Doorzicht is een publicatie van Van Luin, in samenwerking met VLC & Partners waarin specialisten actuele ontwikkelingen met u delen. Bij vragen kunt u altijd contact opnemen met uw contactpersoon.

Doorzicht

September 2022

Ontwikkelingen in de markt voor cyberverzekeringen

Cyberincidenten zijn aan de orde van de dag. Dagelijks lezen we over grote datalekken, ransomware betalingen, en onderzoeken en boetes vanuit toezichthouders zoals de Autoriteit Persoonsgegevens. Naast het feit dat cybercriminelen steeds actiever worden, zijn ze ook steeds creatiever en professioneler. Daardoor wordt het steeds moeilijker om ze buiten de deur te houden. We schetsen kort de ontwikkelingen in de markt van cyberverzekeringen.

Cyberverzekering

Een cyberverzekering vergoedt de financiële schade die een bedrijf lijdt als gevolg van een digitaal risico, ook wel een cyberincident genoemd. Een vergoeding onder een cyberverzekering kunnen we op hoofdlijnen indelen in drie categorieën:

- Incident response diensten. Denk hierbij aan toegang tot cyberincident-responsediensten zoals ICT-forensisch onderzoek. Public relations ter bescherming van het imago, notificatiekosten om klanten te informeren over een cyberincident en juridische diensten om bijvoorbeeld te voldoen aan de AVG.
- Eigen schade. Dit zijn bijvoorbeeld kosten van de response diensten die na de eerste periode worden gemaakt: reconstructiekosten van data, schade door bedrijfsstilstand en afpersingskosten (waaronder vaak ook losgeld).
- Aansprakelijkheid. Hieronder vallen schadevergoeding en juridische bijstand bij aanspraken van derden en onderzoek door de Autoriteit Persoonsgegevens. En bij boetes bij overtreding van de privacyregels (AVG), als de vergoeding van deze boetes wettelijk is toegestaan.

Een jaar of vijf geleden werd het cyberrisico nog maar incidenteel verzekerd. Inmiddels zien we dat deze verzekering steeds meer in het verzekeringspakket zit en aan relevantie heeft gewonnen.

Aantal cyberaanvallen en gemiddelde schade door cyberaanvallen blijven toenemen

Als we kijken naar de afgelopen jaren, zien we dat er weer sprake is van een aanhoudende significante stijging van het aantal cyberaanvallen en de schade die daarbij hoort. Onze wereld wordt simpelweg steeds afhankelijker van digitale technologieën. Denk alleen al aan de nieuwe manier van werken zoals die tijdens en na de coronapandemie verder is ontwikkeld. Deze digitalisering biedt volop kansen en mogelijkheden. We zijn voor ons werk bijvoorbeeld niet meer afhankelijk van plaats en tijd. Maar het brengt ook nieuwe risico's met zich mee.

Door de sterk stijgende schadelast hebben verzekeraars, met name in 2021 en in de eerste helft van 2022 fors ingegrepen met premiestijgingen, verhoging van de eigen risico's en beperkingen van de dekking. Ook is er veel meer aandacht gekomen voor de weerbaarheid van een organisatie bij de acceptatie van nieuwe aanvragen en verlenging van bestaande polissen. Deze verharding van de cyberverzekeringsmarkt zal ook in de tweede helft van 2022 en in 2023 aanhouden.

Verder zien we een wereldwijde discussie ontstaan over het wel of niet vergoeden van losgeldbetalingen en boetes. De landelijke en internationale politiek willen het betalen van losgeld demotiveren. Dit kan gevolgen hebben voor de dekking van dit specifieke cyberrisico. Daarnaast zien we dat de ransomware dekking ook beperkt wordt door de steeds verdere uitbreiding van internationale sanctiewet- en regelgeving. Denk bijvoorbeeld aan hackers met Russische banden die op een sanctielijst staan. In zo'n geval mag een verzekeraar niet betalen.

Focus op cyberweerbaarheid met de cyberverzekering als sluitstuk

De acceptatiecriteria om in aanmerking te komen voor een cyberverzekering kunt u als basismaatregelen zien om uw organisatie weerbaarder te maken tegen een cyberaanval. Zaken die u anno 2022 minimaal op orde moet hebben, zijn onder andere:

- Implementatie van Multi-Factor Authentication (MFA)
- het regelmatig maken van back-ups en het beschermen en testen daarvan
- regelmatig installeren van software updates
- actief patchbeleid voor kritische updates
- het versleutelen van gevoelige informatie
- training of phishing-simulaties om bewustwording van het cyberrisico's bij personeel te vergroten.

Voor de grotere organisaties is het goed om ook een cyberincident response plan te hebben en dit regelmatig te testen.

Al enige tijd besteedt ook de overheid aandacht aan cyber security. En geeft zij handreikingen om de Nederlandse samenleving weerbaarder te maken. Dat doet het ministerie van Justitie en Veiligheid via het Nationaal Cyber Security Centrum. Daarnaast kunt u inzicht krijgen in de risicoklasse waarin uw organisatie valt. Dat kan via het Digital Trust Center van het ministerie van Economische Zaken en Klimaat. Aan de hand van 11 vragen ziet u welke maatregelen u kunt nemen om de digitale beveiliging te verbeteren. Helaas geven deze maatregelen geen 100% zekerheid tegen cyberincidenten. De cyberverzekering blijft daarom als sluitstuk van belang om tot een gedegen vorm van risicomanagement te komen.

Helaas bestaat 100% garantie tegen cyberincidenten niet. Het is dus van groot belang dat uw preventiemaatregelen op niveau blijven. En dat u een goede cyberverzekering heeft om de continuïteit van uw bedrijf te waarborgen

Meer weten?

Heeft u nog vragen over uw verzekering of -risico?
Neem dan contact op met ons:

Sylvia van den Bos

sylvia@vanluin.nl
tel:0302326323
0646384513

Robert Havekotte

robert@vanluin.nl
tel:0302326323
06-29052077

Peter van der Steeg

Peter.vanderSteeg@vanluin.nl
tel:0302326323
06-13826790

WWW.VANLUIN.NL