

A laptop is shown from a low angle, open. The screen and keyboard area are illuminated with a vibrant, multi-colored glow transitioning from blue on the left to red and orange on the right. The rest of the laptop and the background are dark.

Informatiekaart
Cyber 360 Maatwerk

MARKEL

Informatiekaart

Cyber 360 - Maatwerk

Cyberincidenten kunnen grote impact hebben op iedere organisatie. De Cyber 360 polis biedt zowel een ruime dekking als volledige ontzorging in geval van een cyberincident. Deze informatiekaart beschrijft de dekking en de highlights van de Cyber 360 verzekering voor ondernemingen die qua aard en omvang buiten de Cyber 360 standaardpropositie vallen.

Dekking

- **Modulaire opbouw:** De Cyber 360 is standaard opgebouwd uit 7 dekkingsrubrieken

Rubriek	Verzekerd bedrag
1. Aansprakelijkheid	Volledig
2. Data-incident	Volledig
3. Netwerkincident	Volledig
4.a Bedrijfsschade interruptie eigen systemen	Volledig
4.b Bedrijfsschade interruptie IT-dienstverleners	Variabel
5. Cyberafpersing	Variabel
6. Cyberdiefstal	€ 100.000
7. Telefoonincident	€ 100.000

- 1. Aansprakelijkheid:** Biedt dekking voor schade van derden die is ontstaan door een netwerk- of een data-incident en waarvoor verzekerde aansprakelijk wordt gesteld omdat zij tekortgeschoten zou zijn in de beveiliging van haar data of netwerk. Deze rubriek biedt ook dekking voor boetes en onderzoekskosten als verzekerde de AVG heeft overtreden.
- 2. Data-incident:** Biedt dekking ingeval van verlies of onrechtmatige toegang van persoonsgegevens of bedrijfsgeheimen 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.
- 3. Netwerkincident:** Deze dekking wordt geactiveerd als hackers toegang hebben of schade toebrengen tot het netwerk of de

data op het netwerk van verzekerde. 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.

- 4. Bedrijfsschade:** Biedt dekking voor de geleden bedrijfsschade als gevolg van een netwerkinterruptie veroorzaakt door een netwerkincident. Voor veel bedrijven vormt dit het belangrijkste 'catastrofe' risico want geen toegang tot IT betekent al snel geen inkomsten en geregeld neemt het (volledig) 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 wachtermijn:** Voor het dekkingsonderdeel bedrijfsschade geldt een maximale uitkeringstermijn van 12 maanden. De wachtermijn voor Bedrijfsschade is standaard 12 uur en geldt als franchise, oftewel na verstrijken van de wachtermijn vergoeden wij de volledige bedrijfsschade na aftrek van het eigen risico.
- **Afgeleide bedrijfsschade:** De bedrijfsschade die wordt geleden vanwege een netwerkinterruptie bij een IT-dienstverlener omdat deze is gehackt is ook gedekt. Belangrijk omdat bedrijven steeds meer in de cloud werken en afhankelijk zijn van externe leveranciers.
- 5. 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.
- 6. Cyberdiefstal:** Als hackers via een netwerkincident betaalopdrachten manipuleren dan dekt deze rubriek de financiële schade van verzekerde.
- 7. Telefoonincident:** Als hackers via een netwerkincident de telefooncentrale binnendringen en langdurig dure criminele

telefoonnummers bellen dan dekt deze rubriek de financiële schade van verzekerde.

- **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 3 jaar inloop en de mogelijkheid om tegen 50% van de jaarpremie 1 jaar uitloop in te kopen.
- **Dochtermaatschappijen:** Alle huidige en nieuwe Nederlandse meerderheidsdeelnemingen (voor nieuwe deelnemingen geldt een omzetlimiet van 25%) zijn automatisch meeverzekerd en hoeven niet op de polis te worden aangetekend. Via een clause kan de dekking worden uitgebreid met buitenlandse dochtermaatschappijen.

Acceptatie

- **Aanvragen:** De Cyber 360 maatwerk polis kan aangevraagd worden op basis van het cyber 360 maatwerk vragenformulier maar wij accepteren ook vragenformulieren van andere verzekeraars. Op basis van beknopte gegevens ten aanzien van de activiteiten en de IT-beveiliging kan vaak al een indicatieve offerte afgegeven worden.
- **Doelgroep:** De Cyber 360 maatwerk kunnen wij offeren voor organisaties met een geconsolideerde jaaromzet tot €100.000.000 die wereldwijd actief zijn.
- **Branches:** Voor de meeste branches hebben wij verzekeringsmogelijkheden al zijn wij in sommige branches terughoudend. Voor publiekrechtelijke organisaties, infrastructurele bedrijven en/of crypto handelaars hebben wij in het geheel geen mogelijkheden.

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. Het snel en effectief reageren op cyberincidenten is cruciaal om de schade als gevolg van het incident zoveel mogelijk te beperken.
- **Serviceorganisatie:** Markel heeft advocatenkantoor Kennedy Van der Laan 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 en EYE security. 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.
- **Eigen risico serviceorganisatie:** Voor de inzet van de serviceorganisatie of de door haar ingeschakelde partijen geldt geen eigen risico voor werkzaamheden die worden verricht tijdens de eerste 72 uur na inschakeling. Dit doen wij om de drempel om de serviceorganisatie te bellen te verlagen want in geval van een incident is het cruciaal om zo snel mogelijk in te grijpen.

De in deze informatiekaart verstrekte informatie is enkel informatief van aard. Het gestelde op het polisblad en de polisvoorwaarden is altijd leidend.