Informatiekaart
Cyber 360

MARKEL

Informatiekaart Cyber 360

De Cyber 360 verzekering biedt een complete cyberdekking voor het MKB via een eenvoudig acceptatietraject. In deze informatiekaart zetten we de highlights voor u op een rij. Voor een gedetailleerdere beschrijving van de dekking verwijzen wij u naar de verzekeringskaart.

Acceptatie

- **Standaardproduct**: De Cyber 360 is een standaardproduct wat betekent dat de acceptatiecriteria, de premie, de voorwaarden en de verzekerde bedragen vooraf zijn bepaald. De verzekering is eenvoudig en direct af te sluiten door middel van een verkort aanvraagformulier waarin tevens de premiematrix is opgenomen. Indien gewenst kunnen wij op basis van het aanvraagformulier eerst een offerte afgeven. Ook kunnen wij offertes uitwerken op basis van aanvraagformulieren van andere verzekeraars of uitsluitend op basis van de omzet en de aard van de activiteiten. Mocht uw klant niet in aanmerking komen voor de Cyber 360, informeer dan naar onze maatwerkmogelijkheden.
- **Doelgroep**: De Cyber 360 verzekering is bedoeld voor binnen Nederland gevestigde privaatrechtelijke organisaties met een geconsolideerde jaaromzet tot €20.000.000.
- **Uitgesloten branches**: Een beperkt aantal branches is uitgesloten van de standaardpropositie waaronder; professionele gegevensverwerkers, IT-dienstverleners (uitgezonderd softwareontwikkeling en IT-consultancy), high-tech bedrijven en overheidsinstellingen.
- **Niet uitgesloten branches**: Financiële dienstverleners, advocaten, notarissen, logistieke dienstverleners, zorginstellingen en webshops sluiten wij niet uit voor de Cyber 360. Onze propositie bedient daarmee een zeer brede doelgroep.
- **Maximum aantal persoonsgegevens**: Om binnen de acceptatiecriteria te vallen dient de aanvrager de persoonsgegevens van minder dan 100.000 personen te verwerken. Voor medische gegevens ligt de grens op 25.000 personen en creditcardgegevens op 10.000 personen.
- **Dochtermaatschappijen**: Alle huidige en nieuwe Nederlandse meerderheidsdeelnemingen (voor nieuwe deelnemingen geldt een omzetlimiet) zijn automatisch meeverzekerd en hoeven niet op de polis te worden aangetekend. Buitenlandse dochtermaatschappijen die binnnen onze vergunningsmogelijkheden vallen kunnen op aanvraag en tegen een premietoeslag meeverzekerd worden.

Incident respons

- **Schadevergoeding én ontzorging**: Naast de financiële schade als gevolg van een cyberincident biedt de Cyber 360 ook toegang tot een multidisciplinair incident respons team welke verzekerde zoveel mogelijk ontzorgt tijdens het incident. Deze incident respons dienstverlening is vooral voor het MKB van groot belang omdat zij de benodigde expertise niet zelf in huis hebben en de (acute) inzet van specialisten kostbaar is.
- **Serviceorganisatie**: Markel heeft advocatenkantoor Kennedy Van der Laan als serviceorganisatie geselecteerd om de incident respons op de Cyber 360 verzekering te verzorgen. Kennedy Van der Laan heeft veel ervaring in het behandelen van cyberincidenten en verzorgt de intake, de coördinatie en de juridische behandeling van het incident. Tevens schakelen zij zo nodig, en afhankelijk van het type incident, gerenommeerde IT-forensische experts in zoals Northwave, Fox-IT maar ook speciaal op het MKB gerichte partijen. Voor communicatieadvies wordt samengewerkt met communicatiebureau BEX*.
- **24/7 Nederlandstalige noodlijn**: In geval van een incident kan verzekerde 24/7 het Markel Cyber Noodnummer bellen waarna een Nederlandssprekende medewerker van de serviceorganisatie verzekerde te woord zal staan. Zeker binnen het MKB wordt het belangrijk gevonden dat men tijdens een crisis in het Nederlands wordt toegesproken en zijn verhaal kan doen.

MARKEL

Informatiekaart Cyber 360

– **Eigen risico serviceorganisatie**: Voor de inzet van de serviceorganisatie of de door haar ingeschakelde partijen geldt geen sublimiet en geen eigen risico, óók niet na een bepaalde termijn. Deze ruime regeling is uniek in de markt.

Dekking

– **Modulaire opbouw**: De Cyber 360 is opgebouwd uit 7 dekkingsrubrieken die allemaal standaard zijn meeverzekerd op de polis.

Rubriek	Verzekerd bedrag
1. Aansprakelijkheid	Volledig
2. Data-incident	Volledig
3. Netwerkincident	Volledig
4. Bedrijfsschade	Volledig*
5. Cyberafpersing	Volledig
6. Cyberdiefstal	€ 100.000
7. Telefoonincident	€ 100.000

*Voor bedrijfsschade als gevolg van een netwerkinterruptie bij een IT-dienstverlener geldt een sublimiet van 25% met een minimum van € 100.000.

– **Data-incident**: De rubriek data-incident dekt de schade als gevolg van het verlies van persoonsgegevens of vertrouwelijke gegevens van derden. Deze dekking is ook van toepassing als een externe verwerker persoonsgegevens lekt waarvoor verzekerde verantwoordelijk is. Belangrijk omdat hackers zich in toenemende mate richten op IT-dienstverleners.

– **Netwerkincident**: Naast onbevoegd toegang tot het netwerk wordt deze dekking ook geactiveerd bij ongerichte aanvallen, zoals een malware besmetting van de netwerken. Belangrijk omdat niet altijd duidelijk is of de aanval zich op verzekerde richt.

– **Bedrijfsschade**: Voor veel bedrijven het belangrijkste ‘catastrofe’ risico want geen toegang tot IT betekent al snel geen inkomsten en geregeld neemt het herstellen van een cyberincident meerdere weken in beslag. De (binnen de kaders van de voorwaarden) werkelijk geleden bedrijfsschade is gedekt, oftewel wij werken niet met een maximaal dagtarief.

– **Uitkerings- en wachttermijn**: Voor het dekkingsonderdeel bedrijfsschade geldt een maximale uitkeringstermijn van 12 maanden en in plaats van een eigen risico is er een wachttermijn van 12 uur van toepassing.

– **Cyberafpersing**: Indien verzekerde wordt afgeperst door cybercriminelen dekt de verzekering de onderhandelingskosten en, indien verzekerde geen reëel alternatief heeft, het betaalde losgeld om de afpersing te beëindigen.

– **Dekking in de cloud**: Dekking op de polis geldt ongeacht of verzekerde op eigen systemen werkt of in de cloud.

– **Ontdekkingsbeginsel**: De verzekering dekt (uitgezonderd de rubrieken 1 en 6) data- en/of netwerkincidenten die ontdekt worden tijdens de verzekeringsperiode. Belangrijk omdat cyberincidenten voor de ingangsdatum kunnen plaatsvinden maar pas na de ingangsdatum van de polis worden ontdekt.

– **Inloop/uitloopdekking**: Voor de rubriek Aansprakelijkheid biedt de polis standaard onbeperkte inloop en de mogelijkheid om tegen 50% van de jaarpremie 1 jaar uitloop in te kopen.

– **Verzekerd bedrag**: Het minimale verzekerd bedrag dat gekozen kan worden is € 250.000, het maximale verzekerd bedrag is € 2.000.000 als maximum per aanspraak/gebeurtenis en per verzekeringsjaar.

– **Optioneel eigen risico**: Indien het voor verzekerde geen probleem is kleine schades voor eigen rekening te nemen kan men kiezen voor een hoger eigen risico wat resulteert in een premiekorting van 5% of 10%.

MARKEL

Dekkingsoverzicht Cyber 360

Hieronder hebben wij de Cyber 360 standaarddekking schematisch weergegeven. Dit betreft een beknopte beschrijving. Voor de volledige dekking verwijzen wij u naar de voorwaarden.

Rubriek	Verzekerde gebeurtenis	Vergoeding
1. Aansprakelijkheid	Aanspraken die voortvloeien uit een: - Data-incident - Netwerkincident - E-media incident - Virusincident	- kosten van verweer - schadevergoeding - schikking - boetes van creditcard maatschappijen
2. Data-incident	Verlies van persoonsgegevens of vertrouwelijke gegevens van derden	- coördinatie van en onderzoek naar het incident - juridisch advies en reputatiemanagement - notificatiekosten Autoriteit Persoonsgegevens* en de betrokkenen van het data-incident - kredietmonitoringkosten - kosten van verweer in geval van een onderzoek van de toezichthouder - boetes van de toezichthouder bij tekortkoming informatiebeveiliging (voor zover verzekerbaar)
3. Netwerkincident	- een diefstal, beschadiging, vernietiging en/of ontregeling van data of software op de IT-infrastrucuur van verzekerde - onbevoegde toegang tot de IT-infrastructuur van verzekerde; - Ddos aanval op de website van verzekerde	- coördinatie van en onderzoek naar het incident - juridisch advies en reputatiemanagement - IT-forensisch onderzoek - advies en uitvoering van schadebeperkende maatregelen - aanbevelingen om nieuwe netwerkincidenten te voorkomen en het plaatsen van netwerkscanners (post-incident) - herstelkosten om data te reconstrueren en het netwerk weer in de staat te brengen van voor het incident**
4. Bedrijfsschade	Netwerkinterruptie van eigen systemen of van de IT-dienstverlener als gevolg van een netwerkincident	- bedrijfsschade (uitkeringsperiode 12 maanden) - extra kosten om bedrijfsschade te minimaliseren
5. Cyberafpersing	Bedreiging om een data-incident of een netwerkincident uit te voeren of een versleuteling van data van verzekerde (ransomware aanval)	- onderhandelingskosten - losgeld
6. Cyberdiefstal	Netwerkincident waardoor er geld van de bankrekening wordt ontvreemd	- gestolen geld van de bankrekening van verzekerde
7. Telefoonincident	Inbraak in de telefooncentrale	- extra telefoonkosten

* Of een vergelijkbare binnen- of buitenlandse overheidsinstantie die toezicht houdt op de beveiliging van data.

**De kosten voor verbeteringen van het netwerk zijn ook gedekt mits goedgekeurd door verzekeraar.

Markel
Weena 505, 3013 AL Rotterdam, Nederland
+31 (0)10-7981000 info.nl@markel.com

MARKEL