Catastrofale cyberrisico's
Een toenemende zorg

CHUBB®

Cyberincidenten kunnen schade veroorzaken die niet beperkt wordt door tijd of locatie.

Naarmate de wereld verder digitaliseert, nemen de frequentie, ernst en de geraffineerdheid van cyberincidenten toe, evenals de afhankelijkheid van technologie. Kwetsbaarheden en risico's ontwikkelen zich in hoog tempo door de toegenomen interconnectiviteit. Dit brengt enorme en groeiende systeemrisico's met zich mee die niet gemakkelijk te detecteren of te beheersen zijn. Door de combinatie van deze diverse risicoaspecten met mogelijk ernstige en wijdverspreide consequenties, is een cyberramp niet ondenkbaar.

Net als een pandemie kunnen cyberincidenten schade veroorzaken die niet beperkt wordt door tijd of locatie. Het is niet langer theoretisch: cybercriminelen hebben al laten zien dat ze in staat zijn om de leveranciersketen van bedrijven overal ter wereld te verstoren en kritische infrastructuur plat te leggen. Een voorbeeld hiervan is de recente aanval waardoor Colonial Pipeline zijn toevoerleidingen voor brandstof naar de oostkust van de Verenigde Staten moest sluiten. Door de miljarden dollars aan economische schade die recente cyberincidenten aanrichtten, is het niet moeilijk je een voorstelling te maken van de gevolgen die een catastrofale aanval zou hebben voor de financiële situatie van de verzekeringssector.

In tegenstelling tot eerdere, plotseling optredende catastrofale gebeurtenissen, zijn we in het geval van cyber allemaal getuige van de toenemende risico's. Deze waarschuwing vooraf biedt een kans om uw cyberverdediging en financiële waarborgen te verbeteren voordat er zich daadwerkelijk een ramp voordoet.

De cyberverzekering wordt 'volwassen'

Het groeiende aantal cyberverzekeringen betekent niet alleen dat steeds meer bedrijven zich tegen cyberrisico's beschermen, maar ook dat de totale belasting voor de verzekeringssector groeit.

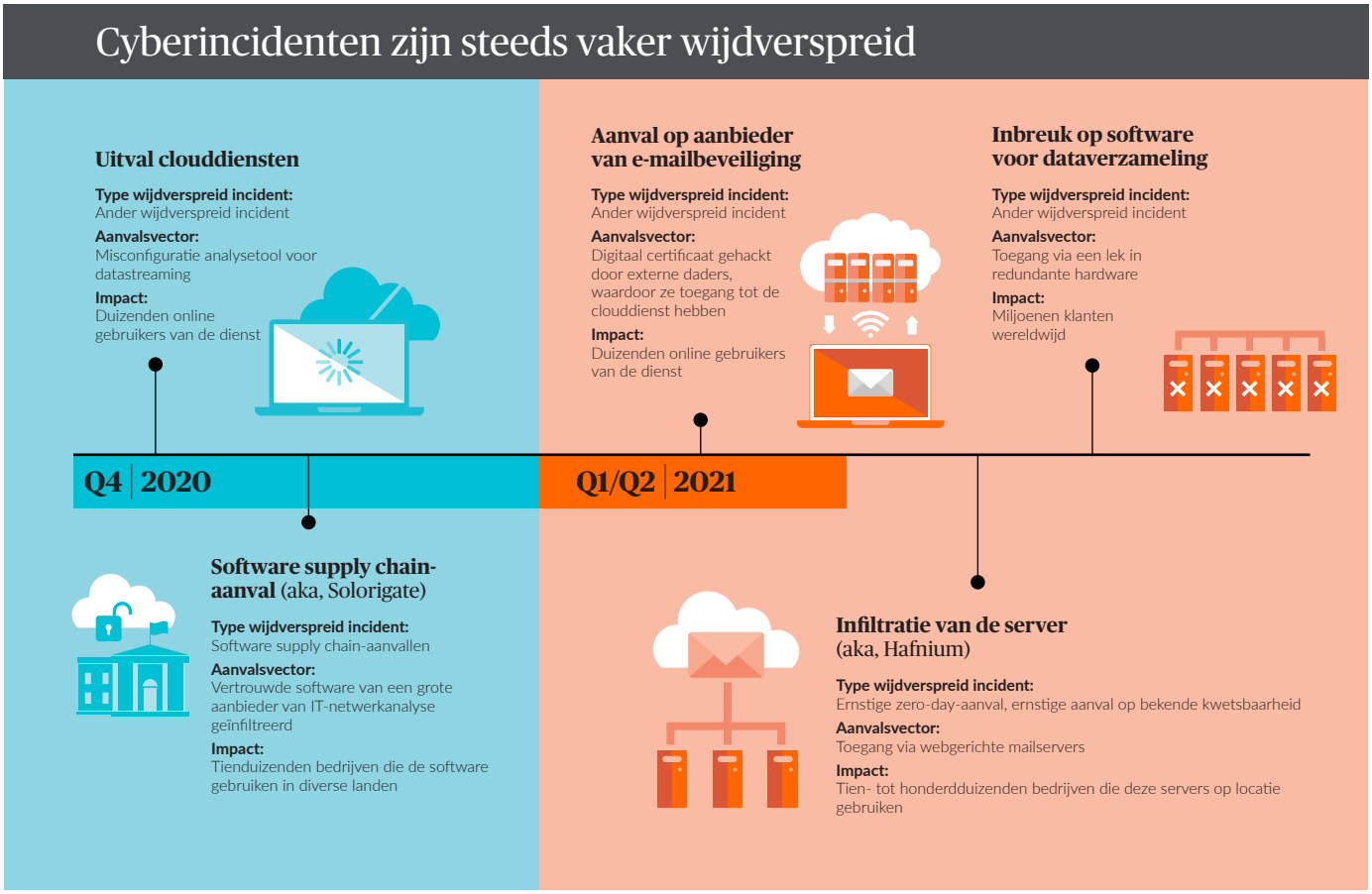
De beloftes van cyberverzekeringen zijn in de afgelopen jaren veelvuldig ingelost: verzekeraars vergoeden de schade na grote cyberincidenten en bieden zo bescherming aan een groot aantal bedrijven wereldwijd.

Tegenwoordig zorgen de belangrijkste dekkingselementen - incidentrespons-kosten, eigen schade en aansprakelijkheid jegens derden, ervoor dat een groot deel van het risico wordt overgedragen en dat er voor organisaties van elke omvang en uit elke sector oplossingen voor risk management bestaan. Daarnaast blijken diensten voor cyber risicomanagement waardevol om bedrijven te helpen risico's te verkleinen en de bescherming van hun technologie aan de voorkant te verbeteren. Incidentrespons-teams blijken effectief in het snel weer online brengen van bedrijven na een cyberincident.

Nu bedrijven steeds vaker kiezen voor een cyberverzekering zijn meer bedrijven beschermd.

Tegelijkertijd hebben bedrijven in de afgelopen jaren hun vermogen verbeterd om weerstand te bieden aan cyberaanvallen en daarvan te herstellen (cyber weerbaarheid). In 2020 meldde 53% van de ondervraagde IT- en beveiligingsprofessionals van overal ter wereld dat hun organisaties een zeer hoog niveau van cyber weerbaarheid kennen, tegen 35% in 2015.

Terwijl cyberverzekeringen duidelijk een steeds belangrijkere rol spelen in het beheersen van cyberrisico's voor organisaties, is het vermogen van verzekeraars om alle potentiële schade op de lange termijn op te vangen, minder zeker.



Toenemende risico's en impact

In een tijdsbestek van 100 dagen, tussen december 2020 en maart 2021, vonden diverse grote aanvallen plaats. Ze troffen uiteenlopende doelen, van supply chain software en e-mailbeveiliging tot data-servers en gemeenschappelijke infrastructuur.

Ondanks dat organisaties zich steeds bewuster zijn van cyberrisico en de gevolgen ervan, nemen het aantal en de ernst van incidenten en bedreigingen alleen maar toe.

In 2020 werden er meer dan 18.000 nieuwe kwetsbaarheden in software gemeld. Dat is bijna drie keer zoveel als in 2015 en dit aantal blijft gestaag toenemen. In 2020 werden bovendien bijna 1,2 miljoen nieuwe malware-bedreigingen ontdekt, meer dan het dubbele van 2015. Bij meer dan 85% van de geslaagde veiligheidsinbreuken in 2020 was er sprake van een menselijke factor, zoals social engineering.

Hoewel tactieken zoals ransomware steeds gebruikelijker en kostbaarder worden, zijn het vooral inbreuken op zakelijk e-mailverkeer en datalekken die ervoor zorgen dat de frequentie van cyberincidenten inmiddels ongekend hoog is. Hierin speelt de COVID-19 pandemie en het toenemende aantal thuiswerkers een belangrijke rol.

Cyberincidenten hebben bovendien een meer wijdverspreide impact. In een tijdsbestek van 100 dagen, tussen december 2020 en maart 2021, vonden diverse grote aanvallen plaats. Ze troffen uiteenlopende doelen, van supply chain software en e-mailbeveiliging tot dataservers en gemeenschappelijke infrastructuur. Wereldwijd werden er meer dan 100.000 organisaties door deze incidenten geraakt.

Een van deze incidenten was Solorigate, een massale supply chain-aanval, waarbij een update van vertrouwde software voor netwerkanalyse een kwaadaardige code bevatte. Zo'n 20.000 bedrijven en overheidsinstanties werden getroffen. Het duurde bijna acht maanden voordat de aanval werd opgemerkt.

Bij een ander incident gebruikte Hafnium, een groep door de overheid gesteunde hackers en criminele organisaties, een tot dan toe onbekende ('zero-day') kwetsbaarheid in een veelgebruikt programma om toegang te krijgen tot de bedrijfsservers van mogelijk honderdduizenden bedrijven.

Spraakmakende incidenten voeren de spanning op

Wanneer zal er zich een echt catastrofaal cyberincident voordoen dat zowel wijdverspreid als destructief is?

Hoe ernstig en kostbaar incidenten als Solorigate en Hafnium ook waren, het had nog veel erger kunnen zijn. Het voornaamste motief voor deze aanvallen bleek spionage te zijn. Maar als het de bedoeling was geweest om kritische data of andere informatie te stelen of te vernietigen, dan zouden de economische gevolgen enorm zijn geweest. Volgens Kevin Mandia, CEO van cybersecuritybedrijf Fire Eye, die getuigde voor de onderzoekscommissie van de Amerikaanse Senaat, hadden de daders achter de Solorigate-aanval zowel de vereiste toegang als de benodigde capaciteiten om een grootschalige verstoring teweeg te brengen6.

Een ander voorbeeld is de NotPetya-aanval in 2017. Hierbij werd een fiscale softwaretool met de naam M.E.Doc besmet met malware. Hoewel M.E.Doc vrijwel uitsluitend in Oekraïne werd gebruikt, trof de malware grote bedrijven over de hele wereld. Dit leidde uiteindelijk tot een geschatte schade van $ 10 miljard. Sommige getroffen bedrijven leden meer dan $ 100 miljoen schade. Als dit type destructieve malware tijdens de Solorigate of Hafnium-aanvallen was ingezet, zou de gecombineerde economische schade exponentieel hoger zijn geweest dan die van NotPetya.

In hetzelfde jaar raakte de WannaCry ransomware-aanval wereldwijd meer dan 200.000 computers. Gelukkig werd hierbij een bekende kwetsbaarheid gebruikt waarvoor al een patch beschikbaar was, dus de meeste gebruikers waren er immuun voor. Als er in plaats daarvan een zero-day kwetsbaarheid zou zijn gebruikt, zou de impact veel wijdverspreider en ernstiger zijn geweest.

We hebben dus al de nodige wijdverspreide incidenten meegemaakt, zoals Solorigate en Hafnium, en destructieve incidenten, zoals NotPetya en WannaCry. De potentiële schade wordt steeds groter. Wanneer zullen we een catastrofaal cyberincident zien, dat zowel wijdverspreid als destructief is?

Potentiële catastrofale cyberrisico's

Doordat organisaties en consumenten steeds afhankelijker zijn van technologie, en de interconnectiviteit tussen technologieën en partners blijft toenemen, is er een situatie ontstaan waarin cyberrisico's zich exponentieel vermenigvuldigen. De volgende risicotypes kunnen, vooral in combinatie met elkaar, mogelijk catastrofale gevolgen hebben.

Ernstige aanvallen op bekende kwetsbaarheden:

Gemiddeld worden er elke dag ongeveer vijftig nieuwe software-kwetsbaarheden gepubliceerd. Als die niet verholpen zijn met een patch, kunnen ze misbruikt worden voor een aanval. Ongeveer vijftien procent van de kwetsbaarheden zijn ernstig, omdat ze gemakkelijk aan te vallen zijn en vanwege gebrek aan toegangscontroles op afstand benaderd kunnen worden. Hierdoor kunnen ze aanzienlijke schade veroorzaken. Aangezien bekende ernstige kwetsbaarheden gemakkelijk op te sporen zijn door criminelen, lopen bedrijven die nalaten ze te herstellen een groot risico hiervan het slachtoffer te worden.

Ernstige zero-day-aanvallen:

Zero-day software-kwetsbaarheden zijn alleen bekend bij cybercriminelen maar nog niet bij anderen. Deze kwetsbaarheden zijn een grote bron van zorg omdat ze gemakkelijk aan te vallen zijn, mogelijk ernstige gevolgen hebben, en vaak onvoldoende beschermd zijn. In andere woorden: zelfs bedrijven met goed georganiseerde programma's voor cyberrisicomanagement kunnen blootgesteld zijn aan zero-day-aanvallen.

Software supply chain-aanvallen:

Software supply chain-aanvallen zijn eigenlijk een Trojaans paard waarmee kwaadwillende partijen systemen binnendringen via vertrouwde, gecertificeerde software. De Solorigate-aanval liet zien dat de criminelen bijzonder geraffineerd te werk gingen door software-ontwikkelingstechnieken in te zetten die overal in de IT-sector gebruikt worden. Deze aanvallen, waarvan er veel lijken te worden aangestuurd of gesteund door buitenlandse overheden, zullen naar verwachting aanhouden en mogelijk in ernst en aantal toenemen. Geopolitieke spanningen, vooral tussen het Westen en zijn tegenstanders, zullen ervoor zorgen dat de dreiging van deze aanvallen in de toekomst steeds groter wordt.

Uitval van infrastructuur:

Aanvallen en andere cyberincidenten waarbij infrastructuur betrokken is, kunnen grootschalige consequenties hebben. In mei 2021 vond er bijvoorbeeld een aanval plaats op Colonial Pipeline, de leverancier van benzine die de oostkust van de Verenigde Staten bedient. Buitenlandse cybercriminelen gebruikten een ransomware-aanval om infrastructuur plat te leggen. Het gevolg was dat de pijpleiding een aantal dagen was afgesloten, waardoor er 45 procent minder brandstof geleverd kon worden aan miljoenen Amerikaanse burgers en bedrijven in diverse staten. Uitval van infrastructuur is een uniek risico omdat het niet alleen een gevolg kan zijn van een cyberaanval, maar ook van systeemstoringen, menselijke fouten, programmeerfouten, of andere niet-kwaadaardige cyberincidenten.

Andere wijdverspreide gebeurtenissen:

Bepaalde type cyberaanvallen kunnen tegelijkertijd, al dan niet automatisch tegen een groot aantal slachtoffers worden ingezet. Het internet en bepaalde telecommunicatiediensten zijn inmiddels cruciale maatschappelijke infrastructuur, waardoor uitval een enorm risico vormt. Soms is een telecombedrijf de enige aanbieder in een middelgrote stad. In andere gevallen worden sommige clouddiensten op zulke grote schaal gebruikt dat de uitval ervan gevolgen heeft voor de activiteiten van duizenden of miljoenen bedrijven. Elke aanvalstechniek die zo massaal kan worden ingezet, kan een catastrofaal cyberincident veroorzaken.

Ransomware-aanvallen:

Hoewel ze niet catastrofaal van aard zijn, worden ransomware-aanvallen, waarbij de elektronische bestanden of informatie van bedrijven of individuen in gijzeling worden gehouden totdat er losgeld is betaald, tegenwoordig met industriële efficiëntie uitgevoerd. Losgeldeisen begonnen ooit bij duizenden dollars maar zijn nu omhooggeschoten naar tientallen miljoenen, waarbij criminelen zich richten op organisaties van elke omvang.

Cyberweerbaarheid verbeteren

Het is belangrijker dan ooit dat organisaties zich voorbereiden op een mogelijke cybercatastrofe.

Nu de cyberrisico's toenemen, ofwel door de aard van de bedrijfsactiviteiten en IT-omgevingen, of criminelen die kwetsbaarheden misbruiken, is het belangrijker dan ooit dat organisaties zijn voorbereid op een mogelijke cybercatastrofe.

Dit begint bij het in kaart brengen van de specifieke risico's waaraan de organisatie is blootgesteld, op basis van de mogelijk catastrofale cyberincidenten die in deze paper besproken worden. Vervolgens moeten de noodzakelijke middelen worden aangewend om de bescherming tegen en de veerkracht na cyberincidenten te verbeteren. Gedeelde aanbieders van IT-diensten vormen een aanzienlijk systeemrisico voor organisaties. Uitgebreid due diligence-onderzoek naar deze aanbieders is daarom een must. Ook moet de redundantie en weerbaarheid rond deze aanbieders worden opgebouwd, naast een beoordeling van de contractvoorwaarden.

Ook zouden organisaties volop gebruik moeten maken van de expertise die hun verzekeringsmakelaar of -agent en hun cyber-verzekeraar in huis hebben. Hoewel IT- , risk management- en bedrijfscontinuïteitsteams vertrouwen kunnen hebben in hun cyberbescherming en incidentresponsmaatregelen, is geen enkele organisatie ooit volledig beschermd tegen alle mogelijke cyberincidenten, vooral de catastrofale.

Veel verzekeraars bieden een heel pakket aan preventiediensten om organisaties te helpen zich beter voor te bereiden op cyberaanvallen. Denk hierbij aan de beoordeling van hun responsvoorbereiding, het benchmarken van hun beveiligingssysteem, het testen van de kwetsbaarheid van netwerken, en het simuleren van veelvoorkomende aanvallen. Organisaties moeten ook voorbereid zijn op ingrijpen wanneer zich een cyberincident voordoet. Een incidentresponsteam van de verzekeraar kan helpen de schade van dergelijke gebeurtenissen te beperken en de organisatie zo snel mogelijk weer volledig operationeel te laten zijn. Deze diensten kunnen het verschil maken tussen het tenauwernood overleven van een groot cyberincident en de bedrijfsactiviteiten met vertrouwen voortzetten.

Voortschrijdende oplossingen

Cyberverzekeringen kunnen net als brandverzekeringen te maken krijgen met catastrofale incidenten.

Op wereldschaal kunnen rampzalige cyberincidenten de handel een halt toeroepen en cruciale infrastructuur lamleggen. Net als bij de coronapandemie is het noodzakelijk dat de overheid en private sector op belangrijke terreinen samenwerken. Denk aan het openbaar maken en melden van cyberincidenten om de consistentie van data te verbeteren, en het vaststellen van juridische kaders om cybercriminelen te ontmoedigen en straffen

De toename van zowel de frequentie als ernst van cyberincidenten is voor verzekeraars aanleiding om hun premies en voorwaarden te herzien. Er zijn nieuwe oplossingen nodig om een stabiele markt voor cyberverzekeringen te kunnen garanderen waarbij men rekening houdt met de mogelijke schaal van catastrofale risico's. Van nauwe samenwerking met de overheid tot het productaanbod van individuele verzekeraars. Voor de verzekeringssector ligt de grootste uitdaging in het samenstellen van polissen die dekkingszekerheid en voldoende bescherming bieden, en die helpen zowel individuele als catastrofale cyberincidenten voor klanten en verzekeraars te beheersen.

Verzekeraars bieden bij traditionele schadeverzekeringen aparte dekking voor catastrofes zoals overstromingen en aardbevingen, om deze risico's transparant te kunnen prijzen en ze te kunnen monitoren. Deze aanpak bevordert de algemene marktstabiliteit en de beschikbaarheid van dekking. Want hoewel veel van de grote aardbevingen, overstromingen en orkanen in de afgelopen vijftig jaar van grote invloed waren op de inkomsten van schade- en ongevallenverzekeraars, leidden ze zelden tot insolventie. De verzekeringssector bleef daardoor veerkrachtig en stabiel voor verzekeringnemers, zelfs in de nasleep van catastrofale gebeurtenissen.

Cyberverzekeringen kunnen net als schadeverzekeringen te maken krijgen met catastrofes. Daarom zou de structuur van cyberverzekeringen meer moeten lijken op die van een traditionele schadeverzekering. De verzekeringssector moet proactief zijn in het apart aanbieden van dekking voor catastrofale gebeurtenissen naast de hoofddekking. Catastrofes mogen niet van de dekking worden uitgesloten maar moeten juist duidelijker gedefinieerd worden, zodat de premievaststelling voor deze dekking transparant verloopt, rekening houdend met de juiste acceptatiecriteria, verzekerde bedragen en eigen risico. Deze benadering zal de cyberverzekeringssector in staat stellen om verzekeringnemers innovatieve oplossingen te bieden, maar garandeert ook de stabiliteit van de markt op de lange termijn.

Over de schrijver

Michael Kessler is Vice President bij Chubb Group en Division President van Chubb's Global Cyber Risk Practice. In deze functie overziet hij alle facetten van de divisie, waaronder de strategie- en productontwikkeling en business development, de verzekerings- en serviceactiviteiten, en de algemene winstgevendheid. De heer Kessler heeft dertig jaar ervaring in de verzekeringssector en actuarieel advies, en was eerder onder andere Chief Reinsurance Officer (2016-2021) bij Chubb. Hij is lid van de American Academy of Actuaries en Fellow bij de Casualty Actuarial Society.

Voetnoten

1. Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market (2021). Geraadpleegd via www.gao.gov/products/gao-21-477
2. Cyber Resilient Organization Report (2020). Geraadpleegd via www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/
3. National Institute of Standards and Technology's National Vulnerability Database. Geraadpleegd via https://nvd.nist.gov/vuln/search
4. V-TEST Institute (2021). Geraadpleegd via www.av-test.org/en/statistics/malware/
5. Verizon 2021 Data Breach Investigations Report (2021). Geraadpleegd via https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf
6. U.S. Senate Select Committee on Intelligence (2021). Geraadpleegd via www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary
7. NIST Security Vulnerability Trends in 2020: An Analysis (2021). Geraadpleegd via www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

Over Chubb
Chubb is de grootste beursgenoteerde schadeverzekeringsmaatschappij ter wereld. Chubb is gevestigd in 54 landen en gebieden, en biedt een diverse groep zakelijke en particuliere klanten schade- en aansprakelijkheidsverzekeringen, persoonlijke ongevallenverzekeringen, aanvullende verzekeringen bij ziekte, herverzekeringen en levensverzekeringen. Onze expertise als verzekeraar stelt ons in staat risico's op een verantwoorde manier te beoordelen, aanvaarden en beheren. Onze klanten kunnen rekenen op een eerlijke behandeling en snelle uitbetaling. Chubb onderscheidt zich door haar brede aanbod van producten en diensten, uitgebreide distributiemogelijkheden, uitzonderlijke financiële kracht en wereldwijde lokale aanwezigheid. Moederbedrijf Chubb Limited is genoteerd aan de New York Stock Exchange (NYSE: CB) en maakt deel uit van de S&P 500-index. Chubb heeft hoofdkantoren in Zürich, New York, Londen, Parijs en andere locaties. Wereldwijd zijn er ongeveer 31.000 medewerkers in dienst. Kijk voor meer informatie op www.chubb.com.

Ga voor meer informatie over Chubbs ervaring en expertise met cyber risk-management naar www.chubb.com/nl/cyber.

Chubb. Insured.℠

NL-USE-8127-MD 10/2022