Rischio Cyber sistemico - aggiornamento prodotto:

FAQ per Broker

CHUBB

Febbraio 2022

Chubb intende mantenere la propria posizione di leader nel settore assicurativo Cyber fornendo la direzione e la struttura necessarie per andare verso un percorso di sostenibilità a lungo termine.

Oggi, la frequenza e la gravità degli eventi Cyber stanno portando le compagnie di assicurazione, tra cui Chubb, a rivalutare i premi, i termini e le condizioni. Negli ultimi mesi vari eventi Cyber a impatto diffuso hanno compromesso diversi obiettivi, dalla catena di fornitura di software e i provider di servizi di posta elettronica, ai data center, alle infrastrutture critiche. Tali eventi sono stati caratterizzati da vari tipi di attacchi informatici con il potenziale di degenerare in eventi catastrofici.

In ragione di ciò, Chubb sta sviluppando soluzioni innovative per gestire questo tipo di esposizioni. Chubb continuerà a fornire le coperture assicurative Cyber di base già offerte ai propri assicurati e partner distributivi, ma intende anche ripensare la copertura assicurativa per gli Eventi a Impatto Diffuso e collaborare con le associazioni di settore e i governi per individuare le varie modalità con cui fornire una certezza di copertura più consapevole per tutte le parti.

Impatto su broker e assicurati Cyber

Chubb prevede che queste nuove soluzioni forniranno ai partner distributivi una maggiore stabilità e crescita a lungo termine nel mercato assicurativo Cyber. I broker avranno un'ampia opportunità di dimostrare la loro esperienza ai clienti, tra cui la capacità di illustrare più chiaramente le coperture disponibili per le esposizioni sistemiche, personalizzare i termini e le condizioni adattandoli alle esposizioni specifiche del cliente e arricchire le diverse coperture con servizi dal valore aggiunto, quali loss mitigation e consulenza sui rischi. Il nuovo approccio di Chubb sfrutterà concetti familiari alla maggior parte dei broker e dei clienti che hanno esperienza nel ramo Property e nelle coperture contro i rischi catastrofici. Nel tempo, un approccio strutturato alla quantificazione del rischio Cyber catastrofico dovrebbe tradursi in una maggiore capacità del mercato assicurativo Cyber.

Il mercato del rischio Cyber

Quali sono le cause degli attuali cambiamenti di strategia in materia di assicurazione Cyber?

Gli incidenti e le minacce informatiche sono in costante aumento ed evoluzione. Oltre 18.000 nuove vulnerabilità software sono state pubblicate nel 2020, quasi il triplo rispetto al 2015 e in continua crescita[1]. Nel frattempo, quasi 1,2 milioni di nuove minacce malware sono state identificate nel 2020, più del doppio rispetto al 2015[2]. Mentre tattiche come il ransomware sono diventate più comuni e costose, la violazione dei dati e la compromissione delle e-mail aziendali continuano a portare la frequenza degli incidenti informatici a livelli tra i più alti di sempre, specialmente con la diffusione di accordi di lavoro da remoto. La crescente frequenza e gravità di tali eventi informatici sta mettendo sotto pressione gli indici di perdita delle compagnie di assicurazione, mentre le esposizioni sistemiche con potenziale catastrofico diventano sempre più evidenti.

Anche altre organizzazioni condividono il punto di vista di Chubb sul tema del rischio Cyber sistemico?

Sì, crediamo che anche altre organizzazioni, governi, autorità di regolamentazione e agenzie di rating abbiano preso atto dell'ampiezza e dell'urgenza di questo argomento. Nel 2020, il Congresso degli Stati Uniti ha istituito la Cyberspace Solarium Commission, presieduta dal senatore Angus King (I-ME) e il deputato Mike Gallagher (R-WI). Dopo uno studio durato un anno, la Commissione ha concluso che gli Stati Uniti sono a rischio di un attacco Cyber catastrofico e sono "pericolosamente precari nel settore informatico".[3]

In Europa, l'Agenzia dell'Unione Europea per la cybersicurezza (ENISA) è stata istituita oltre 15 anni fa per affrontare il crescente numero di gravi incidenti informatici che colpiscono il settore pubblico e privato. Il loro nuovo rapporto pubblicato nell'aprile 2021 evidenzia che, alla luce delle odierne minacce alla sicurezza informatica, la forza lavoro globale per la sicurezza informatica dovrebbe crescere dell'89% affinché le aziende possano difendere in modo efficace le proprie tecnologie informatiche e di comunicazione (TIC). Per far fronte a questa situazione critica, i governi nazionali hanno iniziato ad attuare una serie di programmi e direttive.

Nel Regno Unito, il segretario alla Difesa Ben Wallace ha annunciato in ottobre che il Paese sta costruendo un nuovo centro di lotta digitale per rafforzare la resilienza del Regno Unito agli attacchi informatici.

Inoltre, l'agenzia di rating assicurativo AM Best nel giugno 2021 ha riferito che "le prospettive per il mercato assicurativo informatico sono cupe", osservando "implicazioni di vasta portata dovute agli effetti a cascata dei rischi Cyber e l'assenza di confini geografici o commerciali" e concludendo che gli assicuratori "il cui approccio alla gestione del rischio Cyber è carente , possono trovarsi [loro stessi] soggetti a un rischio di accumulo oltre la [loro] tolleranza al rischio e potrebbero dover affrontare pressioni in termini di rating".[4]

Insight di altre organizzazioni sono disponibili ai seguenti link:

- Executive Order on Improving the Nation's Cybersecurity (US Government): 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 (US Government Accountability Office): www.gao.gov/products/gao-21-477
- Cyber Insurance Rates Could Rise 50% in 2021 (MarshMcLennan Agency): 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/

Come si colloca la strategia di Chubb rispetto al settore?

Gran parte del settore assicurativo Cyber si concentra sulle questioni più circoscritte del ransomware e dell'adeguatezza delle tariffe, riducendo la capacità, aumentando le tariffe e apportando adeguamenti di sottoscrizione specifici per il settore o la copertura. Pur intraprendendo azioni simili, Chubb attinge anche a decenni di esperienza e alla propria dimensione aziendale significativamente più ampia, per concentrarsi su un problema più vasto: i rischi sistemici. Benché altre compagnie abbiano parlato di questa necessità all'interno del nostro settore, ad oggi poche sono state le azioni concrete. È probabile che Chubb guiderà il cambiamento in questo ambito.

Le tecniche avanzate di sottoscrizione Cyber possono mitigare il rischio di catastrofi informatiche?

Chubb ha un team dedicato di ingegneri e sottoscrittori nell'ambito del rischio informatico e stiamo introducendo nuovi strumenti di analisi delle minacce e di intelligenza artificiale all'interno dei nostri processi di sottoscrizione. Inoltre, forniamo ai nostri assicurati Cyber l'accesso a un ventaglio completo di servizi di prevenzione e mitigazione dei danni. Il nostro investimento proattivo in queste aree ha portato i risultati delle sottoscrizioni Cyber di Chubb a sovraperformare il più ampio settore delle assicurazioni Cyber.[5]

Nonostante questi significativi investimenti, molte minacce informatiche sono progettate appositamente per eludere i controlli interni e le best practice. Nessun sistema di sottoscrizione o prevenzione dei danni può eliminare completamente il rischio di catastrofi informatiche.

Cos'è il rischio Cyber sistemico? In che modo Chubb definisce questo termine?

Dal nostro punto di vista, "sistemico" si riferisce a un rischio che ha il potenziale di impattare diversi clienti a causa di elementi comuni o condivisi del rischio, mentre "catastrofico" si riferisce a un rischio sistemico che si manifesta con gravi o ingenti perdite per molti assicurati.

Quali rischi Cyber catastrofici sono emersi negli ultimi anni?

La crescente dipendenza dalla tecnologia da parte delle aziende e dei consumatori, così come l'interconnettività delle tecnologie e dei partner, hanno creato un ambiente in cui i rischi informatici possono avere una diffusione esponenziale. Anche gli attacchi informatici stanno avendo un impatto più diffuso. Nell'arco di 100 giorni, da dicembre 2020 a marzo 2021, svariati attacchi di grande portata hanno compromesso non solo software diffusi su larga scala e provider di servizi di posta elettronica, ma anche data center e infrastrutture critiche. Ben oltre 100.000 aziende di tutto il mondo sono state vittime di questi eventi, con conseguenti interruzioni per milioni di clienti e cittadini, nonché notevoli perdite economiche. Ad esempio, l'attacco alla catena di fornitura del software Solorigate, in cui il malware è stato incorporato in un aggiornamento di un software di monitoraggio della rete ritenuto affidabile, ha colpito 20.000 aziende e agenzie governative. Se l'intento fosse stato di rubare o distruggere dati di importanza critica o altre informazioni le conseguenze sarebbero state molto più gravi.

I seguenti tipi di rischio, soprattutto se combinati, sono stati identificti come potenzialmente in grado di degenerare in eventi catastrofici:

Sfruttamento di vulnerabilità note
Alcune vulnerabilità software, che sono prive di patch di sicurezza, possono essere classificate “Severe”, nel senso che sono facili da sfruttare, possono essere diffuse da remoto con privilegi di accesso limitati e possono causare danni significativi.[6]

Sfruttamento di vulnerabilità Zero-Day
Alcune vulnerabilità software, conosciute dai criminali informatici ma non ancora da tutti gli altri, sono facilmente sfruttabili, potenzialmente gravi e spesso prive di protezione.

Sfruttamento di vulnerabilità nella supply chain del software
Questi attacchi sono di fatto un cavallo di Troia che permette ai malintenzionati di accedere ai sistemi attraverso un software affidabile e certificato.

Interruzione di infrastrutture critiche
Le infrastrutture critiche sociali, quali le reti elettriche e i servizi di telecomunicazione, affrontano il rischio potenziale di guasti su scala molto ampia, siano essi causati da un attacco informatico o da incidenti informatici non dolosi, tra cui guasti del sistema, errori umani o errori di programmazione. Il recente attacco a Colonial Pipeline, la società di fornitura di carburante che serve la costa orientale degli Stati Uniti, ha fatto leva su un’interruzione dell’infrastruttura attraverso un attacco ransomware che ha provocato carenze di fornitura a milioni di cittadini e imprese in diversi stati americani.

Altri Eventi a Impatto Diffuso
Alcuni tipi di attacchi cyber possono essere condotti simultaneamente o automaticamente contro un ampio numero di vittime, risultando in un evento cyber catastrofico. Internet e alcuni servizi di telecomunicazione rappresentano oggi strumenti critici per la continuità operativa delle aziende e alcune grandi aziende di cloud computing sono così ampiamente utilizzate che un’interruzione diffusa potrebbe avere un impatto sulle operazioni commerciali di migliaia o milioni di aziende.

Attacchi ransomware
Benché non siano necessariamente di natura catastrofica, gli attacchi ransomware, che tengono in ostaggio i dati o le informazioni delle aziende o dei singoli individui fino al pagamento di un riscatto, vengono ora eseguiti con efficienza industrializzata, con richieste di riscatto in continuo aumento. Alcuni attacchi distruttivi possono presentarsi come ransomware, come per gli eventi NotPetya e WannaCry.

Il mercato assicurativo Cyber discute da anni di ransomware. Chubb li sta considerando in modo diverso ora?

Abbiamo analizzato le tendenze del ransomware per diversi anni e con l'evolversi di queste tendenze, anche le nostre strategie di assicurazione sono cambiate. Per contribuire alla gestione dei rischi, abbiamo reagito con modifiche alla strategia di sottoscrizione (ad esempio evitando alcune categorie o attività prive di determinati controlli), franchigie, limiti e coassicurazione. Per questi rischi, Chubb sta anche applicando una sottoscrizione basata sui segnali, che analizza i fattori ponderati e i segnali di rischio ottenuti da varie fonti interne ed esterne, per aiutarci a identificare i fattori di rischio per clienti e potenziali clienti. La nuova offerta di prodotti Cyber di Chubb offrirà un numero ancora maggiore di modalità per configurare i sub-limiti, la coassicurazione e la fidelizzazione per i casi di ransomware attraverso contratti assicurativi multipli.

Quanti sinistri per rischio Cyber sistemico ha ricevuto Chubb finora?

Negli ultimi nove mesi Chubb ha ricevuto centinaia di segnalazioni Cyber associate ai principali Eventi informatici a Impatto Diffuso.

Perché continuiamo ad assistere a così tanti cambiamenti nel mercato Cyber? Il settore assicurativo ha sperimentato simili sconvolgimenti in altri rami?

L'assicurazione Cyber è diventata un segmento a sé stante solo negli ultimi anni e ancora adesso è una linea di copertura in continua evoluzione. Nel contempo, i rischi Cyber sono dinamici e aumentano rapidamente sia in termini di complessità sia di gravità. Storicamente il mercato assicurativo nel ramo danni ha subito shock da eventi improvvisi di portata senza precedenti, come il terremoto di San Francisco del 1906 e gli attacchi terroristici dell'11 settembre. Le soluzioni che sono state trovate dopo tali eventi hanno fornito maggiore chiarezza sui singoli rischi, rendendo disponibili coperture separate per i rischi catastrofici. Con le assicurazioni Cyber abbiamo ora l'opportunità di agire sul concetto di prodotto e potenzialmente di creare, insieme ai governi, soluzioni che siano in grado di fornire stabilità nel mercato assicurativo e certezza di copertura per i clienti.

L'offerta Cyber di Chubb

Chubb continuerà ad offrire le stesse coperture che offre ora in ambito Cyber?

Saranno disponibili le stesse coperture base che offriamo al momento: spese di Incident Response, rischio Cyber proprio, Responsabilità Civile Cyber e Responsabilità Professionale/Errori e Omissioni. In aggiunta, Chubb sta operando una distinzione tra Eventi a Impatto Limitato ed Eventi a Impatto Diffuso. Prevediamo che le coperture di base del prodotto continueranno a coprire circa il 90% delle perdite storiche nell'ambito delle coperture standard per Eventi a Impatto Limitato.

Chubb offrirà coperture per rischi di frequenza significativi, ma offrirà anche coperture aggiuntive per i rischi sistemici con un potenziale diffuso e catastrofico, come estensioni del prodotto assicurativo Cyber principale, in un modo più strutturato e sostenibile. Queste saranno indicate collettivamente come coperture per Eventi a Impatto Diffuso, comprensive dei vari sottocomponenti delineati nella polizza. Gli Eventi a Impatto Diffuso e ogni sottocomponente saranno soggetti a limiti, franchigie e importi di coassicurazione specifici. Questo approccio è simile al modo in cui l'assicurazione del ramo danni ha affrontato i rischi catastrofici, quali le inondazioni e i terremoti, per ben oltre un secolo.

Che tipo di estensioni di copertura dobbiamo aspettarci?

Chubb includerà molte estensioni di copertura all'interno del prodotto Cyber di base; estensioni in precedenza offerte solo tramite specifica sottoscrizione. Tra queste sono inclusi i procedimenti di un'autorità di vigilanza, penalità derivanti da carte di pagamento, danno reputazionale, la frode in fattura, la chiusura preventiva e altro ancora. Chubb offrirà estensioni di copertura separate per includere rischi sistemici, come interruzioni del cloud, attacchi alla supply chain del software, sfruttamento di vulnerabilità zero-day, sfruttamento di vulnerabilità note e altri Eventi a Impatto Diffuso. Il grafico a sinistra fornisce una panoramica di questa suddivisione. I clienti e i potenziali clienti dovranno interagire con il loro agente/broker per determinare i rischi Cyber specifici che possono dover gestire in ragione delle loro operazioni e del loro ambiente IT. Verranno quindi selezionate le estensioni di copertura più adatte a loro.

I nostri premi cambieranno per le coperture Cyber?

I premi continueranno a riflettere le esigenze di copertura specifiche di ogni cliente e il profilo di rischio. Laddove sia necessaria l'approvazione da parte delle autorità giurisdizionali per emettere un'assicurazione su base autorizzata, verrà presentata una dichiarazione aggiornata dei tassi e noi sottoscriveremo e fisseremo i prezzi in base a tale dichiarazione dei tassi approvata.

Quando entreranno in vigore questi cambiamenti di prodotto?

Chubb ha già iniziato ad utilizzare questo nuovo approccio sui grandi clienti e nei prossimi mesi lo estenderà ad altri segmenti di mercato. Questo significa che è fondamentale iniziare a lavorare con i risk manager delle aziende clienti con largo anticipo rispetto al rinnovo delle polizze, al fine di identificare i rischi specifici del cliente stesso, nonché analizzare le estensioni di copertura che forniranno la giusta protezione. Questo nuovo approccio sarà adottato nel rispetto delle normative vigenti nei vari Paesi e in Italia è iniziato a partire da gennaio 2022.

Sarà previsto un documento informativo commerciale da allegare al modulo per spiegare i vantaggi?

Sì, sarà possibile scaricare un documento di sintesi

Processo di sottoscrizione

Cosa posso fare per pianificare questi cambiamenti? Avrò a disposizione risorse a supporto delle mie trattative con i clienti e i potenziali clienti?

Oltre a leggere e comprendere queste FAQ, suggeriamo di approfittare di qualsiasi formazione e dei webinar che verranno offerti da Chubb. Materiali quali whitepaper, webinar e video saranno resi disponibili durante l'anno e potranno essere condivisi con gli assicurati. Per maggiori informazioni potete visitare il sito chubb.com/it/cyber o contattare il vostro underwriter locale.

Processo di quotazione

Ci sono alcune considerazioni sottoscrittive che determinano la copertura sistemica e i prezzi offerti da Chubb?

Sì. Diversi fattori influenzeranno la copertura sistemica e i prezzi offerti da Chubb, comprese le dipendenze critiche dell'organizzazione, le protezioni contrattuali con i fornitori di servizi, l'igiene e i controlli di sicurezza informatica, la pianificazione e i test di risposta agli incidenti/resilienza.

Cosa cambia nella definizione dei prezzi della copertura per gli Eventi a Impatto Diffuso?

Chubb si impegna a garantire trasparenza a tutti i clienti e offrirà prezzi, limiti e opzioni di franchigie separati per la copertura sistemica.

Wording di polizza

Quale copertura viene esclusa nei nuovi prodotti Cyber di Chubb?

La copertura per Eventi a Impatto Diffuso non è esclusa. È stata strutturata in modo da fornire in modo trasparente capacità per eventi sottoscritti. Gli assicurati hanno la possibilità di acquistare la copertura per Eventi a Impatto Diffuso, ma non è obbligatoria.

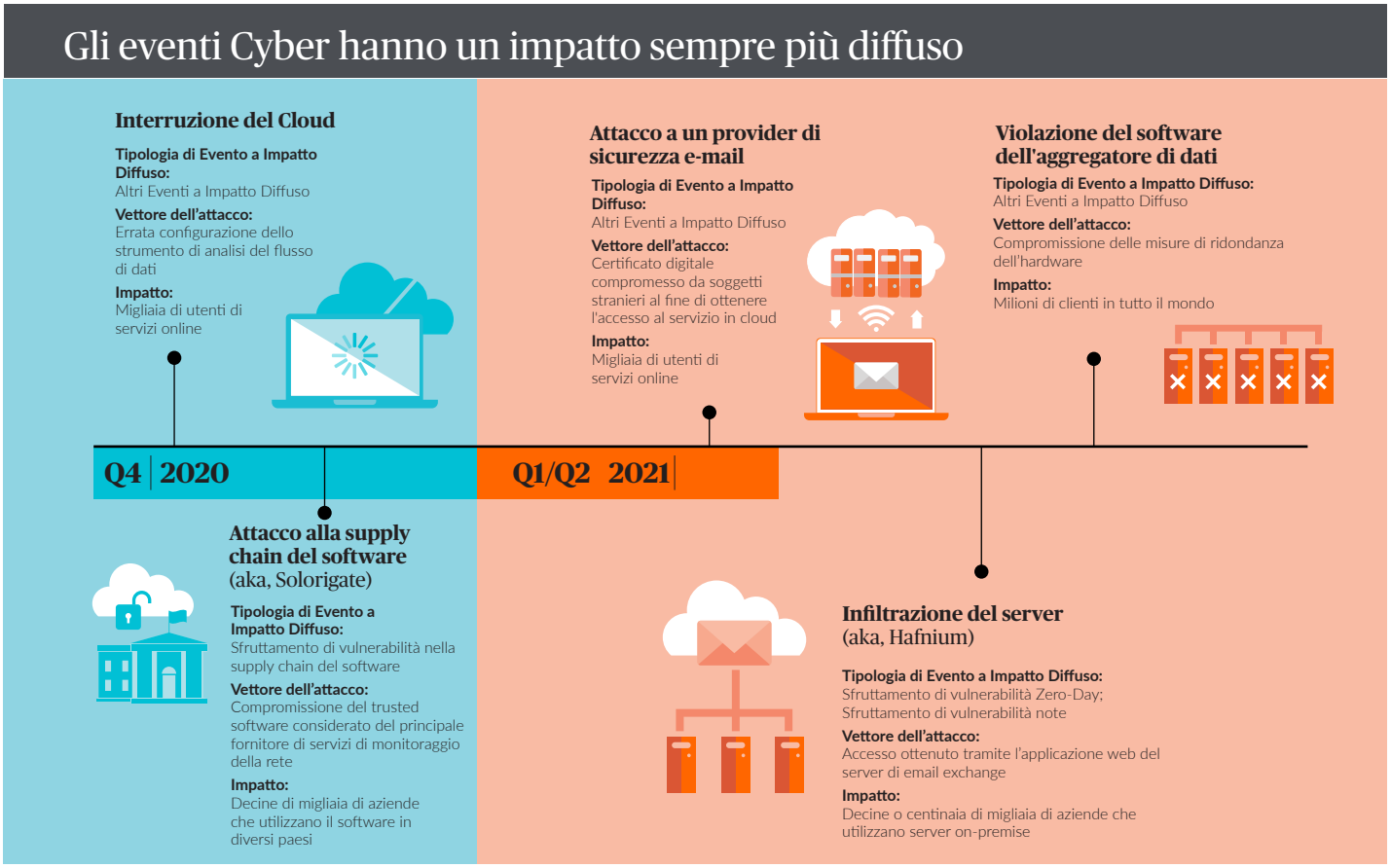
Nella polizza, dove sono descritti i concetti di Evento a Impatto Limitato ed Evento a Impatto Diffuso?

Nella prima pagina della polizza si afferma che gli incidenti Cyber saranno classificati come Eventi a Impatto Limitato o Eventi a Impatto Diffuso. Tali definizioni sono delineate nella Sezione II della polizza. Ulteriori definizioni chiave utilizzate all'interno di questi concetti includono, tra le altre, Causa Diffusa e Gruppo Limitato di Impatto.

Per le polizze che forniscono gli stessi limiti, franchigie e coassicurazione per tutti i tipi di Eventi a Impatto Diffuso, non è importante distinguere tra le quattro sottocategorie di Eventi a Impatto Diffuso. Tuttavia, se sono presenti limiti, franchigie o coassicurazione differenziati, è necessario rivedere le seguenti definizioni di sottocategorie di Eventi a Impatto Diffuso:

- Sfruttamento di vulnerabilità note
- Sfruttamento di vulnerabilità Zero-Day
- Sfruttamento di vulnerabilità nella supply chain del software
- Tutti gli altri Eventi a Impatto Diffuso

La sezione X della polizza affronta gli "Obblighi in caso di incidente Cyber" e descrive in dettaglio come il contraente e Chubb collaboreranno in caso di incidente informatico. Ciò include informazioni sui tempi e sui metodi per determinare se un incidente Cyber si caratterizza come Evento a Impatto Limitato o Evento a Impatto Diffuso. Come sempre, la polizza va letta nella sua interezza.



Potete fornire esempi storici reali di Eventi a Impatto Diffuso?

Esempi di recenti Eventi a Impatto Diffuso sono rappresentati nel grafico soprastante.

Come funziona la coassicurazione? Potete fornire un esempio?

La coassicurazione applicabile agli Eventi a Impatto Diffuso, agli attacchi ransomware e allo sfruttamento di software trascurati è una coassicurazione che "riduce le perdite", il che significa che la coassicurazione dell'assicurato non intacca i limiti dell'assicurazione. Piuttosto, la responsabilità per ogni sinistro è ripartita tra l'assicurato e l'assicuratore, e la quota dell'assicuratore è quindi soggetta al limite applicabile per quel rischio.

Ad esempio, se la polizza ha un sottolimite del 5% del limite di polizza aggregato di 10 milioni di euro per Eventi a Impatto Diffuso, la responsabilità massima dell'assicuratore per qualsiasi perdita da esso provocata al di sotto di tale sottolimite per Eventi a Impatto Diffuso sarebbe di € 500.000 (ovvero, 5% di 10 milioni di euro).

Se la copertura per un Evento a Impatto Diffuso è soggetta a una coassicurazione del 50%, allora un evento da 1 milione di euro di perdite sarebbe ripartito 50/50 tra l'assicurato e l'assicuratore e il sottolimite per Eventi a Impatto Diffuso sarebbe quindi esaurito, perché l'assicuratore avrebbe pagato l'intero sottolimite disponibile di €500.000.

Allo stesso modo, anche una perdita di € 500.000 dovuta ad un Evento a Impatto Diffuso verrebbe ripartita 50/50. Tuttavia, poiché in questa situazione l'assicuratore pagherebbe solo € 250.000, rimarrebbero € 250.000 di sottolimite per Eventi a Impatto Diffuso per eventi futuri.

Fonti

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. Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk (2021). Accessed at www.insurancejournal.com/research/research/ransomware-and-aggregation-issues-call-for-new-approaches-to-cyber-risk/
5. Ibid.
6. NIST Security Vulnerability Trends in 2020: An Analysis (2021). Accessed at www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

A proposito di Chubb

Chubb è la più grande compagnia assicurativa danni al mondo per capitalizzazione quotata in borsa. Opera in 54 paesi e offre, a livello globale, soluzioni assicurative a imprese di ogni dimensione, a professionisti e famiglie. Opera nel Property & Casualty (P&C) e nell'Accident & Health (A&H), con prodotti sia personalizzati sia standardizzati, attraverso una pluralità di canali. L'elevata capacità sottoscrittiva e l'attenzione al servizio ci sono riconosciuti dal mercato, soprattutto riguardo l'equità e la tempestività con cui gestiamo i sinistri. Chubb Limited, la società capogruppo di Chubb, è quotata alla borsa valori di New York (NYSE: CB) e fa parte dell'indice S&P 500. Chubb ha uffici di rappresentanza a Zurigo, New York, Londra, Parigi e in altre sedi, e impiega circa 31.000 persone nel mondo. Ulteriori informazioni su www.chubb.com/it.

Per ulteriori informazioni sull'esperienza e la competenza di Chubb nella gestione dei rischi informatici è possibile visitare il sito chubb.com/it/cyber o contattare il vostro underwriter locale.

Chubb. Insured.℠

Chubb European Group SE, Sede legale: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, Francia - Capitale sociale €896.176.662 i.v.- Rappresentanza generale per l'Italia: Via Fabio Filzi n. 29 - 20124 Milano - Tel. 02 27095.1 - Fax 02 27095.333 - P.I. e C.F. 04124720964 - R.E.A. n. 1728396 - Abilitata ad operare in Italia in regime di stabilimento con numero di iscrizione all'albo IVASS I.00156. L'attività in Italia è regolamentata dall'IVASS, con regimi normativi che potrebbero discostarsi da quelli francesi. Autorizzata con numero di registrazione 450 327 374 RCS Nanterre dall'Autorité de contrôle prudentiel et de résolution (ACPR) 4, Place de Budapest, CS 92459, 75436 PARIS CEDEX 09 RCS e soggetta alle norme del Codice delle Assicurazioni francese. info.italy@chubb.com - www.chubb.com/it