Evento generalizado

Un solo ataque y/o fallo de la tecnología, ampliamente utilizada, podría crear un riesgo de agregación que supere la capacidad de una aseguradora para cubrir el riesgo. Con el fin de ofrecer a los asegurados claridad en la cobertura y estabilidad en el mercado, Chubb proporciona límites, retenciones y coaseguros específicos para dichos eventos generalizados. A continuación, figuran algunos ejemplos hipotéticos de eventos generalizados.

- Ciberataque global al sistema operativo

1

1. El evento

La Empresa 'Ejemplo' tiene más de 500 000 clientes particulares y 5000 clientes corporativos. Un día, sus empleados descubrieron que no podían acceder a ninguna de sus estaciones de trabajo, aplicaciones críticas o datos que dependían de un sistema operativo muy conocido. Afortunadamente, había algunos usuarios en el equipo de IT que podían acceder utilizando dispositivos con un sistema operativo diferente, con los que analizaron cuál era el problema. Una investigación inicial puso de manifiesto problemas críticos en el sistema operativo del servidor, que habían afectado a múltiples sistemas internos y portales de cuentas de clientes.

2

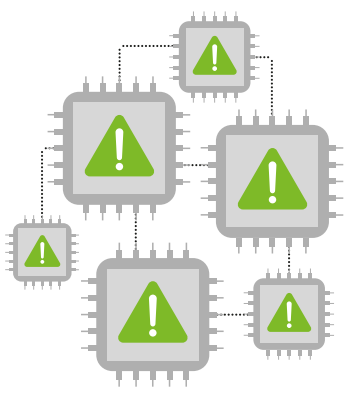
2. El problema

La Empresa 'Ejemplo' notificó el incidente en cuanto lo descubrió y contrató rápidamente a un Gestor de Respuesta a Incidentes, que clasificó el incidente basándose en los hechos iniciales. El Gestor de Respuesta a Incidentes recurrió a una empresa especializada en informática forense para ayudar a la Empresa 'Ejemplo' en la investigación. El Gestor de Respuesta a Incidentes también contrató a abogados y especialistas en relaciones públicas.

Ese mismo día, muchos medios de comunicación informaron de que empresas de todos los tamaños y sectores habían sido víctimas de un ciberataque, y que el problema parecía ir en aumento. Según varias informaciones, todas las víctimas parecían utilizar el mismo sistema operativo de servidor. Al día siguiente, los organismos públicos de ciberseguridad emitieron comunicados oficiales en los que explicaban que el ataque aprovechaba una vulnerabilidad de día cero en un sistema operativo específico, que se propagaba a través de un puerto de red informática de uso común y de cara al público. Como las aplicaciones dependen del sistema operativo, la funcionalidad de las aplicaciones en muchas empresas de todo el mundo se vio gravemente afectada, independientemente de la zona geográfica, el tamaño o el sector.

El equipo de respuesta a incidentes ayudó además con una estrategia de mitigación. El equipo de relaciones públicas elaboró cuidadosamente comunicaciones dirigidas a los clientes de la Empresa 'Ejemplo' para informarles de la causa de la interrupción del servicio. Los asesores jurídicos ayudaron a notificarlo a los organismos legales y reguladores pertinentes, y los especialistas de IT trabajaron para identificar posibles soluciones, utilizando sistemas operativos alternativos mientras esperaban la solución de recuperación del proveedor del sistema operativo y de los investigadores de seguridad.

3



3. La solución

En los días siguientes, investigadores de seguridad, organismos públicos de ciberseguridad y el desarrollador del sistema operativo publicaron información sobre el ataque y la vulnerabilidad. También proporcionaron consejos para las empresas que se habían visto afectadas por el incidente y medidas que debían adoptar todos sus usuarios, aunque aún no se hubieran visto afectados. El Instituto Nacional de Estándares y Tecnología ha catalogado esta vulnerabilidad como Vulnerabilidad y Exposición Común (CVE), con una puntuación base de 10,0, en vista de su grave potencial de impacto y su explotación. Se trata de la puntuación más alta del Sistema de Puntuación de Vulnerabilidad Común (CVSS), que solo se asigna a los incidentes «críticos». Los informes también detallan que el ataque se propagó a través de una herramienta integrada que buscaba puertos abiertos vulnerables y explotaba la vulnerabilidad del sistema operativo en todas las coincidencias positivas.

Se trataba de una vulnerabilidad de día cero porque era conocida y explotada por los ciberdelincuentes antes de que el desarrollador del sistema operativo conociera la vulnerabilidad y creara un parche. El evento fue generalizado porque el acto único repercutió en entidades y personas ajenas al grupo de impacto limitado de la Empresa 'Ejemplo'. El grupo de impacto limitado puede haber incluido a los clientes particulares y corporativos de la Empresa 'Ejemplo', porque los primeros utilizan el sistema operativo afectado y los puertos abiertos. Sin embargo, los informes de los expertos pusieron de manifiesto que este evento había afectado a muchas otras entidades que no tenían ninguna relación con la Empresa 'Ejemplo', por lo que estas partes quedaron excluidas del grupo de impacto limitado.

4

4. El resultado

La cobertura de respuesta al incidente, los costes de recuperación de datos y sistemas, así como la cobertura de seguro por pérdida de interrupción de negocio se activaron inicialmente en respuesta al incidente cibernético. Dado que en pocas horas se dispuso de información que demostraba que se trataba de un evento generalizado, el siniestro estaba sujeto al suplemento de eventos generalizados aplicable de la póliza. Los siniestros cubiertos por la cobertura de respuesta a incidentes, los costes de recuperación de datos y sistemas, y la interrupción de negocio se cubrieron hasta los límites disponibles para el evento generalizado, tras aplicar la franquicia y el coaseguro correspondientes.

Evento generalizado

- Interrupción global de una solución de software común

1

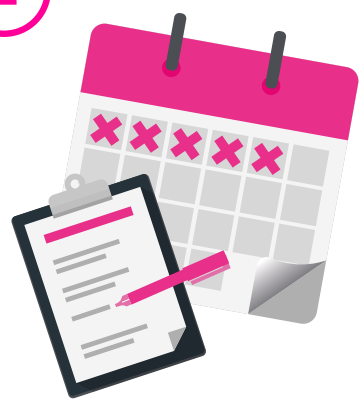
1. El evento

La Empresa ‘Ejemplo’ tenía sedes en el Reino Unido, Francia y Alemania. Sus centros de producción y ventas dependían, todas ellas, de una solución de planificación de recursos empresariales (ERP), basada en la nube de un importante proveedor de *software*. La solución ERP permitía procesar los pedidos de venta, gestionar el inventario, priorizar la producción, gestionar la logística y procesar las nóminas.

Hace dos semanas, la Empresa ‘Ejemplo’ actualizó su sistema ERP de la versión 2.3.2 a la versión 3.0, tras realizar una prueba de penetración y ejecutar la nueva versión en un entorno de pruebas para asegurarse de que no se producirían problemas de rendimiento derivados de la actualización.

La semana pasada, el sistema ERP se bloqueó, restringiendo el acceso de la Empresa ‘Ejemplo’. La Empresa ‘Ejemplo’ se puso en contacto con el equipo de atención al cliente del proveedor de *software* y descubrió que muchos clientes europeos se habían visto afectados por la interrupción. La Empresa ‘Ejemplo’ también se puso en contacto con el Centro de Respuesta a Incidentes Cibernéticos de Chubb para contratar a un Gestor de Respuesta a Incidentes y notificar el incidente al departamento de Siniestros de Chubb. En menos de dos horas, el proveedor de *software* publicó un aviso en su sitio web disculpándose por los problemas. Informaron de que estaban investigando un sistema comprometido en su entorno de producción, y recomendaron realizar comprobaciones periódicas para obtener más información y consejos de recuperación.

2



2. El problema

Al día siguiente, el proveedor de *software* envió un correo electrónico a sus clientes con una descripción de lo que debían buscar para comprobar si se habían visto afectados por el evento, así como con orientaciones sobre lo que debían hacer a continuación. El correo electrónico decía lo siguiente: «Si has estado operando con las versiones 2.3 de ERP o has actualizado a la versión 3.0 en las últimas tres semanas y estás experimentando problemas de accesibilidad, el problema ha sido causado por una actividad maliciosa en los sistemas de producción del servicio en la nube y estamos trabajando para recuperarlo».

La indisponibilidad del sistema ERP para la Empresa ‘Ejemplo’ duró cinco días. En este tiempo, registraron los pedidos manualmente por teléfono y correo electrónico, la producción continuó parcialmente a una capacidad significativamente inferior y las entregas tuvieron que interrumpirse porque no se podía acceder a los datos de los pedidos. Cuando el sistema estuvo finalmente disponible, todos los datos históricos sobre pedidos, inventario, estado de la producción y entregas se habían borrado y no podían recuperarse. El último aviso del proveedor de *software*, enviado por correo electrónico y publicado en su sitio web, confirmaba que el *malware* destructivo había corrompido los datos de producción de los clientes, así como las copias de seguridad. El aviso también detallaba que el evento había afectado a más de 30 000 clientes de ERP en Europa y ciertas zonas de Norteamérica.

3

3. La solución

Para determinar si las secciones de cobertura de evento de impacto limitado o evento generalizado se aplicaban a la póliza de la Empresa ‘Ejemplo’, necesitábamos evaluar quién se vio afectado por este evento y por qué. Las declaraciones realizadas por el proveedor de *software* indicaban que 30 000 clientes que utilizaban las versiones de ERP en la nube afectadas se vieron perjudicados debido a la presencia de código malicioso en los sistemas de producción del proveedor. Las demás empresas se habían visto afectadas no por su relación con la Empresa ‘Ejemplo’, sino por su elección del sistema ERP. Se habrían visto afectadas por este evento, aunque la Empresa ‘Ejemplo’ no fuera cliente.

4

4. El resultado

La información que indicaba que este evento estaba afectando a clientes de toda Europa se envió a la Empresa ‘Ejemplo’ a las dos horas de la interrupción, lo que supuso el primer indicio de que este evento era generalizado. Como resultado, se aplicaron los límites de eventos generalizados, franquicia y coaseguro a los importes de siniestro cubiertos. Esto incluía pérdidas contingentes por interrupción de negocio, costes de recuperación de datos y sistemas, como, por ejemplo, el coste de las soluciones manuales y los esfuerzos de recuperación de datos, los costes de los Gestores de Respuesta a Incidentes y el coste de contratación de terceros para gestionar las relaciones públicas y las comunicaciones con los clientes de la Empresa ‘Ejemplo’, que necesitaban volver a realizar pedidos o gestionar envíos atrasados.