April 2015

Geheimhouden

Met het digitaliseren van de samenleving komt ook de vraag naar beveiliging van vertrouwelijke gegevens. Zo zorgen advocaten voor geheimhouding in een digitale wereld.

Nathalie Gloudemans-Voogd

Bij contactgegevens op de website van advocaat Ot van Daalen staan niet alleen telefoonnummer en e-mailadres, maar ook een PGP-code. PGP staat voor *Pretty Good Privacy* en hoort bij een manier om e-mails te versleutelen. Snappen cliënten het wel als ze een *public PGP key* op de website zien staan? 'Ik heb het mijn cliënten nog nooit hoeven uitleggen,' lacht Van Daalen. Kennelijk trekt Van Daalen, die in 2009 digitale burgerrechtenorganisatie Bits of Freedom oprichtte en sinds 2014 weer privacyrechtadvocaat is met zijn eigen kantoor Digital Defence, een clientèle die beveiligde communicatie begrijpt en belangrijk vindt. Als oud-programmeur weet Van Daalen ook meer van IT-beveiliging dan de gemiddelde advocaat. 'Soms mail ik versleuteld met andere advocaten. Ze downloaden dan wel het programma, maar hebben bijvoorbeeld niet het juiste besturingssysteem. Dan kan encryptie heel onhandig zijn.'

Vertrouwelijkheid is een kernwaarde van de advocatuur en de geheimhoudingsplicht van gedragsregel 6 vloeit daar uit voort. Aparte regels voor vertrouwelijkheid bewaren in het digitale tijdperk zijn er niet. Er is bijvoorbeeld geen verplichting om versleuteld te e-mailen, terwijl elektronische post in het algemeen bekendstaat als onveilig communicatiemiddel. Hoe kunnen advocaten vertrouwelijkheid bewaren in de digitaliserende wereld?

Versleuteling van e-mail leeft niet echt in de advocatuur, ziet Claudia Heemskerk, operationeel manager bij Lexxyn Groep, dat ICT-oplossingen voor de juridische praktijk biedt. 'Er zijn er een paar die wat met encryptie doen, maar het overgrote deel heeft het niet geregeld.'

Een rondvraag langs een aantal kantoren levert een versnipperd beeld op. Zo verstuurt eenpitter Van Daalen wel vaak versleutelde e-mails. Deze slaat hij ook beveiligd op; hij heeft in zijn kantoor een eigen server staan. Ook e-mails vanuit het middelgrote Bird & Bird (privacyrechtspecialist en hoogleraar Recht in de informatiemaatschappij Gerrit-Jan Zwenne is een van de partners) worden soms versleuteld verstuurd, vertelt Dave van den Berg, IT-manager bij de Haagse vestiging. 'Maar niet altijd. Wel hebben we techniek tussen onze servers en internet zitten. Dat filtert en beveiligt het e-mailverkeer,' zegt Van den Berg. Ook Bird & Bird heeft eigen mailservers.

Bij het grootste advocatenkantoor van Nederland, De Brauw, staat standaard *Transport Layer Security* (TLS) aan, een cryptografisch protocol om communicatie over een computernetwerk te beveiligen. 'Hiermee kunnen we e-mail beveiligd vanaf onze mailserver naar een andere mailserver sturen, als die andere partij ook TLS ondersteunt,' vertelt De Brauws IT-manager Jeroen Winkel. De Brauw voorziet voor de e-mail ook andere soorten van encryptie aan, zoals S-MIME en PGP. 'Een *end point to end point* encryptie zoals S-MIME PGP is voor een kantoor als De Brauw en haar cliënten onpraktisch,' legt Winkel uit. 'Bij e-mailcommunicatie met tien geadresseerden moeten er tien keer tien sleutels worden uitgewisseld. Met de cliënten die wij hebben, met hooggeplaatste bestuurders van

grote bedrijven, kan het voorkomen dat iemand die vorm van encryptie niet aan de praat krijgt en dan werkt het helemaal niet.' E-mail beveiligd opslaan is ook onhandig voor dossiervorming bij grote teams; elke advocaat die niet de oorspronkelijk geadresseerde van een versleutelde e-mail was, kan deze niet ontcijferen. '*Server to server* beveiliging zoals met TLS is voldoende en het scheelt in de administratie en snelheid van het proces,' zegt Winkel.

Encryptie is één van de honderden manieren om vertrouwelijkheid te bewaren in een digitale advocatuurlijke praktijk. Een andere maatregel die bijvoorbeeld De Brauw heeft genomen, is het instellen van een eigen *security officer*. Hij verzorgt voorlichting aan het personeel en de partners en denkt mee bij IT-wijzigingen. Ook voert het kantoor een batterij aan standaard beveiligingswerkzaamheden uit. 'We voeren rigoureus elke *security patch* door die partijen als Microsoft uitgeven. Dat kost wel wat tijd, maar daar zijn we heel strikt in,' vertelt Winkel. De Haagse locatie van Bird & Bird op zijn beurt heeft het ISO/IEC 27001:2013 beveiligingscertificaat. 'Wij zijn volgens BSI (dienst voor de beveiliging van informatietechnologie, *red.*) het enige advocatenkantoor in Nederland die dit heeft. Het betekent dat wij serieus nadenken over beveiliging; er is een hele audit geweest voordat we het certificaat kregen. Elke drie jaar worden we gecontroleerd. Ons kantoor in Engeland zelfs elk jaar,' vertelt Van den Berg. Het ISO-certificaat noemt Bird & Bird pitchtes. 'Als klanten vragen hoe wij met data omgaan, kunnen we laten zien dat we gegevens veilig opslaan en houden.' Bij De Brauw werkt IT wel volgens de ISO 27001 beveiligingsnorm, maar het kantoor heeft het certificeringsproces nog niet officieel doorlopen. 'Het is vooral een papieren norm,' vindt Winkel. 'Eigenlijk zeg je dat je hebt opgeschreven hoe je beveiliging invult, maar dat alleen garandeert geen veiligheid.'

Van Daalen:
'Ik snap wel dat de overheid wil digitaliseren, maar ze zet daarmee ook de deur open voor veiligheids-problemen'

De IT markt ontwikkelt doorlopend nieuwe producten opdat advocaten veilig kunnen werken. Heemskerk van Lexxyn Groep vertelt bijvoorbeeld over eigen portals waar cliënten en advocaten veilig met elkaar kunnen communiceren. De Brauw werkt ook met cliëntenportalen. 'Maar wij zien het vooral als een tool om efficiënter met cliënten samen te werken aan documenten die op één plek staan en niet heen en weer gemaild hoeven te worden.' Bij Bird & Bird heet het cliëntenportaal OCS, naar *Online Client System*. 'OCS vergemakkelijkt de uitwisseling van belangrijke informatie tussen onze cliënten en Bird & Bird via een beveiligde en geprivilegieerde website. Ook houden we zo belangrijke documenten op een geordende wijze direct beschikbaar,' legt IT-manager Van den Berg uit.

Ook voor werken op afstand binnen een kantoor worden tools ontwikkeld. I-FourC, dat advocatenkantoren helpt om archieven te digitaliseren, ontwikkelde onlangs een app waarin ook lopende dossiers eenvoudig kunnen worden opgehaald. De dossiers zijn ook offline en beveiligd beschikbaar. Bird & Bird werkt met een vergelijkbaar systeem, vertelt Van den Berg: 'Als onze advocaten een dossier nodig hebben en niet op kantoor zijn kunnen ze met een laptop of tablet ons document management system versleuteld van buitenaf benaderen.'

Bewustwording

Ook eenpitter Van Daalen werkt vooral digitaal. Toch poneerde hij bij het ICT-congres PLEIT in oktober 2014 dat advocaten soms beter terug konden gaan naar papier. 'Er kan minder misgaan met papier. Het is een begrijpelijke trend om alles te digitaliseren, maar het kent ook nadelen. De techniek om te beveiligen is niet goed ontwikkeld,' zegt Van Daalen, die naast advocaat ook onderzoeker privacy en security is bij het Instituut voor Informatierecht van de Universiteit van Amsterdam. 'Ik snap wel dat de overheid wil digitaliseren, maar ze zet daarmee ook de deur open voor veiligheidsproblemen.' Dat kan volgens Van Daalen grote gevolgen hebben: 'Kijk naar DigiNotar; dat was in eerste instantie bedoeld voor notarissen. Toen DigiNotar gehackt werd, lag het hele notariële verkeer stil.'

PGP

Pretty Good Privacy (PGP) is een van de meest gebruikte vercijfermethodes op internet. Binnen PGP hebben gebruikers een eigen *public key* en een geheime sleutel, die nodig zijn om versleutelde berichten te verzenden en ontvangen. PGP hanteert namelijk een vorm van asymmetrische cryptografie: er is een sleutel voor vercijferen en een voor ontcijferen van informatie.
Versimpeld gezegd werkt PGP zo. Een gebruiker stelt een bericht op en PGP comprimeert dat. Daarna maakt het systeem een sessiesleutel aan, waarmee de tekst vercijferd wordt. Met de publieke sleutel van de ontvanger wordt deze sessiesleutel ook weer versleuteld. De ontvanger krijgt daarna beide delen en kan met zijn of haar eigen geheime sleutel de sessiesleutel ontcijferen. Met de sessiesleutel kan de tekst vervolgens worden omgezet in begrijpelijke taal.

Van Daalen pleit ervoor dat digitale beveiliging even grote aandacht krijgt als fysieke beveiliging. Volgens Heemskerk is beveiliging in de digitale wereld niet anders dan in de fysieke wereld: 'Je laat je dossiers niet slingeren in de trein en dus ook niet op onveilige digitale platforms.' Het is duidelijk dat veranderingen niet vanzelf gaan, stelt Van Daalen. 'Het zal niet uit de markt zelf komen. De grote kantoren zullen alleen standaard gaan versleutelen als hun cliënten erom vragen, en dat doen ze niet. De kleinere kantoren volgen de grote.' Volgens Van Daalen helpt het niet dat de overheid vaak fouten op dit gebied maakt. 'Dan zegt de overheid dat telefoonnummers van advocaten niet getapt worden en dan blijkt dat toch te gebeuren. Zo ontstaat wantrouwen.'

'Een groot risico dat wij lopen met onze internationale praktijk is een inbreuk op onze systemen door buitenlandse mogendheden, of partijen die daaraan verbonden zijn,' legt De Brauws IT-manager Winkel uit. Deze partijen zullen overigens wel hun best moeten doen om dat voor elkaar te krijgen, stelt Winkel. 'Maar er zijn partijen waar ook wij een maatje te klein voor zijn om ons tegen te beschermen.' In Amerika is men al een stap verder: daar komen de federale inlichtingendienst FBI en advocatenkantoren bij elkaar om informatie uit te wisselen en elkaar te waarschuwen. 'Waarom ontwikkelen we hier niet ook een platform voor beveiligingskwesties?' Volgens Winkel zou daar een rol voor de Nederlandse orde van advocaten (NOvA) kunnen liggen.

Op congressen waar IT in de advocatuur aan bod komt, zoals PLEIT of De Rechtspraak van Morgen over het project Kwaliteit en Innovatie (KEI), laten sommige advocaten weten dat zij strengere regels van de NOvA op IT-vlak verwachten. Nu zijn er geen specifieke voorschriften voor werken in een digitale omgeving en beveiliging. Volgens de NOvA is dit gedekt door de gedragsregels en de Advocatenwet. Wel heeft de raad van Europese Balies, de CCBE, in 2012 richtlijnen opgesteld voor werken in de *cloud*. Deze richtlijnen zijn vooral bedoeld om aandacht te vestigen op verschillende overwegingen bij gebruik van *cloud computing* diensten. De CCBE adviseert bijvoorbeeld te overwegen een cloud-service provider te kiezen die in de EER gevestigd is; zo verminderen

Heemskerk:
'Beveiliging in de digitale wereld is niet anders dan in de fysieke wereld'

advocaten het risico dat hun provider gegevens moet afstaan aan de nationale autoriteiten. De CCBE geeft ook tips voor de beoordeling van contracten met leveranciers van cloud computingdiensten. Strengere regels van de NOvA zijn niet nodig, volgens Winkel van De Brauw. 'Die zullen toch neerkomen op een inspanningsverplichting. Onze reputatie is reden genoeg voor De Brauw om met beveiliging bezig te zijn, of de NOvA daar nu regels voor schept of niet,' zegt hij. Wel ziet Winkel ruimte voor de NOvA om meer aan voorlichting op dit onderwerp te doen.

Informatieverschaffing, daar ziet ook privacyrechtadvocaat Van Daalen een rol voor de Orde. Of er strengere regels vanuit de NOvA zouden moeten komen, durft hij niet te zeggen. 'Ik denk niet dat advocaten hun e-mails altijd moeten versleutelen. Het is afhankelijk van het risico dat je loopt. En daar moet je je als advocaat van bewust zijn. Het blijkt nu bijvoorbeeld dat Van der Valk in Twente gastenlijsten aan de politie afgeeft. Dus ook als je ergens afspreekt, ben je niet veilig.' Ook Heemskerk pleit voor meer bewustwording: 'Dat je op een terras via onbeveiligde wifi je Facebookpagina checkt is tot daaraan toe. Maar denk erover na als je daarna je werkmail checkt. Weet welke risico's je loopt.' Bij Digital Defence denkt Van Daalen zeker na over de risico's, al betekent dat niet hij altijd e-mail versleutelt of alles op papier doet. 'Maar als cliënten niet met encryptie willen werken, vertel ik hen wel: "Wees je bewust dat het onveilig kan zijn. Als je iets belangrijks wilt vertellen, kom dan langs op kantoor."' Van PGP naar F2F dus: *Face to Face* kan ook een goede beveiliging zijn. «

Tips van experts

Gegevens van cliënten geheimhouden en beveiliging van data vraagt verschillende methoden. Een paar tips van beveiligingsexperts om vandaag al mee te beginnen:

- Voer trouw en direct alle updates uit, hoe irritant dat ook kan zijn. Softwarebedrijven geven niet voor niets deze *security patches* uit. Hackers komen binnen via niet-bijgewerkte software.
- Controleer de internetverbinding als u op een andere locatie dan kantoor werkt. Open wifi-netwerken zijn gevaarlijk. Als u uw mailt checkt, kunnen hackers op eenvoudige wijze meekijken. Zo kunnen ze vertrouwelijke gegevens onderscheppen.
- Wis netwerken waar u buiten kantoor verbinding mee heeft gemaakt, bijvoorbeeld als u van wifi bij uw cliënt gebruikmaakt. Uw telefoon hoeft niet gehackt te worden om uit te lezen welke wifi u heeft gebruikt. Zo geeft u misschien ongewild prijs waar u geweest bent.
- Gebruik in plaats van een wachtwoord een 'wachtzin': gebruik hoofdletters, kleine letters, symbolen en cijfers. Of nog beter: werk met tokens, die een unieke code genereren waarmee u kunt inloggen, of een elektronische identiteitskaart.