Handleiding voor bedrijven en verzekeringsadviseurs

Een kort begrip van de cyberverzekering

Datum: Juli 2022
Auteur: Technische commissie Cyber VNAB

1. Inleiding

a. Doelstelling van dit document

Organisaties worden blootgesteld aan een steeds groter arsenaal aan cyber- en technologierisico's en de potentiële financiële gevaren groeien navenant. We hebben het in dit verband niet alleen over cybercriminaliteit, maar ook over systeemfalen (bijv. een storing binnen het ICT-systeem van de organisatie of bij een ICT-serviceprovider) en fouten of vergissingen van het personeel. Het is dan ook geen verrassing dat organisaties cyberrisico's de laatste jaren steevast als één van hun vijf grootste zorgen noemen.

Daarom is het belangrijk dat de verzekeringsadviseur en (potentiële) verzekerden goede gesprekken voeren inzake cyberrisico's en hoe deze risico's kunnen worden beperkt. Zo nodig bijgestaan door experts op het gebied van cyberrisico's. Een analyse van de risico's, de mogelijkheden van preventie en van verzekering zijn belangrijke gespreksonderwerpen.

Dit document beoogt belangrijke handvatten aan te reiken voor constructieve gesprekken over cyberrisico's tussen verzekeringsadviseurs en verzekerden. Daarnaast probeert het misverstanden of misvattingen inzake de verzekering van cyberrisico's weg te nemen.

b. Geen of beperkte dekking op traditionele standaardverzekeringen

De actualiteit toont dat cyberrisico's toenemen en ook dat verzekerden zich steeds meer bewust zijn dat ook zij kwetsbaar kunnen zijn voor deze risico's. Sommige organisaties verwachten nog steeds dat de schade als gevolg van een cyberincident volledig wordt vergoed door 'traditionele' polissen (zoals Brand- en Bedrijfsschade-verzekeringen, Aansprakelijkheidsverzekering voor Bedrijven en Fraudeverzekeringen). Dat blijkt in de praktijk een misvatting te zijn.

Het probleem is dat cyberrisico's vele gedaanten kennen en op verschillende manieren schade kunnen veroorzaken. Niet voor alle schadeoorzaken is dekking op de traditionele polissen. Bovendien sluiten deze polissen in toenemende mate cyberrisico's expliciet uit van dekking.

Wij schetsen dit hieronder in enkele voorbeelden:

- Een brand- en bedrijfsschadeverzekering dekt materiële schade aan zaken (en de daaruit volgende bedrijfsschade) als gevolg van een gedekt evenement. Bij cyberrisico's is er veelal geen materiële schade en data is geen 'zaak'. Cyberschade is daardoor meestal niet gedekt en de daaruit voortvloeiende gevolgschade (bedrijfsschade/extra kosten) dus ook niet; Reconstructie van data kan wel gedekt zijn op een brandpolis.
- Een aansprakelijkheidsverzekering voor Bedrijven (zonder dekking vermogensschade) dekt de aansprakelijkheid ten opzichte van derden voor zaak- en/of personenschade.

Aangezien een cyberincident in verreweg de meeste gevallen tot zuivere vermogensschade leidt heeft een AVB zeer beperkte dekking voor cyber gerelateerde incidenten.

- Een beroepsaansprakelijkheidsverzekering dekt dat deel van de cyberrisico's (aansprakelijkheid t.o.v. derden) die het gevolg zijn van fouten in de uitvoering van de verzekerde professionele diensten maar zal geen dekking bieden voor AVG boetes of bijstand in geval van onderzoeken vanuit AVG.
- Fraudeverzekering dekt uitsluitend verlies van eigen geld, niet de overige schade als gevolg een cyberincident.

c. Ontwikkelingen

Technologie en digitalisering vormen meer en meer de drijvende kracht achter organisaties en supply chains. Hierdoor worden organisaties in alle sectoren kwetsbaarder voor cyberincidenten. Bovendien evolueren cyberdreigingen in rap tempo en richten steeds grotere economische schade aan waardoor de verzekeringsmarkt zich voortdurend blijft aanpassen op gebied van voorwaarden en acceptatiecriteria om het risico verzekerbaar te houden. Naast ontwikkelingen met betrekking tot de dekking voor financiële schade, zien wij bij cyberriskverzekeringen met name toenemende aandacht voor ondersteuning ter voorkoming van incidenten en ter mitigering van de gevolgen van incidenten. Denk hierbij aan een 24/7 hulplijn, de inzet van experts voor ICT-forensisch onderzoek en crisismanagement, juridische experts en PR consultants, en ook aan de inzet van preventie- en risicobeheertools.

In de komende hoofdstukken zullen wij nader ingaan op de specifieke dekkingen van de cyberverzekering, het acceptatieproces van verzekeraars en de incident response.

2. De dekking van een cyberverzekering

In dit hoofdstuk wordt de dekking van de cyberverzekering behandeld. Polisvoorwaarden verschillen qua dekkingsomvang nog aanzienlijk per verzekeraar, daarom beperken wij ons hier tot de dekkingen die over het algemeen geboden worden op een cyberverzekering .

Een cyberverzekering vergoedt de financiële schade die een bedrijf lijdt als gevolg van een digitaal risico, ook een cyberincident genaamd. De definitie van cyberincident kan per verzekeraarsvoorwaarden verschillen, maar in de basis is een cyberincident een lek of een hack.

Lek : datalek, verlies van persoonsgegevens of vertrouwelijke gegevens
Hack : beveiligingsincident zoals:

- Onbevoegde toegang tot het computersysteem van verzekerde
- Een virusuitbraak zoals een ransomware aanval
- Ddos aanval

a. Drie categorieën vergoedingen

De vergoeding van de cyberverzekering is in te delen in drie categorieën:

1. **Incident response diensten** – Toegang tot cyberincident-responsediensten zoals ICT-forensisch onderzoek, Public Relations ter bescherming van het imago, notificatiekosten om klanten te berichten over het cyberincident en juridische diensten om bijvoorbeeld te voldoen aan de AVG. De kosten van (onderdelen van) deze bijstand wordt door verzekeraars veelal voor een bepaalde periode direct en zonder eigen risico vergoed aan de incident response dienstverlener. Sommige verzekeraars dekken deze diensten in natura.

2. **Eigen schade**

   a) Kosten van de response diensten (zie onder 1) die na de eerste periode worden gemaakt

   b) Reconstructiekosten van data

   c) Schade door bedrijfsstilstand

   d) Afpersingskosten (waaronder vaak ook losgeld)

3. **Aansprakelijkheid** – Schadevergoeding en juridische bijstand in geval van aanspraken van derden en onderzoek door de Autoriteit Persoonsgegevens en boetes bij overtreding van de privacyregels (AVG), mits de vergoeding van deze boetes wettelijk is toegestaan.

b. Hoe werkt de cyberverzekering?

Op het moment dat een cyberincident plaatsvindt bij een organisatie, heeft verzekerde recht op incident response diensten. Door de inzet van incident response diensten wordt de schade beperkt die verzekerde en daarmee ook de verzekeraar als gevolg van het incident kan lijden. De kosten die een organisatie maakt om weer operationeel te worden, zoals het weer herstellen van data, opnieuw installeren van software en het virusvrij maken van de IT-omgeving, zijn ook gedekt. Vervolgens is de bedrijfsstilstandschade die verzekerde lijdt vanwege het cyberincident verzekerd. Dit is vergelijkbaar met een brandverzekering.

Indien een organisatie aansprakelijk wordt gesteld, dan zijn de kosten van verweer en rechtsbijstand verzekerd, zelfs als aansprakelijkheid achteraf niet aangetoond is. Dit dekkingselement is vergelijkbaar met een aansprakelijkheidsverzekering en is op “claims made” basis. De schadeveroorzakende gebeurtenis moet dus binnen de looptijd van de verzekering vallen. Verzekeraars willen soms wel het inloop- en uitlooprisico meeverzekeren voor dit dekkingselement. Bekijk hiervoor de van toepassing zijnde polisvoorwaarden.

c. Gebruikelijke uitsluitingen op een cyber verzekering

- Personenschade en zaakschade
- Fraude door eigen medewerkers
- Opzet
- Contractuele aansprakelijkheid
- Schade die leidt tot voordeel van verzekerde, bijv. verbetering van software
- Schade aan illegaal verkregen data of software
- Uitval van infrastructurele diensten zoals internet, telecommunicatie en nutsvoorzieningen

d. Ransomware beperkingen

Sinds 2021 zijn er steeds meer verzekeraars die schade die is ontstaan door een aanval met ransomware (gedeeltelijk) uitsluiten. Aangezien steeds meer bedrijven slachtoffer worden van ransomware aanvallen, lopen de schadelasten voor verzekeraars (en bedrijven) steeds meer op. Om het risico verzekerbaar te houden kiezen verzekeraars er in toenemende mate voor om een dekkingsbeperking door te voeren, waardoor de schade geleden in alle dekkingselementen nog maar voor een gedeelte vergoed wordt. Het overige gedeelte blijft voor rekening van verzekerde. De definitie van ransomware, en daarmee de omvang van de dekking die wordt uitgesloten of beperkt, kan per verzekeraar behoorlijk verschillen. Aangezien dit een grote impact kan hebben op de dekking is het van belang deze clausules zorgvuldig te analyseren zodat uiteindelijk de afweging gemaakt kan worden of de dekking nog voldoende interessant is voor het bedrijf.

3. Acceptatie van cyberverzekeringen

De aanvraag van een offerte voor een cyberverzekering of van de cyberverzekering zelf, vraagt om een goede voorbereiding door de verzekeringsadviseur en de klant samen. Het kan daarbij behulpzaam zijn om de acceptatie overwegingen van verzekeraars te begrijpen. En oog te hebben voor de verschillen tussen een standaard product en een maatwerkproduct. Dit hoofdstuk zal daarop ingaan; daarnaast wordt ingegaan op de belangrijkste hygiëne in cyberbeveiliging, omdat die veelal de basis zijn van acceptatievereisten van verzekeraars.

De aanvraag van een offerte voor een cyberverzekering of van de cyberverzekering zelf, vraagt om een goede voorbereiding door de verzekeringsadviseur en de klant samen. Het kan daarbij behulpzaam zijn om de acceptatie overwegingen van verzekeraars te begrijpen. En oog te hebben voor de verschillen tussen een standaard product en een maatwerkproduct. Dit hoofdstuk zal daarop ingaan; daarnaast wordt ingegaan op de belangrijkste hygiëne in cyberbeveiliging, omdat die veelal de basis zijn van acceptatievereisten van verzekeraars.

Handleiding voor bedrijven en verzekeringsadviseurs

a. Cyber basis hygiëne

Het traject start bij het hebben van een goede basis aan cyberbeveiliging, ofwel de basis cyber hygiëne. Verzekeraars verwachten dat organisaties een goede basis hygiëne hebben voor ze bereid zijn om een cyberverzekering te accepteren. Verzekeraars zijn de laatste jaren steeds kritischer geworden op de mate van beveiliging van ondernemingen. Het Digital Trust Center (DTC) heeft vijf basisprincipes van veilig digitaal ondernemen ontwikkeld die een leidraad kunnen zijn om de cyber basis hygiëne op orde te krijgen.

b. Standaard vs. maatwerk cyberverzekeringen

De meeste verzekeraars – maar ook niet allemaal – hebben een standaard traject en een maatwerk traject. De informatie die de klant moet aanleveren voor een standaardproduct wijkt doorgaans af van de informatie die nodig is voor een maatwerkproduct. Het is dan ook belangrijk om vooraf goed na te gaan of de klant voldoet aan de voorwaarden voor een standaardproduct of dat maatwerk nodig is. Dit voorkomt onnodig langere doorlooptijden, verkeerde interpretatie van premie/voorwaarden en voorkomt het frustratie om nogmaals andere informatie aan te leveren.

c. Standaardproducten

Standaard cyberproducten kennen een sneller en eenvoudiger acceptatieproces. Bij deze standaard producten is in één oogopslag te zien welke dekkingen, premies en acceptatie eisen voor het bedrijf gelden. Het is daarmee heel gemakkelijk een cyberverzekering af te sluiten, maar hierbij dient opgemerkt te worden dat vooraf goed dient te worden bepaald of een onderneming daadwerkelijk in aanmerking komt voor de standaard:

- Voldoet de onderneming aan alle gestelde criteria?
- Heeft men de beveiligingsacceptatiecriteria op orde?
- Zijn er eventueel andere elementen die ervoor kunnen zorgen dat een verzekeraar de aanvraag afwijst?

Ook voor het standaardproduct is een goede voorbereiding een vereiste. De ondernemingen moeten dan aan vooraf vastgestelde toegangscriteria voldoen zoals:

- Een maximale omzet – 25M omzet is veel gebruikt
- Uitgesloten en veelal sectoren met een hoger risicoprofiel, denk daarbij aan financiële instellingen, zorginstellingen, ICT-ondernemingen, overheid etc.
- Een maximumaantal persoonsgegevens dat wordt verzameld of verwerkt (100.000 is veel gebruikt)

Uiteraard zijn er mogelijk meer toegangscriteria die per verzekeraar kunnen verschillen. Het is belangrijk vooraf te beoordelen of een organisatie hierbinnen valt en of het standaardproduct kan worden gebruikt. In die gevallen dat het niet past zal de verzekeraar een maatwerk traject hanteren.

d. Acceptatiecriteria

Verzekeraars hanteren hun eigen standaard acceptatiecriteria. De criteria zien op de mate van beveiliging van een organisatie.

De meeste verzekeraars hanteren acceptatiecriteria die toezien op:

- Het gebruik van meervoudige authenticatie (ook wel 2FA of MFA genoemd) om in te loggen op afstand in het computersysteem (zoals thuiswerken)
- Het beleid ten aanzien van patches (of ook wel updates genoemd) van kritische systemen
- Het back-up beleid van organisaties waarbij de back-ups offline worden bewaard of in een beveiligde Cloud omgeving
- Dit is slechts een overzicht van de meest belangrijke acceptatiecriteria en deze zullen ook per verzekeraar verschillen; daarnaast kunnen deze wijzigen door veranderende omstandigheden in het cyberrisicolandschap. In de voorbereiding naar een (offerte)aanvraag is het zaak dat organisaties hierop zijn voorbereid en de vragen door de juiste personen in de organisatie worden beantwoord.

Negatieve beantwoording van vragen over het in voldoende mate voldoen aan de acceptatiecriteria leidt mogelijk tot afwijzing door de verzekeraar. In de meeste gevallen kunnen de acceptatiecriteria direct als aanbeveling voor verbetering worden gezien. Het vooraf doornemen van de eisen en zo nodig daarop aanpassingen doen, zal het acceptatieproces bespoedigen en afwijzingen kunnen voorkomen.

e. Maatwerk cyberaanvragen

Wanneer een organisatie niet past binnen een standaardoplossing van een verzekeraar, dan zal moeten worden gezocht naar een maatwerkoplossing. Het traject voor het sluiten van een maatwerkproduct is intensiever dan dat voor een standaardproduct. Een goede voorbereiding is nog belangrijker. Verzekeraars nemen geen offerteaanvragen in behandeling wanneer het voor hen niet duidelijk (genoeg) is op welke manier ondernemingen zijn beveiligd.

Voor maatwerktrajecten hanteren verzekeraars andere aanvraagformulieren en strengere eisen dan voor het standaardproduct. Deze formulieren zijn een stuk uitgebreider en het is zaak dat de juiste personen de formulieren invullen – denk daarbij aan hoofd IT, iemand die verantwoordelijk is voor cyber security (zoals een CISO of CIO), maar vergeet ook de Functionaris gegevensbescherming niet (of iemand met vergelijkbare verantwoordelijkheid). Soms hebben verzekeraars ook aanvullende formulieren ter inventarisatie van specifieke risico's zoals ransomware.

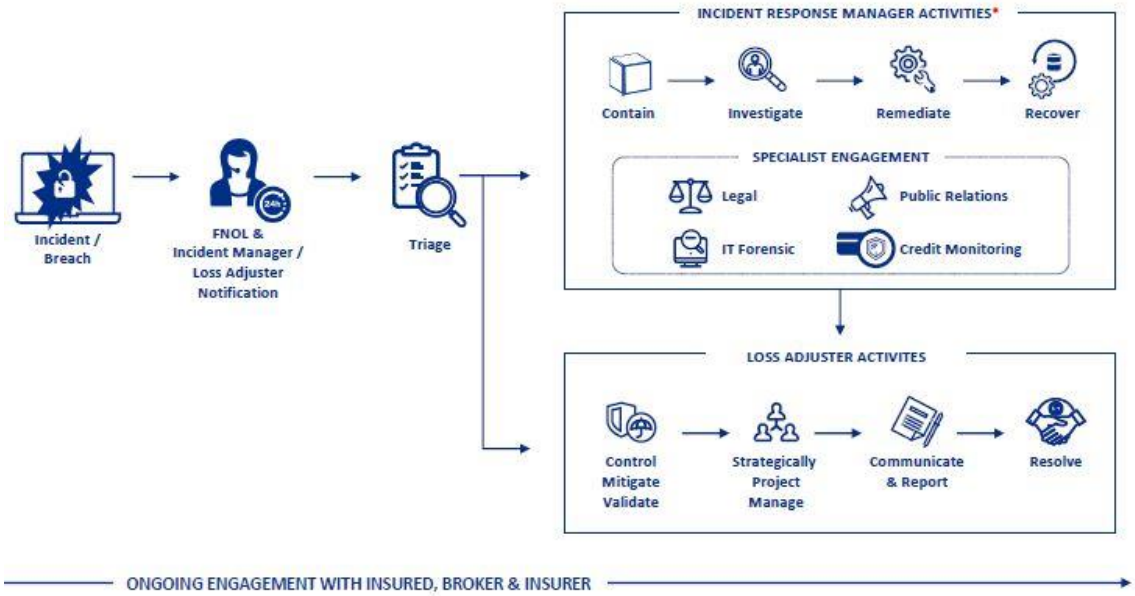
Het maatwerktraject duurt hiermee logischerwijs een stuk langer totdat er een (offerte) aanvraag kan worden ingediend. Het goed voorbereiden en het correct maar ook compleet invullen van de formulieren leidt tot een completer beeld voor de verzekeraar en vergroot de kans op een voorstel.

4. Claims proces - Incident response en schadeafhandeling

Een cyberincident of schade op een cyberpolis kan de verzekerde melden via zijn adviseur. Wanneer er spoed is vereist, kan dat vaak ook via een noodnummer of cyber hotline. Verreweg de meeste cyberpolissen maken gebruik van een zogenaamde cyber hotline waarmee de incident response voor de klant kan worden ingezet.

De incident response is een service en heeft primair het doel om eventuele schade te beperken als gevolg van een gemeld evenement op de cyberpolis. Bij cyberincidenten is snelheid van handelen en maatregelen nemen essentieel voor de beperking van de schade.

Na de incident response fase kan er schade-expertise benodigd zijn om kosten en bedrijfsschade vast te stellen. Vaak gaat de incident response hand-in-hand (schadebeperking) met de schadevaststelling.



Figuur 1: Schematisch weergegeven proces van incident tot schadevaststelling

a. Incident Response

Bij cyberpolissen maken verzekeraars gebruik van externe partners die de incident response volledig kunnen uitvoeren. Meestal is het proces als volgt: Zodra een verzekerde het noodnummer belt, wordt deze in een callcenter te woord gestaan en worden de klantgegevens en kenmerken van het incident genoteerd. Deze eerste melding wordt direct doorgegeven aan de betreffende incident manager die de klant zo spoedig mogelijk terugbelt voor een eerste overleg met de klant. Door het bellen van het noodnummer ontvangt de betrokken verzekeraar ook automatisch een melding van het incident. In feite heeft de verzekerde hiermee het voorval/de schade gemeld.

De incident manager heeft een coördinerende rol in de beheersing van het incident. Afhankelijk van de aard en omvang van het voorval, kan assistentie worden geboden op diverse gebieden. De meest voorkomende benodigde bijstand is op het gebied van IT-forensisch onderzoek en recovery, juridisch advies en crisiscommunicatie. Voor deze specialistische hulp heeft de incident manager meestal een panel van bedrijven gecontracteerd, waarmee gegarandeerd de juiste deskundigheid, beschikbaarheid, snelheid en kosten zijn overeengekomen.

De incident manager adviseert de verzekerde in de te nemen stappen en beslissingen. Hierbij wordt ook de verzekeraar betrokken. De inschakeling van bijvoorbeeld externe specialisten gaat gepaard met kosten en er moeten vaak belangrijke beslissingen worden genomen die ook van invloed kunnen zijn op de dekking. De verzekeraar wil zodoende graag zo vroeg mogelijk betrokken worden in het beslissingsproces.

De incident management fase is voorbij zodra de belangrijkste beslissingen zijn genomen en het incident onder controle is met een redelijke verwachte uitkomst. Deze fase duurt meestal enkele dagen tot hooguit een paar weken, afhankelijk van de omvang en impact van het incident.

b. Schade-expertise

Afhankelijk van de impact van het cyber incident is de inzet van een schade-expert gewenst. Deze expert heeft de taak om de gemaakte kosten en de gevolgschade vast te stellen. De schade-expert zal zich focussen op de gemaakte kosten in relatie tot het incident. Ook wordt gevolgschade in overleg met de verzekerde klant nader in kaart gebracht en vastgesteld.

Voor grotere incidenten kan het daarom wenselijk zijn om direct schade-expertise in te schakelen. Hiermee kunnen keuzes en kosten in een vroeg stadium worden beoordeeld en geaccordeerd.

Het incident en de gevolgen ervan zoals de kosten en de schade zullen door de expert worden beoordeeld, vastgesteld en aan de verzekeraar gerapporteerd. In de praktijk is het daarbij gebruikelijk dat de experts de kosten en schade vaststellen in overleg met de verzekerde klant.