VERDIEPEND ARTIKEL

Cyberrisico's voor particulieren en bedrijven: hoe te verzekeren?

SEPTEMBER 2021

In onze samenleving maken we steeds vaker gebruik van de vele en steeds verdergaande mogelijkheden van automatisering en digitalisering. Dit maakt veel aspecten van ons leven een stuk gemakkelijker, maar brengt ook nieuwe risico's met zich mee: de zogenaamde cyberrisico's. Van schade-adviseurs mag worden verwacht dat zij deze risico's (samen met alle andere soorten risico's) opnemen in de inventarisatie, de risico's en in het advies.

In dit artikel nemen we jou als adviseur mee in wat het cyberrisico inhoudt, wat de mogelijke gevolgen zijn, hoe schade door cyberincidenten zo goed mogelijk kan worden voorkomen en wat de verzekeringsmogelijkheden zijn.

Het cyberrisico

Een cyberrisico is een incident dat zich kan voordoen bij het gebruik van computer- en datanetwerksystemen, waarbij schade kan ontstaan bij gebruiker(s) en/of derden. We geven drie korte voorbeelden:

- Een medewerker stuurt per ongeluk een e-mail met privacygevoelige informatie naar een verkeerd e-mailadres.
- Een kwaadwillende (hacker of cybercrimineel) dringt van buitenaf binnen in een computersysteem.
- De computer crasht als gevolg van kortsluiting in de computer zelf of door een stroomstoring van buitenaf.

De aard en de omvang van de schade als gevolg een cyberincident is afhankelijk van een groot aantal factoren en verschilt per incident en gebruiker.

Als een e-mail met persoonsgevoelige informatie naar een verkeerd e-mailadres wordt gestuurd, is de gevolgschade (privacyschending van één persoon) wellicht minder groot dan wanneer een hacker binnendringt in een computer en het hele systeem versleutelt, waardoor niemand het systeem meer kan gebruiken. In dit laatste geval eist de hacker vaak losgeld, in ruil voor het weer vrijgeven van het systeem.

Hoe langer het systeem onbruikbaar is, des te groter de bedrijfsschade als gevolg van de bedrijfsstilstand. De gebruiker moet (laten) onderzoeken wat de hacker in het systeem heeft gedaan én wat de gevolgen zijn voor de gebruiker(s) enerzijds en voor de personen wiens gegevens in het systeem zijn opgeslagen anderzijds. Als de hacker gegevens misbruikt, openbaar maakt of gebruikt voor identiteitsfraude, is de schade nóg groter. Als een bedrijfssysteem is gehackt, moet het bedrijf dit namelijk melden bij de Autoriteit Persoonsgegevens (AP) en bij de personen wiens gegevens mogelijk of zeker werden misbruikt. In dat melden zit veel kostbare tijd.

Praktijkvoorbeelden

De verhalen van gedupeerden van cyberincidenten, bieden goede handvatten om cyberrisico's (en de gevolgen daarvan) met klanten te bespreken. Een paar voorbeelden:

- In 2015 werd het systeem van een ontwerp-, foto- en filmbedrijf in Goes gehackt. De hacker heeft alles vernietigd dat in de systemen was opgeslagen. Dit heeft geleid tot het faillissement van het bedrijf en van de eigenaar privé.
- In 2019 werd een garagebedrijf in Zutphen slachtoffer van cybercriminaliteit. De schade bedroeg volgens de eigenaar ruim € 50.000.
- In augustus 2019 werd het computersysteem van een Noord-Hollandse kraanverhuurder gehackt. De eigenaar dacht dat iemand een grap met hem uithaalde, tot deze 'grap' hem € 35.000 kostte.
- In april 2021 werd logistiekbedrijf Bakker gehackt. De kaaslevering aan Albert Heijn stagneerde, waardoor deze hack de 'kaashack' werd genoemd.

Voorkomen is beter dan genezen

Wie een computer- en datanetwerksysteem gebruikt, loopt het risico om schade te lijden door een cyberincident. De kans op een dergelijk incident is zelfs vele malen groter dan de kans dat er brand uitbreekt. Gebruikers zijn zich nauwelijks tot niet bewust van de cyberrisico's en de mogelijke gevolgen. Daardoor is er té weinig aandacht voor gedegen beveiliging. Cybercriminelen maken daar op hun beurt weer dankbaar misbruik van.

Ook maken cybercriminelen gebruik van de onwetendheid en de naïviteit van de mens tijdens hun computergebruik. Ze sturen niet van echt te onderscheiden e-mailberichten waarin ze zich voordoen

als een collega, om iemand op die manier op een link te laten klikken, een bijlage te laten openen of een (grote) som geld over te maken.

Door jouw klanten bewust te maken van de mogelijke risico's en ze mee te nemen in hoe ze schade kunnen voorkomen, krijgen cybercriminelen minder kans om toe te slaan.

Handige websites met meer informatie over (simpele) beveiligingsmogelijkheden

- Op www.veiliginternetten.nl staan laagdrempelige tips voor particulieren en bedrijven om veiliger gebruik te maken van digitale systemen en internet.

- Op de website van het Digital trust center (van het ministerie van Economische Zaken en Klimaat) staat een tool voor mkb-bedrijven om eenvoudig, online en anoniem cyberrisico's inzichtelijk te maken.

Verzekeren van cyberrisico's

De meeste bezits- en aansprakelijkheidsverzekeringen bieden géén dekking voor de financiële gevolgen van cyberincidenten. Een speciale cyberverzekering doet dit echter wel: voor schade die de verzekerde zelf lijdt, voor de bijkomende kosten én voor schade aan derden waarvoor de verzekerde aansprakelijk is.

Er zijn verschillende verzekeraars die cyberverzekeringen aanbieden, voor zowel bedrijven als particulieren. Iedere aanbieder hanteert eigen acceptatievoorwaarden. Veelvoorkomende acceptatievoorwaarden zijn:

- Dat bepaalde soorten bedrijven niet kunnen worden verzekerd (zoals bedrijven in de seksindustrie of bedrijven die spelcomputers maken);
- Dat de klant op eigen kosten of op kosten van verzekeraar een risicoscan moet laten uitvoeren; en
- Dat er bepaalde preventiemaatregelen getroffen moeten worden. Denk aan het verplichten van een bepaalde virusscanner *inclusief* onderhoudscontract.

De dekking van de diverse cyberverzekeringen verschilt per verzekeraar. Over het algemeen bieden cyberverzekeraars dekking voor schade als gevolg van cyberincidenten:

1. *Die de verzekerde zelf lijdt, zoals:*
   - Kosten voor onderzoek naar de oorzaak van de schade.
   - Bedrijfsschade als gevolg van het niet gebruiken van het systeem.
   - Meldingskosten van het cyberincident bij de AP en klanten.
   - Betaalde losgelden en boetes (een verzekeraar vergoedt meestal alleen als er vóór de betaling is overlegd met de verzekeraar).
   - Reputatie- en imagoschade.

2. *Die anderen/derden lijden en waarvoor de verzekerde aansprakelijk is, zoals wanneer:*
    - De opgeslagen persoonsgegevens van een klant worden gestolen en er identiteitsfraude mee wordt gepleegd.
    - De privacy van de klant aantoonbaar is aangetast.

Wat onder een cyberincident wordt verstaan, verschilt per verzekeraar. Vaak is er alleen dekking als er sprake is van een cyberaanval door kwaadwillende personen van buitenaf.

De premies van de cyberverzekering verschillen ook per verzekeraar. Voor particulieren is de premie afhankelijk van de hoogte van het te verzekeren bedrag. Deze bedraagt gemiddeld € 10 tot € 15 per maand. De premie van de bedrijven en organisaties wordt vastgesteld aan de hand van de aard van het bedrijf, de omzet en de verzekerde bedragen.

Tot slot

De kans op een cyberincident is vele malen groter dan dat er brand ontstaat. Een cyberverzekering mag en kan niet meer ontbreken in een verzekeringspakket. Het inzichtelijk maken van cyberrisico's en het geven van advies over cyberverzekeringen is nieuw en niet eenvoudig, maar het is wél noodzakelijk dat een schadeadviseur dat doet, in het kader van de zorgplicht.

Over de auteur

Dit artikel is geschreven door Anita Hol-Bubeck, docent en auteur op het gebied van schadeverzekeringen.

Anita verzorgt in samenwerking met Bureau DFO BV webinars en workshops. Ook schreef zij een uitgebreide vaknotitie over dit onderwerp.