

Wet Datalekken

Het is niet prettig dat je persoonlijke gegevens op internet zijn te vinden, geboorteplaats, bankrekeningnummers, de namen van je kinderen, de bestellingen bij Zalando of de route van je laatste vakantietrip. Het is informatie die niet iedereen hoeft te weten. Hoe zorgvuldig moeten bedrijven omgaan met jouw data?

Recentelijk waren de gegevens van een half miljoen deelnemers van de Postcodeloterij vrij beschikbaar (<https://www.nrc.nl/nieuws/2017/04/03/lek-gegevens-450-000-deelnemers-loterijen>). Ook bleken honderdduizenden foto's en mailadressen van bezoekers van de Apenheul maandenlang slecht beveiligd te zijn (<http://nos.nl/artikel/2186499>). Tevens had de zo integer geachte Belastingdienst te maken met ongeoorloofde gegevensuitwisseling (<https://www.rijksoverheid.nl/actueel/nieuws/2017/06/30/onderzoek-naar-databeveiliging-belastingdienst>).

Wat heeft de universiteit hiermee te maken? Er wordt hier geen loterij gehouden, zijn geen primaten en is er een goed contact met de Belastingdienst. Waarover zou de universiteit bezorgd zijn?

Welnu, sinds anderhalf jaar is er een uitbreiding op de Wet bescherming persoonsgegevens (Wbp). Het betreft de meldplicht bij een inbreuk op bestanden met persoonlijke data. Wanneer de beveiliging faalt, is de betreffende instantie verplicht dit te rapporteren aan de Autoriteit Persoonsgegevens. Aangezien de universiteit over veel gegevens van haar medewerkers beschikt (van schoonmaker tot hoogleraar), heeft ook zij te maken met de uitbreiding op de Wbp.

Wanneer is er sprake van een gat in de beveiliging? Als iemand onbevoegd toegang heeft gekregen tot persoonsgegevens en deze naar eigen inzicht kan wijzigen, doorsturen of vernietigen. Bij een datalek betreft het niet alleen het vrijkomen van de gegevens, maar ook het onrechtmatig verwerken ervan. Wanneer doet zich een datalek voor? Dat kan al heel simpel zijn, via een vergeten usb-stick, een verdwenen laptop of kopieën die niet zijn vernietigd.

Onlangs heeft mijn leidinggevende mij geïnformeerd: *Frans, zorgt jij er voor dat jouw administratieve gegevens allemaal ingedekt zijn en volledig ontoegankelijk? Voor de universiteit is dit een speerpunt. Vandaar Clara in de cc, zij werkt bij ons Contractenburo en zal met je overleggen. Want, Frans, bedenk: de mens is in dit alles de zwakste schakel. Dat is wat ze je leren op de eerste les Security.*

Ik kreeg van Clara de opdracht tot het opschonen van onze prikborden: het verwijderen van de lijstjes met verjaardagen van collega's, adressen van bedrijven, telefoonnummers van ict-ers, post-its met info over instanties die bij ons op bezoek zijn geweest. Persoonlijke data, dus weg!

Dat was niet voldoende. Waren al onze Outlook-bestanden inbraakveilig? Wijzigden we elke maand onze wachtwoorden? Wilden we een irisscan overwegen? Clara was nog steeds vriendelijk adviserend, totdat ze erachter kwam dat wij uitgebreide persoonsbestanden hebben van studenten en cursisten, van bedrijven en ministeries, vanaf 1992.

C: *Beste Frans, dit is een heel belangrijk bestand! Wat staat daar allemaal in?*

Ik mail dat het gaat over geboortedata, huisadressen, telefoonnummers van werkgevers...

C: *Stuur me een kopie van enkele bestanden, dan weet ik hoe gevoelig ze zijn.*

Dat lijkt me nu juist in strijd met de Wbp en leg dat uit.

C: *Je kunt de kopieën gewoon bij mij langsbrengen.*

Een week lang laat ik niks van me horen.

C: *Stuur me je toegangscode tot jullie administratie.*

Dat lijkt mij geen goed voorstel.

C: *Maak een speciale toegang met wachtwoord voor mij, dan ga ik zelf aan de slag.* Ik ga daar niet mee akkoord, ze hoort niet bij onze groep. Het blijft weer een tijdje stil.

C: *Hoe weet jij eigenlijk dat je geen last gehad van een hacker?*

F: Bij ons komt nooit iemand binnen.

C: *Weet je dat zeker?*

F: Ja, Kaspersky heeft ernaar gekeken.

Een werkdag later volgt: *Er werkt geen Kaspersky bij onze ict. Wie is dat?*

F: Evgeni Kaspersky.

C: *Maar je hebt toch zeker geen Russen tot je administratie toegelaten???*

Hoe onbegrijpelijk kan veiligheid zijn? Hoeveel ict-humor is toelaatbaar? Welke basiskennis moet je hebben van online privacy beleid (<https://www.kaspersky.nl/>)?

Enfin, deze vragen bleven onbeantwoord, aangezien er een dwingend bericht arriveerde van mijn leidinggevende: *Frans, wat is dit? Wat is er aan de hand met die Wet Datalikken? Clara was zojuist op mijn kamer en ze was in tranen. Ze was helemaal overstuurs. Dat moet je me nu echt uitleggen!*

