SCHADE

Cybercrime verzekeren: wat is verzekerbaar en hoe worden risico's eerlijk gedeeld?

Cybercrime is geen nieuw fenomeen meer. Steeds meer bedrijven en particulieren komen erdoor in de problemen. Waarom spelen schadeverzekeraars niet wat vlotter in op de behoefte aan een verzekering, met name voor particulieren? In dit artikel laat ik zien waar het knelt met de principes van verzekeren, en schijn ik een lichtje over de route naar een adequate premiestelling.

STEEDS GROTER PROBLEEM

Dat cybercrime toeneemt, zien we in de cijfers van de politie: dit jaar al bijna 7.000 aangiftes (tot en met augustus 2020). Met name de laatste jaren stijgt het aantal slachtoffers van cybercriminaliteit steeds harder. Hierdoor wordt de maatschappelijke roep om professionele ondersteuning vanuit verzekeraars steeds groter. De verzekeringsmarkt biedt al dekkingen, maar veel verzekeraars zijn nog zoekende naar welke rol precies voor hen is weggelegd om klanten ook op dit vlak te helpen. Want wat is er verzekerbaar? En hoe stel je daar een goede premie voor vast?

Figuur 1: ontwikkeling aantal geregistreerde cybermisdrijven. Data 2020 t/m augustus.
Bron: data.politie.nl

M. Mattens MSc AAG is werkzaam bij Arcturus BV.

WAT IS VERZEKERBAAR?

Het verzekeren tegen criminaliteit is traditioneel een complexe zaak, omdat je te maken hebt met *moral hazard*: als mensen weten dat ze verzekerd zijn, worden ze mogelijk (iets) onvoorzichtiger. Deze onvoorzichtigheid verhoogt het risico, dus daar kunnen criminelen vervolgens hun geld aan verdienen. Indirect wordt dan een stukje misdaad gefinancierd met verzekeringsgelden.
Het meest bekende voorbeeld hiervan is inbraakrisico. Woninginbraken zijn echter al sinds jaar en dag onder de inboedeldekking verzekerd, dus blijkbaar valt het moral-hazardeffect hier wel mee: de gemiddelde verzekerde beveiligt zijn woning niet veel slechter dan de gemiddelde onverzekerde.

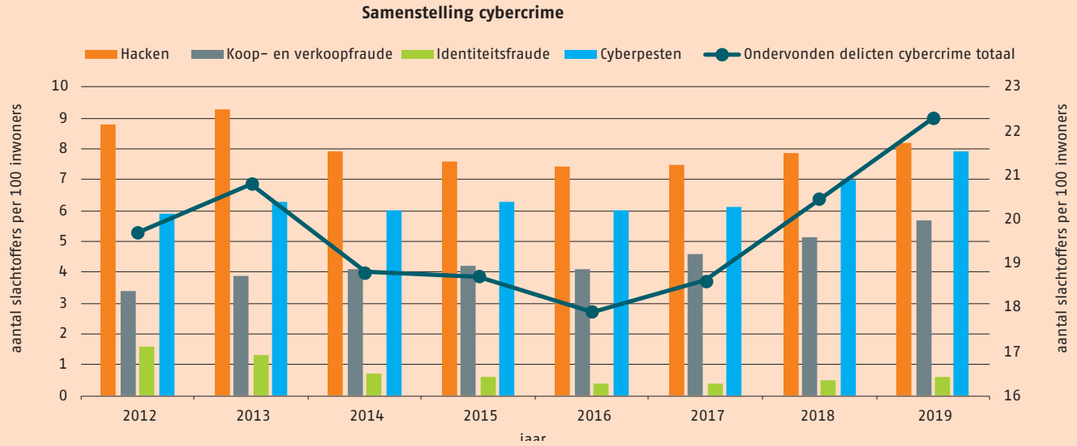
Bij cybercrime speelt moral hazard ook een rol. Een verschil met woninginbraak is echter dat cybercriminelen eigenlijk elk bedrag aan losgeld kunnen vragen wat ze willen, terwijl er uit een huis maar zoveel te stelen is als de inbrekers kunnen tillen. Hierdoor kan de schadelast veel hoger oplopen dan bij de traditioneel gedekte vormen van criminaliteit. Als verzekeraars bereid zouden zijn hieraan mee te betalen, kan er een prikkel ontstaan voor de cybercriminelen om het gevraagde losgeld structureel verder te verhogen. Een verzekerde is dan een véél interessanter potentieel doelwit geworden dan de onverzekerde. Een verzekeraar wil en mag natuurlijk niet misdaad lonend maken.

De eerste verzekeraars die nu een cyberdekking aanbieden voor particulieren (bijvoorbeeld standaard in de inboedelverzekering), bieden daarom géén dekking aan voor de betaling van losgeld, maar voor ondersteuning door cyberexperts bij een (computer)virusinfectie. Daarnaast wordt er sterk ingezet op preventie: tips, tricks en recente ontwikkelingen op het gebied van cybercriminaliteit worden door de verzekeraar met de klant gedeeld. Hierdoor is men beter in staat om problemen te voorkomen en wordt de verzekerde niet aan zijn lot overgelaten mocht het een keer misgaan. Bij schade wordt *salvage* geboden door cyberexperts; zij kunnen mogelijk een deel van de schade oplossen of erger voorkomen. Immers zijn niet alle virusinfecties zodanig dat de computer, of de data en foto's niet meer kunnen worden 'teruggewonnen' van de hackers.

Daarnaast zijn er verzekerde uitkeringen voor online oplichting door webshops en hacken van bankrekeningen en creditcards. Bij deze risico's lijkt moral hazard minder relevant.

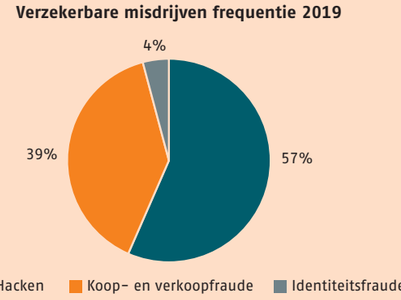
WAT IS EEN ADEQUATE PREMIE?

Het risico is niet stabiel, maar statistieken zijn wel degelijk nodig om het risico in te schatten. Hoe ontwikkelt de frequentie van verschillende soorten cybercrime zich? Dit wordt gemeten in De Veiligheidsmonitor, een tweejaarlijks uitgevoerd bevolkingsonderzoek door het CBS. In Figuur 2 is dit uitgesplitst naar de vier hoofdcomponenten weergegeven.



Figuur 2: Aantal delicten per 100 inwoners naar soort cybercrime.
* 2018 is geïnterpoleerd i.v.m. missende data CBS.

Het bevolkingsonderzoek geeft aan dat de 4700 gemelde misdrijven in 2019 (figuur 1) naar schatting slechts het topje van de ijsberg is. Met naar schatting ruim 23 delicten per 100 inwoners in 2019, komt dat neer op een werkelijk aantal van ruim 4 miljoen cyberdelicten per jaar in Nederland. Onder verzekerbare delicten vallen onder meer hacken, koopfraude en identiteitsfraude. Hiervan zijn naar schatting 14,5 delicten per 100 inwoners. De onderverdeling van deze 14,5 delicten naar de drie verzekerbare soorten staat weergegeven in figuur 3.



Figuur 3: procentueel aandeel verzekerbare cybercrimemisdrijven.

Voor 2020 is het waarschijnlijk dat het aantal geregistreerde misdrijven ruim zal verdubbelen ten opzichte van 2019 (figuur 1).

Deze cijfers kunnen met enige voorzichtigheid naar de toekomst worden geëxtrapoleerd. Hiermee wordt een inschatting van de frequentie per cyberrisico afgeleid. Op basis van het maximum dekkingsbedrag en schadesturingsbeleid kan vervolgens ook een schatting worden gemaakt van de gemiddelde schadelast per claim. De combinatie van schadefrequentie en gemiddelde schadelast kan worden gebruikt om een doorsneepremie vast te stellen.

Een ander issue bij criminaliteit is de onvoorspelbaarheid van het risico. Bij cybercrime speelt dit enerzijds door de snelle technologische ontwikkeling, anderzijds door de criminele innovatiekracht. Criminelen zoeken telkens nieuwe wegen zodra virusbeschermers zijn ontwikkeld tegen hun huidige werkwijze. Een adequate risico-opslag voor het ontstaan van deze *unknown unknowns* blijft daarom nodig om het risico voor de verzekeraar te dekken.

PREMIEDIFFERENTIATIE MOGELIJK?

Klantspecifieke risicofactoren zijn nu nog nauwelijks in te schatten. Een doorsneepremie is in een jonge markt een eerste stap, maar er zijn mogelijk goede redenen om op termijn naar een gedifferentieerd stelsel toe te groeien. Hierbij valt onder meer te denken aan:

- Preventie: sommige mensen hebben geïnvesteerd in goede antivirussoftware;
- Leeftijd: risicobewustzijn en kennis is niet gelijk verdeeld over de leeftijdsgroepen, en sommige leeftijdsgroepen zijn een meer geliefd doelwit van cybercriminelen;
- Gedrag: sommige mensen zoeken relatief vaker veel meer risico, bijvoorbeeld het downloaden van bepaalde (illegale) bestanden;
- Baan of functie: sommige mensen vervullen (zakelijke) functies waardoor ze relatief makkelijk benaderbaar zijn voor criminelen en/of vervullen (zakelijke) functies waardoor ze een aantrekkelijk target worden;
- Dekkingen op maat: onderdelen die apart geprijsd worden.

Hoe dynamisch de wereld van cybercriminaliteit ook is, de sleutel tot het goed kunnen inschatten van risico's is data. Al doende leert men: verzekeraars die het eerste starten met het verzekeren van cyberrisk zullen als eerste de data hebben om tot goede premiedifferentiatie te kunnen komen. Door deze schadelast goed uit te splitsen naar soorten schaden (inzet van experts en schadevergoedingen) en dit te koppelen aan risicokenmerken van de populatie, zijn traditionele actuariële pricing-methodieken zoals GLM zeer bruikbaar. Premiedifferentiatie wordt daardoor op termijn mogelijk.

DE VERZEKERAAR HEEFT IETS TE BIEDEN

Al met al gaan ontwikkelingen op het gebied van cybercriminaliteit dus heel snel. Nu er enkele schapen over de dam zijn lijkt het een kwestie van tijd voordat andere verzekeraars ook deze markt zullen willen gaan betreden. Voor veel mensen is het namelijk een grote nachtmerrie om gegijzeld te worden door hackers. Goede ondersteuning zal daarom best wat waard zijn. Gelukkig zullen ook in dit veld traditionele actuariële pricingmethoden te gebruiken zijn en zal het daarom niet lang duren voordat de cyberverzekeringsmarkt een volwassen markt is.

Blijf rekening houden met criminele innovatiekracht! ■