ONTWIKKELINGEN CYBERVERZEKERINGSMARKT: VAN OPKOMST TOT NIEUWE DYNAMIEK

VERBOND VAN VERZEKERAARS

Januari 2024

Het platform Cyber van het Verbond van Verzekeraars heeft onder andere als doelstelling zijn leden en andere belanghebbenden te informeren over ontwikkelingen in cyberrisico's. In dit paper over marktontwikkelingen staan we stil bij (inter)nationale ontwikkelingen binnen de cyberverzekeringsmarkt.

Dit document maakt onderdeel uit van een reeks van in totaal drie papers die ingaan op cyberrisico's en de verzekerbaarheid ervan. Eerder hebben we de paper 'Systeemrisico's in het cyber(verzekering)domein' gepubliceerd. Daarin zijn we dieper ingegaan op enkele specifieke elementen van cyberdreigingen, die in belangrijke mate bijdragen aan het systeemrisico: ransomware, privacy en het gebrek aan incident data. In oktober 2023 is de whitepaper 'Aandachtspunten bij stille dekkingen in traditionele polissen' gepubliceerd. Aan de hand van voorbeelden hebben we ingezoomd op de zogeheten 'stille dekking' van cyberrisico's die het meest voorkomen in traditionele verzekeringen, zoals verzekeringen voor bedrijfs- en bestuurdersaansprakelijkheid, brand- en technische verzekeringen en motorrijtuigverzekeringen.

Aanleiding

De Nederlandse cyberverzekeringsmarkt heeft in enkele decennia een opmerkelijke transformatie ondergaan, van de introductie door buitenlandse verzekeraars tot verschuivingen in de Nederlandse markt. Oorspronkelijk geïntroduceerd met relatief lage tarieven, heeft de markt zich snel ontwikkeld in reactie op de groeiende digitalisering en het veranderende risicolandschap, met name door de toenemende dreiging van ransomware. Hoewel de markt aanvankelijk te maken had met aanzienlijke premiestijgingen en strenge acceptatiecriteria, lijkt er recentelijk een kentering plaats te vinden met een mogelijke matiging van tarieven en nieuwe spelers die de markt betreden.

In dit paper zoomen we in op de paradoxen en complexiteit van deze transformaties en roepen we op tot gezamenlijke inspanningen om de beheersbaarheid van cyberrisico's en de stabiliteit van de verzekeringsmarkt te waarborgen, benadrukkend dat voortdurende investeringen in IT-beveiliging cruciaal zijn voor doeltreffende en betaalbare bescherming van organisaties.

Achtergrond

Meer dan tien jaar geleden betraden de eerste buitenlandse verzekeraars de Nederlandse cyberverzekeringsmarkt. Ondanks dat deze verzekeringen al jarenlang succesvol waren in de Verenigde Staten, bleek het aanvankelijk een relatief onvolgroeid product. Veelal vertaald vanuit dekkingen met oorsprong uit de Verenigde Staten en het Verenigd Koninkrijk. Sommige verzekeraars legden in eerste instantie de nadruk op de aansprakelijkheidsaspecten terwijl andere juist de nadruk legden op de bedrijfsschade component.
De toenmalig milde tarieven en niet al te strenge acceptatiecriteria leidden tot een snelle penetratie in Nederland. In een markt met weinig vraag maar veel aanbieders van cyberverzekeringen resulteerde dit snel in mildere premies, verbeteringen en uitbreidingen van dekkingen, waarbij de premies uiteindelijk ook daalden. De groeiende digitalisering en de daarmee samenhangende risico's leidden uiteindelijk tot een grotere vraag naar cyberverzekeringen.

Risicolandschap

In de beginjaren waren cyberaanvallen, zoals ransomware, nog zeer gering van invloed op de bedrijfscontinuïteit. Vaak raakte slechts één computer betrokken, wat leidde tot beperkte schade. Bedrijfsschade (omzetverlies) was er nog nauwelijks en het losgeld was zo laag dat dat snel kon worden betaald. Of de computer werd opnieuw opgebouwd waardoor het probleem snel kon worden opgelost.

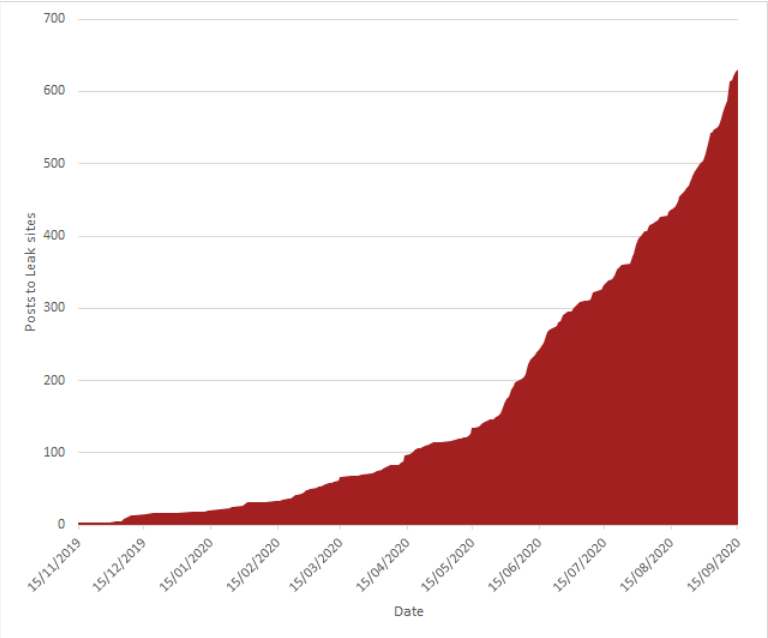
Het risicolandschap is nu geheel omgekeerd. Datalekken hebben dankzij de AVG (Algemene Verordening Gegevensbescherming) een diepgaandere impact gekregen, en ransomware-aanvallen zijn geëvolueerd naar bedreigingen van complete IT-systemen, met miljoenen euro's aan losgeld.
Als voorbeeld: In 2013 waren er (volgens Crowdstrike) 100.000 ransomware aanvallen, waarbij het gemiddelde losgeld EUR 200 bedroeg en dit ontwikkelde zich snel over de jaren tot 2021 in een steile curve naar EUR 6,1 miljoen aan gemiddelde losgeldeisen (bron).

Stijgende professionalisering en complexiteit

Naast de toegenomen gemiddelde losgeldeisen en frequentie van aanvallen, is ransomware verfijnd door zeer professioneel handelende criminele organisaties die technieken hebben ontwikkelend om gehele IT-systemen van organisaties te versleutelen. Zo ontstonden er nieuwe ransomwaretypes, waarbij data eerst werd gestolen en vervolgens werd versleuteld. Dit gaf criminelen de mogelijkheid om organisaties dubbel te chanteren. Enerzijds door in eerste instantie data te ontsluiten. Hierdoor bleek later dat organisaties toch zelf de data konden herstellen (waardoor ze geen losgeld hoefden te betalen) dan resulteerde dat alsnog in het lekken van gestolen data op het Darkweb. Dit met grote reputatieschade tot gevolg. Organisaties in alle sectoren – ongeacht hoe groot of klein ze zijn - zijn kwetsbaar gebleken voor cyberincidenten.
Daarnaast zorgt de proliferatie van de zogenoemde *ransomware-as-a-service* mogelijkheden ertoe dat aanvallen ook door criminelen met een minder grote cyberexpertise uitgevoerd kunnen worden. Het gaat hier om een businessmodel waarbij professionele cybercriminelen een ransomware aanval inclusief dienstverlening verkopen aan andere criminelen.

Dit alles heeft ertoe geleid dat ransomware momenteel het meest voorkomende en impactvolle cyberincident is geworden en nog steeds groeiende.

De onderstaande grafiek van PWC illustreert de groeiende frequentie van data-publicaties na ransomware-incidenten. (bron)



Marktontwikkelingen

Door het veranderende risicolandschap nam de schadelast van verzekeraars toe en bracht de bedrijfstak in een periode van aanpassingen. Zelfs enkele verzekeraars trokken zich terug en staakten het aanbieden van cyberverzekeringen.

Tussen 2020 en 2023 werden aanzienlijke premiestijgingen voor maatwerkcontracten opgemerkt, gepaard gaande met complexe aanvraagprocedures en zware assessments bij de aanvraag van een cyberverzekering. De drempel werd vele malen verhoogd en niet iedereen kon nog een cyberverzekering afsluiten. En degene die nog wel in aanmerking kwam werd nogal eens geconfronteerd met dekkingsbeperkingen.

Voor het mkb en de standaardproducten lag dat iets anders maar ook daar werden acceptatievereisten verzwaard en premies (licht) verhoogd.

Recentelijk lijkt er echter een kentering plaats te vinden en zijn er de eerste indicaties dat die enorme 'verharde' markt van 2020 -2022 nu weer 'zachter' aan het worden is. Nieuwe partijen betreden de markt, waarbij vooral interesse is in excedentverzekeringen. Er is nu meer excedentcapaciteit op de markt dan dat er vraag is, met meer concurrentie als gevolg. Deze trend heeft eind 2023 al geleid tot tariefreducties voor de excedentprogramma's van grotere bedrijven en er zijn eerste tekenen dat deze trend doorsijpelt naar primaire programma's voor met name grote en middelgrote organisaties en bedrijven.

Tegenstrijdigheden en complexiteit van trends

Deze verschuivingen brengen echter paradoxen met zich mee, met name in het licht van recente nieuwsberichten dat het aantal gepubliceerde ransomware-incidenten op het darkweb maand op maand blijft toenemen.

Dit roept fundamentele vragen op over de ware staat van het risicolandschap. In 2023 zijn tariefstijgingen aanzienlijk vertraagd, wat op het eerste gezicht optimisme kan wekken. We weten namelijk ook dat organisaties niet stilgezeten hebben in het verbeteren van hun cyberbeveiliging. Echter, de groeiende dreiging, die wordt gestaafd door het aantal gepubliceerde ransomware-incidenten, roept een verontrustende vraag op. In hoeverre weerspiegelen de tariefcorrecties de werkelijke risicovermindering en in hoeverre zijn ze een verschuiving in de perceptie van dat risico? Of zijn ze alleen maar een (lichte) correctie op de zeer snelle stijging?

Balanceren tussen vooruitgang en bedreiging

Het dynamische terrein van cyberdreigingen ondergaat voortdurend veranderingen, met aanvallen die steeds geavanceerder worden. In deze evolutie groeit ook de complexiteit van technologie, waar organisaties in toenemende mate afhankelijk van worden. Op het eerste gezicht zou je verwachten dat de toenemende cyberbeveiliging van organisatorische beveiliging het risico verkleint en uiteindelijk de schadelast voor verzekeraars doet afnemen.

Echter, de paradox schuilt in de aard van deze evolutie. Terwijl organisaties investeren in geavanceerde beveiligings-maatregelen, perfectioneren criminelen gelijktijdig hun aanvalstechnieken. De verschuiving van grootschalige versleuteling van bedrijfsgegevens naar gerichte aanvallen op kwetsbare systemen of organisaties is een duidelijk voorbeeld van deze trend. Deze veranderingen vereisen een flexibele reactie van verzekeraars, waarbij aanpassingen in acceptatiebeleid noodzakelijk zijn om effectief te anticiperen op de evoluerende patronen van cyberdreigingen.
Het lijkt erop dat we ons nog maar aan het begin bevinden van een bijzondere tijd van cyberverzekeringen, waar fluctuaties een integraal onderdeel zijn van deze voortdurende dynamiek.

Cyberbeveiliging kan nooit 100% effectief zijn, gezien de voortdurende opkomst van nieuwe kwetsbaarheden in systemen en de ingenieuze methoden van criminelen om beveiligingsmaatregelen te omzeilen. Daarom blijft het cruciaal voor organisaties om voortdurend te investeren in IT-beveiliging en het veiligheidsniveau op het hoogst mogelijke niveau te handhaven. Dit vereist continu aandacht van organisaties. En door de opkomst van onder andere Artificial Intelligence (A.I.) moet het menselijke aspect ook niet onderschat worden. Deze voortdurende inspanningen op het gebied van IT-beveiliging zijn van essentieel belang voor het bereiken van langdurige rust en het verkrijgen van een beter voorspelbaar risicobeeld. Dit draagt bij aan de adequate bescherming van organisaties, waardoor het resterende risico op een doeltreffende en betaalbare manier kan worden verzekerd.

We roepen daarom alle belanghebbenden op om continu aandacht te geven aan bovengenoemde ontwikkelingen. Alleen samen kunnen we de cyberrisico's beheersbaar en met name stabiel verzekerbaar houden.