Informatie-fiche

2018

Cyber Plan

Verzekering tegen cyberrisico's

In België doen dagelijks 36 slachtoffers aangifte van cyberaanvallen. Volgens specialisten zal dit aantal de volgende jaren ongetwijfeld nog toenemen. Om uw klanten te beschermen tegen deze bedreigingen lanceert Allianz Cyber Plan: een hybrideverzekering die aansprakelijkheid, bedrijfsschade, eigen schade en informaticabijstand combineert.

Voordelen van Cyber Plan

Cyber Plan dekt de immateriële schade veroorzaakt door cyberaanvallen. Belangrijkste troeven:

- 4 waarborgluiken voor een optimale dekking (aansprakelijkheid, bedrijfsschade, kosten in geval van een crisissituatie en eigen schade)
- Verzekerd kapitaal vanaf 250.000 euro per schadegeval en per verzekeringsjaar
- Hogere bedragen of dekking op maat zijn mogelijk op aanvraag
- 24/7 bijstand van een gespecialiseerd advocatenkantoor en IT-experten om onmiddellijk gepast te reageren op een verzekerd schadegeval
- Eén lage vrijstelling vanaf 2.500 euro
- Duidelijke en transparante algemene voorwaarden
- Bijstand zonder vrijstelling gedurende de eerste 72 uur
- Tegemoetkoming bij kennisgeving in het raam van GDPR

Doelgroep

Cyber Plan richt zich tot alle bedrijven:

- gevestigd in België, zonder enige ondergrens qua grootte
- die de zuivere immateriële schade willen verzekeren waaraan ze zouden kunnen blootgesteld zijn
- voor quasi alle bedrijfsactiviteiten

en biedt hen

- een snel onderschrijfbare standaardoplossing als zij een omzet tot 100.000.000 euro realiseren
- een oplossing op maat als zij een omzet tussen 100.000.000 en 250.000.000 euro realiseren.

Verzekeringnemer

De vennootschap, rechtspersoon.

Je Makelaar Je beste Verzekering

Allianz

Allianz Benelux n.v. – Lakensestraat 35 – 1000 Brussel – Tel.: +32 2 214.61.11 – www.allianz.be – BTW: BE 0403.258.197 – RPR Brussel – Verzekeringsmaatschappij toegelaten door de NBB (Nationale Bank van België) onder codenummer 0097 om alle takken "Leven" en "niet-Leven" te beoefenen – NBB Hoofdzetel: de Berlaimontlaan 14, 1000 Brussel, www.nbb.be
Verantwoordelijke uitgever: G. Deschoolmeester – Lakensestraat 35 – 1000 Brussel – Tel. : +32 2 214 61 11 – 18JUN137

Gedetailleerd overzicht van de waarborgen

Waarborgen aansprakelijkheid	
Inbreuk op persoonsgegevens en aantasting van computergegevens Dekking: • Inbreuken op persoonsgegevens (niet-gemachtigd(e) toegang, gebruik of verspreiding van persoonsgegevens opgeslagen in het computersysteem van de verzekeringnemer of van een dochteronderneming) • Aantasting van computergegevens (met name de niet-opzettelijke mededeling en/of verspreiding van klantgegevens door de verzekerde of door de leverancier van uitbestede diensten).	
Ongeoorloofde toegang tot het netwerk Vergoeding van: • het bedrag van de schadevergoeding • de kosten voor de verdediging voortvloeiend uit een schade-eis tegen een of meer verzekerden en ten gevolge van een ongeoorloofde toegang (bijvoorbeeld: een cyberaanval ten gevolge van een handeling, een fout of een nalatigheid van een verzekerde).	
Inbreuk via publicatie/verspreiding van data Vergoeding van: • het bedrag van de schadevergoeding • de kosten voor de verdediging • voortvloeiend uit een schade-eis tegen een of meer verzekerden en ten gevolge van een inbreuk via publicatie/verspreiding van data. Zijn met name gedekt: de publicatie of verspreiding door de verzekerde van digitale gegevens die aan de oorsprong liggen van: • een niet-opzettelijke inbreuk op de intellectuele eigendomsrechten • laster • een inbreuk op het recht op de eerbiediging van het privéleven van een persoon • de verspreiding van persoonsgegevens of de toe-eigening met commerciële doelen van de naam, het beeld of het uiterlijk van een persoon • een geval van oneerlijke concurrentie enz.	
Administratieve sancties Vergoeding van: • het bedrag van de kosten voor de verdediging • de administratieve sancties zoals de boetes en financiële sancties die aan een verzekerde worden opgelegd ten gevolge van een schade-eis die wordt geformuleerd door een toezichthouder.	

Schade-eisen van leveranciers van elektronische betaaldiensten
Dekking van:
- de schadevergoedingen
- de contractuele boetes
- de kosten voor de verdediging

die voortvloeien uit een schade-eis die wordt ingediend door een leverancier van elektronische betaaldiensten en die gebaseerd is op de niet-opzettelijke schending van eender welke PCI-normen voor gegevensbeveiliging.

Waarborg bedrijfsschade

Dekking van de bedrijfsschade ten gevolge van een onderbreking van de activiteit die te wijten is aan de volledige of gedeeltelijke ontoegankelijkheid van het computersysteem.

Waarborg kosten in geval van een crisissituatie

Kosten van de consultant die de verliezen moet berekenen
Dekking van de erelonen van elke IT-deskundige om de omvang en het bedrag van de verliezen te bepalen.

! Kosten om vast te stellen of een schadegeval gedekt is, zijn uitgesloten.

Kosten van de crisiscommunicatie-consultants
Vergoeding van de erelonen van een crisiscommunicatie-consultant met het oog op het verminderen van de negatieve gevolgen voor de goede naam van de verzekerde.

Kosten voor digitaal onderzoek
Dekking van de erelonen van elke IT-deskundige met het oog op het vaststellen van het al dan niet bestaan en de omvang van:
- een inbreuk op de persoonsgegevens
- een aantasting van computergegevens
- een voorval van bedrijfsschade.

! Deze kosten zijn slechts gedekt indien de verzekerde beschikt over voldoende gegevens om redelijkerwijze het bestaan te vermoeden van de bovenvermelde inbreuken en aantastingen.

Interventiekosten

In geval van een inbreuk op persoonsgegevens of een aantasting van computergegevens worden de erelonen van elke IT-deskundige gedekt voor:

- de analyse van het computersysteem met het oog op de vaststelling van:
- het bestaan, de oorzaak en de omvang van de inbreuk op de persoonsgegevens of de aantasting van computergegevens
- de manier waarop de gevolgen ervan verminderd kunnen worden.
- de identificatie en bewaring van computergegevens die belangrijk zijn in het computersysteem van de verzekerde vennootschap
- de adviezen aan de verzekerde over zijn wettelijke verplichting om alle slachtoffers, klanten en toezichthouders te informeren over een inbreuk op persoonsgegevens of een aantasting van computergegevens
- de kennisgeving van de inbreuk op persoons-gegevens of de aantasting van computergegevens aan een persoon-slachtoffer, aan een derde of aan een toezichthouder, in overeenstemming met de wettelijke verplichtingen
- de adviezen aan de verzekerde over de vergoe-dingsverplichtingen die zijn opgenomen in elk schriftelijke overeenkomst die werd ondertekend tussen de verzekerde en elke derde-dienstverlener
- het beschikbaar maken van een telefonisch informa-tieplatform voor personen-slachtoffers en derden
- het vaststellen en verstrekken aan personen-slacht-offers en aan klanten van:
  - nieuwe referenties van bankrekeningen
  - kredietcontrolediensten (tot zes (6) maanden na de datum van de genoemde inbreuk of aantas-ting)
  - adviezen in verband met het schadegeval met het oog op de naleving van elke andere wettelijke vereiste met betrekking tot de inbreuk op persoonsgegevens die door de verzekerde ten aanzien van de personen-slachtoffers moet worden vervuld.

Uitsluitend indien deze praktijken bij wet zijn toegestaan.

Kosten voor herstel Dekking van de kosten voor het inschakelen van een IT-deskundige ten gevolge van een inbreuk op persoonsgegevens of een aantasting van computergegevens of een voorval van bedrijfsschade om: • het computersysteem van de verzekerden te herstellen in een toestand die vergelijkbaar is met deze van vóór het schadegeval. • de computergegevens of de computerprogramma's van de verzekerden te herstellen, te recupereren of opnieuw te installeren (inclusief de aankoopkosten voor softwarelicenties die nodig zijn om deze computergegevens of computerprogramma's te reproduceren).	Met uitsluiting van: • de kosten om elke beslissing tot herstel na te leven op grond van een uitvoeringsbevel of elk ander herstel in natura en/of op niet-geldelijke wijze, elke toekenning van een dergelijk herstel of elk akkoord ter uitvoering van een dergelijk herstel • de kosten voor de verdediging en de uitgaven van alle aard • de kosten die de verzekerde zou hebben moeten maken als er zich geen voorval van bedrijfsschade zou hebben voorgedaan • de kosten voor het ontwerp, de upgrade, het onderhoud of de verbetering van het computersysteem of van de computerprogramma's • de eigen interne kosten van de verzekerde, met inbegrip van de sociale lasten en de algemene kosten • de kosten voor het herstellen van de gegevens of de computerprogramma's die uitsluitend opgeslagen zijn in het werkgeheugen of in het systeemgeheugen ("RAM").
Waarborgen eigen schade	
Cyberafpersingskosten Terugbetaling van de verliezen geleden ten gevolge van een dreiging tot cyberafpersing.	Dekkingsvoorwaarden: De verzekerde moet: • alle noodzakelijke maatregelen nemen om het bestaan van deze waarborg niet bekend te maken, tenzij deze bekendmaking vereist wordt door de wet. • de betrokken politiediensten of elke publieke autoriteit informeren en volledig met hen meewerken en klacht indienen wegens dreiging tot afpersing binnen 48 uur na de dreiging. • de verliezen te wijten aan de dreiging beperken door een gespecialiseerd advies inzake beveiliging in te schakelen (met schriftelijke toestemming van Allianz). Sublimiet van 25% van het verzekerde bedrag, per schadegeval en per verzekeringsjaar.
Cyberdiefstal Terugbetaling van het giraal geld dat werd gestort of overgeschreven van de rekeningen van de verzekerde vennootschap naar een rekening van een derde als gevolg van een cyberaanval.	Sublimiet van € 50.000 per schadegeval en per verzekeringsjaar.

Omvang van de dekking

Territorialiteit
De waarborg geldt wereldwijd.

In de tijd
Allianz dekt:
- de schade-eisen die worden geformuleerd tijdens de geldigheidsperiode van de overeenkomst
- voor feiten die zich voordeden of fouten die werden begaan
  - tijdens de geldigheidsperiode van de overeenkomst
  - of zelfs vóór de overeenkomst (maar niet gekend bij de ondertekening), en dit zonder tijdslimiet
- de klachten die worden geformuleerd binnen 36 maanden na de overeenkomst en die betrekking hebben op feiten die zich voordeden of fouten die werden begaan tijdens de geldigheidsperiode van de overeenkomst.

Premie

Vanaf 600 euro (exclusief taksen)

Vrijstelling

- Vanaf 2.500 euro
- voor de waarborg bedrijfsschade: periode van 8 uur. Wanneer deze periode overschreden wordt, dekt de tussenkomst de verliezen vanaf het eerste uur van de onderbreking, uitsluitend met aftrek van de geldende forfaitaire vrijstelling.

Taksen

9,25%

Verzekerde bedragen

Formules naar keuze vanaf 250.000 euro.

Vereenvoudigde onderschrijving

Voor Cyber Plan is een snelle vereenvoudigde standaardonderschrijving mogelijk onder de volgende voorwaarden:

1. **De activiteiten en/of producten van de verzekeringsnemer en zijn filialen zijn niet gelinkt aan de volgende landen of gebieden welke, onder andere, het voorwerp uitmaken van internationale economische sancties en/of embargo's. In september 2017 betreft het de volgende landen:**

   Afghanistan, Armenië, Azerbeidzjan, westelijke Balkanlanden, Wit-Rusland, Myanmar, Burundi, Centraalafrikaanse Republiek, China, Cuba, Democratische Republiek Congo, Égypte, Éritrea, Guinea, Guinee-Bissau, Iran, Irak, Libanon, Liberia, Libië, Noord-Korea, Rusland, Somalië, Soedan (Zuid), Soedan (Noord), Syrië, Tunesië, Oekraïne, het Oosten van Oekraïne (Provincies Donetsk, Kharkiv, Louhansk, Zaporizhia en Dnipropetrovsk), de Krim (met inbegrip van zijn territoriale wateren en Sebastopolis), Yemen, Venezuela, Zimbabwe.

   Deze lijst evolueert met de tijd en wij staan tot uw beschikking om u de bijgewerkte informatie te bezorgen over dit onderwerp.

2. **De verzekeringnemer en zijn filialen zijn niet actief in de volgende sectoren die onderworpen zijn aan sectoriële sancties.**

   - Wapens, goederen en technologieën voor militair gebruik, met inbegrip van software bestemd voor militair gebruik.
   - Goederen voor dubbel gebruik, producten en technologieën die een militaire toepassing kunnen hebben.
   - Olie- en gasindustrie (meer bepaald met inbegrip van ruwe petroleum, gas alsook elk ander afgewerkt of halfafgewerkt product).
   - Technologieën bestemd voor gebruik in de nucleaire sector, met inbegrip van software (alle types vermengd).

- Uitvoer van grafiet, ruwe of halfafgewerkte metalen met inbegrip van ijzer, staal, koper, nikkel, aluminium, lood, zink, tin of elk ander basismetaal.
- Uitrusting, technologie en software die kunnen gebruikt worden voor bewaking.
- Uitrusting die kan gebruikt worden voor interne repressie.
- Culturele goederen en andere goederen die een belangrijk archeologisch, historisch, cultureel, wetenschappelijk, zeldzaam of religieus belang hebben.
- Elektriciteitscentrales op steenkool/bruinkool.
- Seksindustrie.
- Kansspelen en weddenschappen.
- Productie of gebruik van asbest.
- Diamanthandel.

3. De verzekeringsnemer en zijn filialen hebben geen activiteiten in volgende industrieën: kansspelen, luchtverkeersleiding, overheidsinstantie, financiële instellingen en pornografie.

4. De geconsolideerde omzet van de verzekeringsnemer en zijn filialen is niet hoger dan 100.000.000 EUR.

5. De geconsolideerde omzet van de verzekeringsnemer en zijn filialen in USA is minder dan 10% van de totale geconsolideerde omzet.

6. De geconsolideerde omzet van de verzekeringsnemer en zijn filialen in e-commerce is minder dan 50% van de totale geconsolideerde omzet.

7. De verzekeringsnemer en zijn filialen hebben minder dan 1 miljoen PII gegevens (Personally Identifiable Data).

   Een persoonsgegeven is iedere informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de "betrokkene" genoemd in de Privacywet). Anders gezegd, een persoonsgegeven is elk gegeven dat in verband kan worden gebracht met een natuurlijke persoon. Het kan gaan om de naam van een persoon, een foto, een telefoonnummer, zelfs een telefoonnummer op het werk, een code, een bankrekeningnummer, een e-mailadres, een vingerafdruk. Om de geschatte hoeveelheid gegevens te schatten, gelieve het aantal "natuurlijke personen" type klanten te berekenen, met wie u werkt in het kader van uw activiteit.

8. De verzekeringsnemer en zijn filialen bevestigen dat ze veiligheidssoftware en controles (zoals anti-virus) op hen IT-systemen en hardware hebben.

9. De verzekeringsnemer en zijn filialen bevestigen dat ze toegangscontrole tot gevoelige data beperkt tot die personen die toegang nodig hebben tot deze data.

10. De verzekeringsnemer en zijn filialen bevestigen dat ze back-up en recovery procedures van toepassing voor "mission critical" systemen, data's en informatie hebben.

11. De verzekeringsnemer is gevestigd in België.

12. De verzekeringsnemer behoort niet tot een andere rechtspersoon (verzekeringsnemer is geen filiaal van een andere juridische entiteit).

13. De verzekeringsnemer en zijn filialen hebben geen cyber polis reeds onderschreven bij AGCS/Allianz Benelux.

14. De verzekeringsnemer en zijn filialen hebben in de afgelopen 3 jaar geen cyber schadegevallen gehad en zijn is niet op de hoogte van omstandigheden die zouden kunnen aanleiding geven tot een onderzoek of schade-eis.

Het bedrijf voldoet niet aan de criteria? Een offerte op maat is ook mogelijk.