HISCOX

CyberClear
by Hiscox

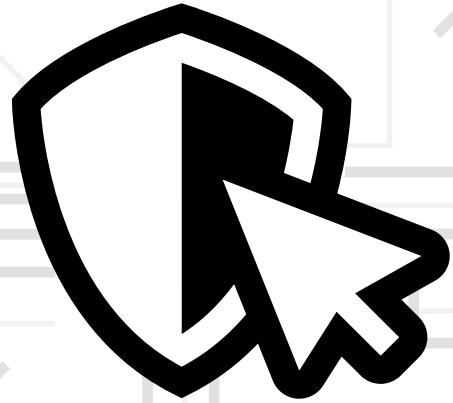
HCC-2022/01

100% veilig bestaat niet

Cybercriminelen kunnen uw computersystemen overnemen en uw data blokkeren, manipuleren of wegnemen. Soms leidt dat ook tot bedrijfstilstand. Vaak is één klik op een foute link al genoeg. Zulke cyberincidenten komen dan ook veel voor, bij alle bedrijven van zzp-er tot multinational. Natuurlijk beveiligt u uw computersystemen hiertegen. Maar wat als het dan toch misgaat? Hoe kunt u de klok dan laten terugzetten tot nét voor het incident?

100% veilig bestaat niet.
CyberClear by Hiscox verzekert u als uw bedrijf ondanks een goede beveiliging slachtoffer wordt van hacking, systeeminbraak, datadiefstal of een andere vorm van cybercriminaliteit. En biedt ook dekking bij een menselijke fout. Bijvoorbeeld wanneer uw werknemer een foutje maakt tijdens het onderhoud aan uw computersysteem, waardoor de toegang tot data verloren raakt. Het is een verzekering die verder gaat dan het vergoeden van schade. Na een inbreuk krijgt u assistentie van ervaren cybersecurity-professionals, met wereldwijd bereik en met uitgebreide juridische expertise. Zij helpen bijvoorbeeld databases en websites te repareren, betrokkenen te informeren en juridische kosten te beperken. Hiscox biedt daarnaast toegang tot diverse preventiediensten bij het afsluiten van een verzekering.

Dekkingen CyberClear by Hiscox



Eigen schade

- Inbreukkosten
- Kosten van bedrijfs-stagnatie (optioneel)
- Schade als gevolg van betaling cyberlosgeld
- Dataherstelkosten en hogere bedrijfskosten
- Public relations-kosten
- Kosten inzet key person-adviseur

Cyberfraude en cyberbedrog

- Elektronische diefstal en telefoonfraude
- Social-engineering (phishing)
- Frauduleus gebruik van de elektronische identiteit van de verzekerde

Aanspraken en onderzoeken

- Privacy- en PCI-aansprakelijkheid
- Privacy- en AVG-onderzoeken
- Online-aansprakelijkheid
- Netwerkbeveiligings-aansprakelijkheid

Aanvullende dekkingen

- Eigen ingreep-kosten voor kosten gemaakt in de eerste 72 uur na incident en melding
- Aanwezigheid bij een gerechtelijke instantie

Eigen schade

De eigen schade is gedekt als deze het gevolg is van een inbreuk, beveiligingsinbreuk, onrechtmatige bedreiging of cyberaanval.

Inbreukkosten

Met instemming van Hiscox worden redelijke en noodzakelijke kosten van een inbreuk vergoed. Zoals juridische kosten, forensische inbreukkosten, meldingen aan betrokkenen en toezichthoudende instanties, kredietbewakingskosten en controle van het darkweb op de aanwezigheid van gestolen data. Dit geldt ook als de inbreuk rechtstreeks wordt veroorzaakt door een toeleverancier. Hiervoor geldt een sublimiet.

Kosten van bedrijfsstagnatie (optionele dekkingen)

Gederfde inkomsten en hogere arbeidskosten zijn gedekt, als die het gevolg zijn van een gedeeltelijke of totale bedrijfsstagnatie na het cyberincident. Als de stagnatie ontstaat door een menselijke fout zijn daarnaast dataherstelkosten en public relations-kosten gedekt. Ook wanneer de stagnatie plaatsvind bij een informatietechnologiedienstverlener waarvan u afhankelijk bent. Voor deze dekkingen moet specifiek gekozen worden en er geldt een maximale vergoeding per dag of een vaste sublimiet.

Schade als gevolg van betaling cyberlosgeld

Advies en begeleiding bij de afhandeling van de eis tot betaling van losgeld, kosten van losgeldeisen en vergoeding van eventueel gestolen losgeld.

Dataherstelkosten en hogere bedrijfskosten

U heeft recht op een onkostenvergoeding voor het opnieuw toegang verkrijgen tot data of software die onbereikbaar is door een incident. Stijgen de bedrijfskosten als direct gevolg van een cyberaanval? Dan zijn deze ook gedekt. Denk aan hogere kosten voor energie- en internetgebruik, kosten om de SEO-positie te herstellen en kosten door het kwaadwillig klikken op pay-per-click-links.

Public relations-kosten

Onder de dekking vallen ook public relations-kosten, gederfde inkomsten en hogere arbeidskosten als gevolg van reputatieschade.

Kosten inzet key person-adviseur

Is een senior manager of directeur druk bezig met de reactie op een incident of inbreuk? Dan worden de kosten voor het inschakelen van een extra adviseur vergoed.

”100% veiligheid bestaat niet. Anticipeer op risico’s die uw bedrijfsactiviteiten in gevaar kunnen brengen. Bescherm uw bedrijf tegen het onverwachte. Wij kunnen u daarbij helpen.”

Aanspraken en onderzoeken

Diverse kosten als gevolg van aanspraken en onderzoeken tegen u zijn gedekt, in verband met;

Privacy- en PCI-aansprakelijkheid
Eventuele schadevergoeding en kosten die u maakt vanwege een claim van derden na een schending van privacy of openbaarmaking van persoonsgegevens, het niet nakomen van PCI DSS, of het verspreiden van vertrouwelijke bedrijfsinformatie.

Privacy- en AVG-onderzoeken
Kosten van privacy of AVG-onderzoeken tegen u, zoals kosten van verweer en opgelegde toezicht maatregelen.

Online-aansprakelijkheid
Kosten van onderzoek en schadevergoeding die voortvloeit uit inbreuk op intellectueel eigendom of een licentie en smaad en laster als gevolg van gehackte communicatiemiddelen zoals e-mail, social media of websites.

Netwerkaansprakelijkheid
Kosten van verweer en schadevergoeding na een claim wegens een virusverspreiding, een ‘denial-of-service’-aanval tegen een derde of een geblokkeerde toegang tot computersystemen of data.

Cyberfraude en cyberbedrog

Bij een eigen schade als gevolg van een inbreuk, beveiligingsinbreuk, onrechtmatige bedreiging of cyberaanval geldt voor onderstaande onderdelen een dekking met sublimiet zoals aangegeven in de polis.

Elektronische diefstal en telefoonfraude
Verlies van geld of zaken als gevolg van activiteiten van een hacker. Ook het onrechtmatig gebruik van uw telefoonlijnen is gedekt.

Social-engineering (phishing)
De kosten van het overboeken of overdragen van middelen in directe reactie op een social-engineeringbericht. Dekking geldt ook voor kosten die u maakt doordat een opdrachtgever middelen overdraagt naar een derde als reactie op een social-engineeringbericht van een hacker, verzonden vanuit uw computersysteem.

Frauduleus gebruik van de elektronische identiteit van de verzekerde
Kosten die voortvloeien uit het misbruik van uw elektronische identiteit. Zoals het bedrag van het verduisterde geld, de kosten van de fraudeuleuze gesprekken en kosten die worden gemaakt om uit een overeenkomst te stappen die is aangegaan door het misbruik van uw elektronische indentiteit.

Aanvullende dekkingen

De volgende aanvullende dekkingen worden verstrekt tot de bijbehorende sublimiet zoals vermeld in de polis.

Eigen ingreep-kosten voor kosten gemaakt in de eerste 72 uur na incident en melding

Schadevergoeding voor redelijke en noodzakelijke kosten die u of een derde maakt om een aanspraak of schade te voorkomen binnen 72 uur na het incident.

Aanwezigheid bij gerechtelijke instantie

Een vergoeding wanneer Hiscox van u (of uw werknemer) verlangt dat u aanwezig bent als getuige bij een rechtzaak vanwege een aanspraak tegen u.

Preventie

Bij het afsluiten van een verzekering krijgt u toegang tot preventiediensten. Voorkomen is immers beter dan schade. Deze services maken u bewust van risico's en mogelijke maatregelen. Zoals de Hiscox CyberClear Academy, waarmee ondernemers en hun medewerkers een 'menselijke firewall' leren bouwen. En zoals de diverse scans en risicoanalyses. Een compleet overzicht vindt u op hiscox.nl.

Hiscox helpt schade te beperken

Wordt u aangesproken of vindt er een incident plaats? Pas bij schade merkt u dat u uitstekend bent verzekerd. We hanteren de hoogste standaard in schadeafhandeling.

Hiscox geeft u advies om de schade te beperken, schakelt experts in en zet alles op alles om de klok terug te draaien.

Zo werkt het

Aanleiding

Een cyberincident heeft plaatsgevonden.

ONDERNEEM DIRECT ACTIE!
Informeer Hiscox en uw verzekeringsadviseur.

24 uurs incident response nummer:

0031 – 20 517 07 00

Wat kunt u van Hiscox verwachten?

1. De eerste 72 uur zijn cruciaal om de schade te beperken en de oorzaak en omvang van het incident te bepalen. Hiscox gaat met u in gesprek en schakelt forensisch experts in om onderzoek te doen. Schade aan computersystemen en/of netwerken wordt hersteld, in samenwerking met toegewezen experts.

2. Bij een datalek bent u verplicht om hiervan zelf binnen 72 uur een melding te maken bij de Autoriteit Persoonsgegevens. Hiscox begeleidt u desgewenst in het maken van de melding.
Ter bescherming van persoonsgegevens en om boetes te voorkomen worden daarnaast, indien nodig, juridisch experts ingeschakeld.

3. Mogelijk zijn er meer betrokkenen? Hiscox kan helpen met het maken van een conceptbrief waarmee u betrokkenen kan informeren. Waar nodig worden daarnaast experts ingeschakeld op het gebied van public relations.

Het volledige incident response plan; met uitleg over uw en Hiscox' verantwoordelijkheden na een incident, kunt u vinden op adviseur.hiscox.nl.

Hiscox Nederland
Arent Janszoon Ernststraat 595B
Postbus 87033
1080 JA Amsterdam

T 00 31 (0)20 517 0700
E hiscox.underwriting@hiscox.nl
www.hiscox.nl

HCC-2022/01