Jaarcongres KNB

Digitale evolutie vergt ook waakzaamheid

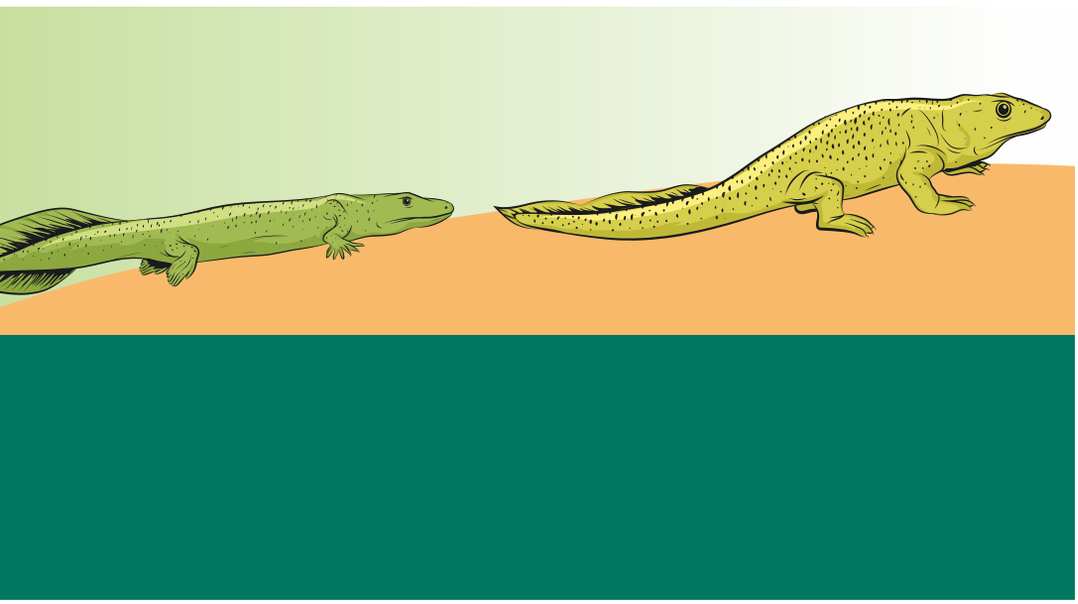
Als notarissen pootjes moeten ontwikkelen om op het digitale droge te kunnen lopen, dwingt de evolutie hen ook tot aanpassing van de zintuigen, zodat zij zich kunnen verdedigen tegen de roofdieren in deze 'habitat'. In de digitale wereld, waaraan het jaarcongres van de Koninklijke Notariële Beroepsorganisatie (KNB) in oktober is gewijd, wemelt het van de kansen en risico's.

TEKST Lex van Almelo | **BEELD** Shutterstock

'De notaris verandert van habitat; hij is als het ware een vis die pootjes moet ontwikkelen op het droge', zei organisator Lineke Minkjan bij de aankondiging van het jaarcongres van 2 oktober over de 'Notaris in de digitale wereld'. De boodschap is duidelijk: om te overleven, moeten notarissen zich aanpassen aan de moderne omgeving.
Wat moet de notaris bijvoorbeeld doen met software, auteursrechten of socialmedia-accounts in nalatenschappen? 'Je kunt een socialmedia-account niet zo maar opheffen, want er kunnen filmpjes of muziek in staan of andere dingen die geld waard zijn', zegt Jelger de Kroon van de Stichting IT-Notaris. De stichting is een door de KNB geaccrediteerde organisatie van gespecialiseerde IT-notarissen en bevordert de juridische deskundigheid op het gebied van IT en recht. Er zijn op dit moment zeventien notariskantoren aangesloten, waaronder DuretTrip Notarissen – het kantoor waar De Kroon partner is. IT-notarissen leveren juridische oplossingen voor problemen in de digitale samenleving. Hoe kan een gemeente bijvoorbeeld bewijzen dat een gewraakte vergunning op een bepaalde dag was gepubliceerd op de gemeentelijke website? Door een notaris dagelijks kopieën van de website te laten maken. Voor zover De Kroon weet, zijn er nog geen gemeenten die van deze 'aantoonbaarheidsservice' gebruikmaken. Maar één van de IT-notaris-kantoren levert deze dienst wel voor de rijksoverheid.

BRONCODE

Boven het digitale droge kunnen regenwolken drijven als notariskantoren of andere bedrijven hun bedrijfsprocessen laten verlopen via de cloud. 'Een adviesbureau had zijn gegevens, formats en financiële administratie volledig in de cloud staan. Daarvoor deed het zaken met een Belgisch bedrijf, dat de diensten inkocht bij derden. Een leverancier van het Belgische bedrijf schortte op een bepaald moment zijn verplichtingen op. Of het nu om een faillissement ging of iets anders, daar ben ik niet achter gekomen', zegt Reinout Rinzema (Ventoux Advocaten). 'Het adviesbureau kon geen rekeningen meer versturen, omdat het geen toegang meer had tot de facturen-administratie. Het bureau heeft niet goed naar het contract gekeken.'
Een andere klant van Rinzema's kantoor, een bedrijf dat webdiensten verleent, zag de lancering van zijn app bijna in rook opgaan. De app zou verkocht gaan worden in de App Store, maar een paar kleine foutjes vertraagden de release. Toen het bedrijf contact zocht met de programmeur stuurde die een sms terug met de boodschap dat hij van de curator niets meer mocht doen nu zijn werkgever failliet was. Uiteindelijk mocht de programmeur verder werken nadat de webdienstverlener de curator 5000 euro had betaald. De dienstverlener had het idee dat zij moest betalen voor iets dat al van haar was. Bedrijven hebben vaak alleen een recht om software te gebruiken. Als zij de software willen aanpassen, hebben zij de broncode nodig. Programmeurs of hun werkgever hebben het auteursrecht op de broncode.



SOFTWARE *ESCROW*

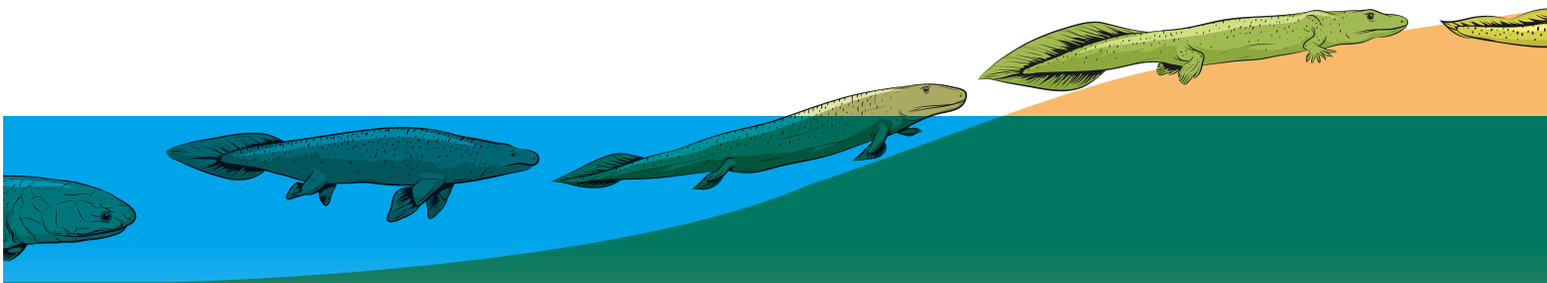
Eén van de manieren om de continuïteit te waarborgen, is software *escrow*. Daarbij spreekt een gebruiker met de programmeur of de software provider af dat de broncode van de software in bewaring wordt gegeven bij een *trusted third party*. Deze vertrouwde derde mag de broncode onder gelimiteerde voorwaarden afgeven aan de gebruiker.
Volgens Jelger de Kroon kan de notaris de rol van bewaarder goed vervullen. Daarbij brengt de notaris ook in beeld waar de gegevens en de software van het notariskantoor of hun cliënten zich bevinden en wie nu precies de rechthebbende op de software is.
Reinout Rinzema is er niet van overtuigd dat de notaris een grootse toekomst wacht als een bewaarder van broncodes. 'De notaris is gewend om een statische toestand vast te leggen, maar de software is dynamisch. Als bewaarder moet je voortdurend controleren of de gebruiker nog door kan werken met de software. Daarvoor heb je technische kennis nodig. De notaris kan zich die natuurlijk eigen maken, maar drijft dan wel ver af van zijn *core business*. Er zijn gespecialiseerde bedrijven die al jaren aan software *escrow* doen en ik denk dat het heel moeilijk is voor de notaris om nog een voet aan de grond krijgen op die markt.'
Maar volgens De Kroon bieden IT-notarissen met hun *escrow*regeling juist 'de meest maximale bescherming die op dit moment in de markt wordt aangeboden'. Vanwege het titelonderzoek én omdat het auteursrecht op de software gedeeltelijk wordt overgedragen. IT-notarissen laten technische experts de broncode controleren. 'Bovendien worden de broncodes periodiek geherdeponeerd.'

INFORMATIEBEVEILIGING

Zoals veel ondernemers hebben ook notarissen vaak geen idee waar hun data en hun software nu eigenlijk precies zijn opgeslagen en wat de risico's zijn van die onbekende woon- en verblijfplaats. Wanneer cliëntgegevens in de cloud staan, is het niet ondenkbaar dat zij zijn opgeslagen op één of meerdere servers buiten de Europese Unie. Is de privacy daar wel voldoende beschermd? Jolanda Storm van de KNB: 'Kunnen lokale autoriteiten dan toegang krijgen tot de gegevens? In Nederland is daar een protocol voor, maar bestaan zulke waarborgen in het buitenland ook?'
De KNB probeert notarissen bewust te maken van de risico's in de digitale wereld, onder meer met een vragenlijst op NotarisNet, het intranet van alle notarissen in Nederland. 'Hebt u op uw kantoor al een beveiligingsbeleid voor persoonsgegevens? Weet u hoe uw software beveiligd is en wat u kunt doen in geval van een calamiteit?' Tot nu toe hebben 'te weinig' notarissen de vragenlijst ingevuld, vindt Storm.
De KNB wil het risicobewustzijn onder meer aanwakkeren met een workshop over informatiebeveiliging, die wordt gegeven door Rob Koch van cybercrimepreventiebedrijf Sebyde. 'Bij de discussie over de beveiliging van vertrouwelijke gegevens gaat het meestal alleen over de techniek. Maar als je de risico's wilt inperken, gaat het ook om de mens en de organisatie', zegt hij.

GRATIS WIFI

Zo moet een organisatie er meteen voor zorgen dat een vertrokken medewerker niet meer kan inloggen op het bedrijfsnetwerk. Koch: 'Oud-medewerkers zijn de ergste hackers en boze oud-medewerkers de allerergste. Hackers zijn niet meer de zestienjarige jongen die bij wijze van hobby probeert ergens binnen te komen. Het gaat om professionele organisaties die systematisch en op grote schaal zoeken naar zwakke plekken in websites.'



'Als je de risico's wilt inperken, gaat het ook om de mens en de organisatie'

Met zogenoemde *phishing mails* verleiden zij medewerkers om op een link te klikken en daarmee vertrouwelijke gegevens prijs te geven. Die gegevens kunnen zij gebruiken om iemand vroeg of laat geld afhandig te maken. Officieel mogen medewerkers natuurlijk geen privémails beantwoorden via het bedrijfsnetwerk. Maar in de praktijk gebeurt dat natuurlijk toch, zegt Koch.
Smartphones en tablets zijn een risicofactor als medewerkers die gebruiken om in te loggen op het bedrijfsnetwerk of bij de bank. De dochter van Koch gaat nog weleens met vriendinnen eten, waarbij eentje de rekening betaalt en de anderen ter plekke hun deel van de rekening overmaken. Koch raadt het af om het wifi-netwerk van het café of restaurant te gebruiken. 'Laat er eentje pinnen en de rest de bedragen pas thuis overmaken. Het is voor een hacker heel gemakkelijk om met een router van 60 euro – die hij bijvoorbeeld in een fietstas voor het café of restaurant stopt – een eigen netwerk op te zetten. Als mensen daarop inloggen, kan de hacker alles uitlezen. Als je het wifi-netwerk van een café of restaurant wilt gebruiken, controleer dan altijd even of dat netwerk inderdaad van het café of restaurant is.'
De tandarts van Rob Koch dacht klantvriendelijk te zijn door wachtende patiënten zijn wifinetwerk beschikbaar te stellen. Koch wees op de risico's en adviseerde hem regelmatig de wachtwoorden te veranderen. Inmiddels is de wifi-service van de tandarts uit de lucht.
Notariskantoren en andere bedrijven moeten volgens Koch een informatiebeveiligingsbeleid op papier zetten, waarin staat hoe de organisatie omgaat met alle risico's. Zo moeten medewerkers hun computer bijvoorbeeld vergrendelen als zij naar het toilet gaan en uitzetten als zij naar huis gaan. En uiteraard nooit zomaar persoonsgegevens prijsgeven als iemand daar telefonisch of per mail om vraagt. Verder moeten zij heel goed uitkijken met usb-sticks, omdat die niet zelden *malware* bevatten. Koch: 'Ook mensen hebben een beveiligingsupdate nodig. Zet security daarom steeds op de agenda.'

WAAKZAAMHEID

Niet alleen de KNB hamert op alertheid. '*Be vigilant*' zette de Engelse Solicitors Regulation Authority eind april boven een oproep tot waakzaamheid. De aanleiding voor de oproep was een klein kantoor dat bij het transport van vastgoed slachtoffer werd van criminelen, die inloggegevens voor de bankrekening buit hadden gemaakt in telefoongesprekken. Eind vorig jaar waren ook vier andere kantoren het doelwit van bankfraudeurs. 'De fraudeurs zijn zeer geraffineerd in hun aanpak en hun script laat hen klinken als of zij echt zijn wie zij zeggen te zijn', waarschuwt de Engelse toezichthouder.
Drie weken later meldde *The Telegraph* een nieuwe *bank scam*. Paul en Ann Lupton verkochten via solicitor Perry Hay & Co een appartement in Zuid-Londen voor 340.000 pond (471.000 euro). Twee dagen voor het transport kregen zij een e-mail van Perry Hay & Co met het verzoek details door te geven over de bankrekening waarop de koopsom kon worden overgemaakt. De Luptons verstuurden de gegevens van hun Barclay-rekening. De mail werd onderschept door fraudeurs, die Perry Hay vervolgens als Luptons een e-mail stuurden met het verzoek de eerder verzonden e-mail te negeren en het bedrag over te maken op een andere bankrekening. Dat deed de solicitor. Barclay blokkeerde de valse bankrekening, nadat de fraudeurs daar al 62.000 pond (86.000 euro) vanaf hadden gehaald. Volgens Peter Hay heeft zijn kantoor geen fout gemaakt. ■