Chubb biedt flexibele en duurzame aanpak voor toenemende cyberrisico's

Verzekeringnemers kunnen een cyberdekking op maat afsluiten voor wijdverspreide incidenten, ransomware-aanvallen en verwaarloosde kwetsbaarheden in software.

Wijdverspreide incidenten

De digitalisering neemt wereldwijd toe en de onderlinge digitale verbondenheid groeit. Breed gebruikte softwareprogramma's en communicatie- en technologieplatforms worden vertrouwd door duizenden of miljoenen bedrijven. Een enkele aanval op of uitval van een van deze veelgebruikte platforms kan leiden tot een opeenstapeling van schades, mogelijk zelfs tot een punt waarop verzekeraars de claims niet langer kunnen betalen. Om stabiliteit te bieden waarbij verzekeringnemers op de juiste dekking kunnen rekenen, biedt Chubb duidelijke en specifieke limieten, eigen risico's en co-assurantie voor dergelijke 'wijdverspreide incidenten'.

Onder de dekking voor wijdverspreide incidenten vallen o.a.:

Wijdverspreide software supply chain-aanvallen

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

Bekende voorbeelden > Solorigate (2020), NotPetya (2017)

Wijdverspreide 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.

Bekend voorbeeld > Hafnium (2021)

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.[1]

Bekend voorbeeld > MSSP Attack (2021)

Alle overige 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.

Bekend voorbeeld > Virginia Cloud Outage (2020)

1NIST Security Vulnerability Trends in 2020: An Analysis (2021). Geraadpleegd via https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf.

De aanvullende dekking voor wijdverspreide incidenten bevat beknopte en doelmatige regels voor schadeafhandeling, zoals:

- De kosten voor incidentresponse tasten de limieten voor wijdverspreide incidenten niet aan totdat er bepaald is dat een incident een wijdverspreid incident is, waarbij de kosten voorafgaand aan die vaststelling niet worden teruggevorderd.
- Verzekeringnemers kunnen ervoor kiezen om bepaalde onderzoeksgegevens niet te delen, wanneer er wederzijds wordt overeengekomen dat een gebeurtenis een wijdverspreid incident is.
- Om verzekeringnemers in staat te stellen de dekking in te kopen die het best aansluit bij de behoeften van hun organisatie worden alle cyberincidenten gecategoriseerd als:
  - een incident met Beperkte Impact (bijv. een plaatselijk incident waarvoor de gebruikelijke regels voor schadevergoeding gelden); of
  - een wijdverspreid incident (bijv. een systeemincident met een afwijkende schadevergoeding, zoals voor het verzekerde bedrag, het eigen risico en co-assurantie)

Ransomware

Ransomware-aanvallen komen steeds vaker voor en nemen toe in ernst. De gevolgen voor verzekeringnemers zijn veel groter dan alleen de hoogte van het losgeldbedrag. Of het losgeld nu wordt betaald of niet, verzekeringnemers krijgen vaak te maken met kosten voor forensisch onderzoek, schade door bedrijfsonderbreking, kosten voor het herstellen van digitale gegevens en mogelijk kosten voor aansprakelijkheid en juridische verdediging.

Met de Ransomware Sublimiet kunnen verzekeringnemers zorgen voor maatwerk in hun verzekerde bedragen, eigen risico, en coassurantie voor schade als gevolg van een ransomware-aanval.

Kwetsbaarheden in software

Het regelmatig updaten van software is een belangrijk aspect voor het beperken van cyberrisico's. Veel schade is te voorkomen door kwetsbare software te herstellen (patchen) voordat cybercriminelen er misbruik van kunnen maken. Niet alle organisaties voeren een software patch meteen door zodra die beschikbaar is. Soms zijn er legitieme redenen waarom software-updates voor gebruik getest moeten worden. Ook problemen met compatibiliteit, capaciteit of eenvoudige logistieke kwesties kunnen ervoor zorgen dat zelfs een goed geleide informatiebeveiligingsorganisatie de patches niet direct toepast. Daarom staat Chubb verzekeringnemers een termijn van 45 dagen toe om software-kwetsbaarheden te herstellen. Het gaat hierbij om kwetsbaarheden die gepubliceerd zijn als Common Vulnerabilities and Exposures (CVE's) in de National Vulnerability Database van het Amerikaanse National Institute for Standards and Technology (NIST).

De achterstallige software sublimiet biedt dekking als de wachttijd van 45 dagen is verstreken. Hierbij verschuift de risicodeling tussen de verzekeringnemer en de verzekeraar stapsgewijs naar de verzekeringnemer, die geleidelijk meer van het risico op zich neemt als de kwetsbaarheid niet is opgelost na respectievelijk 45, 90, 180 en 365 dagen.

Kijk voor meer informatie

op chubb.com/nl/cyber.

Chubb. Insured.℠