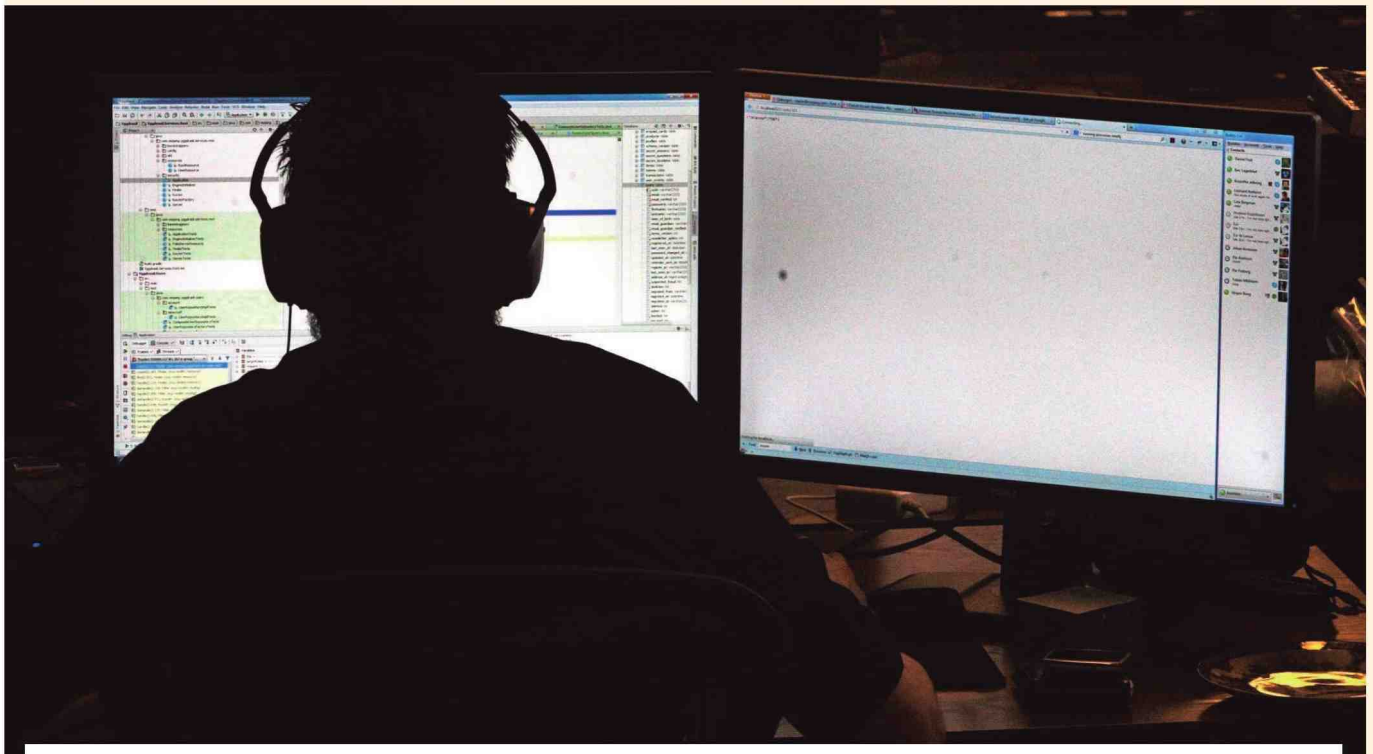

De impact van de grootste cyberaanval uit de geschiedenis zindert nog altijd na, tot bij de verzekeraars. © REUTERS

‘Cyberaanvallen kunnen verzekeraars duur te staan komen’

Werk van cybercriminelen of een oorlogsdaad? Als een Amerikaanse rechter straks beslist dat de wereldwijde cyberaanval NotPetya uit 2017 het eerste was, kan dat een schokgolf sturen door de verzekeringssector.

PIETER SUY

Hackers lanceerden twee jaar geleden de grootste cyberaanval uit de geschiedenis. De impact van de Wannacry-virussen en de NotPetya-gijzelsoftware, die dagenlang de IT-systemen van multinationals zoals de containerrederij Maersk of de Durex-fabrikant Reckitt Benckiser lamlegden, zindert nog altijd na.

De aanval heeft nu een juridische titanenstrijd ontketend tussen de Amerikaanse snoepgigant Mondelez, hier onder meer bekend als de eigenaar van de Côte d’Or-chocolade, en zijn verzekeraar Zurich. Mondelez beweert twee keer te zijn aangevallen door hackers, die duizenden laptops en servers hebben gegijzeld door er een virus op te installeren.

De Amerikaanse multinational claimt dat hij via zijn eigendomsverzekering voor die schade is ingedekt bij Zurich. Wat de Zwitsers nu ontkennen. De verzekeraar wil niet met geld over de brug komen omdat de NotPetya-aanval, waar vermoedelijk de Russische overheid achter zit, een ‘vijandige of oorlogsdaad’ is. Vergelijk het met de kleine lettertjes in uw brandverzekering: daar staat ook dat schade als gevolg van oorlog of terreur niet wordt terugbetaald. Mondelez laat het daar niet bij en eist nu een schadevergoeding van 100 miljoen dollar.

Het juridische potje armworstelen tussen Mondelez en Zurich lijkt een ver-van-ons-bedshow. Maar als de rechter in het voordeel van Mondelez beslist, kan dat volgens experts verstrekkende gevolgen hebben voor de hele verzekeringssector.

‘De zaak draait om zogenaamde stille verzekeringsrisico’s’, zegt Pedro Matthynssens, de CEO van de Belgische verzekeringsmakelaar Vanbreda Risk & Benefits. ‘Veel bedrijven hebben nog een brand- of aansprakelijkheidsverzekering die is opgesteld toen van cyberrisico’s nog geen sprake was. Die teksten zijn dan ook erg dubbelzinnig te interpreteren. En bij schade zal elke partij ze in haar voordeel proberen te interpreteren. Het voordeel van zo’n rechtszaak als die tussen Mondelez en Zurich is dat er nu ten minste transparantie zal komen over wat wordt gedekt en wat niet.’

Als de rechter Mondelez gelijk geeft, kan dat heel de sector veel geld kosten. ‘Zowat in elke grote verzekeringsgroep zijn vandaag risk managers aan het werk die berekenen hoe groot de stille risico’s zijn die dreigen uitbetaald te moeten worden’, weet Matthynssens.

100 miljoen

Het Amerikaanse Mondelez eist een schadevergoeding van 100 miljoen dollar van zijn verzekeraar Zurich.

Op termijn dreigen heel wat spelers in de branche geconfronteerd te worden met zoveel claims dat ze die niet meer allemaal kunnen uitbetalen.

CEO VANBREDA RISK & BENEFITS **PEDRO MATTHYNSSENS**

Volgens de CEO hangt de branche nog meer boven het hoofd. De klassieke brandverzekeringen en aansprakelijkheidspolissen kunnen dan wel een update gebruiken, de voorbije jaren gingen steeds meer verzekeraars gespecialiseerde producten aanbieden waarmee bedrijven zich tegen de fall-out van een cyberaanval kunnen beschermen. Met succes. Door het toenemende aantal cyberaanvallen en sinds de invoering van de strenge Europese privacyregels (GDPR) sluiten steeds meer kmo’s een cyberverzekering af.

In 2017 is het aantal cyberpolissen verdubbeld in vergelijking met 2016. Concrete cijfers voor 2018 zijn nog niet voorhanden, maar experts verwachten dat de trend vorig jaar aanhield.

‘Dat kan uiteindelijk een probleem worden’, vermoedt Matthynssens. ‘Cyberveiligheid is een mooie groeimarkt en veel verzekeraars willen nu zo veel mogelijk marktaandeel veroveren. Ze verkopen volop polissen, maar om hun premies te berekenen kunnen ze niet terugvallen op historische data.’

Dat is enigszins naïef, meent Matthynssens. ‘Cyberaanvallen worden steeds meer een systeemrisico voor verzekeraars. Kleinere schadegevallen van enkele tienduizenden euro’s kan je natuurlijk vrij makkelijk uitbetalen. Maar op termijn dreigen heel wat spelers in de branche geconfronteerd te worden met zoveel claims dat ze die niet meer allemaal kunnen uitbetalen, vrees ik. Steeds meer bedrijven bewaren hun data immers niet in eigen serverparken, maar doen een beroep op de clouddiensten van grote spelers zoals Amazon of Microsoft. Je kan je niet inbeelden wat er gebeurt als die cloudspecialisten gehackt worden.’

Lopen ook de Belgische verzekeraars een risico? Dat valt nog mee, vindt Matthynssens. ‘Vandaag bieden vooral de buitenlandse spelers cyberpolissen aan. Maar je kan dergelijke grote risico’s niet alleen dragen. Na de terreuraanslagen in New York en Madrid hebben de verzekeringsmaatschappijen een gezamenlijk fonds opgericht om slachtoffers te vergoeden. Als het nodig is, worden ze gesteund door de overheid. De risico’s van cyberaanvallen zijn intussen zo groot dat de geesten aan het rijpen zijn om ook daarvoor een gemeenschappelijk fonds op te zetten.’

De Tijd 15/01/2019, bladzijden 12 & 13