CyberStart by Hiscox (CyberClear)

In het kader van de Cyber en Data Risks verzekering (CyberClear) geldt het navolgende:

- Het verzekerd bedrag bedraagt 50.000, - per aanspraak/(eigen)schade en per verzekeringsjaar;
- Het eigen risico 500,- per aanspraak/eigen schade;
- Eigen schade bij bedrijfsstagnatie (business interruption):
  - Eigen schade door bedrijfsstagnatie (BI) en
  - Eigen schade door bedrijfsstagnatie (BI) als gevolg van een menselijke fout.

In afwijking van het verzekerd bedrag hierboven is de maximale vergoeding bij gelijk aan de sublimiet per dag vermeld in het onderstaande schema met een schadevergoedingstermijn van 1 maand en een retentietijd van 12 uur.

Jaarlijkse omzet	**Maximale vergoeding per dag**
€ 0,01 t/m € 250.000, --	€ 250,--
€ 250.001, -- t/m € 500.000, --	€ 500,--
€ 500.001, -- t/m € 1.000.000, --	€ 750,--
> € 1.000.001, -- t/m € 10.000.000, --	€ 1.250,--

- Tevens is het bepaalde onder bedrijfsstagnatie 4.1.5 van de polisvoorwaarden geheel vervangen door het navolgende;
- Na een gedekte stagnatie of eigen schade uit hoofde van 2.1.5, 2.1.6 of 2.1.9 vergoeden wij per dag een bedrag zoals aangegeven in het bovenstaande schema op basis van uw inkomsten gedurende de looptijd van de polis die u hebt opgegeven aan ons op het moment van acceptatie. Dit bedrag is inclusief vergoeding voor hogere arbeidskosten. De schadevergoedingstermijn is 1 maand.
- Als u uw inkomsten niet aan ons heeft opgegeven in de aanloop naar het huidige verzekeringsjaar, dan zullen wij de laatste informatie die u ons heeft verstrekt gebruiken en zullen u na afloop van de schadevergoedingstermijn vragen om een getekende verklaring ter bevestiging dat de schade-uitkering in lijn is met de door u daadwerkelijk geleden schade.
- Optionele dekking eigen schade door stagnatie bij een informatietechnologiedienstverlener waar u afhankelijk van bent (ICT dependent business interruption) is niet van toepassing.
- Er is een sublimiet van € 25.000, -- per verzekeringsjaar per dekkingsonderdeel, (i) elektronische diefstal, (ii) telefoonfraude, (iii) social engineering + social-engineeringschade opdrachtgevers, (iv) frauduleus gebruik van uw elektronische identiteit (deze dekkingsonderdelen cumuleren niet).
- Er is een sublimiet van € 15.000, -- per verzekeringsjaar voor eigen ingreep vergoeding voor kosten gemaakt in de eerste 72 uur na het incident (2.4.1).
- Er is een kostenvergoeding voor uw aanwezigheid bij een gerechtelijke instantie van € 300,- per dag(deel) (2.4.2).
- De van toepassing zijnde polisvoorwaarden zijn CyberClear by Hiscox 2022 (HCC - 2022/01);
- Het rechtsgebied is de gehele wereld exclusief de Verenigde Staten van Amerika en Canada;
- Melding van een aanspraak, een omstandigheid of eigen schade dient zo spoedig als redelijkerwijs mogelijk gericht te worden aan ons (Hiscox Nederland);

(Hiscox incident response team)
Incident responsenummer: + 31 (0)20 517 0700 en per e-mail hiscox.claims@hiscox.nl. Onze voorafgaande schriftelijke toestemming is noodzakelijk voor het inschakelen van experts of het maken van (on)kosten.

In aanvulling op de polisvoorwaarden HCC-2022/01 (3. Dit is niet gedekt), zijn wij niet tot enige vergoeding van schade of kosten (waaronder kosten van verweer) gehouden in verband met of voortvloeiende uit aanspraken, eigen schade of andere aansprakelijkheden indien:

U/verzekerde behoort tot de navolgende branches/sectoren en/of de navolgende diensten levert:

- Financiële instellingen en financieel dienstverleners (Wft)
- Betalingsverwerking (payment serviceproviders)
- Sociale netwerk- en datingplatformen
- Kredietbeoordelaar/ratingbureaus
- Kansspel-sector
- Seksbranche
- Politieke partijen (waaronder wetenschappelijke bureaus)
- Logistiek en op- en overslag
- Lucht- en ruimtevaart
- Defensie- en wapenindustrie
- ICT managed serviceproviders (MSP's)*

* Met ICT managed service providers bedoelen wij informatie- en communicatietechnologie dienstverleners die producten van derden (bijv. AWS, Microsoft Suite) doorverkopen met of zonder aanvullende (configuratie)diensten met toegang op afstand om toegang te krijgen tot de eigen computersystemen op de netwerken van de opdrachtgever voor onderhoud en updates, MSP's die beheerde infrastructuurdiensten (bijv. servers, opslag, netwerken) aanbieden aan opdrachtgevers met behulp van datacenters van derden en die volledig beheerde diensten aanbieden met eigen ontwikkelde software oplossingen, waarbij er verantwoordelijk is voor het beheer, de goede werking, beveiliging en onderhoud, alsmede MSP's die deze end-to-end diensten aanbieden met een eigen infrastructuur (bijv. servers, opslag, netwerken).

Tevens zijn wij niet tot enige vergoeding van schade of kosten (waaronder kosten van verweer) gehouden in verband met of voortvloeiende uit aanspraken, eigen schade of andere aansprakelijkheden indien:

- U/verzekerde gezamenlijk meer dan € 10.000.000 omzet of exploitatiesom heeft;
- U/verzekerde gezamenlijk meer dan 25% van de omzet door export naar de Verenigde Staten van Amerika en/of Canada genereert;
- Er een dochtervennootschap/deelneming buiten de EER (Europese Economische Ruimte) en/of Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland aanwezig is;
- U/verzekerde een lokale dochtervennootschap/deelneming bent/is of een onderdeel uit maakt van een concern/bedrijf met een totale wereldwijde omzet groter dan € 100.000.000 (100 miljoen);
- U/verzekerde toegang op afstand heeft tot de (computer)systemen van derden;
- U/verzekerde van meer dan 500.000 personen gevoelige persoonsgegevens (conform de definitie AVG) heeft en/of heeft opgeslagen in uw eigen netwerk en/of (computer)systemen of bij derden;
- U/verzekerde operationele technologieën (OT)**; industriële controlesystemen (ICS), toezichthoudende controlesystemen (SCADA) of distributed controlesystemen (DCS), gebruikt.

** Operationele technologie is hard- en/of software die een verandering detecteert of veroorzaakt, door middel van de directe bewaking en/of besturing van industriële apparatuur, activa, processen en gebeurtenissen.

Beveiligingsmaatregelen

- Er geen een antivirusprogramma van een gerenommeerde leverancier (bijv. AVG, ESET, McAfee, Norton, Windows Defender) is geïnstalleerd en geactiveerd op uw (computer)systemen, inclusief Apple computers;
- Er niet minimaal wekelijks een back-up wordt gemaakt van ***kritische gegevens en/of systemen en deze los van uw (computer)systeem wordt bewaard dan wel opgeslagen of in één van de volgende cloudoplossingen: Microsoft OneDrive, Google Drive, iCloud of Azure Recovery Services Vault, Amazon, Veeam, IBM;

*** Kritische gegevens/data en kritische systemen worden gedefinieerd als de gegevens/data en systemen die ervoor zorgen dat u inkomsten verliest als ze offline zijn of langer dan 24 uur niet beschikbaar zijn. Waar van toepassing omvat dit ook de gegevens/data van uw klant/opdrachtgever, als een verlies van deze gegevens/data kan leiden tot een aanspraak wegens nalatigheid tegen u.

- Er niet tenminste binnen 30 dagen nadat patches of software updates door de fabrikant zijn uitgegeven de patches en software updates worden uitgevoerd op uw (computer)systemen;
- Er in uw (computer)systeem/netwerkomgeving besturingssystemen die niet langer door de fabrikant worden ondersteund (legacy systems) worden gebruikt, zoals Windows XP, Windows 7 of Windows Server 2008 (tenzij uitsluitend in een geïsoleerde netwerkomgeving dus los van internet of andere (computer)systemen);
- Er binnen het (computer)systeem van verzekeringnemer/verzekerde twee- of multifactor authenticatie (2FA/MFA) wordt gebruikt om de toegang tot alle web-based (e-mail)accounts te beheren (bijv. Office365, Gsuite, Azure, AWS, Salesforce) en om in te loggen op afstand in het (computer)systeem (remote access).

** Operationele technologie is hard- en/of software die een verandering detecteert of veroorzaakt, door middel van de Directe bewaking en/of besturing van industriële apparatuur, activa, processen en gebeurtenissen.

*** Kritische gegevens/data en kritische systemen worden gedefinieerd als de gegevens/data en systemen die ervoor Zorgen dat u inkomsten verliest als ze offline zijn of langer dan 24 uur niet beschikbaar zijn. Waar van toepassing Omvat dit ook de gegevens/data van uw klant/opdrachtgever, als een verlies van deze gegevens/data kan leiden tot een aanspraak wegens nalatigheid tegen u.

HCT1 Terrorismedekking (NHT)

Op deze verzekering is het Clausuleblad Terrorismedekking bij de Nederlandse Herverzekeringsmaatschappij voor Terrorismeschaden N.V. (NHT) van toepassing.
Hiscox verstrekt verzekerde desgewenst, kosteloos, de volledige tekst van het Protocol afwikkeling claims, inclusief toelichting. Ook kan verzekerde het Clausuleblad Terrorismedekking bij de NHT en het Protocol afwikkeling claims, inclusief toelichting, downloaden van de internetsite van de NHT: Www.terrorismeverzekerd.nl.

HCC0 (Mede)verzekerden

Onder u wordt(t)(en) mede verstaan dochtervennootschappen van verzekeringnemer ook zonder eerdere vermelding op het ingevulde aanvraagformulier of (online) verzekeringsvoorstel binnen de kaders van de definitie van dochtervennootschap.

HCC34 Sancties en/of handelsbeperkingen

Wij zijn niet gehouden om dekking of schadeloosstelling te bieden krachtens deze polis, indien dit een inbreuk zou vormen op sanctiewet- en regelgeving (sanctie, verbod of beperking op grond van resoluties van de Verenigde Naties of de handels- of economische sancties, wetten of voorschriften van (landen van) de Europese Unie, het Verenigd Koninkrijk of de Verenigde Staten van Amerika) uit hoofde waarvan het ons verboden is om krachtens deze polis dekking te bieden of een schadeloosstelling uit te keren.

HCC35 (cyber)oorlog uitsluiting

Wij zijn niet tot enige vergoeding van schade of kosten (waaronder kosten van verweer) gehouden in verband met of voortvloeiende uit aanspraken, eigen schade of andere aansprakelijkheden die direct of indirect het gevolg zijn van:

Elke oorlog of cyberoperatie;

- Als een relevante staat een cyberoperatie toeschrijft aan een andere staat, of beweert dat een cyberoperatie is uitgevoerd:
  - Ter ondersteuning van; of
  - Namens

  Een staat, dan wordt voor de toepassing van deze uitsluiting een cyberoperatie geacht te hebben plaatsgevonden, en is deze uitsluiting van toepassing. Een cyberoperatie wordt nog steeds geacht te hebben plaatsgevonden en deze uitsluiting is nog steeds van toepassing indien een staat, met inbegrip van een relevante staat, de toeschrijving of bewering tegenspreekt of ontkent.

- b. Indien er 14 dagen na de datum waarop u voor het eerst melding maakt van een aanspraak, eigen schade of andere aansprakelijkheid, geen toerekening heeft plaatsgevonden zoals hierboven uiteengezet, mogen wij vertrouwen op elke redelijke gevolgtrekking met betrekking tot de toerekening van de cyberoperatie aan een andere staat of degenen die handelen ter ondersteuning van of namens een staat.

Als er een geschil is tussen u en ons over de vraag of er een cyberoperatie heeft plaatsgevonden, is het aan ons om aan te tonen dat deze uitsluiting van toepassing is.

Aanvullende definities in het kader van deze clausule

Computer of digitale technologie

Alle programma's, computernetwerken, software, operationele technologie, op internet aangesloten apparaten, op netwerken aangesloten apparaten, informatietechnologie, communicatiesystemen, met inbegrip van maar niet beperkt tot internet-of-things apparaten, e-mailsystemen, intranet, extranet, websites of cloudcomputingdiensten.

Cyberoperatie

Het gebruik van computer- of digitale technologie door, namens of ter ondersteuning van een staat om gegevens of computer- of digitale technologie in of van een andere staat te verstoren, te blokkeren, te corrumperen, aan te tasten, te manipuleren of te vernietigen.

Oorlog

- Het gebruik van fysiek geweld door een staat tegen een andere staat, al dan niet met een oorlogsverklaring;
- Burgeroorlog, opstand, revolutie of muiterij; en
- Een van de volgende omstandigheden in Nederland veroorzaakt door of ontstaan uit gewapend conflict, burgeroorlog, opstand, binnenlandse onlusten, oproer en muiterij. Deze begrippen zijn gedefinieerd in de tekst, die door het Verbond van Verzekeraars d.d. 2 november 1981 is gedeponeerd ter griffie van de Arrondissementsrechtbank te ‘s-Gravenhage.

Relevante staat

Elke staat;

- Waarin de door een cyberoperatie getroffen gegevens (data) of computer- of digitale technologie
- Zich fysiek bevinden of zijn opgeslagen;
- Die permanent lid is van de Veiligheidsraad van de Verenigde Naties;
- Die lid is van de inlichtingenalliantie "Five Eyes"; of
- Die lid is van de Noord-Atlantische Verdragsorganisatie (NATO).

Staat

Elke soevereine staat.