

Nederlands Dagblad

Christelijk betrokken

Politiek

Hoe meer dossiers, hoe meer lekt

Geplaatst: 08 november 2008 06:00, laatste wijziging: 07 november 2008 21:53

door Jan Salden

DEN HAAG - Overheden en bedrijven lijden aan een haast onstilbare hongers naar informatie. Op steeds meer plaatsen liggen enorme hoeveelheden persoonlijke gegevens opgeslagen. Duizenden mensen hebben daar toegang toe, en dat maakt het risico op het weglekken van informatie groot. „Persoonsgegevens zijn geld waard.“

Ome Brocaar bracht afgelopen zomer voor een werkvakantie een bezoek aan Indonesië. Voorafgaand aan de reis vroeg hij via de website van de Indonesische ambassade een visum aan. Toen hij het daarvoor bestemde formulier had ingevuld, verving hij in het beeldscherm zijn eigen aanvraagnummer door een willekeurig ander. Prompt had hij de visumaanvraag van iemand anders voor zijn neus.

Niet veel later had de student toegang tot de namen, adresgegevens en paspoortnummers van 25.000 andere Nederlanders die sinds begin 2007 een visum hadden aangevraagd. „Ik schrok van wat ik tegenkwam“, aldus Brocaar. „Ik kon precies zien wie wanneer op reis ging. Gouden informatie voor inbrekers.“ Brocaar meldde zijn bevindingen bij de ambassade en het College Bescherming Persoonsgegevens. Maar op zijn e-mails kreeg hij geen reactie. Pas nadat Brocaar naar de media stapte, werd het gat in de beveiliging in alle rijl gedicht.

Het voorval is slechts één voorbeeld van hoe persoonlijke gegevens door onachtzaamheid op straat kunnen komen te liggen. Uit een overzicht van publiciste Karin Spink blijkt het afgelopen jaar op zijn minst twaalf keer vertrouwelijke data onbedoeld te zijn openbaar. Van klantgegevens van banken tot adressen van Defensiepersoneel. En dat zijn alleen nog de incidenten die in de openbaarheid komen.

De kans is groot dat dit soort datalekken in de toekomst vaker voor zal komen, voorspelt Bart Jacobs, hoogleraar computerbeveiliging van de Radboud Universiteit in Nijmegen. „Hoe meer informatie de overheid over ons verzamelt, des te groter het risico dat het een keer mis gaat. En als het dan mis gaat, is de schade aanzienlijk.“

Jacobs verwijst naar het elektronisch patiëntendossier (EPD), dat volgend jaar in gebruik wordt genomen en het arts en makkelijker moet maken gegevens uit te wisselen. „Als een huisarts zijn kast met dossiers per ongeluk open laat staan, krijgt een dief misschien een paar mappen meegesjouwd. Wie het EPD weet te kraken, heeft toegang tot de informatie van miljoenen Nederlanders. En niemand die het opvalt, want je kunt het net zo goed vanuit Rusland doen.“

De kwetsbaarheid van grote databanken zit hem vooral in het grote aantal mensen dat toegang heeft tot een systeem. „Als de databank een grote kluis zou zijn waarin alleen maar gegevens veilig bewaard worden, zou er niets aan de hand zijn“, aldus beveiligingsexpert Mark Koek van het bedrijf Fox-IT. „Maar het EPD is een kluis waar tienduizenden zorgverleners in kunnen. In dat geval is je beveiliging zo sterk als je zwakste schakel. Je



Een verloren USB-stick. Op veel plaatsen liggen enorme hoeveelheden persoonlijke gegevens opgeslagen. Deze gegevens kunnen door onachtzaamheid letterlijk op straat komen te liggen | foto GPD/Emiel Muijderman

kunt mensen wel wijzen op voorschiften, maar daar moeten ze zich dan wel aan houden."

Daar komt bij dat veel werknemers die toegang hebben tot gevoelige informatie amper benul hebben over hoe ze daarmee moeten omgaan. „We vinden het volsprekt normaal dat iemand die auto gaat rijden een rijbewijs moet halen", zegt Hans Nieuwenhuis van de stichting EPN, die onderzoek doet naar effecten van de informatiesamenleving. „Maar voor mensen die toegang hebben tot vertrouwelijke persoonsgegevens is er niets. Waarom laten we een arts geen ICT-rijbewijs halen? Zodat hij weet hoe hij bijvoorbeeld informatie kan coderen."

Omkoping

Toch kan ook dat misbruik niet voorkomen, zegt hoogleraar informatica Chris Verhoef. Hij weigert deelname aan het EPD, simpelweg omdat hij het niet vertrouwt. „Omdat zoveel mensen er toegang toe hebben, is de kans op omkoping groot. Er is altijd wel iemand bereid om tegen betaling vertrouwelijke informatie te leveren. Persoonsgegevens zijn geld waard."

Hoogleraar rechten en informatisering Corien Prins gaat een stap verder. Haar kritiek op de informatiehonger is fundamenteeler. Zo plaatst Prins vraagtekens bij het nut van het patiënten- of kinddossier. „Ik ben daar in het geheel niet van overtuigd. Hoe groot is nu de kans dat mijn Brabantse huisarts mij doorverwijst naar een ziekenhuis in Groningen? En als dat al gebeurt, dan kan dat dossier toch ook op een andere manier met mij mee? Daarover hoor ik niemand." Ik kon precies zien wie wanneer op reis ging. Gouden informatie voor inbrekers.'

----- Datalekken

Het afgelopen jaar kwamen geregeld datalekken in het nieuws. Een aantal voorbeelden uit binnen- en buitenland:

November 2007: Journalisten van het Algemeen Dagblad ontdekken een 340 pagina's tellende lijst met namen, adressen en functies van marinepersoneel op een website van Defensie.

November 2007: De Britse belastingdienst raakt in haar interne post twee cd-roms kwijt met onder meer adressen, bankrekening- en sofinummers van 25 miljoen Britten.

December 2007: Gevoelige gegevens van 55.000 klanten van CZ liggen een week lang op straat door een lek in de website van de zorgverzekeraar.

Juli 2008: Journalisten van de economische website Z24 ontdekken op het internet een presentatie van vermogensbeheerder Fortis MeesPierson. In het document staat informatie over zeer vermogende klanten.

Augustus 2008: Een medewerker van een Duitse loterij stapt naar de politie met een lijst met 17.000 persoonsgegevens die hij van zijn baas had gekregen voor de werving van deelnemers. De lijst blijkt via illegale handel verkregen.

November 2008: De Britse overheid sluit een website na de vondst op een parkeerplaats van een geheugensstick met de wachtwoorden van twaalf miljoen Britten. De wachtwoorden boden toegang hadden tot tal van diensten, zoals belastingteruggave en kinderbijslag.