Wat kan er zoal mis gaan?

Een retailbedrijf constateert verdachte activiteiten op zijn webservers en komt er achter dat iemand op de bedrijfssystemen heeft ingebroken en betaalkaartgegevens van klanten heeft gestolen.

De eerste prioriteit van het bedrijf is het inschakelen van een IT-onderzoeksbureau om het lek te dichten, vast te stellen wat er precies is gebeurd en te achterhalen wiens gegevens gestolen zijn. Vanwege de strikte termijnen voor het indienen van rapportages aan het College Bescherming Persoonsgegevens (CBP) en de betaalkaartbedrijven (PCI-sector) schakelt het retailbedrijf ook een vakdeskundige jurist in die deze stukken opstelt.

Het inschakelen van juristen en forensisch deskundigen gebeurt pas na een advies van College Bescherming Persoonsgegevens (CBP) om de personen van wie gegevens zijn gestolen, daarvan op de hoogte te stellen. Het onderzoeksteam zoekt de contactgegevens bij elkaar en de juristen stellen de brieven op. Het retailbedrijf doet vervolgens honderdduizenden brieven op de bus, verwacht dat veel klanten bezorgd zullen zijn en schakelt een ander deskundig bedrijf in om een callcenter op te zetten en vragen van klanten op te vangen. Het retailbedrijf staat bekend als klantvriendelijke dienstverlener. Om deze reputatie in stand te houden wil het bedrijf de betaaltransacties/kredieten laten bewaken van iedereen die als gevolg van de systeeminbraak schade dreigt te ondervinden en neemt daartoe een vierde bedrijf in de arm.

Bovengenoemd praktijkvoorbeeld is een typisch voorbeeld van een situatie waarvoor onze **Kosten Inbreuk Module** is bedoeld. Maar eenzelfde opeenvolging van gebeurtenissen is ook mogelijk bij verlies van een laptop, mobiele telefoon, USB-stick, een papieren dossier of een andere gegevensdrager waarop gevoelige persoonsgegevens zijn opgeslagen.

De kosten van verweer ingeval van een nader onderzoek door CBP, de PCI-sector of een schadeclaim van een individuele particulier vallen dan onder de **Privacy Protectie Module**. Dit geldt ook voor vorderingen wegens wanprestatie en bepaalde civielrechtelijke boetes.

Wanneer door het hacken tevens schade is ontstaan aan het netwerk van het retailbedrijf of online inkomsten zijn gederfd, dan treden de **Hacker Schade- en Cyber Business Interruption Modules** in werking en heeft het retailbedrijf recht op vergoeding van de gederfde inkomsten en van de kosten van herstel van de systemen.

Informatie

In deze brochure is ons Data Risks by Hiscox verzekeringspakket slechts beknopt samengevat. Voor meer informatie en een offerte kunt u contact opnemen met uw verzekeringsadviseur of bezoek onze website www.hiscox.nl.

Hiscox specialismen in het kort

- bestuurders- en commissarissen aansprakelijkheidsverzekeringen (D&O)
- beroepsaansprakelijkheidsverzekeringen voor diverse beroepsgroepen
- exclusieve opstal- en inboedelverzekeringen voor vermogende particulieren
- opstal- en inboedelverzekeringen voor vakantiewoningen
- specialistische kunst- en kostbaarhedenverzekeringen
- ontvoering- en losgeldverzekeringen (K&R).

HISCOX

Gelderlandplein, 75APostbus 87033, 1080 JA Amsterdam
T +31 (0)20 517 07 00
F 31 (0)20 517 07 01
E hiscox.underwriting@hiscox.nl
I www.hiscox.nl

Hiscox is geregistreerd bij de Autoriteit Financiële Markten onder nummer 12039295.

8588 08/11

WIE KIJKT NAAR UW DATA WANNEER U NIET KIJKT?

HISCOX

Een gerichte (computer) hack of het verlies van een laptop kan grote gevolgen hebben. Denk maar aan verlies van klantinformatie of personeelsgegevens, het in verkeerde handen komen van betaalkaartgegevens, schade aan uw netwerk of derving van online inkomsten en reputatieschade. Of het nu gaat om de kosten die u maakt ingeval van diefstal van gegevens of voor het voeren van verweer in verband met de content op uw website, de Data Risks by Hiscox verzekering biedt optimale bescherming tegen alle data- en online risico's die u loopt.

Hiscox. Verzekerd als geen ander…

Als specialistische verzekeraar voor de zakelijke verzekeringsmarkt onderkent Hiscox het belang van helder communiceren en van een snelle en flexibele manier van werken. Al meer dan 10 jaar bieden wij specialistische cyberverzekeringen aan, waardoor wij in staat zijn u een optimale dekking te bieden. Naast een uitgebreide standaard dekking biedt Hiscox daarom ook:

- zes keuzemodules; u kunt zelf een verzekeringspakket samenstellen dat aansluit op uw bedrijfsactiviteiten
- een wereldwijd netwerk van privacyjuristen en technische (en ICT) deskundigen; u bent dus verzekerd van de beste ondersteuning, ongeacht waar en wanneer u ons nodig heeft
- gratis toegang tot onze internationale portal met informatie over en ondersteuning bij gegevensbeveiliging (Hiscox eRisk Hub™)
- dekking voor inbreuken die veroorzaakt worden door derden die door u zijn ingeschakeld.

Schadefilosofie

Bij schade merkt u pas hoe belangrijk het is om goed verzekerd te zijn. De schadeservice van Hiscox is daarom het belangrijkste aspect van onze dienstverlening. Wanneer u geconfronteerd wordt met een schadeclaim garanderen wij een voorspoedige en deskundige afhandeling. Daarnaast houden onze schadebehandelaars rekening met uw reputatie. Waar andere verzekeraars bij een schadeclaim direct op zoek gaan naar uitsluitingen, is bij Hiscox dekking het uitgangspunt.

Dekkingskenmerken

U heeft de keuze uit zes op elkaar afgestemde modules. Dit geeft u de flexibiliteit om zelf een Data Risks by Hiscox verzekeringspakket samen te stellen die het beste aansluit bij uw onderneming. Hieronder volgt een overzicht van de dekkingskenmerken van de twee hoofdmodules en een korte beschrijving van de andere modules:

Kosten Inbreuk Module

- **Forensisch onderzoek:** wij vergoeden de kosten om uit te zoeken wat er mis is gegaan en om uit te zoeken wiens gegevens in gevaar zijn gebracht.
- **Melding van inbreuk**: wij vergoeden de kosten die u maakt voor het opstellen en versturen van brieven aan gedupeerde betrokkenen, particulieren, betaalkaartbedrijven en toezichthouders.
- **Klantenservice**: wij vergoeden de kosten van het opzetten van een callcenter voor informatievoorziening of servicediensten voor het laten bewaken van de betaalkaarttransacties (kredieten) van gedupeerde betrokkenen.
- **Public relations**: als u ondersteuning nodig heeft bij het herstellen van uw reputatie, kunnen de kosten van een PR-specialist hiervoor voor vergoeding in aanmerking komen.

Privacy Protectie Module

- **Kosten van verweer**: het voeren van verweer tijdens onderzoek door een toezichthouder of betaalkaartbedrijf of een schadeclaim van een individuele particulier is een kostbare zaak. Wij vergoeden de door u gemaakte kosten van verweer en hanteren daarbij geen maximum uurtarief voor juridische bijstand.
- **Boete/schadevergoeding**: naast de kosten van juridische bijstand komen ook civielrechtelijke boetes die door de toezichthouder worden opgelegd (voor zover toegestaan) en de eventuele schade waar men toe veroordeeld is voor vergoeding in aanmerking.
- **Aanspraken door derden**: we vergoeden de kosten van verweer en de kosten voor afhandeling van aanspraken die u op grond van het niet afdoende beveiligen van uw data dient te voldoen.
- **Aanspraken van toezichthouders**: het is vaak een prijzige aangelegenheid om verweer te voeren ten overstaan van onderzoeken door toezichthouders of door de Payment Card Industry Security Standards Council. We vergoeden de kosten van verweer en hanteren daarbij geen maximum uurtarief voor juridische bijstand. Voor zover is toegestaan, vergoeden we ook civielrechtelijke boetes en andere vormen van schadevergoeding die door toezichthouders worden opgelegd.

Cyber Aansprakelijkheid Module

Websitecontent of de inhoud van een e-mail aan een klant kan snel verkeerd worden opgevat of zelfs onbedoeld inbreuk op iemands auteursrechten opleveren. Wanneer u voor de Cyber Aansprakelijkheid Module kiest, helpen wij u bij het afhandelen van schadeclaims die voortvloeien uit de content van uw website en e-mails.

Hacker Schade Module

Ingeval van schade aan uw website, programma's of elektronische gegevens of ingeval van diefstal van een programma of elektronische gegevens door een hacker, heeft u op grond van de Hacker Schade Module recht op vergoeding van de kosten voor herstel of vervanging. Verder regelen wij een beveiligingsexpert die uw systemen naloopt en forensisch onderzoek verricht om de identiteit van de hacker te achterhalen en kunnen wij bovendien een PR-specialist voor u inschakelen.

Cyber Afpersing Module

Een schade onstaat niet alleen wanneer een hacker op uw website en in de beveiliging van gegevens inbreekt. U kunt ook worden gechanteerd met het dreigement dat er op uw systemen zal worden ingebroken als er niet aan bepaalde eisen wordt voldaan. Wanneer u kiest voor de Cyber Afpersing Module schakelen wij een erkend beveiligingsadviesbedrijf in (NetDiligence) om u bij te staan en vergoeden wij ook het bedrag aan losgeld dat u uiteindelijk heeft betaald om de schade voor uw onderneming zo beperkt mogelijk te houden.

Cyber Business Interruption Module

Wat zijn de gevolgen voor u wanneer een hacker, concurrent of andere derde het op uw computersystemen gemunt heeft en verhindert dat u online inkomsten genereert? De inkomsten die u in dat geval misloopt, worden op basis van de Cyber Business Interruption Module door ons vergoed.