

Deze Verzekeringskaart 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 verzekert u zich tegen de gevolgen van hacking, systeeminbraak, diefstal van gegevens, verlies van gegevens, en cyberaanvallen. Ook als dit gebeurt bij uw IT-dienstverlener en u daardoor schade lijdt.



Wat is verzekerd?

- ✓ Deze verzekering dekt uw aansprakelijkheid voor schade geleden door derden, de kosten van uw eigen bedrijf en de gevolgschade. Daarnaast kunt u 24/7 rekenen op hulp van een incident response provider als uw bedrijf door een gebeurtenis getroffen wordt.

Verzekerd bedrag

- ✓ Het verzekerd bedrag staat op uw polis. Dit is het maximale bedrag dat wij in een verzekeringsjaar betalen.

Aansprakelijkheid

- ✓ U bent verzekerd voor schade die anderen lijden als gevolg van uw cyberincident. Als u daarvoor aansprakelijk bent. Bijvoorbeeld door een gegevensinbreuk (digitaal datalek). Of door de verspreiding van een cyberincident via uw computersystemen naar de computersystemen van een ander.

Herstelkosten

- ✓ U bent verzekerd voor de kosten om uw computersysteem, digitale data en software te herstellen en te configureren na een cyberincident op uw computersystemen.

Cyberafpersing

- ✓ U bent verzekerd voor hulp bij cyberafpersing. En voor vergoeding van kosten om de cyberafpersing op te lossen. U bent ook verzekerd voor de vergoeding van losgeld als dat mag volgens de wet.

Bedrijfsschade

- ✓ U bent verzekerd voor de vergoeding van verlies van uw brutowinst als een cyberincident uw digitale data en/of computersystemen volledig of gedeeltelijk onbeschikbaar maakt. U bent ook verzekerd voor schade die ontstaat als uw computersystemen door het cyberincident minder goed werken dan direct voor het cyberincident.



Wat is niet verzekerd?

- ✗ Veroorzaakt een verzekerde zelf met opzet schade? Of fraudeert een verzekerde? Dan is dat niet verzekerd. Ook schade door uitval van uw internetserviceprovider is niet verzekerd, evenals zaak- en letselschade, productaansprakelijkheid en inbeslagname van overheidswege.

Schade door illegale data

- ✗ Is de schade ontstaan door data die u illegaal verkregen hebt? Dan is dat niet gedekt.

Verenigde Staten of Canada

- ✗ Uw aansprakelijkheid voor schade in of volgens het recht van de Verenigde Staten of Canada is niet standaard verzekerd.

Extra informatie

U kunt dit op aanvraag wel meeverzekeren.



Zijn er dekkingsbeperkingen?

Eigen risico

- ! Het eigen risico staat op uw polisblad. Voor bedrijfsschade geldt geen eigen risico. Hier geldt een wachtermijn. De wachtermijn is het aantal uren waarbij de bedrijfsschade door een cyberincident voor uw eigen rekening komt. De wachtermijn staat op uw polisblad.

Preventie-eisen

- ! U bent niet of gedeeltelijk verzekerd als u zich niet houdt aan de preventieafspraken. En de schade daardoor veroorzaakt wordt. Of de schade daardoor verergerd. U bent wel verzekerd als u bewijst dat u zich per ongeluk niet aan de preventieafspraken hield.

Extra informatie

De preventieafspraken staan in uw polisvoorwaarden.

Datalek

- ✓ Kosten voor een expert die het digitale datalek voor u onderzoekt. Hulp en kosten voor het nakomen van verplichtingen vanuit privacywetten. Kosten voor een expert die uw reputatie beschermt. Juridische hulp als de toezichthouder maatregelen tegen u neemt. Vergoeding van een bestuurlijke boete na een gegevensinbreuk.

Extra informatie

Let op! Wij vergoeden een bestuurlijke boete alleen als deze wettelijk verzekeraar is.

Keuze: diefstal van geld en waardemiddelen en telefoonhacking

Cyberdiefstal van geld van uw rekening. Of cyberdiefstal van geld doordat iemand zonder uw toestemming gegevens in uw computersysteem wijzigt. Telefoonhacking: kosten die het gevolg zijn van een cyberincident op uw telefoonsysteem. Bijvoorbeeld belkosten die zonder uw toestemming gemaakt zijn.

Extra informatie

Bij cyberdiefstal en telefoonhacking is het verzekerd bedrag 10% van het totale verzekerd bedrag.

Keuze: PCI-DSS

U bent verzekerd voor de kosten van overtreding van de PCI-DSS standaard door een cyberincident.

Vergoed worden:

- * Kosten voor een expert om de overtreding te onderzoeken.
- * Kosten om opnieuw gecertificeerd te worden voor PCI-DSS.
- * Kosten om betaalkaarten opnieuw uit te geven.
- * Boetes die een betaalkaartmerk u oplegt.

Keuze: Media-aansprakelijkheid

De aansprakelijkheid voor schade van een ander door uw online media-activiteiten. Als u door het digitaal verspreiden van van tekst, beeld, video of geluid aansprakelijk bent voor de gevolgen van: smaad, schending van privacy, inbreuk op auteursrecht, eigendomsrecht.



Waar ben ik gedekt?

- ✓ De verzekering geldt wereldwijd behalve voor aansprakelijkheid. Uw aansprakelijkheid voor schade in of volgens het recht van de Verenigde Staten of Canada is niet standaard verzekerd.



Wat zijn mijn verplichtingen?

Als u de verzekering aanvraagt, moet u onze vragen eerlijk beantwoorden. Veranderingen in uw situatie ontvangen wij graag zo snel mogelijk. Als u schade heeft vragen wij u dit spoedig door te geven. Daarnaast verwachten wij dat u er zoveel mogelijk aan doet om schade te voorkomen en te beperken.



Wanneer en hoe betaal ik?

U kunt kiezen of u de premie maandelijks of eenmaal per jaar betaalt. Betalen kan via een automatische incasso. Of u maakt zelf het bedrag over.



Wanneer begint en eindigt de dekking?

U bent verzekerd vanaf de datum die op het polis staat. Betaalt u de premie niet op tijd? Dan kunnen we de verzekering stoppen.



Hoe zeg ik mijn contract op?

Na het 1e jaar kunt u de verzekering dagelijks opzeggen, met een opzegtermijn van 1 maand. Geef uw opzegging schriftelijk aan ons door.

Version 3, 27-07-2020, Bekijk online: verzekeringskaarten.nl/centraalbeheer/centraal-beheer-cyberverzekering

© Verbond van verzekeraars, www.vanatotzekerheid.nl