[kop] Q&A: De meest gestelde vragen over de CyberClear by Hiscox verzekering

Vraagt uw klant zich af waarom hij een cybercrimeverzekering nodig heeft? Hieronder geven we antwoord op de meest gestelde vragen.

- **Heeft mijn bedrijf een cyber verzekering nodig?**
  Voor alle bedrijven die beschikken over klantgegevens en/of vertrouwelijke informatie is een cyberverzekering aan te bevelen. Een inbreuk kan elk bedrijf overkomen. Dit geldt voor zowel ZZP'ers, kleine, als grote bedrijven. Cyberrisico's nemen toe en steeds meer opdrachtgevers eisen een cyber verzekering. Het wordt echt een 'must have'-dekking. Hiscox biedt onvoorwaardelijke assistentie van ervaren security-professionals. Heeft u een inbreuk? Ervaren professionals helpen u om uw databases en websites te repareren, belanghebbenden de informeren en juridische kosten te beperken.

- **Ben ik al verzekerd tegen cybercrime?**
  Mogelijk heeft u al een zakelijke verzekering waarin cybercrime is opgenomen in de polis. Het is afhankelijk van de voorwaarden of deze verzekering u al voldoende beschermt tegen cybercrime. Wij raden u aan om contact op te nemen met uw verzekeringsadviseur om samen te kijken naar uw specifieke situatie. In de meeste gevallen is de dekking zeer beperkt en komt u slechts voor vergoeding van een gering bedrag in aanmerking. Het kan bijvoorbeeld zijn dat alleen de Third Party-kosten worden vergoed of dat de maximumdekking voor First Party-kosten beperkt is tot slechts € 50.000. Een complete cyber verzekering is profijtelijk voor elk bedrijf en biedt de geruststelling dat de kosten van een potentiële inbreuk geen ontwrichtende werking zullen hebben op de bedrijfsvoering.

- **Welke vormen van data vormen een risico?**
  De risico's betreffen in het algemeen de persoonsgegevens die bedrijven onder beheer hebben, zoals BSN-nummers, rijbewijsnummers, gegevens van betaalkaarten waarmee goederen, diensten en rekeningen worden betaald, gevoelige gegevens van klanten, verzamelde medische gegevens, enzovoort.

- **Als mijn werkelijke risico alleen First Party-gegevens betreft (zoals gegevens van werknemers), heb ik dan zo'n polis wel nodig?**
  Elk bedrijf heeft de taak en verplichting om namens werknemers beheerde gegevens te beschermen. Hetzelfde geldt voor vertrouwelijke gegevens van het bedrijf zelf. Geen enkel bedrijf is immuun tegen aanvallen. Een polis van Hiscox biedt dekking voor verlies of inbreuk op werknemersgegevens.

- **Ik ben geen doelwit zoals Sony, KPN of ASML. Waarom zou ik me zorgen maken?**
  Grote bedrijven halen het nieuws. Kleine niet. Niettemin, als het gaat om inbreuken op gegevens is het niet de vraag of het gebeurt, maar wanneer het gebeurt. Er bestaat een zwarte markt waar gestolen gegevens worden gekocht en verkocht. En hackers worden steeds slimmer. KPN, Sony, ASML en andere grote organisaties hebben complete afdelingen die zich bezighouden met het analyseren van de risico's waaraan het bedrijf is blootgesteld en die meewerken aan het opzetten van beleid en procedures waarmee ze zichzelf kunnen beschermen, maar hackers weten nog steeds gaten in de verdediging te slaan. Kleinere bedrijven die geen netwerkbeveiligers in dienst hebben en niet de middelen hebben om hun gegevens te beschermen, zijn voor hackers een gemakkelijke prooi.

- **Waarom zou ik twijfelen aan mijn IT-afdeling als ze zeggen dat ze al hun zaakjes op orde hebben?**
  ASML, Sony en andere grote bedrijven hebben complete afdelingen die zich bezighouden met IT-beveiliging, maar ze bleken kwetsbaarder dan ze dachten. Eén simpele fout of vergissing,

zoals het niet updaten van software, het niet instellen van de juiste procedures voor authenticatie van leveranciers, of het kwijtraken van een niet-versleutelde laptop waarop gevoelige gegevens zijn opgeslagen, kan al leiden tot een inbreuk. De risico's groeien mee met de technologische ontwikkelingen en hackers gaat steeds slimmer en geraffineerder te werk.

- **Wat zijn de gemiddelde kosten van een gegevensinbreuk?**
  Onder de Nederlandse bedrijven die in 2019 door cybercrime zijn getroffen was de schade gemiddeld €67.000,-. Hoe groter het bedrijf, des te hoger de kosten. Maar ongeacht de grootte van het bedrijf geldt: hoe meer gevoelige gegevens het bedrijf verzamelt, des te hoger de kosten.

- **Ik heb maar een heel klein bedrijf. Hoeveel gaat cybercrime mij kosten en is een verzekering het dan wel waard?**
  Elk bedrijf is blootgesteld aan privacy-risico's, hetzij via gevoelige gegevens van werknemers, hetzij via betalingen die van derden worden geïnd, geleverde diensten enz. Sommige risico's zijn groter dan andere, maar het is belangrijk om te benadrukken dat elk bedrijf met werknemers in dienst aansprakelijk is voor verlies van Third Party-gegevens (met inbegrip van gegevens van werknemers). In 2019 kostte cybercrime het kleinste bedrijf met de geringste risico's gemiddeld ruim €38.000,-. De kosten stapelen zich razendsnel op.

- **Heb ik deze dekking wel nodig als ik gegevens van klanten niet opsla op mijn netwerk?**
  Ja. U slaat klantgegevens weliswaar niet op, maar u hebt wel toegang tot deze gegevens. Uzelf kunt ook de oorzaak zijn van een inbreuk op gegevens van uw klanten. Inbreuk op privacy en eventuele aansprakelijkheid geldt ook voor gegevens en tegenover werknemers.

- **De verwerking van betaalkaarttransacties besteed ik uit aan een derde. Op dat gebied loop ik dus geen risico, klopt dat?**
  Volgens de PCI Compliance Guide, geldt de PCIstandaard voor ALLE organisaties of handelaren, ongeacht de omvang van of het aantal transacties, die gegevens van kaarthouders accepteren, doorgeven of opslaan. En het simpele feit van uitbesteding aan een derde partij ontslaat u niet van de plicht te voldoen aan de PCI-voorschriften. Misschien kunt u zo het risico verminderen en daarmee de PCI-compliance wat vergemakkelijken, maar dat betekent nog niet dat er volledig aan PCI voorbij kan worden gegaan.

- **Als mijn klantgegevens zijn opgeslagen in de cloud berust de aansprakelijkheid toch bij de cloudaanbieder?**
  Dat is niet zeker. Het is in het belang van de verzekerde om contracten op dit gebied zorgvuldig door te spreken met een juridisch adviseur. Zelfs als het risico beperkt is, kan het nog steeds dat de aansprakelijkheid bij de verzekerde wordt gelegd.

- **Dekt een cyberverzekeringspolis het rechtstreeks verlies van gelden?**
  De meeste cyberverzekeringspolissen zijn bedoeld om de schade door verlies van gegevens, niet van gelden (rechtstreeks) te dekken. Bij Hiscox kunnen we voor bepaalde risico's de dekking uitbreiden. Onze polis tegen cybercriminaliteit biedt dekking tegen inbreuken op gegevens. Tot een bepaald bedrag bent u verzekerd tegen het verlies van geld of frauduleuze handelingen.

- **Biedt de polis dekking tegen 'social engineering'?**
  Social engineering is een methode om personen door misleiding beveiligde gegevens afhandig te maken. Slachtoffers van social engineering zijn kwetsbaar door hun ingeboren aard om anderen te vertrouwen en te willen helpen. De meeste verzekeringspolissen dekken verlies van gegevens ongeacht de grondslag van het verlies, al moet wel goed worden gekeken wat de polis hier precies over zegt. Social engineering is een onderdeel van de dekking.

- **Dekt de polis ook gegevensverlies veroorzaakt door malafide medewerkers?**
  De meeste verzekeringspolissen dekken de kosten van gegevensverlies ongeacht de wijze waarop het verlies zijn beslag heeft gekregen. Er zijn echter ook polissen die gegevensinbreuken veroorzaakt door malafide medewerkers uitsluiten. De dekking van de verzekeringspolissen van Hiscox tegen standaardinbreuken op gegevens door malafide medewerkers is overeenkomstig de voorwaarden van de polis, maar bepaalde situaties waarbij leidinggevend personeel van de organisatie betrokken is, kunnen in de polis zijn uitgesloten.

- **Biedt de polis ook dekking tegen offlinerisico's?**
  Zowel digitale als papieren gegevens vallen onder de verzekering.

- **Is er wereldwijde dekking?**
  Wereldwijde dekking is mogelijk bij ons. Onze jurisdictie beperkt zich tot het juridisch rechtsgebied zoals vermeld op de polis.

- **Van welke diensten kan ik als verzekerde gebruik maken om mijn risico verder te beperken?**
  Als verzekerde kunt u gebruik maken van de services die wij u aanbieden in samenwerking met onze partners. ICTRecht stelt gratis een verwerkersovereenkomst op maat voor u op. Ook heeft u recht op een gratis proefperiode van SIDN CyberSterk, waarbij u inzicht krijgt in de kwetsbaarheden van uw bedrijfsnetwerk en websites en maatregelen kunt nemen om het risico op datalekken te verminderen. Met Hiscox' CyberClear Academy leren uw medewerkers de werkwijze van de cybercrimineel herkennen. Zeker bij cybercrime draait risicobeheersing om bewustwording.