Foto: Tjörven Verstraete

Pas op voor de cybercrimineel

Banken krijgen cyberaanval na cyberaanval te verduren. Ook advocatenkantoren blijken een interessant doelwit voor datadieven en afpersers. Maar extra beveiliging vinden kantoren niet nodig. Hoe komen criminelen binnen en wat zijn de gevaren?

Juriaan Mensch

Is het oorlog? Als we het taalgebruik van sommige cybersecurity-experts horen dan lijkt het wel zo. In elk geval zullen luchtvaartmaatschappij KLM, overheidsinstelling DigiD en de banken ING, Rabobank en ABN AMRO de afgelopen maanden wel hebben ervaren als een oorlogssituatie. Zij waren (meermaals) slachtoffer van cyberaanvallen. En dat roept de vraag op of advocatenkantoren goed tegen dergelijke aanvallen goed zijn beschermd.

Dat de dreiging van een cyberaanval ook reëel is voor advocaten blijkt uit onderzoek in het buitenland. In februari van dit jaar publiceerde de Amerikaanse internetbeveiliger Mandiant een rapport dat cyberaanvallen vanuit China op Noord-Amerikaanse bedrijven in kaart bracht. Bij vier advocatenkantoren bleek te zijn ingebroken in de systemen en werden mogelijk vertrouwelijke gegevens gestolen.

Mandiant omschreef advocatenkantoren als een aantrekkelijk doelwit voor hackers, omdat er over vele honderden, soms duizenden bedrijven informatie is te vinden. Een ander onderzoek, het *2013 Verizon Data Breach Investigations report*, laat zien dat van 47.000 incidenten die in negentien landen werd onderzocht, accountants, advocaten, consultants en soortgelijke dienstverleners in bijna een kwart van de gevallen doelwit waren.

Engeland reageerde op het Mandiant-rapport. Daar werden in maart veertig partners van Engelse topkantoren uitgenodigd voor een besloten briefing van het Centre for the Protection of National Infrastructure en het beveiligingsagentschap GCHQ. De Engelse Orde van Advocaten waarschuwde kantoren die internationaal opereren en zich bezighouden met IP-gerelateerde zaken. Datadieven zouden vooral uit zijn op informatie over onderhandelingsstrategieën bij overnames, procedures en intellectueel eigendom.

Zijn Nederlandse kantoren ook op hun hoede? Tien ondervraagde Nederlandse advocatenkantoren laten geen verhoogde staat van paraatheid zien naar aanleiding van het recente nieuws over cybercriminaliteit. Het betreft internationaal opererende kantoren, van middelgroot tot niche door het hele land. Op advocatenkantoor De Brauw Blackstone Westbroek na, wilde liever niemand bij naam worden genoemd. Een enkeling wilde helemaal niet meewerken. ‘Te gevoelig onderwerp.’

De meeste kantoren meldden dat ze al genoeg aan beveiliging doen. Datalekken zijn nauwelijks aan de orde geweest, stellen ze. Eén kantoor geeft een incident toe, maar dan ‘zonder noemenswaardige consequenties’. Geen van de kantoren zegt te maken te hebben gehad met directe aanvallen op de IT-systemen. Wel melden ze dat klanten de laatste tijd meer interesse tonen voor de gebruikte beveiliging.

Afpersing

Volgens Mattijs van Ommeren, security-consultant van Alcyon Security en medeinitiator van de IT-securityconferentie Alt-S, spreekt diegene die zegt nooit doelwit van hackers te zijn geweest niet of niet helemaal de waarheid. ‘Of het is onopgemerkt gebleven. En dat is natuurlijk gevaarlijker.’

Terughacken

Justitie krijgt meer ruimte voor bestrijden van cybercrime

Minister van Justitie Ivo Opstelten (VVD) neemt cybercrime op de korrel. Zijn wetsvoorstel geeft justitie de bevoegdheid om binnen te dringen in een computer, router, gedeelde server of cloudserver waarvan een verdachte gebruikmaakt. Justitie mag dan alle gegevens overnemen die noodzakelijk zijn voor de bewijsgaring. Ook de cloud, dus het geheugen buiten de eigen computer, mag straks worden gehackt. Nederland neemt dan (extraterritoriale) rechtsmacht aan en breidt zo de jurisdictie uit naar alle cloudservers waar ze bij kunnen, ook die in het buitenland. De vraag is hoe de internationale gemeenschap daarop reageert. Dit kan buitenlandse partijen ertoe brengen om ook onbeperkt onze systemen aan te vallen met alle risico's op een digitale wapenwedloop van dien.

Van Ommeren is een *White Hat hacker*, ook wel ethische hacker genoemd. De *Black Hat hackers* zijn de criminele tegenstanders die Van Ommeren voor zijn cliënten buiten de deur probeert te houden. Hij wordt door het midden- en kleinbedrijf, door overheden en door grote financiële instellingen ingehuurd voor veiligheidsadvies en voor penetratietesten waarbij hij zelf digitaal probeert in te breken. En inbreken lukt hem, mits hij genoeg tijd krijgt, vrijwel altijd.

Wat ziet Van Ommeren momenteel als de grootste bedreigingen? 'Afpersing is tegenwoordig in de mode. Criminelen infecteren massaal computers en gijzelen deze door ze ontoegankelijk te maken. Tegen betaling kan de eigenaar dan weer toegang tot zijn eigen computer verkrijgen. Verder zien we een opmars in DDoS-aanvallen: het platleggen van websites en diensten.' Het is zeer goed mogelijk dat recente aanvallen op websites van banken, die het internet- en pinbetalingsverkeer platlegden, pogingen tot afpersing zijn. Deze acties zijn per slot van rekening door niemand opgeëist.
De security-expert verwijst naar Russische websites waar geïnteresseerden voor duizend dollar een maand lang een botnet – een netwerk van geïnfecteerde computers om een aanval mee uit te voeren – kunnen huren om een website naar keuze plat te leggen. 'Afpersing is moeilijk hard te maken,' zegt Van Ommeren. Maar hij kent de tactieken van cybercriminelen en weet dat er een bepaald niveau van frauderisico bij de banken wordt geaccepteerd.

Het is volgens Van Ommeren een simpele afweging na een hack of simpelweg een verloren laptop, waarbij er belangrijke informatie in verkeerde handen is gekomen: hoeveel is de reputatieschade, het verlies van vertrouwen en de schade aan de client waard? Dat heeft een prijs, en criminelen weten dat. Van Ommeren signaleert ook een verschuivende trend: van het stelen van creditcardgegevens naar diefstal van informatie die op andere manieren kan worden gebruikt of verkocht.

Verder is de toenemende opslag van geheimhoudersgegevens in de zogeheten cloud, de verzamelnaam voor externe opslag van informatie, een zorg. 'Je bent als klant niet de enige op die server. Zit er een zwakke plek in de cloudapplicatie, dan kan men zich toegang verschaffen en dan niet alleen tot één klant, maar tot honderden en soms wel duizenden klanten,' zegt Van Ommeren. 'Het kan ook zijn dat jij jouw virtuele server goed hebt beveiligd, terwijl een andere gebruiker dat niet zo goed doet. Men kan via die weg binnendringen tot aan het hostsysteem van de cloudprovider. En zich vervolgens toegang verschaffen tot jouw data.'

Informatie is wel vaak versleuteld, maar Van Ommeren zegt dat het niet veel uitmaakt als 'de sleutel gewoon onder de deurmat' te vinden is. Hackers vinden de sleutel tot de code veelal in gehackte systemen.

Zwakste schakel

De virtuele datarooms in de cloud, die gevoelige informatie bevatten over bijvoorbeeld overnames, zijn beveiligd met niet meer dan een gebruikersnaam en wachtwoord, geeft een kantoor dat anoniem wil blijven toe. Van Ommeren vindt het gebruik van alleen wachtwoorden 'absoluut onvoldoende voor toegang tot gevoelige informatie'. Van Ommeren: 'Mensen zijn altijd de zwakste schakel en honderd procent veilige systemen bestaan niet. Dus elke organisatie moet zich afvragen: wat is mijn digitale inventaris me waard? Wat is de schade die ontstaat als die niet toegankelijk is, of beschadigd raakt dan wel wordt ontvreemd? Met welke investeringen kan ik risico's reduceren? Beveilig iets wat een dubbeltje waard is niet met een kwartje,' zegt Van Ommeren.

De overheid werpt zich op als beschermheer. De Algemene Inlichtingen- en Veiligheidsdienst noemt cybercrime en spionage als speerpunt voor 2013. Minister van Justitie Ivo Opstelten (VVD) wil verregaande bevoegdheden voor de opsporingsdiensten in de wet verankeren met zijn Wetsvoorstel computercriminaliteit. 'Terughacken' klonk de stoere oplossing van Opstelten (zie ook het kader 'Terughacken' op deze pagina). Van Ommeren is er kritisch over.

De overheid heeft volgens hem een kennis- en informatieachterstand. 'Zaken werden tot nu toe opgelost met hulp van particuliere partijen, nog te weinig door het daartoe opgerichte Team High Tech Crime zelf. De opsporingsdiensten beschikken nog over onvoldoende capaciteit. Zo krijgen particuliere beveiligingsbedrijven verregaande hackbevoegdheden. Alsof parkeerwachten vuurwapens krijgen. In feite vertoont dit overeenkomsten met het wegnemen van het geweldsmonopolie bij de staat.'

Van Ommeren is sceptisch over het voorkomen van misbruik van deze macht. 'Er is in de wet geregeld dat een rechter-commissaris beslist wanneer zo'n middel ingezet wordt. Ik weet uit ervaring hoe weinig affiniteit de meeste juristen met techniek hebben. Een rechter-commissaris zal snel ja zeggen als een opsporingsambtenaar of zelfs adviseur binnentreding noodzakelijk acht. In eerdere zaken is het OM teruggefloten door de rechter. Bij onrechtmatig bewijs, verkregen uit illegaal opgeslagen kentekenbeelden bijvoorbeeld. Het is mogelijk dat de privacy van mensen door de nieuwe plannen ernstig wordt geschaad, dus ik vind het vrij gevaarlijk.' «