Chubb affronta i crescenti rischi Cyber con un approccio flessibile e sostenibile

Gli assicurati possono personalizzare i livelli della copertura assicurativa Cyber per Eventi a Impatto Diffuso, Ransomware, Vulnerabilità di software trascurato.

CHUBB®

Eventi a Impatto Diffuso

Il mondo sta diventando ogni anno più digitalizzato e interconnesso. Migliaia se non milioni di aziende si affidano a programmi software, piattaforme di comunicazione e tecnologie ampiamente diffusi. Un singolo attacco o un guasto a una di queste piattaforme o tecnologie ampiamente utilizzate potrebbe creare un rischio aggregato in grado di mettere alla prova la capacità di risposta del settore assicurativo. Al fine di fornire agli assicurati maggiore certezza di copertura e stabilità del mercato assicurativo, Chubb offre limiti, franchigie e coassicurazione personalizzabili e specifici per tali "Eventi a Impatto Diffuso".

Le tipologie di Eventi a Impatto Diffuso coperte includono:

Sfruttamento di vulnerabilità nella supply chain del software

Si tratta di attacchi che consentono ai malintenzionati di accedere ai sistemi attraverso un software affidabile e certificato e rappresentano di fatto un cavallo di Troia per i sistemi.

Casi reali > Solorigate (2020), NotPetya (2017)

Sfruttamento di vulnerabilità zero-day

Si tratta di attacchi derivanti dallo sfruttamento di determinate vulnerabilità del software note ai criminali informatici ma non ancora a nessun altro. Vulnerabilità che possono essere facilmente sfruttabili, gravi e spesso prive di protezione.

Caso reale > Hafnium (2021)

Sfruttamento di vulnerabilità note

Si tratta di attacchi derivanti dallo sfruttamento di vulnerabilità note del software alle quali non sono state applicati patch di sicurezza. Le vulnerabilità sono classificate “Severe” perché sono facili da sfruttare, possono essere diffuse da remoto con privilegi di accesso limitati e possono causare danni significativi.[1]

Caso reale > MSSP Attack (2021)

Tutti gli altri Eventi a Impatto Diffuso

Alcuni tipi di attacchi Cyber possono essere condotti simultaneamente o automaticamente contro un ampio numero di vittime, provocando in ultima istanza un evento Cyber dalle proporzioni catastrofiche. Internet e alcuni servizi di telecomunicazione rappresentano oggi un'infrastruttura sociale critica. Alcune grandi aziende di cloud computing sono così ampiamente utilizzate che un'interruzione potrebbe avere un impatto sulle operazioni commerciali di migliaia o addirittura milioni di aziende.

Caso reale > Virginia Cloud Outage (2020)

[1]NIST Security Vulnerability Trends in 2020: An Analysis (2021). Accessed at https://www.redscan.com/media/Redscan__NIST-Vulnerability-Analysis-2020__v1.0.pdf.

L’appendice per Eventi a Impatto Diffuso prevede disposizioni pratiche e sintetiche nel merito dell’operatività della copertura, tra cui:

- Le spese di incident response non sono soggette ai sottolimiti di copertura per Eventi a Impatto Diffuso fino a quando non viene stabilito che si tratta di un Evento a Impatto Diffuso e non è prevista la restituzione all’Assicuratore delle spese sostenute prima di tale determinazione
- Gli assicurati possono decidere di non condividere le informazioni emerse dalle indagini quando viene appurato che un incidente è un Evento a Impatto Diffuso
- Per consentire agli assicurati di acquistare la copertura che meglio soddisfa le esigenze della propria attività, tutti gli incidenti Cyber sono classificati come:
  - Eventi a Impatto Limitato (ad esempio un evento locale che sarà gestito attraverso le politiche standard di gestione del sinistro)
  - Eventi a Impatto Diffuso (ad esempio, un evento sistemico che sarà gestito considerando limiti, franchigie e scoperti dedicati)

Ransomware

Gli attacchi ransomware sono aumentati notevolmente sia in termini di frequenza sia di gravità. Le perdite per gli assicurati sono molto più ampie del semplice valore dell'importo del riscatto. Indipendentemente dal fatto che il riscatto sia pagato o meno, gli assicurati spesso sostengono spese legali, spese di indagine forense, perdite per interruzione dell'attività, costi di ripristino dei dati digitali e, potenzialmente, costi di responsabilità civile e di difesa legale.

L’endorsement per ransomware consente di personalizzare i limiti di copertura, le franchigie e la coassicurazione per i danni subiti a seguito di ransomware.

Vulnerabilità di Software Trascurato

Mantenere aggiornati i software è un aspetto importante in materia di Cyber security. Molti danni possono essere prevenuti applicando patch al software vulnerabile prima che i criminali informatici abbiano l'opportunità di sfruttarlo, tuttavia alcune aziende potrebbero non intervenire immediatamente. A volte ci sono ragioni legittime per cui gli aggiornamenti software devono essere testati prima di essere implementati e la compatibilità, la capacità o semplici problemi logistici possono impedire anche a un’azienda di sicurezza informatica ben gestita di applicare le patch entro il primo giorno o la prima settimana dal rilascio. Per questo motivo, Chubb offre agli assicurati un periodo di 45 giorni per correggere le vulnerabilità del software pubblicate come Common Vulnerabilities and Exposures (CVE) all'interno del National Vulnerability Database gestito dal National Institute for Standards and Technology (NIST) degli Stati Uniti.

L’appendice per Vulnerabilità di Software Trascurato fornisce copertura dopo la scadenza del periodo di 45 giorni, con una condivisione del rischio tra l’assicurato e l'assicuratore che si sposta gradualmente sull'assicurato, il quale si assume progressivamente una parte maggiore del rischio se la vulnerabilità non viene corretta al 46°, 90°, 180° e 365° giorno.

Per maggiori informazioni

Visita il sito chubb.com/it/cyber