Cyber's frequently asked questions

Veelgestelde vragen over cyberveiligheid en -verzekeringen

Omdat cyberrisico's, en verzekeringen om deze risico's af te dekken, relatief nieuw zijn, zien we dat er nog veel vragen bestaan bij onze klanten. We hebben daarom een aantal veelvoorkomende vragen onder elkaar gezet. Zo krijgt u een beter beeld van het hoe en waarom van een cyberverzekering. Uiteraard kunt u altijd contact met ons opnemen indien u meer vragen heeft of advies wilt inwinnen.

Wat is een cyberverzekering?

De cyberverzekering verzekert, naast de aansprakelijkheid van een onderneming voor door derden geleden schade (inclusief daaruit voortvloeiende gevolgschade), tevens de eigen kosten naar aanleiding van een digitaal risico. Deze risico's kunnen bestaan uit het verloren gaan van gegevens door hacking, maar ook verlies of diefstal van bijvoorbeeld laptops, tablets of usb-sticks.

'Omdat cyberrisico's en verzekeringen om deze risico's af te dekken relatief nieuw zijn, hebben wij een aantal veelvoorkomende vragen beantwoord.'

Dekking cyberverzekering

- aansprakelijkheid voor door derden geleden schades;
- verdedigings- en verweerkosten voor de aansprakelijkheid bij tekortkoming van goed beheer van privacydata en andere digitale risico's;
- onderzoekskosten;
- kosten voor public relations consultancy ter bescherming van het imago;
- klantnotificatiekosten;
- kredietbewakingskosten;
- boetes die door de overheid worden opgelegd (mits wettelijk toegestaan);
- reconstructiekosten van de data;
- cyberdiefstal, ransomware;
- bedrijfsstilstand als gevolg van digitale risico's (optioneel).

Beperkingen en uitsluitingen

- contractuele aansprakelijkheid;
- fraude, opzet;
- schade die leidt tot voordeel van verzekerde;
- bedrijfsactiviteiten als kansspelen, gaming, social media en pornografie;
- schade aan illegaal verkregen data;
- personenschade en zaakschade.

>>

Nut en noodzaak

Is een cyberverzekering zinvol voor mijn organisatie?

Dekking tegen cyberrisico's is van meerwaarde voor elke onderneming die beschikt over vertrouwelijke informatie en/of klantgegevens. Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG, ook wel General Data Protection Regulation (GDPR)) van kracht. Deze Europese privacywetgeving stelt o.a. eisen aan het veilig bewaren van gegevens. Hierdoor lopen bedrijven een aanmerkelijk aansprakelijkheidsrisico. Naast het aansprakelijkheidsrisico voor schade aan derden, kan ook de schade die bedrijven zelf lijden door cybercriminaliteit, systeemfalen en menselijk handelen desastreus zijn. Diefstal of verlies van gevoelige informatie over klanten of werknemers kan iedere onderneming overkomen. Het verlies van één laptop kan al tot ernstige financiële gevolgen en reputatieschade leiden. Een cyberverzekering voorziet daarbij niet alleen in een financiële tegemoetkoming, ook de 'incident response'-diensten worden gedekt.

Is de aansprakelijkheid voor cyberincidenten (bijv. datalekken) verzekerd onder algemene aansprakelijkheidsverzekeringen?

Traditionele aansprakelijkheidsverzekeringen bieden zelden dekking voor aansprakelijkheid naar aanleiding van cyberincidenten. In de regel bieden algemene aansprakelijkheidsverzekeringen alleen dekking in geval van letsel of fysieke schade. Uw cyberverzekering biedt wel dekking voor aansprakelijkheid voor cyberincidenten.

Hoe bepaal ik het eigen risico en de dekkingslimieten bij een cyberverzekering?

Het is van belang om uw cybergerelateerde scenario's na te lopen om inzicht te krijgen in de maximale schade die u als organisatie kunt of wenst te dragen. Die schade bestaat onder andere uit notificatiekosten, it-kosten, dataherstel, juridische kosten, pr-kosten, datadiefstal, afpersing en netwerkinterruptie. Aon heeft expertise op dit gebied en kan u adviseren, zodat u tot een gepaste dekkingslimiet komt. Het eigen risico hangt af van de omvang van uw bedrijf, maar ook van een keuze die u als klant maakt en het risico dat u zelf wenst/kan dragen. Aon kan u hierin adviseren.

Mijn bedrijf maakt gebruik van antivirussoftware en data-encryptie. Is een cyberverzekering dan wel nuttig?

Hoewel deze middelen zeker kunnen helpen schade te voorkomen of beperken, vormen ze geen gegarandeerde bescherming tegen datalekken of andere cyberincidenten. Cybersecurity en cyberverzekeringen zijn complementair aan elkaar. Er zijn tal van voorbeelden van grote multinationals die het slachtoffer werden van cybercrime. Zelfs de beste antivirussoftware en de meest ervaren in-house it-experts konden dit niet verhinderen. Bovendien zijn meer dan 40% van de claims zijn te herleiden naar menselijk of systeem falen.

Mijn it-expert zegt dat onze cybersecuritymaatregelen op orde zijn en wij geen risico lopen. Heb ik een cyberverzekering wel nodig?

Voor cyberrisico's geldt dat zelfs de beste cybersecuritymaatregelen niet kunnen garanderen dat hackers u niet kunnen raken. U kunt een cyberverzekering vergelijken met een brandverzekering. Ondanks blusinstallaties, sprinklers en brandwerend materiaal blijft er altijd risico op een brand. Daarom hebben bedrijven met uitstekende brandpreventie daarnaast een brandverzekering.

Ben ik als mkb-bedrijf een doelwit van hackers?

Een hacker maakt geen onderscheid tussen grote en kleine bedrijven. Veel aanvallen, bijvoorbeeld de recente Petya-aanval, zijn geen doelgerichte aanvallen. Aanvallen als deze kunnen ieder bedrijf raken dat ermee in aanraking komt. Uiteraard is de premie wel afhankelijk van de omvang van uw bedrijf. Juist kleinere bedrijven worden vaak als target gezien door hackers, omdat hun veiligheidsmaatregelen over het algemeen minder uitgebreid zijn dan die van multinationals.

Kan een bestuurder aansprakelijk worden gesteld wanneer het bedrijf geen cyberverzekering heeft?

Cyberincidenten kunnen zowel ondernemingen als individuele bestuurders diep in de portemonnee raken. Zeker nu de AVG na 25 mei 2018 ingevoerd zal worden. Wanneer u als bestuurder de cybersecurity, waaronder een cyberverzekering, bij uw bedrijf niet op orde heeft, kunt u hiervoor persoonlijk aansprakelijk worden gehouden. Een cyberverzekering kan uw bedrijf helpen de financiële impact van een cyberincident te mitigeren.

>>

Is een cyberverzekering wel zinvol als gegevens niet op een eigen netwerk worden opgeslagen, maar op een externe server of in de cloud?

Ja. Ook als een datalek optreedt bij een externe server loopt degene die de data bij de externe partij in beheer heeft gegeven een aansprakelijkheidsrisico. Een cyberverzekering blijft daarom aan te raden, ook als alle gegevens in de cloud staan opgeslagen.

Dekking en voorbeelden

Een medewerker is zijn laptop met privacygevoelige informatie verloren. Valt dit onder de dekking?

Ja. Wanneer het verlies van bijvoorbeeld een laptop of usb-stick met daarop privacygevoelige informatie tot schade leidt, valt deze schade onder de dekking van uw polis.

Is dit ook het geval wanneer een medewerker zijn werktas met privacygevoelige documenten verloren is?

Ja. Een cyberverzekering maakt geen onderscheid tussen een digitaal en niet-digitaal document. De gemene deler is het feit dat in beide gevallen privacygevoelige informatie op straat is gekomen. Veelvoorkomende kosten in dit soort scenario's zijn notificatiekosten, reputatiekosten, juridisch advies, aansprakelijkheid en in ernstige gevallen business-interruptie.

Mijn systemen zijn gehackt en ik moet betalen om toegang te krijgen tot mijn gegevens (ransomware-aanval). Wat heb ik aan mijn cyberpolis?

Wanneer u ontdekt gehackt te zijn, kunt u onmiddellijk bellen naar het crisisnummer dat op uw polis vermeldt staat. De crisismanager zal met u bespreken wat de beste aanpak is om deze zogenaamde ransomware-aanval op te lossen. De kosten - inclusief een eventuele betaling van losgeld - die gemaakt worden om deze situatie op te lossen, vallen onder de dekking van uw verzekering.

Biedt een cyberverzekering dekking als data in de cloud worden opgeslagen en it-diensten worden uitbesteed aan derden?

Ja. Of gegevens nu op een eigen server worden opgeslagen of in de cloud, voor de dekking maakt dit geen verschil. In beide gevallen zijn cyberincidenten doorgaans voor de volledige polis limiet verzekerd conform de dekkingsvoorwaarden, zowel voor eigen schade als voor de aansprakelijkheidsschade jegens derden.

Een cyberverzekering biedt veelal dekking voor pr-kosten. Wat moet ik me hierbij voorstellen?

De meeste verzekeraars bieden een vergoeding voor pr-kosten na een cyberincident. Deze vergoeding valt onder de crisisresponse-diensten. De kosten die u maakt om advies in te winnen bij een communicatie-expert vallen ook onder dekking. De kosten die gemaakt zijn voor het uitvoeren van dit advies zijn echter niet gedekt. Denk hierbij aan de kosten die u maakt bij het inkopen van zowel offline als online advertenties.

Bedrijfsschade

Als een bedrijf door een cyberincident schade lijdt, is dan alleen de bedrijfsschade verzekerd die verband houdt met de online bedrijfsactiviteiten?

Nee. Naast de bedrijfsschade die op online activiteiten geleden wordt, is de bedrijfsschade op offline activiteiten eveneens verzekerd. Dus bijvoorbeeld ook als door een cyberincident de voorraadsystemen niet meer functioneren of de telefooncentrale is uitgeschakeld. De bedrijfsschade die daaruit voortvloeit, is meeverzekerd.

Is bedrijfsschade veroorzaakt door een cyberincident bij een toeleverancier/afnemer ook gedekt op een cyberverzekering?

Dit is niet standaard gedekt, maar kan onder hele specifieke voorwaarden wel in de dekking worden meegenomen. Dit verschilt per verzekeraar.

Er wordt gesproken over gederfde nettowinst, maar mijn bedrijf heeft geen winstoogmerk. Hoe werkt de verzekering dan en wat doet dit met mijn premie?

Voor publieke instellingen is het lastiger om deze gederfde nettowinst te berekenen. Onder het nettoverlies verstaan we bij scholen het verlies van inkomsten door bijvoorbeeld minder aanmeldingen, bij gemeenten is dit bijvoorbeeld verlies door extra werk (overuren). De premie voor gemeenten is doorgaans afhankelijk van het aantal inwoners van de gemeente. Voor onderwijs is dit het aantal leerlingen/studenten. Uw premie wordt aangepast op het verwachte risico en de kosten.

Mijn bedrijf ligt stil door een cyberincident. Hoe worden de bedrijfsinterruptiekosten berekend?

De kostenberekening kan op twee verschillende manieren gemaakt worden. Veel verzekeraars hanteren de nettowinst-methode waarbij het verlies van (nettowinst + de vaste kosten) wordt vergoed. Een andere gebruikte methode is de brutowinst-methode waarbij de (omzet - de variabele kosten) het uitgangspunt zijn.

Wat is het verschil tussen eigen risico en franchise wanneer ik bedrijfsinterruptie heb na een cyberincident?

De verzekeraars die cyberpolissen aanbieden maken gebruik van twee soorten eigen risico: het klassieke eigen risico en franchise. Voordat de dekking ingaat wat betreft bedrijfsinterruptie is van belang:

- het eigen risico: een gelimiteerd bedrag waarover u het risico zelf draagt;
- de wachttijd: een eigen risico in de vorm van een bepaald aantal uur bedrijfsstilstand alvorens de dekking ingaat.

Voor de berekening van het uit te keren bedrag zijn er twee methodes. Stel u heeft in beide scenario's een eigen risico van EUR 25.000 en een wachttijd van 8 uur. De uiteindelijke schade door bedrijfsstilstand betreft EUR 1.000.000 en uw bedrijf heeft 10 uur stilgelegen, waarbij elk uur evenredig is qua kosten (dus EUR 100.000). Bij de ene verzekeraar krijgt u nu EUR 975.000 uitgekeerd en bij de andere verzekeraar slechts EUR 200.000. Hoe kan dit?

In het eerste scenario, het zogenaamde franchisemodel, werkt de wachttijd van 8 uur als een trigger waarna alle kosten minus het eigen risico gedekt worden (1.000.000, - minus 25.000, -). In het tweede scenario worden de kosten pas vergoed die gemaakt zijn nadat de wachttijd is verlopen (2 uur * EUR 100.000). Echter is het eigen risico in dit geval niet meer van toepassing (mits dit bedrag lager is dan de kosten gemaakt tijdens de wachttijd).

Let wel dat kosten niet altijd evenredig zullen zijn en juist in de eerste uren van uw bedrijfsstilstand de kosten kunnen oplopen. Als de bedrijfsinterruptie binnen de wachttijd is opgelost dan draagt u deze kosten zelf.

Wanneer ik niet compliant ben met de GDPR kan ik een forse boete krijgen. Valt deze boete ook onder de dekking?

Een cyberverzekering biedt dekking, mits dit wettelijk is toegestaan, voor door een toezichthouder opgelegde boete in verband met verlies/openbaarmaking van (persoons)gegevens, evenals de daarbij behorende verweerkosten ten tijde van het onderzoek door een toezichthouder. De verweerkosten zoals juridische bijstand worden ook gedekt wanneer de eventueel opgelegde boete dit niet is. Het dekken van deze boetes ligt in veel landen echter gevoelig, doordat dit het doel van de wetgeving kan ondermijnen.

Fraude vs. Cyber

We hebben een man-in-the-middle attack (MITMA) en een van onze medewerkers heeft dat niet tijdig doorzien en levert goederen op een ander adres af

Bij spear phishing is er over het algemeen geen sprake van een inbreuk op het systeem, maar van oplichting via internet door verzameling van informatie van een persoon via bijv. social media. Indien er geen relatie is met informatie die is verkregen door inbreuk op het systeem van verzekerde, is er geen dekking op een cyberverzekering. Ditzelfde geldt voor een MITMA, al geldt daar sneller dat men eerst moet inbreken in het systeem om data te onderscheppen of telefoongesprekken te volgen.

We hebben een MITMA en de hacker verandert een rekeningnummer en de klant betaalt op een ander rekeningnummer

Als gevolg van een inbreuk op het systeem is verlies van geld gedekt. Echter is dit bedrag vaak gesublimiteerd.

Een klant heeft een security breach en als gevolg daarvan kan de situatie zoals beschreven in de voorgaande vraag plaatsvinden

Als het gaat om een situatie bij uw klant dan wordt dit gedekt op grond van aansprakelijkheid op uw cyberverzekering. Als dit bij verzekerde gebeurt dan kan uw klant u als verzekerde hiervoor aansprakelijk stellen en zal het onder de aansprakelijkheidsrubriek vallen.

Een hacker doet zich voor als klant van uw organisatie en (ver)koopt producten of diensten

Als gevolg van een inbreuk op het systeem is verlies van geld gedekt. Echter is dit bedrag vaak gesublimiteerd.

Wat moet ik doen als zich een cyberincident heeft voorgedaan?

Na een cyberincident kunt u het crisisnummer dat op uw cyberpolis vermeld staat, bellen. Er wordt in overleg met de crisismanager bepaald welke partijen ingeschakeld moeten worden om de crisis onder controle te krijgen. Aon heeft een wereldwijd netwerk van specialisten, zoals forensische-, juridische- en cyberexperts en specialisten op het gebied van fraude en public relations, om elk soort cyberincident te kunnen beheersen.

Definities

- **Bedrijfsschade:** een bedrijfsonderbrekingsincident is de ontregeling, verstoring of onmogelijkheid om toegang te krijgen tot uw computersysteem. Ook wel netwerkonderbreking genoemd.

- **Bedrijfsschadetermijn**: de termijn waarbinnen schade geleden door een bedrijfsstilstand dan wel netwerkonderbreking in aanmerking komt voor vergoeding.

- **Cyberincident**: een hack, ransomware-aanval en verloren laptop, dit zijn allemaal cyberincidenten. Een cyberincident is vaak een voorwaarde voor dekking bij een cyberverzekering. Kijk in uw polis voor de exacte definitie van een cyberincident.

- **Distributed Denial of Service Attack (DDoS**): een aanval waarbij meerdere geïnfecteerde systemen worden ingezet om het doelwitsysteem te overspoelen met netwerkverkeer, waardoor dat systeem komt plat te liggen.

- **Hacker**: een persoon die zonder toestemming een netwerk binnendringt door de beveiliging te kraken. Niet altijd met de bedoeling om illegaal informatie toe te eigenen, maar veelal om aan te tonen dat het netwerk onvoldoende beveiligd is.

- **Incident response (ook wel crisis response):** de handelingen in reactie op een cyberincident. Verzekeraars bieden een crisisnummer welke u kunt bellen bij een vermoeden van een cyberincident. Het incident wordt door een gespecialiseerde partij opgepakt en er wordt alles aangedaan om het cyberincident zo snel mogelijk op te lossen.

- **Inlooptermijn**: schades waarvan de oorzaak ligt vóór de ingangsdatum van de verzekering, maar die worden ontdekt tijdens de looptijd ervan zijn in beginsel niet gedekt. Dit zogenaamde inlooprisico kan soms voor een bepaalde periode worden meeverzekerd. De inlooptermijn geeft aan welke periode het inlooprisico meeverzekerd is.

- **Malware:** samentrekking van MALicious softWARE. Deze software is bedoeld om een systeem te beschadigen of te verstoren (virus of Trojaans paard).

- **Man-in-the-middle attack**: een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben. Hierbij bevindt de computer van de aanvaller zich tussen de twee communicerende partijen. De berichten kunnen daarbij mogelijk gelezen en veranderd worden. Ook kunnen berichten worden verzonden die niet door de andere partij zijn geschreven. De naam van de aanval verwijst naar de derde persoon die in het midden tussen de twee partijen staat en de langskomende berichten bekijkt en aanpast.

>>

- **Notificatiekosten**: kosten die u maakt om uw klanten en partners te informeren na een hack of het verlies van persoonsgegevens. Het is wettelijk verplicht betrokkenen te informeren wanneer u persoonsgegevens bent verloren.

- **Responsediensten**: diensten die door het 'incident response'-team worden geadviseerd. Bestaat onder andere uit forensische-, juridische- en cyberexperts en specialisten op het gebied van fraude en public relations.

- **Security Breach**: een security breach is een incident dat onbevoegde toegang tot data, applicaties, diensten, netwerken en/of apparaten tot gevolg heeft door hun onderliggende beveiligingsmechanismen te omzeilen. Een security breach treedt op wanneer een persoon of een applicatie onrechtmatig een privé-, vertrouwelijk of onbevoegde it-perimeter binnendringt.

- **Spear Phishing**: een e-mail die afkomstig lijkt te zijn van een persoon of onderneming die u kent. Maar dat is slechts schijn. De e-mail is eigenlijk afkomstig van dezelfde criminele hackers die uit zijn op uw creditcard- en bankrekeningnummers, wachtwoorden en de financiële gegevens op uw computer

- **Sublimiet**: apart in de polis opgenomen lager verzekerd bedrag voor aan aparte dekking en maakt deel uit van het totaal verzekerd bedrag.

- **Wachttijd bedrijfsstilstand**: vooraf bepaalde periode die verstreken moet zijn alvorens de verzekeraar bedrijfsschade vergoed. De wachttijd kan gezien worden als een vorm van eigen risico en bedraagt meestal enkele uren.

Wij helpen u graag succesvol te ondernemen

Voor overige vragen, kunt u contact opnemen met:

Alexander van Nierop
06 135 844 89
alexander.van.nierop@aon.nl

aon.nl/cyber

1023-01-FAQ-cyberverzekeringen-v2