

Cybersecurity-verzekeringen: waar moet je rekening mee houden?

Een cybersecurity-verzekering kan ondernemers helpen beschermen tegen financiële schade en reputatieschade na een cyberaanval. Maar hoe kies je een polis die bij jouw bedrijf past?

Het is tegenwoordig steeds belangrijker om te zorgen voor een goede beveiliging van digitale systemen en gegevens.

Cyberaanvallen en het lekken van gevoelige informatie kunnen ernstige gevolgen hebben voor bedrijven, zoals financiële verliezen, reputatieschade en zelfs boetes als gevolg van het overtreden van wet- en regelgeving op het gebied van gegevensbescherming. Een cybersecurity-verzekering kan bedrijven helpen bij het afdekken van de kosten die zijn gemoeid met het herstellen van schade die is veroorzaakt door een cyberaanval of het lekken van gevoelige informatie. Bovendien kan het bedrijven ook helpen bij het naleven van wet- en regelgeving en het voorkomen van reputatieschade. Kortom, een cybersecurity-verzekering kan een waardevolle aanvulling zijn op een bedrijfsbeveiligingsstrategie en kan bedrijven helpen bij het beschermen tegen de financiële en reputatiegevolgen van cyberaanvallen.

Bij het kiezen van een cybersecurity-verzekering zijn er een aantal zaken waarmee je rekening moet houden om ervoor te zorgen dat je een verzekering kiest die bij jouw behoeften en situatie past. In dit artikel stippen we een paar belangrijke zaken aan.

Wat precies dekt de verzekering?

Kijk naar de dekking van de verzekering. Het is belangrijk om te weten wat precies is gedekt, zodat je weet wat je kunt verwachten in het geval van een cybersecurity-incident.

Cybersecurity-verzekeringen beschermen tegen de financiële en reputatiegevolgen van cyberaanvallen en het lekken van gevoelige informatie. Maar wat is precies de dekking van zo'n verzekering en waar moet je op letten bij het kiezen ervan?

In het algemeen bieden cybersecurity-verzekeringen dekking voor schade die is veroorzaakt door cyberaanvallen, zoals het stelen of onbruikbaar maken van gegevens. Dit kan bijvoorbeeld het geval zijn als er ransomware op je systemen is geïnstalleerd of als er sprake is van een phishing-aanval waarbij medewerkers of klanten zijn opgelicht. Kijk naar de lijst van cyber-incidenten die gedekt zijn door de verzekering en zorg dat deze overeen komen met jouw behoeften. Soms zijn er bepaalde uitzonderingen op de dekking van een verzekering, zoals bepaalde soorten cyber-incidenten die niet gedekt zijn. Zorg dat je deze uitzonderingen begrijpt en dat ze voor jou acceptabel zijn.

Sommige verzekeringen bieden ook dekking voor schade die is veroorzaakt door menselijke fouten, zoals het per ongeluk versturen van gevoelige informatie aan de verkeerde persoon. Andere verzekeringen kunnen ook dekking bieden voor de kosten die zijn gemoeid met het naleven van wet- en regelgeving op het gebied van gegevensbescherming, zoals het opstellen van privacybeleid of het trainen van medewerkers.

Bij het kiezen van een cybersecurity-verzekering is het belangrijk om goed na te denken over welke soorten risico's je bedrijf loopt en welke soorten dekking je nodig hebt om deze risico's af te dekken. Het kan bijvoorbeeld nuttig zijn om te kiezen voor een verzekering met een brede dekking die schade afdekt die is veroorzaakt door zowel cyberaanvallen als menselijke fouten.

Er zijn vaak limieten aan de dekking van een verzekering, zoals een maximum bedrag dat uitgekeerd kan worden. Kijk naar deze limieten en zorg dat ze voldoende zijn voor jouw situatie. Bedenk ook of je eventueel extra dekking wilt afsluiten om deze limieten te verhogen.

Heeft de maatschappij ervaring met cybersecurity-incidenten?

Vraag naar de ervaring van de verzekeringsmaatschappij met cybersecurity-incidenten. Het is belangrijk om te weten hoe ervaren de verzekeringsmaatschappij is op het gebied van het afhandelen van cybersecurity-incidenten en hoe ze hiermee omgaan.

Een verzekeringsmaatschappij met veel ervaring op het gebied van cybersecurity zal in staat zijn om je te helpen met het beoordelen van jouw risico's en het bieden van advies over hoe je je bedrijf kan beschermen tegen cyberaanvallen. Ze zullen ook bekend zijn met de laatste trends en ontwikkelingen op het gebied van cybersecurity, wat betekent dat ze in staat zullen zijn om jou de beste dekking te bieden voor jouw specifieke situatie.

Een verzekeringsmaatschappij met weinig ervaring op het gebied van cybersecurity kan misschien goedkoper zijn, maar het is belangrijk om te overwegen of dit op lange termijn wel de juiste beslissing is. Als jouw bedrijf het slachtoffer wordt van een cyberaanval, zal je willen dat je verzekeringsmaatschappij je kan helpen bij het herstellen van de schade en het terugwinnen van de verloren gegevens. Als je verzekeraar niet bekend is met de specifieke uitdagingen die cybersecurity met zich meebrengt, kan dit betekenen dat ze niet in staat zullen zijn om jou adequaat te helpen bij het omgaan met de gevolgen van een aanval.

Verzekeringsmaatschappijen met veel ervaring zijn vaak beter in staat om te begrijpen wat er nodig is om bedrijven te beschermen tegen cyberrisico's. Ze hebben waarschijnlijk al eerder met veel verschillende soorten cyberaanvallen te maken gehad en weten

daarom hoe ze de juiste dekking kunnen bieden om bedrijven te beschermen tegen deze risico's. Bovendien hebben verzekeringsmaatschappijen met veel ervaring vaak ook een uitgebreid netwerk van experts en partners die kunnen helpen bij het beheren van cyberrisico's.

Hoe gaat de maatschappij om met claims?

Vraag na hoe de verzekering zal omgaan met claims. Zo hoef je je geen zorgen te maken over hoe je een claim kan indienen wanneer dat nodig blijkt.

Een goede verzekering zal je snel en efficiënt helpen als je te maken krijgt met een cyberaanval, zodat je je bedrijf zo snel mogelijk weer op de rails kunt krijgen. Bij het kiezen van een cybersecurity-verzekering is het daarom belangrijk om na te gaan hoe het claimsproces van de verzekering in zijn werk gaat. Als een verzekeraar bijvoorbeeld een moeilijk of onredelijk claimsproces heeft, kan dit betekenen dat je veel tijd en moeite moet steken in het indienen van een claim en dat je misschien zelfs geen vergoeding krijgt als je recht hebt op een uitkering.

Zorg ervoor dat het claimsproces helder en eenvoudig is, zodat je snel hulp kan krijgen als je die nodig hebt. Kijk bijvoorbeeld of er een speciaal team is dat zich bezighoudt met het afhandelen van cyberclaims, en of er duidelijke richtlijnen zijn voor het indienen van een claim.

Hou ook rekening met de soorten vergoedingen die worden aangeboden door de verzekering. Sommige verzekeringen bieden alleen financiële vergoedingen voor verlies, terwijl andere ook diensten aanbieden zoals hulp bij het herstellen van gegevens of het terugwinnen van toegang tot je systemen. Kies een verzekering die de juiste mix van vergoedingen en diensten biedt om je te helpen bij het herstellen van je bedrijf na een cyberaanval.

Vraag advies voor een betere bescherming

Een cybersecurity-verzekering kan advies en ondersteuning bieden om je bedrijf te beschermen tegen cyberrisico's. Zo kan je efficiënt reageren op een aanval en de schade beperken.

Een van de belangrijkste diensten die een cybersecurity-verzekering kan aanbieden is advies over hoe je je bedrijf kan beveiligen tegen cyberaanvallen. Dit kan bijvoorbeeld advies zijn over hoe je je wachtwoorden kan beveiligen, hoe je phishing-scams kan voorkomen en hoe je kan voorkomen dat je gegevens gestolen worden. Door dit soort advies te volgen, kan je de kans op een cyberaanval verkleinen en je bedrijf beter beschermen. Als je een cybersecurity-verzekering afsluit, kan je vaak ook gebruikmaken van diensten zoals beveiligingsonderzoek en incident response planning. Dit zijn diensten die je helpen om je bedrijf beter te beschermen tegen cyberaanvallen en om snel te kunnen reageren als er iets misgaat. Bijvoorbeeld, beveiligingsonderzoek kan je helpen om zwakke punten in jouw systeem te identificeren en maatregelen te nemen om deze te versterken. Incident response planning kan je helpen om een plan te maken voor wat te doen als jouw bedrijf te maken krijgt met een cyberaanval, zodat je snel en efficiënt kan reageren. Door een verzekering af te sluiten die deze diensten aanbiedt, kan je ervoor zorgen dat je bedrijf beter is voorbereid op cyberaanvallen.

Daarnaast kan een cybersecurity-verzekering ook ondersteuning bieden als je te maken krijgt met een cyberaanval. Als je een claim indient bij jouw verzekering, kan de verzekering je helpen om jouw bedrijf te herstellen na een aanval. Dit kan bijvoorbeeld betekenen dat de verzekering externe experts inschakelt om je te helpen bij het herstellen van gegevens of het terugwinnen van toegang tot jouw systemen. Zo kan een incidentresponse-team samengesteld worden dat kan helpen bij het herstellen van bedrijfsprocessen na een aanval, of een team van juridische experts die kunnen helpen bij het afhandelen van claims en andere zaken. Dit kan je helpen om

snel en efficiënt te reageren op een aanval en om de schade te beperken.

Welke kosten zijn er?

Hou rekening met de kosten die gepaard gaan met een cybersecurity-verzekering. Zo kom je niet voor onverwachte kosten te staan.

Zoals met elke verzekering, zijn de premies voor cybersecurity-verzekeringen afhankelijk van verschillende factoren. Voordat je een cybersecurity-verzekering afsluit, is het daarom verstandig om verschillende verzekeraars, premies en dekkingen te vergelijken om erachter te komen wat het beste bij je bedrijf past. Het kan ook nuttig zijn om advies te vragen aan een verzekeringsmakelaar die je kan helpen bij het maken van een weloverwogen keuze.

Er zijn verschillende kosten waarmee je rekening moet houden bij het afsluiten van een cybersecurity-verzekering. Ten eerste moet je ervoor betalen om de verzekering af te sluiten. Dit is de premie die je betaalt om dekking te krijgen voor cyberrisico's. De hoogte van de premie is afhankelijk van verschillende factoren, zoals de grootte van jouw bedrijf, de sector waarin jouw bedrijf actief is, en de specifieke dekking die je afsluit.

Daarnaast moet je ook rekening houden met eigen risico's. Bijna alle verzekeringen hebben een eigen risico, wat betekent dat je een bepaald bedrag zelf moet betalen als je een claim indient.

Tot slot moet je ook rekening houden met eventuele extra kosten die samenhangen met de verzekering. Dit kan bijvoorbeeld in de vorm zijn van advies- of consultancykosten, of kosten voor het inschakelen van een incidentresponse-team na een aanval. Het is belangrijk om de voorwaarden van de verzekering zorgvuldig te lezen om te weten wat wel en niet gedekt is, zodat je niet voor onverwachte kosten komt te staan.

Auteur: Pieter Philippaerts, DistriNet, KU Leuven

Publicatiedatum: 23 januari 2023