Hiscox Nederland
Postbus 87033, 1080 JA Amsterdam
A. J. Ernststraat 595B, Amsterdam
T 020 517 07 00
F 020 517 07 01
E hiscox.underwriting@hiscox.nl
I adviseur.hiscox.nl

Informatieblad cyber en data risks verzekering 'CyberClear by Hiscox' 2022

Polis samenvatting: dekking in een notendop
De cyber en data risks verzekering van Hiscox (CyberClear) is ontwikkeld om u te ondersteunen en te beschermen tegen evoluerende cyberbedreigingen en risico's in verband met het houden van gegevens, zowel elektronisch als niet-elektronisch. Wij vergoeden aanspraken en onderzoeken die tegen u worden ingesteld tijdens de looptijd van de polis die voortvloeien uit uw cyber- of privacy-aansprakelijkheid. Dit tot het verzekerd bedrag genoemd op het polisblad, en inclusief uw (juridische) kosten van verweer voor gedekte aanspraken en onderzoeken.

Wij vergoeden ook uw eigen schade die voortvloeit uit cyberincidenten ontdekt tijdens de looptijd van de polis, tot het verzekerd bedrag genoemd in de polis. Waaronder vergoeding van dataherstelkosten, gederfde inkomsten (optioneel) en hogere arbeidskosten (optioneel) als gevolg van geheel of gedeeltelijke stagnatie van uw bedrijf.

Wij werken met experts die praktische ondersteuning en hulp bieden bij een aanspraak of eigen schade, waaronder gespecialiseerde IT-forensische bedrijven en juridische- en public relations dienstverleners.

Elk van de dekkingsonderdelen is onderhevig aan een totaal verzekerd bedrag per verzekeringsjaar, wat het hoogste bedrag is dat we onder de polis zullen betalen, ongeacht het aantal aanspraken, eigen schades of onderzoeken. In sommige gevallen is de dekking van uw eigen schade beperkt tot een sublimiet die onderdeel uitmaakt van het totaal verzekerd bedrag, of is de dekking optioneel. Dit laatste betekent dat u specifiek voor deze dekking moet kiezen bij uw verzekeringsaanvraag.

U moet voor elke aanspraak of eigen schade het eigen risico betalen dat in de polis vermeld staat. Ook kan het eigen risico worden uitgedrukt in een aantal uren (retentietijd); de periode na het incident waarvoor u niet gedekt bent. Dit geldt bijvoorbeeld bij stagnatie van uw bedrijf.

Belangrijkste voordelen CyberClear: tegen welke risico's bent u beschermd?
1. Uw eigen schade

Wij bieden dekking bij:
- het onbevoegd verkrijgen van, onbevoegde toegang geven tot, onbevoegd gebruiken of openbaar maken van, of verlies of diefstal van persoonsgegevens of vertrouwelijke bedrijfsinformatie;
- het door u of namens u onvoldoende beveiligen van uw computersysteem tegen onbevoegde toegang of gebruik;
- een dreiging om uw computersystemen te beschadigen of gevoelige informatie te verspreiden als gevolg van een onbevoegde toegang tot uw computersystemen;
- een digitale aanval bedoeld om de toegang tot of de werking van uw computersysteem te verstoren;
- een stagnatie van uw bedrijfsactiviteiten door een handeling of nalaten van een werknemer of een toeleverancier in het werken met elektronische data of software of het onderhouden en ontwikkelen van uw computersysteem (optionele dekking);
- een stagnatie van uw bedrijfsactiviteiten veroorzaakt door een cyberaanval of beveiligingsinbreuk bij een informatietechnologiedienstverlener waar u afhankelijk van bent (optionele dekking).

Als het bovenstaande zich voordoet dan zullen wij u vergoeden voor:
- de kosten van een forensische analyse om een data inbreuk te bevestigen;
- de juridische kosten om een data inbreuk te managen;
- kosten die worden gemaakt om betrokkenen en toezichthoudende instanties op de hoogte te brengen en om kredietbewakingsdiensten te verlenen;
- de kosten van het gevraagde losgeld en de kosten van specialisten om losgeldonderhandelingen te voeren;
- extra bedrijfskosten die direct worden veroorzaakt door een cyberaanval;
- kosten om weer toegang te krijgen tot uw elektronische data en software of deze te herstellen vanaf back-ups of andere bronnen;
- uw gederfde inkomsten en hogere arbeidskosten als uw bedrijf stagneert (optioneel) of uw reputatie wordt geschaad;
- de kosten om een public relations adviseur aan te stellen om uw reputatie te beschermen en uw media accounts te beheren;
- de kosten om een adviseur in te schakelen om uw reactie op het incident te managen.

Wij vergoeden het bovenstaande ook als u schade heeft geleden als gevolg van een data inbreuk bij een toeleverancier van u.

Hiscox Nederland
Postbus 87033, 1080 JA Amsterdam
A. J. Ernststraat 595B, Amsterdam
T 020 517 07 00
F 020 517 07 01
E hiscox.underwriting@hiscox.nl
I adviseur.hiscox.nl

2. Aanspraken en onderzoeken tegen u

Wij bieden dekking als:

- u aansprakelijk wordt gesteld voor inbreuk op of schending van vertrouwelijkheid, persoonsgegevens, vertrouwelijke bedrijfsinformatie of een contractuele verplichting tot geheimhouding;
- er een onderzoek tegen u wordt ingesteld vanwege het onbevoegd verkrijgen, gebruiken, of toegang geven tot persoonsgegevens of vanwege een schending van een wet die de omgang met persoonsgegevens regelt, inclusief AVG-onderzoeken;
- er een aanspraak tegen u wordt ingesteld wegens het niet nakomen van PCI-DSS;
- u vanwege de inhoud van uw e-mail, website of sociale media-accounts aansprakelijk wordt gesteld voor een inbreuk op intellectuele eigendomsrechten, smadelijke of lasterlijke uitlatingen of inbreuk op licenties;
- u wordt verweten de overdracht van een virus, een aanval die een computersysteem onbeschikbaar maakt of het op een andere manier verhinderen van bevoegde toegang tot een computersysteem of gegevens.

3. Cyberfraude en cyberbedrog

Wij vergoeden uw eigen schade als u het volgende overkomt:

- elektronische diefstal van geld, effecten of zaken;
- frauduleus gebruik van uw telefoonlijnen;
- u maakt geld, effecten of zaken over in directe reactie op een social-engineeringbericht;
- uw opdrachtgever maakt geld, effecten of zaken over als reactie op een social-engineeringbericht na een inbreuk op uw netwerk;
- het frauduleus of oneerlijk gebruik van uw elektronische identiteit.

Beperkingen o.a:
Wij zullen uw schade niet vergoeden voor aanspraken, eigen schade, inbreuken, privacy onderzoeken of bedreigingen als gevolg van:

- het verstrekken van professioneel advies of professionele producten of -diensten;
- het uitvallen van een dienst geleverd door een internetaanbieder, telecommunicatieaanbieder of nutsleverancier of enige andere infrastructuurprovider; o.a. KPN, Eneco
- schending van intellectuele eigendomsrechten, behalve wanneer die ontstaat als gevolg van een data-inbreuk door een derde partij, een beveiligingsinbreuk of een aanspraak onder dekkingsonderdeel Online aansprakelijkheid;
- een hack door een vennoot of bestuurder van u;
- persoonlijk letsel, behalve emotioneel leed als gevolg van een inbreuk op privacy of smaad;
- degradatie, achteruitgang of vermindering van de prestatie van uw computersysteem, anders dan als gevolg van een menselijke fout;
- alles wat u wist of redelijkerwijs had moeten weten voordat u de polis afsloot;
- handelingen of nalatigheden die u opzettelijk of roekeloos begaat, vergoelijkt of negeert;
- alle strafrechtelijke, civielrechtelijke of regelgevende boetes, met uitzondering van PCI-kosten en opgelegde toezichtsmaatregelen (waaronder een verzekerbare bestuurlijke boete);
- het onrechtmatig gebruiken of verzamelen van gegevens;
- financiële transacties zoals handel in aandelen, opties, effecten, derivaten of diefstal of verlies van geld of effecten. Behalve als het een gedekte aanspraak of eigen schade volgens 2.3 Cyberfraude en cyberbedrog betreft.

Als u ons na een (vermoedelijk) data inbreuk binnen 72 uur op de hoogte stelt, zien we af van het eigen risico voor eigen schade met betrekking tot die data inbreuk. Dit geldt niet voor een eventuele van toepassing zijnde retentietijd (eigen risico uitgedrukt in uren).

Hiscox Nederland
Postbus 87033, 1080 JA Amsterdam
A. J. Ernststraat 595B, Amsterdam
T 020 517 07 00
F 020 517 07 01
E hiscox.underwriting@hiscox.nl
I adviseur.hiscox.nl

Verschillen 2021 polisvoorwaarden ten opzichte van oudere polisvoorwaarden
Een deel van de Hiscox-verzekerden zijn nog verzekerd onder oudere polisvoorwaarden dan de voorwaarden uit 2021. Hieronder een korte weergave van de belangrijkste punten die in 2021 zijn aangepast. De kern van de dekking onder de 2021 polisvoorwaarden is niet gewijzigd. Wel is er destijds op een aantal punten een verduidelijking of verfijning aangebracht.

Dekkingsuitbreiding
- Eigen risico bij een data inbreuk vervalt bij melding binnen 72 uur (retentietijd blijft van toepassing);
- Retentietijd gaat in onmiddellijk in bij een stagnatie van uw bedrijf (niet pas na melding bij ons);
- Eigen schade dekking voor key person is opgenomen;
- Definitie van geld opgenomen en uitgebreid met o.a. cryptovaluta;
- Vergoeding voor uw aanwezigheid bij een gerechtelijke instantie € 300,-- per dag(deel) is opgenomen.

Verduidelijking
- Definities zijn uitgebreider (o.a. computersysteem en social-engineeringbericht) en een specifieke definitie van oorlog (clausule) is toegevoegd;
- Uitsluiting opgenomen voor systeemdegradatie of -prestatie en aanspraken buiten het rechtsgebied voor verduidelijking (was eerder ook niet gedekt);
- Verduidelijking van uw verantwoordelijkheden ten aanzien van het doorgeven van wijzigingen in omstandigheden en de schadebeperkende maatregelen die u moet nemen na een cyberaanval;
- Verduidelijking van wanneer het eigen risico van toepassing is of wanneer de retentietijd van toepassing is. Waarbij als er voor enige eigen schade een retentietijd van toepassing is er geen eigen risico voor dat genoemde dekkingsonderdeel verschuldigd is.

Nieuw sublimiet
- Cyberfraude en cyberbedrog sublimieten standaard uitgebreid met social engineering en social-engineering opdrachtgevers naast dekking voor elektronische diefstal, telefoonfraude en frauduleus gebruik van uw elektronische identiteit (nu met een sublimiet);
- Sublimiet eigen schade door stagnatie van uw bedrijf als gevolg van menselijke fout is opgenomen;
- Sublimiet eigen schade aan voorraad is opgenomen (voorheen geen sublimiet);
- Sublimiet eigen schade eigen ingreep vergoeding voor kosten gemaakt in de eerste 72 uur: € 15.000,-- (voorheen gedekt boven het verzekerde bedrag), echter hierop is geen eigen risico van toepassing;
- Sublimiet eigen schade door stagnatie van uw bedrijf als gevolg van een stagnatie bij een informatietechnologiedienstverlener waar u van afhankelijk bent (optionele dekking) als gevolg van een beveiligingsinbreuk of een cyberaanval.

Nieuwe uitsluiting of beperking
- Schadevergoedingstermijn bij stagnatie van uw bedrijf bedraagt maximaal 6 maanden (was 12);
- Dekking voor oneerlijke concurrentie of misleidende handelspraktijken mits in verband met een gedekte aanspraak als gevolg schending recht op privacy en de regelgeving daarop is niet meer opgenomen;
- Uitsluiting bij uw faillissement en bij inbeslagname van uw computersysteem;
- Uitsluiting voor het onrechtmatig gebruiken of verzamelen van gegevens.

Hiscox Nederland
Postbus 87033, 1080 JA Amsterdam
A. J. Ernststraat 595B, Amsterdam
T 020 517 07 00
F 020 517 07 01
E hiscox.underwriting@hiscox.nl
I adviseur.hiscox.nl

Verschillen 2022 polisvoorwaarden ten opzichte van 2021 polisvoorwaarden
Hieronder een weergave van de belangrijkste punten die zijn aangepast in de polisvoorwaarden van 2022.

Om de premie niet verder te laten oplopen voor relaties die geen dekking wensen voor bedrijfsstagnatie en bedrijfstagnatie bij een informatietechnologie-dienstverlener waarvan de verzekerde afhankelijk is, of voor wie deze dekkingen niet van toepassing zijn, hebben wij ervoor gekozen om deze optioneel te maken. Daarnaast zijn er vanwege de toenemende cyberdreiging een aantal nieuwe beveiligingseisen opgesteld, en zijn er een aantal nieuwe acceptatiecriteria toegevoegd.

Nieuwe optionele dekking
- In de standaard dekking die we bieden is eigen schade bij bedrijfsstagnatie (business interruption (BI), waaronder door menselijke fout), niet meer meegenomen. Dit is optioneel mee te verzekeren tegen een meerpremie;
- De dekking voor eigen schade bij bedrijfsstagnatie bij een informatietechnologiedienstverlener waarvan u afhankelijk bent (dependent business interruption (DBI)), is ook een optionele dekking geworden tegen een meerpremie. **Het is niet mogelijk om DBI te verzekeren zonder BI.**

Verduidelijking
- Ter verduidelijking staat in de polisvoorwaarden vermeld dat sublimieten van toepassing zijn per aanspraak/ schade en per verzekeringsjaar.

Nieuw sublimiet
- Voor de optionele dekkingen BI en DBI geldt voor kleinere bedrijven dat de maximale vergoeding gekoppeld wordt aan de jaarlijkse omzet van een verzekeringnemer/verzekerde. Gelijk aan de maximale vergoeding 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
€ 0,00 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 € 2.500.000,--	€ 1.250,--

Niet meer gedekt
- Er geldt geen dekking meer voor eigen schade aan voorraad (bederf), zoals vermeld in de 2021 polisvoorwaarden HCC2021/01 onder 2.4.1.

Aangepaste uitsluiting
- Er geldt een nieuwe uitsluiting voor Financiële transacties onder 3.1.21;
- De uitsluiting zaakschade, zoals vermeld in de 2021 polisvoorwaarden onder 3.1.6, is aangepast vanwege de vervallen dekking voor eigen schade aan voorraad (bederf);
- De uitsluiting Uitval van diensten en storing in infrastructuur onder 3.1.3, is verduidelijkt, en uitval van satellieten is toegevoegd aan deze uitsluiting.

Nieuwe acceptatie- en verlengingscriteria
- Er wordt binnen het (computer)systeem van verzekeringnemer/verzekerde twee- of multifactor authenticatie (2FA) gebruikt om de toegang tot alle web-based (e-mail)accounts te beheren en om in te loggen op afstand in het (computer)systeem;
- Er dienen in het computersysteem/ de netwerkomgeving van verzekeringnemer/verzekerde geen besturingssystemen die niet langer door de fabrikant worden ondersteund (legacy systems) te worden gebruikt (tenzij uitsluitend in een geïsoleerde netwerkomgeving dus los van internet of andere computersystemen);
- Tenminste binnen 30 dagen nadat patches of software updates door de fabrikant zijn uitgegeven, dienen de patches en software updates te worden uitgevoerd op de computersystemen van verzekeringnemer/verzekerde;
- Verzekeringnemer/verzekerde is geen dochtervennootschap/deelneming of maakt geen onderdeel uit van een bedrijf met een omzet groter dan € 100.000.000 (100 miljoen);
- Verzekeringnemer/verzekerde is geen franchisenemer of franchisegever (maatwerk voorstel eventueel mogelijk apart aanvragen);
- Er wordt geen operational technology (OT) gebruikt door verzekeringnemer/verzekerde (maatwerk voorstel eventueel mogelijk apart aanvragen) Onder operational technology verstaan wij 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);
- Windows Defender is toegevoegd aan de lijst geaccepteerde Anti-Virus software.

Wijziging clausules
- (Cyber)oorlog uitsluiting;

Hiscox Nederland
Postbus 87033, 1080 JA Amsterdam
A. J. Ernststraat 595B, Amsterdam
T 020 517 07 00
F 020 517 07 01
E hiscox.underwriting@hiscox.nl
I adviseur.hiscox.nl

- Sancties en/of handelsbeperkingen.

Nieuw acceptatiecriterium (alleen van toepassing op nieuwe acceptatie)

- Bedrijven in de volgende sectoren worden niet langer geaccepteerd binnen onze pre-priced cyber & data risks verzekering: managed service providers (MSP), gemeentes, logistiek en warehousing. Voor managed service providers, en voor gemeentes kleiner dan 100.000 inwoners, is een maatwerkvoorstel mogelijk een oplossing. Hiervoor kan de verzekeringsadviseur contact met ons opnemen. Onder een MSP (Managed Service Provider) verstaan wij: Een informatie- en communicatietechnologie bedrijf dat op afstand de informatietechnologie-infrastructuur (IT) en de eindgebruikerssystemen van een opdrachtgever/klant beheert. Deze doorlopende beheerdiensten omvatten onder meer netwerk- en infrastructuurbeheer, applicatiebeheer, het aanbieden van clouddiensten en diensten op het gebied van beveiliging en monitoring. Onder het aanbieden van clouddiensten verstaan wij het aanbieden van diensten volgens de servicemodellen Software as a Service (SaaS), Platform as a Service (PaaS), Network as a Service (NaaS), Desktop as a Service (DaaS), Infrastructure as a Service (IaaS). Hieronder verstaan wij uitdrukkelijk niet de diensten van cloud service providers zoals deze worden aangeboden door onder andere Amazon Web Services, Microsoft Azure, Google cloud en VM ware.