P175 - HCC19 Melding van een incident/schade - PPP

HCC19 Melding van een incident/schade

De vereisten waaraan een melding van een **aanspraak**, een **omstandigheid** of **eigen schade** moet voldoen worden omschreven in de polisvoorwaarden. Elke melding dient zo spoedig als redelijkerwijs mogelijk gericht te worden aan **ons**.

Hiscox Nederland
Postadres Postbus 87033
1080 JA Amsterdam

Telefoon + 31 (0)20 517 0700, en per e-mail **hiscox.claims@hiscox.nl** (Hiscox incident response team).

P176 - HCC20 Anticumulatie - PPP

HCC20 Anticumulatie

In aanvulling op het bepaalde in de polisvoorwaarden Hiscox Cyber en Data Risks (CyberClear) onder 'omvang van de vergoeding' wordt elke schadeloosstelling met betrekking tot een **aanspraak** (inclusief **kosten van verweer**, **bereddings**- en **onkosten**) met betrekking tot de Hiscox beroepsaansprakelijkheidspolis en/of de Hiscox bedrijfsaansprakelijkheidspolis (hierna de andere **polissen**) eveneens in mindering gebracht op het **verzekerd bedrag** van de Hiscox Cyber en Data Risks (CyberClear) **polis** (hierna de onderhavige polis).

Onder geen beding zal de door **ons** betaalde schadeloosstelling uit hoofde van onderhavige **polis** en de andere **polissen** tezamen meer bedragen dan het hoogste **verzekerd bedrag** van één van genoemde **polissen** per **aanspraak** en per **verzekeringsjaar** met inbegrip van **kosten van verweer**, **bereddings**- en (on)**kosten**.
Dit betekent dat het **verzekerd bedrag**, de **kosten van verweer**, **bereddings**- en **(on)kosten** van de **polissen** niet in aanvulling zijn op elkaar.

P177 - HCC21 Sublimiet, retentietijd en eigen risico - PPP

HCC21 Sublimiet, retentietijd en eigen risico

In afwijking van het op het polisblad vermeld **verzekerd bedrag** wordt er per **aanspraak/eigen schade** en per **verzekeringsjaar** niet meer vergoed dan per onderstaande dekking genoemd bedrag.
Dit bedrag geldt als onderdeel van het op het polisblad vermeld **verzekerd bedrag (sublimiet)**.

Eigen schade bij bedrijfsstagnatie (business interruption):

- **eigen schade** door bedrijfsstagnatie (business interruption) gelijk aan het **verzekerd bedr**ag vermeld op het polisblad met een **schadevergoedingstermijn** van 6 maanden en een **retentietijd** van 8 uur;
- **eigen schade** door stagnatie als gevolg van **menselijke fout** (system failure) 20% van het **verzekerd bedrag** zoals vermeld in de **polis** met een maximum van € 250.000,-- met een **schadevergoedingstermijn** van 6 maanden en een **retentietijd** van 8 uur;
- optionele dekking **eigen schade** door stagnatie bij een **informatietechnologiedienstverlener** waar u afhankelijk van bent (ict dependent business interruption) 20% van het **verzekerd bedrag** zoals vermeld in de **polis** met een maximum van € 250.000,-- met een **schadevergoedingstermijn** van 6 maanden en een **retentietijd** van 12 uur uitsluitend indien voor deze optie is gekozen in het Pre Priced Proposal (online)formulier.

Eigen schade dekking cyberfraude en cyberbedrog met een **eigen risico** van € 1.000,-- per schade:

- elektronische diefstal: € 25.000,--;
- telefoonfraude: € 50.000,--;
- social engineering en social-engineeringschade opdrachtgevers: € 25.000,--;
- frauduleus gebruik van **uw** elektronische identiteit: € 50.000,--.

Aanvullende dekkingen/vergoedingen:

- **eigen schade** aan voorraad: 20% van het **verzekerd bedr**ag met een maximum van 250.000,-- met een **eigen risico** van € 2.500 per schade;
- eigen ingreep vergoeding voor kosten gemaakt in de eerste 72 uur: € 15.000,--, hierop is geen **eigen risico** van toepassing;
- kosten voor **uw** aanwezigheid bij een gerechtelijke instantie € 300,-- per dag(deel).

P178 - HCC22 (Mede)verzekerden - PPP

HCC22 (Mede)verzekerden

Onder u word(t)(en) mede verstaan de volgende natuurlijke personen, rechtspersonen of samenwerkingsverbanden:

-

P179 - HCC23 Rechtsgebied - PPP

HCC23 Rechtsgebied

Het rechtsgebied onder deze polis is gehele wereld exclusief de Verenigde Staten van Amerika en Canada.

P181 - HCB21 Aanvullende dekking Cyber en Data Risks - PPP

HCB21 Aanvullende dekking Cyber en Data Risks (CyberClear) in de beroeps-aansprakelijkheidsverzekering

In het kader van de aanvullende dekking inzake Cyber en Data Risks (CyberClear) in de beroepsaansprakelijkheidsverzekering geldt het navolgende:

- het **verzekerd bedrag** per **aanspraak/(eigen)schade** bedraagt € 100.000,- per **aanspraak** en per **verzekeringsjaar** als onderdeel van het **verzekerd bedrag** voor beroepsaansprakelijkheid genoemd op het polisblad;
- het **eigen risico** bedraagt € 1.000,- per **aanspraak/ (eigen)schade**;
- er is geen **retentietijd**, **sublimiet** of optionele dekking van toepassing (met uitzondering van een **sublimiet** van € 25.000,-- per **verzekeringsjaar** per dekkingsonderdeel, (i) elektronische diefstal, (ii) telefoonfraude, (iii) social engineering + social-engineeringschade opdrachtgevers en een **sublimiet** van € 15.000,-- per **verzekeringsjaar** voor eigen ingreep vergoeding 72 uur); kostenvergoeding voor **uw** aanwezigheid bij een gerechtelijke instantie € 300,-- per dag(deel);
- de van toepassing zijnde polisvoorwaarden zijn CyberClear by Hiscox 2021 (HCC 2021/01);
- 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); telefoon + 31 (0)20 517 0700, en per e-mail hiscox.claims@hiscox.nl (Hiscox incident response team).

P182 - HCC25 Oorlog uitsluiting – PPP

HCC25 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:

- **oorlog** of een **cyberoperatie** die wordt uitgevoerd gedurende een **oorlog**; en/of
- **cyberoperaties** als vergeldingsmaatregel tussen **gespecificeerde staten** die ertoe leiden dat twee of meer **gespecificeerde staten getroffen staten** worden; en/of
- een **cyberoperatie** die een belangrijke nadelige invloed heeft op:
  - het functioneren van een **staat** als gevolg van het directe of indirecte effect van de cyberoperatie op de beschikbaarheid, integriteit of levering van een **essentiële dienst** in die **staat**; en/of
  - de veiligheid of verdediging van een **staat**.

Onderdeel 3 is niet van toepassing op het directe of indirecte effect van een **cyberoperatie** op een **computersysteem gelegen buiten de getroffen staat (bystanding cyber asset)**.

Toewijzing

Wij zullen de bewijslast dragen van de toewijzing van een **cyberoperatie** aan een bepaalde **staat**.

De primaire maar niet exclusieve factor bij het bepalen of **wij** voldaan hebben aan de bewijslast voor toewijzing is of de **getroffen staat** waarin het **computersysteem** zich fysiek bevindt de **cyberoperatie** toerekent aan een andere **staat** of aan degenen die namens die andere **staat** optreden.

In afwachting van toewijzing door de **getroffen staat**, kunnen **wij** vertrouwen op een objectief redelijke gevolgtrekking met betrekking tot de toerekening van de **cyberoperatie** aan een andere **staat** of aan degenen die namens die andere **staat** optreden.

In het geval dat de **getroffen staat** de **cyberoperatie** niet toerekent of niet kan toerekenen aan een andere **staat** of degenen die namens die andere **staat** optreden, is het aan ons om te bewijzen dat de uitsluiting van toepassing is door te verwijzen naar ander beschikbaar bewijs.

Definities

Computersysteem gelegen buiten de getroffen staat (bystanding cyber asset)
Een **computersysteem** dat door **u** of door **uw informatietechnologiedienstverleners** wordt gebruikt dat in fysieke zin niet gelegen is in een **getroffen staat** maar nadelige invloed heeft ondervonden van een **cyberoperatie**.

Computersysteem
Elke computer, hardware, software, communicatiesysteem, elektronisch apparaat (daar onder begrepen maar niet beperkt tot smartphone, laptop, tablet, wearable device), server, cloud infrastructuur of microcontroller waaronder elk gelijksoortig systeem of configuratie van het bovengenoemde en de daar bijbehorende input, output, dataopslagapparaat, netwerkapparatuur of backup-faciliteiten.

Cyberoperatie
Het gebruik van een **computersysteem** door of namens een **staat** om de informatie in een **computersysteem** of het **computersysteem** zelf van of in een andere **staat** te verstoren, blokkeren, corrumperen, manipuleren of vernietigen.

Essentiele dienst
Een dienst die essentieel is voor het behoud van vitale functies van een **staat**, daaronder begrepen financiële organisaties en daarbij behorende infrastructuur van de financiële markten, gezondheidsdiensten of nutsvoorzieningen.

Gespecificeerde staten
China, Frankrijk, Duitsland, Japan, Rusland, Verenigd Koninkrijk of Verenigde Staten van Amerika.

Staat
Soevereine staat.

Getroffen Staat
Elke **staat** die door een **cyberoperatie** een belangrijke nadelige invloed ondervindt op:

- het functioneren van een staat als gevolg van het directe of indirecte effect van de **cyberoperatie** op de beschikbaarheid, integriteit of levering van een **essentiële dienst** in die staat; en/of
- de veiligheid of de verdediging van die **staat**.

Oorlog
Het gebruik van fysiek geweld door een **staat** tegen een andere **staat**, al dan niet verklaard.

P183 - HCC26 Uitsluitingen - PPP

HCC26 Uitsluitingen

Wij zullen **u/verzekerde** geen dekking verlenen en niet tot enige vergoeding of betaling van schade of kosten (waaronder **kosten van verweer**) gehouden zijn in verband met of voortvloeiende uit een **aanspraak**, **omstandigheid** of **eigen schade** indien:
U/verzekerde behoort tot de navolgende branches/sectoren en/of de navolgende diensten levert:

- financiële instelling
- advisering van en/ of bemiddeling in financiële producten
- betalingsverwerking (payment processing)
- sociale media en sociale netwerken
- kredietbeoordelaar (ratingbureau)
- kansspel-sector
- seksbranche

Wij zullen **u/verzekerde** tevens geen dekking verlenen en niet tot enige vergoeding of betaling van schade of kosten (waaronder **kosten van verweer**) gehouden zijn in verband met een **aanspraak**, **omstandigheid** of **eigen schade** indien:

- **u/verzekerde** geen antivirus programma van een gerenommeerde leverancier heeft geïnstalleerd en geactiveerd op **uw**/haar **computersystemen**;
- **u/verzekerde** van meer dan 100.000 betaalkaarten (credit cards) gegevens opslaat in **uw**/haar netwerk en/of **uw**/haar **computersystemen** of bij derden (serviceproviders).
- **u/verzekerde** niet tenminste elke maand zowel patches als software updates op **uw**/haar **computersystemen** uitvoert;
- **u/verzekerde** niet minimaal wekelijks een back-up maakt van **uw**/haar kritische gegevens en/of **computersystemen** en deze los van **uw**/haar **computersysteem** bewaart/opslaat of in een van de volgende cloudoplossingen; Microsoft OneDrive, Google Drive, iCloud of Azure Recovery Services, Amazon;
- **u/verzekerde** binnen **uw**/haar **computersysteem** geen gebruik maakt van twee- of multifactor authenticatie (2FA) om de toegang tot alle web-based (e-mail) accounts te beheren en om in te loggen op afstand in **uw**/haar **computersysteem** (remote access). Dit geldt alleen voor bedrijven of instellingen met een omzet/ exploitatiesom boven € 5.000.000.

Kritische gegevens/data en kritische **computersystemen** worden gedefinieerd als de gegevens/data en **computersystemen** 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**.