meijers
zeker verder

Q&A

Cyberverzekering

De cyberverzekering uitgelegd

Het cyberrisico staat in de top 3 van bedrijfsrisico's. Bedrijven moeten daar dus iets mee. Vooral het MKB is het meest voorkomende doelwit van cyberaanvallen. Voor deze bedrijven is het dus extra aantrekkelijk om een cyberverzekering aan te schaffen. Goed risicomanagement vraagt om meer dan alleen een cyberverzekering. Het gaat om de juiste mix van verzekeringen op het gebied van fraude, cyber, bestuurdersaansprakelijkheid en beroepsaansprakelijkheid. Natuurlijk is ook preventie essentieel. In deze Q&A leest u wat een cyberverzekering is en wat dit inhoudt.

Wat vergoedt een cyberverzekering?

Een cyberverzekering vergoedt uw eigen bedrijfsschade, schade bij derden waarvoor u wettelijk aansprakelijk wordt gesteld en de kosten van onderzoek, verweer en herstel. Daarnaast krijgt u direct toegang tot diverse expertbureaus als het misgaat. Denk aan digitaal forensische onderzoekers, juridische ondersteuning en communicatiestrategen om bijvoorbeeld reputatieschade tegen te gaan.

Wat zijn de meest gangbare dekkingen van een cyberverzekering?

- Eigen bedrijfsschade in de vorm van winstderving. Deze bedrijfsschade moet gelinkt zijn aan een cyberincident, maar hoeft niet digitaal van aard te zijn.
- Wettelijke aansprakelijkheid voor schades van derden zoals gelekte persoonsgegevens
- Kosten van onderzoek, verweer, woordvoeringstrategie en herstel.
- Losgeld (soms alleen deels).
- Boetes van bijvoorbeeld de Autoriteit Persoonsgegevens.
- Bewaking van identiteitsfraude en kredietmonitoring na een datalek.

Wat zijn de meest gangbare uitsluitingen?

- Contractuele aansprakelijkheden.
- Fraude (meestal CEO fraude en/of Business Email Compromise), opzet, grove nalatigheid.
- Inbreuk op patenten in media-uitingen.
- Personenschade.
- Materiele schade.

Steeds vaker worden cyberincidenten die het gevolg zijn van kritieke kwetsbaarheden in software, beperkt of uitgesloten van dekking. De reden hiervoor is dat verzekeraars zelf failliet kunnen gaan als ze dit soort veelvoorkomende incidenten verzekeren.

Waarin verschillen verzekeraars?

Een aantal voorbeelden:

- Het wel of niet (geheel) verzekeren van IT-storingen, menselijke fouten, voorraadschade, personenschade en hacks op IT-providers.
- De minimale en maximale tijdsduur waarin gedekte eigen bedrijfsschade is geleden.
- Extra's zoals dekkingen voor het uitloven van een beloning voor de gouden tip die leidt naar een crimineel of een verbeteringsbudget voor upgrades van software en hardware.
- Ook leveren sommige verzekeraars kortingen op preventieve maatregelen en diensten.

Krijg ik toegang tot respons experts die meteen dienstverlening bieden?

Ja. Bijna alle verzekeraars stellen een alarmnummer beschikbaar dat u 24/7 kunt bellen bij een incident. Ook staan gespecialiseerde bedrijven op het gebied van digitaal forensisch onderzoek, juridische bijstand en communicatiestrategie voor u klaar. De kosten hiervan zijn gedekt.

Hoe bepaalt een verzekeraar de premie?

De belangrijkste indicatoren voor een verzekeraar zijn:

- De aard en de digitale weerbaarheid van uw sector en de mate van cyberdreiging daarin
- Uw jaaromzet
- De gevoeligheid en omvang van de informatie in uw bedrijf
- Uw bestaande privacy- en security maatregelen

Kan ik bij elke verzekeraar terecht voor een cyberverzekering?

Verzekeraars zijn kritisch op de risico's die zij accepteren en daarom kunt u niet altijd bij elke verzekeraar terecht. Met vragenformulieren en soms zelfs een interview willen ze een gevoel te krijgen bij het risiconiveau van uw bedrijf. Sommige verzekeraars verzekeren alleen bedrijven uit bepaalde sectoren. Anderen kiezen bijvoorbeeld een doelgroep op basis van hun jaaromzet.

Is het afsluiten van een cyberverzekering onderdeel van behoorlijk bestuur?

Ja en nee. Als bestuurder kunt u aansprakelijk worden gesteld. Bijvoorbeeld voor het niet goed naleven van de AVG. Of het onvoldoende beschermen van de organisatie tegen een ernstig cyberincident. Ons advies is dat er ten minste één grondige analyse moet zijn uitgevoerd of het wel of niet (deels) verzekeren tegen cyberincidenten verstandig of nodig is.

Veelvoorkomende misvattingen

Ik ben niet aansprakelijk als mijn IT provider gehackt wordt

Degene die besluit om informatie te verzamelen en te (laten) verwerken is altijd juridisch aansprakelijk voor de vertrouwelijkheid, beschikbaarheid en correctheid ervan. Als u ervoor kiest om dat te laten doen door externe partijen, bent u nog steeds aansprakelijk.

Ik kan mijn bedrijfsschade verhalen op mijn IT provider

Soms kan dit tot een beperkte hoogte, maar meestal helemaal niet. Slaat u de Service Level Agreement (SLA) met uw IT providers er maar op na en zoek naar de Aansprakelijkheidsparagraaf.

Ik ben niet interessant voor hackers

Deze bewering is zelden waar. Als gegevens voor bedrijven belangrijk zijn, dan zijn ze per definitie ook interessant voor hackers. De kans is groot dat bedrijven willen betalen voor het vrijgeven van vastgezette data of het voorkomen van openbaring. Dit noemen we ransomware. Daarbij zijn veel aanvallen ongericht, waardoor iedereen een potentieel doelwit is. Binnen bepaalde sectoren geldt dat de data zelf al waarde hebben. Data als persoonsgegevens en medische dossiers zijn bijvoorbeeld interessant om identiteitsfraude mee te plegen.

Wij hebben onze beveiliging op orde

Zelfs professionele Cloud- en IT-providers erkennen dat ook zij gehackt kunnen worden. Maar wanneer u afhankelijk bent van mensen kunnen er altijd fouten worden gemaakt. Phishing-linkjes in e-mails, verkeerde bijlagen openen of informatie sturen naar een verkeerd e-mailadres kan voor cybercriminelen net die opening zijn om in het bedrijfsnetwerk in te breken. Ook zien we steeds vaker dat software van derden die je gebruikt en vertrouwt kwetsbaar is. U kunt een cyberverzekering vergelijken met een brandverzekering. Ondanks blusinstallaties, sprinklers en brandwerend materiaal blijft er altijd risico op een brand. Daarom hebben bedrijven met uitstekende brandpreventie daarnaast een brandverzekering.

Wij kunnen prima een tijdje zonder ICT

Er zijn weinig bedrijfsprocessen onafhankelijk van communicatie en informatie. Communicatie verloopt vaak via het internet. Denk aan e-mail, IP-telefonie en videobellen. Ook informatie slaan we digitaal op. Zonder communicatie en informatie liggen bijna alle bedrijfsprocessen stil. Probeer maar eens voor te stellen hoe een week zonder e-mail, toegang tot bestanden en telefonie eruit ziet.

Ik kan zelf opdraaien voor de schade en kosten van een cyberincident

Dat is mogelijk. De vraag is wat eigenlijk de schade en kosten zijn? De praktijk wijst uit dat het gevraagde losgeld bij een ransomware-aanval ongeveer 2% bedraagt van uw jaaromzet . Tel daarbij op de mogelijke winstderving, loonkosten, onderzoek, communicatie- en herstelkosten, kosten van verweer, boetes en aansprakelijkheden. Weet u zeker dat u alles wilt of kunt dragen?

Wat de situatie ook is, verzekeraars keren toch niet uit

Cyberincidenten zijn juridisch lastig specifiek te definiëren en dus wordt er in de verzekeringsvoorwaarden bijna altijd een zeer ruime definitie gekozen zoals ‘elke ongeoorloofde toegang’. Een datalek als gevolg van het verlies van een laptop valt bijvoorbeeld ook onder die definitie. In de praktijk zien we daarom zelden discussie over de aard van een incident en of dat wel of niet gedekt is.

Mijn bedrijfs- of beroepsaansprakelijkheidsverzekering dekt cyberincidenten

Het is ongebruikelijker dat een cyberincident gedekt wordt op een traditionele aansprakelijkheidsverzekering. Weet u zeker of dat in uw geval ook zo is?

We moeten eerst de preventie op orde hebben voordat we een cyberverzekering afsluiten

Tijdens het op orde krijgen van de cybersecurity is het risico het hoogst. Daarom adviseren wij altijd om de verzekering direct af te sluiten op het moment dat de al geïmplementeerde maatregelen voldoende zijn om geaccepteerd te worden door een verzekeraar. Meijers heeft ook partners om uw bedrijf direct veiliger te maken waardoor het afsluiten van een cyberverzekering bijna altijd mogelijk is.

Wij kunnen prima zelf reageren op een cyberincident

In de praktijk is vaak een combinatie nodig van externe experts, uw IT provider(s) en uw eigen organisatie. Denk aan iemand die onderhandelt met de hackers. Een partij die digitaal forensisch onderzoek doet. Of juridische bijstand levert. Een cyberverzekeraar kan dit allemaal faciliteren. Inclusief de kosten. Los hiervan adviseren wij altijd om een aantal plannen klaar te hebben liggen. In het bedrijfscontinuïteitsplan staat hoe de bedrijfsvoering voortgezet wordt tijdens een cyberincident. Het incident respons plan helpt om regie te houden op het incident. Een herstelplan is er om software en data weer aan de praat te krijgen na een incident.

Heeft u vragen?

Neem contact op met Tom Rijgersberg via t.rijgersberg@meijers.nl of bel 06 386 756 13.
Meer informatie vindt u op onze cyberpagina.

meijers
makelaars in assurantiën

Van Heuven
Goedhartlaan 935
1181 LD Amstelveen
Postbus 707
1180 AS Amstelveen
(020) 642 05 24