Cyber
Weerbaarheidscentrum
Greenport

Cyberverzekeringen

Daar waar in de maatschappij risico's ontstaan, zullen na verloop van tijd verzekeraars producten ontwikkelen die bepaalde risico's afdekken. De maatschappelijke ontwikkeling van digitalisering en de daarbij horende weerbaarheid van bedrijven, is daar geen uitzondering op. Daarom zie je de laatste jaren meer verzekeraars cyberverzekeringen aanbieden. Hoe weet je nu of een cyberverzekering voor jou als ondernemer nuttig of van meerwaarde is? Of welke verzekering voor jou geschikt is? Hieronder vind je een aantal vragen en antwoorden die je kunnen helpen en noemen we een aantal concrete stappen die je kunt zetten als je nadenkt over een cyberverzekering.

Wat is een cyberverzekering?

Er bestaat niet één uniforme definitie van de term cyberverzekering. Een verzekering is in de basis een betaling van een premie van een ondernemer aan een verzekeraar waarbij het risico van de ondernemer overgaat naar de verzekeraar. Een cyberverzekering is een verzekering die de directe of indirecte schade kan dekken die je oploopt in, aan of door digitale componenten van je onderneming. Denk hierbij aan het slachtoffer worden van gijzelsoftware of diefstal van bedrijfs- of klantinformatie. Het lastige is dat verzekeraars diverse definities hanteren. Het is dus goed om te weten dat per verzekeraar de dekking, de service en de premie kan verschillen.

Waarom een cyberverzekering?

Of je een cyberverzekering nodig hebt, begint bij het belang dat je wilt beschermen. Ook moet je jezelf afvragen of en in welke mate je al verzekerd bent via andere verzekeringen. In de polisvoorwaarden van je bestaande verzekeringen zou je moeten kunnen terugvinden of schade in, aan of door digitale systemen wordt gedekt. De meerwaarde van een verzekering zal groter worden als je afhankelijk bent van digitale systemen en de informatie in die systemen voor jouw bedrijfsvoering. Andere redenen voor het afsluiten van een cyberverzekering kunnen zijn dat afnemers of leveranciers van jouw bedrijf dit vragen, omdat je verhoogd risico loopt door de producten of diensten die je verkoopt, of omdat je specifieke kennis hebt (intellectueel eigendom zoals ontwerpen).
De basisvraag is daarom: welke risico's wil je verzekeren? De risico's die je met name wil verzekeren zijn de risico's die een hoge impact hebben maar niet vaak voorkomen. In de fysieke wereld kun je daarbij denken aan brand of diefstal. Een brand of diefstal komen, normaal gesproken, niet vaak voor. Maar als het een keer gebeurt, dan lopen de kosten vaak snel op. Weeg dus altijd af of je zelf het risico kunt dragen, of dat je dit niet kunt (of wilt). In dat laatste geval kan een cyberverzekering voor jouw bedrijf een meerwaarde hebben.

Wat wordt er gedekt door een cyberverzekering?

De gevolgen van een cyberincident kunnen verschillende vormen aannemen. Zoals gezegd, is het belangrijk om na te gaan wat je wilt verzekeren en welk risico je kunt en wilt dragen. De kosten van een incident kunnen snel oplopen.

Een cyberverzekering kan dekking verlenen voor:

- **Directe kosten** van een cyberincident: o.a. het repareren of vervangen van hard en software, het herstellen van data, terugvinden van informatie en opnieuw opbouwen van de administratie. Onder directe kosten kan het inhuren van specialisten voor het herstel, verlies van (productie)uren of omzet;
- **Indirecte kosten**: o.a. reputatieschade, boetes van toezichthouders (bijvoorbeeld AVG boetes), schadevergoedingen aan gedupeerden.

Ook kunnen verzekeraars diensten aanbieden die gerelateerd zijn aan cyberincidenten, zoals:

- **Bewustwording, kennis en kunde** van de ondernemer of personeel (bijvoorbeeld ondersteund met online trainingen);
- **Incidentondersteuning** (bijvoorbeeld een 24/7 alarmcentrale en technische ondersteuning);
- **Juridische ondersteuning** (bijvoorbeeld bij datalekken in het kader van de AVG);
- **Forensische diensten** (het uitzoeken wie er achter een aanval zit).

Als laatste wordt er in de markt van cyberverzekeringen gesproken over de mate van veiligheid van een verzekerde. Om in aanmerking te komen voor een verzekering zijn er verzekeraars die eerst van je willen weten of je beveiligingsmaatregelen neemt. Soms vragen verzekeraars of je voor je bedrijf een risicoscan wil uitvoeren. Ook kan het zijn dat een verzekeraar bepaalde instellingen vereist zoals het hebben van een virusscanner of firewall. Of deze eisen gesteld worden verschilt per verzekeraar en zal onderdeel zijn van de polisvoorwaarden. Als je een certificeringstraject hebt doorlopen op informatiebeveiliging, dan kan het regelen van een cyberverzekering gemakkelijker verlopen.

Dit document is gebaseerd op het document 'Cyberverzekeringen'' van het Digital Trust Center. Het originele document is te vinden via https://www.digitaltrustcenter.nl/informatie-advies/cyberverzekeringen