Jaarcongres KNB

Maak meldplicht datalekken *onderdeel van je notariële praktijk!*

De Wet bescherming persoonsgegevens wordt aangevuld. In de wet wordt een meldplicht geïntroduceerd die moet worden vervuld als er sprake is van een inbreuk op de beveiliging. De verwachting is dat deze 1 januari 2016 van kracht wordt. Waar moeten notarissen rekening mee houden?

TEKST Peter Steeman | BEELD Roel Ottow

De gedachte achter de meldplicht is helder. Iedereen moet erop kunnen vertrouwen dat zijn persoonsgegevens, die vaak in honderden bestanden staan, voldoende worden beveiligd. Datalekken komen sporadisch in het nieuws. Uit onderzoek van het Amerikaanse Ponemon Institute blijkt dat wat de publiciteit bereikt maar het topje van de ijsberg is. Het instituut ondervroeg 388 IT-professionals van Amerikaanse zorgaanbieders. 9 van de 10 ondervraagden gaf aan in de afgelopen 2 jaar te maken te hebben gehad met een datalek, 38 procent van hen rapporteerde zelfs meer dan 5 incidenten. De Nederlandse meldplicht datalekken moet het probleem zichtbaar maken en het bewustzijn vergroten.

TROJAANS PAARD

Slechte beveiliging kan leiden tot een datalek en vervolgens tot misbruik van persoonsgegevens, bijvoorbeeld voor identiteitsfraude. 'Maar ook met goede beveiliging kun je als organisatie met een datalek te maken krijgen', aldus Thomas van Essen, advocaat bij SOLV en gespecialiseerd in ICT-recht. 'Een medewerker kan een USB-stick verliezen of per ongeluk een Trojaans paard binnenhalen, een programma waarmee derden toegang tot je computer krijgen. Voor notariskantoren is dat risico vergelijkbaar met andere bedrijven. Als er informatie op straat ligt, moet de notaris inschatten hoe ernstig dat lek is. Een protocol kan daarbij helpen: hoe kwalificeer je het datalek? Wat zijn de mogelijke gevolgen? Je moet laten zien dat je *in control* bent.'

NADELIGE GEVOLGEN

Het opstellen van een protocol zal veel notariskantoren wel lukken. Wat een verdere voorbereiding op de meldplicht weerbarstig maakt, is dat nog niet alle details zijn uitgewerkt. 'De manier waarop de meldplicht geformuleerd is, laat bijvoorbeeld nog wel wat ruimte voor interpretatie', aldus Van Essen. 'Je moet een datalek melden bij het College Bescherming Persoonsgegevens (CBP) als het lek aanzienlijke kans op of ernstige nadelige gevolgen heeft, en ook aan de betrokkenen als het lek waarschijnlijk ongunstige gevolgen zal hebben voor hun persoonlijke levenssfeer. Bedrijven moeten zelf de afweging maken of er sprake is van ernstige nadelige gevolgen. Na inwerkingtreding van de wetswijziging zal het CBP richtsnoeren opstellen die meer duidelijkheid moeten geven over de daadwerkelijke handhaving van deze wetswijziging. Wanneer er nou precies sprake is van "ernstige nadelige gevolgen voor de persoonlijke levenssfeer van betrokkenen"? Een ander probleem is de onbekendheid. Ik vermoed dat veel notariskantoren nog niet op de hoogte zijn van de meldplicht datalekken. De bewustwording bij bedrijven over een goede beveiliging is niet altijd aanwezig. Dat was ook de kritiek van de Eerste Kamer op het wetsvoorstel. Men was niet onder de indruk van de wijze waarop over de noodzaak van een goede beveiliging van persoonsgegevens is gecommuniceerd.'

SCHADELIJK

Datalekken komen maar sporadisch in het nieuws. Als het wel gebeurt, gaat het meestal om spectaculaire gevallen. Zoals de cyberaanval in 2013 op de kassa's van de Amerikaanse

'Steeds vaker zie je een vorm van cybercrime waarbij het systeem door encryptie op slot wordt gezet'

warenhuisketen Target. De betaalgegevens van 40 miljoen klanten vielen in handen van criminelen. Zo op het eerste gezicht lijkt een meldplicht datalekken vooral bedoeld voor organisaties die veel persoonsgegevens beheren, maar die veronderstelling is niet juist, stelt Hester de Vries, advocaat en partner privacyrecht bij Kennedy Van der Laan.
'Hackers zijn niet alleen geïnteresseerd in bedrijven met grote databestanden. Steeds vaker zie je een vorm van cybercrime waarbij het systeem door middel van encryptie op slot wordt gezet. Dan moet losgeld worden betaald, waarna het systeem van de encryptie wordt verlost. Dat is een risico waar iedere dienstverlener die met persoonsgegevens werkt mee te maken heeft.'
De Wet bescherming persoonsgegevens maakt een onderscheid in persoonsgegevens en bijzondere persoonsgegevens. Onder bijzondere persoonsgegevens worden gegevens over ras, politieke voorkeur, godsdienst en gezondheidsgegevens verstaan. Een notaris beschikt waarschijnlijk niet over bijzondere persoonsgegevens, maar dat betekent niet dat daarmee een datalek door de wetgever als minder schadelijk wordt beoordeeld.
'In een toelichting van de wet staat dat ook financiële gegevens als risicovol gelden. Wanneer persoonlijke informatie over een testament via een datalek bij een notariskantoor in handen van derden komt, raakt dat direct aan de persoonlijke levenssfeer.'

ONVERWIJLD

In het geval van verlies van een USB-stick of een *hack* moet dat 'onverwijld' gemeld worden bij het CBP. Bij mogelijke nadelige consequenties voor de privacybescherming moeten ook de betrokkenen worden geïnformeerd. De Vries: 'Het begrip "onverwijld" betekent in de praktijk binnen 24 uur. Als je na 3 dagen nog niets kunt specificeren, heb je een probleem. Of er daadwerkelijk een boete wordt opgelegd, hangt af van de aard van het lek. Het CBP mag een boete onmiddellijk opleggen als de overtreding opzettelijk is begaan. In de meeste gevallen zal ze eerst een "bindende aanwijzing" geven. Pas als de overtreding blijft bestaan, wordt de boete opgelegd. De maximale bestuurlijke boete die het CBP kan opleggen bij overtredingen is 810.000 euro of 10 procent van de jaarlijkse omzet. In de oude situatie was de hoogte van de boete maximaal 4.500 euro.'
Haar advies aan de notaris: zorg dat de detectie van datalekken onderdeel wordt van je beveiliging. De Vries: 'Veel notariskantoren hebben waarschijnlijk een ICT-partner. Maak het een onderdeel van de dienst die je afneemt. Als je zelf de ICT doet, is het je eigen verantwoordelijkheid. Schakel expertise in op het gebied van beveiliging. Het is niet alleen een kwestie van de juiste specificaties, ook organisatorisch moet je stappen zetten. Wat zijn bijvoorbeeld voorwaarden voor het gebruik van eigen mobiele telefoons? Daar moet over zijn nagedacht.' ■

De rol van de KNB

In de bewustwording van de notaris ten aanzien van datelekken heeft de Koninklijke Notariële Beroepsorganisatie (KNB) haar eigen rol. Zo is er een 'vragenlijst beveiliging persoonsgegevens' ontwikkeld, die aangeklikt kan worden op NotarisNet, het intranet van alle notarissen in Nederland. Daarop staan vragen als: 'Hoe is het gesteld met uw digitale kantooromgeving? Zijn uw bestanden voldoende beschermd tegen toegang van buitenaf? Heeft u beleid voor het beheer van toegangscodes? Voor het gebruik van iPhones en voor thuiswerken? Heeft u heldere afspraken met een serviceprovider?'

EERSTE STAP

'De vragenlijst is een eerste stap', stelt Geert Lekkerkerker, wetenschappelijk adviseur bij de KNB. 'Nu wordt die vragenlijst vooral gebruikt in peer reviews. We zullen later dit jaar met aanbevelingen komen voor de beroepsgroep. Het veiligheidsbewustzijn ten aanzien van werken in de digitale wereld moet wel wat scherper. Notarissen vinden het nog heel gewoon om e-mail te gebruiken voor het verzenden van een ontwerptestament, terwijl je op die momenten in feite onbeveiligd communiceert. Het is voor velen een verrassing hoe kwetsbaar bijvoorbeeld ook een website kan zijn voor hackers. Een professionele dienstverlener als de notaris moet dit op orde hebben.'

Ook op het jaarcongres van de KNB op 2 oktober met als thema 'De notaris in de digitale wereld' zal aandacht aan dit onderwerp worden besteed.