

PDF hosted at the Radboud Repository of the Radboud University Nijmegen

The following full text is a publisher's version.

For additional information about this publication click this link.

<http://hdl.handle.net/2066/199633>

Please be advised that this information was generated on 2019-04-26 and may be subject to change.



Astrid van Helvoort:
"Het feit dat hoofdelijke aansprakelijkheid is belegd in de AVG, heeft de acceptatie van het cyberrisico versneld"



Daniël Jacobs:
"Wat steeds vaker voorkomt, is dat verzekeren vragen om een certificaat om aan te tonen dat zij het risico van cyber hebben verzekerd"



Alexander van Nierop:
"Het cyberrisico zal veel meer gedeeld moeten worden, maar of je daar per se een beurscyberpolis voor nodig hebt, is de vraag"



Verzekering van cyberrisico's: ook mét voorwaarden ongrijpbaar genoeg

2017 was een onrustig jaar. Dat was allereerst op het terrein van cyberrisico's, want niet eerder zagen we die zo prominent en zo divers langskomen: e-mailaccounts van leden van het Britse parlement werden gehackt; miljoenen documenten kwamen via een datalek als de *Panama Papers* naar buiten en *ransomware*-aanvallen legden grote bedrijven als Maersk en APM Terminals stil, waardoor ook de economische impact van de cyberrisico's pijnlijk duidelijk werd.

2017 was ook privé een onrustig jaar en wel zodanig dat ik een periode niet gewerkt heb. Voor het eerst in 26 jaar was ik "thuis" en uit een soort zelfbescherming – een persoonlijk *incident response plan* – besloot ik te doen of het verzekeringsrecht niet bestond. Dat ging op zich prima, totdat ik in de auto toevallig een reclamespotje hoorde langskomen. "De Goudse introduceert een verzekering zonder polisvoorwaarden. De eerste verzekering zonder kleine lettertjes die wél uw cyberrisico dekt". Het is een boodschap die bij een verzekeringsjurist binnenkomt. Het moet niet gekker worden, dacht ik. Een mens kan niet eens even weg zijn of "ze" gaan rare dingen doen. Ik heb het op dat moment gelaten, maar ik wil best bekennen dat toen ik begin dit jaar weer ging werken, ik nog in diezelfde week heb opgezocht hoe zo'n polis zonder voorwaarden uitgedacht was. Het was ook in die week dat de redactie van VNAB Visie zich meldde met de vraag of ik mijn column over de cyberverzekering wilde schrijven. De invulling was daarmee gegeven...

Het risico van cyber voelt wat ongrijpbaar. Om die reden vind ik het *position paper* van het Verbond van Verzekeraars qua titel zo treffend: "Virtuele risico's, echte schade". Het stuk dateert alweer uit 2013 maar is op zich nog steeds actueel, waar het fraai inzicht geeft in de verschillende schadeposten en de fasen waarin die een rol (kunnen) spelen. De schade kan bestaan uit kosten in verband met afpersing, extra inzet van IT-capaciteit, kosten van bedrijfsstilstand, herstel van data, notificatie aan toezichthouders, PR-advies, advertentiekosten en zelfs kunnen (aanzienlijke) boetes tot de schade behoren. Het is juist vanuit dat besef dat ik zo benieuwd was naar hoe De Goudse dan dacht dat je dat zonder voorwaarden toch zou kunnen inkaderen. Mij is het inmiddels duidelijk: dat is door de voorwaarden geen voorwaarden te noemen, maar spelregels. Oude wijn in nieuwe zakken.

"SPELREGELS CYBERRISK", waarbij als handvat heeft te gelden dat De Goudse helpt met het voorkomen van een cyberincident. "Als het u toch overkomt, helpen we u met het beperken en herstellen van de schade. Is dit niet mogelijk? Dan ontvangt u een financiële vergoeding." Het is daarmee dus eigenlijk niet meer of minder dan een dappere poging om polisvoorwaarden, die inmiddels branchebreed al op (onduidelijk) B1-taalniveau geschreven zijn, nog verder te vereenvoudigen.

Ik heb er van zitten staren, want hoe goed bedoeld die poging ook kan lijken, moet je niet in ieder geval weten wat een cyberincident is? Wat schade is? Wat "wij vergoeden een boete" betekent? Is dat een, dus één, boete? Het staat er allemaal niet. Als een door cyber getroffen bedrijf stil ligt, valt die schade dan (ook) onder de te vergoeden schade? Of moeten we uit het feit dat – onder "spelregel" elf – aangegeven wordt dat de niet te herstellen schade én de schade voor aansprakelijkstelling door anderen (wel?) gedekt zijn, afleiden dat andere schade dat niet is? De rechter is van dat soort *à contrario* redeneringen – vanuit perspectief van verzekerenbescherming – bepaald geen voorstander, dus listig is het (voor de verzekeraar) allemaal wel. Tegelijkertijd is het een aspect dat breder speelt dan alleen hier. Want voor al die vereenvoudigde polissen geldt dat *less* soms gewoon *less* is. Ik mopper er wat op, maar ook weet ik dat die pogingen om te vereenvoudigen mijn dag vaak kleuren. De verzekeringsjurist in mij wordt stiekempjes namelijk best vrolijk als zij – onder "spelregel" twaalf – als aanhef ziet staan "Wij kunnen u niet verder helpen, als: (...)". Is dat de cryptische aanduiding voor het niet dekken van genoemde schades zonder onvriendelijk te willen lijken? Natuurlijk kan De Goudse verder helpen; er is alleen geen dekking. Ik probeer de opkomende glimlach snel te onderdrukken, want ik realiseer mij: in een wereld, waarin de belangen en (cyber)risico's zo groot zijn, kan je het risico van onduidelijkheid op polisseniveau er niet bij hebben.

Stelling: Het cyberrisico moet onderdeel worden van de standaardopleidingen binnen de branche

Reactie: absoluut!

Bernardo Walta: "Daarnaast denk ik dat je echt opleidingen voor cyberspecialisten gaat krijgen."

Astrid van Helvoort: "Belangrijk is ook te investeren in kennisdeling. Wij organiseren sessies voor onze adviseurs waarin ze hun ervaringen met elkaar kunnen delen."

Yasin Chalabi: "Zelf lees ik veel, woon ik seminars bij en spar ik met securitypartners. Ook komen wij met alle techneuten en specialisten eenmaal per vier maanden bijeen, onder meer om ook wereldwijd alle ontwikkelingen bij te houden."

Daniel Jacobs: "Er is een zoektocht naar deskundigheid. In een snelgroeende markt worden mensen volop weggekocht. Met drie jaar ervaring ben je in deze markt al een senior. Naar een cyberafdeling gaat veel opleidingsgeld toe omdat iemand met relatief weinig ervaring veel bevoegdheid krijgt. En natuurlijk willen we niet dat dit misgaat."

Tot slot: Hebben jullie een prangende vraag aan elkaar?

Bernardo Walta: "Meer een oproep, namelijk dat we er met elkaar voor moeten zorgen dat de markt zich op een goede manier ontwikkelt. Het creëren van bewustzijn is daarbij belangrijk zodat er geen ongelukken gebeuren, waardoor de branche imagoschade lijdt. Ook denk ik dat het goed is als er meer aanbieders komen. Dat is voor een markt altijd goed en zo houd je elkaar scherp. Bovendien bestaat de kans dat de overheid met een ander model gaat komen als wij dit als markt niet goed regelen."

Yasin Chalabi: "Het is belangrijk om in preventie

te investeren. Door goede oplossingen te bieden, wordt de kans op schade minder en voorkom je maatregelen als (enorme) premiestijgingen of invoering/verhoging van eigen risicobedragen."

Alexander van Nierop: "Belangrijk is dat technologiebedrijven echt gaan werken op basis van 'security by design' waardoor een goede beveiliging de standaard wordt. Hiervoor zouden (wereldwijd) strikte regels moeten komen. Daarnaast is een goede samenwerking tussen de verschillende par-

tijen, zoals hard-/softwareleveranciers, verzekeraars en adviseurs essentieel."

Astrid van Helvoort: "We moeten cyberrisico uit de taboesfeer halen. Vaak zeggen klanten in eerste instantie dat ze nog nooit met cyberschade te maken hebben gehad. Eenmaal in gesprek blijkt vaak het tegendeel. Er heerst onterechte schaamte. Het is net als een brand een risico dat ons allemaal kan overkomen; ook als je als bedrijf je zaken goed voor elkaar hebt." <

Markt cyber verdubbeld

De markt voor cyberverzekeringen is in de afgelopen twee jaar meer dan verdubbeld. Het premie-inkomen is van maximaal tien miljoen euro in 2015 gegroeid naar minimaal twintig miljoen in 2017.

Dat blijkt uit een enquête die het Centrum voor Verzekeringsstatistiek medio 2016 en begin dit jaar heeft uitgezet onder zakelijke verzekeraars. Verbondsdirecteur Leo de Boer is blij met de verdubbeling. "Dat betekent immers dat de markt dit nieuwe risico goed oppakt." Toch noemt hij de bewustwording onder klanten nog veel te laag. "Mensen realiseren zich de risico's nog onvoldoende. Samen met diverse stakeholders, waaronder de overheid, het mkb en de IT- en securityspecialisten, moeten wij de bewustwording verder op gang brengen. Hier ligt echt een kans van formaat voor onze sector."

Groei

Het merendeel van de huidige cyberpolissen geeft dekking voor aansprakelijkheid, juridische bijstand, crisismanagement en voor de herstelkosten van websites, programma's of data.

Volgens statisticus Evert van Steenberghe wordt de huidige groei veroorzaakt doordat er meer verzekeraars op de markt van cyberverzekeringen actief zijn, maar ook doordat de portefeuille van veel verzekeraars is gegroeid. "De omzet wordt bijna helemaal behaald op de zakelijke markt", benadrukt hij, "omdat het aandeel van de particuliere markt nog geen tien procent bedraagt."

Meer informatie is onder meer te vinden bij het ministerie van Justitie & Veiligheid en op de website veiliginternetten.nl.