DOOR SJOERD BRETHOUWER
EN TRISTAN STOEVELAAR

De opkomst van cyberverzekeringen in Nederland: kansen en uitdagingen

Cybercrime vormt een groeiende bedreiging voor bedrijven in vrijwel alle sectoren. De dreiging is veelzijdig en voortdurend in ontwikkeling. Veelvoorkomende incidenttypen zijn ransomware-aanvallen, waarbij systemen worden vergrendeld en losgeld wordt geëist, en datalekken, die kunnen ontstaan door onbevoegde toegang tot klantgegevens of intellectueel eigendom. Ook phishing en andere vormen van social engineering blijven effectieve methoden om toegang te verkrijgen tot interne systemen. Daarnaast komen DDoS-aanvallen, die systemen tijdelijk platleggen, ook veel voor. Naast kwaadwillende aanvallen spelen ook menselijke fouten en technische kwetsbaarheden een rol, zoals verkeerd geconfigureerde servers of verouderde software.

De gevolgen kunnen zowel financieel als operationeel ingrijpend zijn. Organisaties maken kosten voor herstel, onderzoek en juridische ondersteuning, en ondervinden indirecte schade zoals omzetverlies, reputatieschade en verlies van klantvertrouwen. Juridische verplichtingen zoals de meldplicht onder de AVG kunnen bovendien leiden tot boetes of aansprakelijkheid. Cyberincidenten raken zelden alleen IT, maar beïnvloeden de hele bedrijfsvoering.

In dit artikel wordt besproken hoe de Nederlandse markt voor cyberverzekeringen zich ontwikkelt als antwoord op deze dreiging. Daarbij komen markttrends, dekkingsmogelijkheden, acceptatiecriteria en uitdagingen rond premiestelling aan bod, evenals het toenemende gebruik van AI bij risicobeheersing.

S.D. Brethouwer MSc AAG (links) is Consulting Actuary bij Milliman.

T. B. Stoevelaar MSc is Consultant bij Milliman.

TRENDS EN SCHADEONTWIKKELINGEN BIJ CYBERINCIDENTEN

Recente cijfers tonen aan dat het percentage bedrijven dat te maken krijgt met cybersecurityincidenten, zowel door interne oorzaken als door aanvallen van buitenaf, de afgelopen jaren in alle bedrijfsgroottes is gedaald. Grote bedrijven blijven relatief vaker doelwit. Zo meldde in 2016 bijna 40% een extern incident, tegenover 16% in 2023 (CBS, 2025).

Ook het aandeel incidenten met directe financiële schade daalde. In 2016 rapporteerde 55% van de getroffen bedrijven kosten na een externe aanval, in 2023 nog slechts 20%. Voor interne oorzaken daalde dit van 41% naar eveneens 20% (CBS, 2025).

Een verklaring voor deze positieve trend is de bredere implementatie van technische en organisatorische beveiligingsmaatregelen. Zo maakt inmiddels 76 procent van de middelgrote bedrijven gebruik van multifactor authenticatie, tegenover slechts 29 procent in 2017 (CBS, 2025). Ook back-ups, netwerksegmentatie en veiligheidstrainingen zijn vaker standaard onderdeel van het IT-beleid.

Toch is verdere daling onwaarschijnlijk. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) wijst op een aanhoudend hoog dreigingsniveau, mede door statelijke actoren, hacktivisten en steeds professionelere cybercriminelen. Deze groepen opereren op afstand en misbruiken gericht kwetsbaarheden in digitale systemen. Door de opkomst van generatieve AI worden aanvallen bovendien technischer, realistischer en moeilijker te detecteren (NCTV, 2024).

Tegelijkertijd nemen de potentiële kosten van incidenten verder toe. Cybersecurity Ventures voorspelt dat de wereldwijde schade door ransomware in 2031 kan oplopen tot 250 miljard dollar per jaar (Sausalito, 2025).

DEKKING ONDER CYBERVERZEKERINGEN EN DE OMVANG VAN DE MARKT

Cyberverzekeringen dekken diverse schadeposten bij digitale incidenten. In de kern gaat het om directe responskosten zoals forensisch onderzoek, juridische bijstand, klantcommunicatie en reputatieherstel. Ook vallen bedrijfsonderbrekingen, aansprakelijkheid na een datalek, en indien toegestaan, bestuurlijke boetes onder de dekking. Bij ransomware zijn herstelkosten en soms ook afkoopsommen inbegrepen (Cyberverzekeringen, 2025).

De markt voor cyberverzekeringen in Nederland is in opkomst, maar blijft vooralsnog beperkt van omvang. Inmiddels bieden ruim tien verzekeraars een cyberverzekering aan, maar veel partijen blijven terughoudend vanwege de onvoorspelbaarheid van het risico en het gebrek aan schadehistorie. Volgens het Verbond van Verzekeraars bedroeg het premievolume circa 111 miljoen euro in 2024, tegenover 101 miljoen euro in 2023 (Verzekeraars, 2025). Internationaal groeit de markt sneller. In 2024 bedroeg het premievolume in de VS circa 10,6 miljard dollar (69% van de wereldmarkt), tegenover 3,3 miljard in Europa. Verwacht wordt dat Europa groeit naar 8,3 miljard dollar in 2030 (24% marktaandeel) (Munich Re, 2025).

HET ACCEPTATIEPROCES VAN CYBERVERZEKERINGEN

Voordat een cyberverzekering wordt verstrekt, beoordeelt de verzekeraar het risico van de aanvrager. Dit begint meestal met een vragenlijst over beveiligingsmaatregelen, eerdere incidenten en de aard van de gegevens. Op basis daarvan wordt een risicoprofiel opgesteld waarop premie, dekking en uitsluitingen worden afgestemd. Organisaties met sterke beveiliging krijgen doorgaans gunstigere voorwaarden. Bij verhoogd risico kan aanvullende documentatie of controle nodig zijn.

Hoewel het acceptatieproces per verzekeraar verschilt, wordt alleen verzekerd als het risico voldoende in beeld is. Dit proces vormt daarmee ook een moment voor organisaties om stil te staan bij hun digitale weerbaarheid (Cyberverzekeringen, 2025). Verzekeringsadviseurs spelen hierbij een cruciale rol, zij helpen bedrijven bij het verbeteren van hun risicoprofiel en het vinden van passende dekking.

Het gebrek aan uniforme polisvoorwaarden bemoeilijkt de toegankelijkheid, vooral voor kleinere bedrijven en publieke instellingen. Verschillen in definities en uitsluitingen maken vergelijking lastig. Meer standaardisatie op dit gebied kan de markttoetreding vergemakkelijken.

MARKTORGANISATIE EN DE BESCHIKBAARHEID VAN CYBERPOLISSEN

De beschikbaarheid van cyberverzekeringen staat onder druk. Door het ontbreken van voorspelbare schadepatronen en het risico op grootschalige incidenten is het lastig voldoende capaciteit aan te bieden. Toch blijft de markt functioneren dankzij herverzekering, risicoselectie en dekkingbeperkingen (Association, 2024).

Veel verzekeraars gebruiken herverzekeringscontracten om hun blootstelling aan extreme scenario's te beperken. Tegelijk worden clausules ingezet om statelijke aanvallen of infrastructuurstoringen uit te sluiten. Ook gelden vaak maxima per incident of jaar. Om het risico verder te beheersen, gelden strikte acceptatievoorwaarden. Alleen organisaties die aantoonbaar investeren in digitale weerbaarheid komen in aanmerking voor bredere dekking.

De markt is niet voor alle doelgroepen even toegankelijk. Grote bedrijven voldoen vaak aan acceptatiecriteria, maar bij hogere dekkingsbehoeften zijn hun opties beperkt. Zij wijken daarom vaak uit naar internationale verzekeraars die meer capaciteit en maatwerk bieden. Voor mkb's en publieke instellingen sluiten beschikbare polissen vaak slecht aan of zijn moeilijk verkrijgbaar, door beperkte middelen, hogere risico's en standaardvoorwaarden.

COMPLEXITEIT VAN PREMIESTELLING EN SCHADERAMING

Een van de grootste uitdagingen in de Nederlandse markt is het ontbreken van een centrale database met gegevens over cyberincidenten. Hoewel er initiatieven in ontwikkeling zijn, verloopt de implementatie traag door onderlinge verschillen tussen verzekeraars.

Daarbij is premiestelling fundamenteel onzeker door gebrek aan betrouwbare data en snel veranderende aanvalstechnieken. Zoals eerder genoemd veroorzaken cyberincidenten directe én indirecte schade, zoals herstelkosten, omzetverlies en reputatieschade, posten die lastig te kwantificeren zijn en sterk variëren per sector.

Ook accumulatierisico's bemoeilijken risicobeoordeling. Een kwetsbaarheid binnen één software of platform kan meerdere partijen tegelijk raken. Door beperkte transparantie in IT-infrastructuren zijn zulke scenario's moeilijk te voorspellen.

Verzekeraars zetten daarom vaker alternatieve databronnen, scenarioanalyses en externe modellen in. De interesse in AI en machine learning groeit, vanwege hun vermogen om dynamisch te reageren op actuele risicodata.

TOEPASSING VAN AI EN MACHINE LEARNING BIJ RISICOBEHEERSING

Door de snelle ontwikkeling van cyberdreigingen verliezen historische schadegegevens snel hun waarde voor risicobeoordeling. De uiteenlopende vormen van schade en accumulatie van risico's maakt traditionele modellen beperkt toepasbaar. Verzekeraars zetten daarom steeds vaker AI en machine learning in om realtime informatie te analyseren, zoals netwerkactiviteit, meldingen van dreigingen en gedragsdata. Deze technologieën maken het mogelijk om risico's dynamisch te volgen en risicoprofielen continu bij te stellen. Ook zijn AI-modellen geschikt om correlaties te herkennen tussen risico's, bijvoorbeeld wanneer meerdere verzekerden tegelijk worden geraakt via gedeelde software. (Matthewson, 2024).

CONCLUSIE

Cyberverzekeringen worden steeds belangrijker in het risicomanagement van bedrijven. Tegelijkertijd heeft de markt serieuze uitdagingen. Het ontbreken van een centrale database, de complexe risico's en een gebrek aan standaardisatie belemmeren toegankelijkheid voor zowel aanbieder als afnemer. Toch nemen het aantal aanbieders en het premievolume toe, en ontstaan er initiatieven voor een centrale database om zo risico's beter te kunnen modelleren.

Daarnaast bieden AI en machine learning modellen mogelijkheden voor dynamische en daarmee accuratere risicobeoordeling. Dit vereist dat verzekeraars blijven investeren in technologische expertise. Voor verdere professionalisering van de markt en betere bescherming tegen cybercriminaliteit is samenwerking tussen verzekeraars, de overheid en bedrijven van belang. ■

Referenties

Association, T. G. (2024). Cyber Risk Accumulation. Opgehaald van https://www.genevaassociation.org/sites/default/files/2023-11/cyber_accumulation_report_91123.pdf

CBS. (2025). Cybersecuritymonitor 2024. Opgehaald van https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

Cyberverzekeringen. (2025). Opgehaald van Cyberverzekeringen.nl: https://www.cyberverzekeringen.nl/aon/

Matthewson, A. (2024). Cyber Insurance: AI and Dynamic Risk Assessment. Opgehaald van https://insurtechdigital.com/articles/cyber-insurance-ai-and-dynamic-risk-assessment

Munich Re. (2025). Cyber insurance: Risks and trends 2025. Opgehaald van https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html

NCTV. (2024). Cybersecuritybeeld Nederland 2024. Opgehaald van https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland

Sausalito, C. (2025). Global ransomware damage costs predicted to reach 250 billion USD by 2031. Opgehaald van Cybersecurity Ventures: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Verzekeraars, V. v. (2025). Cyber. Opgehaald van https://www.verzekeraars.nl/verzekeringsthemas/schade/cyber