Baseline
Informatiebeveiliging Notariaat

Kwaliteitshandboek voor informatiebeveiliging in de maak

Als Russische 'trollen' de mailaccountants van de Amerikaanse Democraten kunnen hacken en journalisten de social media-accounts van Tweede Kamerleden, dan is aandacht voor informatiebeveiliging geen luxe. De Stichting Rechtszekerheid Digitaal komt eind maart met een eerste versie van de Baseline Informatiebeveiliging Notariaat. De rijksoverheid, de gemeenten en de waterschappen gingen het notariaat al voor.

TEKST Lex van Almelo | **BEELD** Truus van Gog

'Een incident met de rioleringspompen in een gemeente liet zien dat het mogelijk is om op afstand via internet pompen en vergelijkbare systemen als sluizen en gemalen te hacken. In dergelijke gevallen is ook de fysieke veiligheid van burgers in het geding. De belangrijkste les uit de incidenten is dan ook dat er behoefte is aan een fundamentele oplossing van het informatieveiligheidsprobleem bij gemeenten. De Rijksoverheid gaat eveneens nadere eisen stellen aan de beveiliging van de gemeentelijke informatiehuishouding, bijvoorbeeld als voorwaarde om aangesloten te zijn en te blijven op DigiD. Ook in het onderzoek van de Onderzoeksraad voor Veiligheid naar het DigiNotar-incident is een dergelijk *(sic)* aanbeveling opgenomen. De eerste stap op dit pad is het ontwikkelen van een integrale Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten.' [Uit het voorwoord van de Baseline Informatiebeveiliging Nederlandse Gemeenten – red.]

NATTE VOETEN

De gemeenten hebben al een baseline, net als de rijksoverheid en de waterschappen. Als deze overheidsinstanties zich aan de baselinevoorschriften houden, neemt de kans op natte voeten voor burgers af. De baselines van de overheid zijn een driedelig boekwerk, waarin staat waaraan de organisaties en de systemen moeten voldoen. Deze normen zijn afgeleid van de internationale standaarden voor informatiebeveiliging ISO 27.001 en 27.002. Het bestuur van de Stichting Rechtszekerheid Digitaal (zie kader) heeft de overheidsbaseline toegeschreven op het notariaat. Henk Broekema en Sander Smits zijn de notarissen in dit bestuur.
De Baseline Informatiebeveiliging Notariaat bestaat uit drie onderdelen. De strategische baseline bevat meer de algemene regels en eisen voor organisaties. Zo moet duidelijk zijn wie welke taken en verantwoordelijkheid heeft. In het notariaat is elke notaris verantwoordelijk voor informatiebeveiliging, ook op een kantoor met meerdere notarissen. Henk Broekema: 'Dat is nu ook al zo, dus in dit opzicht verandert er niet veel.' Sander Smits: 'Maar soms is het raadzaam om het nog even op te schrijven en expliciet te maken.'
Algemene normen op kantoorniveau zijn te vinden in het tactische of operationele deel van de baseline. Specifieke normen voor bijvoorbeeld de omgang met wachtwoorden, voor specifieke software en voor werken in de cloud komen in de losse hoofdstukken waarin de algemene normen praktisch worden uitgewerkt. De hoofdstukken met de praktische uitwerking zullen stapsgewijs worden ingevoerd, afhankelijk van de haalbaarheid, de urgentie voor de beroepsgroep en de capaciteit van de Stichting Rechtszekerheid Digitaal, de Koninklijke Notariële Beroepsorganisatie (KNB) en de softwareleveranciers. Sander Smits: 'Het is niet zinvol en haalbaar om de hele baseline in een keer over de beroepsgroep uit te storten.' De baseline is geen boekwerk dat je van A tot Z gaat lezen, zegt Henk Broekema: 'Het is een soort kwaliteitshandboek voor het notariaat, waaraan elk kantoor zijn eigen kantoorboek kan aanpassen.'

STICKER

In de praktijk blijkt zelfs zoiets voor de hand liggends als een wachtwoordenbeleid nogal eens vatbaar voor verbetering. In de baseline komt bijvoorbeeld te staan hoe sterk wachtwoorden moeten zijn en hoe vaak medewer-

kers moeten wisselen van wachtwoord.
Henk Broekema: 'Er zijn ook kantoren waar een plakkertje op de computer zit met de inlognaam en het wachtwoord. Hackers kunnen dat stickertje misschien niet zien, maar bij een inbraak in het kantoor is dit niet veilig.'
In de baseline zullen ook normen staan voor hardware en software waarmee medewerkers zich kunnen identificeren en kunnen inloggen op het systeem. Om datalekken te voorkomen, zullen kantoren verder een beleid moeten hebben voor het meenemen van eigen telefoons en laptops waarop vertrouwelijke persoonsgegevens staan. Verlies of diefstal van gegevensdragers is immers een veelvoorkomend datalek. (Zie kader Datalekken.)

Kun je de normen uit de baseline negeren?
Sander Smits, lachend: 'Dat kan altijd.
De normen die wij opstellen geven in eerste instantie aan waar het naartoe gaat. De KNB kan dit proces versnellen door de regels bindend te maken en ze geheel of gedeeltelijk de status van Verordening te geven, dan wel op te nemen in een reglement. In dat geval kunnen de normen ook onderdeel worden van de audits. De verwachting is dat de baseline op den duur ook in het tuchtrecht een rol zal spelen om te bepalen wat een redelijk handelend notaris zou doen.'

Is voldoen aan de baseline een soort keurmerk?
Henk Broekema: 'Niet de baseline, maar de notaris is het keurmerk. De baseline zorgt ervoor dat de notaris dat keurmerk blijft houden.'

Nooit meer DigiNotar-incidenten dankzij de baseline?
Sander Smits: 'Je kunt informatielekken nooit helemaal voorkomen. Zelfs Google, Apple en Microsoft blijken kwetsbaar. Behalve lekken voorkomen, is het ook belangrijk de schade zo veel mogelijk te beperken als er wel iets misgaat.'
Henk Broekema: 'Overigens was DigiNotar toen het misging al in handen van een buitenlandse partij en lange tijd niet meer zo notarieel, zeker niet op het operationeel gebied.'
Sander Smits: 'Het zou dus niet helemaal terecht zijn om het DigiNotar-debacle te associëren met het notariaat.'

VEGETARIËRS

Als pen en blocnote zijn opgeborgen en de armen in de jassen worden gestoken, uiten Smits en Broekema hun zorgen over het politieke klimaat in bijvoorbeeld Polen. Daar houdt de inlichtingendienst burgers in de gaten en geeft de machtigste politicus van de regeringspartij in één adem aan dat hij niet alleen een hekel heeft aan etnische minderheden en homoseksuelen, maar ook de pest heeft aan fietsers en vegetariërs. Smits en Broekema willen maar zeggen dat misbruik van persoonsgegevens dichterbij is dan je denkt en persoonsinformatie dus veilig opgeslagen moet zijn. Smits denkt dat het notariaat hier een belangrijke rol bij kan vervullen.
'Maar alleen als het notariaat zelf voldoende controle kan houden over de data.' ■

DATALEKKEN

Na een klein jaar heeft de meldplicht datalekken bijna 5.500 meldingen opgeleverd. De meest voorkomende lekken zijn volgens de Autoriteit Persoonsgegevens:

- iemand die inzage krijgt in de persoonsgegevens van anderen, bijvoorbeeld in een klantenportaal;
- verlies van een USB-stick of andere hardware met onversleutelde persoonsgegevens;
- diefstal van een laptop of smartphone met persoonsgegevens;
- poststukken met persoonsgegevens die niet aankomen of geopend terugkomen;
- een e-mail met persoonsgegevens die terechtkomt bij de verkeerde ontvanger.

Een variant op het laatste soort lek is dat je de verkeerde informatie naar de goede ontvanger stuurt. Dat overkwam de medewerker van een notariskantoor toen zij abusievelijk de verkeerde conceptakte van levering toestuurde aan een cliënt. Daarin stond onder meer het paspoortnummer van een andere cliënt. De notaris meldde het datalek keurig bij de Autoriteit Persoonsgegevens, die overigens niet precies bijhoudt hoeveel meldingen afkomstig zijn van het notariaat. De meerderheid van de meldingen komt uit de gezondheids- en welzijnssector (29 procent), de financiële dienstverlening (17 procent) en het openbaar bestuur (15 procent). De specialistische zakelijke dienstverlening nam 3 procent van de meldingen voor haar rekening.

RECHTSZEKERHEID DIGITAAL

Sander Smits en Henk Broekema zijn voorzitter respectievelijk secretaris/penningmeester van de Stichting Rechtszekerheid Digitaal. Naast hen zit ook Bert Mulder, lector Informatie, Technologie en Samenleving bij de Haagse Hogeschool, in het bestuur. Deze, door de KNB opgerichte maar onafhankelijke, stichting ontwikkelt:

- generieke richtlijnen voor informatiebeveiliging;
- richtlijnen voor specifieke toepassingen, zoals de uitgifte van digitale ID's door notarissen.