

Overheid zal veel meer informatie over burgers verliezen

Door [Redactie security.nl](#) op vrijdag 23 november 2007 09:23

Het [incident](#) met de Engelse Belastingdienst die de gegevens van 25 miljoen Britten kwijtraakte staat niet op zichzelf, niet alleen was het de derde keer in korte tijd dat men persoonsgegevens verloor, er zijn honderden databases met persoonlijke informatie die kwetsbaar zijn. Volgens de denktank [Demos](#) zijn er zeker 600 publieke en private databases die persoonlijke informatie over burgers bevatten, zonder dat zij dit vaak weten.

Het rapport van Demos verschijnt volgende maand, maar nu al [roept](#) het op om de "information commissioner", een soort privacywaakhond, meer rechten tegen zowel publieke als private instellingen te geven die databases beheren. Hij zou bijvoorbeeld zonder toestemming van de databasebeheerders controles moeten kunnen uitvoeren. Ook moet er een debat komen over de privacy risico's die het uitwisselen van informatie tussen overheden, om naar eigen zeggen publieke dienstverlening te personaliseren en verbeteren, met zich meebrengt.

Zo moet het straks onmogelijk voor ambtenaren worden om informatie zonder juist "paper trail" te verplaatsen. Tevens wil men de identiteitskaart weer ter sprake brengen, en welke gegevens die zou moeten bevatten.

Wat betreft de Engelse Belastingdienst blijkt dat men in september al een laptop met de gegevens van 400 mensen verloor, en vorige maand verdween ook al een CD-rom met de post, dit keer met de gegevens van 15.000 mensen. Tevens had de rekenkamer om geanonimiseerde gegevens gevraagd, maar de Belastingdienst verstrekke onversleutelde persoonlijke informatie.

"Als het gaat om computerbeveiliging zijn er twee dingen die je moet onthouden. Ten eerste is security altijd afhankelijk van een combinatie van technologie en beleid, en ten tweede dat geen enkel systeem helemaal veilig is. Het is daarom veiliger om aan te nemen dat er incidenten plaatsvinden, en dat je kijkt hoe je de schade kunt beperken. Dat betekent zo min mogelijk informatie opslaan en verplaatsen, gegevens anonimiseren, linken naar persoonlijke details in andere databases, en het gebruik van encryptie. Al die dingen werden niet bij de Belastingdienst gedaan", aldus [The Economist](#).

UBM Global: organisaties met medewerkers die nog geen encryptie discipline en mentaliteit hebben, kunnen worden geholpen met DriveLock software voor beveiliging van USB-sticks en overige externe drives die – optioneel als standaard door de organisatie te configureren - geen wachtwoord, code of biometrie gebruiken om informatie te beveiligen, maar alleen op bepaalde computers of bij bepaalde medewerkers functioneren.

DriveLock Encryptie versleutelt – na eerst de gebruiker te waarschuwen - niet-encrypte USB-sticks automatisch. DriveLock herkent de gebruiker, waardoor de gebruiker geen wachtwoord hoeft te verzinnen en te onthouden. Bovendien kan een teamgenoot, die in dezelfde gebruikersgroep zit, ook deze USB-stick gebruiken. De onderlinge uitwisselbaarheid is erg handig bij een (tijdelijke) taakgroep die werkt aan

een vertrouwelijke zaak of voor dezelfde patiënt of cliënt. Deze onderlinge uitwisselbaarheid is mogelijk bij alle soorten verwijderbare drives.