Overwegingen rondom verzekering cyberrisico's

TLP:CLEAR

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

ZA CERT

Inhoud

1. Inleiding

Veel organisaties worstelen met de vraag of het verstandig is een cyberrisicoverzekering af te sluiten. Of om deze te verlengen tegen nieuwe voorwaarden. Z-CERT heeft op basis van ervaringen in het deelnemersveld deze whitepaper opgesteld. Het doel ervan is om zorgaanbieders inzicht te verschaffen in de werking van een dergelijke verzekering en om hen te helpen een passende afweging te maken. Het is nadrukkelijk geen advies om al dan niet te verzekeren. Het is ook géén vergelijkend onderzoek van verzekeraars.

Doelgroep

Deze whitepaper is vooral geschreven voor de rollen die beslissen over het afsluiten van een cyberrisicoverzekering. Bij de ene deelnemer is dat een bestuurder of directeur, bij de andere de IT-manager of juist een financieel verantwoordelijke. Voor een tweede doelgroep, te weten rollen die de besluitvorming ondersteunen, wil dit document de handvatten bieden om een afgewogen advies te kunnen geven.

Leeswijzer

Na dit inleidende hoofdstuk behandelen we in hoofdstuk 2 op hoofdlijnen hoe een polis van een cyberrisicoverzekering er uitziet. Als dat bekend is, kunt u in hoofdstuk 3 de kern van deze white-paper vinden: waarom verzekeren? Of waarom juist niet? In elke paragraaf van dit hoofdstuk komt een belangrijke variabele aan bod. Elke paragraaf bevat handelingsperspectief. Zowel voor het scenario waarin u zich verzekert als wanneer u besluit dit niet te doen...

Bronnen

https://www.digitaltrustcenter.nl/informatie-advies/cyberverzekeringen

https://www.verzekeraars.nl/verzekeringsthemas/schade/cyber

https://www.z-cert.nl/wp-content/uploads/2022/02/Z-CERT_RapportDreigingsbeeld_2021.pdf

https://ondernemersplein.kvk.nl/bestuurdersaansprakelijkheid-en-persoonlijke-aansprakelijkheid/

https://open.overheid.nl/repository/ronl-62106f41-5177-4ae4-9a26-baad7116f59e/1/pdf/antwoorden-kamervragen-over-het-bericht-dat-het-ministerie-van-jenv-de-mogelijkheden-onderzoekt-om-verzekeraars-te-verbieden-om--...-902b8fc.pdf

https://nos.nl/artikel/2398399-overheid-in-actie-tegen-betalen-van-losgeld-aan-ransomware-criminelen

https://ploum.nl/kenniscentrum/nieuws/overwegingen-over-verplichtingen-en-aansprakelijkheden-op-het-gebied-van-cybersecurity-nu-en-in-de-toekomst

Verbeteridee?

Cyberdreigingen en de verzekeringsmarkt zijn sterk in beweging. Wet- en regelgeving over incident response in de zorgsector verandert ook (NIS2). Er komt dus vast een nieuwe versie van deze whitepaper. Verbeterideeën voor die nieuwe versie zijn welkom, liefst via een email naar info@z-cert.nl.

Aan dit document kunnen geen rechten worden ontleend.

2. Kenmerken cyberverzekeringen

In dit hoofdstuk beschrijven we op hoofdlijnen hoe een dekking van een cyberrisicoverzekering er uit ziet en hoe deze aan veranderingen onderhevig is door ontwikkelingen in de wereld, de cybersecuritydreigingen en de verzekeringsmarkt.

2.1. Wat is een cyberverzekering?

Met een cyber(risico)verzekering neemt een verzekeringsmaatschappij een (deel van) een cyberrisico over. Zij doet dit tegen betaling van een premie en onder voorwaarden. Met andere woorden, met een cyberverzekering draagt een zorginstelling de financiële gevolgen van een cyberincident over aan de verzekeraar, waarbij zij zelf wel verantwoordelijk blijft voor dat risico.

De kosten van een polis verschillen sterk. De omvang van de organisatie en het risicoprofiel zijn hierin belangrijke variabelen. In een offertetraject vragen de verzekeraars om een vragenlijst in te vullen over de getroffen beveiligingsmaatregelen binnen de zorginstelling. Aanvullend wordt soms met tests beoordeeld of de maatregelen daadwerkelijk bestaan. Op deze manier bepaalt de verzekeraar het risicoprofiel en daarmee de voorgestelde verzekeringspremie.

2.2. Gangbare dekking

Een cyberverzekering bestaat uit afspraken over de vergoeding van:

- *Incident response*, bijvoorbeeld forensisch onderzoek, juridische ondersteuning. Via de verzekeraar kan de verzekerde de ondersteuning organiseren. Als bij andere partijen ondersteuning ingehuurd wordt, zullen de kosten daarvan normaliter vergoed worden.
- *Aansprakelijkheid*, bijvoorbeeld door derden die schade ondervinden, verweerkosten, claims en boetes.
- *Eigen schade*, waaronder kosten voor herstel van data, eventueel betaald losgeld bij gijzelsoftware, kosten van callcenterservices om betrokkenen bij een datalek te informeren, of de inhuur van een PR bureau om reputatieschade te voorkomen.

Bij de meeste verzekeraars omvat de polis van verzekeringen tegen cyberrisico's een dekking voor risico's rondom gijzelsoftware, datalekken, uitval vanwege DDoS aanvallen en dergelijke. De bij Z-CERT bekende verzekeringen zijn niet modulair opgebouwd.

2.3. Trends in de markt

Verzekeringen voor cyberrisico's zijn in vergelijking met andersoortige polissen nog relatief onvolwassen. Lang niet alle verzekeraars bieden een dergelijke polis aan en de voorwaarden zijn de afgelopen jaren sterk aan verandering onderhevig. Het inzetten van een tussenpersoon kan nuttig zijn om de verschillende verzekeraars met elkaar te vergelijken. Ontwikkelingen die tot veranderingen in de polisvoorwaarden leiden, komen in deze paragraaf aan de orde. In paragraaf 2.4 lichten we enkele recente veranderingen toe.

2.3.1. Gijzelsoftware

Gijzelsoftware of ransomware mag als risico bekend verondersteld worden. Voor zorgaanbieders vaak één van de grotere risico's en de aanleiding om na te denken over een verzekering. De markt voor gijzelsoftware is de laatste jaren steeds professioneler geworden. Het wordt steeds makkelijker om een aanval uit te (laten) voeren en zijn er steeds meer organisaties slachtoffer.

2.3.2. Wijdverbreide incidenten

Soms wordt een organisatie gericht aangevallen. Steeds vaker scannen aanvallers geautomatiseerd op kwetsbaarheden bij organisaties. Ben je kwetsbaar dan word je aangevallen. Bekende voorbeelden hiervan zijn kwetsbaarheden in Microsoft Exchange, log4j, Kaseya, en Solarwinds. Als gevolg van het misbruiken van dergelijke kwetsbaarheden worden in korte tijd zeer veel organisaties aangevallen, wat uiteraard ook leidt tot een ander risicoprofiel voor verzekeraars. Verzekeraars noemen dit 'wijdverbreide incidenten'.

2.4. Reactie verzekeraars op trends

Verzekeraars bieden kortlopende polissen

Ten eerste, vanwege de relatief onvolwassen markt en de beschreven ontwikkelingen willen verzekeraars kortlopende polissen afsluiten. Tegenwoordig is uitzonderlijk en in veel gevallen onmogelijk om een polis voor langer dan 1 jaar af te sluiten. Zo behouden verzekeraars de mogelijkheid om de polis te stoppen en nieuwe voorwaarden of dekkingen af te spreken.

Co-assurantie: hoger eigen risico, lagere dekking

Een tweede gevolg is dat de eigen risico's hoger worden en de dekkingen bij gijzelsoftware en wijdverbreide incidenten vaak een lager bedrag kennen dan de overige onderdelen van de polis. Dit heet in de polis 'co-assurantie': verzekeraar en verzekeringsnemer dragen beide een percentage bij in het afdekken van het risico.

Meer detail in risicobeoordeling

Tenslotte proberen verzekeraars een steeds gedetailleerder beeld te krijgen bij de risico's voordat ze een polis afsluiten met een (zorg) organisatie. Dat houdt in: meer vragen over de volwassenheid van de beveiligingsorganisatie.

De vragen concentreren zich op multifactorauthenticatie, grip op autorisaties, de snelheid van patchen en business continuity management. Meer offertes aanvragen houdt in: meer verschillende vragenlijsten invullen.

2.4.1. Rekenvoorbeeld

We sluiten dit hoofdstuk af met een rekenvoorbeeld om de uitkering bij een mogelijk incident en *fictieve* polisvoorwaarden toe te lichten:

Een verzekeringsnemer heeft een verzekerd bedrag van €4 miljoen per gebeurtenis. Voor gijzelsoftware is een maximum uit te keren bedrag van €2 miljoen afgesproken. Het eigen risico is €250.000 per gebeurtenis en het co-assurantiepercentage voor gijzelsoftware en wijdverbreide incidenten is 50%.

Bij een incident met gijzelsoftware is de schade becijferd op bijvoorbeeld €6.250.000. Met de bovenstaande gegevens leidt dat tot de volgende rekensom:

Geclaimde schade	:	6.250.000
Af: eigen risico	:	250.000
		6.000.000
Af: co-assurantie (50%)	:	3.000.000
		3.000.000
Plafond gijzelsoftware	:	2.000.000

In dit voorbeeld keert de verzekeraar €2 miljoen uit en zijn de overige kosten voor de verzekeringsnemer.

3. Wel of niet verzekeren?

Bij het managen van risico's is het gebruikelijk om onderscheid te maken naar de kans dat een risico heeft en de verwachte impact zodra een risico zich voordoet. Verzekeren is een typische maatregel om risico's af te dekken die zich kenmerken door een kleine kans en een grote impact.

3.1. Algemeen

In algemene zin is het raadzaam om allereerst maatregelen te treffen die de kans van optreden verkleinen. Dit zijn vaak inhoudelijke maatregelen die een verzekeraar vereist voordat het überhaupt mogelijk is om een verzekering af te sluiten.

Voorbeeld:
Het implementeren van multifactorauthenticatie verkleint de kans getroffen te worden door een aanval met gijzelsoftware enorm. Het begin van een dergelijke aanval is namelijk in veel gevallen het misbruik van gelekte inloggegevens. Door multifactorauthenticatie in te zetten lukt het niet om alleen met gebruikersnaam en wachtwoord in te loggen. Een andere zeer belangrijke preventieve maatregel is het snel patchen van ernstige kwetsbaarheden.

Handelingsperspectief
Beoordeel de risico's die u wilt verzekeren. Tref maatregelen om de kans te verkleinen en overweeg daarna(ast) een verzekering als de impact hoog blijft en de kans niet binnen beschikbare middelen verder verkleind kan worden. Of accepteer het restrisico.

3.2. Financieel

De jaarlijkse kosten van een verzekering zijn in veel gevallen fors. Het rekenvoorbeeld uit paragraaf 2.4.1 bevat fictieve maar realistische bedragen. Vanuit financieel oogpunt is het van belang om in ogenschouw te nemen of er een reservering of voorziening voor calamiteiten bestaat en of het qua liquiditeit mogelijk is om een piek in de kosten op te vangen. Als beide niet het geval is, wordt het aantrekkelijker om te verzekeren.

Het ministerie van J&V heeft in 2021 aangegeven dat er geen voornemens zijn om het betalen van losgeld in het kader van gijzelsoftware wettelijk te verbieden. Wel wordt onderzocht of het mogelijk is verzekeraars te verbieden dit losgeld te vergoeden. Bij het schrijven van dit document, was de status dan wel de uitkomst van dit onderzoek nog niet bekend.

Handelingsperspectief
Als alternatief voor de premiebetalingen van een verzekering van cyberrisico's kunt u jaarlijks een bedrag begroten om een voorziening te treffen voor cyberincidenten of om extra preventieve maatregelen te implementeren.

3.3. Ondersteuning bij incidenten

Het is gangbaar dat een verzekering als onderdeel van de polis inhoudelijke ondersteuning biedt om de schade van een incident zo klein mogelijk te maken. In die gevallen geldt een randvoorwaarde dat een incident kort na detectie gemeld wordt bij de verzekeraar. Niet of te laat melden kan betekenen dat de verzekeraar niet uitkeert. Neem dit dus op in uw incident response draaiboek.
De ondersteuning van een verzekeraar gaat verder en is breder dan de ondersteuning die Z-CERT haar deelnemers kan bieden. Z-CERT zal niet namens u met hackers onderhandelen of forensisch onderzoek uitvoeren. Een verzekeraar kan op deze vlakken wel professionele ondersteuning bieden.

Handelingsperspectief
Als u besluit zich niet te verzekeren, overweeg dan om een geschikte marktpartij te contracteren met als doel om in geval van incidenten forensische, IT- of andere benodigde expertise in te huren. Een dergelijke marktpartij zal in veel gevallen alvast voorbereidende werkzaamheden uitvoeren, door bijvoorbeeld te checken of de preventieve maatregelen effectief zijn en uw IT-omgeving te leren kennen. Daardoor kan men in geval van een incident direct aan de slag.

Let op: als u ondersteuning krijgt via een verzekeraar, dan heeft de verzekeraar normaalgesproken meerdere marktpartijen gecontracteerd en is de kans dus groter dat er een marktpartij is die capaciteit heeft om u te helpen. Als u zelf een marktpartij contracteert is het dus belangrijk om beschikbaarheidsafspraken te maken. Bijvoorbeeld gegarandeerde ondersteuning binnen 4 uur na het doen van een melding.

3.4. Bestuurdersaansprakelijkheid

Als een bestuurder zijn taken niet goed uitvoert kan hij of zij daarvoor persoonlijk aansprakelijk gesteld worden. Bestuurdersaansprakelijkheidsverzekeringen dekken dit risico af. In de polissen van die verzekeringen worden claims vanwege wanbeleid rondom cyberdreigingen soms expliciet uitgesloten.

Handelingsperspectief

In het kader van bovenstaande aansprakelijkheid is het raadzaam om de afwegingen rondom het afsluiten van een cyberrisicoverzekering goed vast te leggen en te delen met de Raad van Toezicht. Het afsluiten van een cyberrisicoverzekering kan immers achteraf als wanbeleid uitgelegd worden (geldverspilling) en het niet afsluiten ook (onaanvaardbaar risico). Als de NIS2 wetgeving in Nederland van kracht wordt, veranderen de eisen rondom informatiebeveiliging bij zorgaanbieders. Het is daarom belangrijk om de ontwikkeling rondom deze wetgeving te volgen.

3.5. Inzicht in IT-kwetsbaarheden

Vanuit IT-perspectief is het offertetraject van een cyberrisicoverzekering tijdrovend omdat er relatief veel informatie opgevraagd wordt door de kandidaat-verzekeraar. Tegelijkertijd is dit ook een kans om inzicht te krijgen in de kwetsbaarheden. Allereerst natuurlijk doordat de vragenlijsten ook inzicht geven in nog te treffen maatregelen in de IT-infrastructuur. Maar ook omdat sommige verzekeraars standaard een open poort scan uitvoeren op de te verzekeren domeinen of inloggegevens verstrekken voor een tool waarmee een beperkt aantal weken te zien is hoe kwaadwillenden vanaf het publieke internet naar de te verzekeren IT-omgeving kijken: zien ze besmette endpoints? Zijn oude communicatieprotocollen nog actief? Het gebruik van dergelijke tooling biedt mooie kansen tot verbetering.

Handelingsperspectief
Vraag voorafgaand aan het offertetraject aan de kandidaat verzekeraars hoe zij uw risicoprofiel gaan beoordelen. Vraag een zeer beperkt aantal offertes aan en overweeg daarbij ten minste één partij te betrekken die u gedetailleerd inzicht geeft in bovengenoemde kwetsbaarheden.

De in paragraaf 3.3 behandelde marktpartijen zullen aan het begin van een samenwerking normaliter ook een dergelijke analyse maken. Of: laat uw omgeving zelf met behulp van tooling scannen op kwetsbaarheden die vanaf internet te misbruiken zijn.

Nota bene
Z-CERT verwacht op termijn met de Kwetsbaarheden Analyse Tool (KAT) van het ministerie van VWS een dergelijke scan dienst aan te kunnen bieden aan deelnemers.

3.6. Verzekeren in relatie tot uitbestede IT

Veel zorgaanbieders maken gebruik van één of meer SaaS-diensten. Kleinere zorgaanbieders hebben soms hun volledige IT uitbesteed aan een IT-dienstverlener. In dit soort situaties dringt de vraag zich op of een cyberverzekering waarde heeft: de verantwoordelijkheid ligt toch bij de leverancier?

Hoewel je een dienst uitbesteedt, blijf je als zorgaanbieder zelf eindverantwoordelijk. De leverancier heeft een zorgplicht maar dat is geen resultaatverplichting. Het is daarom nodig om contractuele afspraken te maken over verantwoordelijkheden en bijkomende aansprakelijkheid. Een verzekering kan kosten dekken die niet onder de aansprakelijkheid van de leverancier vallen. En andersom, verzeker vooral geen diensten die wel onder de aansprakelijkheid van de leverancier blijken vallen. Hier ligt het risico van onder- én oververzekering op de loer.

Handelingsperspectief
Maak heldere afspraken over welke partij voor welke dienst en welke beveiligingsmaatregel verantwoordelijk is. Evalueer aansprakelijkheidsafspraken in uw contracten met leveranciers en probeer deze bij (her)contracteringen passend af te spreken.
De hoogte van afgesproken aansprakelijkheidsbedragen en de situaties waarin u een leverancier aansprakelijk kunt stellen zijn input voor uw risicoprofiel en de afweging om al dan niet te willen verzekeren. Ga in de aangeboden verzekeringspolis goed na hoe de polis werkt in voornoemde situatie dat u schade heeft door een incident bij een leverancier.

3.7. Ethisch

Cyberrisicoverzekeringen worden door deelnemers vooral ingezet om het risico van gijzelsoftware te verzekeren. Polissen omvatten in de regel ook dekking voor het betaalde losgeld. Daarbij hoort de principiële vraag of je losgeld wilt betalen aan de aanvaller. Zie ook paragraaf 3.2 over ontwikkelingen vanuit de overheid omtrent het betalen van losgeld.

Het tegengeluid is dat losgeld betalen ethisch juist goed te verantwoorden is, omdat je hoogstwaarschijnlijk door losgeld te betalen de totale kosten van een aanval lager houdt dan als je niet wilt betalen. Daarnaast zal bij het betalen van losgeld in veel gevallen de doorlooptijd van herstel korter zijn, wat de overlast voor patiënten, cliënten en (zorg)medewerkers beperkt. Overigens is het betalen van losgeld geen garantie voor snelle ontsleuteling of het niet openbaar maken van buitgemaakte gegevens.

Handelingsperspectief
Neem nu een standpunt in over de vraag al dan niet losgeld te willen betalen (en documenteer dat goed gezien paragraaf 3.4). Het is nu een betere tijd om hierover het gesprek aan te gaan dan tijdens de looptijd van een aanval met gijzelsoftware.

3.8. Samenvatting en conclusie

Het afsluiten van een cyberverzekering maakt een IT-omgeving niet veiliger. De kans op een aanval of datalek wordt niet kleiner door een verzekering. Met een cyberverzekering kunt u risico's op cyberincidenten deels overdragen aan een verzekering. Het is daarom allereerst belangrijk om te bepalen welke risico's u onderkent en hoe u deze wilt behandelen. Neem daarin ook de risico's bij belangrijke leveranciers in ogenschouw. Vooral risico's met kleine kans en grote impact komen in aanmerking om te verzekeren. Ook de omvang van een aanwezige calamiteitenreserve is belangrijk om in ogenschouw te nemen.

De in dit hoofdstuk beschreven overwegingen beogen u te helpen bij het maken van de afweging over het afsluiten van een cyberverzekering. Of een cyberverzekering de meest geschikte risicobeperkende maatregel is, valt niet in zijn algemeenheid te beantwoorden. Alternatieven zijn investeren in preventieve maatregelen en/of het contracteren van een marktpartij om op het moment van een groot incident extra expertise beschikbaar te hebben.

Stichting Z-CERT
Stationsplein 121
3818 LE Amersfoort
033 737 06 09

info@z-cert.nl
www.z-cert.nl