oktober 2013

Position paper

Virtuele risico's, echte schade

Over het verzekeren van cyberrisico’s

Dit position paper biedt verzekeraars en verzekerden inzicht in het fenomeen cyberrisico. Cybercriminaliteit is aan de orde van de dag, maar houdt een wat ongrijpbaar karakter. Het Verbond vindt dat verzekeraars bij dit onderwerp een belangrijke rol kunnen spelen en doet in dit paper een aanzet voor het verzekeren van cyberrisico’s.

VERBOND VAN VERZEKERAARS

In position papers geeft het Verbond van Verzekeraars zijn mening, standpuntbepaling en argumentatie daarbij over een concreet vraagstuk of actuele ontwikkeling op het snijvlak van politiek, samenleving en verzekeringsbedrijfstak.

Dit position paper is tevens te vinden op de website van het Verbond van Verzekeraars: www.verzekeraars.nl onder de button ‘Publicaties/Downloads/Position papers’.

Meer informatie over de inhoud van dit position paper:
dhr. drs. J.A. Schaffers
telefoon: +31 70 3338611
e-mail: j.schaffers@verzekeraars.nl

Dit is een uitgave van het
Verbond van Verzekeraars
Bordewijklaan 2
Postbus 93450
2509 AL Den Haag

Inleiding

Spionage, oorlogvoering, terrorisme, een bedrijf oplichten: het kan tegenwoordig allemaal via internet. En het gebeurt ook. De kranten stonden het afgelopen jaar vol met cyberincidenten. Denk aan DDoS aanvallen die websites platlegden, grote hoeveelheden wachtwoorden die gestolen werden, bedrijven die gechanteerd werden op straffe van het openbaar maken van informatie en gemeenten die massaal met een virus te maken hadden.

Dit soort incidenten heeft vaak financiële schade tot gevolg, die wereldwijd op meer dan 100 miljard euro wordt geschat. Zo kost het repareren van websites tijd en geld, evenals het herstellen van gegevens en het informeren van klanten. Regelmatig komt dan ook de vraag op of de schade als gevolg van cybercriminaliteit verzekerbaar is. In dit paper willen we duidelijk maken welke echte schade er kan voortkomen uit de virtuele wereld en wat daartegen is te doen. Het Verbond wil daarmee het ongrijpbare grijpbaar maken.

Dit paper is bedoeld voor twee groepen lezers. Ten eerste voor partijen uit de verzekeringsbranche in Nederland. Omdat cyberincidenten een relatief nieuw risico zijn, zijn er in Nederland nog maar weinig verzekeraars die een verzekering aanbieden voor cyberrisico's. Dit paper is voor die partijen als handvat bedoeld om hen te helpen te begrijpen wat het risico precies is, hoe het zich verhoudt tot traditionele verzekeringen en hoe verzekeraars wellicht zelf oplossingen voor dit fenomeen kunnen aanbieden.

Ten tweede is dit paper bedoeld voor verzekerden, in eerste instantie bedrijven, die zich wellicht afvragen welke risico's zij precies lopen en wat er zoal verzekerbaar is. Omdat de markt voor cyberverzekeringen nog volop in ontwikkeling is, zal het voor klanten niet altijd eenvoudig zijn te begrijpen hoe het aanbod zich verhoudt tot hun vraag. Dit paper probeert dan ook duidelijkheid te geven over de diverse dekkingen die er zijn, zodat zij goed geïnformeerd besluiten kunnen nemen.

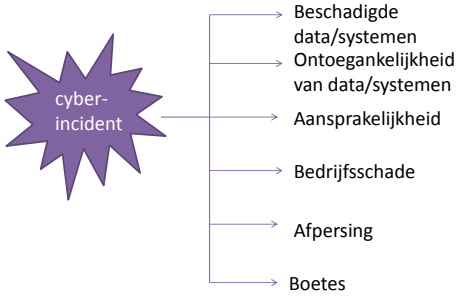
1. Wat verstaan verzekeraars onder cyberrisico?

Verzekeraars verstaan onder een cyberrisico het financiële nadeel dat een verzekerde oploopt door of via computer- en/of ICT-systemen, zonder dat er sprake is van materiële schade. Die materiële schade, zoals een brand die een serverruimte vernielt, wordt via traditionele verzekeringen gedekt.

De drie voornaamste manieren waarop cyberrisico's ontstaan:

1. Door een moedwillige aanval van buitenaf, bijvoorbeeld een virus, DDos-aanval of een hack. DDos-aanvallen (distributed denial of service) hebben tot doel websites zodanig te belasten, dat ze door de bedoelde gebruikers niet langer te benaderen zijn. Recent werden onder andere DigiD, Rijksoverheid.nl en diverse banken nog slachtoffer van dit soort aanvallen.
2. Door een menselijke fout, al dan niet opzettelijk, waaronder verlies of diefstal van (een onderdeel van) een computersysteem of data van de verzekerde die persoonsgegevens bevatten. Een boze oud-medewerker kan bijvoorbeeld moedwillig belangrijke gegevens verduisteren of een opening in het systeem publiceren.
3. Door technisch falen van eigen of externe IT-systemen, servers, hard- en software.

Bovengenoemde incidenten leiden tot een verlies van of beschadiging aan data, (on)toegankelijkheid van systemen, aansprakelijkheid, bedrijfsschade, afpersing en boetes. Dat zijn allemaal zaken die geld kosten: data moet worden hersteld of er moet onderzoek worden gedaan naar de herkomst van de bedreiging. De oorzaak is het cyberincident, het gevolg is de financiële schade. In een tekening ziet dit er als volgt uit:



2. Wat dekken cyberverzekeringen?

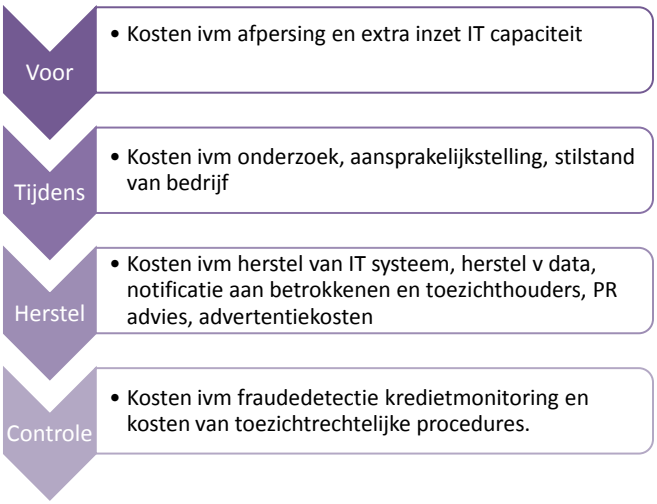
De verzekeringsdekking verschilt natuurlijk per verzekeraar. Daarnaast kan deze ook van moment tot moment verschillen, aangezien de markt nog volop in ontwikkeling is. Hieronder geven we aan wat het aanbod momenteel is op de Nederlandse verzekeringsmarkt. De verzekeringsdekking valt uiteen in twee hoofdmoten: de schade aan derden en, in mindere mate, de schade die de onderneming zelf oploopt. Om de dekking verder te verduidelijken, kijken we naar de schade, zoals deze zich door de tijd heen ontwikkelt:

1. **Voordat het cyberincident zich manifesteert**
   Wanneer er een vermoeden is van een cyberincident, kan er al schade ontstaan. Soms worden bedrijven afgeperst, onder dreiging van een DDoS-aanval of bewust lekken van privacygevoelige gegevens. Het kan nodig zijn dat een verzekerde extra IT-capaciteit inkoopt uit voorzorg om op deze wijze de DDoS aanval te voorkomen. Hiermee zijn kosten gemoeid, die kunnen worden verzekerd. Ook de begeleiding en betaling van afpersing kunnen afgedekt worden met een verzekering.
2. **Tijdens de manifestatie van het cyberincident**

A. In deze fase gaat het allereerst om kosten die worden gemaakt om het probleem te onderzoeken, bijvoorbeeld door een forensisch IT-specialist. Het doel van dit onderzoek is om het risico te beperken en de organisatie te beschermen.
B. Wanneer een datalek zich voordoet, kan de organisatie hiervoor aansprakelijk worden gesteld. Deze aansprakelijkstelling kan ontstaan doordat een melding is gedaan van een lek bij een bevoegde autoriteit, of juist doordat die melding niet is gedaan. In de samenleving begint steeds meer het bewustzijn te leven dat individuen organisaties aansprakelijk kunnen stellen voor geleden schade in verband met gegevensverwerking en -lekken. De gedupeerden kunnen een civielrechtelijke actie starten op basis van onrechtmatige daad. Ook deze schade en kosten van verweer zijn verzekerbaar. Daarnaast kunnen de kosten van wettelijk verplichte notificatie richting gedupeerden onderdeel zijn van de verzekeringsdekking.
C. Tot slot kan als gevolg van een cyberincident het interne en/of externe netwerk van een organisatie worden stilgelegd, waardoor inkomsten worden gemist. Middels een bedrijfsschadedekking worden deze gemiste inkomsten vergoed. Hierbij kan ook worden gedacht aan betalingsplatformen van banken.

3. **Herstelfase**
   In deze fase gaat het om kosten die worden gemaakt om het probleem te herstellen. Denk aan het herstel van het IT-systeem en het herstel van verloren data. Ook de kosten die gepaard gaan met de notificatie bij toezichthouders, zoals juridische expertise, kunnen worden gedekt. Daarnaast bestaan er verzekeringsdekkingen die de kosten voor de inhuur van een communicatieadviesbureau vergoeden om hierdoor reputatieschade te voorkomen of te beperken.
4. **Controlefase**
   In deze fase gaat het om de kosten van toezichtrechtelijke procedures en kredietmonitoringdiensten (om te zien of bijvoorbeeld gestolen creditcardgegevens worden misbruikt).

In een tekening ziet dit er als volgt uit:



3. Preventie

Ook als bedrijven of particulieren zich hebben verzekerd tegen cyberrisico's, dan nog zullen ze alles moeten doen om een cyberincident te voorkomen. Niet alleen omdat de premies daardoor laag blijven, de verzekeringsvoorwaarden het voorschrijven of omdat niet alle schade onder de dekking valt (denk aan imagoschade), maar ook omdat de wetgever het eist. In artikel 12 van de Wet bescherming persoonsgegevens staat dat een bedrijf 'passende beveiligingsmaatregelen' moet nemen bij het verwerken van persoonsgegevens. Alhoewel deze wetgeving alleen gekoppeld is aan het mogelijk lekken van persoonsgegevens, kunnen contractpartners ook passende beveiliging verwachten bij het verwerken van gevoelige bedrijfsin-

formatie. In de nieuwe richtsnoeren voor beveiligingsmaatregelen van het College Bescherming Persoonsgegevens wordt de term ‘passende beveiliging’ uitgelegd. Om blijvend te voldoen aan de norm ‘passende beveiliging’, moeten gegevensbeveiliging en privacybescherming onderdeel zijn van de reguliere ‘plan-do-check-act’-cyclus.

Welke beveiligingsmaatregelen een bedrijf neemt, is onder meer afhankelijk van de betrouwbaarheidseisen die worden gesteld aan de informatie- of computersystemen. Deze eisen kunnen worden opgesteld naar aanleiding van een ‘Privacy impact assessment’. In zo’n assessment wordt gekeken wat de gevolgen zijn voor één betrokkene, als de door het bedrijf verwerkte gegevens openbaar zouden worden gemaakt. De hoeveelheid gelekte gegevens van één betrokkene in combinatie met de gevoeligheid van de gegevens zijn hiervoor van belang.

In sommige branches, bijvoorbeeld in de zorg of bij het verwerken van creditcardgegevens, is al sprake van een zogenaamde ‘industriestandaard’ (bv. HIPAA of PCI DSS). Deze standaarden schrijven voor welke maatregelen er minimaal moeten worden genomen op het gebied van gegevensbescherming. De meeste bedrijven zullen echter zelf moeten bepalen welke beveiligingsmaatregelen ze nemen. Die maatregelen hebben tot doel een incident te voorkomen of de gevolgen te beperken, soms een combinatie van beide. Hieronder een aantal voorbeelden:

- Beleidsdocument voor informatiebeveiliging
- Toewijzen van verantwoordelijkheden voor informatiebeveiliging
- Beveiligingsbewustzijn
- Fysieke beveiliging en beveiliging van apparatuur
- Toegangsbeveiliging
- Logging en controle
- Correcte verwerking in toepassingssystemen
- Beheer van technische kwetsbaarheden
- Incidentenbeheer
- Afhandeling van datalekken en beveiligingsincidenten
- Continuïteitsbeheer
- Monitoring van bedrijfsnetwerken
- Versleuteling van gegevens

4. Privacywetgeving

De Wet bescherming persoonsgegevens (Wbp) bevat zoals hiervoor aangegeven de belangrijkste regels voor de omgang met persoonsgegevens. De wet is een Nederlandse uitwerking van de Europese Richtlijn bescherming persoonsgegevens. Volgens de Wbp heeft de burger bepaalde rechten, zoals het recht om te weten wat er met zijn persoonsgegevens gebeurt. Hij mag zijn gegevens te allen tijde inzien en mag bijvoorbeeld ook vragen zijn gegevens te corrigeren of bezwaar maken tegen de verwerking van zijn persoonsgegevens. Als iemand bezwaar maakt tegen het gebruik van persoonsgegevens voor ‘direct marketing’, moet een bedrijf dit bezwaar honoreren.

Organisaties die persoonsgegevens verwerken, hebben bepaalde plichten. Zo mogen persoonsgegevens alleen worden verzameld en verwerkt als daarvoor welbepaalde en uitdrukkelijk omschreven doelen zijn en deze doelen gerechtvaardigd zijn door bijvoorbeeld toestemming van de betrokken burger. Ook moeten zij – uitzonderingsgevallen daargelaten – de burger laten weten wat zij met zijn gegevens (gaan) doen.

Op nationaal niveau ligt er momenteel een wetsvoorstel tot wijziging van de Wbp bij de Tweede Kamer. Dat wetsvoorstel bevat een meldplicht bij geconstateerde inbreuken op beveiligingsmaatregelen voor persoonsgegevens en een uitbreiding van de bevoegdheid tot het opleggen van een bestuurlijke boete door het College bescherming persoonsgegevens. Die boete kan oplopen tot € 450.000. De meldplicht voor da-

talekken geldt – sinds 5 juni 2012 – al voor een telecomprovider, Internet Service Provider of hostingbedrijf (oftewel een aanbieder van informatiediensten), in het geval van beveiligingsincidenten waarbij persoonsgegevens zijn betrokken. Dergelijke incidenten moeten worden gemeld aan toezichthouder Autoriteit Consument & Markt (voorheen: OPTA) en in sommige gevallen is er ook een informatieplicht aan de betrokkenen.

In het voorjaar van 2012 publiceerde de Europese Commissie een voorstel voor een nieuwe Europese Privacyverordening, die de nationale wetten voor bescherming van persoonsgegevens moet vervangen. Anders dan een EU-richtlijn, hoeft een EU-verordening niet te worden omgezet in nationale wetgeving en is zij derhalve onmiddellijk bindend. De verordening wordt nu door het Europees Parlement bestudeerd. Als het parlement het eens is, moet nog overeenstemming worden bereikt met de Europese Raad van Ministers. Verwacht wordt dat de verordening zal leiden tot onder andere:

- het recht om vergeten te worden;
- een verplichting voor bedrijven om een gegevensfunctionaris aan te stellen;
- een verplichting voor bedrijven om een datalek binnen 24 uur te melden bij de toezichthouder en de betrokkene, op straffe van een boete.

Vooral dit laatste onderdeel zal naar verwachting een nieuwe fase inluiden in de bewustwording van cyberrisico's: enerzijds zullen bedrijven zelf hun processen beter op orde moeten hebben, anderzijds zullen burgers meer te weten komen over incidenten. In de concept EU Privacyverordening is voorzien in boetes die kunnen oplopen tot maximaal €1.000.000 of twee procent van de wereldwijde jaaromzet.

5. Preparatie

In paragraaf twee van dit paper beschreven we het verloop van een cyberincident in vier fases: voor, tijdens en in de herstel- en controlefase. De verzekerde zal in de fase vóór een incident preventieve activiteiten moeten ondernemen. Dit kan onder andere door de aanschaf en het onderhouden van antivirussoftware, waardoor de kans op een incident afneemt. Ook is het van belang om een goed passwordbeleid te volgen. De kans op een hack blijft echter altijd bestaan. Zelfs de computers van het Pentagon zijn niet veilig voor hackers. Voor dat restrisico is een cyberverzekering van belang: om de financiële gevolgen af te dekken op het moment dat een hacker toch doordringt.

Naast de financiële gevolgen kan een cyberincident ook immateriële gevolgen hebben. Zo kan het imago van het bedrijf een flinke deuk oplopen. Die schade kan enorm zijn, maar is lastig te objectiveren en wordt daarom door verzekeraars grotendeels niet verzekerd. Wel kunnen verzekeraars de verzekerde helpen om verdere (imago)schade te voorkomen. Voor veel ondernemers is het, op het moment dat een incident zich voordoet, namelijk lastig te bepalen welke stappen ze moeten zetten, welke rechten en plichten ze hebben, hoe ze met klanten of het bredere publiek moeten communiceren, etcetera. De verzekeraar kan daar in overleg met de verzekerde een plan voor schrijven. In de VS doen verzekeraars dit al volop. Daar wordt gesproken over een *incident response plan*. Naast een beschrijving van de stappen die worden gezet bij een incident, staan er ook concrete namen en nummers in, bijvoorbeeld van IT-bedrijven, juristen en communicatiedeskundigen, die de klant kunnen bijstaan tijdens een incident. Zo'n *incident response plan* dient zowel het belang van de verzekeraar als de verzekerde. Een goede reactie op het moment dat het fout gaat, kan de schade immers beperken. Zelfs als de data al volledig verloren zijn, kan door een goede communicatiestrategie de imagoschade voor het bedrijf nog beperkt worden.

6. Verhouding tot traditionele verzekeringen

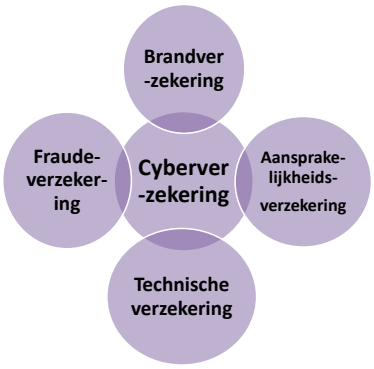
De indruk bestaat dat sommige cyberrisico's al gedekt zijn op enkele traditionele verzekeringen. Zo kan een bestaande bedrijfsschadeverzekering een deel van de gevolgschade dekken die door een cyberincident ontstaat. De belangrijkste bestaande verzekeringen die dit al dekken, zijn de brand- en technische verzekeringen (machinebreuk/computer), de aansprakelijkheidsverzekering en de fraudeverzekering.

Brand- en technische verzekeringen
Brand- en technische verzekeringen in de zakelijke markt bieden ofwel een all-risk dekking ofwel een dekking waarbij alleen specifieke schadeoorzaken verzekerd zijn. De all-risk dekkingen komen veel voor in de grootzakelijke markt, de specifieke oorzaken variant komt veel voor in de MKB-markt. In beide gevallen zal de overlap met cyberverzekeringen doorgaans klein zijn. Bij een all-risk dekking is in principe alle materiële schade gedekt. In het geval dat een cyberincident dus ook materiële schade tot gevolg heeft, dan kan voor die materiële schade dekking worden gevonden bij de brandverzekering. Denk bijvoorbeeld aan de hacker die via een computerverbinding een lopende band of machine hackt, waardoor deze in elkaar draait. Verzekeraars beschouwen schade aan data echter zelden als materiële schade. Voor de schade aan data is dan ook een cyberverzekering van belang. Bij een verzekering die alleen specifieke schadeoorzaken verzekert wordt tot op heden cyberschade zelden meeverzekerd. De overlap is daarom in beide dekkingsvarianten minimaal.

Aansprakelijkheidsverzekeringen
De algemene aansprakelijkheidsverzekering biedt in de regel alleen dekking voor zaak- en letselschade. Financieel nadeel valt hier niet onder, dus schade door cyberrisico ook niet. Ook een beroepsaansprakelijkheidsverzekering biedt onvoldoende dekking voor cyberincidenten. Toch kan het in sommige gevallen onderdeel uitmaken van de dekking. Dit is echter eerder uitzondering dan regel.

Fraudeverzekeringen
De commerciële fraudeverzekering biedt dekking voor de directe financiële gevolgen van frauduleus handelen door werknemers en gespecificeerde soorten van frauduleus handelen door derden, waaronder afpersing, vervalsing van onder andere geld of documenten en computerfraude. Hierdoor kan er overlap ontstaan met de cyberverzekering, aangezien deze eveneens dekking biedt voor financieel nadeel als gevolg van afpersing, bijvoorbeeld bij encryptie van gegevens. Daarnaast kan overlap bestaan binnen de computerfraudedekking. Voor deze uitkering moet binnen de fraudeverzekering echter wel sprake zijn van daadwerkelijk verlies van financiële middelen (verlies van saldo op bankrekeningen). De kosten om een aanval af te wenden vallen buiten veel verzekeringsdekkingen. Daarnaast worden deze dekkingen binnen de fraudeverzekering veelal beperkt.

Mind the gap
Geen enkele traditionele verzekering biedt dus uitgebreide dekking in geval van cyberincidenten. Daarom heeft een cyberriskverzekering in veel gevallen toegevoegde waarde. Analyseer de bestaande verzekeringen op mogelijke overlap, maar: *mind the gap!*



7. Boetes
Als gevolg van datalekken kunnen bedrijven te maken krijgen met boetes. De vraag rijst of deze boetes verzekerbaar zijn. Het antwoord daarop heeft twee kanten: enerzijds is het verzekeren van boetes vaak maatschappelijk en politiek niet wenselijk en kan het in strijd zijn met de openbare orde of goede zeden

(artikel 3:40 BW). Als bedrijven hiervoor een verzekering zouden kunnen afsluiten, dan zou deze verzekering immers tot gevolg hebben dat de prikkel die van de boete geacht wordt uit te gaan, vermindert. Ook wordt wel gesteld dat het verzekeren in strijd zou kunnen zijn met de plicht voor integere en adequate beleidsvoering die aan verzekeraars is opgelegd in art 4:11 lid 2 Wft of de plicht voortvloeiend uit de Gedragscode Verzekeraars van het Verbond om zich maatschappelijk verantwoord te gedragen. De andere kant van de medaille is dat het verzekeren van boetes in de regel aanvaardbaar wordt geacht, tenzij de boete betrekking heeft op opzettelijk handelen. Met andere woorden: als een bedrijf wordt gehackt, terwijl het alle redelijke beveiligingsmaatregelen heeft genomen, en het bedrijf krijgt toch een boete opgelegd, dan wordt het verzekeren daarvan mogelijk en aanvaardbaar geacht. In de praktijk dekken veel verzekeraars dan ook dergelijke boetes, met inbegrip van de onderzoekskosten, kosten van verweer en rechtsbijstand.

8. Outsourcing

Outsourcing van bepaalde activiteiten zorgt voor een extra dimensie van het cyberrisico. Bij outsourcing kunt u denken aan het uitbesteden van de salarisadministratie, het inkopen van cloudcomputingdiensten en het onderbrengen van data bij datacenters. In de Wet bescherming persoonsgegevens (Wbp) is vastgelegd dat een bedrijf zelf verantwoordelijk blijft voor de integriteit en de beveiliging van de verzamelde (gevoelige) gegevens, ongeacht of een en ander is uitbesteed. Uitbesteding zorgt er (als het goed is) voor dat bepaalde activiteiten worden overgelaten aan een professionele partij, met als gevolg dat de ‘verantwoordelijke’ een stuk minder grip op de zaak krijgt. Neemt de partij aan wie het werk en de gegevens zijn uitbesteed het wel zo nauw met alle regels rondom privacyschending en gegevensbeveiliging? Zal hij het eerlijk doorgeven als er sprake is van een lek? Immers: het imago van een dergelijke partij staat dan direct op het spel. Op het moment van schade is het ook nog maar de vraag of het bedrijf direct toegang krijgt tot de serverruimtes en of het lek direct kan worden gedicht zonder al te veel beschadigingen aan de data.

Het is voor bedrijven dan ook erg belangrijk om doordachte beslissingen te nemen bij uitbesteding. Zeker op het moment dat er veel gevoelige gegevens worden verwerkt of opgeslagen, is het van belang om in ieder geval te weten waar dit gebeurt (is dit wel binnen Nederland?), hoe dit gebeurt, hoe ervoor gezorgd wordt dat het veilig gebeurt en hoe de crisisherstelplannen van een insourcer er uitzien.

Cyberrisico’s via uitbesteding zijn overigens wel verzekerbaar. Bovengenoemde punten zijn daarbij belangrijk voor de acceptatie van risico’s. Ongeacht of de data worden beheerd bij een serviceprovider en of er gebruik wordt gemaakt van IT-systemen van de provider, nemen de meeste cyberverzekeringen dit mee in de dekking.

9. Voor wie is een cyberverzekering interessant?

Waarschijnlijk zullen cyberverzekeringen op den duur de normaalste zaak van de wereld worden, net zoals een inboedel- of opstalverzekering dat nu ook is. Op dit moment zal een cyberverzekering vooral interessant zijn voor bedrijven die in sterke mate afhankelijk zijn van IT-systemen of die veel gegevens beheren. Voor hen is het risico om schade te lijden door cyberincidenten immers groter. Dit geldt overigens niet noodzakelijk voor grote bedrijven. Een webwinkel beschikt ook al gauw over duizenden contacten, die waarde of juist verlies kunnen opleveren. Juist zo’n kleine ondernemer heeft vaak niet alle kennis in huis om de informatiebeveiliging goed te regelen. Aan de andere kant zijn ook banken, overheden en bijvoorbeeld telecomproviders potentiële verzekerden: hoe goed zij hun beveiliging ook op orde hebben, de hacker beschikt eveneens over de laatste technologieën. Het kan voor alle organisaties dus interessant zijn een cyberverzekering af te sluiten.

10. Verzekeraars en overheid werken samen aan cybersecurity

Je zou het bijna vergeten: verzekeraars kunnen natuurlijk ook zélf worden getroffen door cyberincidenten. Het Verbond vindt dat verzekeraars een verantwoordelijkheid hebben om de weerbaarheid van hun IT-systemen en processen op een acceptabel niveau te brengen. Sinds dit jaar werkt de bedrijfstak daarom nauw samen met het Nationaal Cyber Security Centrum (NCSC). In dit verband is de oprichting van een platform voor verzekeraars binnen het zogeheten Informatieknooppunt Cybersecurity een belangrijke mijlpaal. Binnen het Informatieknooppunt delen verzekeraars onderling, en met overheidsdiensten en andere (vitale) sectoren, informatie over incidenten, kwetsbaarheden en maatregelen. Hierdoor zijn alle partijen beter in staat om goede risicoanalyses te maken en adequate maatregelen te treffen. Door deel te nemen aan het Informatieknooppunt, leveren verzekeraars een bijdrage aan een meer robuuste Nederlandse economie.

11. Conclusie

Cyberrisico’s worden in Nederland nog lang niet zo veel verzekerd als in de Verenigde Staten. Toch zien we de behoefte ook in Europa steeds meer toenemen. Experts verwachten dat op termijn een dekking voor cyberrisico’s net zo normaal zal zijn als een brand- of aansprakelijkheidsverzekering. Dat komt doordat de bedrijfscontinuïteit net zo goed door cyberrisico’s in gevaar kan komen, als door een brand of een diefstal. De kosten van het herstellen van data, het notificeren van autoriteiten en het communiceren met klanten na een cyberincident, kunnen immers fors oplopen. Daarbij is het voor klanten en verzekeraars goed om te weten dat het verzekeren van cyberrisico’s niet goed mogelijk is zonder voldoende informatiebeveiliging. En omdat de kans op een cyberincident ondanks goede informatiebeveiliging nooit helemaal uitgesloten is, is het vaak ook verstandig voorbereid te zijn op het moment dat het dan toch mis loopt. Die voorbereiding kan een verzekerde zelf ter hand nemen, maar daar kunnen verzekeraars ook een rol in spelen.