

# Cyberverzekeringen

Verkenning naar de Nederlandse  
verzekeringmarkt

27-02-2023

**De digitalisering van de samenleving neemt steeds verder toe.** We bestellen online onze boodschappen, vergaderen via videoconferencing en onze huizen staan vol slimme apparatuur (IoT-apparaten). Onze data worden opgeslagen in de cloud, in plaats van in archiefkasten en bedrijven die online platformdiensten aanbieden behoren tot de meest waardevolle ondernemingen ter wereld.

**Deze ontwikkeling brengt nieuwe cyberrisico's met zich mee.** Bedrijven zijn inmiddels volledig afhankelijk van een goed werkende (externe) IT-infrastructuur. Als deze niet meer functioneert valt het hele bedrijf stil. Onze persoonlijke data lopen een groot risico op diefstal, wat concrete gevolgen als creditcardfraude of identiteitsdiefstal kan hebben. Oorlog en terrorisme vinden ook digitaal plaats, net als diefstal van bedrijfsgegevens.

**Deze nieuwe risico's zijn dynamisch, complex en nemen toe.** Het aantal ransomware-aanvallen is in de afgelopen jaren zeer sterk toegenomen.<sup>1</sup> Kwetsbaarheden in hardware als Meltdown en Spectre brengen nieuwe risico's voor consumenten en bedrijven met zich mee.<sup>2</sup> Het is moeilijk te voorspellen welke cyberrisico's er over vijf jaar spelen. Consumenten en bedrijven zijn zich (nog) beperkt bewust van deze risico's blijkt uit de gesprekken die de AFM heeft gevoerd met verzekeraars.

**Er zijn verzekeringsproducten op de markt om het cyberrisico te mitigeren.** Deze cyberverzekeringen dekken risico's rondom aansprakelijkheid en eigen schade af voor klanten, en bieden vaak ook dienstverlening als een cyberincident zich voordoet. Hiermee kunnen consumenten en het MKB dit risico voor zichzelf of hun onderneming afdekken.

**De AFM heeft de afgelopen maanden een verkenning uitgevoerd naar de markt voor cyberverzekeringen.** De reden hiervan is dat dit een relatief nieuw type risico is en dat de hoeveelheid cyberaanvallen in de afgelopen jaren, in het bijzonder tijdens de coronaperiode, sterk is toegenomen. Hierdoor neemt ook het risico waaraan consumenten en ondernemingen blootstaan toe. De AFM vindt het belangrijk om mogelijke risico's tijdig te signaleren, en heeft daarom een verkenning uitgevoerd naar dit product. Hierdoor is de AFM ook in staat om, gezien het grensoverschrijdende karakter van dit onderwerp, internationaal aandacht te vragen voor uitkomsten van de verkenning. Daarnaast is het een grensoverschrijdend risico in een internationaal speelveld van marktpartijen, waar de AFM in het bijzonder aandacht voor heeft.

**De markt voor zowel (klein)zakelijke als particuliere cyberverzekeringen is nog klein, maar gaat naar verwachting groeien.**<sup>3</sup> De marktomvang was € 36 miljoen in 2021, terwijl dat voor een product als aansprakelijkheidsverzekeringen ongeveer € 850 miljoen was. Op de zakelijke markt is het aantal Nederlandse verzekeraars dat een eigen product voert beperkt. Op de particuliere markt zijn er meer Nederlandse verzekeraars actief.

**De AFM constateert dat het nog moeilijk is om cyberverzekeringen onderling te vergelijken, om drie redenen.** Dit zijn: complexiteit van de voorwaarden, een verschillende uitleg van kernbegrippen en dekkingen die niet volledig expliciet zijn gemaakt door verzekeraars.

- 1. Het cyberrisico en de voorwaarden van de verzekering zijn dynamisch en complex.** Omdat het cyberrisico voornamelijk een IT-risico is, vraagt het product ook een bepaalde mate van IT-kennis. Dit maakt het lastiger voorwaarden te doorgronden, en vraagt ook van adviseurs nieuwe/aanvullende kennis om een goede risico-inschatting te kunnen maken. Omdat het risico doorlopend aan verandering onderhevig is, wijzigen ook de verzekeringsvoorwaarden continu. Het is dus van belang dat wijzigingen helder worden gecommuniceerd aan klanten, dat bij productontwikkeling rekening

---

<sup>1</sup> [Ransomware Attacks Hit Two Out Of Three Organizations In 2021: Here's What You Need To Know \(forbes.com\)](#)

<sup>2</sup> [Meltdown and Spectre \(meltdownattack.com\)](#)

<sup>3</sup> [Cyberverzekeringsmarkt in 2021 gegroeid naar 36 miljoen euro \(verzekeraars.nl\)](#)

wordt gehouden met de PARP-richtlijnen en dat polisvoorwaarden op de meest transparant mogelijke wijze worden vormgegeven. Dit maakt het voor klanten en adviseurs mogelijk om doorlopend te beoordelen of het product nog bij de persoonlijke situatie past en het klantbelang centraal te blijven stellen.

2. **Een verschillende uitleg van kernbegrippen maakt het moeilijk om dekkingen met elkaar te vergelijken.** Verzekeringen die dekking bieden voor bedrijfsschade na een cyberincident kunnen onderling inhoudelijk sterk verschillen, omdat de definitie van een ‘cyberincident’ tussen verzekeraars verschilt. Deze kan uiteenlopen van dekking voor menselijke fouten, programmeerfouten en hacks tot uitsluitend een dekking voor kwaadaardige aanvallen. Ook in andere definities zien we verschillen, zoals ‘infrastructuur’ of ‘computernetwerk’, die sterk van invloed kunnen zijn op de dekking die de klant ontvangt. Het op dezelfde wijze definiëren van deze begrippen komt – in het belang van de klant – het begrip en de onderlinge vergelijkbaarheid van de producten ten goede.
3. **Tot slot ziet de AFM dat niet alle voorwaarden expliciet worden gemaakt.** Een voorbeeld hiervan is de uitsluiting voor schade ontstaan door oorlog. Dit is ten tijde van de invasie van Oekraïne door Rusland geen hypothetisch risico meer.<sup>4</sup> Het is moeilijk om van cyberincidenten vast te stellen of deze een oorlogsdaad waren en veel verzekeraars vertrouwen hierbij op externe specialisten of overheden. De AFM constateert dat niet in alle voorwaarden duidelijk wordt gemaakt op welke bronnen de verzekeraar zich baseert om een cyberincident als oorlogsdaad te categoriseren. Op het moment dat een dergelijk incident zich voordoet is niet op voorhand duidelijk of deze wel of niet onder de verzekeringsdekking valt, wat geen zekerheid biedt aan de verzekerde. Het draagt bij aan het begrip van het product – en de onderlinge vergelijkbaarheid – als informatie hierover zo transparant en volledig mogelijk is.

**Het is van belang dat verzekeraars doorlopend beoordelen hoe zij zo transparant mogelijk kunnen communiceren over de dekking van de cyberverzekeringen, en dat de sector gezamenlijk bekijkt hoe zij – gezien de groei van deze markt – nu al kan bijdragen aan de onderlinge vergelijkbaarheid van het productaanbod. Het internationale karakter van deze markt zorgt hierin voor een extra uitdaging.** Gezien de complexiteit en veranderlijkheid van zowel de productopbouw als het cyberrisico is het bij deze producten extra van belang dat informatieverstrekking doorlopend bijdraagt aan het begrip van het product door de klant. Een betere onderlinge vergelijkbaarheid van de dekking en werking van het product kan hieraan bijdragen. Zo worden klanten en adviseurs in staat gesteld om nu en in de toekomst de juiste risico’s af te dekken en worden voorzienbare teleurstellingen voorkomen.

---

<sup>4</sup> [New “Prestige” ransomware impacts organizations in Ukraine and Poland - Microsoft Security Blog](#)



**Autoriteit Financiële Markten**

Postbus 11723 | 1001 GS Amsterdam

**Telefoon**

020 797 2000

[www.afm.nl](http://www.afm.nl)

**Dataclassificatie**

AFM - Publiek

Follow us: →



*De AFM maakt zich sterk voor eerlijke en transparante financiële markten.*

*Als onafhankelijke gedragstoezichthouder dragen wij bij aan duurzaam financieel welzijn in Nederland.*

De tekst van deze publicatie is met zorg samengesteld en is informatief van aard. U kunt er geen rechten aan ontleen. Door veranderende wet- en regelgeving op nationaal en internationaal niveau is het mogelijk dat de tekst niet actueel is op het moment dat u deze leest. De Autoriteit Financiële Markten (AFM) is niet aansprakelijk voor de eventuele gevolgen – bijvoorbeeld geleden verlies of gederfde winst – ontstaan door of in verband met acties ondernomen naar aanleiding van deze tekst.

© Copyright AFM 2023