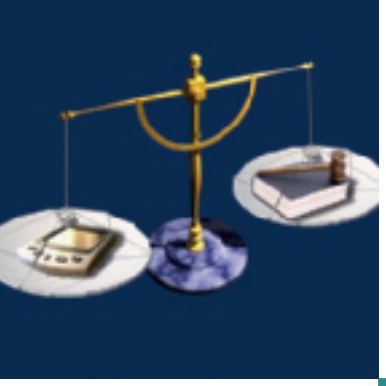
Datalekken: een reality check

van Eijk, N.

Publication date
2012
Document Version
Final published version
Published in
BTG-Magazine



COLUMN

Datalekken: een *reality check*

Column **Nico van Eijk**

De datum van 1 januari ligt al ruim achter ons, maar dat hoeft geen reden te zijn om nog een voorspelling te doen: 2012 wordt het jaar waarin datalekken en daarmee samenhangende internetveiligheid hoog op de agenda komen te staan. Dat stonden deze zaken natuurlijk altijd al, maar nu wordt het menens. Met flauwe praatjes over goede voorlichting en zelfregulering komt men niet meer weg. De borreltijd is over.

De reeks incidenten neemt niet af: van 'incidenten' is dus geen sprake meer. Internet journalist Brenno de Winter organiseerde vorig jaar Lektober en wist bijna iedere dag wel weer een nieuw datalek-verhaal boven water te krijgen. Zelfs zijn eigen server werd gekraakt. De dag waarop ik deze column schrijf, blijkt het mis te zijn bij bierbrouwer Bavaria. 'Privédata van ruim 100.000 Bavaria-klanten gehackt' zo bericht De Winter, die inmiddels de prijs voor journalist van het jaar in ontvangst heeft mogen nemen.

Datalekken zijn niet of nauwelijks geregeld. In de Telecommunicatiewet is er alleen een bepaling voor datalekken bij telecomproviders. De praktijk wijst uit dat daar zich niet de grootste problemen voordoen. Neen, de echte datalekken vinden plaats aan de randen van het internet. Bedrijven en instellingen die hun servers op het internet aansluiten zonder deugdelijke beveiliging. Overheden en thuiswinkels die software niet upgraden of onder het motto *if it ain't broke, don't fix it* blijven vertrouwen op verouderde systemen.

Recent werd met een spetterende lasershow het Nationaal Cyber Security Centrum geopend. Dit moet 'hét expertisecentrum' worden op het terrein van cyber security inclusief de bestrijding van datalekken. Dat klinkt goed en ambitieus, maar kan ook holle retoriek blijken. Het centrum en zijn activiteiten ontberen een formele basis en zijn gebaseerd op (vrijblijvende) publieke private samenwerking. Het klassieke poldergevaar – veel praten, weinig daden – ligt daarmee op de loer.

Terwijl het juist daar om gaat: daden. Europese en nationale overheden breiden meldplichten over datalekken uit. Daarmee zijn datalekken als zodanig nog niet uit de wereld. Regelgevers zullen daarom vrijwel zeker met aanvullende regels komen om betrokken marktpartijen tot actie te dwingen. Partijen zoals de genoemde, die zich bezig houden met het aanbieden van diensten aan eindgebruikers of die grote hoeveelheden data koppelen aan het internet, al dan niet via 'cloud'-achtige structuren. Het zal niet eenvoudig zijn om tot een juist pakket aan maatregelen te komen.

Hier liggen ook kansen voor de betrokken marktpartijen (inclusief hun belangenorganisaties, zoals BTG). Informatie verstrekken over datalekken moet niet afhankelijk zijn van overheidsregels, maar moet uit eigen verantwoordelijkheidsbesef. Bedrijven en personen wiens gegevens zijn gecompromitteerd moeten daarvan vanzelfsprekend op de hoogte worden gesteld. Voor aandeelhouders moet duidelijk zijn wat de werkelijke bedrijfsrisico's zijn. Datalekken worden nu slechts terloops genoemd in jaarverslagen of andere communicatie met de aandeelhouders. Dat kan veel systematischer en inzichtelijker.

Maar bovenal moet het 'datalek-proof' zijn van de organisatie niet als een kost maar als een opbrengst worden gezien. Hoogwaardige beveiliging die stringent door forensische experts wordt getest en geaudit, daar kan men trots op zijn. Om het maar even politiek incorrect te formuleren: een beetje VOC mentaliteit zou ons ten aanzien van internetveiligheid niet misstaan.

Alle datalekken voorkomen is een illusie. Desalniettemin: meer transparantie helpt herhaling voorkomen en leidt tot adequater optreden. Meer zelfreflectie bij organisaties maakt dat hun systemen uiteindelijk robuuster worden.