Chubb aborda los crecientes riesgos cibernéticos con un enfoque flexible y sostenible

Los asegurados pueden adaptar los niveles de cobertura del seguro de cyber para Eventos de Impacto generalizado, Ataques ransomware y Eventos de software vulnerable.

Eventos de impacto generalizado

El mundo se va digitalizando e interconectando cada vez más año tras año. Los programas informáticos, las plataformas de comunicación y las tecnologías de uso generalizado son aprovechadas y a menudo utilizadas por miles o millones de empresas. Un solo ataque y/o fallo de una de estas plataformas o tecnologías ampliamente utilizadas podría crear un riesgo de agregación que supere la capacidad de aseguramiento del sector asegurador. Con el fin de ofrecer a los asegurados claridad en la cobertura y estabilidad en el mercado, Chubb proporciona límites, retenciones y coaseguros afirmativos y específicos para dichos «Eventos de impacto generalizado».

Los tipos de peligros por Eventos de impacto generalizado cubiertos son los siguientes:

Eventos de impacto generalizado de la cadena de suministro de *software*

Se trata de ataques que permiten a los perpetradores entrar en los sistemas a través de *software* de confianza y certificado, y son, a efectos prácticos, troyanos para un sistema.

Ejemplos reales > Solorigate (2020), NotPetya (2017)

Eventos de impacto generalizado graves de día cero

Estos ataques se derivan de determinadas vulnerabilidades de *software* conocidas por los ciberdelincuentes, pero aún no por el resto; vulnerabilidades que se pueden aprovechar fácilmente, son potencialmente graves y a menudo carecen de protección.

Ejemplo real > Hafnio (2021)

Eventos de impacto generalizado por vulnerabilidades graves conocidas

Se trata de ataques derivados de graves vulnerabilidades de *software* conocidas y no parcheadas. Las vulnerabilidades se consideran graves, ya que son fáciles de aprovechar, se pueden desplegar remotamente con privilegios de acceso limitados y causar un efecto adverso considerable.[1]

Ejemplo real > Ataque MSSP (2021)

Resto de Eventos de impacto generalizado

Existen algunos tipos de ciberataques que pueden llevarse a cabo simultánea y automáticamente contra un gran número de víctimas, provocando en última instancia un suceso cibernético catastrófico. Internet y algunos servicios de telecomunicaciones han alcanzado el nivel de infraestructura crítica para la sociedad, y algunas grandes empresas de computación en la nube son tan utilizadas que una interrupción generalizada podría afectar a las operaciones comerciales de miles o incluso millones de empresas.

Ejemplo real > Virginia Cloud Outage (2020)

1Tendencias de las vulnerabilidades de seguridad en 2020 según NIST: Análisis (2021). Consultado en https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf.

Los Eventos de impacto generalizado recogen normas de ajuste de pérdidas concisas y sensatas, por ejemplo:

- Los gastos de respuesta a incidentes no erosionan los límites de los Eventos de impacto generalizado hasta después de que se determine que un incidente es un Evento de impacto generalizado, sin que se devuelvan los gastos originados antes de esa determinación.
- Los asegurados pueden optar por no compartir determinados tipos de datos de investigación cuando se acuerda mutuamente que un incidente es un Evento de impacto generalizado.
- Para que los asegurados puedan contratar la cobertura que mejor se adapte a las necesidades de su organización, todos los incidentes cibernéticos se clasifican como:
  - Eventos de impacto limitado (por ejemplo, un evento local con normas de pérdida habituales)
  - o Eventos de impacto generalizado (por ejemplo, un evento sistemático con diferencias de ajuste de pérdidas estructurales como el límite, la retención y el coaseguro)

Ransomware

Los ataques de *Ransomware* han crecido drásticamente tanto en frecuencia como en gravedad. Las implicaciones de las pérdidas para los asegurados son mucho más amplias que el valor del importe del rescate. Tanto si se paga el rescate como si no, los asegurados suelen incurrir en costes legales, gastos de investigación forense, pérdidas por interrupción de la actividad, costes de recuperación de datos digitales y puede que costes de responsabilidad civil y defensa legal.

Los Casos de *Ransomware* permiten adaptar los límites de la cobertura, la retención y el coaseguro para las pérdidas originadas a resultas de un *Ransomware*.

Evento de software vulnerable

Mantener el *software* actualizado es un aspecto importante de una buena higiene de ciberriesgos. Muchas pérdidas pueden evitarse parcheando el *software* vulnerable antes de que los ciberdelincuentes tengan la oportunidad de explotarlo, pero algunas organizaciones pueden no hacerlo de inmediato. A veces hay razones legítimas por las que las actualizaciones de *software* deben probarse antes de ser desplegadas, y la compatibilidad, la capacidad o simples problemas logísticos pueden impedir incluso a una organización de seguridad de la información bien gestionada desplegar los parches en el primer día o semana desde su lanzamiento. Por ese motivo, Chubb ofrece a los asegurados un periodo de gracia de 45 días para parchear las vulnerabilidades de *software* que se publican como Vulnerabilidades y Exposiciones Comunes (CVE) dentro de la Base de Datos Nacional de Vulnerabilidades operada por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST).

Los Eventos de *software* vulnerables ofrecen cobertura tras el vencimiento del periodo de gracia de 45 días, y el reparto de riesgos entre el asegurado y la aseguradora se desplaza progresivamente hacia el asegurado, que asume un riesgo cada vez mayor si la vulnerabilidad no se parchea en los puntos de 46, 90, 180 y 365 días.

Para obtener más información

Visite chubb.com/es/cyber