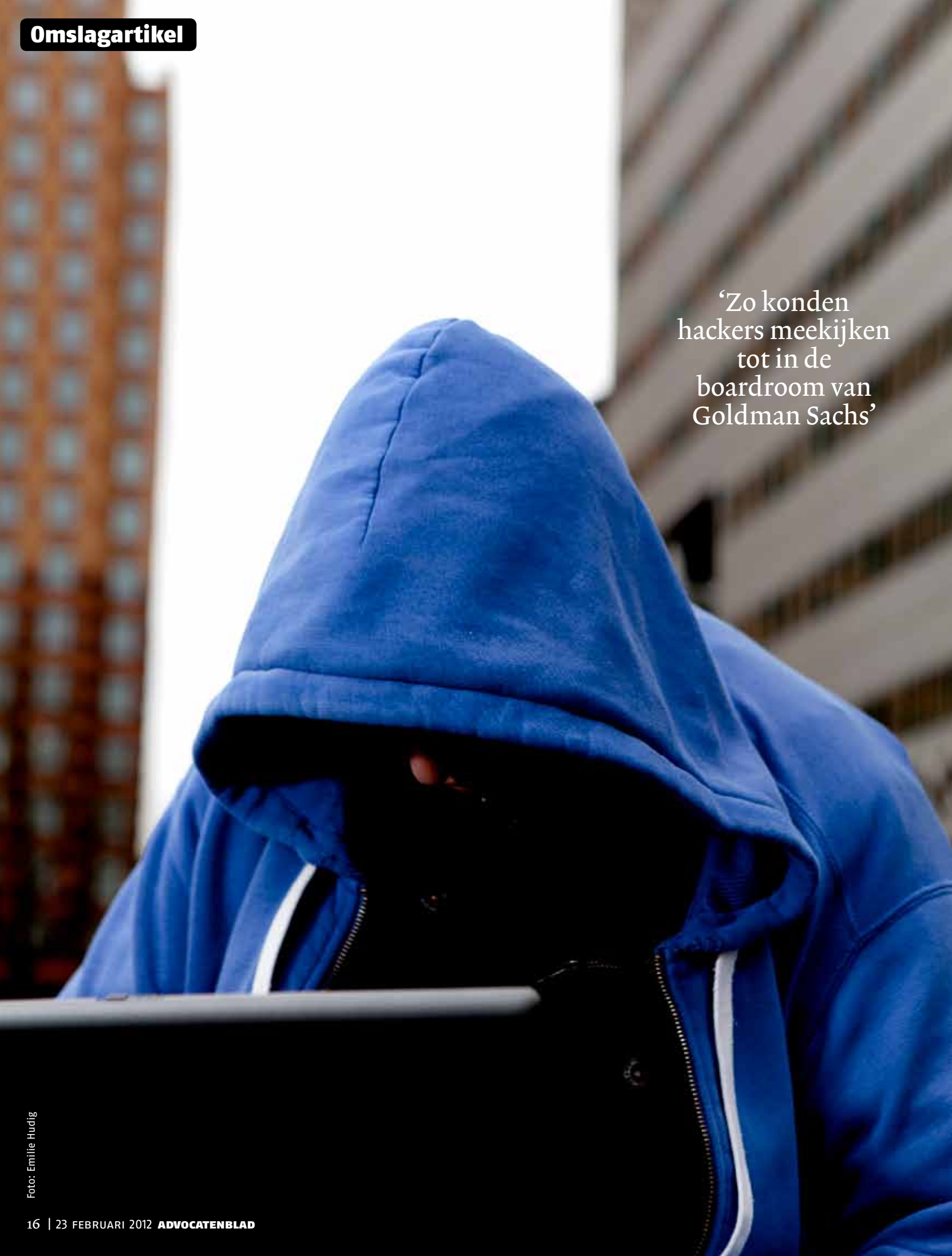

‘Zo konden hackers meekijken tot in de boardroom van Goldman Sachs’

Foto: Emilie Hudig

Hackers azen op advocaatgeheimen

Slecht nieuws voor wie denkt dat de advocatuur na het DigiNotar-drama in rustiger vaarwater terecht was gekomen. Niet alleen beseffen hackers steeds meer wat er te halen valt bij advocaten, u bent zelf de zwakste schakel in het veiligheidssysteem.

Door Mark Maathuis

De tijd dat de meerderheid van kantoormedewerkers aangaf zijn wachtwoord te willen ruilen voor een chocoladereep is helaas voorbij. Niet omdat men sindsdien zoveel bewuster geworden is van online risico's, maar omdat hackers allang niet meer zo diep in de buidel hoeven te tasten. Dankzij de steeds verder digitaliserende werkplek, de vervaagde grenzen met het online privébestaan en de voorspelbaarheid van wachtwoorden behelst het kraken van een wachtwoord vaak niet meer dan het combineren van wat Facebook- en e-mailgegevens. Daarnaast denken Nederlanders over het algemeen dat het wel goed zit met hun online veiligheid. Zo bleek onlangs uit een onderzoek dat Microsoft in 27 Europese landen liet uitvoeren dat Nederland in vergelijking minder goed beveiligd is. Weliswaar heeft het merendeel een antivirusprogramma, maar slechts vijftig procent checkt bijvoorbeeld de betrouwbaarheid van een site als men daar een betaling doet en meer dan driekwart heeft voor elk online account hetzelfde wachtwoord.

Onder advocaten, bij wet beschermde hoeders van kostbare informatie, zouden deze cijfers lager moeten zijn. Maar ook dan lopen zijn niet minder risico, integendeel. Naast de trofeewaarde lijken hackers zich steeds beter de financiële waarde te realiseren van informatie die bij advocaten te halen is. Dat ondervonden bijvoorbeeld vier Canadese advocatenkantoren eind vorig jaar toen hackers hun computers doorzochten op informatie over ophanden zijnde overnames van clienten. Rond diezelfde tijd werdbekend dat een Amerikaans advocatenkantoor slachtoffer was geworden van cyberaanvallen vanuit China terwijl het kantoor een cliënt bijstond in een miljardenclaim tegen de Chinese overheid. En als het hackerscollectief Anonymous er daadwerkelijk in geslaagd is begin februari dossiers te stelen van Amerikaanse soldaten die verdacht worden van oorlogsmisdaden heeft men ook daar goud in handen.

> 'Driekwart heeft voor elk online account hetzelfde wachtwoord'

Op de parkeerplaats

Gezien de dodelijke pr rondom een gehackt advocatenkantoor is het aannemelijk dat deze voorbeelden slechts het topje van de ijsberg vormen. Helaas draagt dat doodzwijgen bij aan het in stand houden van de meeste digitale gevaren. Dat een gewaarschuwd mens voor twee telt is handig, zeker als je bedenkt dat datzelfde mens in elk veiligheidssysteem de zwakste schakel is. Op dat gegeven baseerde 's werelds beroemdste hacker Kevin Mitnick – bekend van onder andere inbraken in de computers van het Pentagon – zijn hacktechniek *social engineering*. En het zou weleens deze methode kunnen zijn die 'in het kader van advocaten boys interessant is,' aldus 'Jan Peters', IT-specialist die zijn echte naam niet geeft vanwege zijn vorige carrière toen hij als professioneel hacker bij een softwarefabrikant de systemen van klanten testte.

Wie *social engineering* associeert met dubbele identiteiten, plaksnorren of andere *Mission Impossible*-rekwisieten, maakt het zichzelf te moeilijk, aldus Peters. 'Hoe hack je een advocatenkantoor? Maak een oude USB-stick met daarop een verborgen hackprogramma zoals een *keylogger* (een programma waarmee toetsaanslagen en zelfs muisbewegingen van een computergebruiker kan worden geregistreerd, red.) Gooi hem – of een paar – op de parkeerplaats van een advocatenkantoor op de grond. Goeie kans dat een secretaresse, partner of medewerker het ding ziet, oppraapt en denkt: Hé, eens kijken wat daar op staat! Op het moment dat het ding in een computer van het advocatenkantoor wordt gestoken, slaat de *keylogger* alle toetsaanslagen op en mailt ze automatisch naar de hacker. Alle wachtwoorden, dossiers, confidentiële informatie en, nog belangrijker, systeeminformatie van de computers en het netwerk van het advocatenkantoor zijn dan bij de hacker bekend. Hij kan vervolgens rustig alles manipuleren en zijn eigen sporen uitwissen voordat hij verder naar zijn volgende projectje gaat.'

Soms is zelfs een strategisch geplaatste USB-stick al te veel moeite, zo maakte Rapid7 onlangs pijnlijk duidelijk. Deze Amerikaanse online veiligheidsspecialist struinde in opdracht van een aantal advocatenkantoren via een speciaal geschreven programmaatje in een paar uur ongeveer drie procent van internet af. Daarbij stuitte men op zo'n 5000 video conference systemen waarbij iedereen die het maar wilde, kon inloggen omdat de systemen bewust buiten de beschermende (en vertragende) firewall geplaatst waren; ook werden inkomende verzoeken om aan de »

conferentie deel te nemen vrijwel zonder enige controle geaccepteerd. Zo kon men meekijken in vergaderzalen van advocatenkantoren, in de gesprekruimte van een gevangenis en zelfs in de boardroom van Goldman Sachs.

STORK 3 en 4

Dichter bij huis is het drama rondom DigiNotar een teken aan de wand. Nadat afgelopen oktober hackers 247 frauduleuze certificaten hadden kunnen aanmaken, besloot toenmalig minister Piet Hein Donner het vertrouwen in het bedrijf op te zeggen. Een stap die de Orde ook nam, met alle gevolgen van dien. Zo moest men op zoek naar een nieuw authenticatiemiddel zodat de veiligheid van de digitale communicatie met de balie en de Raden voor de rechtspraak en Rechtsbijstand gegarandeerd kon blijven worden.

De site van de Orde werd ondertussen ook kritisch bekeken, zegt Jan Leliveld, als lid van de Algemene Raad medeverantwoordelijk voor dat nieuwe authenticatiemiddel. ‘We hebben een hacker ingeschakeld voor een stresstest. Vervolgens hebben wij de processen doorgelopen en onderzocht waar we welke informatie digitaal uitwisselen met advocaten. Tot slot: wat vinden wij, los van wat anderen doen, het gewenste veiligheidsniveau?’ Conclusie van deze risicoanalyse is de keuze voor een middel met beveiligingsniveau STORK 3. ‘Dat betekent dat je iets moet weten, bijvoorbeeld een wachtwoord, iets moet hebben, bijvoorbeeld een pasje, voordat je iets kunt,’ zegt Leliveld.

Voor STORK 4, het niveau waarop de Rechtspraak gaat opereren en dat extra inspanningen vraagt, is niet gekozen, zegt Leliveld. ‘Vooropgesteld: iedere advocaat die dat wil, kan zelf voor STORK 4 kiezen, de processen zullen daarop zijn ingericht. Maar de Orde wil dit vooralsnog niet verplicht stellen aan de advocaat. Een dergelijk STORK 4-niveau is veel duurder. Daarnaast werken de vele advocaten die er zijn met minstens zoveel verschillende systemen. Als daarin aanpassingen moeten plaatsvinden, zijn dat er meteen heel veel.’ Bovendien stemmen de andere partijen met wie digitale informatie uitwisseling plaatsvindt, zoals de Rechtspraak ermee in dat de Orde de komende drie jaar op dit niveau opereert, zegt Leliveld, ‘tijd die nodig is om te zien of dit de richting is die voor de definitieve oplossing opgaat. We verwachten dat het nieuwe authenticatiemiddel voor 1 oktober 2012 gebruikt kan worden. Die planning is wel ambitieus, maar er wordt ook door veel medewerkers hard aan gewerkt.’

Archief als kunststukje

Niet alleen hackers, maar ook softwarebedrijven lijken de advocatuur te hebben ontdekt. Volgens Jeroen Strik, directeur van Iron Mountain Benelux, is de aandacht voor de sector mede te wijten aan Nederlandse en Europese wetgeving die in navolging van de Amerikaanse steeds strenger wordt. ‘Wij zijn een Amerikaans bedrijf en je weet wat ze zeggen, “wat daar gebeurt, gebeurt hier over een paar jaar.” Daarnaast speelt de Autoriteit Financiële Markten, waar veel partijen mee te maken hebben, een belangrijke rol in deze ontwikkeling.’

Keerzijde van het omzetten van het archief en alle andere papierstromen in enen en nullen is wat Strik overdigitalisatie noemt. ‘Iron Mountain is groot geworden met fysiek documentbeheer. Er staat hier zo’n 130.000 kilometer aan papier opgeslagen dus we weten waar we het over hebben. Vroeger met papieren archieven waar niemand bij kon was het credo “bewaar maar”, terwijl het eindeloos bewaren van digitale dossiers risico’s kan opleveren. Ook wordt op veel plekken het fysieke archief als een kunststukje onderhouden. Vraag je naar het digitale archiefbeleid, dan blijft het stil. Terwijl men wel op het hart gedrukt wordt de deur dicht te doen, blijven digitale deuren vaak gewoon openstaan.’

Een situatie die zal voortduren, aldus Strik, ‘totdat er een keerpunt in de bewustwording optreedt. Het is toch onbegrijpelijk, maar als je iets in een envelop stopt, loop je alles nog even na voordat je hem dichtplakt; en een mailtje met een paar pdf’s stuur je zo door. Digitaal is natuurlijk makkelijk en snel maar met het risico van ongebreidelde kopieën en verlies van authenticiteit. Daar moet je als bedrijf over nadenken. Zo hebben we net een enquête gehouden onder Amerikaanse advocatenkantoren en daaruit bleek dat 28 procent van de ondervraagde kantoren paperless was. Heel mooi, maar tegelijkertijd bleek dertig procent überhaupt geen digitaal beleid te voeren. Voor hen geldt, dat zo-

lang er geen grote ongelukken gebeuren, IT tijdens het partneroverleg niet op de agenda hoeft te staat.' Terwijl er zonder directe digitale crisis ook al genoeg te bespreken is, aldus Strik. 'Moeten we dossiers opslaan in de cloud? Wat is dat überhaupt? Hoe toon je aan dat niemand er meer aan kan komen? Of dat niemand er aan gezeten heeft? Wat kun je nog als de cloud een uur of zelfs een dag uit de lucht is? Vragen die je jezelf moet stellen omdat je als uitbestedende partij eindverantwoordelijke bent en een advocaat die zijn dossier kwijt is, dat is een nachtmerrie.'

'Een zekere ontdigitalisering is aanstaande'

'Niet meer van deze tijd'

De advocatuur zou juist daarom weleens aanleiding kunnen geven tot de volgende ontwikkeling, meent Strik, wijzend op trendwatcher Adjiedj Bakas. Deze schrijft in zijn rapport *De grote stagnatie begint nu echt: trends voor 2012* dat door het toegenomen aantal digitale incidenten er 'een zekere ontdigitalisering aanstaande is. Bedrijven zullen de opslag van hun kwetsbare informatie *off the grid* willen verzorgen – zelfs data-opslag op papier zal weer terrein winnen.' Maar met minder radicale stappen is de veiligheid ook al te verbeteren, meent Strik. 'Op advocatenkantoren bestaat bijvoorbeeld een systeem om een back-up te maken van alle digitale documenten. Die bestanden kunnen digitaal gestuurd worden, maar wij kunnen die kopie ook fysiek komen halen. Dat kun je niet meer van deze tijd noemen, maar is het onveilig opbergen van informatie dat dan wel?' «

Foto: Sjoerd van der Hucht

Jan Leliveld