



HISCOX

Verzekerd van expertise

Cyberverzekeringen van Hiscox

Verzekerd van continuïteit,
sterke preventie en snel,
digitaal aanvraagproces

www.hiscox.be

Bedrijven beschermen tegen cyberdreigingen: **een cruciale uitdaging voor uw klanten!**

In een steeds meer gedigitaliseerde wereld worden de risico's van cyberaanvallen op bedrijven groter ... en dus ook de behoeften van uw klanten om zich hiertegen te beschermen! Met de CyberClear-verzekeringen van Hiscox biedt u ze deze bescherming, zodat ze niet alleen staan tegenover cyberrisico's.



Wat is een cyberdreiging?

- Een medewerker van een bedrijf schrijft € 25.000 over aan cybercriminelen nadat hij werd misleid door een phishing-e-mail die ogenschijnlijk door een senior manager was verzonden.
- Een medewerker vergeet in de trein zijn laptop waarop persoonsgegevens staan, met als gevolg een meldingsplicht op grond van de AVG.
- De bestanden van een klein bedrijf worden plotseling versleuteld en een hacker vraagt losgeld.
- Een medewerker configureert in het weekend foutief een software-update, waardoor de systemen crashen en de bedrijfsactiviteit stilvalt.

De dreiging komt steeds dichterbij en wordt steeds duurder

- In 2020 kreeg bijna één op de twee bedrijven te maken met een cyberaanval.*
- De geleden schade bedraagt al gauw meer dan € 10.000 en soms zelfs enkele miljoenen euro's.*
- In meer dan 15% van de gevallen bracht de aanval het voortbestaan van het bedrijf in gevaar.*

* Cijfers uit het Hiscox Cyber Readiness Report 2021.

Een e-mail openen was een alledaagse en onschuldige handeling... maar vandaag niet meer!

Met een eenvoudige frauduleuze e-mail kan uw klant het slachtoffer worden van een opportunistische hacker die het misschien gemunt heeft op zijn klanten. De gevolgen zijn meervoudig:



Operationele gevolgen:

tijdverlies bij het oplossen van het incident, technische werkloosheid, enz.



Reputatiegevolgen:

verlies van geloofwaardigheid bij klanten, enz.



Financiële gevolgen:

omzetverlies, cashflow-problemen, enz.

Vermijd het risico dat uw klant alleen komt te staan in geval van een cyberincident.

Is een verzekering tegen cyberdreiging echt **onmisbaar**?

Ja, want in een wereld die steeds sneller verandert, evolueren ook de risico's... Het is daarom essentieel dat de professionele dekkingen en verzekeringen zich mee aanpassen, zodat uw klanten écht beschermd zijn.

- Omdat de technische beveiligingen onvoldoende zijn.
- Omdat andere beroepsverzekeringen dit risico niet dekken.



Technische beveiliging en de cyberverzekering en vullen elkaar aan:



Technische beveiliging

- De eerste verdediging tegen een cyberincident
- Essentieel maar niet onfeilbaar
- Sluit menselijke fouten niet uit



Een specifieke Cyberverzekering

Beheert de crisis dankzij:

- ✓ een selectie van de beste experts
- ✓ een snelle mobilisatie van hun diensten
- ✓ een vergoeding van hun prestaties

Waarom dekken andere verzekeringen uw klant niet?



Alleen een cyberverzekering ondersteunt uw klant in geval van een cybercrisis en helpt om de impact op zijn bedrijf te minimaliseren.



De verzekering voor beroepsaansprakelijkheid?

Dekt alleen de schade geleden door een klant/derde partij die de kwaliteit van de dienstverlening betwist, maar het dekt geen schade die verband houdt met een cyberaanval op het bedrijf.



De verzekering voor alle risico's in informatica?

Dekt enkel materiële schade en de gevolgen daarvan voor de IT-apparatuur, maar het dekt geen verlies van gegevens, openbaarmaking van gevoelige informatie, enz.

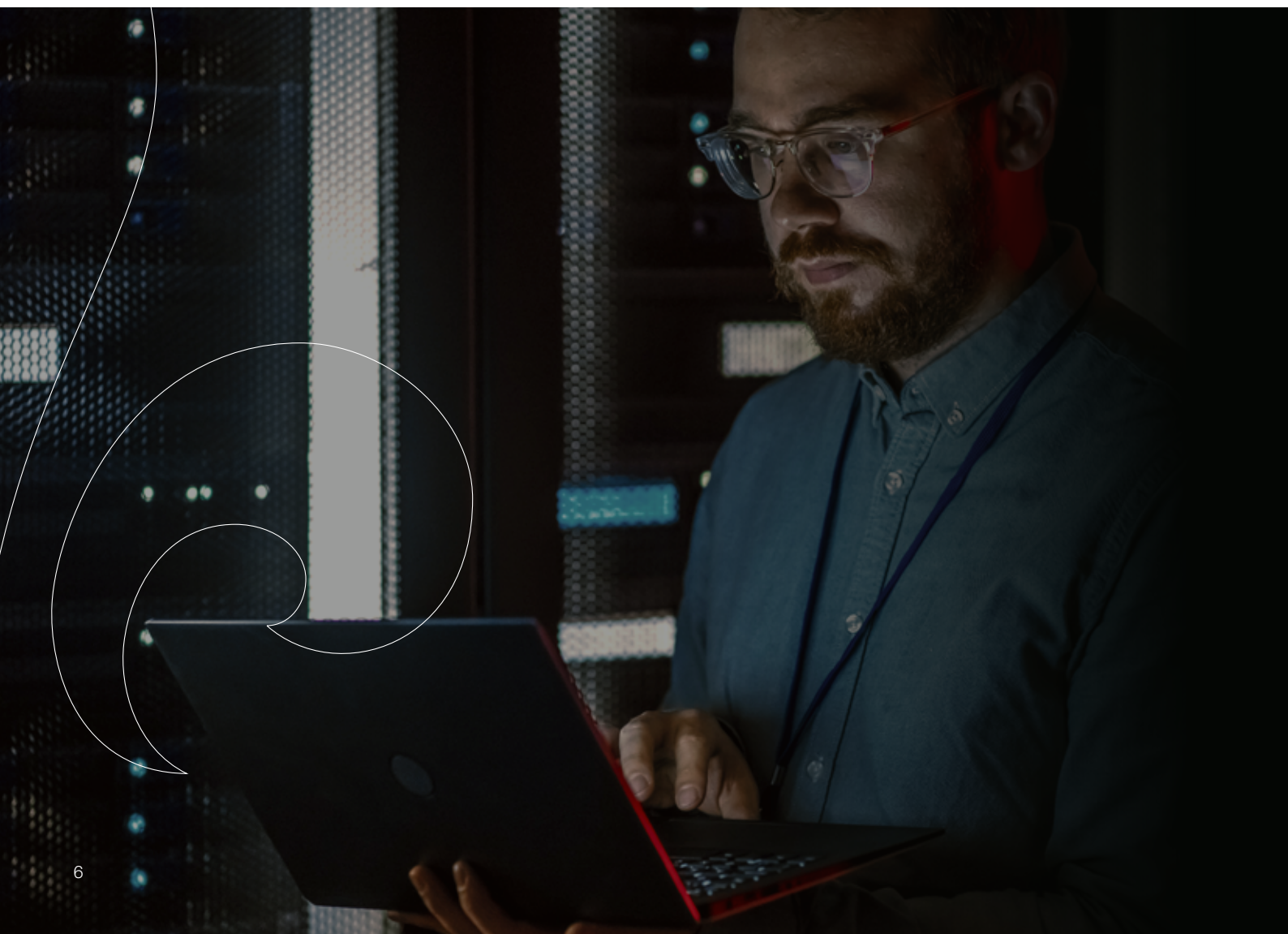


De fraudeverzekering?

Dekt alleen de gevolgen van onwettige handelingen die tegen uw klant gericht zijn (zoals misbruik van vertrouwen, vervalsing en gebruik van vervalsing, fraude) met als doel om onrechtmatig waarde of goederen te verkrijgen, maar het geeft in het bijzonder geen dekking voor cyberafpersing en aanvallen op de integriteit van het informatiesysteem en/of van de gegevens waarover het bedrijf beschikt.

Volledige ondersteuning tegen cyberdreigingen. Vóór, tijdens en na!

Onze CyberClear-verzekeringen bieden uw klanten 100% bescherming. Op alle vlakken en op elk moment... ook preventief, dankzij talrijke diensten en opleidingen. Zo staan uw klanten sterker wanneer ze te maken krijgen met een cyberdreiging!



Wat onderscheidt de CyberClear-verzekeringen van Hiscox van de andere cyberproducten op de markt?

CyberClear en CyberClear Premium zijn complete oplossingen voor cyberbeveiliging die uw klanten begeleiden op technisch, juridisch, menselijk en financieel vlak... vóór, tijdens en na een crisis!

Vóór een crisis? Inderdaad: Hiscox werkt al in een vroeg stadium samen met uw klanten, met name door hun medewerkers op te leiden in alle aspecten van cyberbeveiliging. En de polis biedt uw klanten tijdens en na een crisis brede garanties tegen cyberrisico's, waarbij ze genieten van de expertise van een netwerk van experts.

Welke dekkingen biedt een CyberClear verzekering?

Preventie

Wij bieden uw klanten verschillende preventiediensten en opleidingen, aangepast aan de omvang van hun bedrijf:

- onbeperkte toegang tot de Hiscox Cyber Insight-scan en het bijbehorende rapport: detectie van kwetsbaarheden inclusief aanbevelingen;
- toegang tot beveiligingsopleidingen van CybSafe inclusief phishingsimulaties voor medewerkers;
- mogelijkheid om scans te herhalen en risico's actief te beheren;
- Norton Small Business-software voor cybersecurity, geschikt voor maximaal 20 toestellen (uitsluitend bij de Cyberverzekering Premium).

Bijstand

- Bij een incident en met een eenvoudig telefoontje, mobiliseren we onmiddellijk de noodzakelijke specialisten om de crisis te beheersen: **informaticaexperts + gespecialiseerde advocaten + specialisten in crisiscommunicatie**
- Zonder vrijstelling

Operationele kosten

We dekken de verschillende uitgaven, kosten en operationele verliezen die veroorzaakt werden door een cyberincident:

- gevolgen van inkomstenderving en kosten van corrigerende maatregelen;
- kosten van de kennisgeving van de inbreuk op de gegevens aan regelgevende instanties en personen;
- kosten voor het terughalen van verloren, gestolen of beschadigde gegevens;
- credit monitoring;
- kosten voor verbetering;
- cyberdiefstal;
- ransomware;
- juridische- en onderzoekskosten voor regelgevers.

Aansprakelijkheid

We behandelen alle klachten om uw commerciële belangen te beschermen:

- schade aan derden (klanten, prospecten, leveranciers, enz.) en in het bijzonder schade als gevolg van een inbreuk in verband met persoonlijke en professionele gegevens, een virusoverdracht...

De verzekeringen in één oogopslag

CyberClear Basis

- Slechts twee technische vragen voor onderschrijving voor ondernemingen tot € 25 miljoen omzet: wordt er gebruikgemaakt van multifactorauthenticatie (MFA) of single sign-on? Is er een back-up, losgekoppeld of in de cloud?
- CybSafe. Via dit platform krijgen medewerkers phishingsimulaties en kunnen ze opleidingen volgen over onder meer veilig e-mailgebruik en handelen bij een cyberincident.
- Hiscox Cyber Insight Pro-risicoscan. Door gewoon een URL of domeinnaam in te geven, ziet u waar mogelijke kwetsbaarheden zitten en hoe uw onderneming er online voor staat.
- Eén selfserviceportaal om alles zelf te beheren. Van CybSafe-opleidingen tot de kwetsbaarheidsscan van Hiscox Cyber Insight, alles overzichtelijk gebundeld op één plaats.

CyberClear Premium

In de kern gelijk aan de Cyberverzekering, maar met deze extra's:

- ✓ Norton Small Business-software voor cybersecurity, geschikt voor maximaal 20 toestellen;
- ✓ zonder franchise.

HISCOX CYBER HOTLINE 24/7

24 uren incident response nummer

0800 90255 gratis nummer, alleen binnen België

078 059001 nationaal tarief, bereikbaar binnen België en internationaal met landnummer +32



Tools om zich voor te bereiden op een cyberaanval

Preventietrainingen, checks, scans en Norton Small Business-software. Uw klanten beschikken over de beste tools om zich voor te bereiden op en zich te beschermen tegen cybercriminelen!

CybSafe

CybSafe versterkt het digitale bewustzijn van medewerkers via korte, begrijpelijke en direct toepasbare veiligheidslessen. Het helpt bedrijven risico's te verminderen door gedrag te sturen in plaats van enkel op technologie te vertrouwen.

Wat klanten hierbij winnen:

- praktische micro-trainingen die inspelen op actuele dreigingen, zoals phishing simulaties;
- inzicht in risicovol gedrag binnen het bedrijf, met duidelijke rapportering;
- sterkere bescherming tegen phishing, zwakke wachtwoorden en datalekken;
- minder incidenten en minder onderbrekingen in de dagelijkse werking;
- continue updates zonder technische complexiteit voor de gebruiker.

Kwetsbaarheidsscans van Hiscox Cyber Insight

Gratis kwetsbaarheidsscans van de website en extern zichtbare IT. Hiscox Cyber Insight analyseert de buitenkant van de IT-omgeving en brengt kwetsbaarheden helder in kaart. De klant ontvangt een beknopt rapport met concrete aanbevelingen.

Hiscox Cyber Maturity Model

Met deze volledige online evaluatietest kunnen bedrijven eenvoudig hun capaciteit meten om cyberrisico's te beheersen. Zo kunnen ze beter de sterktes en zwaktes van hun cyberbeveiliging begrijpen. Met behulp van mensen, processen en technologie worden zes belangrijke domeinen van cyberbeveiliging beoordeeld in een multidimensionale benadering. Dankzij het interactieve model van de tool kunnen bedrijven hun prestaties vergelijken met die van andere spelers. De tool geeft het bedrijf een score en legt daarnaast uit welke maatregelen cyberexperts kunnen nemen om de cyberweerbaarheid te verbeteren.

Hiscox Cyber Health Check

Met deze snelle tool hoeft u slechts 7 vragen over cyberbeveiliging te beantwoorden om het risiconiveau van uw klant te kennen: laag, gemiddeld of hoog. Gebruik de tool om een eerste gesprek met uw klant aan te gaan over het belang van goede praktijken voor cyberbeveiliging.

Norton Small Business bij CyberClear Premium

Cyberbeveiligingsoplossing speciaal ontwikkeld voor kleine bedrijven, die helpt apparaten en gegevens beter te beveiligen tegen bedreigingen zoals virussen, malware en phishing. Met als belangrijkste functies:

- ✓ device security: antivirus en firewall;
- ✓ gratis cloud backup: herstel bij ransomware of dataverlies;
- ✓ gratis VPN: veilige verbindingen, ook op publieke netwerken;
- ✓ software updater: signaleert verouderde software en updates;
- ✓ password manager: veilig wachtwoordbeheer;
- ✓ business customer support: ondersteuning bij vragen over de beveiligingssoftware;
- ✓ business tech support: hulp bij algemene IT-problemen;
- ✓ monitoring van financiële en social media-accounts.

Per klant kunnen tot 20 apparaten worden beschermd.

Aanvullende waarborg: vaste dagelijkse voorschotvergoeding

Kmo's met een jaaromzet tot 2,5 miljoen euro ontvangen een vaste dagelijkse voorschotvergoeding gedurende maximaal 30 dagen, uitbetaald zonder te wachten op de beoordeling van de werkelijke schade. Deze onmiddellijke financiële steun stelt u in staat snel dringende kosten op te vangen en uw activiteiten voort te zetten.

Nadien worden de reële verliezen opnieuw geëvalueerd, zonder bijpremie. U wordt dan vergoed voor het exacte bedrag van uw schade, zonder het verzekerde plafond te overschrijden. Zo hebt u de zekerheid dat u correct wordt begeleid, in overeenstemming met uw werkelijke behoeften.

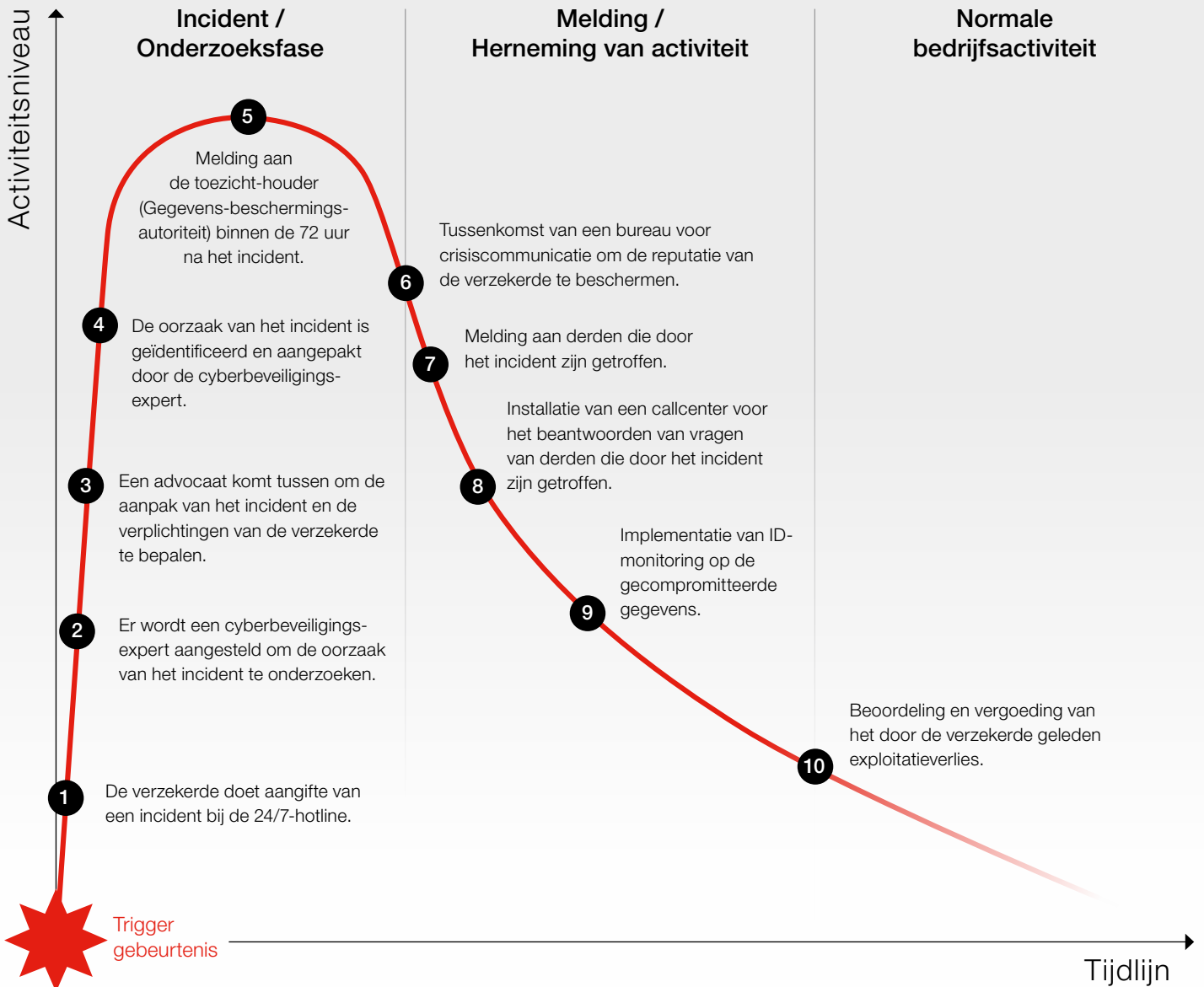
Wat we voor uw klanten doen **bij een crisis**

Zodra zich een crisis voordoet, nemen we voor uw klanten het heft in handen. En voor een maximale efficiëntie wordt onze tussenkomst minutieus voorbereid om uw klanten te beschermen tot in het kleinste detail.



Hiscox regelt alles

Onze experts begeleiden u vanaf de aangifte van het cyberincident tot de oplossing ervan.



7 goede redenen om een CyberClear-verzekering van Hiscox aan uw klanten voor te stellen

- 1** **24/7-hotline:** wij bieden onze verzekerden bijstand ZONDER VRIJSTELLING om hen zo goed mogelijk te helpen tijdens een cyberincident, via hiscox.claims@hiscox.be en 0800 90255 (gratis nummer, alleen binnen België) of 078 059001 (nationaal tarief, bereikbaar binnen België en internationaal met landnummer +32)
- 2** **Eenvoud:** Een CyberClear-verzekering van Hiscox is gewoon ... duidelijk. U weet precies waarvoor uw klant verzekerd is.
- 3** **Toegang tot een netwerk met de beste experts uit de sector:** cyberbeveiligingsexperts, advocaten gespecialiseerd in gegevensbescherming, experts in crisisbeheer ...
- 4** **10 jaar ervaring** in cyberverzekeringen: we kennen ons vak!
- 5** **Toekomstgericht:** CyberClear by Hiscox dekt niet alleen de risico's die uw klanten vandaag lopen. Onze polissen zijn bijzonder uitgebreid en beschermen hen tegen digitale risico's, bedreigingen en aanvallen die criminelen in de komende jaren kunnen ontwikkelen.
- 6** **Meer dan 220.000 tevreden klanten** in Europa.
- 7** **Eenvoudige en snelle onderschrijving:** uw klant is binnen enkele minuten verzekerd, via een pre-priced proposal (PPP) of rechtstreeks via onze portal voor verzekeringsmakelaars.



Hun verhaal, onze tussenkomst

Ontdek aan de hand van deze vier voorbeelden hoe Hiscox tussenkomt en uw klanten uit de cybervalstrikken bevrijdt.

Een dure phishing-ervaring

Sector **Voedingsindustrie**

Omzet + € 40 mio

Kost van het schadegeval € 49.000

Een medewerker van een bedrijf in de voedings-industrie werd slachtoffer van phishing toen hij een valse e-mail ontving van een senior manager. In de mail werd hem gevraagd om € 49.000 over te maken naar een specifieke bankrekening. In de veronderstelling dat het om een authentiek verzoek ging, gaf de werknemer het geld vrij. Noch de bank van het bedrijf, noch de ontvangende bank, was in staat om het geld terug te vorderen. De e-mail in kwestie was eigenlijk afkomstig van een Gmail-account dat aangemaakt was om het echte adres van de manager na te bootsen.

Tussenkomst van Hiscox

Toen het bedrijf zich realiseerde wat er was gebeurd, belde het ons. We stuurden onmiddellijk een risico-expert en een bedrijf gespecialiseerd in cybersecurity om te bepalen of er een kwetsbaarheid was in de systemen van de verzekerde en of er persoonsgegevens gecompromitteerd waren. We hebben het verloren geld binnen een maand na de aangifte terugbetaald. In dit geval was er geen datalek en was er dus geen melding nodig. Als aanvullende garantie kan dekking tot 50.000 euro worden geboden voor verliezen bij verduistering van betalingen.

Een IT-bedrijf loopt in de val

Sector **Technologie**

Omzet + € 40 mio

Kost van het schadegeval € 70.000

Een technologiebedrijf merkte op dat er malware was geïnstalleerd op een van zijn servers.

Tussenkomst van Hiscox

We hebben onmiddellijk onze cyberbeveiligingsexpert ingeschakeld om de functies van de malware te analyseren en te onderzoeken hoe hij in de systemen van onze klant kon terechtkomen. De server bevatte een grote hoeveelheid persoonsgegevens. Daarom onderzochten we of er een belangrijke kwetsbaarheid was en of het risico bestond dat deze gegevens gecompromitteerd waren. Gezien de mogelijke gevolgen hebben we een expert op het gebied van gegevensbescherming gestuurd om toezicht te houden op het onderzoek. De analyse bevestigde dat de malware een mining-programma was, maar gelukkig zonder al te veel ernstige gevolgen: er werden geen andere datalekken vastgesteld.

Een gepeperde rekening voor het restaurant

Sector Horeca
Omzet € 0-10 mio
Kost van het schadegeval € 29.000

Een ransomware-aanval versleutelde het volledige informaticasysteem van een restaurant, waardoor zelfs hun fysieke kassa's werden aangetast en transacties onmogelijk werden.

Tussenkost van Hiscox

Nadat alle andere opties waren uitgeput, bleek het betalen van losgeld de meest effectieve manier te zijn om de systemen van het restaurant te herstellen. We hebben daarom de kosten van het losgeld gedragen, evenals de IT-kosten voor de decodering en het volledig herstellen van de systeemfuncties. We hebben ook onze expert gestuurd om mogelijke inbreuken op persoonsgegevens op te sporen. Naast deze kosten compenseerden we ook het door het restaurant geleden exploitatieverlies als gevolg van de tijdelijke onmogelijkheid om zijn activiteit uit te oefenen.

Pr-adviseurs en Bitcoins

Sector Marketing
Omzet € 0-1 mio
Kost van het schadegeval € 44.000

Een pr-bureau stelde vast dat er een probleem was met hun e-mails. De vaste IT-onderaannemer deed een onderzoek en oordeelde dat er waarschijnlijk kwaad opzet in het spel was. De verzekerde nam vervolgens contact met ons op en we stuurden onze cyber-beveiligingsexpert ter plaatse. Die bevestigde dat de verzekerde het slachtoffer was van een aanval. De computersystemen van het bedrijf waren besmet met een cryptojacking-programma dat bedoeld was voor bitcoin-mining.

Uit het onderzoek bleek ook dat de hackers die deze malware installeerden, in de systemen van de verzekerde waren binnengedrongen en mogelijk de integriteit van persoonsgegevens hadden bedreigd.

Tussenkost van Hiscox

Na onderzoek van de ernst van de inbraak, heeft onze IT-expert de malware verwijderd en de beveiligingsproblemen in de systemen verholpen.

We hebben ons gespecialiseerd advocatenkantoor gemachtigd om de klant te ondersteunen bij zijn meldingsverplichtingen en we hebben de meldingen gedaan aan de toezichthouders en aan de betrokken personen.

Veelgestelde vragen

Waarom een cyberverzekering afsluiten?

Uw klanten zijn hoogstwaarschijnlijk verzekerd tegen risico's zoals brand, overstroming en professionele nalatigheid, maar ze lopen net zo goed (en misschien meer) risico op een cyberaanval. Deze aanvallen kunnen leiden tot omzetverlies en reputatieschade, en tot aanzienlijke kosten om de aanval te beheersen en financiële sancties.

Dekken de beroepsverzekeringen deze risico's dan niet?

Nee. Standaard beroepsverzekeringen bieden geen volledige bescherming. Daarom hebben uw klanten een cyberverzekering nodig.

Uw klant denkt niet dat hij het doelwit is van hackers ...

Veel online criminaliteit is niet specifiek gericht op een bepaald bedrijf. De verantwoordelijken achter deze aanvallen gebruiken vaak tools om op internet op zoek te gaan naar kwetsbare systemen. Hackers zullen dan misbruik maken van deze kwetsbaarheid, ongeacht het slachtoffer dat erachter zit.

Uw klant heeft geen online activiteiten. Heeft deze verzekering voor hem nut?

Veel bedrijven beschouwen zichzelf als 'offline' en denken daarom dat ze geen cyberverzekering nodig hebben. Toch heeft onderzoek aangetoond dat 94% van de bedrijven vandaag de dag online diensten gebruiken: het verzenden van e-mails of online opzoeken door het personeel, het gebruik van bankdiensten of online aankoopplatforms bedoeld voor hun klanten... Zo zijn ze feitelijk blootgesteld aan cyberrisico's.

Uw klant beschikt niet over persoonsgegevens. Heeft hij deze verzekering dan toch nodig?

De definitie van persoonsgegevens in de zin van de AVG is zeer ruim. Ze omvat bijvoorbeeld ook professionele e-mailadressen. Uw klant moet ook rekening houden met de gegevens waarover hij beschikt van zijn leveranciers, van zijn medewerkers (in het verleden en het heden) en van sollicitanten. Bovendien hebben de meeste schadegevallen die we behandelen geen betrekking op inbreuken op persoonsgegevens, maar op exploitatieverliezen, datacorruptie of systeemstoringen. Dit zijn allemaal situaties waarmee uw klant te maken kan krijgen, ook al beschikt hij niet over veel persoonsgegevens.

Biedt deze verzekering uitsluitend bescherming tegen computeraanvallen?

Nee. Hoewel de meeste schadegevallen betrekking hebben op cybercriminaliteit, kunnen ook menselijke fouten aan de oorsprong liggen. Bijvoorbeeld: een e-mail die naar een verkeerde ontvanger gestuurd werd, een aktetas die in de trein vergeten werd of een systeem dat foutief geconfigureerd werd.

Wat onderscheidt een CyberClear-verzekering van andere cyberproducten op de markt?

Een CyberClear-verzekering is een complete oplossing voor cyberbescherming die uw klanten ondersteunt op technisch, juridisch, menselijk en financieel vlak... tijdens en na de crisis. Hiscox begeleidt uw klanten ook al in een vroeg stadium, met name door hun medewerkers op te leiden in cyberbeveiliging. De polis biedt uw klanten brede garanties tegen cyberrisico's en laat hen gedurende de looptijd van hun contract genieten van de expertise van een netwerk van experts.



Nog vragen?

Wij beantwoorden ze graag!

Contacteer ons:

+32 (0)2 788 26 00

hiscox.underwriting@hiscox.be

Ombudsman van de Verzekeringen:

De Meeûssquare 35, 1000 Brussel Tel. 00 32 (0) 25 47 58 71

E-mail info@ombudsman-insurance.be www.ombudsman-insurance.be

Hiscox SA:

Belgische bijkantoor, met maatschappelijke zetel te 1130 Brussel, Bourgetlaan 42 B8, is ingeschreven bij de Kruispuntbank van Ondernemingen onder het nummer 0683.642.934, en erkend door de Nationale Bank van België ("NBB" - de Berlaimontlaan 14, 1000 Brussel, België) onder nummer 3099; Hiscox SA is een Luxemburgse verzekeringsmaatschappij met maatschappelijke zetel te 35F, avenue John F. Kennedy, 1855 Luxemburg, Groothertogdom Luxemburg (Handels- en bedrijvenregister: B217018). Ze staat onder toezicht van het Commissariat aux Assurances ("CAA" - 7, boulevard Joseph II, 1840 Luxemburg, Groothertogdom Luxemburg).