Verzekeringen voor de gevolgen van cybercrime

RendementOnline

Door redactie FA Rendement

3 september 2021 | 5 minuten

De kans dat uw organisatie slachtoffer wordt van een of andere vorm van cybercriminaliteit is de afgelopen jaren flink toegenomen. Er komen ook steeds nieuwe bedreigingen bij. Denk bijvoorbeeld aan datagijzeling via ransomware, waarmee onlangs zelfs een gerenommeerd instituut als de Universiteit Maastricht te maken kreeg. Is het mogelijk om zulke risico's of de schade via een cybercrimeverzekering af te dekken?

Verzekeraars hebben voor vrijwel alle risico's wel een product met polis op de plank liggen. Dus ook voor de risico's die u als organisatie loopt bij een digitaal incident. Dat ligt tegenwoordig zowat overal op de loer. Denk aan besmettingen met malware of aan hacking waarbij gegevens verloren gaan of gestolen worden.

De laatste tijd is daar ook nog gijzeling met ransomware bijgekomen. Dit is eigenlijk een combinatie van hacking en malware. Cybercriminelen dringen door tot uw systeem om daar alle gegevens zodanig te versleutelen dat u er niet meer bij kunt. Vervolgens kunt u door betaling van losgeld de sleutel krijgen om de data weer toegankelijk te maken.

Een cyberaanval veroorzaakt downtime

Deze listige criminele procedure kan enorme schade veroorzaken: van het ene op het andere moment kunt u uw werk niet meer uitvoeren. Uw organisatie heeft niet alle gegevens beschikbaar over klanten of relaties en het antwoord op hun vragen moet u schuldig blijven.

Anders gezegd: een aanval met malware of ransomware veroorzaakt 'downtime', oftewel een onderbreking in de continuïteit van het werk, en onbeschikbaarheid van de bedrijfsdata. Dat heeft niet alleen gevolgen voor uw organisatie, maar ook voor de gehele relatieketen die daaraan gekoppeld is. Om van de privacyaspecten nog maar te zwijgen.

> **Er kunnen er heel wat kosten opdoemen naar aanleiding van een cyberincident**

Losgeld voor uw data

Als uw organisatie het slachtoffer wordt van een gijzeling, is het losgeld dat u moet betalen niet het enige probleem. Nog afgezien van het feit of u dat wel zou moeten doen en of u er wel de data mee terugkrijgt, sommige digitale gijzelnemers nemen niet eens de moeite om na het ontvangen van het losgeld de sleutels beschikbaar te stellen. Er zijn dan ook heel wat organisaties die uit principe niet onderhandelen met afpersers, en dus ook digitale gijzelnemers nooit losgeld zouden betalen.

Zo'n houding kan alleen maar succesvol zijn als u voldoende maatregelen heeft getroffen om zo snel mogelijk de downtime te beëindigen. Dat kan bijvoorbeeld door adequate, up-to-date en veilige back-ups klaar te hebben staan, die u direct op nieuwe machines in een verse ICT-infrastructuur kunt plaatsen.

Een loffelijk streven, maar dan nog kunnen er heel wat indirecte gevolgen en kosten opdoemen naar aanleiding van het cyberincident. Twee of meer dagen downtime is gebruikelijk, en in sommige gevallen loopt het zelfs op tot meer dan tien dagen.

Immense gevolgen en kosten bij cyberincident

Het is nauwelijks te berekenen wat voor (financiële) schadepost downtime kan opleveren. Terwijl er tegelijkertijd ook nog de noodzaak kan zijn om machines of de complete infrastructuur te vervangen naar aanleiding van het incident. En wat dacht u van het inhuren van specialisten en adviseurs om de situatie onder controle te krijgen?

Bijkomende gevolgen – die bovendien nog veel later aan het licht kunnen komen – zijn de eventuele aansprakelijkheid of schadeclaims die relaties kunnen neerleggen bij uw organisatie. Of het misbruik dat de cybercriminelen van de gegijzelde of gestolen data kunnen maken. Vergeet ook de reputatieschade niet waar u als getroffen organisatie last van kunt krijgen.

Lang verhaal kort: een cyberincident kan immense gevolgen hebben, enorme schade berokkenen en veel onverwachte kosten met zich meebrengen.

> **Verzekeraars kunnen de reddingsboei zijn bij een cyberincident**

Verzeker gevolgen cyberincident

Terug naar de verzekeraars. Zij kunnen de reddingsboei zijn als uw organisatie dreigt te verdrinken als gevolg van een cyberincident. Er zijn diverse partijen die verzekeringsproducten aanbieden tegen cybercrime. In onze Marktanalyse cybercrimeverzekeringen vindt u enkele aanbieders met hun producten en de zaken die zij afdekken.

Ondanks de afspraak in de verzekeringswereld om verzekeringen via overzichtelijke kaarten in beeld te brengen, blijft het lastig om de producten met elkaar te vergelijken. Wat bij de een als vanzelfsprekend meeverzekerd is, kan bij een andere partij juist zijn uitgezonderd. Daarom eerst even de overeenkomsten:

- Meestal is de productomschrijving iets in de trant van ‘Verzekering tegen de (financiële) gevolgen van hacking, systeeminbraak, verlies of diefstal van data, en aanvallen door cybercriminelen’.
- Vrijwel alle producten vergoeden de kosten voor inhuur van technische of juridische specialisten en voor crisis- en incidentmanagers.
- Opzet, fraude of ondeskundig gebruik is in vrijwel alle polissen en voorwaarden reden om niet uit te keren. In sommige producten zijn zelfs expliciete preventieafspraken geformuleerd.
- De verzekering betreft vrijwel altijd alleen de gegevens, niet de schade aan apparatuur of het letsel van mensen.
- De meeste producten gelden wereldwijd, vaak wel met uitzondering van aansprakelijkheid voor schade in, of volgens het recht van de VS of Canada. Ook kunnen in de polis andere dekkingsafspraken zijn opgenomen.
- Verschillen zijn er natuurlijk ook. Bij sommige verzekeraars is bijvoorbeeld ook de schade meeverzekerd die door fouten van programmeurs of gebruikers zijn ontstaan.

Daarnaast heeft alles zijn prijs, ook verzekeringen. Dus wat kost nu zo’n verzekering tegen cyberincidenten? Dat is van een aantal zaken afhankelijk, zoals het (maximaal) afgesproken verzekerde bedrag per geval, de vorm of hoogte van het eigen risico, de volledigheid van de soorten

incidenten die worden gedekt en de grootte van uw organisatie.

Bij sommige verzekeringsproducten zijn bepaalde incidentsoorten ondergebracht in een aanvullende verzekering. Zo zijn de kosten bij een hackincident met de telefooncentrale bij de meeste producten inclusief, maar bij Interpolis is dat een aanvullende module.

Pech voor erotische sector

Soms zijn bepaalde typen bedrijven uitgesloten van een cybercrimeverzekering. Denk bijvoorbeeld aan providers, financiële dienstverleners, sociale media of aanbieders van ‘adult entertainment’.

Cybercrimeverzekeringen lastig te vergelijken

Bij het vergelijken van offertes voor eenzelfde soort uitgangssituatie blijken de premies elkaar niet al te veel te ontlopen. Maar zoals vaak met verzekeringsproducten, is het behoorlijk lastig vergelijken.

Het liefst wil uw organisatie voor de meest volledige dekking met een zo laag mogelijke premie gaan. Niet onverstandig dus om de volledigheid van de dekking van verschillende verzekeringsproducten nauwkeurig te bestuderen alvorens een keuze te maken.

Let bijvoorbeeld ook goed op of het maximale verzekerde bedrag per gebeurtenis of per verzekeringsjaar geldt. Dat is namelijk niet bij alle verzekeraars hetzelfde. Vraag vooral ook offertes op bij de diverse aanbieders en bestudeer hun polisvoorwaarden aandachtig.

Dit is een artikel van de redactie van FA Rendement

FA Rendement is dé informatiebron voor administrateurs, boekhouders, controllers en andere financiële professionals. Wat is er veranderd op het gebied van financieel-administratieve wet- en regelgeving, en hoe kunt u als specialist deze informatie direct in uw dagelijkse werk toepassen? Daarnaast moet u op de hoogte zijn van onder meer de fiscaliteit, automatisering, de loon- en salarisadministratie, sociale voorzieningen, debiteurenbeheer en inkoop.

De onafhankelijke en ervaren redactie van FA Rendement zit bovenop het nieuws en vertelt u als eerste wat de ontwikkelingen zijn. Altijd in heldere taal en met een praktische insteek, zodat u de informatie direct kunt vertalen naar uw eigen werksituatie. FA Rendement is daarnaast multimediaal. De voor uw vakgebied relevante informatie verschijnt:

- ✓ dagelijks op het digitale platform Rendement Online, waar u onder meer het laatste nieuws, checklists, rekentools, maatwerkbrieven en verdiepingsartikelen tot uw beschikking heeft;
- ✓ wekelijks gebundeld in een e-mailnieuwsbrief;
- ✓ maandelijks in het vakblad FA Rendement, boordevol nieuws en achtergrondartikelen, digitaal en op de mat;
- ✓ tweemaandelijks in een handzaam themadossier: een pocketboekje dat iedere editie een complex onderwerp uitdiept.