Draaiboek voor datalekken nodig

Slordig omgaan met persoonsgegevens kan leiden tot boete

Een 'datalek' klinkt op zichzelf al eng, maar wordt nog enger als je het moet melden aan een toezichthouder die een boete kan opleggen van maximaal 8,2 ton. Door deze explosieve cocktail van de datalekmeldplicht, die op 1 januari is ingevoerd, was de belangstelling voor het seminar *Privacy en datalekken in de notariële praktijk* van de Koninklijke Notariële Beroepsorganisatie (KNB) enorm. Hier volgen de belangrijkste lessen en tips voor notarissen en hun cliënten.

TEKST Lex van Almelo | **BEELD** Roel Ottow

1 WAT IS EEN DATALEK?

Een datalek is meer dan een computerinbraak. Het is een beveiligingsincident waarbij persoonsgegevens verloren gaan of waarbij het redelijkerwijs niet valt uit te sluiten dat persoonsgegevens onrechtmatig worden verwerkt. Een laptop of telefoon met persoonsgegevens verliezen, is ook een datalek. Een computercrash zonder back-up kan ook een datalek zijn, omdat je daardoor niet meer de beschikking hebt over de gegevens. Computergijzeling valt ook onder de definitie. Daarbij maakt een hacker bestanden op de computer pas weer leesbaar en toegankelijk als hij een paar honderd euro krijgt. Ook werken in de cloud heeft een lekrisico. Al was het maar omdat de gegevens op een server terecht kunnen komen in een land waar de persoonsgegevens minder goed worden beschermd. Zo bewaren programma's als *Sales force*, *Dropbox* en *Peoplesoft* gegevens in de Verenigde Staten. Het beschermingsniveau is daar onvoldoende, zo zei het Europese Hof van Justitie onlangs over het *Safe Harbor agreement*. De Europese toezichthouders onderzoeken nu of het nieuwe *EU-US Privacy Shield* afdoende bescherming biedt.

Dat maakt het er niet gemakkelijker op om langs contractuele weg voldoende privacywaarborgen te bedingen (zie ook punt 6). Is een akte of een kopie naar een verkeerd adres sturen een datalek? Advocaat-hoogleraar Gerrit Jan Zwenne: 'De Autoriteit Persoonsgegevens zegt dat het geen lek is als de brief ongeopend terugkomt, maar als-ie onderweg geopend is wel.' Of het een datalek is als de conceptakte per e-mail wordt verstuurd en wordt onderschept, hangt af van de inhoud. Zwenne: 'Als het burgerservicenummer erin staat wel. Het gaat om de kans op ernstig nadelige gevolgen voor het datasubject.' Of de betrokken cliënt toestemming heeft gegeven voor het onveilig versturen, maakt misschien verschil voor de aansprakelijkheid, maar niet voor de meldplicht.

TIP
Een conceptakte met persoonsgegevens kun je beter beschikbaar stellen via een beveiligd portaal of digitaal dossier dan via de e-mail.

2 WAT ZIJN PERSOONSGEGEVENS?

Als je aan de hand van een gegeven zonder onevenredige inspanning de identiteit van een individu kunt achterhalen, is het een persoonsgegeven. Een kopie van een paspoort is uiteraard een persoonsgegeven, maar het burgerservicenummer en het inschrijvingsnummer bij de Kamer van Koophandel ook. Volgens de Autoriteit Persoonsgegevens zijn een mobiel nummer en een IP-adres eveneens persoonsgegevens, maar een mobiele telefoon of computer die puur dient voor persoonlijk en huishoudelijk gebruik niet.

TIP
Op de website van de Autoriteit Persoonsgegevens staat meer informatie over persoonsgegevens.

3 HOE GROOT IS DE KANS OP EEN DATALEK?

Op het internet staan talloze handleidingen voor hoe je een virus kunt downloaden. Hackers komen de computer binnen met zogenoemde *phishing mails*, waarin je wordt verleid op een link te klikken. Zo'n mail kan eruitzien

als een factuur, maar bijvoorbeeld ook als uitnodiging voor het jaarcongres van de KNB. Ton Oosterwijk van informatiebeveiligingsbedrijf Factor 50 geeft als voorbeeld een zakenrelatie die er ook is ingetuind bij een mailtje dat zogenaamd van Intrum Justitia was. 'Wij hebben het opgelost door een nieuwe harde schijf in de computer te plaatsen en de back-up terug te zetten.'
In de Thalys of een café-restaurant bestaat de kans dat hackers via de open wifi-verbinding alles meelezen wat op het scherm van de iPhone, tablet of laptop verschijnt. Wie met een app de rekening van diner of drank betaalt, loopt het risico dat hackers het wachtwoord achterhalen. Het kan ook zijn dat hackers een wachtwoord onderscheppen via een andere site – cheaptickets.com bijvoorbeeld – en kijken of dat wachtwoord ook werkt bij telebankieren.

TIPS

- Twijfel je aan de betrouwbaarheid van een e-mail, klik dan met de rechtermuisknop op de afzender. Komt het adres niet overeen met het officiële adres van het bedrijf, gooi het dan weg.
- Typ geen wachtwoorden in en verstuur geen vertrouwelijke gegevens als je op een openbaar wifi-netwerk zit.
- Zorg dat je verschillende wachtwoorden hebt, die 'sterk' genoeg zijn. Een sterk wachtwoord bestaat bijvoorbeeld uit de beginletters van een zin en heeft hoofdletters, cijfers en bijzondere tekens. Bijvoorbeeld: IhNMvm2016$eusod (In het *Notariaat Magazine* van maart 2016 stond een uitstekend stuk over datalekken).
- Bewaar alle wachtwoorden versleuteld in een digitale kluis of gebruik een wachtwoordmanager. Dan hoef je maar één (lang) wachtwoord te onthouden. Download de software hiervoor via een officiële leverancier.
- Beveilig de verbinding voor de klanten, bijvoorbeeld met een https://-webadres. Klik op het groene slotje van een beveiligde https://-site als je meer informatie over beveiliging en privacy wilt.
- Update de besturingssoftware van de computer steeds.

4 WAT HOUDT DE MELDPLICHT IN?

Als het beveiligingslek 'ernstig nadelige gevolgen' kan hebben voor de betrokken persoon moet het incident binnen 72 uur worden gemeld bij de Autoriteit Persoonsgegevens. Als het lek 'ongunstige gevolgen' kan hebben voor het datasubject moet je het (ook) melden aan de betrokken persoon. De gevolgen zijn groter naarmate er meer of gevoeliger persoonsgegevens verloren zijn gegaan. Als het gaat om gegevens waarmee identiteitsfraude kan worden gepleegd, is melden geboden. De ledenadministratie van de tennisvereniging valt volgens de Autoriteit Persoonsgegevens echter niet onder de datalekmeldplicht.

TIP
Raadpleeg de website van het Meldloket datalekken Autoriteit Persoonsgegevens.

5 HOE GROOT IS DE KANS OP EEN BOETE?

De maximale boete die de Autoriteit Persoonsgegevens kan opleggen, is 820.000 euro of 10 procent van de Nederlandse omzet. Als (naar verwachting) in mei 2018 de Europese Privacyverordening van kracht wordt, kan de boete oplopen tot 20 miljoen euro of 2 procent van de wereldwijde groepsomzet. Die maxima gelden echter voor grove overtredingen. Voordat de Autoriteit Persoonsgegevens een boete kan opleggen, moet zij eerst een bindende aanwijzing geven. De boete volgt pas als je daaraan niet tijdig voldoet. Gerrit-Jan Zwenne: 'Er worden in 2016 60.000 meldingen verwacht, dus 90 procent van de meldingen wordt niet onderzocht.'

TIP
Bij twijfel toch maar melden. De kans dat de melding gevolgen heeft, is klein.

6 WAT MOET JE ALS NOTARIS ONDER MEER DOEN?

Breng de kwetsbaarheden in kaart met alle medewerkers, maak een draaiboek en oefen alsof er een datalek is. De rollen moeten helder zijn. De notaris moet in de bewerkersovereenkomst afspreken dat de ingehuurde bewerker van de gegevens hem binnen 48 uur informeert over het datalek. De salarisverwerker of de boekhouder in de cloud zijn bewerkers. Zelf is de notaris geen bewerker als hij of zij gegevens aanlevert aan het Kadaster, het Centraal Testamentenregister of Het Centraal Digitaal Repertorium. In de bewerkersovereenkomst moet geheimhouding en adequate bescherming van de gegevens worden geregeld. Jeroen Wittink van Factor 50: 'U hebt het recht om te laten controleren of de leverancier uw gegevens veilig verwerkt.'
Voor het draaiboek is maatwerk nodig. Wittink: 'Hoe zien de risico's er concreet uit? Wie gaat het managen? Wie communiceert erover en wat gaat die persoon zeggen? Als een datalek de wereld in gaat, gaan medewerkers erop reageren via sociale media. Dat moet je niet hebben.' Dagvoorzitter Jolanda Storm (KNB): 'Communicatie is belangrijk. Een datalek kan het hele notariaat raken. De afdeling communicatie van de KNB zal in zo'n geval graag meedenken.'
Jeroen Wittink: 'Zoek de balans, maak er geen rupsje-nooit-genoeg van. Als je het dichttimmert, gaan mensen eromheen.'

TIPS

- Zorg voor een draaiboek en een heldere rolverdeling.
- Breng de risico's in kaart met een *privacy impact assessment*.
- Oefen alsof er een datalek is.
- Controleer of de bewerker de gegevens wel veilig verwerkt.
- Neem de maatregelen op in bestaande protocollen en afspraken.

7 KUN JE JE VERZEKEREN TEGEN DATALEKKEN?

Gedeeltelijk. Je kunt je verzekeren tegen een boete en de kosten van communicatie, naar het datalek zoeken, enzovoort. Verzekeraars stellen verschillende eisen. De KNB kijkt momenteel naar bruikbare producten, zoals aanvullende dekking in de beroepsaansprakelijkheidsverzekering en naar de speciale verzekeringen voor cyberrisico's. De imagoschade voor je kantoor en het notariaat kun je uiteraard niet 'wegverzekeren'.

TIP
Verzeker het risico en zorg dat je aan de verzekeringseisen voldoet.