

De kwaal en het middel

Hacken is niet alleen lucratief voor criminelen, maar ook voor cyberexperts.

Toen binnen zes maanden drie relaties van mij slachtoffer werden van een hack en ik voor de tweede keer aan tafel zat bij een van de bekendste cybersecurityfirma's van ons land, realiseerde ik me dat cybersecurity zowel een steeds groter probleem als big business aan het worden is. Gelukkig had mijn vriend Fred, het recentste slachtoffer van de Akira-ransomware, een verzekeringspolis. Eén tip: zet die vooral niet in de cloud of op je harde schijf, want het eerste waar naar hackers op zoek gaan is een polis. En als ze die polis hebben, dan ben je aan de beurt.

In het gesprek dat ik met de verzekeraar voerde, vertelde die dat ze op dit moment meer uitkeren aan losgeld voor hackers dan aan andere shades. Groepen als Cactus en Akira zijn nu marktleiders. Dit zijn professioneel geleide bedrijven, met handboeken die voorschrijven hoeveel korting hackers maximaal mogen geven en welk percentage van de omzet ze moeten vragen aan een onderneming die gegijzeld is. Ze hebben software waarmee je binnen-dringt bij bedrijven en verstrekt licenties aan hackers. Die zetten bedrijven op slot en staan een deel van het losgeld af aan de organisatie. Een verzekeraar verleent slachtoffers altijd een 'voorlopige dekking' en

verwijst door naar een van de twee leidende cybersecurityexperts van het land. Ik dacht dat we in de advocatuur stevige tarieven hadden, maar deze experts rekenen 550 euro en buiten kantooruren zelfs 1100 euro per uur. Misschien gek, maar meestal worden bedrijven niet gehackt tijdens kantooruren. 'Aan de dood en de liefde wordt geld verdiend', zei mijn vader altijd. Daar kan hacken aan worden toegevoegd. En dan beginnen de onderhandelingen met, zoals cyberexperts dat noemen, de TA oftewel de *threat*

**VERZEKERAARS GEVEN
BONUSSEN AAN HUN
MEDEWERKERS BIJ NIET-
UITGEKEERDE BEDRAGEN.
OPPASSEN DUS!**

actor (lees: crimineel). Je krijgt te maken met iemand die twintig jaar ervaring heeft als onderhandelaar bij de politie en wiens motto is: aangezien de verzekeraar toch betaalt, kun je maar beter gewoon de vraagprijzen bieden. Als ik één ding heb geleerd van de drie dossiers die ik behandeld heb, dan is het dat de vraagprijs een vraagprijs is. Een cybersecurityfirma verstookt rustig 50.000 tot 100.000



euro per week en aan het eind van de rit is het nog spannend of de verzekeraar uitkeert. Die geven immers bonussen aan hun medewerkers bij niet-uitgekeerde bedragen. Oppassen dus!

In de casus van mijn vriend betaalden we minder dan de helft van wat de ervaren onderhandelaar van de door de verzekeraar ingeschakelde expert adviseerde. En aan het eind van het traject kwam de aap uit de mouw. Naast de uurtarieven, een risico-opslag van 3,5 procent over het losgeld en btw kwam er nog een extra vergoeding op tafel voor de cybersecurityfirma: 5000 euro voor 'risico'. Op mijn vraag welk risico de adviseur liep en of dit niet al verdisconteerd was in zijn uurtarief, kreeg ik geen duidelijk antwoord. Op mijn aanbod om dat risico weg te nemen door middel van een vrijwaring werd bits geantwoord: 'Dan betaal je de bitcoins toch zelf?' Zo is de een z'n dood de ander z'n brood. En resteert de vraag wat erger is: de kwaal of het middel? •