De noodzaak van goede internetbeveiliging

‘Help, we zijn gehackt!’

Hackers proberen in te breken in de digitale bestanden van overheden, bedrijven en burgers. Steeds vaker worden ook notariskantoren belaagd, waarbij het risico van datalekken groot is. ‘Pak de ICT-beveiliging integraal aan’, luidt daarom het advies.

TEKST Jolanda aan de Stegge | BEELD Truus van Gog

Sinds medio vorig jaar weet notaris Karelsen meer van het ransomvirus dan hem lief is. Een medewerker opende een zipbijlage die bij een mailtje was gevoegd en even later bleken honderdduizenden digitale bestanden van het kantoor van buitenaf versleuteld. Dit virus heet niet voor niks het ‘losgeldvirus’: tegen betaling van een paar duizend euro in bitcoins zou de afzender de bestanden weer vrijgeven, stond in een bericht. De in allerijl opgeroepen automatiseerder legde het ICT-systeem van het kantoor plat, leegde dat en plaatste een back-up terug voorzien van de nieuwste firewalls en geüpdatete beveiligingen. Karelsen: ‘Dankzij een goede back-up kon onze automatiseerder alles terugzetten, anders was betalen onze enige optie geweest. Wij kwamen er met een sisser vanaf.’

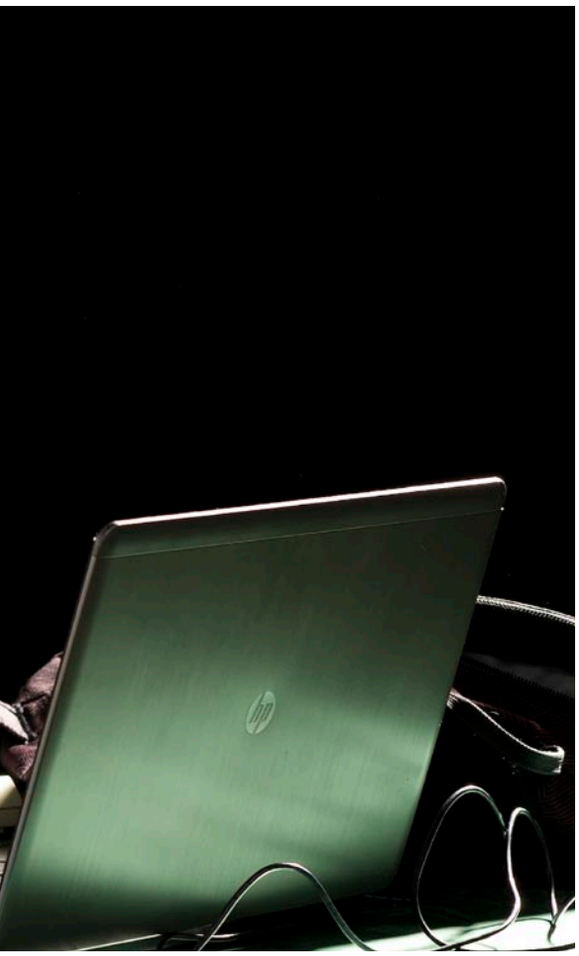
VERTROUWENWEKKENDE MAIL

Het kantoor van kandidaat-notaris Wieman ondervond meer last van een cyberincident. Het hele bedrijf werkt in de cloud. Op kantoor zelf staan geen fileservers: dit is volledig uitbesteed en ook de beveiliging was up-to-date, veronderstelde men. Eind oktober ontvingen alle kantoormedewerkers een mail vanaf het eigen office-info-mailadres. ‘Wil je even kijken naar deze bijlage? Dankjewel’, luidde de begeleidende tekst, waar een Word-bestand bij zat. Al stond er geen e-mailhandtekening onder, het zag er vertrouwenwekkend uit en meerdere mensen klikten het open. Binnen een paar uur raakten alle bestanden waar de betreffende medewerkers toegang toe hadden versleuteld. Wieman: ‘Het ging over vrijwel alle dossiers van 2008 tot 2014. Wie ergens op klikte, kreeg de instructie: betaal zoveel bitcoins, dan geven wij de sleutel vrij.’ De cloudprovider werd onmiddellijk aan het werk gezet om de schade te beperken. Omdat elke nacht een back-up wordt gemaakt, dacht iedereen optimistisch: dit kost hooguit het werk van één dag. Een illusie, het bleek te gaan om een gloednieuw virus dat op het moment van de aanval nog niet detecteerbaar was door de geavanceerde virusscanner. Het zorgde ervoor dat elke back-up vastliep op het moment dat hij werd teruggezet. Gespecialiseerde bedrijven werden ingeschakeld, maar het virus was slimmer dan de experts.

Na een zenuwslopende week vol stress bleek dat vooral oude dossiers waren aangetast. Uiteindelijk lukte het een back-up van drie maanden eerder te installeren. In de tussentijd sloeg iedereen zijn werk voor de zekerheid zowel lokaal op als in de cloud. Wieman: ‘Het was heel vervelend. Onze cloudprovider heeft er zeker zestig uur werk aan gehad. Nu – zeven maanden later – worden we er nog soms mee geconfronteerd. Af en toe stuiten we op een leeg dossier, omdat er waarschijnlijk iets niet helemaal goed is gegaan met het terugzetten van de back-up. Dan plaatst onze provider dat individuele dossier weer terug.’

DATALEK MELDEN

Toch hadden beide notariskantoren in zekere zin mazzel: deze virussen legden een ontoegankelijk schild om hun documenten, maar de hackers konden niet bij de persoonlijke gegevens van hun cliënten en de akten. Er was dus geen sprake van een datalek, waarbij derden de beschikking krijgen over vertrouwelijke informatie, met alle gevolgen van dien. Sinds 1 januari 2016 verplicht de Wet bescherming persoonsgegevens (Wbp) overheden, organisaties en bedrijven om serieuze datalekken te melden.
Omdat het notariaat grossiert in privacygevoelige informatie en intellectueel eigendom dient het zich krachtig te beschermen



‘Data worden wel “het nieuwe goud” genoemd’

tegen cybercriminaliteit, zegt Gerard de Weerd. ‘100 procent voorkomen, kun je een aanval niet, maar je kunt het cybercriminelen wel moeilijk maken.’ Als unit manager bij Ilionx is hij verantwoordelijk voor de business information security. Zijn team helpt overheden, organisaties en bedrijven zich weerbaarder te maken tegen cyberincidenten en -aanvallen.

CREDITCARDNUMMERS

Als je kantoor is gehackt, moet je een deskundig bedrijf inschakelen en nooit betalen, antwoordt hij beslist, want hij kent genoeg voorbeelden waarbij na betaling de versleuteling *níét* werd opgeheven. De motieven en methoden van hackers lopen uiteen. ‘Sommigen willen geld, anderen zijn op zoek naar persoonsgegevens (creditcardnummers, wachtwoorden en inlogcodes) om te verhandelen: data worden wel “het nieuwe goud” genoemd. Weer anderen zoeken naar staatsgeheimen of militaire informatie. Het gaat om intelligente en creatieve mensen die continu bezig zijn hun systematiek en aanvallen te verbeteren.’
Een hacker weet wat het bedrijfsleven doet, dat is zijn business. Hij gaat op onderzoek uit via alle virtuele informatiebronnen die hij kan vinden. Overal plaatst hij cameraatjes en onderzoekt waar hij gaatjes kan maken, waar hij *ransomware* kan achterlaten.
Dat nestelt zich in een systeem en sluist informatie naar de afzender. Op die manier verkrijgt de hacker veel informatie, waarmee hij uiteindelijk zijn slag slaat.

PRIVACYGEVOELIG

Vanwege alle privacygevoelige gegevens is het notariaat een aantrekkelijk doelwit voor hackers. Daarom pleit Gerard de Weerd voor een integrale aanpak van de beveiliging. ‘Informatiebeveiliging moet je als een vanzelfsprekend onderdeel borgen in het bedrijfsbeleid en moet zich richten op mensen, processen en techniek. Bekijk de bedrijfsprocessen, maak risicoanalyses, neem maatregelen en stel bijvoorbeeld voor medewerkers gouden regels op: zo doen wij dit in ons kantoor. Mocht er onverhoopt toch ooit sprake zijn van een datalek, dan kun je de Autoriteit Persoonsgegevens laten zien welke stappen er zijn genomen om lekken te voorkomen.’
Het menselijke aspect acht hij van groot belang. ‘Het heeft geen zin de nieuwste technologische beveiliging te installeren als medewerkers bijvoorbeeld akten ongecodeerd per e-mail verzenden, zoals maar al te vaak gebeurt.
En wees niet naïef: criminelen richten zich op zwakke schakels en proberen soms medewerkers om te kopen.’ Hij doelt op politiemol Mark M., die essentiële informatie doorspeelde naar criminelen.

VOORKOMEN

Op de eerdergenoemde notariskantoren zijn na de cyberincidenten de nodige maatregelen getroffen. Bij kandidaat-notaris Wieman wordt nagedacht over de vragen: moet iedereen op kantoor toegang hebben tot alle gebieden op de server? En: moeten we wel helemaal overgaan op digitale akten? Zijn collega’s en hij waren in oktober dolblij dat de papieren akten nog gewoon in de kluis lagen. Notaris Karelsen: ‘Je kunt je zo goed mogelijk beveiligen, maar dit kun je niet voorkomen. Zelfs het Pentagon wordt gehackt, terwijl die beveiliging honderden miljoenen bedraagt. Je zult moeten accepteren dat er soms zal worden ingebroken, ook in de toekomst. Dat neemt niet weg dat elk kantoor zich zo goed mogelijk dient te beschermen.’ ■

Om privacyredenen zijn de namen van notaris Karelsen en kandidaat-notaris Wieman gefingeerd.

Cybercriminaliteit levert criminelen inmiddels meer op dan de ‘gewone’ criminaliteit. Het leidt op jaarbasis tot een schadepost van tien miljard euro. Hiervan wordt 75 procent via hacking weggehaald bij het bedrijfsleven, 15 procent bij de overheid en 10 procent bij de burger. Bedrijfsspionage via hacking is een van de meest voorkomende vormen van schade voor het bedrijfsleven. Daar komt bij dat Nederland voor hackers een aantrekkelijk land is als *stepping stone*. Vanwege de dichte virtuele infrastructuur en goede koppeling komen cybercriminelen betrekkelijk gemakkelijk van het ene netwerk in het andere.