Cyber 360 MISE 2023

Informatiedocument over het verzekeringsproduct

Onderneming: Markel, schadeverzekeraar, vergunning: 12046126 (NL)

Product: Cyber 360 MISE 2023

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?

Een cyberincident kan grote gevolgen hebben voor de continuïteit en dagelijkse bedrijfsvoering van een onderneming. Met de Cyber 360 verzekering van Markel wentelt verzekeringnemer de gedekte cyberrisico's en bijkomende kosten af. Deze verzekering is bedoeld voor privaatrechtelijke organisaties die in Nederland zijn gevestigd en een geconsolideerde jaaromzet hebben van maximaal € 25.000.000.

Een belangrijk element naast de schadevergoeding is de voor verzekerde toegankelijke incident response dienstverlening van Kennedy van der Laan. Kennedy van der Laan heeft veel ervaring op gebied van cyberincidenten, biedt een 24/7 Nederlandstalige hotline en schakelt met IT-forensische partijen als Northwave en Fox-IT.

Wat is verzekerd?

De Cyber 360 verzekering is zowel een eigen schade (first party) verzekering als een aansprakelijkheidsverzekering (third party). De polis kent een modulaire opbouw met 7 dekkingsrubrieken die standaard zijn meeverzekerd op de polis.

Rubrieken:
1. Aansprakelijkheid (volledig);
2. Data-Incident (volledig);
3. Netwerkincident (volledig);
4. Bedrijfsschade (volledig);
- Voor het dekkingsonderdeel bedrijfsschade geldt een maximale uitkeringstermijn van 12 maanden. In plaats van een eigen risico is er een wachttermijn van 8 uur van toepassing voor bedrijfsschade die het gevolg is van een netwerkincident;
- Voor het dekkingsonderdeel bedrijfsschade die het gevolg is van niet-kwaadaardige incidenten, zoals bedienings- of systeemfouten, geldt een wachttermijn van 12 uur en een sublimiet van € 250.000 als maximum per gebeurtenis en per verzekeringsjaar;
- Het dekkingsonderdeel bedrijfsschade kan gedeselecteerd worden tegen 15% premiekorting. Interessant voor non-profit instellingen waarvoor deze dekking beperkte meerwaarde heeft;
5. Cyberafpersing (volledig);
6. Cyberdiefstal (incl. CEO-fraude & Social Engineering / sublimiet € 100.000);
7. Telefoonincident (sublimiet € 100.000).

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

Wat is niet verzekerd?

Alle Rubrieken

✖ Deze verzekering biedt geen dekking voor schade die ontstaat:
- door een vermogensdelict, onrechtmatig bevoordelen of (ander) frauduleus handelen door of in samenwerking met een verzekerde;
- door opzet of bewuste roekeloosheid van een verzekerde;
- door storingen of uitval van satellieten, internet-, telecomnetwerken of nutsvoorzieningen die niet onder beheer van de verzekerde vallen;
- vóór de oprichting of aankoop van een dochterbedrijf dat verzekeringnemer na de startdatum van de verzekering heeft overgenomen;
- aan personen en zaken.

Aansprakelijkheid

✖ Deze verzekering biedt geen dekking voor aanspraken die verband houden met en/of voortvloeien uit:
- aansprakelijkheidsverhogende bedingen (hierop zijn enkele uitzonderingen van toepassing);
- auteursrecht, octrooirecht en andere intellectuele eigendomsrechten (deze uitsluiting is niet van toepassing op een e-media incident);
- bekende omstandigheden;
- bestuurdersaansprakelijkheid.

Verzekerd bedrag

✔ De verzekerde bedragen die gekozen kunnen worden variëren van minimaal € 100.000 tot maximaal € 2.500.000 per aanspraak/ gebeurtenis en per verzekeringsjaar. Indien meerdere rubrieken worden geactiveerd geldt het totale verzekerde bedrag als maximum.

Aansprakelijkheid

✔ De rubriek aansprakelijkheid biedt dekking voor schade van derden en de kosten van verweer voortvloeiende uit een data-incident, een netwerkincident, een e-media incident of een virusincident welke heeft plaatsgevonden tijdens de verzekerings- of inloopperiode en waarvoor verzekerde aansprakelijk wordt gesteld. Deze rubriek biedt ook dekking voor boetes en onderzoekskosten als verzekerde de AVG heeft overtreden.

Extra informatie

Een e-media-incident is een onbedoelde:
- aantasting van iemands eer of goede naam;
- schending van auteursrechten, octrooirechten of andere intellectuele eigendomsrechten;
- schending van de privacy van natuurlijke personen.

Dit moet het gevolg zijn van de inhoud van de website van de verzekerde, door digitale berichten die de verzekerde verstuurt, of door uitingen op sociale media.

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.

Extra informatie

Gedekt zijn de kosten van de serviceorganisatie om een data-incident te coördineren, te onderzoeken, en, indien noodzakelijk, te melden aan de Autoriteit Persoonsgegevens (AP) en betrokkenen. Daarnaast dekt deze rubriek de kosten om identiteitsdiefstal bij betrokkenen te voorkomen, reputatieschade te beperken en - voor zover dat wettelijk is toegestaan - boetes die zijn opgelegd door de AP.

Bedrijfsschade

✖ Deze verzekering biedt geen dekking voor bedrijfsschade die:
- ook zou zijn ontstaan zonder de netwerkstoring of de storing bij een IT-dienstverlener;
- bestaat uit boetes door contractbreuk, vertraging of het niet uitvoeren van opdrachten;
- bestaat uit oninbare vorderingen (afschrijving op debiteuren);
- geen verband heeft met de normale bedrijfsactiviteiten, zoals opbrengsten uit kapitaaltransacties of handel in onroerend goed.

Extra informatie

Deze verzekering dekt geen bedrijfsschade door niet-kwaadaardige systeem- of bedieningsfouten die verband houdt met:
- Vervuiling: schade door het (dreigend) vrijkomen of verspreiden van verontreinigende stoffen, of door maatregelen om deze op te ruimen of te behandelen;
- Fysieke gebeurtenissen: schade door o.a. brand, rook, explosie, bliksem, storm, water(overlast), overstroming, aardbeving, vulkaanuitbarsting, vloedgolf, aardverschuiving, hagel, andere natuurrampen of elektromagnetische straling;
- Overheidsingrijpen: schade door inbeslagname, nationalisatie of vernietiging van de IT-infrastructuur door of in opdracht van de overheid;
- Datamigratie: schade die ontstaat bij het overzetten van data naar een ander netwerk.

Cyberdiefstal (incl. CEO-fraude & Social Engineering)

✖ Betalingsverzoeken die uitsluitend mondeling of telefonisch plaatsvinden zijn uitgesloten van dekking.

Telefoonincident

✖ Deze verzekering biedt geen dekking voor schade die het gevolg is van netwerkincidenten die zijn uitgevoerd in samenwerking met of met medeweten van een verzekerde.

Zijn er dekkingsbeperkingen?

! In de polisvoorwaarden zijn enkele IT-beveiligingsmaatregelen als dekkingsvoorwaarde opgenomen, het is belangrijk dat aan deze maatregelen wordt voldaan. Een uitzondering hierop is als de tekortkoming zich buiten de directe invloedsfeer bevond of als het incident ook zonder deze tekortkoming had plaatsgevonden.

Netwerkincident

✔ De rubriek netwerkincident dekt de kosten van de serviceorganisatie om een netwerkincident te coördineren, IT-forensisch onderzoek te verrichten alsmede het uitvoeren en adviseren van schade-mitigerende maatregelen. Tevens dekt de verzekering de kosten die gemaakt worden om de IT-infrastructuur en de data van verzekerde weer in de staat te brengen zoals deze zich bevond voor het netwerkincident.

Bedrijfsschade

✔ De rubriek bedrijfsschade dekt de bedrijfsschade en de extra kosten die worden geleden tijdens de uitkeringstermijn als gevolg van een netwerkinterruptie veroorzaakt door een netwerkincident. Tevens wordt de bedrijfsschade vergoed als het netwerk op advies van de serviceorganisatie wordt uitgeschakeld met als doel verdere schade te voorkomen.

Cyberafpersing

✔ De rubriek cyberafpersing dekt de kosten om te bemiddelen bij, of onderzoek te doen naar een cyberafpersing alsmede de vergoeding (losgeld) om de cyberafpersing te beëindigen. Onder cyberafpersing wordt verstaan een dreigement om een data- of netwerkincident uit te voeren of een losgeldeis na uitvoering van een cyberincident zoals een ransomware aanval.

Cyberdiefstal (incl. CEO-fraude & Social Engineering)

✔ De rubriek Cyberdiefstal (inclusief CEO-fraude en Social Engineering) biedt dekking voor schade die ontstaat wanneer cybercriminelen een betalingsverzoek manipuleren of een transactie wijzigen. Belangrijk: deze dekking geldt ook voor betalingsverzoeken die buiten het netwerk van de verzekerde zijn gemanipuleerd, waaronder vormen van CEO-fraude en social engineering.

Extra informatie

Voorwaarde voor dekking is dat verzekerde een betalingsprotocol heeft opgesteld met een bevoegdhedenmatrix en een vier-ogen principe voor transacties vanaf € 10.000 en dat dit protocol bij de overboeking niet is geschonden.

Telefoonincident

✔ Als hackers via een netwerkincident de telefooncentrale binnendringen en langdurig dure criminele telefoonnummers bellen dan dekt deze rubriek de financiële schade van verzekerde.

Eigen Risico

! Bij een omzet:
- tot € 1.000.000 geldt een verplicht eigen risico van € 500,-
- van € 1.000.000 tot en met € 10.000.000 geldt een verplicht eigen risico van € 1.000,-
- van € 10.000.000 tot en met € 25.000.000 geldt een verplicht eigen risico van € 2.500,-

Extra informatie

Indien verschillende rubrieken van toepassing zijn zal het eigen risico slechts éénmaal toegepast worden.

Het eigen risico is niet van toepassing op:
- honoraria en kosten van de serviceorganisatie;
- bedrijfsschade, in plaats hiervan geldt een wachttermijn van 8 uur voor bedrijfsschade als gevolg van een netwerkincident en een wachttermijn van 12 uur voor bedrijfsschade als gevolg van een systeem/bedieningsfout.

Bereddingskosten

! Bereddingskosten zijn gedekt binnen het verzekerd bedrag en zover niet reeds gedekt op de polis.

In- en uitloop

✔ Voor de rubriek aansprakelijkheid biedt de polis standaard onbeperkte inloop en de mogelijkheid om beëindiging van de polis tegen 50% van de jaarpremie 1 jaar uitloop in te kopen. Een langere uitloop kan op verzoek en tegen een premieopslag worden ingekocht.

Extra informatie

Er geldt een nameldingstermijn van 4 maanden.

Dochterondernemingen

✔ Alle huidige en nieuwe dochterondernemingen binnen de EU, IJsland, Liechtenstein, Noorwegen en het Verenigd Koninkrijk zijn automatisch meeverzekerd en hoeven niet op de polis te worden aangetekend

Endpoint Detection & Response (EDR)

✔ 15% premiekorting indien EDR is ingeregeld op minimaal 85% van de werkstations/laptops.

Waar ben ik gedekt?

✔ Werelddekking (exclusief USA/Canada voor de rubriek aansprakelijkheid). Geen geografische beperking voor cyberaanvallen vanuit USA/Canada. Voor dekking is leidend waar geografisch de schade wordt geleden, niet waar de aanval plaatsvindt.

Wat zijn mijn verplichtingen?

Als je de verzekering aanvraagt, dien je onze vragen eerlijk te beantwoorden. Je bent verplicht de schade zo spoedig mogelijk te melden bij de serviceorganisatie en de verzekeraar, daarnaast dien je schade zoveel mogelijk te beperken. Meld belangrijke veranderingen in je situatie zo snel mogelijk.

Hoe en wanneer betaal ik?

Je kunt kiezen of je de premie per kwartaal (4% toeslag), halfjaar (3% toeslag) of jaar betaalt. Betalen kan via een automatische incasso. Of je maakt zelf het bedrag over. Je betaalt de premie aan degene van wie je de nota krijgt. Dat kan de tussenpersoon of de verzekeraar zijn.

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?

Na het eerste jaar kun je de verzekering dagelijks opzeggen. Er geldt een opzegtermijn van een maand. Opzeggen doe je schriftelijk. Markel conformeert zich aan de Gedragscode Geïnformeerde Verlenging en Contracttermijnen Particuliere en Zakelijke Schade- en Inkomensverzekeringen.

Extra informatie

Markel Insurance SE, rechtspersoon naar Europees recht, gevestigd te München, tevens handelend onder de naam Markel. Het adres van Markel is Weena 505, 3013 AL te Rotterdam.

Versie 3, 16-12-2025, Bekijk online: verzekeringskaarten.nl/markelintl/cyber-360-mise-2023-v3-25-06