Cyber systeemrisico's/ Product update

FAQ's voor tussenpersonen

CHUBB

April 2022

Chubb zet zich in om zijn leidende positie in de markt te behouden door richting en structuuir te bieden die zorgt voor stabiliteit op de lange termijn.

De frequentie en ernst van de cyberincidenten waar we momenteel mee te maken hebben, is voor veel verzekeraars, waaronder Chubb, aanleiding om hun premies en voorwaarden te herzien. In de afgelopen maanden werden software leveranciersketens en aanbieders van e-mailbeveiliging, dataservers en infrastructuur het doelwit van wijdverspreide cyberincidenten. Deze cyberaanvallen - van uiteenlopende aard - hadden catastrofale gevolgen kunnen hebben.

Chubb blijft verzekeringsnemers en distributiepartners die dekkingscomponenten bieden die ze van ons gewend zijn. Daarnaast herzien wij onze voorwaarden met betrekking tot dekking van wijdverspreide incidenten. Samen met brancheverenigingen en overheden werken wij aan manieren om partijen zoveel mogelijk zekerheid te kunnen bieden.

Impact op verzekering-nemers en tussenpersonen

Met nieuwe oplossingen voor partners zorgt Chubb op de lange termijn voor meer stabiliteit en groei binnen de cyberverzekeringsmarkt.
Door een duidelijke omschrijving van de dekking voor systeemrisico's zullen tussenpersonen beter in staat zijn hun klanten op dit gebied te adviseren.
Daarnaast kan gemakkelijker worden ingegaan op klantspecifieke behoeften, bijvoorbeeld op het gebied van schade-behandeling en risk engineering services.
De nieuwe benadering berust op bewezen concepten die al sinds jaar en dag van toepassing zijn op brand- en catastrofe-verzekeringen.
Veel tussenpersonen zullen hier dan ook al ervaring mee hebben. Na verloop van tijd zou een gestructureerde aanpak van het kwantificeren van cyberrisico's moeten resulteren in meer capaciteit voor cyberverzekeringen op de markt.

De markt voor cyberrisico's

Wat is de aanleiding voor de huidige strategiewijziging voor cyberverzekeringen?

Het aantal cyberincidenten en -bedreigingen neemt toe en de aard ervan verandert. In 2020 werden meer dan 18.000 nieuwe kwetsbaarheden in software gemeld, bijna drie keer zoveel als in 2015 en dit aantal blijft gestaag toenemen. [1] Ondertussen werden er in 2020 bijna 1,2 miljoen nieuwe malware-bedreigingen ontdekt, meer dan het dubbele van 2015. [2] Terwijl aanvallen als ransomware steeds gebruikelijker en schadelijker worden, zijn het vooral inbreuken op zakelijk e-mailverkeer en datalekken die ervoor zorgen dat de frequentie van cyberincidenten inmiddels ongekend hoog is. Hieraan ligt vooral het toegenomen thuiswerken ten grondslag. De toegenomen frequentie en ernst van dergelijke cyberincidenten zet de schadelast van verzekeraars onder druk terwijl de blootstelling van systemen aan mogelijke rampen steeds groter wordt.

Delen andere organisaties het standpunt van Chubb over het onderwerp cybersysteemrisico?

Ja, ook andere organisaties, overheden, toezichthouders en ratingagentschappen zijn zich bewust van de omvang en urgentie van dit onderwerp. In 2020 richtte het Amerikaanse Congres de Cyberspace Solarium Commission op, voorgezeten door senator Angus King en parlementslid Mike Gallagher. Na een onderzoek van een jaar, concludeerde de Commissie dat de Verenigde Staten risico loopt op een catastrofale cyberaanval en "op cybergebied gevaarlijk onveilig is." [3]

In Europa werd meer dan 15 jaar geleden het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) opgericht om het stijgende aantal ernstige cyberincidenten met gevolgen voor de publieke en private sector te bestrijden. In hun nieuwe rapport, dat in april 2021 verscheen, wordt benadrukt dat in het licht van de huidige cybersecurity-bedreigingen de wereldwijde bestrijdingscapaciteit met 89% zou moeten groeien om organisaties in staat te stellen hun kritische informatie- en communicatietechnologie (ICT) effectief te beschermen. Om deze situatie het hoofd te bieden, zijn nationale overheden begonnen met de implementatie van diverse programma's en beleidsmaatregelen.

In het Verenigd Koninkrijk kondigde minister van defensie Ben Wallace in oktober 2021 aan dat het land aan een nieuw digitaal defensiecentrum bouwt zodat het VK beter weerstand kan bieden aan cyberaanvallen.

Daarnaast meldde ratingsagentschap AM Best in juni 2021 dat "de vooruitzichten voor de cyberverzekeringsmarkt grimmig zijn", en wezen zij op "de verstrekkende gevolgen van de kettingreacties van cyberrisico's en het ontbreken van geografische of commerciële grenzen". Concluderend stelde zij dat verzekeraars "wiens benadering van risicomanagement onvoldoende is als het aankomt op cyber, [zichzelf] kunnen blootstellen aan een opeenstapeling van risico's die [hun] risicotolerantie overtreft en waardoor hun rating onder druk kan komen te staan." [4]

De links hieronder geven toegang tot rapportages van andere organisaties:

- Executive Order on Improving the Nation's Cybersecurity (Amerikaanse regering): https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market (Amerikaanse rekenkamer): www.gao.gov/products/gao-21-477
- Cyber Insurance Rates Could Rise 50% in 2021 (ratingkantoor MarshMcLennan): https://www.marshmma.com/blog/cyber-insurance-rates-could-rise-50-in-2021
- Balancing Risk and Opportunity Through Better Decisions (Aon): www.aon.com/2021-cyber-security-risk-report/

Hoe verschilt Chubb's strategie met die van de rest van de industrie?

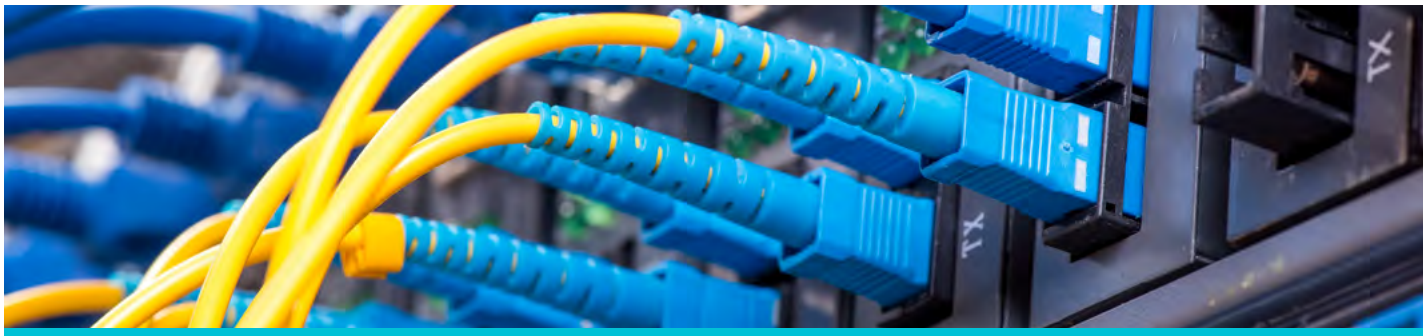
Het grootste deel van de cyberverzekeringssector richt zich op de impact van ransomware en de juiste hoogte van premies, en pakt deze problemen aan door het verlagen van dekkingen, hogere premies, en sectorspecifieke of dekkingsspecifieke aanpassingen van hun verzekeringen. Hoewel Chubb vergelijkbare aanpassingen doet, zetten we ook onze decennialange ervaring en bedrijfsomvang in om ons op het grotere plaatje van de blootstelling aan systeemrisico's te focussen. En hoewel andere organisaties binnen onze sector veel hebben gesproken over de noodzaak hiervan, is er relatief weinig actie ondernomen.

Kunnen geavanceerde acceptatietechnieken voor cyberrisico's het risico op catastrofale cyberincidenten verkleinen?

Chubb heeft een toegewijd team van cyberspecialisten, zowel op het gebied van acceptatie als op het gebied van risk engineering. Daarnaast zijn we momenteel bezig met de implementatie van een nieuwe manier om cyberbedreigingen te analyseren als ook de introductie van AI tools voor onze acceptatieprocessen. Dankzij de investering in deze tools en technieken lopen we in de industrie voorop als het gaat om acceptatie. [5]

Welke catastrofale cyberrisico's zijn in de afgelopen jaren in opkomst?

De toenemende afhankelijkheid van technologie door organisaties en consumenten en de interconnectiviteit tussen technologieën en partners hebben een situatie geschapen waarin cyberrisico's zich exponentieel vermenigvuldigen. Cyberincidenten hebben bovendien een meer wijdverspreide impact. In een tijdsbestek van 100 dagen tussen december 2020 en maart 2021 raakten diverse grote aanvallen doelen die uiteenliepen van leveranciers van software en e-mailbeveiliging, tot dataservers en gemeentelijke infrastructuur. In totaal werden meer dan 100.000 organisaties van over de hele wereld door deze incidenten geraakt, wat resulteerde in verstoringen voor miljoenen consumenten en burgers, naast aanzienlijke economische schade. De aanval op de leverancierssketen van Solorigate, waarbij een update van vertrouwde software voor netwerkanalyse kwaadaardige programmatuur bevatte, trof 20.000 bedrijven en overheidsinstanties. Er was bij dit incident niet de intentie om kritische data of andere informatie te stelen of te vernietigen. Als dit wel het geval was geweest, dan had dit incident een veel grotere impact gehad.



De volgende risicotypes kunnen, vooral indien gecombineerd, mogelijk uitmonden in catastrofale gebeurtenissen:

Wijdverspreide aanvallen op bekende ernstige kwetsbaarheden:

Dit zijn aanvallen op bekende ernstige kwetsbaarheden in software die niet verholpen zijn met een patch. Deze kwetsbaarheden zijn gemakkelijk en zonder voorafgaande toegang tot het netwerk aan te vallen en kunnen zeer schadelijke gevolgen hebben. [5]

Ernstige zero-day-aanvallen:

Deze aanvallen richten zich op zwakke plekken in software. Omdat deze wel bekend zijn bij cybercriminelen maar nog niet bij anderen, kunnen criminelen er eenvoudig gebruik van maken.

Software supply chain-aanvallen:

Met deze aanvallen verschaffen criminelen zich toegang tot een systeem via vertrouwde, gecertificeerde software.

Uitval van infrastructuur:

Kritische infrastructuur, zoals elektriciteitsnetwerken en telecommunicatiediensten, lopen het risico om op enorme schaal uit te vallen, of dat nu door een cyberaanval of een ander cyberincident is, zoals systeemuitval, menselijke fouten of programmeerfouten. De aanval in 2021 op Colonial Pipeline, de leverancier van benzine die de oostkust van de Verenigde Staten bedient, was een ransomware-aanval die zorgde voor uitval van de infrastructuur. Hierdoor kwamen miljoenen burgers en bedrijven in meerdere staten zonder brandstof te zitten.

Andere wijdverspreide incidenten:

Bepaalde types cyberaanvallen kunnen tegelijkertijd, al dan niet automatisch tegen een groot aantal slachtoffers worden ingezet, wat uiteindelijk tot een catastrofaal cyberincident leidt. Het internet en bepaalde telecommunicatiediensten zijn inmiddels cruciale maatschappelijke infrastructuur. Sommige clouddiensten worden op zulke grote schaal gebruikt dat de uitval ervan gevolgen kan hebben voor de activiteiten van duizenden of zelfs miljoenen bedrijven.

Ransomware-aanvallen:

Hoewel ze niet systemisch 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 geautomatiseerde efficiëntie uitgevoerd, waarbij het geëiste bedrag aan losgeld steeds hoger wordt. Sommige destructieve aanvallen vinden plaats onder het mom van ransomware, zoals de NotPetya en WannaCry-aanvallen.

In de cyber verzekeringsmarkt is ransomware al jaren onderwerp van gesprek. Is Chubb hier in de loop der tijd anders tegenaan gaan kijken?

We analyseren de trends op het gebied van ransomware nu al een aantal jaren. Deze trends ontwikkelen zich in een bepaalde richting, net als onze verzekeringsstrategieën. Om de risico's te kunnen beheersen, hebben wij veranderingen aangebracht in onze acceptatiestrategie (bijvoorbeeld door het vermijden van bepaalde segmenten of bedrijven die bepaalde controles niet in huis hebben), eigen risico's, sublimieten en coassurantie. Chubb past daarnaast 'signal-based' acceptatie toe voor deze risico's. Hierbij worden factoren en risicosignalen geanalyseerd die ons bereiken via verschillende interne en externe bronnen. Chubbs nieuwe cyber productaanbod biedt nog meer mogelijkheden voor het configureren van sublimieten, coassurantie en eigen risico's in het geval van ransomware-aanvallen.

Hoeveel claims voor cyber systeemrisico's heeft Chubb tot nu toe ontvangen?

In de afgelopen negen maanden heeft Chubb honderden meldingen ontvangen met betrekking tot grote wijdverspreide cyberincidenten.

Waarom blijven we zoveel verschuivingen zien in de cybermarkt? Hebben zich in andere delen van de verzekeringssector ook dergelijke verschuivingen voorgedaan?

Cyberverzekeringen zijn in de afgelopen jaren uitgegroeid tot een 'volwassen' segment en het is nog steeds volop in ontwikkeling. Cyberrisico's zijn dynamisch en nemen snel toe in zowel complexiteit als ernst. In het verleden zorgden gebeurtenissen van ongekende omvang, zoals de aardbeving in San Francisco van 1906 en de terroristische aanslagen op 11 september 2001, voor een schok op de verzekeringsmarkt. In de nasleep daarvan werden vervolgens oplossingen ontwikkeld die meer duidelijkheid over deze gevaren brachten en aparte dekkingen mogelijk maakten voor catastrofale risico's. Met de cyberverzekering hebben we nu de kans om ons complete productontwerp te verbeteren en ook om oplossingen te ontwikkelen in samenwerking met overheden die voor stabiliteit op de verzekeringsmarkt zorgen, en passende dekking voor klanten faciliteren.

Chubbs aanbod van cyberproducten

Zal Chubb de bestaande cyberdekking blijven aanbieden?

De dekking die we momenteel aanbieden, - incident responsekosten, eigen schade en aansprakelijkheidsschade -, zal beschikbaar blijven. Daarnaast maakt Chubb onderscheid tussen gebeurtenissen met een beperkte impact en grootschalige incidenten. Ongeveer 90% van de historische schades valt onder de basisdekking van onze verzekering voor gebeurtenissen met een beperkte impact.

Chubb zal daarnaast dekking bieden voor wijdeverspreide en mogelijk catastrofale systeemrisico's. Door deze dekking als uitbreiding op de basisdekking te bieden, zorgen we voor een gestructureerde en duurzame aanpak. Deze dekking zal vallen onder de noemer 'Wijdverspreid incident en bevat de subcomponenten omschreven in de polis. Op Wijdverspreide Incidenten en bijbehorende subcomponenten zullen specifieke dekkingslimieten, eigen risico's en coassurantie van toepassing zijn. Deze aanpak is vergelijkbaar met de manier waarop catastrophes als aardbevingen en overstromingen al sinds jaar en dag door de brandverzekering worden geadresseerd.

Verzekerings-proces

Met welke types dekkingsuitbreidingen moeten we rekening houden?

Chubb gaat zijn cyberverzekeringsproduct uitbreiden met dekkingselementen die voorheen alleen via aanhangsels konden worden toegevoegd. Hieronder vallen uitbreidingen als boetes van toezichthouders, PCI boetese and assessments, reputatieschade, frauduleuze overdrachten en preventieve bedrijfssluiting. Chubb zal daarnaast apart dekking aanbieden voor wijdverspreide incidenten zoals software supply chain-aanvallen, ernstige zero-day-aanvallen en aanvallen op bekende kwetsbaarheden. Klant en prospect zullen samen met hun tussenpersoon moeten bepalen met welke unieke cyberrisico's zij vanuit hun bedrijfsvoering en IT-omgeving te maken hebben, om vervolgens de dekkingsuitbreiding te kiezen die voor hun het meest zinvol is.

Zal Chubb zijn premies veranderen voor cyberdekking?

De premies zullen de specifieke dekkingsbehoeften en het risicoprofiel van elke klant blijven weerspiegelen.

Wanneer gaan deze productwijzigingen in?

Chubb heeft deze benadering al gebruikt voor grote accounts, en in de komende maanden zullen we deze uitbreiden naar andere marktsegmenten. Het is van groot belang om ruim van tevoren aan de slag te gaan met de riskmanagers van klanten om hun specifieke risico's in kaart te brengen en de dekkingsuitbreidingen te bespreken die hen de juiste bescherming bieden.

Wat kan ik doen om mij op deze veranderingen voor te bereiden? Is er informatie beschikbaar die ik kan gebruiken voor mijn gesprekken met klanten en prospects?

Naast dit document zijn er diverse andere documenten beschikbaar als ook een video waarin de wijzigingen helder uiteengezet worden. U vindt deze allemaal terug op onze webpagina.

Offerteproces

Zijn er specifieke acceptatiecriteria van invloed op de dekking en premiestelling die Chubb biedt voor systeemrisico's?

Ja. Diverse factoren zijn van invloed op de dekking en premie die Chubb aanbiedt voor systeemrisico's, zoals de kritische afhankelijkheden van bedrijven, contractuele bescherming van dienstverleners, de naleving en het toezicht op cyber security, en de planning en het testen van incidentrespons/resilience.

In welk opzicht verandert de premiestructuur voor de dekking van wijdverspreide incidenten?

Om zoveel mogelijk transparantie te waarborgen biedt Chubb premies, limieten en eigen risico's op maat aan voor systeemrisico's.

Polisformulier

Welke dekking wordt uitgesloten in het nieuwe cyberproduct van Chubb?

Er is geen sprake van uitsluiting van dekking voor wijdverspreide incidenten. Deze dekking wordt echter separaat aangeboden om zovvel mogelijk duidelijkheid en transparantie te scheppen. Verzekeringnemers beslissen zelf of ze deze dekking wel of niet afnemen.

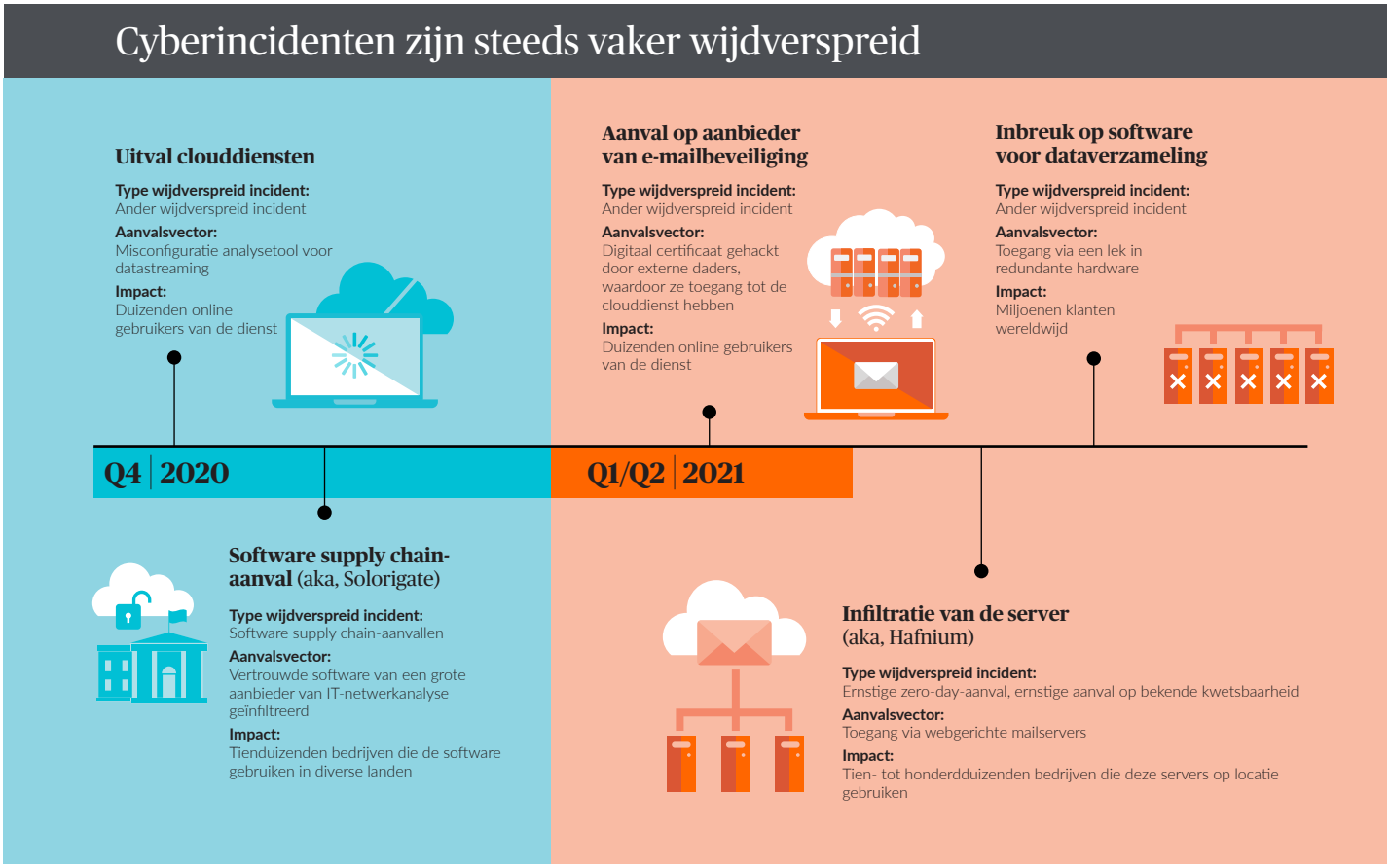
Waar in de polis wordt uitgelegd wat 'gebeurtenissen met een beperkte omvang' en 'wijdverspreide incidenten' zijn?

Op de polis of in de offerte staat vermeld dat cyberincidenten worden onderverdeeld naar ofwel een gebeurtenis met beperkte omvang of een wijdverspreid incident. De definities hiervan vindt u in de specifieke clausuletekst. Hier vindt u ook de definities van andere belangrijke termen terug, zoals een wijdverspreide trigger en groep met beperkte impact.

Voor polissen die dezelfde verzekerde bedragen, eigen risico en coassurantie bieden voor alle wijdverspreide incidenten, is het verschil tussen de subcategorieën niet relevant. Wanneer deze zaken echter verschillen van incident tot incident, dan dient het volgende onderscheid gemaakt te worden:

- Wijdverspreide ernstige aanvallen op bekende kwetsbaarheden
- Wijdverspreide ernstige zero-day-aanvallen
- Wijdverspreidee software supply chain-aanvallen
- Alle overige wijdverspreide incidenten

In de polisvoorwaarden en clausules wordt nader invulling gegeven aan hoe de verzekeringnemer en Chubb zullen samenwerken bij een cyberincicdent. Dit omvat onder meer informatie over de timing en methodes om te bepalen of een cyberincident een gebeurtenis met beperkte impact is of een wijdverspreid incident. Neem de polis zoals altijd in zijn geheel door.



Hoe werkt het eigen aandeel percentage? Kunt u hiervan een voorbeeld geven?

Het eigen aandeel percentage dat van toepassing is op wijdverspreide incidenten, ransomeware-aanvallen en aanvallen op kwetsbaarheden in software is een 'loss-reducing' coassurantie. Dit betekent dat het eigen aandeel percentage geen gevolgen heeft voor de verzekerde bedragen. In plaats daarvan wordt de verantwoordelijkheid voor elke schade verdeeld over de verzekeringnemer en de verzekeraar. Op het deel van de verzekeraar is het specifieke verzekerde bedrag voor dat risico van toepassing.

Bijvoorbeeld: als de polis een sublimiet van 5% van de in totaal $ 10 miljoen polisdekking voor een wijdverspreid incident heeft, dan is de maximale aansprakelijkheid van de verzekeraar voor een wijdverspreid incident volgens die sublimiet $ 500.000 (dat wil zeggen 5% van $ 10 miljoen).

Als een wijdverspreid incident een eigen aandeel percentage heeft van 50%, dan zou een schade van $ 1 miljoen 50/50 verdeeld worden over de verzekerde en de verzekeraar. De sublimiet voor wijdverspreide incidenten zou daarmee zijn opgesoupeerd omdat de verzekeraar het volledige beschikbare bedrag van $ 500.000 van de sublimiet betaalt.

Als een wijdverspreid incident daarentegen een schade van $ 500.000 veroorzaakt, zou die ook 50/50 verdeeld worden, maar omdat de verzekeraar in deze situatie slechts $ 250.000 uitkeert, zou er binnen de sublimiet voor wijdverspreide incidenten nog $ 250.000 overblijven voor toekomstige gebeurtenissen.

Voetnoten

1. National Institute of Standards and Technology's National Vulnerability Database. Accessed at https://nvd.nist.gov/vuln/search
2. AV-TEST Institute (2021). Accessed at www.av-test.org/en/statistics/malware/
3. Federal Commission Warns Dangerously Insecure U.S. At Risk of 'Catastrophic' Cyber Attack (2020). Accessed at www.forbes.com/sites/daveywinder/2020/03/14/make-america-safe-again-federal-commission-warns-us-at-risk-of-catastrophic-cyber-attack/?sh=244402e34d27
4. Ibid.
5. NIST Security Vulnerability Trends in 2020: An Analysis (2021). Accessed at 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 hebben wij meer dan 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.℠