Markel

CYBER CRIME VERZEKERING

Steeds meer organisaties werken digitaal of geautomatiseerd. Hierdoor neemt cybercriminaliteit en het aantal cyberincidenten toe. De Cyber Crime verzekering van Markel biedt dekking voor de risico's die mkb'ers lopen op financiële schade als gevolg van cybercriminaliteit of cyberincidenten.

HIGHLIGHTS

- De Cyber Crime verzekering is bedoeld voor binnen Nederland gevestigde privaatrechtelijke rechtspersonen, vennootschappen, maatschappen en eenmanszaken met een omzet tot EUR 10.000.000,00. Voor financiële ondernemingen is de omzetgrens EUR 5.000.000,00.
- De Cyber Crime verzekering kent een aansprakelijkheidsdekking (third party) en een eigen schade (first party) dekking.
- Voor de Cyber Crime verzekering heeft Markel verzekerde bedragen tussen EUR 250.000,00 per gebeurtenis/aanspraak en per verzekeringsjaar en EUR 1.000.000,00 per gebeurtenis/aanspraak en per verzekeringsjaar beschikbaar.
- Vergoeding van de honoraria en kosten van de serviceorganisatie om te bemiddelen bij een cyberafpersing en eventueel de te betalen vergoeding om de cyberafpersing te beëindigen.
- Voor de rubrieken cyberafpersing, cyberdiefstal en telefoonincident geldt een sublimiet van EUR 100.000,00 per gebeurtenis.
- Bereddingskosten worden zo nodig boven het verzekerd bedrag vergoed bij eigen schade dekking.
- Vergoeding van de redelijke en noodzakelijke externe kosten om elektronisch opgeslagen data te reconstrueren, te vervangen of te herstellen.
- Er geldt een eigen risico van EUR 500,00 per gebeurtenis/aanspraak. U kunt ook kiezen voor een hoger eigen risico. Dan krijgt u een korting op de premie.
- Voor het dekkingsonderdeel bedrijfsschade geldt een maximale uitkeringstermijn van 12 maanden, geen eigen risico en een wachttermijn van 24 uur.
- Samenwerking met serviceorganisaties die bij een (vermoedelijk) cyberincident ook buiten kantooruren kunnen worden bereikt.
- Het eigen risico geldt niet voor de vergoeding van de kosten van de serviceorganisatie (of van de kosten die in opdracht van de serviceorganisatie zijn gemaakt).
- Het dekkingsgebied is de Europese Unie en het Verenigd Koninkrijk.
- Dekking voor de kosten van verweer en eventuele schade in verband met een aanspraak door verlies van persoonsgegevens en/of vertrouwelijke informatie.
- Dekking voor de kosten van verweer en juridisch advies in verband met verzekerbare, bestuurlijke boetes.
- Dekking voor de aansprakelijkheid voor door betaalkaart-maatschappijen geleden schade als gevolg van een overtreding van de Payment Card Industry Data Security Standards.
- Eenvoudig af te sluiten door middel van alleen een aanvraagformulier, waarbij de premie vooraf bekend is.

CYBER CRIME EN CYBERINCIDENTEN

We spreken van cyber crime als er een misdaad wordt gepleegd door middel van ICT, gericht op ICT. Bij cyberincidenten is er sprake van een ICT-verstoring in de dienstverlening en/of het ongeoorloofd openbaren, verkrijgen en/of wijzigen van vertrouwelijke informatie.

CYBERWEERBAARHEID

Het gebruik van digitale media neemt toe waarmee ook de kans dat u te maken krijgt met cybercriminaliteit of een cyberincident toeneemt. Het cyberrisico is echter niet alleen aanwezig bij een internetshop of bij grote bedrijven die dagelijks een hoge frequentie aan financiële transacties verwerken. Een DDoS aanval, ransomware, netwerkincident, phishing of een virusinfectie; ieder bedrijf krijgt er een keer mee te maken. Elke organisatie uit elke branche, klein en groot, heeft te maken met een zekere mate van cyberrisico. Organisaties worden steeds vaker blootgesteld aan de gevaren van technologie. De weerbaarheid van een bedrijf begint bij de juiste kennis en bewustwording van systemen en de digitale gevaren binnen de organisatie. Adequate beveiliging van systemen is ook van groot belang. Hiermee kan een groot gedeelte van cybercriminaliteit en cyberincidenten buiten de deur worden gehouden. Echter sluit je het risico op een cyberincident niet helemaal uit. De Cyber Crime verzekering van Markel kan hierin een oplossing bieden wanneer een bedrijf toch te maken krijgt met een cyberaanval.

AANSPRAKELIJKHEID

Een cyberincident heeft soms ook gevolgen voor uw klanten en/of leveranciers. De aansprakelijkheidsdekking op de Cyber Crime verzekering dekt de aansprakelijkheid van een verzekerde voor door derden geleden schade als gevolg van een data incident, e-media incident, netwerkincident en virusincident.

EIGEN SCHADE

De Cyber Crime verzekering kent ook een eigen schade dekking. Dit is schade die een bedrijf heeft geleden als gevolg van een cyberincident. De Cyber Crime verzekering kent hierin 6 dekkingsonderdelen:

- data incident
- netwerkincident - extra kosten
- netwerkincident - bedrijfsschade
- cyberafpersing
- cyberdiefstal
- telefoonincident

ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG)

Veel bedrijven gebruiken persoonsgegevens en wisselen deze uit. In de AVG staan de belangrijkste regels hoe om te gaan met persoonsgegevens in het belang van de privacy van de personen. Persoonsgegevens kunnen door een datalek op straat liggen, waarvoor het bedrijf aansprakelijk is. Cybercriminelen kunnen persoonsgegevens stelen en hiermee bijvoorbeeld fraude plegen.
Verlies van persoonsgegevens is gedekt op de polis van Markel, mits deze het gevolg is van een gericht netwerkincident op de computer van verzekerde. De autoriteit persoonsgegevens hanteert zeer korte termijnen na ontdekking van een mogelijk datalek. Het is dus van groot belang om een (vermoedelijk) verlies van persoonsgegevens onmiddellijk te melden bij de Autoriteit Persoonsgegevens. Onze serviceorganisaties kunnen u ook buiten kantooruren hierbij helpen.

BEDRIJFSSCHADE

Bij bedrijfsschade denk je vaak aan een bedrijfsonderbreking als gevolg van brand, inbraak, overstroming etc. Tegenwoordig zijn we ook steeds meer afhankelijk geworden van technologie en kunnen de bedrijfsactiviteiten ook stil komen te liggen vanwege een cyberaanval op de computers. Markel dekt de bedrijfsschade die voortvloeit uit een netwerkincident voor maximaal 12 maanden. Er geldt een wachttermijn van 24 uur en geen eigen risico.

CRISISMANAGEMENT

Wij maken gebruik van externe expertisebureaus die worden ingeschakeld om:

- oorzaak en omvang vast te stellen van het data incident
- reputatieschade te beperken als gevolg van het data incident
- het verlies van persoonsgegevens en verlies van vertrouwelijke gegevens in goede banen te leiden bij een data incident
- financiële transacties te monitoren
- te bemiddelen bij of te onderzoeken naar de oorzaak van een cyberafpersing

De verzekering vergoedt de honoraria en kosten van deze expertisebureaus.

Buiten kantooruren kan het (vermoedelijke) cyberincident gemeld worden aan de op het polisblad vermelde serviceorganisatie. De verplichting tot het melden aan de verzekeraar blijft gelden.

MARKEL

Cyber Crime verzekering

Voor meer informatie over onze verzekeringen kunt u uiteraard met ons in contact treden via onderstaande contactgegevens:

010-7981000
info.nl@markel.com
www.markelinsurance.nl