NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Meldplicht datalekken: angst is slechte raadgever

Nart Wielaard

De nieuwe meldplicht datalekken doet veel stof opwaaien en mediaberichten zaaien angst over de ingrijpende gevolgen van datalekken, zoals forse boetes en negatieve publiciteit. Dat is begrijpelijk, maar angst leidt waarschijnlijk niet tot een meer zorgvuldige omgang met persoonsgegevens. Organisaties moeten geen beleid op dat punt ontwikkelen omdat het moet, maar omdat het ertoe doet voor hun eigen succes. Wie met die bril naar deze uitdaging kijkt, ontwikkelt daarmee ook vanzelf de op principes gebaseerde aanpak die door de wetgever is beoogd.

Auteur Nart Wielaard heeft deze bijdrage geschreven op uitnodiging van NOREA, de beroepsorganisatie van IT-auditors. Samen met Sander Klous publiceerde hij eerder dit jaar het boek 'Wij zijn big data' .

Waarom leggen we dijken aan? Omdat we dat in de wet met elkaar hebben afgesproken of omdat we graag een onbekommerd leven met droge voeten willen? Waarom nemen kinderen een beugel? Omdat dat moet van de tandarts of omdat ze later een mooi gebit willen? Het zijn natuurlijk retorische vragen. Het bestaansrecht van dijken en beugels komt voort uit het feit dat ze een belangrijke rol vervullen. Dat is volstrekt logisch.

Er is echter iets merkwaardigs aan de hand zodra het gaat over de zorgvuldige omgang met persoonlijke data. De logica van de dijken en de beugels gaat dan blijkbaar niet meer op. Want bij het formuleren van beleid op dit punt redeneren organisaties vooral vanuit wettelijke verplichtingen en de angst om niet aan die wet te voldoen. Terwijl ze beter de waarde van veiligheid kunnen redeneren: een zorgvuldige omgang met persoonlijke data is in het huidige digitale tijdperk een essentiële voorwaarde voor succes. Wie het op dit punt beter doet dan de concurrent zal doeltreffender zijn én behoudt het vertrouwen van de klant.

Deze houding is begrijpelijk gezien de talrijke mediaberichten over wat er zoal misgaat. Incidenten zoals die rond het lekken van persoonsinformatie van datingsite Ashley Madison boezemen bestuurders de nodige angst in. *Die angst* is feitelijk al decennia lang de strategie om hen te verleiden tot investeringen in het verhogen van de digitale veiligheid. Ze hebben eigenlijk nooit geleerd om daarbij vanuit eigen kracht te redeneren.

Het is de vraag of deze strategie nog wel werkt of dat bestuurders inmiddels murw zijn gebeukt met de negatieve berichten. Misschien zou het slimmer zijn om de upside van een goede beveiliging – als onderscheidend vermogen in deze digitale tijd – aan hen te verkopen in plaats van te waarschuwen voor de downside van slechte beveiliging. Een reisbureau verkoopt immers ook geen vluchten naar de zon met verkleumde fietsers die tegen de wind in fietsen, maar met foto's van prachtige stranden.

Een tweede vraag is of deze insteek wel tot de beste resultaten – een zorgvuldige omgang met data – leidt. Want redeneren uit angst leidt vrijwel automatisch tot een eenzijdige focus op het centraal stellen van de relevante wetten en regels. En het doel van het security beleid is uiteraard niet een 10 halen voor compliance; het doel is een zorgvuldige omgang met data voor een succesvolle bedrijfsvoering, en als gevolg daarvan het voldoen aan compliance eisen. Vooral in die volgorde. Redeneren vanuit eigen kracht en inschattingen dus.

Dat is juist nu – met de implementatie van de genoemde meldplicht – van essentieel belang. Deze meldplicht houdt – zoals waarschijnlijk bekend is – in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken, datalekken moeten melden aan de Autoriteit Persoonsgegevens (voorheen het College Bescherming Persoonsgegevens). In bepaalde gevallen moet er ook een melding worden gedaan aan de betrokkenen zelf, diegenen van wie persoonsgegevens zijn gelekt. Het gaat hierbij om datalekken waarbij er kans is op verlies of onrechtmatige verwerking van persoonsgegevens.

Ook nu duiken weer de nodige angst zaaiende berichten op in de media: de verantwoordelijken kunnen haast niet anders dan nachtmerries krijgen over wat er allemaal fout kan gaan. Ook al omdat datalekken niet alleen de reputatie aantasten maar nu ook serieuze financiële consequenties kunnen krijgen. De boete kan immers oplopen tot 820.000 euro of zelfs 10% van de jaaromzet. Wat minder duidelijk over het voetlicht komt is dat de wet sterk op principes is gebaseerd en daarmee juist een uitnodiging is om vanuit eigen kracht te redeneren. de Autoriteit Persoonsgegevens heeft beleidsregels voor de meldplicht datalekken opgesteld en roept bedrijven, overheden en andere organisaties op om zelf een beredeneerde afweging maken of een concreet datalek dat hen overkomt onder het bereik van de wettelijke meldplicht valt.

Elke organisatie heeft in grote lijnen te maken met drie uitdagingen:

- Voorkomen: een datalek wordt voorkomen door zicht te hebben op nut en noodzaak van een verwerking van persoonsgegevens. Daarnaast is risicomanagement nodig om te bepalen wat passende beveiligingsmaatregelen zijn;
- Detecteren: signaleren dat een datalek heeft plaatsgevonden. De organisatie zal maatregelen moeten treffen om vast te stellen dat een inbreuk op de beveiliging heeft plaatsgevonden;
- Opvolgen: als een datalek plaatsvindt dient de organisatie zo snel mogelijk het lek te dichten en het verlies van data beperken. Vervolgens zal via een efficiënt proces het datalek geregistreerd, beoordeeld, afgewogen en mogelijk gemeld dienen te worden. Ten slotte zijn er maatregelen ingericht om te leren van bestaande datalekken.

De eerste twee uitdagingen kunnen feitelijk niet nieuw zijn voor organisaties en horen thuis in het integraal risicomanagement van de organisatie. Cyber Security Assessment (CSA) en Privacy Impact Assessment (PIA) – beide producten van NOREA – bieden handvatten om hier richting in te geven.

De derde is uiteraard wel nieuw waar het gaat om de afwegingen over de meldplicht. De toezichthouder verwacht van organisaties dat zij alles in het werk stellen om te komen tot een transparante en zorgvuldige afweging. Dat vraagt om de juiste voorbereiding, de juiste processen en de juiste expertise. Het kan een complexe materie zijn die vraagt om het inschakelen van kennis die niet binnen de organisatie zelf aanwezig is. Gewapend met die kennis kan dan vanuit eigen kracht een gedegen afweging worden gemaakt. Wie op deze manier omgaat met de meldplicht zal waarschijnlijk ook de in de beoordeling achteraf door de toezichthouder weinig verwijten krijgen. Meer dan ooit is het dus zaak om niet vanuit angst te redeneren.