Cyberverzekering

Informatiedocument over het verzekeringsproduct

Onderneming: AIG Europe S.A., Netherlands branch, schadeverzekeraar, vergunning: 12046265 (NL)

Product: ProfessionalEdge Cyber

Dit informatiedocument geeft alleen een samenvatting van de verzekering. In de polisvoorwaarden staat uitgebreid waarvoor iemand wel en niet is verzekerd.

Welk soort verzekering is dit?

Met deze verzekering verzeker je je bedrijf tegen de gevolgen van Cyberincidenten zoals hacking, virussen, malware en ransomware, DDoS-aanvallen en datalekken maar ook fouten tijdens het gebruik, onderhoud of de verbetering van het ICT-systeem.

Extra informatie

{Mogelijk extra detail-informatie of toelichting van begrippen}

Wat is verzekerd?

✔ Deze verzekering dekt de financiële gevolgen van een cyberincident zoals hacken, ransomware en datalekken.

Verzekerd bedrag

✔ Afhankelijk van de keuze maar een limiet vanaf EUR 100.000,00 per evenement per jaar is mogelijk.

First response

✔ Deze dekking biedt direct toegang tot een juridisch adviseur, cyber IT-expert en PR-specialist. Zij helpen u in de meest kritische periode van een cyberincident: de eerste 48 uur. In deze periode heeft u geen eigen risico.

Incident Management

✔ Incident Management biedt na de first response dekking voor alle additionele noodzakelijke kosten voor de juridische, IT én PR-diensten. Hiernaast is er dekking voor het monitoren van verloren data, herstellen van data en de kosten om betrokkenen te informeren.

Cyberafpersing

✔ Cyberafpersing biedt dekking als u slachtoffer wordt van afpersing, of als u daartoe bedreigd wordt. De meest bekende vorm van Cyberafpersing is ransomware. Dit is inclusief de dekking voor losgeld om de afpersing te stoppen, maar ook vergoedingen voor adviseurs om u daarbij bij te staan in het onderhandelingsproces.

Wat is niet verzekerd?

✖ Veroorzaak je zelf met opzet schade? Of fraudeer je? Dan is dat niet verzekerd.

Storingen

✖ Elektronisch of mechanisch gebrek van infrastructuur die niet onder het beheer van de verzekerde valt, is uitgesloten van de dekking. Daarnaast is er ook geen dekking voor satellietuitval.

Personen- en/of zaakschade

✖ Niet verzekerd is lichamelijk letsel, ziekte of overlijden en verlies of vernietiging van zaken, anders dan gegevens.

Sanctiewetgeving

✖ Uitgesloten zijn schadeuitkeringen die toezien op sancties die zijn ingesteld naar aanleiding van een schendig of bedreiging van de internationale vrede en veiligheid. De Verenigde Naties (VN) en de Europese Unie (EU) hanteren al jaren sancties tegen bepaalde landen, met als doel de activiteiten of het beleid in die landen te veranderen. Sancties kunnen ook gelden voor een organisatie of een persoon.

Zijn er dekkingsbeperkingen?

Eigen Risico

! Voor deze verzekering geldt altijd een eigen risico behalve voor de First response service

Telefoonhacking en Computercriminaliteit

✔ Telefoonhacking vergoedt de kosten als u telefoonkosten heeft door ongeoorloofd toegang tot uw telefoonsysteem. Computercriminaliteit vergoedt frauduleuze bank overboekingen indien cybercriminelen zijn binnengedringen in uw ICT-netwerk. Deze financiële schade wordt vergoed met een sublimiet van EUR 100.000 voor telefoonhacking en EUR 25.000 voor computercriminaliteit.

Boetes & Aansprakelijkheid

✔ Dit onderdeel biedt dekking voor claims van derden door het falen van de netwerkbeveiliging of verlies van gegevens. Er is dekking voor de kosten van juridische verdediging en vergoeding van de aansprakelijkstelling. Ook is de juridische verdediging door een onderzoek van een toezichthouder gedekt, net als een daaruit voortvloeiende wettelijk te verzekeren boete.

Bedrijfsschade: netwerkonderbreking

✔ Netwerkonderbreking dekt bedrijfsschade als gevolg van stilstand van IT systemen na een cyberincident. Vergoed is het verlies in netto-inkomen en bijkomende vaste kosten, zoals personeel en huur. Maar ook de extra kosten die gemaakt moeten worden om zo snel mogelijk weer up en running te zijn. Netwerkonderbreking IT Outsourcer dekt bedrijfsschade als gevolg van een cyberincident bij uw IT-dienstverlener.

Ransomware

! In sommige gevallen kan het zijn dat er voor ransomware aanvallen een beperktere dekking geldt. Meestal met een sublimit ter hoogte van de helft van het totale limiet, waarbij voor iedere schade die toeziet op ransomware, de helft (50%) van de schade wordt vergoed tot maximaal het sublimiet. De andere helft wordt door uzelf bijgedragen. Voor alle andere cyberincidenten geldt dan nog wel het volledige limiet.

Waar ben ik gedekt?

✔ De dekking geldt wereldwijd, ook in de Verenigde Staten en Canada.

Wat zijn mijn verplichtingen?

Als je de verzekering aanvraagt, moet je onze vragen eerlijk beantwoorden. Je moet zoveel mogelijk doen om schade te voorkomen en beperken. Meld schade zo snel mogelijk en geef veranderingen in je situatie zo snel mogelijk door.

Hoe en wanneer betaal ik?

Je betaalt de premie jaarlijks.

Wanneer begint en eindigt de dekking?

De verzekering begint op de datum die op de polis staat. Betaal je de premie niet op tijd? Dan kunnen we de verzekering stoppen.

Hoe zeg ik mijn contract op?

Je kunt de verzekering schriftelijk opzeggen rekeninghoudend met een opzegtermijn van 2 maanden.

Versie 4, 28-03-2024, Bekijk online: verzekeringskaarten.nl/aig/cyber-verzekering