikkelen datalekken zich nu overal ter wereld tot een 'sweet spot' voor privacyhandhavers. Des te curieuzer is het dat Knoops zo opzichtig tegenover de media verklaart dat hij het datalek rondom het Wilders-proces niet aan de Autoriteit Persoonsgegevens heeft gemeld.

Door de lange praktijk in de VS bestaan talloze publieke datasets over datalekken. Recent heeft IT-beveiliger Trend Micro de data van stichting Privacy Clearing House met alle Amerikaanse datalekken tussen 2005 en 2015 netjes op een rijtje gezet. Wat blijkt: ruwweg 60% is te wijten aan doodgewone oorzaken als het ontbreken van een intern IT-beleid, een verloren usb-stick of het lekken van gegevens door 'insiders', zoals werknemers die data doorverkopen op de zwarte markt. Tegen geavanceerde cybercrime kunnen organisaties zich niet eenvoudig wapenen, maar juist bij zulke alledaagse oorzaken ligt het laaghangende fruit voor intern IT-beleid en bij de toezichthouder als het misgaat.

Door datalekken is de tijd dat het grondrecht op privacy als abstract werd gezien voorgoed voorbij

Geavanceerde beveiligingstechnologie is dus maar een deel van je verdedigingsstrategie. Sterker nog, technologie kan nog zo duur en glimmend zijn, de gebruiker omzeilt interne regels meteen als beveiligingsmaatregelen normaal gebruik in de weg zitten. Denk maar aan Hillary Clinton, die het beveiligingsbeleid van de overheid in de wind sloeg en zelfs als minister van buitenlandse zaken haar eigen onveilige e-mailservers en Blackberry bleef gebruiken. Technologie, functionaliteit, strak intern beleid en continue training voor medewerkers, het zijn allemaal basiselementen om datalekken, wantrouwende gebruikers en boetes te voorkomen.

Door datalekken zijn de tijden dat het grondrecht op privacy als abstract gezien werd voorgoed voorbij. Iedere serieuze organisatie maakt nu haast met het beveiligen van data en het beschermen van privacy. Dat toont de volwassenwording van privacy in onze datasamenleving waarin ons lijf en lede in databases staat. Dat geldt al helemaal voor ziekenhuizen, banken en advocaten die extreem gevoelige data moeten beschermen van patiënten en cliënten. En al helemáál als je de verdediging op je neemt van een controversieel politicus in de meest besproken juridische procedure van het jaar.

Axel Arnbak is advocaat bij De Brauw Blackstone & Westbroek en onderzoeker aan het Instituut voor Informatierecht (UvA). Reacties: @axelarnbak