SYSTEEMRISICO'S IN HET CYBERDOMEIN

VERBOND VAN VERZEKERAARS

Juni 2023

In dit paper schetsen we het systeemrisico in het cyber(verzekering)domein. Ook gaan we dieper in op enkele specifieke elementen van cyberdreigingen, die in belangrijke mate bijdragen aan dit systeemrisico: Ransomware, Privacy en het gebrek aan Incidentdata.

Dit paper maakt onderdeel uit van een reeks van papers die ingaan op cyberrisico's en de verzekerbaarheid ervan. Later dit jaar volgen nog papers over 'Stille verzekeringsdekking' (zie het kader) en 'Marktontwikkelingen' waarin we stilstaan bij internationale ontwikkelingen.
Eerder is uitgebreid gerapporteerd over de Risicoklassenindeling Digitale Veiligheid en de behoefte aan en ontwikkeling van aanpalende keurmerken. Op onze website is hierover nadere informatie te vinden.

Stille dekking
Definitie stille dekking: Dekking voor schade als gevolg van een cyberrisico op een traditionele verzekering. Het risico is niet in- of uitgesloten. Dit kan betekenen dat schade als gevolg van een cyberrisico onbedoeld gedekt is.
In het paper over 'stille dekking' zal worden ingegaan op dekking voor of uitsluiting van digitale (cyber)risico's in traditionele verzekeringen, zoals een auto-, brand-, of (beroeps)-aansprakelijkheidsverzekering.

INLEIDING

De Nederlandse samenleving is in hoge mate gedigitaliseerd. Computers en digitale processen zijn integraal onderdeel van bedrijfsmatige en sociale processen. Er zijn nauwelijks meer bedrijven of sectoren te vinden die onafhankelijk zijn van computer-systemen. Ook in ons sociale leven is de computer, in al zijn verschijningsvormen, niet meer weg te denken. Dit gaat gepaard met steeds meer en grotere risico's, die vaak sterk met elkaar verbonden zijn. Tegelijkertijd is er nog nauwelijks vraag naar verzekeringen voor het afdekken van digitale risico's, ook is er een beperkt aanbod van cyberverzekeringen. Minder dan 20 procent van de bedrijven heeft een cyberverzekering afgesloten en de omvang van de cyberverzekeringsmarkt is met 35 miljoen euro in 2021 zeer bescheiden te noemen (bron: DAC 2022). Voor grote (internationaal opererende) bedrijven is het afsluiten van cyberdekking gangbaar, hoewel ook daar de toegankelijkheid onder druk staat door oplopende schadelast, met hogere premies en strengere voorwaarden tot gevolg. Particulieren en ondernemers in het midden- en kleinbedrijf verzekeren zich niet of nauwelijks. In het Blog 'Blik op cyberverzekeringen' wordt bij het voorgaande stilgestaan.

Verzekeraars hebben zelf natuurlijk ook te maken met cyberrisico's. In de eerste plaats in eigen huis. Ze zijn in hoge mate gedigitaliseerd en sterk afhankelijk van geïntegreerde systemen voor beoordeling van risico's, administratie van polissen, communicatie, controles op fraude, voorkomen van witwassen, naleving van sanctiewetgeving en het afwikkelen van schades. Hoewel verzekeraars formeel geen onderdeel zijn van de vitale infrastructuur, nemen ze de risico's zeer serieus en treffen vergelijkbare maatregelen om incidenten te voorkomen of de gevolgen ervan te mitigeren. Hiervoor heeft het Verbond van Verzekeraars al in 2017 een i-CERT ingericht (Computer Emergency Response Team voor de verzekeringssector). Dit is een centrale dienst die alle aangesloten verzekeraars doorlopend informeert en adviseert over cyberbedreigingen en -incidenten. Het maakt verzekeraars digitaal weerbaarder en draagt bij aan verbetering van de informatie-beveiliging in de hele keten. Daarnaast wordt nauw samengewerkt met toezichthouders, zoals de Autoriteit Financiële Markten, Autoriteit Persoonsgegevens, De Nederlandsche Bank en met het Nationaal Cyber Security Centrum en het Digital Trust Center.

Zonder dat we dit eigenlijk voldoende beseffen is hier deels sprake van systeemrisico's. Mede daardoor zijn cyberrisico's vooralsnog op bescheiden schaal verzekerbaar. In dit paper schetsen we welke systeemrisico's er zijn in het digitale domein en wat de gevolgen zijn voor het verzekeren van cyberrisico's. Aangegeven wordt waarom het voor verzekeraars nog altijd lastig is om (grootschalig) risicodekking te bieden en welke stappen genomen (kunnen) worden om dit te helpen verbeteren. Speciale aandacht gaat daarbij uit naar de gevolgen van gijzelsoftware (ransomware), die kwaadwillende partijen gebruiken om computer(systemen) te gijzelen met als doel losgeld te ontvangen, gegevens te stelen, of activiteiten door bedrijven of organisaties lam te leggen om commerciële of politieke redenen. Daarnaast beperkt de toegenomen aandacht voor privacy, hoe noodzakelijk ook, de mogelijkheden tot het verzekeren van cyberrisico's.

SYSTEEMRISICO'S

"Systeemrisico's" verwijzen naar risico's die zo groot zijn dat zij in staat zijn economische en maatschappelijke verliezen te veroorzaken die leiden tot het ineenstorten van een heel systeem. Systeemrisico's hebben tegelijkertijd invloed op een groot deel van de samenleving en raken meerdere regio's, industrieën en verzekeringsklassen. Dit zorgt ervoor dat traditionele risico-overdrachtsmechanismen (lees: verzekeren) ongeschikt zijn, omdat het risico niet kan worden verdeeld of effectief kan worden geabsorbeerd. Bovendien zijn de risico's ook uiterst moeilijk te kwantificeren en te begrijpen. Omdat systeemrisico's zeer zelden voorkomen, weten klanten niet van hun bestaan waardoor ze het risico voor verzekeraars onderschatten.

Verzekeraars nemen systeemrisico's zeer serieus, omdat ze een bedreiging vormen voor het voortbestaan van verzekeraars en de verzekeringsbranche, maar ook kunnen leiden tot de ineenstorting van een heel systeem.

Het beperken van systeemrisico's is complex. Dergelijke risico's worden vergroot door drie maatschappelijke kwetsbaarheden:

- Onderlinge afhankelijkheid

Langere en complexere toeleveringsketens verergeren de onderlinge afhankelijkheid van de samenleving en de blootstelling aan systeemrisico's.

- Interconnectiviteit van risico

De toenemende interconnectiviteit van risico's vermindert het vermogen van verzekeraars om systeemrisico's effectief te diversifiëren.

- Wereldwijde impact

De globalisering van de samenleving heeft het mogelijk gemaakt dat systeemrisico's tegelijkertijd meerdere landen over de hele wereld kunnen beïnvloeden.

Diverse grote internationale (her)verzekeraars wijzen op de mogelijke onverzekerbaarheid van systeemrisico's in de toekomst. Hierbij wordt vaak een vergelijking gemaakt met pandemieën en aardbevingen.
Een goed voorbeeld voor de cyberverzekering is de Log4j kwetsbaarheid (zie NCSC). Log4j is een hulpprogramma voor logboekregistratie. Indien deze kwetsbaarheid uitgebuit wordt kan een hacker op afstand een code uitvoeren op de server, of in het programma waar deze software gebruikt wordt. Hierdoor kan hij eventueel data stelen of een ransomware aanval uitvoeren waardoor bepaalde kritische systemen versleuteld worden. Log4j wordt door sommige organisaties vergeleken met suiker; je komt het tegen op onverwachte plaatsen. De schatting is dat miljoenen applicaties deze specifieke kwetsbaarheid hebben. De totale schade is nog niet te overzien. Mogelijk hebben hackers al ingangen bij bedrijven gecreëerd die pas in een later stadium tevoorschijn zullen komen.

Een ander voorbeeld is de aanval op vitale infrastructuur zoals de Amerikaanse pijpleiding (Colonial Pipeline Ransomware attack). Hierdoor kwam de brandstofvoorziening in het oosten van Noord-Amerika in gevaar. Door het betalen van losgeld kon de voorziening naar enige dagen weer hersteld worden. De hackers waren hier duidelijk op geld uit en hadden geen politieke intenties. Een politieke activist had ook zgn. "Wiper software" kunnen installeren. Hierdoor had de software waarschijnlijk volledig opnieuw moeten worden ontwikkeld.
De consequentie hiervan is nauwelijks te overzien vooral als bijvoorbeeld in Nederland met het internet verbonden systemen van de vitale infrastructuur worden aangevallen.
Ook neemt de afhankelijkheid van centrale Clouddiensten sterk toe. Steeds meer bedrijven maken gebruik van diensten van aanbieders zoals MS Azure, AWS of GCS. Als bijvoorbeeld

meerdere bedrijven uit dezelfde branche of keten van deze diensten gebruik maken, kan een grootschalig incident bij een van deze dienstverleners leiden tot het niet beschikbaar zijn van kritische systemen. Dit vormt een groot risico voor de samenleving bijvoorbeeld als hierdoor de kritische infrastructuur wordt geraakt of de voedselvoorziening in gevaar komt.

Om in de toekomst cyberverzekeringen betaalbaar te houden of überhaupt aan te kunnen bieden nemen diverse verzekeraars inmiddels maatregelen in de vorm van het aanpassen van polisvoorwaarden door het beperken of uitsluiten van dekkingen voor specifieke risico's, zoals bijvoorbeeld het beperken van de dekking in geval van wijdverspreide kwetsbaarheden, bij het gebruik van verouderde software, of als verzekerden hun systemen niet goed bijhouden (software updates en het maken van betrouwbare back-ups).

Ook wordt er gewerkt aan het uitsluiten van oorlogsrisico's. Sommige verzekeraars sluiten een 'cyberoorlog' inmiddels al uit. Op andere polissen zoals bij brandverzekeringen wordt dit standaard uitgesloten. Het probleem bij cyberaanvallen is dat het niet altijd duidelijk is of de aanval een oorlogsdaad is of niet terwijl dit bij brandrisico's in het algemeen vrij duidelijk is. De recente oorlog in Oekraïne heeft dit onderwerp weer actueel gemaakt.

In het rapport "Verzekeraars in een veranderende wereld" geeft DNB aan dat *"cyberaanvallen in potentie kunnen uitgroeien tot een systeemcrisis, bijvoorbeeld wanneer vitale digitale processen in de telecommunicatie en energievoorziening, bij de overheid of transport ontoegankelijk gemaakt worden."* Een van de beleidsaanbevelingen uit dat rapport is dat betere dekking van de samenleving tegen schade van overstromingen en cyberincidenten een brede aanpak vergt, waarin zowel overheid als verzekeraars een rol hebben In de Verenigde Staten en in Europa zijn inmiddels oproepen gedaan door verzekeraars en diverse andere belanghebbenden om publiek-private samenwerkingen op te zetten, waarbij de overheid garant staat voor schades die de verzekerbaarheid overtreffen. Momenteel zijn in diverse landen zulke samenwerkingen al aanwezig voor bijvoorbeeld het (her)verzekeren van terroristische aanslagen. Deze samenwerkingen rond terrorismeschade zijn opgezet na de aanslag op het World Trade Center in New York. Nederland heeft hiervoor de Nederlandse Herverzekeringsmaatschappij voor Terrorismeschaden (NHT) opgericht.

RANSOMWARE

Het aantal ransomware aanvallen blijft toenemen. In het eerste half jaar van 2022 zijn er wereldwijd circa 236 miljoen aanvallen geconstateerd. Op het moment dat dit soort dreigingen toenemen neemt de kans toe dat de risico's onbeheersbaar worden en komt de verzekerbaarheid in geding. Dit is begonnen met het uitvoeren van Ddos aanvallen, vervolgens het versleutelen van systemen en data, waardoor bedrijven hun productie dienden stil te leggen, gevolgd door het stelen van data en dreigen deze openbaar te maken als er geen losgeld wordt betaald.
De nieuwste ontwikkelingen, onder ander gedreven door de oorlog in Oekraïne, is Wiperware. Hierbij wordt data en/of software volledig vernietigd. Ook wordt de horizontale bedrijfsketen aangevallen door het afpersen van IT-bedrijven. Hackers dreigen hun klanten aan te vallen als er geen losgeld wordt betaald en tenslotte is de verwachting dat binnenkort de eerste Killerware wordt verspreid. Hierdoor kunnen mensen - als er niet wordt betaald - ernstig worden verwond of zelfs gedood, enkel door het overnemen van software besturingen. Een voorbeeld is het dreigement; De signalering bij alle spoorwegovergangen uitschakelen waardoor het treinverkeer stil komt te staan.

Veel bedrijven kiezen eieren voor hun geld en betalen alsnog losgeld. Dit om weer zo snel mogelijk operationeel te zijn en de schade door de bedrijfsonderbreking te minimaliseren. Wereldwijd heeft de verzekeringsmarkt hierop gereageerd door premies flink te verhogen en voorwaarden aan te scherpen. Een voorbeeld hiervan is het delen van het risico met de

verzekerde. Laatstgenoemde krijgt dan een bepaald percentage van de schade vergoed of er wordt een limiet ingesteld. Ook de acceptatievoorwaarden zijn flink aangescherpt. Een voorbeeld daarvan zijn de preventie-eisen die door veel verzekeraars worden afgedwongen zoals Multi Factor Authenticatie (MFA), Offline back-ups en Endpoint Detectie & Response systemen.

Internationaal zijn er ook andere ontwikkelingen zoals in de Verenigde Staten waar een aantal verzekeraars gezamenlijk data verzamelen om meer concrete risicomitigerende maatregelen te kunnen delen binnen de verzekeringsindustrie (CyberAcuView). In delen van Europa bieden sommige verzekeraars geen dekking meer voor het betalen van losgeld of trekken zich terug uit de markt of beperken zich tot specifieke doelgroepen.

Het vergoeden van losgeld is niet vanzelfsprekend. Niet alle cyberverzekeringen bieden hier dekking voor en als het al gedekt is zijn er belangrijke voorwaarden. Het moet ingezet worden als het laatste redmiddel. De cyberverzekering biedt eerst de nodige service om bijvoorbeeld na de hack nog back-ups tevoorschijn te halen. Als dat allemaal niet lukt en de verzekerde kiest om losgeld te betalen, omdat zijn bedrijf stilstaat of gevoelige informatie dreigt te verliezen, kan de verzekerde dit vergoed krijgen door de verzekeraar.

Ook overheden roeren zich. The White House heeft een "Counter Ransomware Initiative" georganiseerd en hiervoor 36 landen uitgenodigd, waaronder Nederland. In Frankrijk is een wet aangenomen die in maart 2023 in werking is getreden over het betalen van losgeld. Franse bedrijven mogen in het uiterste geval losgeld betalen, maar moeten dit dan verplicht melden bij de overheid. In andere landen, waaronder Nederland, zijn er ook discussies of het verzekeren van losgeld verboden moet worden. Met als argument dat het niet wenselijk is om criminaliteit te faciliteren. De Nederlandse overheid pleit er in alle gevallen voor dat aangifte wordt gedaan van cybercriminaliteit, zodat de opsporingsdiensten gericht aan de slag kunnen. Het Verbond van Verzekeraars ondersteunt deze oproep.

Het Verbond van Verzekeraars vindt een verbod op het verzekeren van losgeldbetaling niet effectief, zeker als dat alleen door Nederland wordt ingevoerd. Bedrijven zullen dan mogelijk uitwijken naar andere landen. Een dergelijk verbod in Nederland alleen zal overigens niet het gewenste resultaat opleveren, aangezien veel bedrijven ook buiten Nederland gevestigd zijn. Ook is het aandeel bedrijven met een cyberverzekering nog altijd klein waardoor de meeste bedrijven die besluiten losgeld te betalen sowieso geen verzekeringsdekking hebben. Het zijn juist de verzekerde bedrijven die, mede door de door de verzekeraar gestelde voorwaarden, relatief goed beschermd zijn en dus een kleinere kans lopen om slachtoffer te worden. Het Verbond van Verzekeraars ziet wel meerwaarde in een meldplicht voor dergelijke losgeldbetalingen, zoals in Frankrijk.

Het betalen van losgeld kan ook onder de sanctiewetgeving vallen. Vanwege het internationale karakter van de meeste verzekeringsmaatschappijen dienen zij vaak rekening te houden met de sanctiewetgeving van meerdere landen. Ook bedrijven die ransomware betalen dienen vooraf te controleren of de criminele organisatie aan wie zij betalen onder de sanctiewetgeving valt, deze staan immers geregistreerd als een terroristische organisatie en verzekeraars mogen en kunnen dan niet uitbetalen.

PRIVACY

Diefstal van data, al dan niet door ransomware aanvallen, neemt nog steeds toe. Zo claimde in december 2022 een hacker gegevens van meer dan 400 miljoen gebruikers van Twitter in handen te hebben. De aandacht van lokale privacy-autoriteiten voor schendingen van de privacywetgeving zoals de Algemene Verordening Gegevensbescherming (AVG) of nationale wetgeving heeft de laatste jaren verhoogde aandacht. Inmiddels zijn er een aantal succesvolle boetes uitgedeeld met name aan de zogenaamde Big Tech bedrijven. De recentelijk boete van circa 400 miljoen euro aan Meta, vanwege het schenden van de AVG-wetgeving, is hier een goed voorbeeld van. De verwachting is dat ook bedrijven lager in de keten verhoogd aandacht gaan krijgen van de privacy-autoriteiten. Vooral Spanje is erg actief in het opleggen van boetes. Circa 30% van de boetes die zijn uitgedeeld in Europa, zijn door de Spaanse autoriteiten uitgedeeld, gevolgd door Italië, Roemenië en Hongarije. Ook de hoogte van de boetes verschilt per land. De Europese privacy-autoriteit probeert hier wat meer consistentie in te krijgen. De verwachting is dat deze actie tot hogere boetes zal leiden. Inmiddels is het aantal boetes, als gevolg van het niet voldoen aan de privacywetgeving, in Europa in 2022 verdubbeld tot een bedrag van 2,9 miljard euro.

In 2021 heeft de Duitse rechter uitspraak gedaan in een zaak waar sprake was van diefstal van persoonsgegevens.. Een klager kreeg €2500 uitbetaald voor diefstal van zijn persoonsgegevens bij een financiële instelling. Dit is een vergoeding voor immateriële schade. De gegevens van de betrokken persoon zijn niet werkelijk misbruikt, maar het feit dat dat wel zou kunnen gebeuren was voldoende voor een schadevergoeding op basis van de Duitse interpretatie van de privacywetgeving. Dit zou wel eens een paradigma shift kunnen zijn en leiden tot veel hogere vergoedingen voor gedupeerden, vooral als dergelijke schadevergoedingen in collectieve schadeclaims worden toegewezen.

De toename van diefstal van persoonsgegevens leidt ook tot scherpere wetgeving. Dit om organisaties te dwingen meer aandacht te schenken aan een goede beveiliging van data. Zo is bijvoorbeeld in Australië een wet aangenomen die het mogelijk maakt om bedrijven, die vaker zijn getroffen bij diefstal van data, verhoogde boetes op te leggen tot een bedrag van 33,7 miljoen Australische dollars. Het aantal boetes dat wordt opgelegd door de privacy-autoriteiten neemt nog steeds toe. Op dit moment zijn het – zoals hierboven genoemd - met name de Big Tech bedrijven zoals Meta en TikTok die onder verhoogde aandacht staan. De verwachting is dat de komende jaren ook ander branches een verhoogde aandacht krijgen van de lokale privacy autoriteiten.

VERGROTEN INZICHTEN IN DIGITALE RISICO'S

Verder moet het inzicht in de risico's en de gevolgen worden vergroot, waarvoor het verzamelen en delen van informatie essentieel is. Omdat het verzekeren van cyberrisico's nog niet vanzelfsprekend is, worden er relatief weinig verzekeringen afgesloten en is ook het aantal verzekerde incidenten klein ten opzichte van de traditionele verzekeringen zoals brand- en motorrijtuigverzekeringen. Hierdoor is het voor verzekeraars lastig om de risico's adequaat in te schatten en te beprijzen. Inmiddels heeft SIVI samen met het Verbond van Verzekeraars een gezamenlijke taxonomie ontwikkeld voor de indeling van schadeoorzaken cyber. Partijen in de verzekeringsketen is gevraagd om deze indeling in hun systemen op te nemen en bij te houden, zodat de afzonderlijk verzamelde gegevens vergelijkbaar en optelbaar zijn.

Insurance Europe, de Europese koepelorganisatie van verzekeraars, pleit al geruime tijd in Brussel voor meer systematisch verzamelen en delen van gegevens over cyberincidenten, onder andere bij de verplichte meldingen in het kader van de Algemene Verordening Gegevensbescherming (AVG). Om dit te faciliteren heeft Insurance Europe zelfs een template

ontwikkeld en pleit het voor toegang ook voor verzekeraars van aldus verzamelde en geanonimiseerde gegevens. Helaas is dit nog altijd niet gerealiseerd..

Het Verbond van Verzekeraars bepleit dat verzekeraars toegang krijgen tot geanonimiseerde of geaggregeerde gegevens die de Autoriteit Persoonsgegevens al verzamelt vanwege de meldingsplicht bij datalekken. Door rond cyberincidenten meer en gestructureerd gegevens te gaan verzamelen en te ontsluiten, kan (onder andere door verzekeraars) beter inzicht worden verkregen in incidenten, ook in de context van genomen maatregelen. Zo kan antwoord worden gevonden op vragen als: wat er is gebeurd, mate van schade en mate van preventie. Daarmee kunnen verzekeraars cyberrisico's beter inschatten en verzekerings-producten passender maken.

CONCLUSIE

Om systeemrisico's in het digitale domein het hoofd te bieden en deze beter verzekerbaar te maken moet er veel gebeuren. Het risicobewustzijn van burgers, bedrijven en organisaties moet verder omhoog en moet aangevuld worden met acties die systemen en ons gedrag daadwerkelijk veiliger maken. De instrumenten die het Digital Trust Center, de Rijksoverheid, maar ook marktpartijen aanbieden moeten verbeterd, uitgebreid en nog nadrukkelijker gepromoot worden. Ook verzekeraars en verzekeringsadviseurs spelen hierin een belangrijke rol. Verder is beter ontsluiten van data over cyberincidenten een essentiële randvoorwaarde voor verdere groei van de cyberverzekeringsmarkt.